Exam
Manual

LearnSmart

CompTIA (SY0-301)
Security +

This LearnSmart Exam Manual breaks down the most important concepts you need to master in order to successfully complete the CompTIA Security+ (SY0-301) exam. By studying this guide, you will become familiar with an array of exam-related content, including:

- Network Security
- Compliance and Operational Security
- Threats and Vulnerabilities
- Cryptography
- And More!

Give yourself the competitive edge necessary to further your career as a security professional and purchase this exam manual today!

Security+ (SY0-301)
LearnSmart Exam Manual

Product ID: 13079
Production Date: November 21, 2011

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

1-800-418-6789
solutions@learnsmartsystems.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Abstract

Congratulations on your decision to enhance your career prospects by adding the CompTIA Security+ certification to your resume! Having a list of top-notch certifications on your resume is bound to make potential employers think to themselves, "This person has the skills, knowledge and motivation to get the job done!" Security is important – this point cannot be overstated. According to a 2010 Web Security Statistics report, the average website had nearly thirteen serious vulnerabilities and industries with a greater number of vulnerabilities yielded the lowest remediation rates. Therefore, since we keep our homes secure, we must keep our networks secure.

A vendor-neutral entry-level credential that demonstrates the candidate's understanding of concepts relative to Information Security in the workplace, the CompTIA Security+ certification paves the way for experienced professionals seeking careers as security architects, security engineers, security consultants, information assurance technicians, security administrators, systems administrators, or network administrators – and considering how rapidly technology evolves and presents new security risks and concerns, these careers aren't going away any time soon. According to CompTIA's website, companies that favor Security+ professionals include Hitachi Information Systems (Japan), Trend Micro (Philippines), Lockheed Martin, the U.S. State Department, Prestariang Systems Sdn. Bhd. (Malaysia), and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman. In addition, CompTIA Security+ is an ideal certification for military personnel or military contractors at the U.S. Department of Defense.

The CompTIA Security+ (SY0-301) exam is tough – there is no need to pretend otherwise. Focusing on prevention and detection, the new exam has been updated to include more coverage of operational security, risks and cryptography. That's why proper training and preparation are not optional: they're absolutely essential. This LearnSmart Exam Manual will help you prepare for the exam, which you must pass in order to earn your CompTIA Security+ certification. To ensure that you get the most out of this exam manual, it has been organized to reflect the actual format of the exam. In other words, the material covered in each chapter reflects topics and objectives tested in a particular domain.

In addition, you'll notice that at the end of the manual, there are review questions designed to test your ability to recall important concepts and terms. Being able to correctly answer these questions (as well as taking practice exams that mimic the format and breadth of the actual exam) is a good indicator that you'll succeed on the CompTIA Security+ (SY0-301) exam.

About

As mentioned, the CompTIA Security+ designation is achieved by passing one exam that covers a range of Information Security topics such as network security, compliance, threats and vulnerabilities, host security, identity management, cryptography, and more. The exam can be taken through an authorized testing center, such as Pearson VUE or Prometric . As of August 2011, the exam costs $266 USD per attempt. Currently, the exam consists of 100 multiple-choice questions that the candidate must answer within 90 minutes, achieving a passing score of 750 out of a possible 900.

CompTIA's Security+ certification is aimed towards IT professionals who possess the following:

- Two years of experience in an IT administration role, with a focus on security.
- Day-to-day experience dealing with information security issues and solutions.
- Broad knowledge of security terminology, risks, vulnerabilities, threats, and countermeasures as defined in the next section.

This certification is well-suited to network and security administrators independent of the industry they work in. The CompTIA Security+ certification also serves as a great stepping-stone to more advanced certifications, such as the (ISC)² SSCP and CISSP, and the SANS GIAC. In addition, the Security+ credential is recognized as an elective credit towards some Microsoft certification tracks. The Security+ certification is valid for three years from the date of issue and can be renewed by either re-testing, or maintaining the required continuing educational units (CEU) and paying an annual fee.

This LearnSmart Exam Manual includes the information that candidates need to pass the exam, and addresses the challenges that organizations face when deploying and supporting technologies in their environment. This manual is structured to follow the six Information Security domains as defined by CompTIA:

- Network Security
- Compliance and Operational Security
- Threats and Vulnerabilities
- Application, Data, and Host Security
- Access Control and Identity Management
- Cryptography

Study Tips

As when taking any exam, preparation is everything. In most cases, reading only one book will not sufficiently prepare you for an exam as challenging as the CompTIA Security+ (SY0-301) exam. Therefore, in addition to knowing all aspects of the information presented in this manual, you will want to take advantage of all the other resources and exam preparation materials at your disposal.

For example, online video training allows you to customize your learning experience and absorb information at your own pace. You can watch video chapters as many times as necessary to understand particularly difficult concepts. Of course, unless you are especially good at retaining information you gather in a lecture environment, watching a video may not be enough.

While watching your video training course, you should refer to the exam manual and/or a concise glossary that defines security-related terms. As when learning the vocabulary and nuances of a foreign language, you want to cover all your bases and make sure your security vocabulary is rich and varied. You want to know, for example, that a worm in this context doesn't refer to an earthworm found in your backyard, so make sure you understand that every term's context is vastly different from most others. Along the same vein, take note of all unfamiliar terms. Even the most experienced security professionals may encounter terms with which they are unfamiliar. Once you become familiar with these terms, consider making flash cards and testing how many of them you can correctly identify.

Another effective way to prepare for the CompTIA Security+ (SY0-301) exam is to take as many full-length practice exams as possible. Practice makes perfect, right? Taking practice exams enables you to measure your progress, as well as grow familiar with the physical environment of the actual exam – in particular, the length of time and number of questions. Simulating the exam environment beforehand will prevent you from experiencing shock or panic on exam day when you realize you don't have the advantage of taking coffee breaks or referring to your exam manual or video training course.

With that in mind, when taking the actual exam, manage your time well. You should have more than enough time to complete the exam, but don't spend too much time on any one question. If you get stuck, return to the question at the end of the exam. If you're sufficiently prepared, you'll encounter many questions that seem easy. You want to make sure that you have time to answer all of the questions – easy and difficult – on the exam.

Because the questions on the Security+ (SY0-301) exam are multiple choice, try to eliminate two of the possible choices. That way, if you have to take a guess, you can base your guess on the answers that are most likely to be correct. If you get stuck on an answer, mark it and come back to it later on. You may be able to use some of the other exam questions to figure out the answer that you are stuck on. If you still can't figure out a question, don't be afraid to guess. If you completely skip a question, that question is scored as if you answered it incorrectly. If you guess at an answer there is at least a chance that you could get the answer right.

Domain 1 – Network Security

Every network is unique, and architecturally defined physically by its equipment and connections, and logically through the applications, services, and industries it serves. Network infrastructures can be complex, and ensuring that the appropriate security controls are in place can be an involved process. While organizations must be able to conduct business efficiently and effectively, they must also be able to do so in a secure manner. Remember, leaving a network carelessly unsecured is like leaving the front door unlocked at night.

That being said, it can be challenging for both businesses and security professionals to balance the needs of the business with that of security. Security professionals need to recognize that the impact to business processes must be minimal – which is to say, integration of security controls should be as seamless as possible.

Naturally, achieving seamless integration can be challenging: each device, connection, protocol, and interface comprising a network carries its own set of concerns and considerations that security professionals must be able to recognize, communicate, and address when implementing the security solutions that will protect the network from intrusions, data loss, and outages.

Security Functions and Purposes of Network Devices and Technologies

Firewalls

Firewalls are an integral part of an organization's overall network security strategy and are often the first line of defense when protecting against threats that originate from the Internet. Right now, you may be picturing a tall brick structure in flames, but in this context, a firewall is an **appliance** or software package that logically segregates public and private networks, and monitors the traffic that is transmitted between them. Remember that firewalls monitor traffic travelling in both directions – into a network (**ingress**) and out of a network (**egress**). Also, firewalls may be deployed to protect internal sub-networks within a larger network scope. To identify which traffic should be allowed or denied, firewalls utilize rule sets and other traffic filtering mechanisms. **Figures 1 and 2** show how firewalls operate within an internal network and throughout a larger network, respectively.

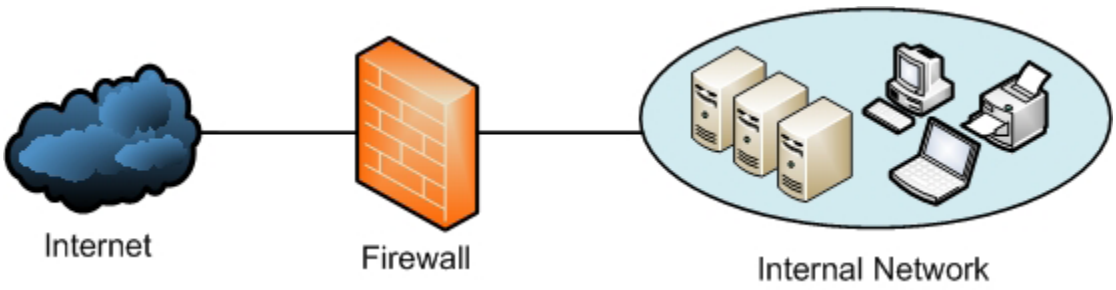

Figure 1: Internet facing firewall deployed at the network perimeter

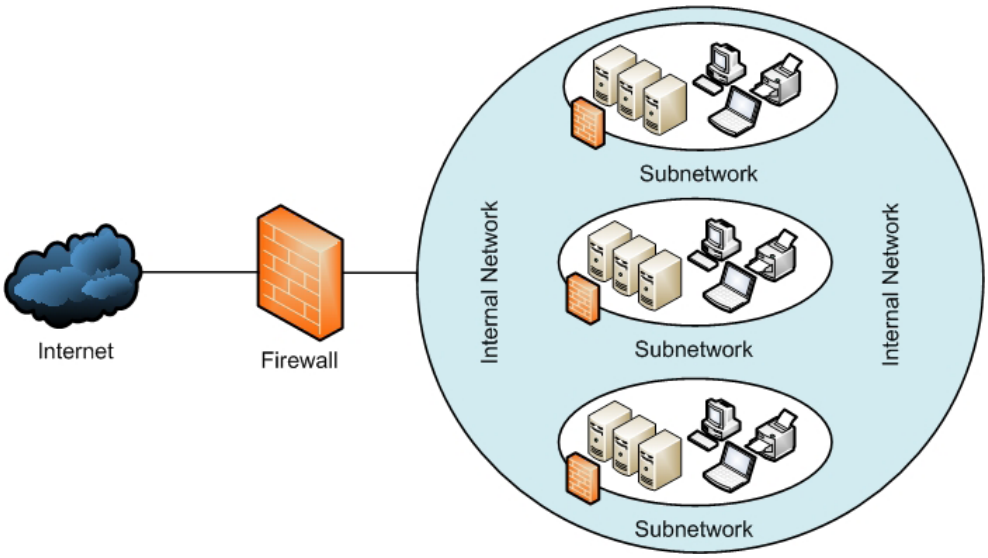

Figure 2: Firewall deployment throughout a network

Since their inception, firewalls have evolved significantly with respect to how they function, what platforms they support, and their placement on a network. Modern firewalls perform a deep packet analysis of network traffic by combining application filtering and intrusion prevention technology into a single unit. Due to the advancements seen in the latest threats, firewalls are frequently deployed on internal networks and to workstations and servers – not just to the network perimeter.

Packet Filtering Firewall

The first generation of firewalls employed **packet filtering** as a security control to monitor network traffic. Packet filtering firewalls operate at the first three layers of the **OSI model** (Physical, Data-Link, and Network layers) and determine whether the packets should be allowed or dropped by comparing the information contained in pre-defined rule sets to the information contained in the packet. Bear in mind that most routers are also capable of packet filtering.

Figure 3: The OSI Model

The **rule sets**, or **access control lists** (ACLs), are typically configured to make a decision about the packet by analyzing packet headers for source and destination addresses, protocols, ports (TCP/UDP), or a combination thereof. In other words, like a person waiting in line to enter an exclusive club, the packet is examined from top to bottom, and then accepted or denied.

While packet filtering firewalls perform well, are scalable, and can restrict the flow of traffic, they are susceptible to attacks that exploit vulnerabilities in applications, and are unable to detect network packets that contain forged (spoofed) network addresses.

Application Filtering Firewall

The second generation of firewalls provided a means of filtering content in network traffic by operating at layers one through seven of the OSI model. **Application filtering firewalls** examine the service being requested (web, DNS, FTP, etc.), port usage, and the input and output commands being called. **Application firewalls** are often implemented in a proxy or reverse proxy configuration and require pre-defined rule sets or an ability to "learn" what is considered "normal" behavior for an application. This process is often referred to as **baselining**. Application filtering firewalls are effective at stopping peer-to-peer network traffic and are a key component used in Next Generation firewalls.

Stateful Firewall

Stateful firewalls are considered the third generation of firewall, and use **stateful packet inspection** to restrict the flow of traffic between hosts. Stateful firewalls maintain a state table to record communication sessions. The state table is checked for an existing connection when a packet is received. If the state table doesn't contain any connections relative to the information in the packet, then the packet will be compared against the firewall's ACL to determine if a new connection should be allowed. Stateful firewalls operate at layers one through four of the OSI model.

Next Generation Firewall (NGF)

Next generation firewalls are the newest type of firewall. Vendors and security analysts have rapidly adopted this term. Next Generation firewalls attempt to combine some of the most popular network perimeter security controls into a single system. Often, this combination results in the pairing of an application filter and an **intrusion prevention system (IPS)**. Each vendor's offering in this space differs, and some solutions also include inspection of URL content and malware identification.

Dual-Homed and Multi-Homed Firewalls

A **dual-homed firewall** has two network interfaces: one for the external network, and the other for the internal network. On the other hand, a **multi-homed firewall** can contain multiple interfaces for both internal and external connections which are often used to define an organization's **demilitarized zone (DMZ)**. DMZ segments are used to allow Internet facing services—such as e-mail, DNS, servers, and more—to exist without exposing the internal network. **Figure 4** illustrates this particular configuration.

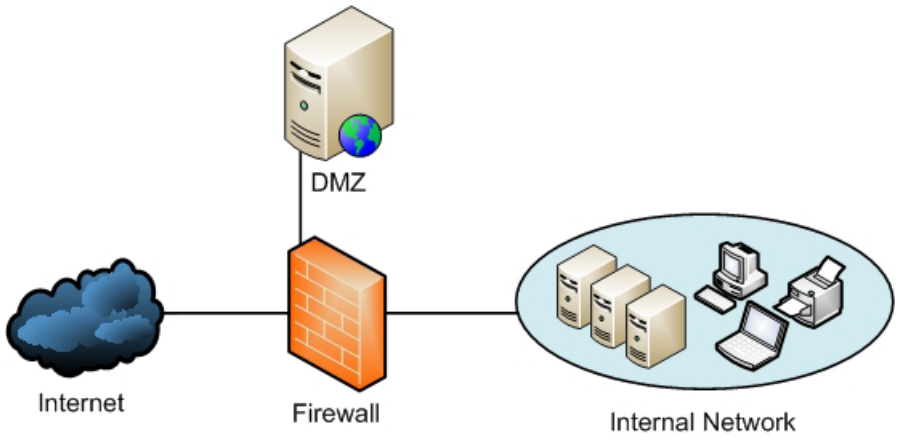

Figure 4: Standard Demilitarized Zone (DMZ) configuration

Screened Subnet

A **screened subnet** is defined by a configuration where all external traffic is first passed through a router and then to a firewall. If the traffic is destined for hosts on the internal network, it must first pass through another firewall. **Figure 5** shows how a DMZ is typically configured as a screened subnet.

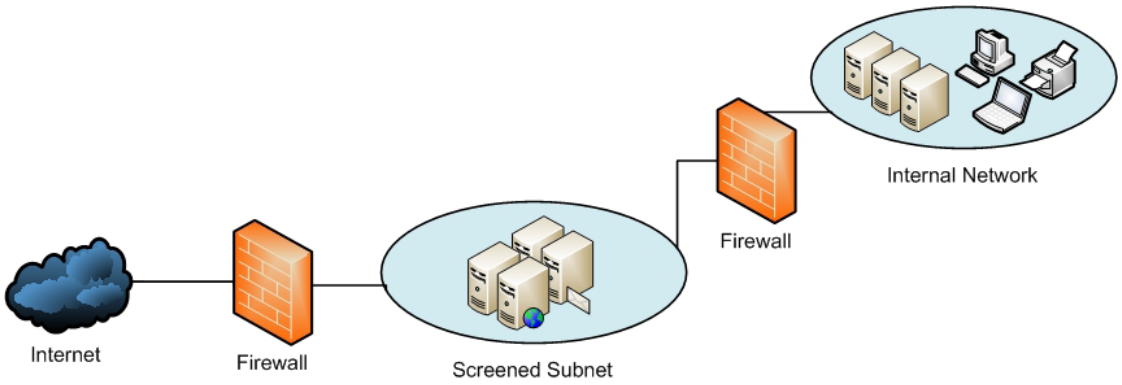

Figure 5: Standard Screened Subnet configuration

Routers

Network **routers** are packet-switching devices with enhanced traffic-handling capabilities. While switches are used primarily to join local network segments, routers establish connectivity between public and private networks (or among separate private networks). A router communicates in network-layer (OSI layer 3) protocol packets and multi-protocol routers translate between several different network protocols. Also, routers forward packets based on source and destination IP addresses and may provide basic security through ACLs.

Routers are often used in combination with a firewall (especially on an Internet-facing connection). Some routers include a firewall or firewall capabilities. Routers can also perform **network address translation (NAT)**, which hides the addresses of systems behind the router from the systems that establish connections through the external interface of the router. The router replies to those connections with an address that is unique to the router. Using routing tables, the router is able to forward traffic to the proper destination.

Unlike firewalls, routers are not devices that are dedicated to security, and several hardening guidelines should be followed when adding a router to a network. Special attention should be given to Internet-facing routers, wireless routers, and wireless access points as they are more exposed than routers on an internal network or those that are connected only by physical cables. Both NAT and securing routers are discussed later in this manual.

Switches

Network **switches** operate at OSI protocol layers one and two (and sometimes layer three) devices that connect separate computers and network segments. Switches come in different shapes and sizes, ranging from compact four-port Ethernet units to enterprise-class 48-port Gigabit Ethernet designs.

Network traffic is delivered directly between sender and recipient since switches forward frames based on MAC address. Unlike hubs, which broadcast all traffic on all ports, switches reduce network traffic by only delivering traffic to the port on the switch that the host is connected to. Switches are able to deliver in this way because they maintain a table that maps device MAC addresses to switchport numbers.

More modern switches, also known as multilayer switches, can inspect packets, prioritize traffic, perform routing, serve as load balancers, and add Quality of Service (QoS) functionality to network traffic.

Also, network switches are capable of creating **virtual LANs (VLANs)** to enhance corporate network administration and security. A VLAN is a logical grouping of systems whose deployment can be driven by security, business, or resource requirements instead of physical location.

Unfortunately, switches can be vulnerable to numerous types of attacks like **MAC spoofing**, **MAC flooding**, **ARP spoofing**, and **Denial-of-Service (DoS)**. Switches and VLANs need to be properly configured to defend against these attacks.

Load Balancers

Load balancers are primarily available in two different forms, hardware and software, and can vary greatly in terms of the services they provide. Another type of load balancing is **round robin DNS**. Round robin DNS does not require dedicated hardware or software and works by assigning multiple IP addresses to a single **fully qualified domain name (FQDN)**.

The primary benefit of a load balancer, as the name would suggest, is to distribute the load between multiple systems, networks, or devices so that a single entity that is providing a resource is not overwhelmed. Load balancing also adds redundancy in the event a system fails.

There are other benefits as well. Load balancers are a frequent requirement in a business continuity plan, and serve as a compensating control that allows services to continue to be available should one of the resources behind the load balancer fail due to attack or an outage. Load balancers can serve as an effective control against **Denial of Service (DoS)** attacks targeted at resources connected to the load balancer.

Implementing redundancy behind load balancers (e.g., clustering) further expands on the benefits gained by deploying a load balancing solution.

Proxies

A **proxy server** services requests by playing a middleman role, brokering deals between client and server. By nature, the proxy evaluates connection requests against administrative rules and may selectively filter traffic matching certain criteria or conditions. Proxies keep internal machines hidden and anonymous and enhance network performance by caching commonly-requested resources. Proxy placement may be at individual workstations or centralized at a gateway server.

Reverse Proxy

Reverse proxies receive requests from external sources, such as the Internet, and forward those requests to systems dedicated to handle them. Reverse proxies provide a layer of defense by concealing systems on the internal network and responding on their behalf. The most common deployment for a reverse proxy is on an Internet-facing segment that serves web pages or applications to users on the Internet.

Application firewalls are often implemented in a proxy or reverse proxy configuration.

Web Security Gateways

Web security gateways are a critical component used to protect systems from Internet-based attacks and enforce corporate security policies on a network. Because web browsers that are outdated or don't have current security updates installed can pose a serious security risk to a network, web security gateways serve as a key component in a defense-in-depth, residing at the Internet Gateway in an organization. Essentially, to address potential risks, they filter inbound and outbound web traffic, malicious code, unacceptable content, and application usage.

Most web security gateways are available as appliances and offer several modules that can be licensed together or individually. While the primary purpose of a web security gateway is to filter web traffic for content and malicious code, they can also detect and take action on applications (e.g., instant messaging), enforce e-mail security controls, prevent data leakage, and more. Web security gateways can also serve as an effective defense against drive-by downloads and zero-day/zero-hour threats that originate from the Internet. Drive-by downloads and drive-by installations are downloads or installations of programs that occur on a user's system without his or her consent.

Virtual Private Network (VPN) Concentrators

Virtual Private Networks (VPNs) provide a secure way for remote users to connect into a company's internal network over the Internet. VPNs can also be deployed to create connections between organizations or remote offices. Offered by multiple vendors and differing in feature set model by model, **VPN concentrators** are commonly deployed where a network needs to support a substantial amount of incoming VPN connections. VPN concentrators are available in both a SSL and IPSec configuration, and a few vendors offer support for both. Higher end VPN concentrators are capable of encrypting the entire session and then destroying the data once the session terminates. Some VPN concentrators incorporate firewall technologies and can permit or deny access based on a health check of connecting systems (e.g., anti-virus, security patches). VPN concentrators can also provide remediation options for discovered issues.

Network Intrusion Detection System (NIDS)

Certain network attack sequences leave traceable patterns that become scanning engine "signatures" used to detect further occurrences of attack. A **network intrusion detection system (NIDS)** identifies malicious network activity by matching signatures against observed traffic. NIDS identifies Denial of Service (DoS) attacks, port scans, invalid connection requests, malware behavior, and more. When these items are identified, the NIDS alerts administrators so that the incident can be investigated.

Network Intrusion Prevention System (NIPS)

A **network intrusion prevention system** performs the same duties as NIDS but with a more active role: instead of alerting administrators (like NIDS) the NIPS takes immediate action. Upon detection of a certain attack or suspicious traffic pattern, the NIPS will take some predefined action against the event—such as closing the connection, issuing firewall block rules against the host, and so forth. No human interaction is required to stop the attack.

Protocol Analyzers (Packet Sniffers)

Network protocol analyzers or **packet sniffers** set a workstation's network interface into **promiscuous mode,** which is a more permissive state allowing the network stack to process packets destined for other computers—packets normally filtered out by the NIC. The sniffer serves as a viewfinder into network traffic patterns and protocols enabling administrators to observe private conversations, sensitive transactions, and special relationships between other computers for investigatory or troubleshooting purposes. In the wrong hands, however, protocol analyzers can permit eavesdropping and interception of sensitive protocol transactions.

Anti-Spam and E-Mail Hygiene

Here, we're not talking about preparing strange dinner meat or soaping down your in-box. Rather, spam, phishing, scams, and messages with malicious code attached are unsolicited e-mail messages and are dynamic problems of exponential proportion because of the free accessibility and cost of sending electronic messages, which is very inexpensive and sometimes free. The unsolicited e-mail problem has now spanned other technological divides to include phone-based text message spamming and Voice over IP (VoIP) systems.

Regulatory compliance and best practice drive most companies to include a data loss prevention mechanism in their messaging infrastructure. In addition, messaging systems can include a secure e-mail program that reroutes and encrypts messages meeting certain pre-defined criteria.

Current **e-mail filtering solutions** can use a variety of methods to prevent the delivery of unsolicited messages and ensure delivery of legitimate ones. Most offerings include black listing (blocked), white listing (approved), heuristic analysis, malware scanners, content-filters, Bayesian analysis, reputation scoring, address harvesting prevention, and DNS reverse lookup (Sender ID, SPF), and leverage the cloud to identify zero hour/zero day spam attacks.

E-mail filtering solutions are available in both hardware and software versions and are most effective when placed closest to the source of the messages to be filtered. For example, filtering e-mail from the Internet should be implemented at the gateway, and filtering of e-mail messages created by internal systems should have a filtering program running on the first mail server they establish a connection with.

All-In-One Security Appliances

All-in-one security appliances combine the most common and critical security controls that organizations often deploy separately at the Internet gateway. These appliances can be customized to the needs of the environment by licensing the different modules together (hopefully at a better price) or separately. Some of the solutions that security appliances can provide include combined firewall, IPS, IDS, e-mail filtering, web filtering, malware scanning, VPN support, and more.

Web Application Firewalls versus Network Firewalls

Web application firewalls serve a specific role in protecting web-based applications that are accessed by users who reside on the Internet. Web filtering firewalls provide countermeasures that network firewalls don't, and vice versa. Web application firewalls monitor web traffic that is destined for a web server by scanning for SQL injection attacks, cross-site scripting, vandalism, and other malicious code. Web application firewalls are also capable of learning how the application should operate as well as validating user input and sanitizing output.

In order for an organization to be PCI compliant, companies that process credit card transactions over the Internet need to either deploy a web application firewall or complete a vulnerability assessment of the web application's environment.

The **Open Web Application Security Project (OWASP)** certifies web application firewalls that meet or exceed specific requirements.

Internet Content Filters

An **Internet content filter** constrains various types of information that is permitted into a network, often through web browsing, by using filters that scan web traffic for keywords, hostnames, URLs, and malware, to prevent access to unsavory or malicious material. As there are no restrictions on what is permitted on the Internet, individuals and organizations are able to set their own policies to control and restrict content delivery to end-users using content filters, especially where material is of objectionable or questionable nature.

Web security gateways, all-in-one security appliances, and host-based solutions are available to address the risks that are associated with accessing content hosted on the Internet.

URL Filtering

Uniform Resource Locator (URL) filtering examines hyperlinks and URLs for keywords, malicious code, and commands. URL scanners often use reputation services and access the content in a sandboxed environment to determine if the payload of the resource being requested is malicious in nature. A plug-in is often needed to examine tiny or short URLs, a technique often used by attackers.

URL filtering is often used by both web and e-mail scanning engines.

Content Inspection

Content inspection filters examine the content displayed in web pages for content deemed unacceptable, unrelated, or sensitive to an organization's business. Organizations often implement a content filter to prevent access to specific content and as a data loss prevention control.

Malware Inspection

Malware inspection or **malware scanning engines** examine web content and files being downloaded from, or uploaded to, the Internet for malicious software. Filtering for malware at the Internet gateway in addition to host-based malware scanning increases the level of scrutiny that web traffic is under, and is strongly recommended as a part of an overall defense-in-depth strategy.

Apply and Implement Secure Network Administration Principles

Rule-Based Security Management

Rule-based security management typically defines the scope of what type of activity should be permitted on a network. Systems that use filters or rule-driven controls to monitor and enforce security policies on communications and IT-related activities support this design. Firewalls, web filters, e-mail filters, IPS/IDS, and proxies are examples of systems that implement a rule-based security model. Rules either allow or explicitly deny an action to occur, and if there is no match in the rule set for the activity, then it should be implicitly denied, meaning the last rule in the set should have a default action of denied.

Firewall Rules

Rules used by a firewall should follow the concept of deny all unless intentionally allowed, by configuring the action of the last rule in the set to block or deny-any. This rule is dedicated to dropping traffic that didn't meet the criteria in the defined rule set. Not only is this design the most secure, but it also provides an effective discussion point for needing to validate the business requirements that require a new rule or change in the existing rule set.

VLAN Management

As discussed earlier, switches create VLANs in order to create a logical grouping of systems that can be driven by security, business, or resource requirements instead of physical location. Preventing access to other VLANs or network resources is defined by creating a specific deny function or simply removing or avoiding the creation of unwarranted routes. Administering this configuration is known as **VLAN Management**. Some switches include a VLAN management solution that gives administrators visibility and control over their VLAN environment.

Secure Router Configuration

Routers, as mentioned, are not security devices, and while current routers may include some firewall technologies like port-blocking and packet-filtering, routers are vulnerable to attack and need to be configured in a secure manner prior to deployment on a network.

Some of the most common configuration steps employed when securing a router are to provide a unique name for the device, assign a password (and encrypt it if possible), define IP addresses and ranges, disable unnecessary ports, backup and document the configuration, and block ICMP redirect traffic. Blocking ICMP redirect traffic serves as a preventive security control against the ping of death, ICMP floods, and other attacks that leverage the ICMP protocol.

Wireless routers and wireless access points may require additional steps, and are covered later in this manual.

Access Control Lists (ACL)

An **access control list** forms the most basic security checklist against which permitted accesses and actions are evaluated. ACLs define which actions a subject may take when accessing, creating, executing, or modifying a given object (e.g., applications, data, processes, services). Administrators define basic permission schemes that determine how users interact individually or collectively with a protected resource.

Typically, access control lists are derived by leveraging the information defined in mandatory access (security labels), discretionary access (group membership), role-based (job function), or rule-based (actions) access models. Numerous technologies ranging from file/folder permissions to firewalls maintain access control lists to prevent unauthorized access to resources.

Port Security

Port security falls under two categories based on the OSI model: physical and network. **Physical port security** might encompass things like Ethernet jacks and USB ports, whereas **network port security** primarily addresses port usage by the TCP and UDP protocols.

Physical port security, as with network jacks, can be unplugged from the patch panel when not in use, or enabled using MAC address recognition. Blocking physical USB ports on a local system can be implemented using physical plugs, BIOS settings, or device control software. Most device control products allow the use of permitted devices only, providing a nice balance between business requirements and security needs.

On the other hand, **network ports** are frequently monitored by firewalls, and unused ports are often closed. However, of the 65,535 ports available, a fair amount of the most commonly used ports (0-1023) are often open. Attackers commonly use port scanners to determine which ports are available on a network and what services are allowed on them. Ensuring that only ports necessary to support the business are in use, and rules are implemented to match only the required traffic flow to and from those ports, increases a network's security posture greatly.

Port knocking is a technique that treats all network ports as closed until a connection on that port is requested. At that point, the firewall rules are automatically modified if the connecting system transmits the correct sequence in the connection string, or supplies an encrypted packet.

802.1x

802.1x is an Institute of Electrical and Electronics Engineers (IEEE) port authentication standard that controls access to the network and can serve as an effective means for preventing network access by rogue systems. The inception of 802.1x arose because of the vulnerabilities discovered in Wired Equivalent Privacy (WEP), and is now frequently used with RADIUS systems, network access control (NAC), network access protection (NAP), TACACS+ and others.

802.1x encapsulates Extensible Authentication Protocol (EAP) packets in Ethernet frames for transmission over wired and wireless networks, without using the Point-to-Point Tunneling Protocol that EAP was originally designed to work with. EAP is a method of providing several different means of authentication (e.g., token IDs, digital certificates, user ID/password) when network connections are made. Also, 802.1x can be configured to create an encrypted tunnel to pass credentials between the device and authentication server.

Known as supplicants, devices wishing to connect to the network are first directed to an authenticator where credentials will be provided (e.g., digital certificate or user ID/password set). The authenticator forwards the credentials to the authentication server where the they are validated, and access is either granted or denied.

Flood Guards

A **flood guard** can be a standalone device or a component of a firewall and is implemented to detect and prevent denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks that are generated by flooding the network with packets. Specific examples of these types of attack include SYN flood, ICMP flood, MAC flood, UDP flood, and Ping flood. All of these attacks attempt to overwhelm the target system with network requests with the goal of disrupting services or taking them offline altogether.

A flood guard acts as a preventive control by monitoring network traffic to recognize when a DoS attack is underway due to flooding, and then takes action by dropping the packets and/or implementing the necessary filtering rules on routers and switches.

Loop Protection

Looping, in network terms, is when transmissions repeat and consume bandwidth unnecessarily. Attackers can take advantage of looping to cause denial-of-service (DoS) attacks as they can be quite a disruptive technique. Looping can be combated by enabling the spanning tree protocol (STP) on the switches in a network. Bridges also support the use of STP. The STP records the network paths available and then makes pre-defined decisions about the active and standby routes, eliminating the ones that could allow looping to occur.

Implicit Deny

An **implicit deny** security stance views all things as suspicious that aren't specifically and selectively deemed permissible. An open network computing environment where anyone or anything may connect implicitly allows traffic, whereas a safeguarded network boundary that only permits certain IP addresses and/or service ports and blocks everything else implicitly denies traffic. Traffic that is blocked to certain ports or from specific addresses is said to **explicitly deny**.

This concept ("deny all unless specifically allowed") can be applied to most information security concepts.

Prevent Network Bridging by Network Separation

Network bridging, while useful in some scenarios, can introduce operational problems and introduce security risks on a network. Network bridging can degrade network performance overall as it does not localize broadcasts and can create loops. One of the most undesirable and yet common types of network bridging is established when a laptop is connected to both a wired and wireless network. This connection creates a security concern as traffic could move from one network to the other.

Two effective ways of **preventing network bridging** are separating networks and configuring Ethernet ports to disconnect if bridging is detected on a host machine. As mentioned earlier, VLANs can be defined in switches to create logically isolated networks, firewalls routers, and physical separation of networks can also be effective solutions in **preventing network bridging**.

Log Analysis

Analyzing logs is an important task that security professionals must undertake. Ensuring that systems are generating logs can not only help with troubleshooting, but also with security incidents, audits, and investigations. Analyzing logs for security events can be a tedious task, especially when reviewing multiple logs on multiple systems that reside in numerous locations, as with during an audit or investigation. Some systems, like a network intrusion detection system (NIDS), work by analyzing logged data to identify threats.

Security Event Managers (SEM) and Security information Event Managers (SIEM)

Security Event Managers (SEM), also known as Security Information Event Managers (SIEM), were introduced as a component that could store, analyze, and mine information from multiple logs that exist on multiple systems across a network. SIEMs create a local copy of the logs they receive and can provide a forensically-sound archive of logged information (even if the original log is destroyed), can identify similar events in multiple log files, can send alerts based on its findings, and can include an interface for scouring data in the logs efficiently.

Distinguish and Differentiate Network Design Elements and Compounds

Demilitarized Zone (DMZ)

A network's demilitarized zone (DMZ) is the dividing line between a public and private network. In most arrangements, the DMZ establishes a physically separate buffer and containment area for public-facing private company servers such as web and FTP servers. This portion of the network is kept separate from the protected internal network, providing a compromise between offering public services and operating private servers without fully exposing private networks to high risk or hostile environments.

Subnetting

A **subnetwork**, or **subnet**, is a compartmental collection of designated layer three IP addresses that corresponds to end-user computers, gateway devices, company servers, and other intermediary devices and network endpoints. **Subnetting** is the process of logically dividing a network into classes of smaller networks to prevent Ethernet collisions and address assignment conflicts.

Subdivided networks can be individually guarded by firewalls and granted different access rights and network permissions according to job functions. Common classes include Class A, Class B, and Class C subnets that all correspond to increasingly smaller sizes of network segment.

Virtual LAN (VLAN)

The **Virtual Local Area Network (VLAN)** is a logical network arrangement that logically segments a single physical switched network into multiple logical networks. Actual LAN segments that comprise the VLAN may be spread across a campus, city, or different regions or territories throughout the country. A single organization may employ multiple individually-protected VLAN broadcast domains (i.e., Human Resources and Data Entry departments) to isolate cross-contaminations (such as virus and worm outbreaks), separately manage departmental groups, and so forth.

Network Address Translation (NAT)

An organization may share a single public external (Internet) connection among several internal computers using **network address translation (NAT)**, which is a one-to-many mapping of public-to-private IP address spaces. While it is possible to deploy NAT for a one-to-one mapping, it is most commonly used for one-to-many mappings. NAT reduces the need for several public IP addresses through an ISP by establishing an administratively-defined address pool mapping the internal network and repackaging those connections as a single source (usually centralized at a gateway or router device) without exposing those internal endpoints to the Internet.

Note: As defined in RFC 1918, the Internet Assigned Numbers Authority (IANA), has reserved the following routable IP address ranges for use on private Intranets: 10.0.0.0 - 10.255.255.255 (16,777,216 addresses) 172.16.0.0 - 172.31.255.255 (1,048,576 addresses) 192.168.0.0 - 192.168.255.255 (65,536 addresses).

Remote Access

Remote access is a popular technology for employees and maybe even more so for administrators. The convenience of connecting to networks remotely can be considered invaluable. Remote access solutions are available in a variety of implementation options. Some examples would include remote desktop / terminal services (Windows), virtual private networks (VPN), or even dial-up.

Regardless of the remote access solution chosen, measures to protect the remote access servers must be implemented as their purpose is to provide access to resources on the internal network. Since RAS systems are often publicly accessible, they need to be hardened and are important systems to audit.

Remote Access Servers (RAS)

Remote Access Servers (RAS) are systems that allow you to connect to a server, usually via modem from the Internet, to be authenticated and granted access to internal network resources.

Remote access servers enforce policies (RAS policies) on connecting systems to mandate that certain requirements are met and the communication session operates within specific parameters. Some examples would include restricting time (availability, timeouts, and session length), enforcing the use a specific authentication mechanism, and more. RAS Policies can also direct the network traffic to travel along a specific route. Since RAS servers are usually placed in the DMZ, the next device in the route should be a firewall.

Telephony

Telecommunications or **telephony** encompasses the general use of phone equipment to provide voice communications over great distances. Telephony transmits and translates analog voice information to digital voice formats to provide long-haul connections for human communication. As a catchall term, telephony includes digital computers, wireless phones, and voicemail systems.

Network Access Control (NAC)

Network access control is a networking security strategy and solution that attempts to validate the presence of functioning security controls on the connecting system (e.g., virus protection, operating system, personal firewall, service packs) prior to allowing access to the network. NAC also defines user or system authentication (e.g., 802.1x) and network security enforcement procedures.

A significant usage of NAC is to enforce system health requirements that are checked upon accessing the network: systems deemed "unhealthy" (outdated anti-malware signatures, missing security patches) are administratively prohibited to connect or directed to a resource (e.g., Intranet Web site) that can help them resolve the discovered issues like downloading security updates or installing malware definitions. Once the issues are mitigated, the user can attempt to reconnect to the network.

Virtualization

Virtualization is another popular technology that provides great flexibility and added value when designing a data center, consolidating systems, creating business continuity procedures, testing new technologies, and more. Virtualization hardware or software allows for the creation of multiple (virtual) operating systems, known as guests, on a single physical device known as a host.

While the logical systems reside on a single physical system, they run in their own logically segmented memory space and in many ways, act independently of the host. Both the physical system and guest systems should be configured in a secure manner and guests need to undergo the same scrutiny as their physical host (e.g., virus protection, patch management, personal firewall).

Some security products include the ability to protect certain components of the virtual environment, like the prevention of terminating virtual machine processes.

Cloud Computing

Cloud computing refers to an environment where all applications, data, and processing occur on a hosted server or network of servers that reside on the Internet or in a privately owned network cloud. Cloud providers are vendors that provide this service and users normally do not need to install any software on their devices.

Cloud computing has its benefits in that all servers, operating systems, infrastructure, and issues are the responsibility of the cloud provider. Further, cloud providers offer centralized (off-site) data storage, and cloud-hosted solutions typically include redundancy, load-balancing, and failover. These examples can prove to be valuable when developing business continuity and disaster recovery plans. Relieving a business of addressing these items locally can free up administrative resources and reduce costs. While the benefits of cloud computing are significant, cloud-hosted services carry their own security concerns.

The more an organization relies on cloud-based resources, the busier (and more important) the Internet connection becomes. Companies leveraging cloud services for most of their applications should consider implementing multiple Internet connections with failover and/or load-balancing, should one fail.

Cloud computing also has its drawbacks, and several security related questions need to be addressed before engaging with a cloud service provider. Examples of these questions include the following:

- Does my current security policy address cloud computing?
- What physical security controls are in place at the facility housing the systems?
- How and where will my data be stored? Who can access my data?
- What levels of encryption will be in place and how will they be used?
- Will I have access to the systems?
- What are your business continuity and disaster recovery strategies? Are they tested regularly?
- Is my data replicated to other facility/facilities? Where are they located?
- Is the provider SAS 70 compliant?
- What logical security controls are in place at the facility?
- What incident response procedures exist? How and when will I be notified of a breach?

Implement and Use Common Protocols

IPSec

The **Internet protocol security** suite is a network level (OSI layer 3) cryptographic framework that essentially provides two services: authentication header (AH) and encapsulating security payload (ESP). Together these services provide authentication with data integrity (AH) and encryption of encapsulated protocol payload data (ESP). The following bulleted list outlines how IPSec ensures secure communication.

- Provides data authenticity and integrity checking by first verifying identities between parties in a conversation. IPSec prevents IP spoofing exploits and man-in-the-middle attacks.
- Provides anti-replay protection by serializing messages with sequence numbers to ensure integrity of transmitted data on the receiving end. Captured packets cannot be later reused.

- Provides non-repudiation to undeniably prove a message's source of origin. Messages cannot be forged or ownership denied once digitally signed, sealed, and sent.
- Provides strong encryption to plaintext communications protocols or vulnerable network delivery services. IPSec protects against eavesdropping, interception, and sniffing attacks.

Modes of Operation

- **Transport mode:** Only encrypts the packet payload (data being transferred) and is commonly used between endpoints (host to host) and gateways (host to gateway) in a network. Plaintext Telnet sessions can be transported from workstation to router (the actual destination) through IPSec. Commonly used for host-to-host connections.
- **Tunnel mode:** Typically used between gateways (such as through two routers) in a network topology. Operates like a proxy for "hidden" hosts and the entire packet (including the header) is encrypted. Secure connectivity between branch office and corporate headquarters or home office is a typical application.

IPSec Key Management

Crucial key management functions of IPSec provide authentication, distribution, and generation of cryptographic keys used to establish secure communications. **The Internet security association and key management protocol** (ISAKMP) establishes this elemental key management functionality and also incorporates mechanisms to negotiate, establish, modify, and delete security associations (SAs) and all respective attributes.

ISAKMP offers a flexible, scalable, and standard methodology for distributing cryptographic Internet Key Exchange (IKE) keys and SAs within high-risk security settings. There are procedures for authenticating peers and; creating, generating, and managing keys or SAs. There are also mechanisms to neutralize common network attacks.

Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is a popular network management protocol that can be used to collect network events and statistics from network-attached devices that are running SNMP agents. Agents can be activated to monitor services like WINS and DHCP, and devices like routers, hubs, printers, and servers. SNMP can be used to provide details relative to network performance, configure some devices (to a certain degree), and alert administrators when something needs attention.

SNMP versions 1 and 2 transmit in clear text, and the default community strings (public and private) are set to read/write. SNMP version 3 adds packet encryption providing confidentiality and integrity of the data transmitted. Upon installation, the default community strings should be changed and SNMP should be disabled altogether on devices that don't require it.

Secure Shell (SSH)

Secure Shell (SSH) embodies an international standard (comprising several RFCs) that establishes secure logins, channels, and transfers between networked devices. SSH was originally designed to address an administrative need for a secure remote login and shell. SSH ensures network privacy by preventing eavesdropping, interception, or tampering of the connection by a malicious third-party entity.

The primary problem with standard Telnet, FTP, and network file sharing (NFS) transactions is that they transmit details in cleintext (such as login credentials and exchanged content) that are useful in leveraging an attack. Cryptography naturally suits these purposes (remote login, shell, and file copying) and SSH provides the necessary means. SSH version 2 (SSH2) can use traditional username/password logins, public key cryptography, and several alternative forms of authentication. SSH operates over port 22.

Domain Name System (DNS)

The **Domain Name System (DNS)** retains records about hosts and resolves host names to IP addresses so systems can be accessed by name (or IP address). DNS is a core component in network computing that has many benefits; however, the openness of DNS has made it the subject of various attacks that range in frequency, intensity, and sophistication.

DNS can potentially reveal an entire organizational footprint including network devices, service versions, and server roles. An organization's name servers require substantial auditing and assessment to identify weaknesses and detect vulnerabilities. Inconsistencies in domain reversals (name-to-IP and back), zone transfers, RFC non-compliance, and outdated software versions are just a few issues plaguing public-facing DNS.

Transport Layer Security (TLS)

The **transport layer security** protocol obsoletes and replaces its precursor, the SSLv3 protocol. TLS provides the same functionality and follows the Internet Engineering Task Force (IETF) standards track (RFC 5246), which is based on earlier SSL specifications originally developed by Netscape.

That said, TLS is not backward-compatible with SSL but does establish cryptographically-secure endpoint connectivity that resists eavesdropping, tampering, and message forgery. Similar authentication and communications confidentiality concepts and components also apply. TLS supports a bidirectional authentication mode where both parties of a conversation are mutually authenticated.

TLS composes three basic phases:

1. Peer negotiation for algorithm support.
2. Key exchange and endpoint authentication.
3. Symmetric cipher encryption and message authentication.

The TLS protocol comprises two layers:

1. **TLS Record protocol:** operates at the lowest level to provide connection security. The TLS record encapsulates data for secure exchange.
2. **TLS Handshake protocol:** establishes client-server connectivity through a complex protocol exchange that defines parameters and properties for secure communications.

Secure Socket Layer (SSL)

The **secure socket layer** is a transport layer (OSI layer 4) encryption protocol used to secure end-to-end tunnels through which HTTP or other application traffic may pass. An exemplary application is for securing electronic commerce and financial web transactions via SSL-wrapped HTTP (HTTPS). An SSL session is *stateful* in that connection states are maintained from session initiation to connection teardown. SSL was originally developed by Netscape, but even subsequent versions (e.g., SSLv2, SSLv3) are rendered obsolete by Transport Layer Security (TLS).

Transmission Control Protocol / Internet Protocol (TCP/IP)

TCP/IP is a vital component in computer networking and the Internet. TCP and IP are technically part of a suite of protocols and are frequently referred to as TCP/IP as they are often used together and are the most popular of the protocols.

TCP is widely used by Internet applications, file transfer, e-mail, and more. TCP provides a dependable data stream between programs running on different systems and can request that packets be resent if they didn't arrive or corrupt ones are received.

The primary function of IP is to address hosts and route packets from source to destination over networks. IP addresses are assigned to hosts and can be subnetted to create multiple networks, which the IP protocol can route over. IP works in conjunction with TCP to ensure data integrity.

FTP Secure (FTPS)

FTP Secure (FTPS) adds support to the File Transfer Protocol (FTP) for Transport Layer Security (TLS) and Secure Sockets Layer (SSL), so connecting systems can transfer files securely, usually over the Internet. Note, however, that Secure FTP and SSH File Transfer Protocol are commonly confused with FTPS. These are different, and are discussed later in the exam manual.

FTPS can operate in two different mode: **explicit** or **implicit**.

In **explicit mode**, FTPS-aware clients negotiate with the FTPS server and agree on an encryption method to use. If the client doesn't support FTPS, the FTPS server can choose to drop, allow with limited functionality, or allow the connection unrestricted.

Conversely, in **implicit mode**, all clients must be FTPS-aware and upon establishing a connection, are required to establish an encrypted session with the FTPS server.

Hypertext Transfer Protocol Secure (HTTPS)

Much of the Interne's visually presentable side is made possible through the **hypertext transfer protocol**, a de facto standard TCP mechanism for exchanging content and messages between web browsers and servers. From an end-user standpoint, HTTP provides unbounded flexibility and remarkable delivery over a range of document types, file formats, and streaming multimedia. From a security practitioner's viewpoint, such openness and variety attracts malware and malicious activity.

HTTP is an application layer (OSI layer 7) transport method that operates plaintext-every transmission is sent in original, unencrypted format and open to interception by malicious third-party eavesdroppers. SSL and TLS provide an essential security service to HTTP (HTTPS) that ensures several preventive and protective measures are taken to resist interception, manipulation, or observation by unauthorized parties —particularly those placed between endpoints of a secure conversation. As a web-based protocol, HTTPS is integrated into popular web browsers to encrypt and decrypt page requests across TCP port 443 (instead of HTTP's usual port 80). HTTPS connections operate below the application layer to encrypt HTTP messages prior to transmission and decrypting incoming messages upon arrival.

Note: HTTPS is not identical to secure HTTP (S-HTTP, RFC 2660), an alternative, though less widely-used, URI scheme for encrypting web transactions.

Secure FTP or SSH FTP (SFTP)

Secure FTP, also known as SSH FTP (SFTP), and FTP Secure are similar in that they provide mechanisms for transferring files in a secure manner, but they differ in how they accomplish the task. While FTP Secure (FTPS), described previously, uses SSL or TLS to encrypt the flow of traffic, Secure FTP uses a Secure Shell (SSH) to tunnel a FTP session to the SFTP server. Clients wishing to use SFTP must do so with a SFTP client, or through a command line. Standard FTP clients will not work, and SFTP clients will not work with standard FTP servers.

Secure Copy (SCP)

Secure Copy (SCP) is a protocol that is used to transfer files through a Secure Shell (SSH) session. SCP uses the remote copy (RCP) command on UNIX systems to transfer files through a SSH session. SCP differs from FTP in that the permissions and timestamps of the files can be preserved by including them with the files being transferred. This ensures the integrity and confidentiality of the data in transit. SCP sessions are immune to packet sniffers.

Internet Control Message Protocol (ICMP)

The **Internet Control Message Protocol (ICMP)** is an important one especially to system administrator. It is part of the Internet Protocol (IP) suite, and is not normally used for transmitting data. ICMP is primarily used for transmitting error messages and used by tools such as traceroute and ping.

Routers can be configured to block the delivery of ICMP traffic in an effort to prevent attacks like the ping of death, ICMP flooding, and Smurf attacks on the network.

IPv4 vs. IPv6

IPv4

IP version 4 is the most widely used protocol in computer networking. IPv4 addresses are a 32-bit value commonly displayed in dotted decimal form for ease of use (e.g., 192.168.1.5). The IPv4 address space can consist of 2x32 or over 4.2 billion unique addresses.

IPv6

IP version 6 was designed to succeed IPv4 and was created to address the concern that the number of public IPv4 addresses may be exhausted. The invention of network address translation (NAT) helped ease those concerns in the short term, but the concern remains a valid one. IPv6 uses 128-bit addresses and its range is $2\times^{128}$ which is far greater than that of IPv4 and is often expressed only by mathematical formula. IPSec support is mandatory in IPv6.

Commonly Used Default Network Ports

The Internet Assigned Numbers Authority maintains and assigns port usage to applications and processes. The range of ports is divided into three categories well known, registered, and private/dynamic. Well known ports are those in the range of 0-1023, registered ports range from 1024-41951, and the private/dynamic port range is 41952-65535.

Pots usage is often scrutinized when deploying technology in an environment. Default ports should be changed (when possible), and well-known ports should only communicate with un-trusted sources through a firewall. For your convenience, these default network ports are presented in the following chart.

Protocol	Port
File Transfer (FTP)	21
Secure FTP / SSH FTP (SFTP)	22
FTP Secure (FTPS)	989 (data), 990 (command)
Trivial File Transfer Protocol (TFTP)	69
Telnet	23
Hypertext Transfer Protocol (HTTP)	80
Hypertext Transfer Protocol Secure (HTTPS)	443
Secure Copy (SCP)	22
Secure Shell (SSH)	22
Simple Mail Transport Protocol (SMTP)	25
Simple Network Management Protocol (SNMP)	160, 161, 162
NetBIOS	137 (name service), 138 (datagram), 139 (session)

Figure 6: Default Network Ports

Implementing Wireless Networks in a Secure Manner

Wi-Fi Protected Access (WPA)

Wi-Fi-Protected Access (WPA) is available in two versions, WPA and WPA2. WPA was created to address the shortcomings of Wireless Equivalent Privacy (WEP) in which the static private key could be easily cracked. WPA uses the Temporal Key Integrity Protocol (TKIP) encryption model, covered later in this guide, and adds encryption keys dynamically to each packet. WPA also performs message integrity checks, which prevents attackers from capturing and modifying packets. WPA is implemented on the wireless access point (WAP) and is used with one of the authentication protocols to provide a secure means of authenticating and transmitting data over a wireless network.

Wi-Fi Protected Access 2 (WPA2)

WPA2 was introduced shortly after WPA was made available and is its successor as it provides stronger security measures that addressed the limitations of TKIP. WPA2 uses the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP is an advanced cryptographic mechanism that was designed to protect the confidentiality of data. In addition, CCMP provides authentication and access control to WPA2 connections.

WPA2 personal (or pre-shared keys – WPA2-PSK) was created for small office and home users to create a secured wireless network, when a 802.1x server normally wouldn't be a part of the topology. Unless a strong passphrase and uncommon Service Set Identifier (SSID) are used, WPA2-PSK is vulnerable to brute force attacks. Further, not broadcasting the SSID can provide an additional layer of protection.

WPA2 is implemented on the wireless access point (WAP) and is used with one of the authentication protocols to provide a secure means of authenticating and transmitting data over a wireless network.

Extensible Authentication Protocol (EAP)

The Extensible Authentication Protocol (EAP) is a framework, not an authentication mechanism, for transmitting the information used by one of the many EAP authentication methods for connecting to wireless networks. Some of the most common methods in use by WPA and WPA2 today include EAP-TLS, PEAP, and LEAP.

Protected Extensible Authentication Protocol (PEAP)

The Protected Extensible Authentication Protocol (PEAP) was developed by Cisco, RSA, and Microsoft and encapsulates EAP in an authenticated and encrypted TLS tunnel. PEAP establishes an encrypted TLS tunnel between the client and authentication server to pass user credentials so they are protected from eavesdropping.

Lightweight Extensible Authentication Protocol (LEAP)

The **Lightweight Extensible Authentication Protocol (LEAP)** was created by Cisco and is often used in wireless LAN devices. LEAP uses a modified version of the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), and user credentials are not secured in the best possible manner. If an organization requires LEAP, strong passwords must be used, but it is recommended that organizations replace LEAP deployments with EAP-TLS or PEAP since the rotating key can be discovered by attackers.

MAC Address Filtering

Media Access Control (MAC) address filtering uses the unique values assigned to network cards to permit or deny access to a wireless network through the use of block or allow lists that contain the MAC addresses. MAC filtering provides an additional layer of access protection, but should be used in conjunction with other controls, like 802.1x, to establish a secured wireless networking environment as valid MAC addresses can be captured and then used on a different system (spoofing).

Service Set Identifiers (SSID) Broadcast

One of the most simple and common best practices in wireless security is to change the SSID on a wireless device, like a router, and then disable broadcasting of the SSID. While this technique may not stop most serious attackers as SSIDs are transmitted in plain text, it is part of the overall wireless security strategy and should be used in combination with WPA2 and other best practices like employing MAC filtering, changing the default administration password, and enabling encryption.

Wardriving

Freely broadcast wireless transmissions suffer from a similar problem as data emanation. The practice of actively seeking wireless radio devices and mapping network entities from a moving vehicle is called **wardriving**. Laptops and PDAs are most commonly used, but specialized designs comprising multiple antenna arrays and adapter cards are also used. GPS may also be employed as a means to measure and mark locations for an overhead visualization of wireless hotspots.

Disabling SSID broadcast alone is insufficient to prevent discovery of the access point through wardriving. Using VPNs to foil eavesdropping, isolate access points (APs) from the internal network, eradicate rogue APs (an unauthorized access point that is placed on-site), filter unauthorized MACs, and confine radio coverage to internal assets is another step that can be taken to lower the risks of wardriving.

Temporal Key Integrity Protocol (TKIP)

WPA uses the **Temporal Key Integrity Protocol (TKIP)** encryption model by adding encryption keys dynamically to each packet. TKIP was developed to address the security weakness of WEP – without having to replace hardware. TKIP added security controls that were missing in WEP: key-mixing functions, anti-replay sequence counter, and a 64-bit message integrity check. Since TKIP is built on top of WEP, it is also vulnerable to attack and is being phased out.

Cipher Block Chaining Message Authentication Code Protocol (CCMP)

As discussed earlier, WPA2 uses the Counter Mode with **Cipher Block Chaining Message Authentication Code Protocol (CCMP)**. CCMP was created to address the weaknesses in TKIP. CCMP is the industry standard for WPA2 and is an advanced cryptographic mechanism that was designed to protect the confidentiality of data. In addition, CCMP provides authentication and access control to WPA2 connections.

Antenna Placement and Power Level Controls

Antenna placement and reducing the power level of the antenna for wireless networks can help limit the accessibility of the wireless access point by unauthorized external systems. While the practice of these as security controls is debated, power level reduction and antenna placement can make it more difficult for attackers to attach to the access point from outside of the building, such as from a vehicle. Unfortunately, this practice can have an impact on users who are allowed to connect to the wireless network. As a general practice, the antenna should be placed in the center of the area it is to cover but may take several configuration attempts to fine-tune. Attackers can create devices from common materials that can allow them to locate and attach to the wireless network, regardless of antenna placement. As such, this is not considered a strong deterrent and should be used only in combination with the other wireless security controls discussed earlier in this exam manual. If the correct security controls are in place on a wireless network, antenna placements and reducing the power level may not be of concern.

Domain 2 – Compliance and Operational Security

Risk Related Concepts

Zapping out problems before they arise is a cornerstone of risk management. IT security has its own version of **risk management**—a collection of methods and mechanisms designed to assess, document, and reduce operational risks associated with the manner in which companies conduct business. New technologies, system changes, partnerships, acquisitions, incidents, and accidents are several examples that can introduce risk into an organization's environment.

Risk can pose various threats to the enterprise network, corporate assets, or personal safety. Risk management concentrates administrative activity to manage uncertainty, handle threats, and enforce policies that ensure conformance with risk management procedures, protocols, and processes.

Before diving into risk calculation, it is imperative that security professionals understand the terms used and their application in the risk analysis process. Try to familiarize yourself with the following risk categories, risk factors and terms.

Risk Categories

- **Damage:** Results in physical loss of an asset or the inability to access assets.
- **Disclosure:** Revealing critical information regardless of how or where it's revealed.
- **Losses:** Permanent or temporary, including the alteration of data or inability to access data.

Risk Factors

- **Physical damage:** Results from natural disasters or other factors, such as power loss or vandalism.
- **General malfunctions:** Expected mechanical failure of system and network devices.

- **Malicious activity:** Intentional acts from inside and outside the network including misuse of information, unauthorized disclosures, and attacks against informational assets.
- **Human error:** Accidental and incidental occurrences, often without intention.
- **Application error:** Program and operating system failures that are typically accidental, as actively exploited application errors are intentional attacks.

Key Terms

- **Threat** - An imminent or pending event of undesirable consequence or outcome.
- **Exposure** - Potential disclosure of privately withheld information resulting from a vulnerability.
- **Uncertainty** - Lack of confidence or reliable data regarding any element of the risk assessment.
- **Vulnerability** - Susceptibility to attack as identified by systemic weaknesses.
- **Losses** - Realized (monetary) losses that occur through exploited vulnerabilities.
- **Asset Value** - Measurable numeric quantity that resembles the value of a resource.
- **Exposure Factor (EF)** - Percentage of loss an asset could incur due to an identified threat. Multiplied by the asset's value, the exposure factor is used to determine the Single Loss Expectancy (SLE).
- **Annualized Rate of Occurrence (ARO)** - The annualized rate of occurrence (ARO), reflects the number of times in a year that an identified threat could take place. Obtaining this number varies from analyzing statistical data to guessing.
- **Single Loss Expectancy (SLE)** - Cost of an event that is realized by multiplying the asset's value by the exposure factor, if a threat were to be successful.
- **Asset Value x Exposure Factor (EF)** - Single Loss Expectancy (SLE).
- **Annualized Loss Expectancy (ALE)** - The annualized loss expectancy (ALE) is calculated by multiplying the single loss expectancy (SLE) and annualized rate of occurrence (ARO).
- **Single Loss Expectancy (SLE**) - x Annualized Rate of Occurrence (ARO) = Annualized Loss Expectancy (ALE).

Control Types

A **control** is a component that is put into place to implement and enforce the security requirements of the organization. Security controls are put into place to reduce the likelihood that an incident will occur, and/or to minimize the impact of an incident. Controls can be ***administrative*** (or procedural), ***operational***, ***physical***, ***environmental***, and ***technical*** (or logical).

Administrative / Procedural Controls

Administrative (or procedural) controls include an organization's policies, procedures, standards, and guidelines. Security policies are high-level documents that serve as a foundation for an organization's security posture. Standards dictate how the policy will be enforced. Guidelines include a set of best practices that are recommended when dealing with a particular situation, usually one that is addressed in a policy. Finally, procedures are step-by-step detailed instructions for addressing security-related issues ranging from implementing technology to addressing incidents. In order for these controls to be effective, they must be validated, kept current, and made available to the appropriate personnel within the company.

Operational Controls

Operational controls primarily deal with security in a production environment as their purpose is to maintain the integrity of an Information Security program by ensuring that business is being conducted in as secure a manner as possible and incidents are properly addressed. Some examples of operation controls include risk assessments, change management, and incident response.

Physical and Environmental Controls

Physical and environmental controls address the risk that unauthorized access to a facility, equipment, information, or resources could be achieved in person by an attacker. Some examples of physical security controls include fences, gates and checkpoints, landscape design, locked doors and keycard systems, cameras, security guards and guard dogs, and bollards (used to prevent a vehicle from forcefully driving into a building). Examples of environmental controls would include temperature, humidity, airflow, and water – and are most commonly found in data centers.

While many of these controls are also deployed inside a facility, deploying effective environmental controls outside of the facility is equally or more important as they are often the first line of defense when protecting from an on-premise attack.

Technical / Logical Controls

Technical (or logical) controls include the controls that most security professionals are familiar with as this control category is comprised of the security hardware and software like passwords, firewalls, NIDS, NIPS, content filters, encryption, and more. Technical controls are put in place to support the enforcement of corporate information security policies by restricting access to, and ensuring proper usage of company resources by appropriate personnel.

False Positives

A **false positive** occurs when an expected or normally permitted event triggers an alarm or is prevented from executing (blocked). The frequency of false positives can be offset by changes to the control responsible for generating the false positive. A control with a very strict design will likely generate more false positives, but is proven to be more effective at preventing and detecting actual incidents that violate security policies and warrant an immediate action. Whereas, a control with a more lax design will reduce the frequency that false positives may occur, but are typically less secure overall.

False Negatives

A **false negative** is defined as a security incident that goes undetected or prevented, when it normally wouldn't be allowed. A spam message that arrives in an e-mail inbox with a score of "pass" or "safe," and a keycard that permits access when it should have denied it are examples of a false negative.

Importance of Information Security Policies

Information Security policies, as stated previously, comprise the foundation of an organization's Information Security program and serve as a high-level document that communicates the organization's stance on Information Security related concepts, risks, and controls. Information Security policies are an integral component for an organization's Information Security practice as it serves as a basis from which all other security related items are put in place.

In order to be effective, Information Security policies must be supported by top level management, be documented and maintained, communicated, understood, and agreed upon by all employees. Exceptions to Information Security policies should be captured in risk assessments, and regular audits should take place to ensure the effectiveness of the security controls that help enforce the requirements of the policies.

Inherently through their existence and communication alone, Information Security policies are a big step in reducing risk. Coupled with potential disciplinary action and effective safeguards, risk can be further reduced through policy enforcement and routine auditing. Some examples of Information Security policies include acceptable use, network access, remote access, vendors and third party, physical security, access control, and more.

Common Information Security Policies and Practices

Privacy Policy

A **privacy policy** states how an organization obtains, uses, and safeguards customer and employee data. Information in a privacy policy can be influenced by law, corporate policy, best practices, company location/locations served, and more. Privacy policies are usually published where they can be accessed easily by the customer or employer.

Acceptable Use Policy

An **acceptable use policy (AUP)** outlines absolute conditions, behavioral expectations, and enforced rules for a given computer system or network—as defined by administrators, security professionals, and legal experts. AUP is written for business, corporations, institutions, providers, and universities to reduce the potential for legal action taken by a user and legal conditions applicable to end-user interactions. AUP is often used to establish explicit end-user acceptance or denial of AUP terms prior to granting (or rejecting) access to protected resources and systems. Documented policy often mirrors Terms of Service conditions specified by email and Internet service providers.

Information Security Policy

An Information Security policy often states that an organization will maintain and support an Information Security program, outline the primary objectives of the program, and reference several supporting policies that further define the role of security and expectations of everyone in the company. Information Security policies also outline which departments or personnel are responsible for various tasks and reference other documentation like corporate standards, guidelines, and procedures.

Company security policy objectives are derived from several key sources including governmental legislature, federal regulations, industry practices, and organization-specific considerations. Other non-mainstream sources also indirectly contribute to policy development but none are more pervasive and persuasive than the laws and mandates imposed by federal or governmental bodies, which often demand proven compliance under penalty of law. These two primary sources often direct organizations in handling patient records (healthcare), credit information (e-commerce), personal information (state agencies), or other processes related to securing confidential data and functions.

Mandatory Vacation

Employees operating in sensitive areas of the business should be forced to take vacations in what is known as a **mandatory vacation** policy. In their absence, other individuals fulfill their roles and responsibilities and are capable of detecting fraudulent behavior, inappropriate activity, or erroneous results. Any problems specifically related to the original employee's accounts or activities will be noticeable in their absence—either a previously unknown problem will be discovered or an existing problem may temporarily cease.

Job Rotation

The process of **job rotation** is usually implemented as part of human resources (HR) management plan to rearrange and reallocate personnel among numerous jobs to provide a breadth and depth of experience in the various interrelated duties. Job rotation allows qualified employees to gain insight into the inner processes and workings of an organization, reduces individual boredom, and stimulates satisfaction through routine variation.

Separation of Duties

A **separation of duties** selectively assigns access rights focal to a person's requirements to complete a given task. Separation of duties creates an appropriate level of checks and balances upon the activities of individuals operating in a given job capacity by preventing any one individual from gaining too much insight or control over business operations. In a security context, separation of duties disseminates the tasks of a particularly sensitive job among multiple users who function in individual capacities rather than as a collective group.

Principle of Least Privilege

The **principle of least privilege** is an important security concept and design consideration that grants the lowest amount of privilege possible to perform some task. Access rights are assigned according to what an individual's roles require such as opening some file, modifying some data, and viewing some results. In a security context, this restrictive permission protects against giving users sufficient rights to damage or disrupt sensitive higher-level functions and processes.

Need to Know

The **need to know** principle dictates that employees should only be granted sufficient information to perform designated tasks—and nothing more. Conceptually speaking, this policy principle complements the principle of least privilege and helps achieve similar security objectives by reducing the amount of damage caused by any individual leaving the company or manipulating the company. Without formal information classification and security labeling practices, the need to know sensitive or privileged information is the strongest preventive practice against tactics.

Due Care

Simply defined, **due care** means knowing and performing the proper course of action in every situation and taking responsibility for those actions. Due care is the action, behavior, or character expected of a reasonably prudent person to act upon, regardless of the individual's security function or occupational role. Due care also defines the steps taken by a company to prove responsibilities for actions taken during the organization's daily routines and business operations. A business exercises due care by implementing policies, procedures, and processes to protect its assets, personnel, and resources.

Due Diligence

Due diligence in a computer security context is part of the information technology procurement process to ensure risks are known, threats are managed, vulnerabilities are protected, and exposures are safeguarded from attack. During mergers and acquisitions, due diligence reviews identify and assess business risks associated with acquiring, integrating, and operating separate business components.

Calculating Risk

Risk calculation starts by determining the value of the asset and the likelihood and frequency in which threats can exploit vulnerabilities in an effort to determine the appropriate safeguard(s) for the indentified asset(s). Calculating risk and performing risk analysis is a critical step in choosing what safeguards to implement (mitigation) and what the appropriate budget of the safeguard should be. A company can also choose to accept the risk, transfer the risk (insurance), or avoid the risk altogether by removing the component related to the asset that is generating the risk.

Risk assessments resolve assumptions and uncertainties about risks and threats into clearly considered and well-defined analysis reports. Information security assesses risks through types of risks (risk categories) and how those risks occur (risk factors).

Objectives for Calculating Risk

The primary objectives for calculating risk include the following:

- Identifying and quantifying the value of company assets.
- Identifying the vulnerabilities and the threats that can exploit them.
- Identifying the likelihood, frequency, and impact of the potential threats.
- Recommending cost-effective countermeasures to protect the asset from the threat, or alternate methods of dealing with the risk.

Quantitative versus Qualitative Risk Analysis

The purpose of a **quantitative risk assessment** is to calculate risk by assigning numeric values to all components of the risk assessment.

The purpose of a **qualitative risk** assessment is to calculate risk by using best practices, experience, opinions, and the practicality that a vulnerability could be exploited, allowing an incident to occur.

Steps for Calculating Risk and Determining Costs

1. **Identifying Assets and Assigning Values**
   In this step, security professionals will need to address questions like: What is the cost to recover or replace the asset? Does the asset generate profit? Is it valuable to the organization's competitors? Can the company be held liable if the asset is compromised?

2. **Estimating Losses**
   In this step, the potential costs relative to the threats that could impact the asset, such as physical damage, data leakage, productivity loss, cost of recovery, and more are identified. Further, the single loss expectancy (SLE) for each asset and threat is also determined in this phase.

3. **Threat Analysis**
   In this step, details and supporting information regarding the identified threats are gathered and the annualized rate of occurrence (ARO) is calculated.

4. **Annual Loss Potential**
   In this step, the annualized loss expectancy (ALE) for each threat is calculated and a cost-benefit analysis that includes the costs associated with countermeasures and recovery is performed.

5. **Addressing the Risk**
   In the final phase, addressing the risk, a recommendation is made on how to handle the risk: reduce / mitigate, accept, avoid, or transfer.

   - **Reduce or Mitigate the Risk** – Implementing security controls, changing system configurations, and altering business processes are a few examples of actions organizations can take to reduce risk.
   - **Accept the Risk** – While it sometimes isn't the most popular option, companies can choose to accept the risk and continue to use the asset. Accepting the risk is often allowed when the asset is mission-critical and the cost of the countermeasure is more expensive than the value of the asset, or no countermeasure exists.
   - **Avoid the Risk** – Avoiding the risk typically involves the elimination of the asset altogether, or a transformation that results in the risk being eliminated. The latter can introduce new risks that would need to be addressed separately.
   - **Transfer the Risk** – Organizations often transfer the risk by taking out an insurance policy.

Security Risks and Cloud Computing

In Domain 1, cloud computing was defined, its benefits were outlined, and several drawbacks and security concerns were discussed. Cloud computing and virtualization are often coupled together, and the risks inherent with virtualization should also be considered if the cloud provider's infrastructure relies on virtual machines.

As the cloud continues to increase in popularity, despite the debate that it's nothing more than a marketing term, security professionals must ask the right questions when engaging with a cloud provider and obtain an understanding of the risks associated with cloud-based services. Some common examples include:

- Privacy of company and customer data
- Physical security for the facility and backups
- Network, system, and data access (local and remotely)
- Performance and service interruptions
- Migrating off the cloud or to another cloud provider

Security Risks and Virtualization

In Domain 1, **virtualization** was defined, its benefits were outlined, and several drawbacks and security concerns were discussed. When addressing security risks associated with virtualization, the process is very similar to that of assessing the risk of a physical system since virtualized guests are essentially separate computers. For example, an anti-malware product on a physical host will not detect malicious code on a virtualized system.

When analyzing risk with respect to virtualization, treat both the physical (host) system and virtual (guest) systems as physical hosts. Some common risk examples as they pertain to virtualization include:

- Unmonitored communication between virtual machines on the same host
- Consolidating multiple systems/applications onto a single physical device (single point of failure)
- Virtual guests could be accessed through a compromised host system / hypervisor

Risk Mitigation Strategies

Choosing and Implementing Countermeasures Based on Risk

Once the risks have been identified during a risk analysis, countermeasures must be recommended and implemented to mitigate the risk. Countermeasures can include a variety of controls like physical, technical, logical, operational, and administrative. As a general rule of thumb, *if the costs associated with the countermeasure(s) outweigh the value of the asset, then the countermeasure(s) should not be implemented*. When selecting a countermeasure, the following should be taken into consideration:

- Costs: purchase, design, deployment, support, and maintenance
- Compatibility and changes to the organization's processes and infrastructure
- Effectiveness of the countermeasure should be able to be validated
- The countermeasure should operate as independently as possible

Change Management

Change Management is an IT service management discipline with the sole objective of ensuring that standardized methods and procedures establish sufficient management, monitoring, and reporting of changes to a controlled IT infrastructure. Change management tracks alterations to the IT infrastructure that may arise reactively or responsively due to externally-imposed requirements (e.g., legislative, regulatory, or industrial changes) or from internally-imposed initiatives (e.g., efficiency enhancement, security improvement, implementation upgrade). The process of managing change ensures that standardized methods, processes, and procedures are used to facilitate efficient, prompt handling of change while striking balance between change and consequence.

Incident Management

Incident Management, with respect to computers, networks, and data, is a process that organizations employ to discover, record, and take action on security-related incidents. Incident management today is often handled by an incident response team and typically includes the monitoring of a Security Events Manager (SEM), Security Incident Manager (SIM) system, or both (SEIM). Security event and incident managers monitor activity from multiple systems and correlate and process the captured activity to identify security-related issues. Incident management also provides a valid means of identifying vulnerabilities and risks in an environment as they are uncovered when investigating and resolving incidents. The information contained within previously documented incidents can be leveraged when performing new risk assessments or implementing security controls.

User Rights and Permissions Reviews

When analyzing the risk related to an asset, **user rights and access permissions** to the asset should be reviewed regularly. Assigning the appropriate level of access to the right personnel, and regularly reviewing those access permissions can act as a very effective countermeasure when mitigating risk.

Performing Routine Security Audits

A **security audit** is the collective means through which a risk assessment is conducted to ensure compliance of enforced organizational or regulatory security policy. Security audits challenge the mechanisms and methods used to enforce a given security policy with the end result of verifying and validating the correctness (in implementation and functionality) of those implements. Manual security assessments involve staff interviews, vulnerability scanning, application access review, and operating system access control enforcement. Automated security assessments are software-driven methods of producing system-generated audit reports or establishing the monitoring and reporting of system changes.

Implementing Policies and Procedures to Prevent Data Loss or Theft

Data leakage (data loss), whether intentional or unintentional, can have severe consequences for an organization, and specific policies, procedures, and controls need to be in place to address this issue. At the highest level, an information protection policy should exist and address how data should be protected, transmitted, and stored. The more properly classified data is within an organization (no small undertaking), the easier it will be to protect it and detect incidents. Several vendors offer several different types of data loss prevention (DLP) solutions that can work at different parts of a network. DLP products work by monitoring the content of files and network traffic, and scanning for content that is deemed private or confidential. DLP technologies can take certain actions to protect data, like applying encryption, preventing copying to the clipboard, preventing printing, and more.

In addition to best practice, there are laws and regulations that specifically address protecting and handling incidents related to personally identifiable information (PII). Laws and regulations like HIPAA, Sarbanes Oxley (SOX), California SB-1386, SAS 70, and GLBA provide guidelines and procedures that must be followed and audited regularly for an organization to be recognized as compliant.

The unauthorized disclosure of proprietary and private data is one of the biggest risks organizations face. Like the policy, incident response procedures also play a key role and should include procedures that deal directly with the loss of sensitive information. An information protection policy should address several items, which are outlined below:

- Which systems can store sensitive information.
- How sensitive information should be transmitted (data in motion) and stored (data at rest).
- Who can access sensitive information and how they can use it.
- How sensitive information should be destroyed.

Incident Response Procedures

Incident response procedures are the most vital component to managing incidents. Incident response procedures are carried out by the incident response team; however, many others play a key role when addressing incidents (e.g., help desk, management). Incident response procedures should be well documented and help desk personnel should be well versed on how to filter out false positives to identify true security incidents that pose a threat. Most incident response procedures follow a structure similar to the ones outlined by the Information Technology Infrastructure Library (ITIL), shown below:

1. An incident is identified and recorded.
2. The incident is classified and initial investigation steps should be prepared.
3. An investigation and diagnosis of the incident begins.
4. The incident is resolved and recovery steps are taken.
5. The incident is closed.
6. The incident is monitored, tracked, documented, and communicated to the identified owners of the incident as well as those who are affected by it.

As mentioned above, incident management also provides a valid means of identifying vulnerabilities and risks in an environment as they are uncovered when investigating and resolving incidents. The information contained within previously documented incidents can be leveraged when performing new risk assessments or implementing security controls.

Basic Computer Forensic Procedures

Digital forensics (or computer forensics) is a specific branch pertaining to acquiring, intercepting, or seizing legal evidence contained within computers, electronics, and digital storage mediums. Computer forensics searches **digital artifacts** (e.g., disk drives, ROM discs, electronic documents, image formats) or even packet sequences in network traffic. The objective is to explain the current state of those digital artifacts as evidence in a criminal investigation. Obviously there are certain industry and legal restrictions, requirements, and regulations enforced when using digital information as evidence in pursuit of a criminal conviction.

Basic computer forensics is focused on the identification, preservation, and presentation of electronic information that is relative to an investigation.

When addressing incidents, basic computer forensic procedures should be strictly adhered to, should the incident result in a more formal investigation that could possibly result in legal action. These basic computer forensic procedures should be followed precisely in order to preserve the integrity of the captured information and systems so they can be admitted as evidence in a court of law.

1. **Prepare** – Obtain the correct tools and procedures for carrying out the investigation.

2. **Collect** – Obtain the evidence in a forensically sound manner, preserving the original and creating copies from which to work. There are several sub-steps when collecting evidence, and some examples include creating a hash value of the original evidence, using a write-blocking tool to preserve the evidence, documenting the steps and evidence collected to show a chain of custody, and collecting files that may be present in a computer's memory.

    a. **Order of volatility** – Information on computers exist in multiple places and in different states and it is important to recognize what information to capture first to reduce the risk of losing it, like with memory cache or temporary files. RFC 3227, Guidelines for Evidence Collection and Archiving, provides a detailed volatility outline. The basic outline is as follows: memory, temporary files, disk, remote logs, physical setup, and backup media. Several tools exist for computer forensic specialists that recognize this order when capturing information.

b. **Capture system image** – Computer forensic experts need to capture a bit-level copy of the system, and hashes for both the original and copy will be generated to prove they are identical. The original system is sealed and marked as evidence and the forensic expert works off of the imaged copy.

c. **Network traffic and logs** – Depending on the incident, computer forensic experts must also be prepared to capture and analyze network traffic and/or log files.

d. **Capture video** – If security cameras exist at the crime scene, any captured video must be included as evidence. Video footage is extremely difficult to argue and serves as a vital component in an investigation. Some investigators also choose to record or take photos of the crime scene and/or the evidence collection process.

e. **Record time offset** – When capturing files and data during an investigation, the time on the local system and the timestamp on system files should be matched against a known time standard and the results recorded. This is useful in the event the local system time is incorrect and helps investigators determine a more accurate timeline of events.

f. **Take hashes** – Any data or system that is to be collected as evidence should be copied and have a hash value generated for each. As mentioned above, this proves that both the original and copy are identical and allows investigators to work from the copy.

g. **Screenshots** – When capturing evidence at a crime scene, computer forensic experts should use a digital camera (not the print screen key on the suspect system) to capture anything that is displayed on the computer monitor.

h. **Witnesses** – Anyone who witnessed the crime or has information about it should be questioned and his or her comments included with the investigative report.

i. **Track man hours and expense** – Tracking the time and money spent on investigations helps calculate and trend how long certain investigations should take. This information can also be useful when recreating an audit trail and presenting the chain of custody.

3. **Examine** – The evidence and copies thereof are cataloged and preserved.

4. **Analyze** – The copy of the evidence is analyzed using a wide range of tools and techniques to determine what information resides in the captured media.

5. **Report** – A report is prepared and presented.

Damage and Loss Control

Damage control and loss control refer to identical processes of preventing further destruction to company assets or disruption to company resources. It's the effort to curtail damage and minimize loss and regain control of an out-of-control situation. Damage/loss control procedures are developed according to site-specific conditions and circumstances, which vary according to regional, environmental, and territorial threats.

Chain of Custody

Among the more crucial aspects of securing evidence of any nature is the **chain of custody** or chronological history documenting its capture, custody, and control. Analysis, disposition, and transfer of evidence (both digital and physical) must be conducted in a careful, scrupulous manner to avoid allegations of tampering, tainting, or compromising misconduct. Even the slightest discrepancy in the chronological events describing the nature of evidence is sufficient grounds for compromise.

The chain of custody addresses who, what, when, where, why, and how, and each needs to be documented in a chain of custody log when collecting evidence. The court and opposing attorneys could question each of these items, and if there is a break anywhere in the chain (e.g., someone unauthorized had access to the evidence), then the integrity of the evidence is lost and it could be dismissed.

Incident Response: First Responder

In **incident response**, one of the key roles on the incident response team is that of the **first responder**. The first responder performs an initial analysis of the incident and gathers any additional information that may not have been included when the incident was first reported. One of the core responsibilities of the first responder is to assess the criticality of the event, and escalate the case if the situation warrants it.

Security Awareness and Training

Security awareness and training is an administrative tool used to reduce risk in an environment. Users are informed about the role they play in keeping the environment secure and they are also educated on the various company security policies. Security awareness training must be completed routinely, and encompass all levels of personnel, technical and non-technical. Training materials should be adjusted accordingly. Adjustments to the training program should be made after monitoring the effectiveness of the program.

Security Policy Training and Procedures

Every employee needs to be informed of company security policy, which can vary by industry or business. Companies need to provide training regimens to inform its employees of site-specific threats, associative vulnerabilities, and best practices. End-users are typically among the weakest links in any organizational security chain and a quality security awareness program based on company security policy is essential to any Information Security program.

Personally Identifiable Information (PII)

Generically defined, **personally identifiable information** is a class of data pertaining to the contact, location, or identification of specific individuals. The NIST *Guide to Protecting the Confidentiality of Personally Identifiable Information* specifically describes PII this way:

Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. ... which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

PII is currently a hot topic because of many high-profile data thefts and information attacks supportive of identity theft rings and crimes against business clients and consumers. Stored PII falls under several federal and industrial regulations that dictate how confidential data is stored, transmitted, and ultimately destroyed – all depending upon the nature of the business and the sensitivity of the information.

Information Classification

Information classification restricts access to protected information as restricted by law or regulation to particular classes of personnel. Formal security clearances are required to access and handle classified information, which is categorized into a series of security labels defining their secretive nature (e.g., Secret, Top Secret, or Classified). Some corporations and non-governmental organizations also assign sensitive information in compartments of access to prevent foreign dissemination to U.S. nationals and originator-controlled dissemination enabling the tracking of sensitive information.

Data Labeling, Handling, and Disposal

Disposing of sensitive information is a delicate issue – both in terms of application and consequence. Some companies and organizations fail to properly sanitize sensitive information (electronically and mechanically) prior to disposal, which has led to several high-profile cases of sensitive information being exposed to unauthorized sources.

Organizations should have a clear and concise method for labeling data, which will drive the proper handling and destruction methods. The focus on data handling usually lies around mitigating risks and preventing disclosure of proprietary information. Data loss prevention (DLP) solutions are often implemented to mitigate the risks involved with handling data. Secure disposal requires the appropriate method of destruction to match the level of confidentiality or secrecy involved with the data, which could include several encrypted passes against the full capacity of a storage volume to physical destruction.

Compliance with Laws, Best Practices, and Standards

Company security policy objectives are derived from several key sources including governmental legislature, federal regulations, industry practices, and organization-specific considerations. Other non-mainstream sources also indirectly contribute to policy development but none are more pervasive and persuasive than the laws and mandates imposed by federal or governmental bodies, which often demand proven compliance under penalty of law. These two primary sources often direct organizations in handling patient records (healthcare), credit information (e-commerce), personal information (state agencies), or other processes related to securing confidential data and functions.

Users must be educated on the laws and standards to which their organization must adhere. By informing users of the proper best practices, processes, and procedures, the better chance an organization has to be "compliant." Compliant, however, does not necessarily equate to "secure," and vice versa. There are many factors involved to become and remain compliant and while there is some overlap, each has its own set of requirements. Some examples are provided below.

- **California SB 1386** – Requires anyone conducting business in the state of California, and who has access to personally identifiable information in electronic form, to disclose any security breaches in a reasonable amount of time and only if the data was unencrypted.
- **Sarbanes Oxley (SOX)** – Protects investors by improving the integrity of transactions and of corporate disclosures by requiring oversight, auditing requirements, and accurate financial reporting, and by assigning responsibility directly to the CEO of the organization.
- **Health Insurance Portability and Accountability (HIPAA)** – Regulates the handling, usage, and disclosure of an individual's personal health information (PHI).

User Habits

Addressing user habits during security awareness training helps ensure that individuals are educated on and use best practices in their day-to-day work routine. This category often encompasses topics like sharing passwords, locking computers, identifying fraudulent web sites and e-mail, not discussing sensitive matters in open areas, proper handling of data, and more. These are all items that users can relate to and execute effectively.

End-users should be properly educated and trained on using strong passwords, sharing or revealing passwords, how to handle sensitive data, keeping desks clean, and company policies that address items like tailgating and the use of personally owned devices.

Threat Awareness

As discussed earlier, a threat (person, malware, etc.) exploits vulnerabilities (weaknesses in a system or process). When conducting security awareness training, users need to be educated on the threats and vulnerabilities to which an organization is susceptible. Raising awareness around threats and vulnerabilities helps users prevent and/or identify potential incidents. Threats and vulnerabilities, and specific examples of each, are covered in the next domain. When delivering security awareness training to end-users, emphasis should be placed on threats that end-users might be exposed to like computer viruses, and phishing e-mail and fraudulent offers. IT staff should be informed about more advanced issues like zero-day exploits, blended threats, botnets, and incident response.

Social Networking and Peer-to-Peer

Security awareness training should address the use of **social networking and peer-to-peer** technologies like a bit torrent and file sharing, alongside the risks they present to an organization. While there can sometimes be a business need for these items, many organizations now prevent or restrict the use of social networking sites and peer-to-peer networking.

While they have their benefits, the risks associated with both social networking and peer-to-peer solutions in a corporate environment often outweigh those benefits. Some specific examples include data leakage, virus and malware infections, and copyright violations.

Aspects of Business Continuity

Business continuity planning (BCP) defines how a company can restore failed functions (which are critical for running the business) to a normal operating state and within a specified time period. BCP requires regular testing and modification to ensure that the plan is effective and successful. Business continuity planning and disaster recovery are often connected as the two processes complement each other.

Business Impact Analysis

The **Business Impact Analysis (BIA)** identifies the critical services, systems, and processes that are vital to an organization's environment. The BIA also identifies the amount of time an organization can allow the component to be down (maximum tolerable downtime).

Removing Single Points of Failure

A **single point of failure** is defined as interruption to any single component of an overall system that individually (and negatively) affects an entire system. An example is where a single router, gateway, or public link failure adversely affects an entire network of end-users. **High-availability (HA) systems** (e.g., applications, systems, networks) are often given redundant or doubled-up defenses against these singular failures: clustering, doubled network interfaces, storage drives, server configurations, power supplies, etc.

Business Continuity Planning and Testing

As mentioned above, BCP requires regular **testing** and modification to ensure that the plan is effective and successful. The goal of the testing is to ensure that the plan will properly restore the necessary systems and business functions and that the plan falls within the requirements defined for recovery. Items that fail during testing can be addressed and tested again later, which is the primary purpose of the tests. BCP testing is usually conducted annually or bi-annually and, depending on the item to recover, the process can be simple or extremely complex.

Continuity of Operations

IT security encompasses more than just the obvious security provisions. Nowhere is this more evident than in business continuity planning (BCP) and disaster recovery (DR), two similar though separate aspects of IT security practice. BCP seeks to establish the means, methods, and mechanisms through which interrupted business functions are restored to working order.

DR is a complementary strategy that establishes the policies, protocols, and procedures necessary to recover disrupted business operations with designated off-site facilities for potential relocation. Common concepts used among both BCP and DR planning follow.

Continuity of operations focuses on eliminating single points of failure and leverages high availability, load-balancing, fault tolerance, and redundant systems and network connections to achieve the goal. Most outages will require as close to a duplicate as possible of the original system or business process.

Tools like backup generators, uninterrupted power supplies, spare parts, and redundant disk sets (RAID) help reduce downtime. Continuity of operations can also make use of a cold, warm, or hot site to recover failed operations.

Backup Generator

Computers, devices, and equipment all draw power. Interruption to power is disruptive to service levels built upon these cornerstone infrastructure elements and affects business operations entirely. Emergency power systems provide on-site backup resources in crisis. When **backup generators** are activated, power consumption is configured to only allow critical systems and devices.

Spare Parts

Having **spare parts** or extra hardware on-hand to replace component failures in mission-critical systems is essential to executing efficient and effective recovery phases. A thorough assessment accounts for all critical components that can reasonably have standby replacements in the event of their total failure. Part of maintaining service level agreements (at the provider level) and high-availability service operation (at the subscriber level) means employing multiple redundant systems and having multiple spare parts to handle multiple potential failures.

Uninterrupted Power Supply (UPS)

Some events are unavoidable but most can be prevented or protected against causing serious damage to critical business components. The **uninterrupted power supply (UPS)** is a universal standby power source that supplies a limited amount of battery backup power when the primary source fails. A UPS instantly takes over when the original power source becomes unavailable to provide continuous power to sustain safe and proper computer shutdowns or continue operating a few critical business operations for a limited period of time. A UPS can serve as a complementary component to backup generators, allowing systems to function properly until the generator comes online.

Disaster Recovery (DR)

Planning for **disaster recovery (DR)** requires formal assessment of risk, threat, and vulnerability specific to a work site, facility, and operational nature. DR planning accounts for all the negative consequence that comes from major disruptions to organizational function or operation, including the least-likely remote possibilities.

The final product is the disaster recovery plan—a comprehensive statement of consistent actions to be taken before, during, and after a disaster of any origin. This plan must be documented, periodically tested, reviewed, and revised for the duration of its existence. Most importantly, the DR plan must ensure recovery of operations and availability of critical resources in the event of a disaster with the primary objective of protecting the organization in the event that part or all of its operations are halted.

IT Contingency Planning

Contingency plans are predecessors to business continuity (BCP) and disaster recovery (DR) that address the question "What if something goes wrong?" Contingency planning prioritizes and lists in order the mission-critical functions and applications that are to be recovered. Contingency planning identifies single points of failure and helps to simplify the BCP and DR process by eliminating any discovered SPOFs.

Succession Planning

Succession planning identifies and outlines personnel who are capable of filling key roles in the event of an outage or disaster. This can include the original/routine personnel who are familiar with the process or service, and/or it can include personnel who are capable of assuming the role when necessary.

Impact and Proper Use of Environmental Controls

A damaged or destroyed working environment is an unsecured working environment. Imagine receiving significant structural damage to a building that exposes sensitive server hardware and workstation computers. Securing those items becomes increasingly problematic with regard to the nature and intensity of damage sustained—it's not like you can rebuild insulated brick walls overnight or repair structural damage with tools on hand. Fire, electricity, gas, water, and natural elements continually conspire to damage the working environment and disrupt security.

Heating, Ventilation, and Air Conditioning (HVAC)

Ideal environmental conditions collectively preserve the delicate hardware and sensitive instrumentation used to secure and maintain the business infrastructure. High heat, excess humidity, water damage, turbulent winds, and violent thunderstorms can adversely affect the enterprise landscape in a multitude of ways. Design considerations for **HVAC** include: independent power source, positive air pressure (i.e., air constantly flows out to avoid inbound contamination), protected intake vents to prevent intrusions or tampering, local and remote monitoring of environmental conditions, emergency cutoff, and secure placement of the HVAC system.

Fire Suppression

A proper **fire suppression** system seeks to slow or halt the spread of a fiery outbreak. Many chemical, liquid, and other types of suppression systems exist to address the various particulars and needs of a given environment. Certain high-value computing assets may be protected by alternative suppression systems that reduce further incidental damage (i.e., water damage) in the process of extinguishing flames or fluctuating temperatures.

Shielding

Shielding sensitive equipment from errant emanations and environmental interference is instrumental in maintaining an orderly, secure computing environment. Shielded cabling, such as coaxial, safely encapsulates a copper core in layers of protective sheathing materials. This prevents unintentional damage during installation and usage, and also serves as an indicator to intrusive splicing. Shielded monitors prevent sensitive emanations from being observed by passive parties, who may watch undetected over a sensitive end-user session.

Hot and Cold Aisles

Incorporating **hot and cold aisles** in a data center is a fairly recent design concept that allows for proper airflow and reduces the possibility of equipment overheating due to ambient room temperature. The goal is to separate hot (exhaust) and cold (inlet) air. Implementing hot and cold aisles works by placing cabinets in a specific formation where the front sides of the server cabinets face each other, creating cold aisles, and the rear of the cabinets create a hot aisle.

Environmental Monitoring

Temperature, humidity, airflow, and water are critical items to monitor in data centers. Preventing issues is always more appealing than recovering from them, and implementing the proper environmental monitoring controls in a data center will help ensure uptime and system availability. Baselines should be established and any fluctuations detected outside of the baseline range should be addressed immediately.

Humidity and Temperature Controls

Sensors that can detect changes in temperature and humidity should be placed in the data center to effectively monitor the environment. Some solutions have the ability to take corrective action (e.g., enabling a dehumidifier).

Video Surveillance

Video is an effective means of monitoring any environment and any recorded footage can be very valuable in an investigation, especially due to the inarguable nature of the material. Real-time video monitoring, however, requires the presence of an actual person, typically a security guard, and to be most effective, cameras should be placed in critical locations with ample light and the best possible range of view. When possible, bubble cameras should be used as attackers are uncertain about which direction the camera is pointing or if the camera is being controlled remotely.

Disaster Recovery Plans and Procedures

Disaster recovery carries the grave implication that some disastrous event has caused disruption or destruction to ongoing business operations. A disaster can be any natural or man-made event ranging from environmental accidents to extreme weather and workplace incidents to acts of terrorism. Either way the end result is constant: business operations are crippled and impaired in some critical manner. Disaster recovery exercises must be carried out regularly to ensure effectiveness of the DR plan and to identify and resolve any deficiencies identified during the exercise.

Disaster Recovery Exercises

Few DR plans are static documents that are never exercised or rehearsed. DR is a trend-following live document format that adapts to changing circumstantial, environmental, or surrounding conditions. DR rehearsal exercises the mechanisms, methods, and manpower that facilitate recovery procedures. **Pilot testing** is the practice of validating application updates, configuration changes, and system modifications prior to deployment. Perhaps nowhere is this more necessary than in proving the correctness of DR strategies. DR exercises can range from walkthrough simulations to complete failover testing.

Backups, Execution, and Frequency

The best recovery strategy for disruptions and disaster includes current, consistent backups. The best recovery strategy is specific to the conditions, considerations, and criteria for a given site or situation. It can be simple (e.g., tape, USB, CD, DVD) or complex (e.g., cloud hosted, offsite, mirroring, encrypted) to suit a variety of needs, but every backup process must be repeated and consistent. Backup methods are summarized below.

While data backups can also be created using online services (cloud based), there are overhead and security implications to thoroughly consider. Offsite data backups also present unique advantages and disadvantages that must be specially considered for each site and situation.

- **Full backup** – The starting point for all other types; contains a complete set of data representing replicated folders and files selected for duplication. Restores all files and folders and results in faster and simpler restore operations but may be inefficient in terms of processing overhead. Full backups are commonly compressed and then encrypted.
- **Differential backup** – Contains only files that have changed since the last full backup and considerably shortens backup and restore periods. Overdoing differential backups can cause backup image size to grow beyond the baseline full backup image.
- **Incremental backup –** Stores all files changed since the last full, differential, or incremental backup procedure. Completes in less time than other methods but individually processes incremental backup images during restoration, which can elongate recovery times.
- **Mirror backup –** Similar to full backup but typically without file compression, encryption, or password protections offered by commercial solutions. Mirror backups are exact duplicates of original on-disk data.

Redundancy and Fault Tolerance

- **Redundant Servers**
  Redundant servers and redundant services create safety net-like fail-over conditions where primary server or service functions are carried out by alternate secondary servers and services. Redundant server and service setups create an operational setting where much-needed resources are constantly accessible because backup and standby units are poised to take over when primary units are taken out. Redundant servers and services also provide **clustering** or **load-balancing** capabilities that distribute large computing or network transactions across multiple servers and services to reduce performance impact and resource utilization.
- **Redundant Network Connections**
  A redundant ISP or VPN network configuration continues the same pattern of failover safety as redundant servers and services. Critical business transactions require dedicated public leased lines or other specific arrangements where reliable, sustained connectivity is assured.

- **Redundant Array of Independent Disks (RAID)**
  Redundant array of independent disks enhances the way information is stored and retrieved in high-availability, data-rich computing environments where timely accessibility is required. RAID establishes a multi-disk configuration useful for enhancing write/read performance (striping), data reliability (mirroring), or both (striping and mirroring) at various levels. The most common RAID levels deployed include **RAID 1** (disk mirroring), and **RAID 5** (disk striping with parity across all disks). **RAID 0** (striping without parity) is used strictly for performance and provides no fault tolerance. **RAID 6** (striping with double distributed parity) can continue functioning with two failed drives. Some RAID configurations can be combined to create hybrid solutions, for example, **RAID 1+0 (or RAID 10)**, adds a stripe set to mirrored disks (minimum of 4) and can continue functioning provided none of the mirror sets lose both drives.

  RAID Array Classifications:

  a. **Failure-Resistant** – protects against data loss due to disk failure.
  b. **Failure-Tolerant** – protects against data loss due to component failure.
  c. **Disaster-Tolerant** – systems using multiple zones to provide access to stored data.

Clustering

A **cluster** is a group of systems which are connected together and monitored, usually by a heartbeat packet, to distribute the workload (load-balancing) or to failover (high availability) to other systems should an outage occur.

Load Balancing

Load balancers were discussed thoroughly in Domain 1 and are available in two different forms, hardware and software. The primary benefits of a load balancer, as the name would suggest, is to distribute the load between multiple systems, networks, or devices so that a single entity that is providing a resource is not overwhelmed. Load balancing also adds redundancy in the event a system fails.

High Availability

Availability – the quality of being accessible when necessary – is a key element in the **Confidentiality-Integrity-Availability (CIA) Triad**, discussed later in this guide. Being available refers to the ability for the user community to freely access a system or service, but **high-availability** denotes a more drastic nature where a business is operating at minimal capacity due to unplanned downtime or unscheduled interruption. Despite disruption to major company operations, critical business functions may continue until a full recovery is complete.

Cold Site

A **cold site** is a low-cost, entry-level backup site solution with the most time-consuming recovery phase of all other site options. No original hardware, software, or information is carried over until a disruptive event occurs. Lack of setup lowers initial investment cost but incurs additional cost when restoring the failed services. Cold sites require very little to no maintenance.

Warm Site

A **warm site** comprises the necessary computing equipment and network connectivity to make a more graceful and timely recovery phase than with cold sites, but with a clearly added cost increase. Warm sites may contain backups that may not be the most recent, but are much closer to the recovery goal line. Any warm site will require a moderate amount of maintenance to keep it at operating capacity.

Hot Site

A **hot site** is any backup site location where an interrupted business may continue full operation following a natural disaster or unnatural disruption. Hot sites are specifically defined as being exact duplicates of the original environment, fully operational in every way including near-complete backups of original information. As expected, every hot site requires a heavy amount of maintenance to keep operational including up-to-date changes, mirrored configurations, and recent information. Hot sites are the most expensive form of site an organization can adopt, but the time to restore is greatly reduced as compared to the other site options.

Mean Time to Restore (MTR) Mean Time Between Failures (MTBF)

The **mean time to restore (MTR)** is the average amount of time the restoration of a system or process will take when recovering from an outage and is usually outlined in a maintenance contract. The **mean time between failures (MTBF)** is the amount of time that passes between system failures and is defined by the vendor who manufacturers the equipment.

Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

Recovery Time Objective (RTO) is defined as the amount of time within which a failed system or process must be restored and includes the time necessary for resolving the outage and testing functionality. A **Recovery Point Objective (RPO)** is also referred to as the acceptable amount of loss a company can incur during an outage. The RPO is the target point in time that data must be recovered from after a failed mission-critical system or process has been restored.

Confidentiality, Integrity, and Availability

Three concepts comprise the CIA triad: **confidentiality, integrity, and availability**. Combined, these concepts form the basis of well-designed security architectures, frameworks, and platforms. When designing a security control infrastructure, the ultimate objective should be to provide controls for these three elements. The following are common definitions of these terms that can be applied to assess security risks.

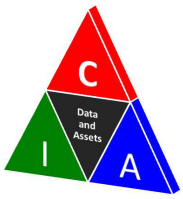

Figure 7: The CIA Triad

- **Confidentiality** prevents sensitive information from being disclosed to unauthorized recipients. The intent is to reduce or eliminate the risk of financial loss, public embarrassment, or legal liability from unauthorized disclosure of sensitive or critical information.
- **Integrity** ensures that information resources are changed only in a specified and authorized manner. In this case, the goal of security is to reduce or eliminate risk to the business if critical information is accidentally or intentionally manipulated or corrupted.
- **Availability** ensures that systems operate promptly and service is not denied to authorized users. The risk to the business takes the form of missed opportunities or interruption of operations because of the inaccessibility of information.

Domain 3 – Threats and Vulnerabilities

All people have weaknesses and vulnerabilities. IT systems are no different. Here, **vulnerability** is defined as a weakness in a system that could permit unauthorized access to that system and its data. Along those lines, a **threat** (e.g., person, malware) exploits vulnerabilities to obtain such access. The range of threats, exploits, and vulnerabilities is almost immeasurable as new ones are discovered daily. Threats are unpredictable in nature, and security professionals must focus on reducing or eliminating the vulnerabilities that exist in their environment in an effort to prevent successful attacks and unauthorized access. The most common threats and assessment techniques to detect weaknesses in a network environment are covered throughout this domain.

Types of Malware

Blended Threats

Blended threats are advanced exploits that combine functionality from different types of malware (viruses, worms, Trojans, etc.) and leverage multiple vulnerabilities and attack vectors to be successful and spread throughout a network.

Adware

Advertising-supported software or **adware** is any program that automatically displays or downloads advertisements during application usage. Adware may accompany or integrate into a larger software package and install usage monitoring components, but mostly its purpose is to custom tailor advertisements for targeted users.

Certain types of adware can also be classified as spyware if they perform the same information gathering and snooping functions. **Spyware** is defined later in this section. However, adware is mostly harmless in that it only produces advertisements for goods and services or extended features not included as part of some free or limited software package.

Virus

A computer **virus** is any form of malicious code that spreads from system to system by attaching itself to data or executable files (e.g., exe, scr, dll) after a user runs the file that contains the malicious code. In order to propagate, computer viruses require human interaction. Viruses attach to (infect) files on local systems shared ,network drives, removable media, e-mail, and other resources. USB drives that contain a virus can infect other systems once the USB drive is connected and the autorun component of the USB device activates. Each virus is specifically designed to attack systems in a particular way and target particular areas. The following list briefly describes the different features and forms a virus may take:

- **Resident virus** – A terminate-and-stay resident virus that permanently attaches to the host computer and operates in memory (RAM). It attempts to load before other mechanisms (such as anti-virus software) that attempt to analyze, detect, and identify its purpose and origin and can bypass, interrupt, or manipulate basic operating system functions.
- **Direct action virus** – An aggressive form that replicates and takes direct action when triggered by a condition (e.g., system startup or launching a specific program), date, or event. The direct action virus typically resides in operating system folders or the root directory path where it can be readily accessed and activated to carry out its tasks when the system boots up.
- **Overwrite virus** – A virus that can partially or completely delete information contained in the files it infects, even replacing portions of application code with its own payload. Viruses of this kind are generally easy to identify with anti-virus software, as they generally tend to alter end-user and system applications in noticeable and identifiable ways.

- **Macro virus** – Certain applications contain embedded scripting or "macro" languages enabling users to automate long series of operations as single shorthand actions. A **macro virus** targets these applications by containing code that replicates and replaces other macros to launch the virus payload when common functions are called.
- **Polymorphic virus** – A virus that can avoid detection through cyclic changes to its original form. Such a virus may encode or encrypt certain code segments that are transformed during run-time as usable code segments, then later encrypt differently than before to evade detection.
- **File infectors** – The traditional virus is a file infector that targets executables to cause direct or indirect execution of its payload. Most viruses fall under this category and are further classified depending on what is targeted and the actions taken during the infection process.
- **Companion virus** – Another typical type of viral infector, the **companion virus** accompanies another ordinary executable file. When the source file executes, control is passed to the companion virus and the end-user remains completely unaware.
- **Boot sector virus** – Boot sector viruses target the system's boot sector to ensure that the virus always loads before the operating system. A boot sector contains the information necessary to execute programs and mount volumes, as well as locate and start the operating system. Though less common, these viruses still flourish since master boot records (MBR) and other disk allocation methods see continued use.
- **Multipartite virus** – Commonly reside in memory and are distributed through infected media. When the media is inserted into the computer, the virus moves to the boot sector and infects files on the system.
- **Stealth virus** – Stealth viruses attempt to trick anti-virus software (e.g., reporting as detected and cleaned), or are able to hide from anti-malware engines altogether.

Worm

Worms are as undesirable as they sound. A **computer worm** is exploitive malicious code like a virus in that it self-replicates; however, all similarity ends there, as one thing a worm does that a virus cannot do is replicate directly across networks. Worms are also generally designed to leverage some software, system, or service vulnerability to enable propagation across network connections.

Spyware

If the term *spyware* brings to mind images of people watching you without your knowledge or consent, you're on the right track. **Spyware** refers to computer software installed surreptitiously and without the owner's or operator's consent and then attempts to harvest personal information (e.g., usage trends, software licenses, sites visited), invades privacy, or manipulates browser activity. Such software appears to be legitimate but contains hidden functionality that is otherwise undesirable and unwarranted.

Trojan

In *The Aeneid*, Greek warriors packed into an enormous wooden horse disguised as a victory trophy and invaded the city of Troy, thereby managing to wreak havoc on unsuspecting rivals. This story's outcome isn't far from what happens with respect to network security. The classic **Trojan horse** is a class of computer threats that seemingly performs a desirable function (launch a game, activate an e-card) but instead transparently or invisibly conducts malicious activity to allow unauthorized access and/or usage of the affected machine. A Trojan horse application is often disguised as a legitimate application or a portion of some software suite and opens a back door into the system when invoked by the user unless designed to trigger upon some condition, date, or event.

Rootkits

Malware consisting of a program or collection of programs designed to hide one's presence and activity on a compromised system is called a **rootkit**. An attacker must first gain access for the rootkit to be truly effective and various layers of the operating system are manipulated to disguise activities, applications, and connectivity from watchful administrators.

Backdoors

A **backdoor** is any unauthorized, unguarded, and undocumented manner of access that bypasses normal security protocols, processes, and procedures. If an attacker gains access to a system and they wish to reconnect to that system later, then they will often reconfigure that system to allow access through the same means and usually reconnect undetected. Attackers will use rootkits to assist in the opening of back doors as well as the concealment of the backdoor access and activity.

It is not uncommon for malware to create a backdoor and notify the attacker once the system is successfully infected. This technique is often employed when the malware is designed to configure the target system to join a botnet, a collection of infected computers controlled by attackers over the Internet. Botnets are further defined later in this section.

Logic Bomb

Any malicious code that lies dormant until triggered by some condition, date, or event is called a **logic bomb**. A trusted insider could emplace a logic bomb to cause damage in the event of their firing or as part of industrial espionage for a competitor. Generally, logic bombs appear as part of some other unsuspecting software package and are invoked without the end-user's knowledge.

Botnets

A collection of networked computers that have been compromised by malware operating in a collected, cohesive fashion (coordinated by a controller computer) is called a **botnet**. Individual computers are captured and controlled by a **bot** or malicious application that leverages remote control for an attacker, the **bot herder**. Command and control channels are often basic IRC channels containing other bots within the botnet. Bot herders can use botnets for various activities and will sometimes advertise and sell their services in the underground and black market. Bot herders can leverage the combined computing power of their botnets to launch targeted Denial of Service (DoS) attacks, run spamming campaigns, and more.

Types of Attacks

Man in the Middle (MitM)

An attacker that can get in-between a trusted client-server connection can perform a **man-in-the-middle (MitM) attack**, which is the interception and tampering of data by an unauthorized third party. Email, FTP, web and even Secure Shell (SSH) connections can be subject to MitM attacks. MitM attacks involve intercepting and entering into a private conversation by eavesdropping and/or modifying data, without the user's knowledge. Figure 8 illustrates this type of attack.

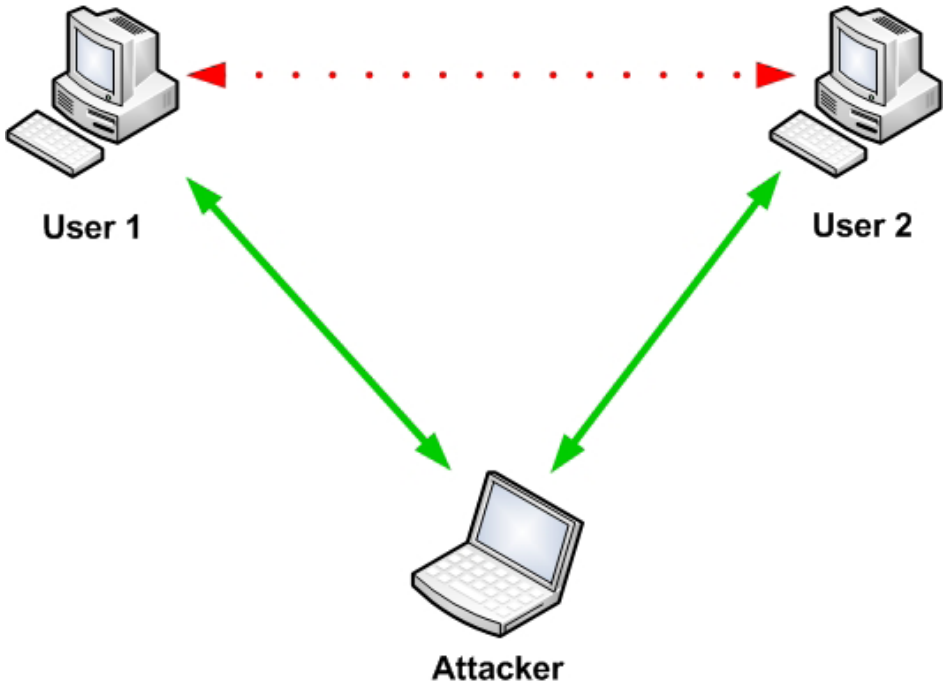

Figure 8: Man in the Middle

Man in the Browser (MitB)

Similar to MitM attacks, a man-in-the-browser attack is a fairly new term defined as an attack that infects the web browser and modifies web content (e.g., transactions) without the user or host's knowledge. MitB attacks can be successful even if the connection is encrypted or the user is bound to strong authentication. Verifying transactions, like a bank calling the customer by phone before the web-based transaction is allowed to complete, is an example of a way to counter MitB attacks.

Denial of Service (DoS)

As the name implies, a **denial of service attack** renders legitimate resources unavailable to authorize entities (e.g., applications, users, services). DoS attack frequency and intensity varies: it may require a single packet or a sustained flood of service requests to saturate a server or service to the point of making it unable to respond in a timely fashion. Local DoS attacks render individual workstation or server computers unresponsive while a remote or network-specific DoS affects multiple users and connections.

Distributed Denial of Service (DDoS)

The scalable version of DoS is the **distributed denial of service** or **DDoS** attack. Multiple computers employ the same application, platform and protocol attack methods as the DoS variety but with the magnified impact of tens, hundreds, or thousands of participants. Harnessing large groups of zombie computers – attacker-controlled client PCs and sometimes server computers—leverages the multiplying power of several workhorses to saturate and overfill a target so that legitimate users are denied access.

TCP Replay

A **TCP replay** attack reuses captured network packets in modified form against an original party of some trusted network conversation. Weak network stack implementations may foolishly parse and process the tampered protocol data and establish a trusted but bogus connection. The TCP replay attack may be a prelude to further attack, such as activating an authentication mechanism that in turn enables a secure connection from an attacker-controlled (thus unauthorized) source.

Ping of Death

The **ping of death** exploits the maximum size limit that ping (ICMP) packets should be. Attackers would craft packets that were equal to or exceeded the 65,535-byte limit causing the computer to crash (a normal ping is 32 or 84 bytes). To date, this vulnerability has been closed on most systems and current NIPS/NIDS/FWs are able to detect it. Attackers can also execute a ping flood, a type of DoS attack, which sends an overwhelming amount of ping traffic to a system, preventing delivery of other network traffic.

Smurf Attack

Don't let its name deceive you. There is nothing cartoonish and cuddly about a **smurf attack**, which is a denial of service attack that takes advantage of vulnerabilities in network configuration, and uses packets containing a spoofed IP address (belonging to the target victim) to direct an overwhelming amount of traffic to the victim's system. Using the ping utility, the attacker sends a significant amount of Internet Control Message Protocol (ICMP) ECHO REQUEST messages to devices that will broadcast the traffic throughout the network, and any machine that is online will return all responses (ECHO REPLY) to the victim's system. Networks that aren't configured to stop broadcast traffic, filter ICMP traffic, or reject packets that have forged IP addresses are vulnerable to smurf attacks and can also be used as an amplifying network to carry out attacks on other networks.

Spoofing

Spoofing is a form of abuse based on identity and trust. Spoofing appears in many forms as an attempt to gain authorized access by an illegitimate party posing as a legitimate source. An assumed identity links the various forms of attack: sending email under a false identity, manipulating target network stacks using bogus protocol information, and forging parameters in a chain of messages or communication are just a few examples.

Spam

Unsolicited commercial email messages (UCE), particularly those sent indiscriminately to tens, hundreds, or thousands of e-mail addresses is called **spam**. Spam is the electronic form of postal "junk mail," filling inboxes with useless and unrequested material typically used for marketing purposes. Spam can also be malicious in nature ranging from messages that contain hyperlinks that connect to malicious downloads or phishing schemes requesting personal information. Many examples exist and spammers often guess at e-mail addresses, buy valid ones, or perform directory harvesting attacks to obtain valid ones. Directory or address harvesting is accomplished by the attacker repeatedly sending email messages to a valid domain, and then filtering out any non-deliverable receipts.

Phishing

Phishing is the criminally fraudulent process of obtaining personal information directly from the source while masquerading as a trustworthy entity (e.g., on-duty manager, system administrator, loan officer). During a phishing scheme, attackers pose as institutions the target recipient may do business or be familiar with (e.g., bank, not-for-profit [donations]). User credentials, credit details, financial information, and other PII are frequently the valued gains that attackers are seeking from phishing schemes. Phishing takes many forms ranging from e-mail spam to instant messages and even mobile phone texts and usually redirect to a web site that appears to be legitimate.

Spam over Instant Messaging (SPIM)

Unsolicited messages that are sent via instant messaging applications such as Yahoo Instant Messenger and Windows Live Messenger are often referred to as **Spam over Instant Messaging (SPIM).** A couple of the countermeasures used to combat SPIM include plug-ins for the IM client and only accepting messages from people on your contact list, a/k/a white listing. Organizations that use IM internally often deploy spam and content filters for their Instant Messaging platform.

Vishing is term that has been adopted to define social engineering attacks that occur through a telephone conversation by exploiting weaknesses in Voice over IP (VoIP). Vishing is further defined in the next section.

Spear Phishing

As with phishing, **spear phishing** also attempts to obtain personal or confidential information by imitating a legitimate source. However, spear phishing is targeted at a group of victims that have something in common, like using a specific bank or service, or working for the same company. Spear phishing attacks can be quite effective as the messages are well-crafted and convincing since they often look almost identical to the real thing. Security awareness, properly configured spam and e-mail filters, and regular patching (in the event the phishing message contains a link to web site housing malicious code) help combat spear phishing. One example of a spear phishing campaign would include messages that "require" a user to change the logon credentials by visiting the bank's web site. Unbeknownst to the user, the site is fake, their password does not get changed, and the attacker now has the user's legitimate logon credentials in his or her possession.

Xmas Attack

In computer networking, a packet that has all options enabled for the protocol in use is referred to as a Xmas packet. Attackers monitor how the target system will process such a packet, which can allow the attacker to obtain technical details about the target system's operating system. Xmas packets are usually categorized as malicious and can be detected using newer firewalls or intrusion detection systems (IDS). A large amount of Xmas packets sent to a victim's computer can result in denial of service as they require more resources to process.

Pharming

Pharming is similar to phishing with respect to its goals and objectives, but pharming leverages domain name service (DNS) poisoning, which will redirect a web page to an illegitimate source when a victim attempts to access a valid web site. Attackers will modify (poison) domain name service (DNS) records to send valid URL requests elsewhere. The site the victim is redirected to is convincingly identical to the original, and are often short-lived.

Privilege Escalation

Multi-user computer systems are designed for interaction among numerous users and user groups, each having separate and incompatible permissions to perform various activities. For a system attacker, the ideal user account has administrative privileges on the system and is permitted to perform virtually any task—particularly those that further intrusion, infiltration, or interception of valuable information. A **privilege escalation** attack exploits a configuration error, design flaw, or exposed vulnerability in a privileged security application to gain illegitimate access to protected resources.

Malicious Insider Threat

The insider threat, or **malicious insider threat**, is one of the most significant things an organization is vulnerable to as the attacker has already been granted some level of access to company resources. An insider is usually an employee or someone who does business with the organization and is trusted to a degree. As the level of access the insider has increases, so should the level of security controls placed around the assets. The insider threat poses the greatest risk to system availability, confidential, and proprietary information, such as trade secrets and PII of customers, and motivation can vary from revenge to financial gain.

DNS Poisoning

The **Domain Name Service (DNS)** is a caching service that maps information related to assigned numeric IP addresses and easily-memorable domain name identifiers. DNS translates between the dotted-decimal notation addresses (63.146.189.101) and the domain name (preplogic.com). DNS cache poisoning occurs when a server receives information that does not originate from an authoritative source (and is therefore illegitimate and invalid) and serves it to unsuspecting victims. Subscribers of an ISP are affected when their DNS lookups produce incorrect results (i.e., redirection to a bogus or imposter site of the attacker's choosing).

ARP Poisoning

ARP spoofing or **ARP cache poisoning** is an attack against Ethernet that enables an attacker to sniff frames on a switched network and redirect endpoint traffic through an attacker-controlled machine. It operates on the principle that faked ARP messages can be sent with sufficient volume and regularity that false associations between hardware (MAC) and protocol (IP) are possible, thus invalidating the ARP cache.

An attacker may also launch DoS or perform man-in-the-middle (MitM) attacks through a well-placed machine under control. ARP is not designed for ID validation on its transactions, which makes this attack feasible on modern networks that do not protect the ARP cache or maintain static route tables.

Transitive Access

A **transitive access attack** is defined by gaining unauthorized access to a system that has access to the system the attacker is truly targeting. A transitive attack takes place because the attacker doesn't have direct access to the target system that contains the assets they desire. For example, attackers may attempt to compromise workstations or systems in the more publically accessible demilitarized zone (DMZ) with the expectation that those systems have access to others, usually on an internal network. This process can continue until the attacker gains access to the system they were ultimately targeting.

Client-Side Attacks

A **client-side attack** is an attack where vulnerabilities in a client's operating system, applications, or services are exploited and control of the client is often obtained in the process, like with botnets. In the past, servers were the primary target of attack as they usually hold the resources most valuable to the attacker. The focus of attacking clients shifted due to the number of applications and services they run, access to resources, and the amount of known vulnerabilities that exist in the client-side environment.

Types of Social Engineering Attacks

Shoulder Surfing

Shoulder surfing is another low-tech attack that's really a basic invasion of privacy by nosy busybodies and unscrupulous individuals overlooking your computing activities. An observer may be posted around or behind you in a cubicle setting, standing within sight of your ATM transaction, or stationed within range of binoculars, but the overall end-result remains identical. Truly effective shoulder surfing attacks are difficult for the victim to detect because they're preoccupied by some activity (e.g., inputting a PIN, typing a password, pressing a numeric keypad) that engages their full attention—and the attacker's.

Dumpster Diving

Classic **dumpster diving** (also called **trashing**) is the practice of sifting through garbage to recover discarded items of value to the dumpster diver. In a computing context, dumpster diving is the invasive act of rifling through waste bins to discover confidential, proprietary, or sensitive information carelessly discarded without consideration to its value. The dumpster diver varies in sophistication and targets whatever information suits: financial data related to acquisitions and mergers; employee payroll information; credit card details; social security numbers; and any other manner of private data.

Tailgating

Tailgating is the process of following someone through a restricted area after they have provided their access credentials (e.g., key card). The tailgater rides off of the credentials of the person before them and no record of the tailgater entering the area is recorded, with the exception of video monitoring.

Tailgating can occur intentionally or unintentionally and with or without consent. High security areas may have stricter screening mechanisms in place (e.g., ID check by a person not just a system) or might implement mantraps to prevent tailgating. With a mantrap, an individual provides his or her access credentials and enters an area that includes another access door where the individual must provide the credentials again before entering the restricted area. Access through the second door is granted only when the first door closes and credentials are validated again.

Impersonation

A commonality between threats like phishing, pharming, and vishing, is that of **impersonation** – mimicking the behavior and/or appearance of someone or something else. Attackers who use vishing will often impersonate help desk personnel, employees, or financial institutions to convince the victim that they are legitimate. Impersonation is the primary technique that ultimately determines whether the attack will be successful or not. Impersonators can also appear on premise wearing certain clothes like a maintenance uniform, or presenting forged credentials like an ID card to obtain access.

Hoaxes

A **hoax** is a low-tech attack predating upon the collective general naiveté or technological ignorance of its target audience. The hoax is an attempt to dupe or deceive its audience into accepting, believing, or conceiving that a falsehood is real and true. Classic Internet hoax format follows traditional urban legends but are generally reworked or written in a computing context and use e-mail or web sites as a vehicle for delivery. Internet hoaxes are essentially practical jokes intended to mislead its readers with no ill effect, but in some cases the wrong hoax at the right time can have consequence—such as announcing false reports of financial or internal troubles to drop a company's stock value. Other common hoaxes indicated that computers were infected with a virus and that a specific file needs to be deleted to remove or prevent infection (typically a valid system file or file of importance).

Whaling

Whaling is a targeted phishing scheme that focuses on corporate executives and high-level employees as the victims. Corporate executives, high-level managers, and the like are the targeted victims because of their access to sensitive corporate resources. Whaling schemes are commonly delivered via e-mail, are intricate and very well crafted, and can often fly under the radar as the targeted recipient list is very small.

Voice Phishing (Vishing)

Vishing is term that has been adopted to define social engineering attacks that occur through a telephone conversation and often by exploiting weaknesses in Voice over IP (VoIP). The goal of a social engineering attack is to convince a person into releasing personal or confidential information by posing as a legitimate source. Vishing's goal is identical to that of phishing in that the target asset to be gained by the attacker is typically financial information, access credentials, or PII.

Types of Wireless Attacks

Rogue Access Points (APs)

There are many problems with **rogue APs**, which are unauthorized wireless installations on a protected network. A rogue AP exposes unsuspecting clients to all sorts of attack vectors (e.g., hijacking, phishing, data theft) and backdoors can grant access to unauthorized parties. It can also destabilize a wireless network by causing wireless channel conflicts among connecting client devices or other APs and can cause other disruptive harm. Detection of rogue APs is possible through wireless intrusion detection systems and radio spectrum monitoring for unauthorized entries.

Evil Twin

Attackers can deploy rogue Wi-Fi access points (AP) to lure victims into connecting to what appears to be a legitimate hotspot. Attackers will then monitor the connections to the rogue AP and/or redirect the victim to a malicious web site in an effort to steal logon credentials and other sensitive information.

Interference

Wireless **interference** impacts availability of the network and access to resources. Some forms of wireless transmission are more vulnerable to interference than others. While interference with wireless networks is usually unintentional, attackers can use jammers, devices that purposely interfere with wireless access points, to cause issues and create a denial of service.

Wardriving and Wireless Broadcast

The practice of actively seeking freely broadcast wireless transmissions and obtaining unauthorized access to the network from a moving vehicle is called **wardriving**. Laptops and PDAs are most commonly used in wardriving, but specialized designs comprising multiple antenna arrays and adapter cards are also used. GPS may also be employed as a means to measure and mark locations to generate an overhead visualization of detected wireless hotspots.

Wireless networking uses Service Set Identifiers (SSIDs) to identify 802.11 LAN segments and is the most direct means by which wireless networks are discovered. Disabling SSID broadcast alone is insufficient to prevent discovery through wardriving or other practices. VPNs can be implemented to foil eavesdropping, APs should be isolated from the internal (wired) network, rogue APs should be detected and eradicated, MAC address filtering should be used, and the use of 802.1x authentication can be used to deter wardriving and unauthorized access. In addition, the default admin password should be changed and firmware should be kept current on the device serving as the AP.

Bluejacking

Bluetooth (BT) is a wireless communication technology that uses hardware modules that allow devices to communicate over short distances using short wavelength radio transmissions. Bluetooth is not immune to attack and as a simplistic wireless protocol, it provides weak security against casual and complicated techniques alike. **Bluejacking** is a method of issuing unsolicited anonymous text messages to BT-enabled mobile phones. These messages often link to malicious web sites or are used in phishing schemes.

Bluesnarfing

Bluesnarfing is unauthorized access (and copying) of information through a Bluetooth wireless connection. More sophisticated attacks can coerce passing BT-enabled phones to dial attacker-controlled long distance numbers and rack up calling charges of unsuspecting subscribers.

Warchalking

Warchalking is the process of advertising the location of open Wi-Fi access points in public places (e.g., walls, signs, and sidewalks). While similar to the "Free Wi-Fi" or "Hotspot Available" signs commonly seen in commercial establishments, warchalking symbols indicate the location of APs, with no regard as to who owns them.

IV Attack

IV stands for initialization vector, which uses the symmetric key and the RC4 cipher to apply randomness to the encryption process. Unfortunately with Wi-Fi, WEP specifically, the same IV value might be used repeatedly, which could allow an attacker to discover the encryption key that is used.

(Note: Network protocol analyzers or **"packet sniffers"** are another type of attack discussed previously.)

Types of Application Attacks

Cross-Site Scripting (XSS)

A **cross-site scripting (XSS)** attack occurs when an attacker is able to convince a victim to run a malicious script within a web browsing session. The malicious script (e.g., java, ActiveX) exploits vulnerabilities of the web browser or web application. The result can be stolen logon credentials, page redirection, hijacked sessions, data theft, or a combination thereof. XSS attacks are in wide use and there are two primary types of XSS attacks, stored and reflected. To defend against XSS attacks, multiple security controls should be implemented on the client ranging from anti-malware software to keeping web browsers and web applications current with their version and security patches. On the server side, organizations should deploy web filtering gateways or next generation firewalls, and validate the input sent to the servers by clients. Input validation attempts to cripple such attacks by removing any unnecessary elements. Output that is processed by the server and then sent to clients should be validated / sanitized to ensure no malicious code exists. Output sanitization can be more effective than input validation.

- **Stored XSS Attack** – The malicious code resides on a web page or in a database, isn't generated dynamically, and is initiated in the user's browser session on page launch.
- **Reflected XSS Attack** – The malicious script is sent to the user after the server receives a request from the client session and is launched when the server returns the results of the request to the web browser. Hyperlinks containing commands within them are commonly used to activate reflected XSS attacks.

Cross-Site Request Forgery (XSRF, CSRF, or Sea Surf)

Attackers create a web page that contains malicious code and tricks end-users into launching that page, like through a targeted spear-phishing campaign. **XSRF** attacks execute under the identity and with the rights assigned to the end-user and typically trick the user into performing actions they didn't plan on doing like changing account information, purchasing products, and more.

SQL Injection

A **SQL injection** attack occurs when SQL commands that will execute on the database are sent through a web based application. Attackers are able to manipulate the database using SQL injection attacks and can steal data, change product prices, and carry out other nefarious activities. Database Activity Monitoring (DAM) and Database Firewall products monitor traffic sent to databases to validate input and detect and eliminate SQL injection attacks.

Lightweight Directory Access Protocol (LDAP) Injection

Lightweight Directory Access Protocol (LDAP) connects systems and applications to the directory in a company so entries in the directory tree can be queried and/or modified to customize the output sent to the client. **LDAP injection** attacks prey on vulnerabilities in web applications that have access to query or modify the directory tree. While less common, LDAP injection attacks are very similar to SQL injection attacks in the way they work and in that the content of the request is not validated.

Extensible Markup Language (XML) Injection

XML has a wide variety of uses from providing web services, rich Internet content, system configuration, to acting as a database. Similar to both SQL and LDAP injection, attackers exploit vulnerabilities and the openness of XML to inject malicious code, modify the application's behavior, and retrieve or modify data. Preventing **XML injection** attacks also requires the validation of input, and more extensive deployments may choose to deploy a monitoring or firewall solution for added protection.

Directory Traversal / Command Injection

Internet facing web servers are a common target for attack and should be hardened to prevent unauthorized access, preserve the integrity of the data, and ensure availability of the system. **Directory traversal injection attacks** exploit vulnerabilities in the hypertext transfer protocol (HTTP) to access data and files on the local file system of the web server. Attackers are also able to then run commands locally on the web server, which could allow further access into the internal network, like to a connected database or directory server. As with the other injection attacks mentioned, input validation, regular patching, and monitoring solutions are effective ways to combat this threat.

Buffer Overflow

A **buffer overflow** attack redirects program execution flow to perform attacker-defined tasks by overfilling the boundaries of a stack or memory-based storage region. By carefully crafting a payload and trampling over important code constructs, attackers may leverage control over a program that would otherwise crash or corrupt data. Buffer overflow attacks may target applications, services, and operating system (kernel) code.

Zero Day

Zero day vulnerabilities and **zero day exploits** are terms used throughout the security industry to describe attacks that have not yet been observed and leverage a vulnerability that has only been discovered by attackers, or is a recent discovery that does not yet have a fix. Behavioral monitoring, like with NIPS/NIDS systems and heuristic scanning engines, can sometimes be an effective means of defense, but most often the best defense against zero day attacks is the overall process of following best practices and implementing the proper defense-in-depth strategies and incident response procedures.

Cookies

Unlike the delicious chocolate chip variety most of us are inclined to imagine, internet **cookies** are text files that help track and maintain various site-related activity from your web browser. Cookies facilitate authentication, session tracking, and maintenance of user-specific data (such as browsing preferences). They are simply non-executable pieces of data that affect the operation of a web server—not the web browser—in very specific ways, but are generally viewed as untrustworthy because cookies keep tabs on browsing and viewing habits. Attackers can craft malicious cookies that can monitor web activity of the victim.

Attachments

Attachments are files that are sent along with e-mail messages or uploaded through a web page to a server. Using anti-spam and e-mail filtering products, most e-mail systems today prevent the delivery or uploading of files that aren't business related and usually contain malicious code (e.g., EXE, INI, SCR). Servers that allow the uploading of files also restrict which types of files can be submitted and scan the ones that are allowed for malicious code. In some instances, these restrictions can't be in place and scanners that look for malicious code should be deployed.

Malicious Add-Ons

Web browsers can run multiple add-ons or extensions to increase functionality and interact with media rich web sites and range in purpose, behavior, and provider. Most add-ons are based on scripts (e.g., ActiveX, java) and run client-side. Some examples include toolbars, extensions, and search providers. While these add-ons can add value and better the user experience, they can also be exploited. Add-ons that are completely malicious in nature also exist. Malicious add-ons can range in purpose from compromising web browsing sessions or the local system to siphoning data and more. Organizations should lock down web browser configurations, prevent the use of unauthorized plug-ins, and filter Internet activity for malicious code.

Session Hijacking

Session hijacking or **TCP/IP hijacking** involves an attacker forcibly gaining control over a legitimate conversation between a trusted connection between two parties. Session hijacking is possible when the attacker is able to intercept transmission details between the two sources (being positioned somewhere along the line between source and destination) and then carry out a MiTM attack, impersonating one of the legitimate client connections and communicating with the other, while they are under the belief they are still speaking with the same entity. IPSec is an example of a countermeasure to session hijacking as mutual authentication is required and the transmission is encrypted.

Header Manipulation

Header manipulation is another form of attack that relies on the absence of input validation. Header manipulation modifies the header information contained in HTTP requests that are passed to web applications through clients and can be used to initiate XSS attacks, hijack pages, redirect web pages, and more.

Types of Mitigation and Deterrent Techniques

Manual Bypassing of Electronic Controls

Fail Safe / Secure vs. Fail Open

When a system fails it can do so in one of two ways: securely or opened. An example of a **failsafe** or **fail secure** scenario would be a physical lock that fails, but remains locked, or a system that when failing terminates all processes that are currently running with elevated or system level privileges so they cannot be exploited later.

A **fail open** example would include the opposite: a door lock that fails but remains unlocked, or maybe a spam filter that fails and allows the delivery of all e-mail.

There are reasons to implement both fail states and when choosing products, vendors should be questioned as to how their products handle failures, especially when handling sensitive data, or needing to comply with regulatory or legal restrictions. Systems that contain sensitive information and process critical transactions should fail in a secure manner and the health of both the data and system should be validated before it is brought back online.

Monitoring System Logs

Networks today contain numerous logs that exist on multiple devices and are overwritten and updated usually in real time. To ease the burden on monitoring each individual log for anomalies, as discussed in Domain 2, many organizations today are correlating logs from multiple systems for central analysis by a Security Events Manager (SEM), Security Incident Manager (SIM), or both (SIEM). The information stored in log files is invaluable and serves as a key component when investigating incidents and troubleshooting. Log file size and entry limits should be set appropriately and should be backed up regularly, especially on mission-critical systems. Log types include the following:

- **Event logs** – Contain information related to system configuration, issues, failures, and changes.
- **Audit logs** – Created specifically to record system changes in a simple form.
- **Security logs** – Track and record security specific information like intrusion attempts or malware infections.
- **Access logs** – Stores both successful and unsuccessful access attempts made against resources that are being monitored.

Physical Security

A comprehensive security strategy covers all boundaries whether electronic, mechanical, physical, or virtual. The strongest security solutions are significantly weakened when exposed to direct attack, and insufficient physical protection is the shortest and surest path there. That pervasive defense-in-depth strategy also encompasses physical protections to site, facility, equipment, and personnel.

Hardware Locks

Hardware locks create the most basic and fundamental form of security. A hardened server sporting the latest in cryptographic and security technologies is indefensible without the security doors and locking mechanisms that safeguard the server room. There are many types of electronic and mechanical locks that suit a number of purposes (e.g., combination locks, keycard entry, biometric authentication, keyring keys), which must be chosen to fit the circumstances and conditions.

Door Access Systems

A **door access system** is any self-contained security system that provides physical access control to secured rooms and buildings. They typically operate in stand-alone environments, accessed by a single management computer for programming and reporting tasks. Systems may feature keypads, card readers, or some biometric form of authentication for authorized entry.

Physical Tokens

Any physical token is specifically a something-you-have authentication factor. The most basic and commonly understood form is the key access card and corresponding card reader that permits employee entry to an electronically-guarded entrance. Smartcards contain integrated circuitry and embedded chips, RSA SecurIDs cyclically generate pass codes, and proximity cards use radio frequency (RF) transmission for physical token access.

Mantraps

Original **mantraps** were mechanical devices designed to catch poachers and trespassers, and the modern variant takes a page from that history. Modern mantrap usage employs physical access controls that restrict human passage into protected sites, facilities, and rooms. In extreme cases, a series of protections might include guarded double-doors presenting differing security challenges of varying complexity and design.

Video Surveillance

Closed-circuit television (CCTV) and other forms of video surveillance provide adequate passive monitoring devices that augment existing physical access and control strategies. Video surveillance makes for an ideal witness during investigations and an unbiased observer for monitoring tasks. Units range from low-power charge coupled devices CCDs (an integrated circuit that allows for high quality recording in lowlight situations),to infrared, ultraviolet, and thermal trigger systems. CCTV cameras becoming increasingly more powerful and smaller in size for optimal placement, and some systems include specialized equipment for capturing license plates and other items that are reflective or don't normally record well. Video monitoring must be persistent and augmented by recording and cataloging practices to be truly effective.

Fencing

Fencing is one of the first lines of defense and acts as an effective deterrent in both keeping unauthorized visitors out, and directing visitors to an authorized point of entry (e.g., security gate). Fencing can be used to keep people out or keep people in, especially when applied to high security environments that may also choose to deploy high fencing, electric fencing, and/or barbed wire.

Proximity Readers

A **proximity reader** uses radio frequencies to monitor for and accept signals transmitted from proximity cards that people carry on them. The use of proximity readers can serve as an efficient tool to allow faster access to an area by automatically permitting access to authorized personnel. If the person is unauthorized, access simply isn't granted.

Access List

A primitive form of physical access control is the **access log**, which is basically a "guest list" of individuals permitted (and sometimes expressly forbidden) access or entry. Receptionists are often called gatekeepers because they singularly allow or deny passage based upon whatever rules are under enforcement, and that usually means consulting a checklist or access log, which can keep details such as who entered where, the duration of stay or visitation, who the person came to see, etc.

Physical Access Control (ID badges)

A complementary component to physical access logs is the employee identification (ID) badge. IDs permit spot-checks of authorized credentials and are among the more primitive forms of access control. ID badges may or may not contain an employee photograph, magnetic stripe or bar code, and other anti-tampering features depending on the level of secrecy and strength of security required.

Hardening

The practice of **hardening** a computer system follows a series of protocols, procedures, and policies that define and describe system security. Blocking unused ports, removing unnecessary services, deleting unused applications, and plugging all known holes are just some activities involved in the system hardening process. The National Institute of Standards and Technology (NIST), System Administration, Networking, and Security Institute (SANS), and others publish guidelines and checklists for hardening various platforms, services, applications, devices, and more. Proper system hardening is usually required and audited when organizations need to be in compliance and is very effective in reducing the attack surface of a particular technology.

Some of the more basic and common hardening practices include:

- **Disabling Unnecessary Services** – Any services that will not be used for day-to-day business should be disabled to reduce the likelihood they will be exploited.
- **Protect Management Interfaces and Applications** – Systems and applications that are used strictly for administration and security should be locked down and restricted for use only by those who are authorized to use them.
- **Password Protection** – Default passwords should be changed on all systems and any passwords that are stored (data at rest) and transmitted (data in motion) should be encrypted. In addition, complex passwords should always be used, especially on critical systems, and this policy should be enforced.
- **Disabling Unnecessary Accounts** – Ideally an unnecessary account should be deleted, but in some cases this may not be feasible for multiple reasons. Some systems come pre-configured with multiple accounts that serve different purposes on the computer. For example, Windows systems include a built-in account named "guest" that permits a guest access to a computer. While this access level is restricted, if there is no intention of using the account, a complex password should be assigned to it and it should be disabled. Attackers frequently target systems and attempt to login or attack the passwords of built-in accounts.

Port Security

- ***MAC Limiting and MAC Filtering –*** MAC addresses are unique identifier numbers attached to network interface cards (NICs) and can be used by a router, for example, to restrict access to the network. MAC addresses can also be intercepted and spoofed by attackers to gain access and MAC filtering should be used in conjunction with other network security control techniques. MAC limiting restricts the number of MAC addresses that can be learned on Layer 2 access interfaces on the switch. MAC limiting prevents the addition of an additional switch.
- ***802.1x*** – 802.1x was discussed in detail in Domain 1, and is a popular security control used to monitor network access. 802.1x is a port authentication mechanism that controls access to the network and is primarily deployed using digital certificates. 802.1x encapsulates Extensible Authentication Protocol (EAP) packets in Ethernet frames for transmission over wired and wireless networks. 802.1x can also be configured to create an encrypted tunnel to pass credentials between the device and authentication server. Devices, also known as supplicants, wishing to connect to the network are first directed to an authenticator where credentials will be provided (e.g., digital certificate or user ID/password set). The authenticator forwards the credentials to the authentication server where the credentials are validated and access is either granted or denied.
- ***Disabling Unused Ports*** – Ports that will not be used, whether physical (wall jack) or logical (router or firewall), should be disabled. With respect to firewalls and systems, disabling unused ports frees up much needed resources that monitor the ports that are in use. As mentioned earlier in this guide, ports that are in use should be carefully monitored and systems that handle sensitive information or process critical transactions should change default port assignments when possible.

- ***Security Posture*** – The current status and effectiveness of an organization's security policies, procedures, controls, and technologies defines the overall **security posture**. Organizations have both a desired or target security posture and a realized one (what's actually in effect). Baseline configurations, security monitoring, and remediation comprise the process that improves a company's security posture.

- ***Security Templates*** – A security template defines the secure basis for building – or creating – security. Templates simplify the process of managing large computer environments and streamline the implementation of several interrelated devices. Windows Server uses predefined security templates to increase network security, which can then be modified to suit site-specific requirements. Similarly, Linux systems using policy enforcement systems can also create, modify, and utilize security templates to achieve a secure baseline.

- ***Initial Baseline Configuration*** – A configuration baseline is a configuration management strategy that establishes all basic principles and best practices. Configuration baselines are used as the basis for future builds, releases, and changes of system software and hardware components within a hierarchical computing environment. Baselines are ideal for establishing a default secure disposition for various computer and network elements using security templates across several devices. Variations from the baseline often go through a change management process and/or are monitored by special security tools that detect changes to the baseline in an effort to detect intrusions.

- ***Continuous Security Monitoring*** – Continuous monitoring of the environment, system changes, issues, and security incidents provide justification to remediate issues and further improve the security posture of a company. Systems should be monitored for both approved and unapproved changes to the baseline and then remediated accordingly.

- ***Remediation*** – Remediation occurs when changes to the security baseline are proposed or detected. Incident response, risk analysis, and/or change management procedures should be implemented to determine if the change is malicious in nature and should be mitigated, or if it should be allowed, since a change to the baseline configuration may be warranted.

- ***Reporting*** - Every publicly held company is a publicly accountable labor force responsible for disclosing earnings and successes or reporting losses and failures. Governmental agencies, financial organizations, and healthcare institutions are responsible for disclosing attacks, exposures, and thefts related to personally identifiable information. Electronic commerce and online payment systems are responsible for reporting compromises to account holder information. Certain industries are held to revealing particular crimes as they affect clients, customers, or consumers in very specific ways as governed by federal mandates, governmental laws, and industry regulations. Organizations should carefully monitor alarms and alerts, and frequently perform trend analysis on the environment to accurately report on the security posture of a company and address incidents effectively. Proper reporting and response procedures will minimize the impact on the network and its resources as well as identify common vectors of attacks and threats that the organization frequently addresses.

- ***Detective Controls vs. Preventative Controls*** – Detective and preventative controls, while both very important, are very different. Detective controls, like a log, NIDS, or video footage can all be useful in determining what happened and providing a trail of activity that can be reviewed. However, detective controls are only effective for reporting on what has already occurred and provide almost no means of prevention. Granted a security camera may deter an attacker from carrying out a malicious activity, thus preventing the malicious act, it is not designed to stop anything and only records what it sees. The same is true of NIDS, which will alert administrators that an intrusion may have or is taking place. Preventative controls, on the other hand, are the exact opposite and the two complement each other quite nicely. As the name suggests, preventative controls are deployed with the intention of stopping intrusions before they can be successful. Preventative controls, like detective controls, record activity and can alert when an event is taking place, but the focus is on stopping malicious activity in real time. NIPS, anti-malware software, and security guards are all examples of preventative controls.

Implement Assessment Tools and Techniques to Discover Security Threats and Vulnerabilities

Vulnerability Scanning and Interpreting Results

Vulnerability scanning is the automated process of identifying security exposures, risks, threats, and vulnerabilities. Original scanning tools like SAINT and SATAN pioneered the vulnerability scanning field to assist administrators in detecting system and network vulnerabilities, the results of which are as current and relevant as the tool and its checklist database. A **vulnerability assessment** is a method of identifying, quantifying, and prioritizing system or network vulnerability (as enumerated by vulnerability scanning) and naturally complements risk assessment where both catalog, identify, rank, and mitigate risk starting with high-priority items first.

Vulnerability scans can include numerous false positives or findings the tool deems critical, when in reality they may not impact the organization. Vulnerability scans should be performed routinely, always be carried out with the permission of the organization, and the results should be kept confidential.

Scanning Tools

Various tools exist to assist with vulnerability scans, and some vendors offer all-in-one solutions to make the process a bit easier. Unfortunately, while a vulnerability scan may be fairly easy to initiate, interpretation of and remediating the results may not.

- ***Protocol Analyzer / Sniffer*** – Computer networks are monitored using network protocol analyzers or Ethernet "sniffers." Such devices are capable of capturing, filtering, and displaying network traffic so that administrators can visualize various interactions and interconnections. The sniffer is a powerful protocol visualization tool that is also capable of decoding unencrypted protocol payloads, enabling observers to dissect and study higher-level communications—including instant messaging, file transfers, and email messages. Access and installation of protocol analyzers should be administratively prohibited by all but a select few personnel. Guarding against unauthorized analysis is made possible by employing encrypted communications protocols and services or wrapping plaintext protocols in cryptographic tunnels.
- ***Vulnerability Scanners*** – Vulnerability scanners are all-in-one tools that focus on enumerating reachable network services and identifying vulnerabilities based on a number of "fingerprinting" methods. Vulnerability scanning also incorporates functionality to identify configuration and operational weaknesses such as outdated product versions, weak passwords, open ports, running services, and more. A vulnerability scanner provides a summarized report of its findings along with recommended mitigation techniques and/or hyperlinks to more detailed information.
- ***Honeypots and Honeynets*** – Honeypots are fake servers that are set up as low-hanging fruit to entice attackers away from sensitive systems and as containment for observing intruder or automaton (i.e., bots and worms) behavior. An organization uses honeypots to draw unwanted attention away from real computers and operators and serve as early-warning indicators of a break-in. Honeypots often mimic the behavior of their legitimate counterparts to entice attackers to attach to the honeypot instead of the production system. A network composed of honeypots is called a honeynet, which is used to monitor more diverse network conditions and interactions among more sophisticated attackers or attack strategies. Honeypots and honeynets are frequently deployed in demilitarized zones(DMZ).

- ***Port Scanner*** – An integral aspect of a network vulnerability assessment is the **port scanner**, a software tool used to identify listening ports and (to some extent) enumerate listening services. Port scanners are the investigatory tools through which good and bad discoveries are made by administrators and intruders alike. Each port scanner varies in form, function, and feature but all serve a similar purpose in locating the open portals through which most attackers attempt to make entry.
- ***Network Mapper*** – A network mapper is a higher-level learning tool that helps users document and visualize the network topography or logical arrangement and layout of devices. Where a port scanner gains perspective into individual system attributes, a network mapper gains a more comprehensive viewpoint into the attributes of the larger encompassing network. Network mappers use common tools like ping and trace route to determine where systems are located, what route they take, and whether or not they are online. Nmap, a popular network mapping tool, can identify services running on the host, like SNMP, what operating system and version is installed, if any firewalls exists, and more. Network mappers are invaluable tools for network administrators, hackers, and penetration testers alike.
- ***Risk Calculation*** – After performing vulnerability assessments, the findings must be analyzed and risk must be calculated, especially if a finding must remain in a vulnerable state. As discussed in Domain 2, **risk calculation** starts by determining the value of the asset and the likelihood and frequency in which threats can exploit vulnerabilities in an effort to determine the appropriate safeguard(s) for the **identified** asset(s). Once vulnerabilities are discovered, the threats that can exploit the vulnerability must be assessed and the likelihood of their occurrence calculated in order to determine a proper course of action.

Assessment Types

- **Risk Assessments** – Resolve assumptions and uncertainties about risks and threats into clearly considered and well-defined analysis reports. Information security assesses risks through types of risks (risk categories) and how those risks occur (risk factors). Risk assessments can be either quantitative or qualitative.
- **Threat Assessments** – The process of reviewing a particular threat, its capabilities and impact, and the likelihood that it can effectively exploit vulnerabilities and successfully carry out an attack. New threats should be analyzed as they are discovered and announced publicly.
- **Vulnerability Assessments** – Identifying, quantifying, and prioritizing system or network vulnerability (as enumerated by vulnerability scanning) and naturally complements risk assessment where both catalog, identify, rank, and mitigate risk, starting with high-priority items first.

Assessment Techniques

- **Baseline Reporting** – A baseline report captures the existing configuration of a company's network and computing environment and serves as a tool for identifying areas that need better security controls, changes in processing, and more. Baseline reporting also captures the existing environment and can serve as an important tool for establishing the approved minimum level of functionality at which systems and the network should be operating. Deviations from the baseline should be reported, approved, and monitored continuously.
- **Code Review** – Regular code reviews support the "secure by design" principle that attempts to identify and resolve security issues in code prior to release into a production environment. Code reviews should be a required part of any company that develops and releases code to minimize the release of updates as issues are discovered with the application later. Code reviews can be quite involved or simple, and online resources as well as some third parties provide this service. In addition to security flaws, code review can also reveal issues with the application and helps ensure that a quality, as well as secure, product is released.

- **Determining the Attack Surface** – By performing routine vulnerability assessments, researching new and existing threats, and conducting regular risk assessments, companies are able to calculate the attack surface and overall security posture of the environment. Penetration testing, discussed below, is another invaluable tool that can help reveal the attack surface and overall vulnerable state of the network.
- **Architecture** – Reviewing the existing network and system architecture of an organization should be a routine process and can identify areas that may be vulnerable to attack and/or need more strict security controls.
- **Design Reviews** – Reviewing the design documentation of existing, new, or proposed system deployments and changes also provides an opportunity for security professionals to uncover and address potential security risks and should be a part of the change management process to ensure technologies are designed to operate in a secure manner.

Proper Use of Penetration Testing versus Vulnerability Scanning

Penetration testing and **vulnerability assessments** are both crucial components of the overall security assessment framework. The most distinguishable difference is that penetration testing continues where a vulnerability assessment ends. Vulnerability assessments are discovery processes meant to identify sources of risk to system or network; penetration testing furthers this assessment by conducting live exploitive attacks against identified vulnerabilities (targets of threat and areas of risk).

Penetration testing is also referred to as ethical hacking; however, the validity of the term "ethical hacker" is debated still today. The primary difference between penetration testing and vulnerability scanning is that penetration testing actually exploits a vulnerability and access to a target resource is obtained to prove without a doubt that the system or resource is vulnerable to attack. As with vulnerability scanning, penetration scanning should occur routinely and only with the permission of the owner whose systems and network are being targeted. Penetration testing can be carried out using a wide range of tools or with a vendor provided solution.

Penetration testing evaluates system security by simulating malicious attacks and involves active analysis for potential system or network vulnerability. Analysis and activity is conducted from the viewpoint of an attacker to provide near-realistic impact. Technical solutions are provided for both testing and assessment phases, but only penetration testing takes active measures to validate assessment results.

In summary, penetration testing proves that security controls may be ineffective and can be bypassed, and valid obtainable threats exist to exploit identified vulnerabilities. Findings can either be captured in a risk assessment or mitigated. **Vulnerability scanning** is a passive activity that validates the existence of security controls and identifies any misconfigured items that can leave systems open to attack. Penetration testing can be carried out as a black box, grey box, or white box tests which are discussed in further detail below.

Black Box

A **black box**, or blind penetration test, occurs when the test has no prior knowledge of the systems or environment to be tested and the first step in the process will be to identify the location of the systems.

White Box

A **white box**, or full disclosure penetration test, is one that occurs after the penetration tester has been provided with access to and all details about the network and systems connected to it.

Grey Box

A **grey box** test is defined as any version of penetration test that lies between a black box (blind) or white box (full details) testing approach.

Domain 4 – Application, Data and Host Security

The Importance of Application Security

There is an enormous range of computing applications on the market that serve the needs of both home and business users. The multitude and functionality of applications available create a challenge for both organizations and security professionals in that certain security controls must be implemented to protect them and the data they process.

Fuzzing

Fuzz testing (**fuzzing**) is a process that tests programs for security vulnerabilities, bugs, and errors through the use of a fuzz testing tool (fuzzer) that will input random, obscure, incorrect, or malicious data (fuzz) into the application to determine the outcome. Fuzzing can be effective for testing applications against buffer overflows, error handling, XSS vulnerabilities, SQL injection, and more. Fuzzing is a popular technique for vulnerability testers, penetration testers, and hackers.

Secure Coding Concepts

Developing secure code is a secure by design concept and requires developers and security experts to work collaboratively during each step of the software development lifecycle process. By doing so, this helps ensure that issues and vulnerabilities are discovered and resolved early on. The end result is that developers can release much more stable and secure code and reduce the amount of fixes and version upgrades that will need to be issued later.

Error and Exception Handling

As discussed in the last domain, when systems fail they can either fail safe (fail secure) or fail open. Applications can also fail in either one of these manners, with the former of course being preferred. How an application continues to function when a serious error or failure occurs can be written into the source code by the developer. The developer should provide specific instructions to the application on how it should respond to the different types of errors, write detailed information to a log file, and display a minimal amount of technical information to the end user. Developers should also be sure to create and maintain supporting documentation for controls like these.

Input Validation

An application that sanitizes the data received from users, files, or other programs and services is said to provide **input validation**. Cleansing input of unsanitary constructs or illegal sequences purifies the input stream from tainted values that can alter program execution.

Input validation controls should follow a default deny process, unless the input is specifically allowed. In programming, this is often referred to as a white list approach and tends to be the most secure. Input validation can include, but is not limited to, minimizing and maximizing the allowed length of the field, checking/restricting a numeric range, and denying commands and restricting special character usage. For example, if a web site asks for a phone number and the user submits the phone number in the format of (010) 555-1234, but the web page changes it to display 0105551234, then the system validated the input by removing the unnecessary characters and then verifying that the remaining data was purely numeric and within a specific range.

Web applications commonly receive a lot of invalid inputs from various unchecked sources—not all of which is malicious—but particularly clever coders can manipulate an application's flow to reveal sensitive information, store malicious code, apply configuration changes, or implement other forms of attack. Input validation attempts to cripple such attacks by removing any unnecessary elements.

Cross-Site Scripting (XSS) Prevention

As discussed in Domain 3, XSS is an increasingly popular form of attack that leverages vulnerabilities that are typically found in dynamically-generated web page content. A XSS attack is carried out by attackers who inject code or data into the pages of unsuspecting victims. XSS attacks can provide a platform for further attack – such as phishing or browser exploits.

Redirection and misdirection are major components of XSS attacks. XSS can be used to hijack an active web session, snoop on private postings, guide unwitting users to attacker-controlled servers, and perform other types of attack.

Methods to prevent XSS attacks can occur on two sides, that of the programmer, and that of the end user. End users can implement security controls on their workstations to detect and/or prevent XSS attacks, such as running anti-malware software (ensure script scanning is enabled), running host-based IPS, locking down web browsing, for malicious code, and more. Programmers, however, can play a larger role in XSS prevention by validating input and addressing vulnerabilities by releasing security patches in a timely manner.

End-users can only assume that programmers are taking these precautions seriously, but as discussed, a layered security approach is the most effective and end-users should take precautions as well. Newer web browsers contain multiple security controls and out-of-the-box they provide a decent level of protection. Some browsers even contain components that filter specifically for XSS attacks and block them. If it's not enabled by default, users should configure their web browsers to scan for phishing schemes, viruses (on download), prompt to allow/block scripting or applications, and more.

Cross-Site Request Forgery (XSRF) Prevention

XSRF attacks, while not as common as other attack methods, can be quite effective and are able to execute a wide range of tasks. XSRF is similar to XSS, but one of the main distinctions is that the executed attack command is run against the hosting web server by the client – and the web server (supposedly) already trusts the client system. This relies on the fact that a previous session was established, credentials are saved somewhere in the browser, or the target web server hasn't been configured to reject certain commands or drop invalid input. XSRF attacks can be capable of executing purchases, manipulating logon credentials, and more.

Preventing XSRF attacks can be difficult, but end-users can install add-ons for their web browsers, empty temporary Internet files regularly, keep web browsers patched, always logoff of sites when done, avoid remembering logon information in the browser, and follow other best practices.

Administrators can help prevent XSRF attacks by deploying web application firewalls and enabling them to scan HTTP referrer headers for spoofing. Webmasters and coders should limit the lifetime of cookies and configure the application to require that authentication information is included with the HTTP request that performs any sensitive operation (e.g., banking transactions).

Application Configuration Baseline (Proper Settings)

Creating and capturing a baseline for applications can be just as important as doing so for systems. Baselines, as discussed earlier, serve a critical role for supporting both security and troubleshooting initiatives. As applications are configured, tested, and adjusted, and the process repeated for deployment, a baseline that has been captured along the way can ensure the same version of the application with identical configurations is deployed, security controls are enforced, and a rollback point is provided to revert to should the need arise.

Application Hardening

As explained previously, the practice of **hardening** an application is similar to that of an operating system or other device and follows a series of protocols, procedures, and policies that define and describe the security configuration of the application. This often includes, but is not limited to, preventing the use or enabling of specific features and tools, ensuring that certain options like auto save are always enabled, preventing the removal or install modification of the application, and so on.

Application Patch Management

Patch management is the practice of routine maintenance and upkeep of application, service, and system patches. It's an area of systems management driven by a cycle of acquiring, validating, and implementing patches to computer systems in a methodical manner and requires up-to-date knowledge of current security issues and trends. The patching of applications can sometimes prove more difficult than that of operating systems, given the diverse number of applications that may be deployed in any given network.

(Patch management is described in further detail in the next few pages.)

Carry Out Appropriate Procedures to Establish Host Security

Operating System Security and Settings

Operating Systems, in regard to computing security, have come a long way in the past several years, but they are by no means bulletproof and numerous technologies, processes, and best practices exist to help protect them from attack. Today, this methodology is commonly referred to as Endpoint Security and encompasses system hardening, patch management, and the use of multiple tools like anti-malware, host-based IPS, host-based firewalls, encryption, device control, and more. Operating systems can be hardened to define a certain secure configuration, but that configuration must be captured in a baseline, applied to any new systems, and not have a negative impact on business functions.

Anti-Malware

Anti-malware solutions are a critical endpoint security control and are one of the most frequently implemented. Anti-malware products monitor files, processes, and other activity on systems to ensure that no malicious code is present. In addition to monitoring files and processes in real time, malware scanners also typically run on a scheduled basis to check for the presence of malicious files that lie dormant on the machine. Anti-malware solutions require frequent signature updates so they can properly detect and eradicate the most recent threats, and the majority of products available today also leverage heuristic scanning to monitor the behavior of code for malicious activity, a complementary control to signature-based scanning. In addition to endpoints, anti-malware scanning engines are also often included with web security filters, next generation firewalls, e-mail filtering, anti-spam solutions, and more.

Anti-Virus

As outlined in the previous domain, a computer **virus** is any form of malicious code that spreads from system to system by attaching itself to data or files. Viruses typically self-replicate on local systems; however, they can extend to other computers by targeting network drive shares, removable media, and other communal resources.

Anti-Virus technologies monitor files as they are executed, written to, or read from disk. Anti-Virus products are one of the oldest security controls and can be found on almost every system and at every ingress/egress point in networks today.

Anti-Spam

Anti-Spam and e-mail filtering solutions monitor e-mail messages that enter and leave a company, and like anti-virus products, they use multiple mechanisms to discern legitimate from illegitimate e-mail messages. Anti-spam filters can leverage heuristics, databases, DNS records, message format, attachment and content type, IP addresses, connection information, and more to combat spam.

Anti-Spyware

Computer software installed surreptitiously and without the owner's or operator's consent and then attempts to harvest personal information (e.g., usage trends, software licenses, sites visited), invades privacy, or manipulates browser activity is called **spyware.** Such software appears to be legitimate but contains hidden functionality that is otherwise undesirable and unwarranted.

Anti-Spyware products monitor and address these types of threats and are often incorporated with anti-virus or other endpoint security solutions.

Pop-Up Blockers

A common advertising trick on the Internet is to launch an additional web page when a user visits a site. While this can have legitimate uses (e.g., logon prompt), it is more often used to force advertisements or deliver malicious code. Some programmers generate a pop-under (resides beneath the original window), and can include functionality that prevents or discourages the closing of the window.

Web browsers such as Firefox, Safari, and Internet Explorer include pop-up controls which are customizable.

Host-Based Firewalls

Firewalls were discussed extensively in the first domain, but from a network perspective. Host-based firewalls are included with the most popular operating systems and are always in software form. Most endpoint security suites include a host-based firewall alongside other components. Due to the advancement and frequent release of computer threats, firewalls started to be deployed to hosts directly in order to support the defense in depth strategy.

Patch Management

Patch management is the practice of routine maintenance and upkeep of application, service, and system patches. It's an area of systems management driven by a cycle of acquiring, validating, and implementing patches to computer systems in a methodical manner and requires up-to-date knowledge of current security issues and trends.

The release cycle for fixes, enhancements, and updates, security related or not, usually follows no set schedule. Some do, however, like with service packs and Microsoft's "Patch Tuesday," which occurs on the second Tuesday of each month. Due to the unpredictability surrounding new vulnerabilities and exploits, plenty of out-of-band security updates have been released by Microsoft and others. Depending on severity and necessity, a hotfix or update may be released instantly upon vendor notification or follow a lengthy prioritized development cycle for later release date.

Organizations should closely monitor their vendor's web sites and newsletters for such releases and develop a process in which patches, updates, service packs, and major product upgrades are tested. The process should consist of a review team, pilot group, production deployment plan, and rollback procedures. Organizations should also include a process that addresses the need to review and deploy critical updates that might address a zero day situation and need to be placed into production immediately. Several tools exist today to assist administrators with the significant task of keeping all systems and applications up-to-date.

Hotfixes are often released out-of-band and sometimes address customer-specific issues only. Hotfixes will usually be included in a future patch or service pack. Updates and patches that are released regularly and not branded with the "hotfix" label, should be reviewed, tested, and deployed to impacted systems as they often address security vulnerabilities.

Microsoft uses the term **service pack** to describe a collection of fixes, enhancements, and updates that were released after the last major version or service pack. Service packs can be incremental in that a later service pack contains files not present in earlier service packs or, more commonly, they can be cumulative in that they contain all previous files.

Hardware Security

A company's computing assets require physical protection as much as they do logical protection, and the level of protection increases with the value of the asset. For example, if a laptop that is stolen contains proprietary information and that laptop is encrypted, then the confidentiality and integrity of the data on that laptop is ensured, but the availability of the data isn't. While physical security controls can't prevent every attack or incident from occurring, they do serve a very valid and purposeful role in deterring theft and supporting the three components of the CIA triad.

Computer security threats, risks, and vulnerabilities are not restricted to software; even hardware can cause significant security violations. Several key aspects of the system require adequate protection against tampering and manipulation by unauthorized parties. Sensitive applications, services, and processes can be disrupted and security mechanisms bypassed by employing or modifying various hardware configurations.

Basic Input/Output System (BIOS)

Every PC has a BIOS, which is specialized boot firmware designed to identify and initialize system devices prior to turning over control to the operating system. A computer's BIOS prepares the machine in a process called **bootstrapping** or just **booting**. Most computers provide basic access to BIOS settings through configuration menus invoked prior to boot-up. When users can perform unauthorized changes to BIOS settings they can bypass local security settings and violate company security policy.

The most common approach to securing the BIOS includes setting an administrative password so that users cannot change boot device priorities, enable or disable features, or utilize unauthorized devices. If an attacker can boot from external media, none of the system's local security settings is effective and the internal storage volumes themselves are completely open to attack (installing backdoors, Trojans, or rootkits) and manipulation (data theft, tampering, or trashing).

USB Devices

Any removable storage media can present a series of issues in the protected workplace. Sensitive information can be passed beyond security controls and taken outside of the security perimeter. An individual can also knowingly or unknowingly introduce malware to the local system or attached network or use bootable USB media to bypass local security restrictions. Specialized USB devices can also harvest information, interrupt operation, or copy data on the fly and in some cases transparently to the end-user.

USB devices access should be selectively enabled and tightly controlled (e.g., disabling autorun and adding encryption) to prevent users from bypassing restrictions, overcoming security, or subverting control. Malware infections make little distinction about their storage media, just so long as it holds (and in some cases transports) its code for future use. Sensitive data cannot determine what storage devices are authorized or unauthorized, and will gladly store wherever accepted.

Cable Locks

Cable locks can be used to secure almost anything, but the most common implementation is typically for workstations, monitors, and laptops as they often have built-in connectors that the cable lock can connect to. Cable locks are an inexpensive and very effective theft deterrent.

Safe

Sensitive and proprietary information, whether on paper or media, should be kept in a secure and locked place when not in use. Safes come in various sizes and styles and organizations use them in a number of ways. Items that should be placed in safes might include copies of digital certificates, investigative material, trade secrets, physical keys, and more.

Locking Cabinets

The term locking cabinets can be applied to a variety of things ranging from paper files to network routers. Locking cabinets provide a physical barrier that prevents unauthorized access to documents, servers, switches, and any other equipment that a business believes should be stored in a secure manner.

Host Software Baselining

Hosts should be released to production or built with a specific baseline imposed. This would include the proper operating system version and configuration as well as the appropriate applications required to both protect the system and allow the users to perform their work. If modifications to existing systems are required, they should be added to the existing baseline and the baseline should be reapplied to the systems.

Mobile Devices

Mobile devices are popular tools that offer a lot of functionality, usually at a reasonable price. The types of devices range from cell phones to tablets, with multiple variants from numerous vendors in between. Most smart phones and tablets available today can run mobile versions of the applications that computers run and include several ways to communicate with various networks. Mobile computing applications are hugely popular, and thousands exist. If the phone is configured to store data in the cloud, then the security risk is reduced even if the device is lost or stolen, provided other best practices like device encryption and strong password enforcement are enforced.

While mobile devices are feature rich, convenient, affordable, and more common than laptop computers, they often aren't properly secured or, even worse, are under the control of the organization. These mobile devices, as mentioned, offer numerous ways to connect: 3G, 4G, WiFi, Bluetooth, USB, Infrared, etc., and are capable of storing a significant amount of data.

The emergence of the mobile phone marked a trend that would soon find itself merging with other portable technologies (e.g., image capturers, video recorders, music players, digital organizers) and converging on the corporate workspace. Because mobile phones are no longer just mobile phones, they pose a considerable security threat for a number of reasons.

Bluetooth and 802.11 wireless have become popular items among recent cell phone designs, which means that attacks can originate from or be destined for equipped phones. Newer phones are also capable of executing a range of compiled and scripted code, leaving many forms of computer-related attacks feasible on these platforms. Phones equipped with cameras are capable of photographing sensitive equipment and information that is otherwise restricted to authorized parties.

When deploying or managing mobile devices in a network, several security considerations must be taken into account and compensating controls should be implemented to mitigate the inherent risks.

Screen Lock

Mobile devices like workstations should lock the screen and display a password prompt after a specific amount of time has passed. This control helps protect the contents of the device if it is lost or stolen, but it does not prevent full access to the system as attackers could attempt to access the device via one of the communication channels (e.g., Bluetooth, WiFi, USB, etc.). Some screen lock options support the erasing of the device after *X*-number of invalid attempts and/or support the use of either a four-digit PIN or strong password.

Strong Password

Most mobile devices allow the use of either a four-digit PIN or strong password; however, the form factor of such devices usually makes entering strong passwords difficult, and as mentioned earlier, will not prevent other forms of attack. While strong passwords are always preferred over simpler ones, this is one area where the exception to the rule can often be found. Organizations should leverage all of the different options available for securing mobile devices and not rely solely on strong passwords.

Device Encryption

Mobile devices (including any internal storage cards) should be encrypted – especially when the devices are issued by a company, synchronize files between other systems like a workstation, and have access to the corporate e-mail system/network. Unfortunately, while these devices are powered on or unlocked, encryption may not be in full effect and the data may still be vulnerable to unauthorized access.

Remote Wipe/Sanitation

Remote wipe is a popular feature and can be found in a variety of products like AT&T's Mobile Me, Blackberry Enterprise Server, Microsoft's Outlook Web Access, and more. The most effective remote wipe solutions should erase the storage card, the phone's operating system, and system configuration.

Voice Encryption

Conversations on cell phones are not immune to eavesdropping if the attacker has the right equipment and is within range of the conversation. Voice encryption is not commonly deployed, and recent studies revealed that a lot of the voice encryption products available were fairly simple to crack.

GPS Tracking

Cell phones and tablets include GPS chips that allow users to find their location on a map, search for nearby businesses, and more. Using GPS, mobile devices and their paths of travel can be tracked and recorded by the device owner, an organization, or an attacker.

Virtualization

Virtualization was covered in detail in Domain 1 and is defined as hardware or software that allows for the creation of multiple (virtual) operating systems, known as guests, on a single physical device known as a host.

While the logical systems reside on a single physical system, they run in their own logically segmented memory space and in many ways act independently of the host. Both the physical system and guest systems should be configured in a secure manner and guests need to undergo the same scrutiny as their physical host (e.g., virus protection, patch management, personal firewall).

Some security products include the ability to protect certain components of the virtual environment, like the prevention of terminating virtual machine processes. Companies that develop virtualization solutions like VMware and Microsoft are investing heavily in new technologies that deliver a more secure virtualization host solution.

Data Security

Data resides in multiple places on a network, takes on numerous formats, and lives in three states: data-in-rest, data-in-motion, and data-in-use. Data -in-rest is defined as data that has been written to media, but is not being transmitted or accessed. Data-in-motion describes the data that is travelling over a network at any given time. Data-in-use refers to data that is currently being created, modified, or deleted.

Data Loss Prevention (DLP)

Data loss prevention (DLP) is the process of ensuring that sensitive and/or proprietary information does not land in the wrong hands. Many regulatory initiatives like PCI-DSS and HIPAA directly state that some form of data loss prevention should be implemented.

DLP solutions can come in either hardware or software form and reside on either hosts directly or at network ingress/egress points. For example, an e-mail filter that includes DLP functionality might redirect messages to an encryption appliance if sensitive information is discovered in the message and/or attachment. DLP solutions can be very flexible and allow administrators to choose what actions users can execute on different forms of data (e.g., print screening, copy/paste, printing, forwarding, moving to disk).

Data Encryption

To ensure the confidentiality of information, encryption is often deployed. Data encryption can be implemented in numerous places on a network, and the most common locations, with the exception of network traffic, are discussed in the next sections.

Full Disk

Full disk encryption is the process of encrypting the entire hard drive of a computer. It's common for corporate laptops to be issued with fully encrypted drives to ensure the confidentiality of the data, should the device get lost or be stolen. Attackers have, however, discovered ways to obtain the decryption key if the system is powered on. This is a fairly advanced attack technique and requires physical access to the system. Full disk encryption should be used in combination with a strong password that is required on system start (prior to OS logon being presented) and is a popular and effective security control used today. Some organizations also encrypt the drives of workstations and removable media.

Database

Database encryption is more involved than full disk encryption, but it is also more effective because of the way it operates. Database encryption is typically included with the database software and encrypts the contents of the database and enforces encryption of the data until an authorized entity provides the correct key and attempts to read or modify the data.

Individual Files

Encrypting individual files is less popular than whole-drive encryption solutions, usually because the rest of the drive isn't encrypted. Individual file or folder encryption does have its benefits and comes in handy when needed. For example, if a user wants to transmit sensitive information over an unsecured medium like to an FTP server on the Internet, then he or she could choose to encrypt the file itself, where moving the file off of an encrypted drive does not mean that the file remains encrypted.

Removable Media

As with mobile devices, removable media is portable, convenient, popular, and easily lost or stolen. Removable media differs from mobile devices, though, usually in respect to size capacity. Removable media can come in many forms – CDs, DVDs, tapes, flash drives, and removable hard drives – and encryption solutions exist for each. Most organizations enforce encryption on removable media and some even prevent or restrict the use of removable media by certain personnel. Another commonly implemented best practice is to encrypt backups, especially when they are stored off-site.

Mobile Devices

When supporting or adopting mobile devices, companies should determine the need and requirements for encrypting these units if they will be permitted to store company proprietary information. Most mobile devices do not support encryption natively, but numerous products exist that do.

Hardware-Based Encryption Devices

Hardware-based encryption includes an appliance or chipset that is designed to perform encryption functions and store keys instead of software. Hardware-based encryption, on a laptop for example, can encrypt the laptop's hard drive regardless of the operating system that is running on it. Some hardware encryption appliances reside on the network, can analyze traffic, and choose to encrypt the information if necessary. For example, e-mail security appliances can encrypt e-mail messages that are found to contain sensitive information in message subjects, bodies, and/or attachments.

Trusted Platform Module (TPM)

At the time of writing, the current version of the Trusted Platform Module (TPM) stands at 1.2 (revision 116), and is a brainchild of the Trusted Computing Group. TPM chips are soldered to computer motherboards and generate crypto keys for use by the system and applications. Full disk encryption products can leverage TPM to protect the keys that were used to encrypt the drives and develop an integrity pathway for starting the system (BIOS, boot record, OS).TPM is not allowed in some countries like China and Russia, and the Trusted Computing Group has come under fire in the past regarding privacy concerns because of the information that is stored in the TPM. The TPM was invented to provide an industry standard and a more secure mechanism than software for enabling system security.

Hardware Security Module (HSM)

Hardware security modules (HSM) are advanced, specialized crypto processors that were designed to address large encryption calculations, provide key generation, manage and secure key storage, accelerate SSL connections, and more. HSM modules are typically implemented as hardware adapters or networked devices and include tamper-proof controls to protect their inner workings and content.

USB Encryption

Some USB storage devices (e.g., flash drives, removable hard drives) come preloaded with an encryption product (hardware or software). However, unlike enterprise level solutions, there is no centralized management, device revocation, key management, or other features that meet the flexibility needs of a corporate environment. USB devices that include hardware-based encryption mechanisms are usually much more costly than software-based versions, and more advanced models will self-destruct if the device is physically tampered with.

Hard Drive Encryption

Hard drive encryption, as discussed earlier in this domain, comes in either hardware- or software-based forms, with hardware versions usually being more efficient, robust, and secure. While some systems or devices include built-in hardware-based encryption solutions, there may be better alternatives depending on the needs of the organization. Numerous solutions for encrypting hard drives exist today, and some are free like TrueCrypt or Microsoft's BitLocker, which can sometimes be easier to manage, cost less, and be just as effective.

Cloud computing

As discussed in both Domains 1 and 2, cloud computing is a hot commodity in today's market, but its advantages come with security concerns that any organization which plans on engaging with a cloud provider should address. Concerns vary depending on whether or not the cloud is a private or publicly run environment, and what services are being used – Platform as a Service (PaaS), Software as a Service (SaaS), or Infrastructure as a Service (IaaS).

- **Platform as a Service (PaaS)** – A service that provides all of the underlying infrastructure, hardware, and software necessary to develop and host applications, perform testing, and more.
- **Software as a Service (SaaS)** – A service that provides subscription-based access to software. Business productivity software like Microsoft Office (Office 365) is a popular SaaS option.
- **Infrastructure as a Service (IaaS)** – A service that provides all necessary components – hardware, software, operating systems, and network – and charges business various rates, usually based on total usage.

Some examples that impact data security specifically are listed below and may increase or decrease in the level of concern, depending on whether the organization is engaging with a public cloud provider (less control), or in a private cloud where they might have direct control over several items. Questions asked regarding these items may include the following:

- How and where will my data be stored?
- Who can access my data?
- What levels of encryption will be in place and how will they be used?
- What are your business continuity and disaster recovery strategies? Are they tested regularly?
- Is my data replicated to other facility/facilities? Where are they located?
- What about privacy of company and customer data?
- What about physical security for the facility and backups?
- What about network, system, and data access (local and remotely)?
- What logical security controls are in place at the facility?
- What incident response procedures exist? How and when will I be notified of a breach?

Domain 5 – Access Control and Identity Management

Authentication Services

The term authenticate means to render something authentic, grant sufficient authority, or entitle sufficient credit to determine as real and true. In a secure computing context, authenticity identifies a subject authorized to access a computer or network object (i.e., application resources and system services). Authentication is the process of factually verifying that a user or entity actually owns a claimed identity.

The term authentication entails the following:

- Authentication is the process of finding out if something is exactly what it appears to be. For example, a user can be authenticated into a Windows Domain based on credentials, such as username and password. The Domain authenticates you and provides access if the user correctly verifies his or her identity and has the proper credentials.
- The weakness with authentication is the fact that if your credentials are compromised, then there is the possibility that they can be exploited by someone else.

When a user attempts to access a resource, he or she must provide the required credentials that prove that he or she is who he or she is claiming to be. The most common method of authentication is the use of a username/account number and password pair. The username or account number identifies the user and the password authenticates it on the system. This is also referred to as single-factor authentication. The single factor in this case is the password, which is known only to the user. Two-factor or multi-factor authentication is also widely in use and requires that in addition to a username/password pair (something you know), the user must also provide something they have, something they are, or a combination thereof. These concepts are discussed further in this domain.

Remote Authentication Dial-In User System (RADIUS)

Authenticating remote entities is a different challenge than when dealing with local users and groups. The **Remote Authentication Dial-In User Service (RADIUS)** is a standards-based (IETF RFC 2865 and 2866) client-server protocol that manages and maintains user profiles in a centrally-administered database that provides protective connectivity for guarded resources. RADIUS is often used in dial-up user connections and enterprise-grade wireless authentication setups to authenticate users, authorize access, and enable communications with internal computers, servers, and network devices.

Remote Access Server (RAS)

Remote Access Servers (RAS) are systems that allow you to connect to a server, usually over the Internet, to be authenticated to internal resources. If you are properly authenticated, then you are granted access to resources you are authorized to use.

Terminal Access Controller Access Control System (TACACS)

Terminal Access Controller Access Control System (TACACS*)* is a standards-based (IETF RFC 1490) remote authentication protocol that enables a remote access server (RAS) to forward a user's credentials onto a proper authentication server. TACACS uses static passwords for authentication and has been replaced by TACACS+.

Extended TACACS (XTACACS)

Extended TACACS (XTACACS) was introduced by Cisco and is proprietary to their systems. Unlike TACACS, which combines authenticating and authorizing into one process, XTACACS separates them, as well as auditing, into individual processes improving security and performance. XTACACS is also superseded by TACACS+.

TACACS+

TACACS+ is a completely rewritten version of TACACS and introduces support for multi-factor or strong-factor authentication and works similarly to a RADIUS system. Like XTACACS, TACACS+ also separates authentication, authorization, and auditing processes. TACACS+, however, is built-on TCP and encrypts all information exchanged between client and server, where RADIUS leverages UDP and transmits some information in clear text. TACACS+ is incompatible with TACACS or XTACACS and is a Cisco proprietary protocol.

Kerberos

Kerberos is an standards-based (IETF RFC 4120) authentication protocol that uses symmetric key cryptography and was designed to provide a single sign-on solution in a client-server network model. Kerberos uses a Key Distribution Center (KDC) for centralized authentication and relies heavily on time-stamped tickets that are received from the Ticket Granting Server (TGS) when a client requests access. Kerberos is platform agnostic and is the primary authentication mechanism used in both UNIX and Windows environments. Kerberos is scalable, supports mutual authentication (client and server prove identity to each other), and prevents the use of expired tickets which in turn can prevent spoofing and replay-based attacks.

Authentication Steps:

1. User submits logon credentials.
2. The Authentication Service (AS) on the Key Distribution Center (KDC) encrypts (using the user's password as the secret key) and sends a Ticket Granting Ticket (TGT) to the user's system.
3. When the user requests access to a resource (e.g., shared folder, printer), the TGT is submitted to the KDC and processed by the Ticket Granting Service (TGS), which proves the user was previously authenticated.
4. An additional ticket is sent by the TGS to the user's system and will be used to access the resource. This ticket contains the authentication information necessary to access the resource.
5. The resource decrypts the ticket and grants access.

Lightweight Directory Access Protocol (LDAP)

The **lightweight directory access protocol (LDAP)** is a standards-based (IETF RFC 4510) application protocol used to query and modify TCP/IP directory services, or sets of objects organized into a logical hierarchy. LDAP sorts organizational resources into a directory tree that branches into entries representative of people, organizational units (OUs), network objects (e.g., printers, storage), and documents. Like a telephone directory keeps categorical entries of individuals and businesses, LDAP maintains a similar resource for categorizing and enumerating computer-related assets.

Fundamental Concepts and Best Practices Related to Authentication, Authorization, and Access control

Identification vs. Authentication

Everyone has an identity that composes indicative or signifying traits: proper names, official titles, physical attributes, established reputations, and so forth. Identity distinguishes one individual from another based on a number of characteristics including complexion, ethnicity, and heritage. Through this identity other attributes are assigned: attribution of authorship, ownership, and membership into authorized groups.

- **Identification** is the act of claiming a specific identity with verifiable proof to support such a claim.
- **Authentication** is the process of verifying a claimed identity by validating one or more forms of proof.

What we provide as identification (to prove our identity) is analyzed and considered by a person or computer (an authority) to grant or deny our authentication.

Authentication (single-factor) and Authorization

An **authentication factor** is any piece of information used to prove or verify an identity or appearance for the purposes of obtaining security access or clearance to a protected resource. Authentication factors break down into the following categories:

Single-factor authentication uses a form of identification (e.g., account number, username as something you *know*) combined with one form of authentication (e.g., password, passphrase, PIN) to verify an identity and grant access to a resource. Single-factor authentication is vulnerable to brute force attacks on both the identification and authentication factors and the use of complex passwords. Avoiding easily guessable account IDs is strongly recommended. For increased security and accountability, two-factor or multi-factor authentication can be implemented.

Two-Factor and Multi-Factor Authentication

When something you *know* is combined with either something you *have* or something you *are* and used for authentication purposes, it's referred to as **two-factor authentication**. Including another authentication option beyond two is commonly referred to as **multi-factor** or **strong-factor authentication.**

- **Something you know:** password, passphrase, PIN, answer to secret questions.
- **Something you have:** physical token (fob), smart card, bank card.
- **Something you are:** retinal or iris scan, fingerprint, palm scan, face recognition.

Two-factor authentication delivers a higher level of assurance than single-factor authentication and multi-factor authentication provides the strongest form of authentication possible, but at higher implementation and maintenance costs than any other form.

Biometrics

Among the latest forms of authentication is **biometrics**, which measures biological data samples and recording of individual characteristics to uniquely identify authorized persons. Biometric readers sample various forms of biological data (e.g., fingerprints, retinas, voices) in search of distinguishing features that provably verify a user's identity.

Biometrics is an example of the "something you *are*" type of authentication. Biometric-based authentication is considered an accurate and reliable authentication method since it links the verification process to an individual (something you are), not to a card, account number, PIN, or password (something you have or know). Biometric characteristics are extremely difficult to imitate, and cannot be shared, forgotten, or lost. Biometric authentication processes are automated instead of relying on manual verification. Fingerprint, retinal eye scans, face recognition, and voice analysis are some common biometric authentication methods.

Tokens

Any physical **token** falls under the "something you *have*" authentication factor. The most basic and commonly understood form is the key access card and corresponding card reader that permits employee entry to an electronically-guarded entrance. Smartcards contain integrated circuitry and embedded chips, RSA SecurIDs cyclically generate pass codes, and proximity cards use radio frequency (RF) transmission to identify physical tokens and grant or deny access.

Common Access Card (CAC)

The **Common Access Card (CAC)** is a form of smart card adopted by and issued through the U.S. Department of Defense (DoD) and was created to strengthen and simplify authentication to government owned and operated resources. CAC cards serve as a form of ID and with a "something you *have*" authentication factor and, in addition to accessing networks, CACs are used for electronic signatures, e-mail encryption, and granting physical access to facilities.

Personal Identification Verification Card

Personal identification verification cards can come in many forms and are a popular physical access control with companies, government agencies, and organizations worldwide. Personal identification verification cards can be as simple as a photo, name, and title that prove identity to security guards, or they can also include additional functionality such as acting as a keycard for electronic door access. A driver's license is one of the oldest examples of a personal identification verification card and most today include magnetic strips that contain data that can be scanned to validate the card and prove a person's identity. This too is a "something you *have*" authentication factor type.

Smart Card

Smart cards contain integrated circuit chips with memory and processing capabilities to store personal information about a user. Smart cards support two-factor authentication (something you *know* and something you *have*) with the use of a card reader and requiring a password to the computer, smart card, or both. Smart cards themselves are not passwords, but may require a simple PIN-based password for access to the certificate or other data stored on that device.

Least Privilege

The **principle of least privilege** is an important security concept and design consideration that grants the lowest amount of privilege possible to perform some task. Access rights are assigned according to what an individual's roles require such as opening some file, modifying some data, and viewing some results. In a security context, this restrictive permission protects against giving users sufficient rights to damage or disrupt sensitive higher-level functions and processes.

Separation of Duties

A **separation of duties** selectively assigns access rights focal to a person's requirements to complete a given task. Separation of duties creates an appropriate level of checks and balances upon the activities of individuals operating in a given job capacity by preventing any one individual from gaining too much insight or control over business operations. In a security context, separation of duties disseminates the tasks of a particularly sensitive job among multiple users who function in individual capacities rather than as a collective group effort.

Single Sign-On (SSO)

The **single sign-on (SSO)** access method enables users to log in once and gain access to multiple applications/systems without being prompted to enter credentials any further. Different applications and services support varying authentication mechanisms, so SSO provides the translation layer to store and match against the various credentials among these differing implementations. The more complex an environment is, the more difficult (and expensive) a single sign-on initiative is to achieve. Often referred to as a panacea, single sign-on is usually found in an implemented form that more closely resembles simplified sign-on. Single sign-on simplifies the user experience, but proper security awareness training is required to inform users on how to protect their access credentials as an attacker could theoretically gain access to multiple resources by obtaining the proper credentials. Due to this vulnerability, it is highly recommended that SSO implementations utilize two-factor authentication at a minimum.

Access Control Lists (ACLs)

As covered in Domain 1, an **access control list** forms the most basic security checklist against which permitted accesses and actions are evaluated. ACLs define which actions a subject may take when accessing, creating, executing, or modifying a given object (e.g., applications, data, processes, services). Administrators define basic permission schemes that determine how users interact individually or collectively with a protected resource.

Access control lists are typically derived by leveraging the information defined in mandatory access (security labels), discretionary access (group membership), role based (job function), or rule based (actions) access models. Numerous technologies ranging from file/folder permissions to firewalls maintain access control lists to prevent unauthorized access to resources.

Access Control

Every multiple-user computer system utilizes login accounts to distinguish individual account holders and assign varying permissions based upon end-user job roles and responsibilities. **Access control** is the encompassing practice of allowing and denying access, entry, or usage to some protected resource by authorized and unauthorized individuals or groups.

Access control methodologies are the pervasive protocols and procedures that establish secure baselines and practices. Access control mechanisms manage both physical (i.e., entry to server rooms) and logical resources (i.e., access to server computers). Enforcement of access control methodologies through access control mechanisms entails the following:

- Measures taken to grant or deny access to resources for entities (users, computers, services) that have been successfully authenticated.
- Being able to access necessary resources, and then being able to control those resources.
- Understanding access control, making sure you know the differences between authentication, controlling access, authorization, and accountability.

Mandatory Access Control (MAC)

Mandatory access control (MAC) is a multi-level security that identifies people, services, and systems as *subjects* and all other resources as *objects*. MAC uses subject and object labeling called *security labels* to define the role, responsibility, and rights for those entities on a protected system. Subject access is restricted based on the sensitivity of the information contained in objects and the formal authorization or *clearance* level of that subject.

Mandatory access control uses the following security labels to identify assets:

- Top Secret
- Secret
- Confidential
- Sensitive (not classified)
- Unclassified

Discretionary Access Control (DAC)

Discretionary access control (DAC) is a simplistic means of restricting access to objects based on subject or identity or group membership. DAC is discretionary in that object owners can pass permission unrestrained (even indirectly) onto other subjects. Under DAC, ACLs are applied to system resources (e.g., files and folders) that define the permissions users (or subjects) have.

Role-Based / Rule-Based Access Control (RBAC)

- ***Role-Based Access Control (RBAC)*** – A role-based access control (RBAC) model defines permissions according to job roles that determine an individual's or group's ability to access data or system resources. RBAC is used interchangeably with non-discretionary access control and forms a third complementary solution to both DAC and MAC. A basic ACL forms the most common basis for RBAC. Role-based access control takes a secure approach to controlling access that is easiest to manage and maintain because the access controls do not require modification as individuals assume new job roles and responsibilities.
- ***Rule-Based Access Control (RBAC)*** – A rule-based access control model (RBAC)—which contracts to the same abbreviated form as role-based access control, creating some confusion—allows or denies access to objects based on a set of administratively-defined rules. Like DAC, rule-based access control maintains security attributes in ACLs associated with each object.

- When a subject attempts to access a protected object, the ACLs for that object are consulted before granting any form of access. Rule-based ACLs may block resource access during certain periods or within scheduled blocks of time throughout the weeks and months (such as restricting network access after hours). Like MAC, the ACL permissions cannot be assigned and administered by object owners.

Implicit Deny

An **implicit deny** security stance views all things as suspicious that aren't specifically and selectively deemed permissible (anything not explicitly allowed). An open network computing environment where anyone or anything may connect implicitly allows traffic, whereas a safeguarded network boundary that only permits certain IP addresses and/or service ports and blocks everything else implicitly denies traffic. Traffic that is blocked to certain ports or from specific addresses is said to *explicitly* deny. Think of the implicit deny as a safety net for anything you did not specifically allow previously.

Time-of-Day Restrictions

Contemporary network access policies are typically enforced through **time-of-day restrictions** that specify a certain period during operational hours when authorized users may access the Internet or certain aspects of the LAN. Time constraints curb after-hours network interactions and contain traffic activity in manageable periods.

Trusted Operating System (OS)

Controlling access to resources by platform (and version) can be an effective control type, especially when an organization uses very few platforms. **Trusted OS** enforcement can often be found in use with SSL VPNs, Network Access Control (NAC), and Network Access Protection (NAP) implementations, and usually specify a minimal specific service pack or patch version along with the OS requirements.

Mandatory Vacations

Employees operating in sensitive areas of the business should be forced to take vacations in what is known as a **mandatory vacation** policy. In their absence, other individuals fulfill their roles and responsibilities and are capable of detecting fraudulent behavior, inappropriate activity, or erroneous results. Any problems specifically related to the original employee's accounts or activities will be noticeable in their absence—either a previously unknown problem will be discovered or an existing problem may temporarily cease.

Job Rotation

The process of **job rotation** is usually implemented as part of human resources (HR) management plan to rearrange and reallocate personnel among numerous jobs to provide a breadth and depth of experience in the various interrelated duties. Job rotation allows qualified employees to gain insight into the inner processes and workings of an organization, reduces individual boredom, and stimulates satisfaction through routine variation.

Implement Appropriate Security Controls when Performing Account Management

Account management can be a daunting task, but it is a critical one. As mentioned earlier in this guide, built-in accounts and employees/contractors that are no longer employed at the organization must be disabled or deleted and access to administrative level accounts should be tightly controlled. Numerous other best practices can also be followed – for example, disabling accounts when users go on extended leaves. This section describes some of the issues and mitigating controls relative to account management.

Mitigating Issues Associated with Users with Multiple Accounts/Roles

Multiple accounts should be deployed when certain functions, usually administrative, should be carried out separately from day-to-day work tasks. A regular account should not have administrative rights, and should only have access to the resources needed to perform their duties. If a user requires administrative rights or serves an administrative role in the organization, then the proper credentials (role) must be obtained and used. Enforcing this type of policy prevents unauthorized access, reduces incidents, and enhances auditing and accountability.

Account Policy Enforcement

Enforcing account policies can ensure that user IDs follow a specific format; that passwords are complex, changed frequently, and not re-used; and that even the times of day the account can be used to access resources is restricted. Capturing these requirements and others defined by the organization into an enforceable account policy plays a big role in protecting assets and controlling access to resources.

Password Complexity

The strength of a password is a function of its complexity, length, and randomness. Even the strongest encryption algorithm from the best cryptographic implementation cannot protect against poor end-user password choices—and those choices are vast and varied. An established password complexity security policy augmented by digital, electronic, and mechanical enforcement ensures that users make appropriately challenging password choices every time. Enforcements against derivative username passwords (alexa/alexa123), dictionary words (spelled forward and backward), short lengths, sequence (abcdefg), repetition (555555), and non-varied character composition (i.e., only letters or numbers) provide the greatest initial strength for your security policy strategy.

Complex passwords should be at least eight characters or more (this is heavily debated) and should contain at least one upper case letter, one number, and/or one special character (e.g., @$!=). Powerful and effective password crackers exist today that are capable of identifying even some complex passwords, but simple passwords can be hacked within seconds, whereas it may take days, weeks, or months to crack more complex ones.

Expiration

Passwords should **expire** regularly (e.g., 90 days) and systems should force a password change when they do.

Reuse

When passwords expire, users frequently attempt to **reuse** the last password or a variant of the previous password that might simply have a number appended at the end (e.g., lastpwd123). Account policies should prevent the reuse of previous passwords (amount to be determined) and passwords that bear a likeness to them.

Recovery

Password recovery is becoming less and less popular and is commonly displaced by password resets using pre-defined secret question and answer pairs. Other means of resetting passwords might include a visit or phone call to a help desk where other information like employee ID or a call-back to the user's desk phone might be required to permit the reset if a self-service password reset mechanism doesn't exist. Password recovery implies that the password is stored somewhere that it can easily be retrieved from, which doesn't follow best practice.

Length

The current industry standard for **password length** remains at eight characters, but as mentioned above, this is constantly debated with multiple numbers being promoted as a new (effective) standard since too many simple and common passwords are still in use today. Regardless of how complex the password may be, the shorter it is, the easier it is to guess and is why a happy medium between length and complexity must be obtained.

Disablement

Accounts should be **disabled** when certain criteria defined by the organization are in effect. This can include extended absence from the workplace, time/day restrictions, or situations where the employee/contractor is no longer with the company, but their account needs to remain intact for transfer of duties, investigations, or other reasons.

Lockout

Another important account policy to enforce is that of **account lockout**. Accounts should be configured to lock out after a certain number of bad password attempts (usually three or five) and administrators should be alerted in some fashion when this occurs. As mentioned earlier, some systems allow users to reset their passwords by answering a serious of pre-defined secret question and answer pairs, a/k/a self-service password reset, otherwise a call to the help desk is necessary.

Group Based and User Assigned Privileges

Group membership can simplify administration when configuring access rights to resources as anyone in the group has the same permissions as everyone else. Group membership also allows for flexible deployment of policies, resource assignments, software distribution, and other administrative functions. It is important to note that if an individual is granted access to a resource through one group, but denied access to the same resource through membership in another group, then access is denied as a deny permission always takes precedence.

User assigned privileges are assigned directly to individual accounts and do not use group membership. In large environments user assigned privileges can be cumbersome to administer and group membership should be used when possible.

Domain 6 – Cryptography

The application of cryptography—the discipline and application of concealing or disguising information—has been around for centuries, but only since the age of secure computing has its true potential been revealed. The field of computer cryptography encompasses many concepts, constructs, and components that vary from simplistic to sophisticated. Usage and understanding of the principles, properties, and protocols is essential for earning Security+ certification and necessary for becoming a paid security professional.

Summarize General Cryptography Concepts

Cryptography is the formal practice and study of concealing or disguising information. **Encryption** is the process of converting ordinary information (or **plaintext**) into unintelligible data (**ciphertext**). The reverse process of converting ciphertext into plaintext is called **decryption**. Cryptographic algorithms are the software components that drive encryption and decryption, which often use a cryptographic key to prevent simple analysis of encrypted data.

Cryptography is a richly diversified area of the Information Security field that is full of numerous algorithms, products, and tactics, techniques used for deployment or integration. As a Security+ practitioner, you must possess a firm comprehension of cryptographic principles and firm understanding in their practical applications. Cryptography is the science and practice of concealing confidential messages; **cryptanalysis** is the science of analyzing and deciphering those messages.

Symmetric vs. Asymmetric

- **Symmetric key** cryptography (also called **shared-key** or **private-key** encryption) algorithms use identical or similar encryption keys for processing encryption and decryption. Encryption keys may be trivially related in that they're exactly alike or simply transformed for slight variance. Both keys represent a **shared secret** between two or more parties used to maintain private conversations and confidential communications. Examples of symmetric key algorithms include: DES, 3DES, RC2/RC4/RC5/RC6, IDEA, AES (Rijndael, MARS, Serpent, Twofish) and Blowfish. These algorithms are discussed in further detail throughout this domain.
- **Asymmetric key** cryptography secures private communications between parties without the exchange of secret or shared keys and instead uses separate keys for encryption and decryption routines. Similar but separate **public-key** cryptography is a subset of asymmetric cryptography that uses public and private key pairs. Keys used to encrypt messages (private) vastly differ from keys used to decrypt messages (public). However, only the public key is ever distributed or published; the private key remains sole ownership of the respective party. Despite both keys being mathematically related, it's infeasible and improbable to derive the private key from the public key (as is the case with symmetric keys). Examples of asymmetric key cryptography include: Diffie-Hellman (D-H) Key Exchange, RSA, DSA, El-Gamal, and elliptic curve, which are discussed in further detail throughout this domain.

Fundamental Differences and Encryption Methods

Block vs. Stream

- **Stream Cipher:** A symmetric cipher in which the plaintext digits are combined with a pseudo-random cipher bitstream. Each plaintext character is encrypted serially and singly. Transformation of successive digits varies during encryption and is dependent upon the current state of execution.

- **Block Cipher**: A symmetric cipher that operates on fixed-length groups of bits (termed blocks) with constant transformation. A block cipher might consume a 128-bit block of plaintext as input and output a corresponding 128-bit block of ciphertext. Exact transformation is controlled using the secret key. Decryption is similar in that the decryption algorithm takes a 128-bit block of ciphertext together with the secret key, and yields the original 128-bit block of plaintext.

Transport Encryption

Transport encryption provides confidentiality for data-in-motion and fulfills the need for private communications, especially over the Internet. Transport encryption helps ensure that data cannot be intercepted and interpreted by an unauthorized entity. Numerous transport encryption solutions exist and can be applied to internal network communications, e-commerce solutions, VPN, e-mail, FTP sessions, SSH tunnels, and more. Shown below is an example of transport layer encryption being applied to VPN connections that access a private network from the Internet. Requirements and deployment designs for encrypting data will differ from organization to organization.

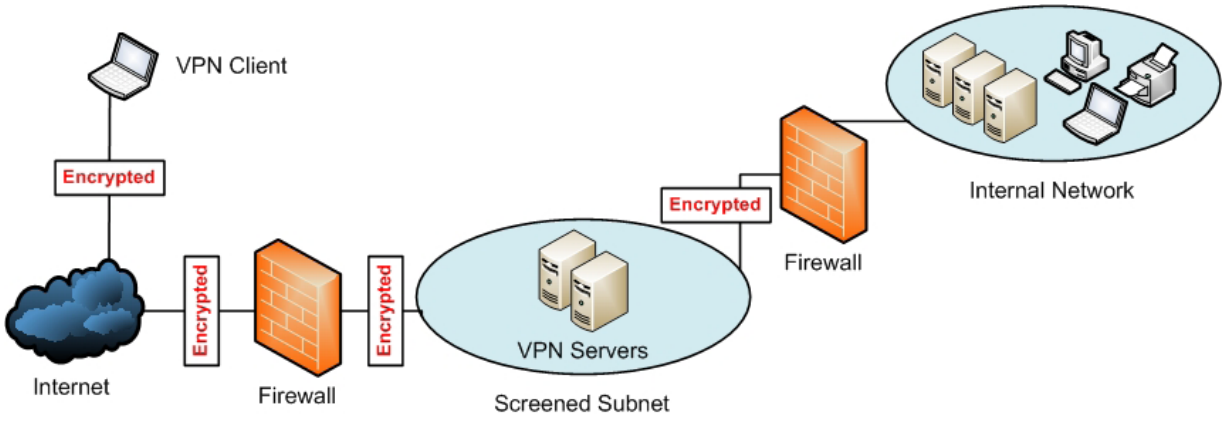

Figure 9: Transport Encryption

Non-Repudiation

Accountability is a crucial factor in computer security generally and computer cryptography specifically. One way to provide **non-repudiation** or undeniable proof of authorship is to digitally sign communications, documents, and messages with a private key. Non-repudiation ensures that a party cannot refute the authorship, delivery, or validity of a digitally-signed article. Its meaning and application in computer security defines services that provide proof of integrity and origin of data, and also assured genuine authentication. IPSec and S/MIME are examples of technologies that include support for non-repudiation.

Hashing

The cryptographic **hash** function takes an arbitrary block of data and produces a fixed-size string called the **hash value** for later verification. The resultant hash value ensures that once data is received it has not been altered at any point between sender and recipient. Hashes provide message integrity checks, digital signatures, secure authentication, and various information security applications. Hashing is considered a one-way function because the resulting hash value is useless in reconstructing the arbitrary data it was created from originally.

Many cryptographic functions, services, and protocols rely upon hashing algorithms that create checksums of data for integrity verification purposes. One surefire way to ensure reliable, tamper-proof transmission between sender and recipient (whether tampering is human or machine is irrelevant) is through hashing or checksumming techniques. Hash strengths and solutions come in many varieties, some of which are provably vulnerable to calculate attack and others have yet to be "broken." Example hashing algorithms are defined later in this domain and include: Hash of Variable Length (HAVAL), Message Digest (MD4, MD5, etc.), RACE Integrity Primitives Evaluation Message Digest (RIPEMD), and Secure Hash Algorithm (SHA).

Key Escrow

Key escrow (also called **key recovery, trusted third-party** or the **fair cryptosystem**) arranges for public and private decryption key storage so that an authorized third-party may gain access in circumstances of need. Typically the decryption key to an encrypted communication is kept among only the person(s) directly involved; however, in certain cases a third-party individual (i.e., company or governmental entity) may require possession of decryption keys to investigate an incident or confirm a relationship between parties. A variety of key recovery requirements has been suggested by government agencies conducting covert surveillance within dynamically changing environments encompassing any number of old and new tactics, techniques, and technologies.

Key escrow systems that must furnish timely law enforcement access to an entire key or plaintext transformation present an unprecedented path to encrypted data recovery. This alternate path is beyond user control and removes a fundamental safeguard against mistaken or fraudulent release of keys or information. Non-recoverable systems can be designed and implemented without any such alternative recovery paths since they're unnecessary for ordinary operation and undesirable in many cases.

Steganography

Security through obscurity is generally an ill-advised security practice, but **steganography** is exactly that: an encryption method that encapsulates the message, obscuring it from view so that only sender and recipient are aware of its existence. Steganography most commonly conceals information within unassuming computer files. Audio, photo, and video formats are prime choices, and other documents or text-based files work as well. While cryptography disguises the meaning of a message, steganography disguises its presence to drawing attention and avoid detection.

Digital Signatures

A **digital signature** is an electronic identifier derived from public-key (asymmetric) cryptography used to authenticate a message and give undeniable proof of authorship by the author/sender. Digital signatures are easily transportable, difficult to forge, and conceal various data including contracts, email, and messages sent across the network. Private keys are used to create digital signatures (providing ownership) and a secure hash of the entire document or message is signed so that any change to content invalidates the signature (providing integrity).

Use of Proven Technologies

Computer security delicately balances controls and countermeasures against engaging threats and risk to achieve a favorable defense strategy. The use of proven technologies ensures the highest level of capability and confidence in such a security strategy and significantly increases positive results. A cryptographic algorithm that has never seen widespread use or undergone serious scientific analysis has not proven itself viable in the take-no-chances world of IT security. Likewise, other unproven access control, security monitoring, or other threat mitigation strategies should never be relied upon to secure a modern computing environment. However, an unproven technology is entirely welcome in developmental labs under pilot testing programs that attempt to ascertain a security component's viability before deployment in the production environment.

Elliptic Curve and Quantum Cryptography

- **Elliptic curve cryptography** is an approach to public-key cryptography that is based on the algebraic structure of elliptic curves over finite fields. ECC operates on smaller keys compared to RSA keys for more efficient performance. It also offers considerably greater security for a given key size and more compact implementations for a given level of security.
- **Quantum cryptography** is the process of using the physical properties of light to perform a secure private key exchange between two trusted parties. The keys are generated using a one-time pad, defined later in this domain, and eliminates the need for a Public Key Infrastructure (PKI). Quantum cryptography does require special hardware and would work best over fiber connections. Quantum cryptography implements a mechanism where the position of photon particles are measured by the recipient to ensure that eavesdropping of the connection is not occurring. The recipient, because of the relationship with the sender, knows what pattern to measure the photons for, where an attacker/eavesdropper would have to guess – ultimately guessing wrong and alerting of their presence. This theoretical cryptographic approach has been advertised as unbreakable or bulletproof because if the light transmission is intercepted in any way, it alters the light stream and would alert the sender and/or recipient of a breach. However, recent studies by researchers developing quantum cryptography technologies have shown that quantum cryptography is not immune to attack and eavesdropping vulnerabilities have been discovered.

Use and Apply Appropriate Cryptographic Tools and Products

Wireless Equivalent Privacy (WEP) vs. WiFi Protected Access (WPA) and WPA2 using a Preshared Key (WPA2-PSK)

As mentioned earlier in this guide, **Wi-Fi-Protected Access (WPA)** is available in two versions, WPA and WPA2, with WPA2 being the more secure and preferred solution. WPA was created to address the shortcomings of Wireless Equivalent Privacy (WEP) in which the static private key could be easily cracked. WPA uses the Temporal Key Integrity Protocol (TKIP) encryption model adding encryption keys dynamically to each packet. WPA also performs message integrity checks, which prevents attackers from capturing and modifying packets.

TKIP added security controls that were missing in WEP: key-mixing functions, anti-replay sequence counter, and a 64-bit message integrity check. Since TKIP is built on top of WEP, it is also vulnerable to attack and is being phased out.

WPA2 was introduced shortly after WPA was made available and is its successor as it provides stronger security measures that addressed the limitations of TKIP. WPA2 uses the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP is an advanced cryptographic mechanism that was designed to protect the confidentiality of data. In addition, CCMP provides authentication and access control to WPA2 connections.

WPA2 personal (or pre-shared keys), WPA2-PSK, was created for small office and home users to create a secured wireless network, when an 802.1x server normally wouldn't be a part of the topology.

WPA/WPA2 Enterprise processes 802.1x authentication requests through a Remote Access Dial-In User Server (RADIUS) system and is often configured to prompt for logon credentials once the connection is established. This type of configuration is more complex and rarely found in small offices and home networks.

Unless a strong passphrase and uncommon Service Set Identifier (SSID) are used, WPA2-PSK is vulnerable to brute force attacks. Further, not broadcasting the SSID can provide an additional layer of protection. When a host and WAP establish a connection, each device encrypts the traffic using 256-bit keys.

MD5

Message digest algorithm 5 is a widely used Internet standard (RFC 1321) hashing function that produces a 128-bit hash value expressed as a 32-character hexadecimal product. Though commonly used to check the validity of critical system files, it also serves anti-tampering functions for digital certificates, obscures password entries, verifies downloaded content, and secures network transmissions.

It has been provably demonstrated that MD5 is not collision-resistant to a number of attacks and is therefore unsuitable for applications relying upon this feature (such as file integrity checkers). Two files of differing content and construction can indeed share an identical MD5 checksum and it's also possible to forge SSL certificates that pass validity checks. Extra care and precaution must be taken when using MD5 algorithms and applications in high-risk security contexts.

When some applications and systems store passwords, they are often hashed so they are not easily readable. For example, if a user were to enter "password" as his or her password for an application and chose to store it on the local system (i.e., remember my credentials), the application might (should) generate a hash value consisting of various numbers and letters, as shown below. Hashes can be reversed however, and simple text like "password" can be easily revealed as multiple tools and hash databases are readily available.

MD5 hash of the text string "*password*": 5f4dcc3b5aa765d61d8327deb882cf99

Secure Hash Algorithm (SHA)

The **secure hash algorithm** is a set of cryptographic functions originally designed by the National Security Agency (NSA) and later revised and published by NIST as a federal information processing standard (FIPS). SHA is a checksum algorithm that is capable of producing fixed and variable digest sizes up to 512 bits. SHA algorithms are differently structured and distinguished as SHA-0, SHA-1, and SHA-2, the latter of which uses variable digest sizes (e.g., SHA-224, SHA-256, SHA-384, SHA-512). SHA-1 is based on principles similar to MD5 but uses a more conservative design.

Proof that certain forms of SHA are broken shows that collisions occur in fewer hash operations than brute force attacks based on hash length. That means cryptanalysis can reveal hash collisions in less time and effort than it takes to exhaustively iterate over the entire key space (in bits) of a given SHA algorithm, which means compromises its integrity and invalidates it for high-risk security usage.

As described above, hash values are created by hash generators and can be implemented in many scenarios. Displayed below are two SHA hash values, one generated using SHA1 (160-bit) and SHA256 (256-bit). Stronger hashing algorithms equate to longer hash values and may take more time to generate, but they also equate to a more secure solution that significantly increases the difficulty when trying to reverse the value.

SHA hashes of the text string "*password*":

sha1: 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8

sha256: 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

RACE Integrity Primitives Evaluation Message Digest (RIPEMD)

RIPEMD is an early (circa 1996) 160-bit message digest algorithm and is based on functionality in MD4. Other versions of RIPEMD also exist (128, 256, 320), but RIPEMD has not been widely adopted primarily because of security issues with the 128-bit version and availability of SHA.

Similar to the examples given with MD5 and SHA, two different RIPEMD hash values are displayed below. A table outlining and comparing the most common hashing algorithms is included later in this domain.

RIPEMD hashes of the text string "*password*":

ripemd128: c9c6d316d6dc4d952a789fd4b8858ed7

ripemd256: f94cf96c79103c3ccad10d308c02a1db73b986e2c48962e96ecd305e0b80ef1b

Advanced Encryption Standard (AES)

The **advanced encryption standard** comprises three block ciphers (AES-128, AES-192, AES-256) adopted from a larger collection. AES operates quickly in software and hardware implementations and requires little memory usage for operation. As a NIST Federal Information Processing Standard (FIPS) AES has passed a rigorous five-year standardization process where competing designs were evaluated for fitness until an appropriate selection was made, and is now among the most popular ciphers used in symmetric key cryptography. The different block cipher specs represent fixed-size increases and decreases to corresponding block sizes and corresponding cryptographic strength.

Data Encryption Standard (DES)

The **data encryption standard** is a deprecated 56-bit block cipher once used internationally, but has become obsolete by simple algorithmic attacks and bested by more robust algorithms and methods. As of 1999, DES was collaboratively broken by a team of security researchers forever casting DES into the annals of antiquated encryption algorithms. DES serves mostly historical purpose as one of the first and foremost block cipher encryption standards.

Triple Data Encryption Standard DES (3DES or Triple DES)

As a follow-up to its provably broken precursor, Triple DES builds upon the same 56-bit cipher but enlarges that key space without code alteration or algorithm switch. Additional cipher rounds and steps are essential to preventing attacks against basic DES and can operate with variations to number of keys used and the order of operations performed. Generally speaking, 3DES with three keys has a 168-bit key length but is effectively provided only 112-bit strength due to algorithmic shortcomings and generally slow computational performance. 3DES is itself disappearing from use in favor of more resistant algorithms such as AES.

Hash-Based Message Authentication Code (HMAC)

HMAC uses a secret key with a hashing algorithm (e.g., MD5, SHA-2, etc.) to generate a MAC value that can be applied to and sent with a message. It's important to note that the secret key isn't sent with the message, nor does it actually encrypt the message. When the recipient receives the message (and MAC value), the recipient then uses a secret key with the received message to generate a MAC value and compares the two to validate that the message hasn't been altered. This ensures integrity of the message during transmission, but it does not provide confidentiality or non-repudiation. By adding the use of a secret key, MAC helps prevent an attacker from modifying the original message and sending it with an identical message digest.

Rivest-Shamir-Adleman (RSA)

The **Rivest-Shamir-Adleman** algorithm (named for its authors) is a foundational cipher that pioneered the first practical application and programmatic implementation of public-key cryptography. RSA is used for encrypting messages and generating digital signatures and continues to operate industrial-strength security applications and protocols like PGP, SSH, and many others. Public and secret keys are derived from the factors of very large, dynamically computed numbers. RSA generally combines a padding scheme—additional or modified data used to further vary encryption—to prevent a number of known algorithmic attacks against it and defeat cryptanalysis on resulting ciphertext.

Rivest Cipher 4 (RC4)

RC4 is a 128-bit stream cipher that has been used with SSL, RDP, WEP, WPA, and more. RC4 is still in use today, but it typically isn't included with newer technologies like RC5 and RC6 are (all three were designed by Ron Rivest). The semi-predictable nature of the key used with RC4 to encrypt messages ultimately led to the replacement of WEP with WPA and 802.11 (WPA2).

One-Time Pads

Cryptography includes the **one-time pad** encryption algorithm that combines plaintext input with a random key or "pad" of equal length and used only once. Modular arithmetic—a system designed for integers where values wrap around after reaching a certain maximal value—combines both aspects into the final encoded output. In a binary arithmetic format, the exclusive-or (XOR) operation performs the same task. One-time pads provide perfect secrecy whenever the generated key is truly random, kept secret, and never reused.

Challenge-Handshake Authentication Protocol (CHAP)

The **challenge-handshake authentication protocol (CHAP)** is a protocol that allows users to securely connect to a system, and is typically used with point-to-point protocol (PPP) connections. CHAP was created to replace PAP due to it being vulnerable to eavesdropping and passing of authentication credentials (username/password) in clear text. CHAP uses a one-way MD5 hash function. If the hash values match from sender and receiver, then the authentication process continues and the connection is established. CHAP will sever a connection with the client if a (random) authentication challenge sent to the client fails. If the client passes the challenge, the connection is kept alive.

In 1998 Microsoft modified and branded its own version of CHAP, MS-CHAP. MS-CHAP currently exists in two versions, MS-CHAPv1 and MS-CHAPv2. MS-CHAPv1 was introduced with Windows NT 4 (SP4, specifically), and support for MS-CHAPv1 was dropped with the release of Windows Vista.

One way MS-CHAPv1 differs from CHAP is that the remote server only requires the hash (MD4) of the password to validate the challenge response, whereas CHAP required it in plaintext. Among other enhancements, MS-CHAPv2 introduced mutual (two-way) authentication and separate keys are generated for both received and transmitted data.

Password Authentication Protocol (PAP)

The **password authentication protocol (PAP)** is a simple authentication protocol connecting end-users to network access servers as used with point-to-point protocol (PPP), like CHAP. PAP, however, transmits plaintext ASCII passwords across the network and is therefore insecure, despite seeing usage as a last resort in absence of stronger authentication protocols (like CHAP or EAP).

NT LAN Manager (NTLM)

NT LAN Manager (NTLM) succeeds and replaces the original LAN Manager SMB-based remote access authentication protocol and is similar to Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP). NTLM is proprietary to Microsoft networks and employs a challenge-response sequence to negotiate secure channels between clients wishing to authenticate and servers requesting authentication. NTLM allows clients and servers to negotiate secure parameters and request or require supported features.

NTLM challenge-response follows this format:

- **Type 1 message:** client sends a message that contains attributes flagging requested or supported features.
- **Type 2 message:** server sends a reply containing a similar set of flags supported or required by the server (negotiating connection parameters) and a random challenge.
- **Type 3 message:** client calculates response based on Type 2 message challenge, the method of which differs according to negotiated NTLM parameters, then issues the final message.

NT LAN Manager v2 (NTLMv2)

Like MS-CHAPv2, NTLMv2 was released with Windows NT 4 SP4 and added mutual (two-way) authentication support. NTLM and NTLMv2 are no longer recommended as most Active Directory environments use Kerberos exclusively, and Microsoft along with others recommend against its use with other applications, unless absolutely necessary because of the ease in which passwords can be cracked and its lack of support for current cryptography methods like AES.

Blowfish

Blowfish is a symmetric key block cipher that puts 64-bit blocks of data through 16 rounds of cryptographic functions using a key length that can vary from 32 to 448 bits in size. Bruce Schneier invented Blowfish and released it to the public domain patent free as a viable alternative to DES. Blowfish is still in use and to date no successful cryptanalysis attack for the full blown version has been discovered.

TwoFish

TwoFish was also created by Bruce Schneier, the inventor of Blowfish, but unlike Blowfish which works with 64-bit blocks of data, TwoFish works with 128-bit blocks of data. As with Blowfish, TwoFish is a block cipher, but the maximum length of the keys used for encryption can't exceed 256-bits, in contrast to Blowfish which allows the use of 448-bit keys.

Pretty Good Privacy (PGP)

Pretty good privacy is a cryptographic application used to encrypt and decrypt e-mail for transmission across the public Internet. It's free for single-user usage and commercially sold to corporate environments (comprising multiple users) and represents a complete public-private key cryptosystem capable of protecting stored files, exchanging digital signatures, and providing secure authentication. PGP employs several algorithms including DSA, RSA, MD5, and SHA to provide the services that support data encryption, user authentication, message integrity, and key management.

Gnu Privacy Guard (GPG)

GNU is a UNIX-ish operating system that is free to download and use. GnuPG or Gnu Privacy Guard, is an open source cryptographic application based on OpenPGP and PGP and is a product of the GNU Project, creators of the GNU operating system. GnuPG operates from a command line, is compatible with Windows, Linux, and Mac, and has several graphical interfaces that can be added on for ease of use. GnuPG provides the ability to encrypt and sign data and includes a key management system. GnuPG also integrates easily with many public key exchange systems. S/MIME support was added to version 2 of GPG.

Whole Disk Encryption

Whole or full disk encryption was discussed at length in Domain 4 and is the process of encrypting the entire hard drive of a computer. Full disk encryption should be used in combination with a strong password that is required on system start (prior to OS logon being presented) and is a popular and effective security control used today.

Comparative Strengths of Algorithms

When selecting and evaluating encryption algorithms, many deciding factors play a role, but the most prominent is that of key length. Keys, as previously mentioned, are randomly generated values derived from the keyspace – the range used to create keys. Larger keyspaces equate to more key possibilities and more random key generation. The more random the key and the larger the keyspace, the more secure the solution. Larger key lengths and higher rounds of computation certainly increase the level of protection, but they also require significant computing power to complete. The table below compares the details of the most commonly used symmetric cryptography solutions.

Comparison of Symmetric Key Algorithms

Name	Cipher	Data Block	Key Length (bits)	Rounds
AES	Block	128	128, 192, or 256	10, 12, or 14
DES	Block	64	56	16
3DES	Block	64	56, 112, or 168	48 (3 DES equivalent rounds)
Blowfish	Block	64	1 to 448	16
TwoFish	Block	128	128, 192, 256	16
IDEA	Block	64	128	8.5
RC4	Stream	varies	40 to 2048	256
RC5	Block (variable)	32, 64, or 128	0 to 2040	1 to 255
RC6	Block	128	128, 192, or 256	20

Figure 10: Symmetric Key Algorithms

Comparison of Hashing Algorithms

Name / Function		Hash Value (Digest Size, Output)
MD2		128-bit
MD4		128-bit
MD5		128-bit
RIPEMD		160-bit
SHA-**1**		160-bit
SHA-**2**	SHA-224	224-bit
	SHA-256	256-bit
	SHA-384	384-bit
	SHA-512	512-bit

Figure 11: Hashing Algorithms

Use of Algorithms with Transport Encryption

Secure Socket Layer (SSL)

A symmetric key based cryptographic protocol that operates over TCP port 443 at the transport layer (layer 4) of the OSI model to provide secure communications over the Internet (e.g., banking, shopping). Due to limitations and vulnerabilities in SSL, Transport Layer Security (TLS) was created and both are in wide use today, with TLS being preferred. Session keys can be implemented in either 40-bit or 128-bit forms.

Transport Layer Security (TLS)

TLS, as mentioned, is replacing its predecessor SSL as a preferred transport encryption protocol due to its advancements in cryptography and interoperability with other technologies. Like SSL, TLS operates at the transport layer of the OSI model and usually operates over the default TCP port 443. TLS can also function over port 80 and the session keys used for encryption can range from 128-bit through 256-bit.

IPSec

IPSec is a network level (OSI layer 3) cryptographic framework that can operate in two different modes (transport or tunnel) and provides two services: authentication header (AH) and encapsulating security payload (ESP). IPSec serves the following functions:

- Verifies identities between parties in a conversation.
- Provides non-repudiation to undeniably prove a message's source of origin.
- Prevents IP spoofing exploits and man-in-the-middle attacks.
- Captured packets cannot be reused later (anti-replay protection).
- Protects against eavesdropping, interception, and sniffing attacks.

Transport Mode
Only encrypts the packet payload (data being transferred) and is commonly set between endpoints (host to host) and gateways (host to gateway) in a network.

Tunnel Mode
Typically used between gateways (such as through two routers) in a network topology. Tunnel mode operates like a proxy for "hidden" hosts and the entire packet (including the header) is encrypted.

Secure Shell (SSH)
As discussed in Domain 1, Secure Shell was originally designed to address an administrative need for a secure remote login and shell. SSH ensures network privacy by preventing eavesdropping, interception, or tampering of the connection by a malicious third-party entity. SSH supports a wide range of encryption algorithms.

The primary problem with standard Telnet, FTP, and network file sharing (NFS) transactions is that they transmit in cleartext (such as login credentials and exchanged content). Cryptography naturally suits these purposes (remote login, shell, and file copying) and SSH provides the necessary means. SSH version 2 (SSH2) can use traditional username/password logins, public key cryptography, and several alternative forms of authentication. SSH-2 is the newest version of Secure Shell and includes numerous enhancements over the previous version (SSH-1), like adding support for Diffie-Helman key exchange.

HTTPS
As covered in Domain 1, SSL and TLS provide an essential security service to HTTP (HTTPS) that ensures several preventive and protective measures are taken to resist interception, manipulation, or observation by unauthorized parties—particularly those placed between endpoints of a secure conversation. As a web-based protocol, HTTPS is integrated into popular web browsers to encrypt and decrypt page requests across TCP port 443 (instead of HTTP's usual port 80). HTTPS connections operate below the application layer to encrypt HTTP messages prior to transmission and decrypting incoming messages upon arrival.

Note: HTTPS is not identical to secure HTTP (S-HTTP, RFC 2660), an alternative, though less widely used, URI scheme for encrypting Web transactions.

Secure/Multipurpose Internet Mail Extensions (S/MIME)

Asymmetric encryption mechanism using RSA (described earlier in this domain) that encrypts an e-mail message using the recipient's public key and then attaches the encrypted message to a new e-mail message. Some solutions don't attach the original, but retain an encrypted copy on-site and only distribute a notification e-mail to the recipient with a link to the original message. S/MIME follows the IETF standards track and is defined in a number of RFCs. It provides cryptographic security services for email including: secure authentication, message integrity, non-repudiation or origin, end-user privacy and data security.

Note: Secure FTP, FTP Secure (FTPS), Secure HTTP, HTTP Secure (HTTPS), Secure Shell (SSH), IPSec, SSL, and TLS were also discussed at length in Domain 1, Network Security.

The Core Concepts of Public Key Infrastructure (PKI)

The underlying concepts of public-key cryptography are known, published, and widely utilized in many security scenarios. It's called ***asymmetric*** cryptography because separate keys are used for encrypting messages (public key) and decrypting messages (private key), which enables untrusted users to sign and seal a cryptographic message that only the intended recipient may "open." PKI uses multiple components to provide a single solution for issuing, tracking, validating, and managing digital certificates and keys.

Digital Certificates

Digital certificates are signed by a Certificate Authority (CA), see below, and are used for authentication and to verify that a public key belongs to a specific individual (person or company). Digital certificates are electronic documents bound to a public key and contain details about the owner of the public key, such as name, address, issuing CA, expiration date, and so on.

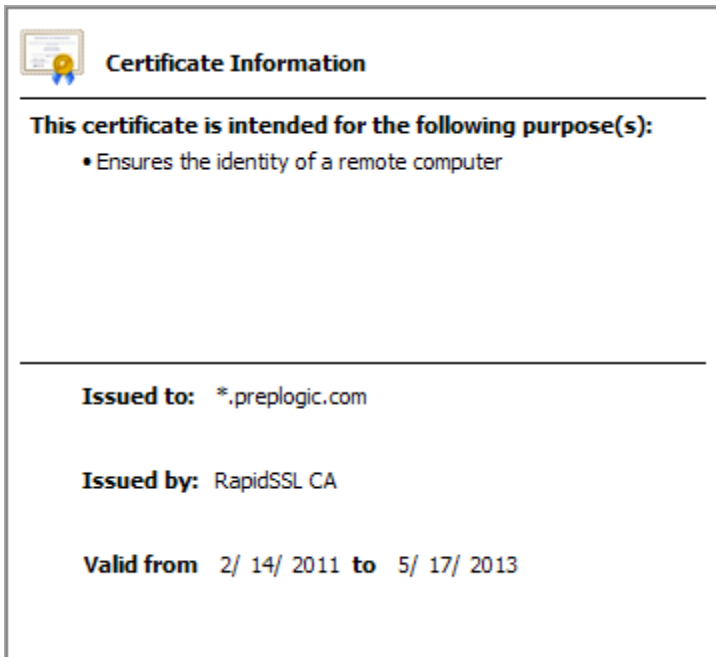

Figure 12: Example of a digital certificate

Certificate Authorities (CA)

A **certificate authority** or **certification authority** is any trusted third-party entity that issues digital certificates for use by other parties and are characteristic of PKI cryptography. Commercial CAs charge for services but alternative providers freely issue digital certificates for public consumption. Companies, institutions, and governments may implement their own internal entrusted CAs to sidestep potential exposures, risks, and threats associated with external entities.

Certificate Revocation List (CRL)

PKI cryptosystems utilize the **certificate revocation list** to maintain invalidated certificate entries. CRLs are generated and periodically published following a clearly-defined timeframe and can publish immediately following a recent certificate revocation. The CRL is always issued by the CA that issues the corresponding certificates and every CRL contains a valid lifetime (usually 24 hours or less) during which time it may be consulted by a PKI application for verification prior to use. RFC 5280 outlines the ten reasons to revoke a certificate.

According to RFC 3280, there are two states of certificate revocation:

1. **Revoked:** a certificate is irreversibly revoked if improperly issued, its private key considered compromised, or for lack of adherence to policy requirements (e.g., falsifying documents, misrepresented software behavior, general policy violations).
2. **Hold:** a reversible status used to denote temporary invalidity, as in the case of a lost private key; however, should the user relocate that key the certificate status can be revalidated thus removing its entry from future CRLs.

Public Key Infrastructure (PKI)

The **public key infrastructure** is a combination of cryptographic algorithms, technologies, protocols, policies, and services that enables senders and recipients to securely exchange secrets and confidential information across the public Internet. PKI encapsulates sensitive transactions for transmission across the untrusted public network using a trusted mutual authority—a Certificate Authority (CA), which issues digital certificates for provable identification. PKI consists of the CA issuer, a Registration Authority (RA) verifier, a directory of stored certificates, and a certificate management system.

Recovery Agent

A recovery agent leverages key escrow (see the "Key Escrow" section later in this domain) and acts as a third party who has the appropriate access to the keys that are needed for decrypting files. For example, if a user had encrypted files and that user then leaves the organization, the key needed to decrypt the files would be obtained from key escrow through a recovery agent.

Public Keys and Private Keys

Asymmetric cryptography introduces the concept of public and private key pairs used for secure exchange of private information across a public network medium. Public and private key construction enables sender and recipient to act as signers of private information (via public key) without having to divulge, expose, or reveal any aspect of the decryption (private) key.

Private keys must be closely guarded and kept secret, where public keys are intended for distribution. While messages can be encrypted by anyone with a public key, only the owner of the private key that is paired with the public key used for encryption can decrypt the message.

Key Registration

Among many likely services to be found in PKI, **key registration** is initially the most important because it handles the issuance of new certificates for public keys. Key registration binds user identities to digital certificates (as produced by the registration authority) for use with certificate authorities. The registration process may be carried out in software (by the CA) or under human supervision.

Registration Authority

A **registration authority** is tasked with verifying user identities and then instructing the certificate authority to issue digital certificates. RAs are a core component of the public-key infrastructure, which enables individuals and organizations to security exchange sensitive information. However, an RA is only responsible for authentication and identification of subjects but does not sign or issue digital certificates, which is sole responsibility of the certificate authority.

Key Escrow

Key escrow (also called **key recovery, trusted third party** or the **fair cryptosystem**) arranges for public and private decryption key storage so that an authorized third party may gain access in circumstances of need. Typically the decryption key to an encrypted communication is kept among only the person(s) directly involved; however, in certain cases a third-party individual (i.e., company or governmental entity) may require possession of decryption keys to investigate an incident or confirm a relationship between parties. A variety of key recovery requirements have been suggested by government agencies conducting covert surveillance within dynamically changing environments encompassing any number of old and new tactics, techniques, and technologies.

Key escrow systems that must furnish timely law enforcement access to an entire key or plaintext transformation present an unprecedented path to encrypted data recovery. This alternate path is beyond user control and removes a fundamental safeguard against mistaken or fraudulent release of keys or information. Non-recoverable systems can be designed and implemented without any such alternative recovery paths since they're unnecessary for ordinary operation and undesirable in many cases.

Trust Models

The certificate trust model establishes a baseline for entrusting users in a secure exchange. **Direct trust** is where two communicating parties are responsible for manually verifying signatures. **Indirect trust** uses a third party using a CA-issued or self-signed certificate for communication. A hierarchical trust model requires that all party certificates be issued by an independent third-party entity that may issue certificates itself or certificates used to issue certificates in a chain of subordinates.

PKI based on a hierarchical CA model is composed of well-defined trust and naming standards. Under this arrangement multiple CAs are organized into clearly defined parent-child relationships. Child CAs are certified by parent CA-issued certificates, which binds a CA public key to its identity. Basic types of CA trust model include:

- **Root trust model:** A CA is either a root or subordinate, and use of offline root CAs provides the highest level of security.
- **Network trust model:** Also called ***cross-certification***, every CA is both root and subordinate.
- **Hybrid trust model:** Combine elements of both rooted and network trust models.

PKI Implementation and Certificate Management

PKI certificate management protocols (like X.509)-defined for all relevant aspects of certificate creation, issuance, and management—help maintain the PKI management model. You must plan all parts of your PKI carefully to avoid subtly compromising or significantly weakening security. For security reasons, the private key used to digitally sign certificates should never be shared with anyone or transmitted across the Internet. Certificates contain the following: name, serial number, expiration date, a copy of the certificate holder's public key, and the digital signature of the issuing authority. Some digital certificates conform to the X.509 standard, which is an international standard specifying the formats for public-key certificates, certificate revocation lists (CRLs), attribute certificates, and certification path validation.

Failure to adequately plan for a secure root CA within a PKI hierarchy could compromise every certificate issued by that CA. Designing PKI to support a single application or process without forward consideration for future requirements can force you to redesign and redeploy, which may also compromise security and availability. Follow industry and organizational best practices for certificate management, enable CRL checking for native-mode clients, and protect the integrity of client authentication certificates. Use certificate trust lists to define the trusted root CAs, use Active Domain in Windows networks to deploy site server signing certificates, and guard that site server's certificate. Use a new key pair when renewing the server certificate and verify that all certificates are kept in secure certificate stores.

Practice Questions

Now it's time to see how much information you've retained. Don't get upset if you can't recall specific terms or definitions. Instead, take advantage of the fact that you may have forgotten some information. In other words, take note of all the questions that give you difficulty and return to that particular section in the exam manual. Remember, Rome wasn't built in a day. In time, as long as you continue studying and practicing answering questions, you will have built your own empire of security-related knowledge.

Domain 1 - Network Security

1. At which layers of the OSI model does an Application filtering firewall operate?
   - ❍ A. Layers 1-3 only
   - ❍ B. Layer 7 only
   - ❍ C. All
   - ❍ D. Host layers only

2. What security benefit does the creation of VLANs provide?
   - ❍ A. A reduction in administrative overhead
   - ❍ B. Isolation of network traffic and communication
   - ❍ C. Prevention of MAC spoofing and MAC flooding
   - ❍ D. Availability

3. Which of the following typically follows the implicit deny concept?
   - ❍ A. Firewall rule set
   - ❍ B. Keycard access
   - ❍ C. Airport security checkpoint
   - ❍ D. All of the above

4. FTP Secure (FTPS) encrypts FTP traffic using SSL for the secure transfer of files over the Internet and can operate in what two modes? Choose two.
   - ❍ A. Transport mode
   - ❍ B. Explicit mode
   - ❍ C. Tunnel mode
   - ❍ D. Implicit mode

5. Internet Protocol Security Suite (IPSec) VPNs provide which of the following? Choose all that apply.
   - ❍ A. Confidentiality
   - ❍ B. Integrity
   - ❍ C. Availability
   - ❍ D. DoS prevention

Domain 2 – Compliance and Operational Security

1. What does the Recovery Time Objective (RTO) define?
   - ❍ A. Amount of time that passes between system failures
   - ❍ B. Amount of time the restoration of a system or process will take when recovering from an outage
   - ❍ C. Amount of time a failed system or process must be restored within
   - ❍ D. Target point in time that data must be recovered from after a prolonged outage

2. Which of the following identifies the percentage of loss an asset could incur due to a specific threat?
   - ❍ A. Annualized Rate of Occurrence
   - ❍ B. Single Loss Expectancy
   - ❍ C. Exposure Factor
   - ❍ D. Annualized Loss Expectancy

3. Which of the following sites require the least amount of preparation when recovering from an outage?
   - ❍ A. Warm site
   - ❍ B. Hot site
   - ❍ C. Remote site
   - ❍ D. Cold site

4. Which redundant array of independent disks (RAID) level adds a stripe set to mirrored drives?
   - ❍ A. RAID 0
   - ❍ B. RAID 1
   - ❍ C. RAID 5
   - ❍ D. RAID 10

5. Which control category includes risk assessments, change management, and incident response?
   - ❍ A. Administrative / Procedural Controls
   - ❍ B. Operational Controls
   - ❍ C. Physical and Environmental Controls
   - ❍ D. Technical / Logical Controls

Domain 3 – Threats and Vulnerabilities

1. Which type of computer virus can avoid detection through cyclic changes to its original form?
   - ❍ A. Companion virus
   - ❍ B. Multipartite virus
   - ❍ C. Polymorphic virus
   - ❍ D. Worm

2. Which type of threat consists of a program or collection of programs designed to hide one's presence and activity on a compromised system?
   - ❍ A. Logic bomb
   - ❍ B. Trojan
   - ❍ C. Spyware
   - ❍ D. Rootkit

3. Which of the following attacks is not a form of Denial of Service (DoS)?
   - ❍ A. TCP replay
   - ❍ B. Ping flood
   - ❍ C. Smurf
   - ❍ D. Xmas attack

4. Which type of attack is targeted at a group of victims that have something in common, like using a specific bank or service, or working for the same company?
   - ❍ A. Phishing
   - ❍ B. Pharming
   - ❍ C. Vishing
   - ❍ D. Spear phishing

5. Which type of injection attack exploits vulnerabilities in the hypertext transfer protocol (HTTP) to access data and files on the local file system of the web server?
   - ❍ A. SQL Injection
   - ❍ B. Directory Traversal / Command Injection
   - ❍ C. LDAP Injection
   - ❍ D. Extensible Markup Language (XML) Injection

Domain 4 – Application, Data, and Host Security

1. What is the best way to prevent cross-site scripting (XSS) attacks?
   - ❍ A. By deploying anti-virus software
   - ❍ B. By requiring two-factor authentication
   - ❍ C. By deploying a NIDS
   - ❍ D. By validating input and sanitizing output

2. Which security control protects the confidentiality of data on a mobile device?
   - ❍ A. Screen lock
   - ❍ B. Device encryption
   - ❍ C. Anti-malware software
   - ❍ D. Remote wipe

3. Which of the following tests programs for security vulnerabilities, bugs, and errors?
   - ❍ A. Fuzzing
   - ❍ B. Vulnerability scanning
   - ❍ C. Penetration testing
   - ❍ D. Risk assessment

4. Which technical security control is the most effective at defending against zero-day exploits, when no security update for the vulnerability being leveraged exists?
   - ❍ A. Anti-virus
   - ❍ B. Network intrusion prevention system
   - ❍ C. Network intrusion detection system
   - ❍ D. Anti-spyware

5. Which of the following statements about patch management is false?
   - ❍ A. A patch management strategy should include all hardware and software
   - ❍ B. Patches should always be downloaded and installed immediately upon release
   - ❍ C. Patches should be tested prior to release into production
   - ❍ D. Systems should be scanned regularly to identify missing patches

Domain 5 – Access Control and Identity Management

1. Which of the following is not a type of biometric authentication?
   - ❍ A. Retina scan
   - ❍ B. Voice recognition
   - ❍ C. Smart card
   - ❍ D. Fingerprint scan

2. Separation of duties, mandatory vacations, and job rotation are examples of what type of security control?
   - ❍ A. Administrative
   - ❍ B. Technical
   - ❍ C. Physical
   - ❍ D. Environmental

3. Which access control model uses subject and object labeling?
   - A. Mandatory Access Control (MAC)
   - B. Discretionary Access Control (DAC)
   - C. Role-Based Access Control (RBAC)
   - D. Rule-Based Access Control (RBAC)

4. Which of the following encrypts all information exchanged between client and server?
   - A. RADIUS
   - B. TACACS
   - C. XTACACS
   - D. TACACS+

5. Kerberos uses which of the following for centralized authentication?
   - A. Ticket Granting Service
   - B. Ticket Granting Ticket
   - C. Key Distribution Center
   - D. Authentication Service

Domain 6 – Cryptography

1. Which of the following are examples of asymmetric key cryptography? Choose all that apply.
   - A. 3DES
   - B. AES
   - C. RSA
   - D. Diffie-Hellman

2. Quantum cryptography generates keys using a one-time pad and uses which of the following to exchange the private keys securely?
   - A. SSL
   - B. IPSec
   - C. Light
   - D. SSH

3. Which of the following processes 802.1x authentication requests through a Remote Access Dial-In User Server (RADIUS) system?
   - A. WPA2
   - B. WPA2-Enterprise
   - C. WPA
   - D. WEP

4. The SHA-1 hashing algorithm uses what size hash value?
   - A. 128-bit
   - B. 160-bit
   - C. 256-bit
   - D. 384-bit

5. Which one of the following added support for mutual (two-way) authentication?
   - A. CHAP
   - B. MS-CHAPv1
   - C. MS-CHAPv2
   - D. NTLMv1

Answers and Explanations

Okay, now that you've answered the questions to the best of your ability, it's time to see how many you answered correctly and how many you answered incorrectly. Remember, don't get upset – nobody is going to send you a report card for how well or how poorly you performed. The questions are meant to help you, not tear down your confidence levels. Below, not only will you find detailed explanations detailing why your selection was correct, you'll also find explanations for why the remaining answers are incorrect.

Domain 1 – Network Security

1. At which layers of the OSI model does an Application filtering firewall operate?
    A. Incorrect. Packet filtering firewalls operate at layers 1-3 (only) of the OSI model.
    B. Incorrect. All firewalls operate at layers 1-3 and some, like application filtering and next generation firewalls, operate at all layers.
    C. Correct. Application filtering firewalls operate at all seven layers of the OSI model.
    D. Incorrect. All firewalls operate at layers 1-3 and some, like application filtering and next generation firewalls, operate at all layers. The host layers of the OSI model include 4-7.

2. What security benefit does the creation of VLANs provide?
    A. Incorrect. While reduced administrative overhead is a benefit to expenses and resources, it is not a security benefit.
    B. Correct. VLANs create a deny-all unless specifically allowed networking environment for systems that are grouped together based on business needs or other logical requirements.
    C. Incorrect. Switches are vulnerable to MAC spoofing and MAC flooding attacks and the creation of VLANs does not prevent them.
    D. Incorrect. VLANs do not add redundancy, fail over, or provide any means for recovering from an outage or failure.

3. Which of the following typically follows the implicit deny concept?
    A. Incorrect. While firewall rule sets do follow the implicit deny concept, so do the others, making D the correct answer.
    B. Incorrect. While access systems that use keycards do follow the implicit deny concept, so do the others, making D the correct answer.
    C. Incorrect. While airport security checkpoints do follow the implicit deny concept, so do the others, making D the correct answer.
    D. Correct. All of the above follow the implicit deny concept of deny/block all unless explicitly allowed/permitted.

4. FTP Secure (FTPS) encrypts FTP traffic using SSL for the secure transfer of files over the Internet and can operate in what two modes? Choose two.
    A. Incorrect. IPSec VPNs can use a transport mode, but FTPS doesn't.
    B. Correct. FTPS can operate in either explicit mode (encryption level and type is negotiated) or implicit mode (encryption level and type is pre-defined and required by the server).
    C. Incorrect. Secure FTP (SFTP), not FTPS, tunnels FTP traffic through a Secure Shell (SSH) session. IPSec VPNs can also operate in tunnel mode.
    D. Correct. FTPS can operate in either explicit mode (encryption level and type is negotiated) or implicit mode (encryption level and type is pre-defined and required by the server).

5. Internet Protocol Security Suite (IPSec) VPNs provide which of the following? Choose all that apply.
    - **A. Correct. IPSec VPNs protect against eavesdropping, interception, and sniffing attacks by encrypting the connection between the user and VPN server.**
    - **B. Correct. IPSec VPNs use Authentication Headers to verify identities between parties in a conversation before data can be transmitted. IPSec VPNs also serialize messages with sequence numbers, which ensures integrity of transmitted data on the receiving end.**
    - C. Incorrect. IPSec VPNs do not improve the availability of network resources or data.
    - D. Incorrect. While IPSec VPNs can deter MiTM, replay, and spoofing attacks, they are not designed to protect against DoS attacks.

Domain 2 – Compliance and Operational Security

1. What does the Recovery Time Objective (RTO) define?
    - A. Incorrect. The Mean Time Between Failures (MTBF) is the amount of time that passes between system failures.
    - B. Incorrect. The Mean Time to Restore (MTR) is the amount of time the restoration of a system or process will take when recovering from an outage.
    - **C. Correct. The Recovery Time Objective (RTO) is the amount of time a failed system or process must be restored within.**
    - D. Incorrect. The Return Point Objective is the target point in time that data must be recovered from after a prolonged outage.

2. Which of the following identifies the percentage of loss an asset could incur due to a specific threat?
    - A. Incorrect. The ARO reflects the number of times in a year that an identified threat could take place.
    - B. Incorrect. The SLE is the cost of an event that is realized by multiplying the asset's value by the exposure factor, if a threat were to be successful. *Asset Value x Exposure Factor (EF) = Single Loss Expectancy (SLE).*
    - **C. Correct. The Exposure Factor (EF) identifies the percentage of loss an asset could incur due to a specific threat.**
    - D. Incorrect. The ALE is calculated by multiplying the single loss expectancy (SLE) and annualized rate of occurrence (ARO).

3. Which of the following sites require the least amount of preparation when recovering from an outage?
    - A. Incorrect. Warm sites require a moderate amount of maintenance to keep it at operating capacity and may not contain the most recent backups.
    - **B. Correct. Hot sites are specifically defined as being exact duplicates of the original environment, fully operational in every way including near-complete backups of original information.**
    - C. Incorrect. Unless specifically designated and configured as a fail-over location, a remote site doesn't have the means for recovering from an outage.
    - D. Incorrect. Cold sites are a low cost, entry-level backup site solution with the most time-consuming recovery phase of all other site options.

4. Which redundant array of independent disks (RAID) level adds a stripe set to mirrored drives?
    A. Incorrect. RAID 0 (striping without parity) is used strictly for performance and provides no fault-tolerance.
    B. Incorrect. RAID 1 is disk mirroring, but only requires 2 disks and does not add a stripe set.
    C. Incorrect. RAID 5 provides disk striping with parity across all disks, but not in a mirrored configuration.
    D. Correct. RAID 10 or RAID 1+0 requires a minimum of 4 disks and adds a stripe set to mirrored drives.

5. Which control category includes risk assessments, change management, and incident response?
    A. Incorrect. Administrative / procedural controls include an organizations policies, procedures, standards, and guidelines.
    B. Correct. Operational controls include risk assessments, change management, and incident response.
    C. Incorrect. Some examples of physical security controls include fences, gates, and checkpoints, landscape design, locked doors and keycard systems, cameras, and security guards. Examples of environmental controls would include temperature, humidity, airflow, and water.
    D. Incorrect. Technical / logical controls include passwords, firewalls, NIDS, NIPS, content filters, encryption, and more.

Domain 3 – Threats and Vulnerabilities

1. Which type of computer virus can avoid detection through cyclic changes to its original form?
    A. Incorrect. A companion virus is one that accompanies another ordinary executable file.
    B. Incorrect. Multipartite viruses reside in memory and are distributed through infected media.
    C. Correct. Polymorphic viruses avoid detection through cyclic changes to its original form.
    D. Incorrect. While similar in some ways, a worm is not a type of computer virus.

2. Which type of threat consists of a program or collection of programs designed to hide one's presence and activity on a compromised system?
    A. Incorrect. A logic bomb is defined as malicious code that lies dormant until triggered by some condition, date, or event.
    B. Incorrect. A Trojan horse application is malware disguised as a legitimate application.
    C. Incorrect. Spyware is installed surreptitiously and without the owner's or operator's consent and then attempts to harvest personal information.
    D. Correct. A rootkit consists of a program or collection of programs designed to hide one's presence and activity on a compromised system.

3. Which of the following attacks is not a form of Denial of Service (DoS)?
    A. Correct. A TCP replay attack reuses captured network packets in modified form against an original party of some trusted network conversation, but is not a type of DoS attack.
    B. Incorrect. A ping flood, a type of DoS attack, sends an overwhelming amount of ping traffic to a system, preventing delivery of other network traffic.
    C. Incorrect. A smurf attack is a DoS attack that takes advantage of vulnerabilities in network configuration and uses packets containing a spoofed IP address (belonging to the target victim) to direct an overwhelming amount of traffic to the victim's system.
    D. Incorrect. In computer networking, a packet that has all options enabled for the protocol in use is referred to as a Xmas packet. A large amount of Xmas packets sent to a victim's computer can result in denial of service as they require more resources to process.

4. Which type of attack is targeted at a group of victims that have something in common, like using a specific bank or service, or working for the same company?
    A. Incorrect. Phishing campaigns are often sent blindly to the Internet. While phishing has the same goal and presentation as spear phishing (obtaining personal information directly from the source while masquerading as a trustworthy entity), spear phishing campaigns specifically target and are sent only to a group of individuals based on something they have in common.
    B. Incorrect. Pharming leverages DNS poisoning, which will redirect a web page to an illegitimate source when a victim attempts to access a valid web site.
    C. Incorrect. Vishing is a social engineering attack that occurs through a telephone conversation and often exploits weaknesses in Voice over IP (VoIP).
    D. Correct. Spear phishing is a type of attack that is targeted at a group of victims that have something in common, like using a specific bank or service, or working for the same company.

5. Which type of injection attack exploits vulnerabilities in the hypertext transfer protocol (HTTP) to access data and files on the local file system of the web server?
    A. Incorrect. A SQL injection attack occurs when SQL commands that will execute on the database are sent through a web based application.
    B. Correct. A directory traversal or command injection attack exploits vulnerabilities in the hypertext transfer protocol (HTTP) to access data and files on the local file system of the web server.
    C. Incorrect. LDAP injection attacks prey on vulnerabilities in web applications that have access to query or modify the directory tree.
    D. Incorrect. XML injection attacks exploit vulnerabilities and the openness of XML to inject malicious code, modify the application's behavior, and retrieve or modify data.

Domain 4 – Application, Data, and Host Security

1. What is the best way to prevent cross-site scripting (XSS) attacks?
    A. Incorrect. While some anti-virus products may include the ability to detect and scan scripts and visited web pages, the best and most effective way to defend against XSS attacks is for programmers to validate input and sanitize the output of their web-based applications.
    B. Incorrect. Requiring two-factor authentication will not help prevent or detect XSS attacks.
    C. Incorrect. Network intrusion detection systems do not prevent attacks, they only alert on them.
    D. Correct. Programmers should validate input and sanitize the output of their web-based applications to ensure no malicious code is entered into their application, or that visitors are not presented with malicious code when accessing the program.

2. Which security control protects the confidentiality of data on a mobile device?
    A. Incorrect. While locking the screen when the device is not in use should be implemented, it does not protect the confidentiality of the data on the device as an attacker could access the phone using other means like through a USB or Bluetooth connection.
    B. Correct. Encrypting the device protects the confidentiality of the data on the unit.
    C. Incorrect. Anti-malware software does not protect the confidentiality of the data on the unit.
    D. Incorrect. A remote wipe relies on multiple factors to be successful and does not guarantee the confidentiality of the data on the unit.

3. Which of the following tests programs for security vulnerabilities, bugs, and errors?
   - **A. Correct. Fuzz testing (fuzzing) is a process that tests programs for security vulnerabilities, bugs, and errors through the use of a fuzz testing tool (fuzzer) that will input random, obscure, incorrect, or malicious data (fuzz) into the application to determine the outcome.**
   - B. Incorrect. Vulnerability scanning analyzes operating systems in addition to programs and while it identifies security weaknesses, it does not look for bugs and errors in an application.
   - C. Incorrect. Penetration testing finds and exploits security vulnerabilities in systems, protocols, networks, operating systems, and applications to determine if a system can be hacked and what an organization's security posture is. Penetration testing does not look for bugs and errors in an application.
   - D. Incorrect. Risk assessments capture identified risks and recommend mitigating controls and other courses of action, but they do not test programs for security vulnerabilities, bugs, and errors.

4. Which technical security control is the most effective at defending against zero-day exploits, when no security update for the vulnerability being leveraged exists?
   - A. Incorrect. While anti-virus programs can detect some unknown or unreported threats using heuristics, a NIPS is more effective as it analyzes the behavior of the malicious code and compares it against a baseline.
   - **B. Correct. A NIPS analyzes the behavior of malicious code, compares it against a baseline, and can take action against an unidentified threat without requiring human intervention.**
   - C. Incorrect. A NIDS is a detective control that relies on signatures and does not take any action on an identified threat.
   - D. Incorrect. Anti-spyware software scans the local host for malicious programs that capture sensitive information without the user's knowledge.

5. Which of the following statements about patch management is false?
   - A. Incorrect. A patch management strategy should include all hardware and software.
   - **B. Correct. Patches should always be reviewed, tested, and piloted prior to release in production.**
   - C. Incorrect. Patches should be tested prior to release into production.
   - D. Incorrect. Systems should be scanned regularly to identify missing patches.

Domain 5 – Access Control and Identity Management

1. Which of the following is not a type of biometric authentication?
   - A. Incorrect. A retina scan is a form of biometric authentication.
   - B. Incorrect. Voice recognition is a form of biometric authentication.
   - **C. Correct. A smart card is not a form of biometric authentication (something you *are*).**
   - D. Incorrect. A fingerprint scan is a form of biometric authentication.

2. Separation of duties, mandatory vacations, and job rotation are examples of what type of security control?
   - **A. Correct. Separation of duties, mandatory vacations, and job rotation are examples of administrative security controls.**
   - B. Incorrect. Technical controls include things like passwords, firewalls, NIDS, NIPS, content filters, encryption, and more.
   - C. Incorrect. Some examples of physical security controls include keycard systems, cameras, security guards, and bollards (used to prevent a vehicle from forcefully driving into a building).
   - D. Incorrect. Examples of environmental controls would include temperature, humidity, airflow, and water.

3. Which access control model uses subject and object labeling?
   - **A. Correct. Mandatory Access Control (MAC) uses subject and object labeling to allow or deny access to resources.**
   - B. Incorrect. Discretionary Access Control (DAC) restricts access to objects based on subject or identity or group membership.
   - C. Incorrect. A Role-Based Access Control (RBAC)model defines permissions according to job function.
   - D. Incorrect. A Rule-Based Access Control (RBAC) model allows or denies access to objects based on a set of administratively-defined rules.

4. Which of the following encrypts all information exchanged between client and server?
   - A. Incorrect. RADIUS leverages UDP and transmits some information in clear text.
   - B. Incorrect. TACACS does not encrypt all information exchanged between client and server.
   - C. Incorrect. XTACACS does not encrypt all information exchanged between client and server.
   - **D. Correct. TACACS+ is a completely rewritten version of TACACS and introduced support for multi-factor or strong-factor authentication, works similarly to a RADIUS system, and encrypts all information exchanged between client and server.**

5. Kerberos uses which of the following for centralized authentication?
   - A. Incorrect. The Ticket Granting Service (TGS) processes service requests received from the user.
   - B. Incorrect. The Key Distribution Center (KDC) verifies the user's credentials, and then creates, encrypts, and sends the TGT to the user.
   - **C. Correct. Kerberos uses a Key Distribution Center (KDC) for centralized authentication and relies heavily on time stamped tickets that are received from the Ticket Granting Server (TGS) when a client requests access.**
   - D. Incorrect. The Authentication Service encrypts and sends a Ticket Granting Ticket to the user's system.

Domain 6 – Cryptography

1. Which of the following are examples of asymmetric key cryptography? Choose all that apply.
   - A. Incorrect. 3DES is an example of symmetric key cryptography.
   - B. Incorrect. AES is an example of symmetric key cryptography.
   - **C. Correct. RSA is an example of asymmetric key cryptography.**
   - **D. Correct. Diffie-Hellman is an example of asymmetric key cryptography.**

2. Quantum cryptography generates keys using a one-time pad and uses which of the following to exchange the private keys securely?
   - A. Incorrect. Web sites and other technologies use SSL to encrypt communication sessions.
   - B. Incorrect. VPNs use IPSec to encrypt communication sessions.
   - **C. Correct. Quantum cryptography uses the physical properties of light to perform a secure private key exchange between two trusted parties.**
   - D. Incorrect. Secure Shell (SSH) creates an encrypted communication session between hosts.

3. Which of the following processes 802.1x authentication requests through a Remote Access Dial-In User Server (RADIUS) system?
    A. Incorrect. WPA2 uses the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP).
    B. Correct. WPA2-Enterprise processes 802.1x authentication requests through a Remote Access Dial-In User Server (RADIUS) system.
    C. Incorrect. WPA uses the Temporal Key Integrity Protocol (TKIP) encryption model adding encryption keys dynamically to each packet.
    D. Incorrect. WEP uses the RC4 stream cipher.

4. The SHA-1 hashing algorithm uses what size hash value?
    A. Incorrect. MD2, MD4, and MD5 use 128-bit hash values.
    B. Correct. SHA-1 uses a 160-bit hash value.
    C. Incorrect. SHA-256 uses a 256-bit hash value.
    D. Incorrect. SHA-384 uses a 384-bit hash value.

5. Which one of the following added support for mutual (two-way) authentication?
    A. Incorrect. CHAP compares one-way MD5 hashes between client and server to allow authentication to occur.
    B. Incorrect. MS-CHAPv1 only requires the hash (MD4) of the password to validate the challenge response.
    C. Correct. MS-CHAPv2 added support for mutual (two-way) authentication.
    D. Incorrect. NTLMv2, not NTLMv1, added support for mutual (two-way) authentication in Windows NT 4 SP4, but is being phased out by Kerberos.