Threat Domains

A threat domain is an area of control, authority, or protection that attackers can exploit to gain access to a system. Cyber threat categories include software attacks and errors, sabotage, human error, theft, hardware failures, utility interruption, and natural disasters. Internal threats are usually carried out by current or former employees and other contract partners. The source of an external threat typically stems from amateur or skilled attackers who can exploit vulnerabilities in networked devices, or use social engineering techniques. A user domain includes anyone with access to an organization's information system. Common user threats include poorly enforced security policies, data theft, unauthorized downloads and media, unauthorized VPNs and websites, and destruction of systems, applications, or data. Individual devices, LANs and private and public clouds are also vulnerable to attack. There are complex threats such as an APT and an algorithm attack. Cybercriminals use backdoor programs to gain unauthorized access to a system by bypassing the normal authentication procedures. Backdoors grant cybercriminals continued access to a system, even if the organization has fixed the original vulnerability used to attack the system. Most rootkits exploit software vulnerabilities to gain access to resources and modify system files. Rootkits can also modify system forensics and monitoring tools, making them very hard to detect.

The dark web is encrypted web content that is not indexed by conventional search engines and requires specific software, authorization, or configurations to access. IOCs such as malware signatures or domain names provide evidence of security breaches. AIS enables the real-time exchange of cybersecurity threat indicators using standardized and structured languages called STIX and TAXII.

1.6.1 What Did I Learn in this Module?

Threat Domains

Deception

Social engineering is a non-technical strategy that attempts to manipulate individuals into performing certain actions or divulging confidential information. Pretexting is when an individual lies to gain access to privileged data. Quid pro quo attacks are a request for personal information in exchange for something. Identity fraud is using a person's stolen identity to obtain goods or services by deception.

Social engineering tactics include impersonating an authority figure, intimidation, consensus ("everyone is doing it"), pretending something is scarce or that a situation is urgent, building familiarity and trust with an employee to eventually leverage that into access. Shoulder surfing is looking over a target's shoulder to gain valuable information such as PINs, access codes or credit card details. Criminals do not always have to be near their victim to shoulder surf, they can use binoculars or security cameras to obtain this information. Dumpster diving is going through a target's trash to see what information has been thrown out. Piggybacking or tailgating is when a criminal follows an authorized person to gain physical entry into a secure location or a restricted area. Other methods of deception include invoice scams, watering hole attacks, typosquatting, prepending, and influence campaigns.

Organizations need to promote awareness of social engineering tactics and properly educate employees on prevention measures.

Deception

Cyber Attacks

Malware is any code that can be used to steal data, bypass access controls, cause harm to or compromise a system. A virus is a type of computer program that, when executed, replicates, and attaches itself to other files by inserting its own code into it. A worm is a malicious software program that replicates by independently exploiting vulnerabilities in networks. A Trojan horse is malware that carries out malicious operations by masking its true intent. A logic bomb is a malicious program that waits for a trigger to set off the malicious code. Ransomware is designed to hold a computer system or the data it contains captive until a payment is made. DoS attacks work by creating an overwhelming quantity of traffic or by sending maliciously formatted packets that cannot be identified by an application, causing the receiving device to run slowly or crash. DDoS attacks are similar but originate from multiple coordinated sources. DNS attacks include spoofing and hijacking.

Layer 2 attacks include MAC address, ARP and IP spoofing, MAC flooding, man-in-the-middle, and man-in-the-mobile. Zero-Day attacks exploit software vulnerabilities before they become known. Keyboard logging (keylogging) logs keystrokes and configures the keylogger software to send the log file to the criminal. This log file can reveal usernames, passwords, websites visited, etc.

To defend against these attacks use firewalls, stay current on upgrades and patches, distribute the workload across server systems, and block external ICMP packets with firewalls.

1.6.1 What Did I Learn in this Module?

Cyber Attacks

Wireless and Mobile Device Attacks

Grayware is an unwanted application that behaves in an annoying or undesirable manner. SMiShing is fake text messages which prompt you to visit a malicious website or call a fraudulent phone number, which may result in malware being downloaded onto your device. A rogue access point is a wireless access point installed on a secure network without authorization. An evil twin attack is where the attacker's access point is set up to look like a better connection option. Radio frequency jamming is deliberately jamming the transmission of a radio or satellite station to prevent a wireless signal from reaching the receiving station.

Bluejacking sends unauthorized messages or shocking images to another Bluetooth device. Bluesnarfing is when an attacker copies information from a target's device using Bluetooth. WEP and WPA are security protocols that were designed to secure wireless networks. WPA2 is an improved security protocol. Unlike WEP, an attacker cannot recover WPA2's encryption key by observing network traffic.

To defend against wireless and mobile device attacks: change default configurations. Restrict access point placement by placing these devices outside the firewall or in a DMZ. Use WLAN tools to detect rogue access points or unauthorized workstations. Have a policy for guest access to a Wi-Fi network. Employees should use a remote access VPN for WLAN access.

Wireless and Mobile Device Attacks

Application and Other Attacks

XSS is a vulnerability found in many web applications. Types of Code Injection attacks include XML, SQL, DLL, and LDAP. A buffer overflow occurs when data is written beyond the limits of a buffer. Remote code execution is exploiting application vulnerabilities to execute any command with the privileges of the authorized user. Other application attacks include CSRF, race condition, improper input handling, error handling, API, replay, directory traversal, and resource exhaustion.

Write solid code to defend against an application attack. Treat and validate all input from outside of a function as if it is hostile. Keep all software up to date. Spam is unsolicited email that is usually a method of advertising. Some spam is sent in bulk by computers infected with viruses or worms. Phishing is when a user is contacted using email or instant message by a threat actor masquerading as a legitimate person. Spear phishing sends customized emails to a specific person based on information the attacker knows about them. Other common scams include vishing, pharming, and whaling. Other types of attacks include physical attacks to equipment, adversarial AI attacks, supply chain attacks and cloud-based attacks.

Use antivirus software to defend against email and browser attacks. Never assume that email attachments are safe. Always scan attachments before opening them. Become a member of the Anti-Phishing Working Group (APWG). All software should be kept up-to-date.

2.3.1 What Did I Learn in this Module?

Click on each of the headings to see a summary of the topics in this module.

Current State of Affairs

Network security relates directly to an organization's business continuity. Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people's privacy, and compromise the integrity of information. These breaches can result in lost revenue for corporations, theft of intellectual property, lawsuits, and can even threaten public safety. Many tools are available to help network administrators adapt, develop, and implement threat mitigation techniques, including the Cisco Talos Intelligence Group. An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network. Data is likely to be an organization's most valuable asset. Various DLP controls must be implemented, that combine strategic, operational, and tactical measures. Common data loss vectors include email and social networking, unencrypted data devices, cloud storage devices, removable media, hard copy, and improper access control.

Who is Attacking Our Network?

Click on each of the headings to see a summary of the topics in this module.

Current State of Affairs

Who is Attacking Our Network?

Understanding network security requires you to understand the following terms: threat, vulnerability, attack surface, exploit, and risk. Risk management is the process that balances the operational costs of providing protective measures with the gains achieved by protecting the asset. Four common ways to manage risk are risk acceptance, risk avoidance, risk reduction, and risk transfer. Hacker is a term used to describe a threat actor. White hat hackers are ethical hackers using their skills for good, ethical, and legal purposes. Grey hat hackers are individuals who commit crimes and do unethical things, but not for personal gain or to cause damage. Black hat hackers are criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks. Threat actors include script kiddies, vulnerability brokers, hacktivists, cybercriminals, and state-sponsored hackers. Many network attacks can be prevented by sharing information about IOCs. Many governments are promoting cybersecurity. CISA and NCSA are examples of such organizations.

3.4.1 What Did I Learn in this Module?

Click the headings to see a summary of the topics covered in this module.

IP PDU Details

IP was designed as a Layer 3 connectionless protocol. The IPv4 header consists of several fields while the IPv6 header contains fewer fields. It is important for security analysts to understand the different fields in both the IPv4 and IPv6 headers.

IP Vulnerabilities

TCP and UDP Vulnerabilities

IP PDU Details

IP Vulnerabilities

There are different types of attacks that target IP. Common IP-related attacks include:

- ICMP attacks
- Denial-of-Service (DoS) attacks
- Distributed Denial-of-Service (DoS) attacks
- Address spoofing attacks
- Man-in-the-middle attack (MiTM)
- Session hijacking

ICMP was developed to carry diagnostic messages and to report error conditions when routes, hosts, and ports are unavailable. Threat actors use ICMP for reconnaissance and scanning attacks. Threat actors also use ICMP for DoS and DDoS attacks. Threat actors often use amplification and reflection techniques to create DoS attacks. Threat actors also use resource exhaustion attacks to consume the resources of a target host to either crash it or to consume the resources of a network. IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user. Address spoofing attacks can be non-blind spoofing to hijack a session, or blind spoofing to create a DoS attack. MAC address spoofing attacks are used when threat actors have access to the internal network.

3.4.1 What Did I Learn in this Module?

IP Vulnerabilities

TCP and UDP Vulnerabilities

TCP segment and UDP datagram information appear immediately after the IP header. It is important to understand Layer 4 headers and their functions in data communication. TCP provides reliable delivery, flow control, and stateful communication. TCP stateful communication between two parties occurs during the TCP three-way handshake. Threat actors can conduct a variety of TCP related attacks:

- TCP port scans
- TCP SYN Flood attack
- TCP Reset Attack
- TCP Session Hijacking attack

The UDP segment (i.e., datagram) is much smaller than the TCP segment, which makes it very desirable for use by protocols that make simple request and reply transactions such as DNS, DHCP, SNMP, and others. Threat actors can conduct UDP flood attacks which sweep through all the known UDP ports on a server trying to find closed ports. This can create a DoS situation.

IP Services

Hosts broadcast an ARP Request to other hosts on the network segment to determine the MAC address of a host with a particular IP address. Any client can send an unsolicited ARP Reply called a “gratuitous ARP.” This feature of ARP also means that any host can claim to be the owner of any IP/MAC they choose. A threat actor can poison the ARP cache of devices on the local network, creating an MiTM attack to redirect traffic.

The Domain Name Service (DNS) protocol defines an automated service that matches resource names with the required numeric IP host address. It includes the message format for queries, responses, and data. It uses resource records (RR) to identify the type of DNS response. DNS is crucial to the operation of a network and should be secured accordingly. Many organizations use the services of publicly open DNS servers to provide responses to queries. DNS open resolvers are vulnerable to multiple malicious activities, including DNS cache poisoning, in which falsified records are provided to the open resolver. DNS amplification and reflection attacks are another type of attack in which the benign nature of the DNS protocol is exploited to cause DoS/DDoS attacks. In DNS resource utilization attacks, a DoS attack is launched against the DNS server itself. Threat actors often hide using DNS stealth techniques such as Fast Flux, in which malicious servers will rapidly change their IP address. Threat actors use Double IP Flux, in which threat actors will rapidly change both their domain name to IP mapping and their authoritative name server. Threat actors may also use domain shadowing to hide the source of their attacks by gathering domain account credentials in order to silently create multiple sub-domains to be used during attacks. DNS in the enterprise is sometimes overlooked as a protocol which can be used by botnets. Threat actors who use DNS tunneling place non-DNS traffic within DNS traffic. This method often circumvents security solutions. To be able to stop DNS tunneling, a filter that inspects DNS traffic must be used. Dynamic DNS servers are popular with threat actors and traffic that uses dynamic DNS should be a special concern of the cybersecurity analyst.

DHCP uses a simple exchange of broadcast and unicast messages to provide hosts with addressing information. A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. The rogue server might provide incorrect default gateway information, DNS server information, or IP addressing information.

4.4.1 What Did I Learn in this Module?

Enterprise Services

World Wide Web browsers are used by almost everyone. Blocking web browsing completely is not an option because businesses need access to the web. Cybersecurity analysts must have a good understanding of how a standard web-based attack works. The common stages of a typical web attack include the victim unknowingly visiting a web page that has been compromised by malware. The compromised web page redirects the user to a site that hosts malicious code. The browser is made to visit this site and malicious code infects their computer. This is known as a drive-by download. Regardless of the type of attack being used, the main goal of the threat actor is to ensure the victim’s web browser ends up on the threat actor’s web page, which then serves the malicious exploit to the victim. Some malicious sites take advantage of vulnerable plugins or browser vulnerabilities to compromise the client’s system. Larger networks rely on IDSs to scan downloaded files for malware. If detected, the IDS issues alerts and records the event to log files for later analysis. Server connection logs can often reveal information about the type of scan or attack. The different groups of connection status codes include **Informational 1xx, Successful 2xx, Redirection 3xx, Client Error 4xx,** and **Server Error 5xx.**To defend against web-based attacks, countermeasures that should be used include always updating the OS and browsers with current patches and updates, using a web proxy to block malicious sites, using the best security practices from the Open Web Application Security Project (OWASP) when developing web applications, and educating end users by showing them how to avoid web-based attacks.

There are a number of attacks that use email to carry malware payloads or to phish for personal information. SMTP servers can also have vulnerabilities and should be kept up to date with patches. Email security appliances can detect and block many types of known email threats including phishing, spam, and malware.

Web applications commonly connect to databases. Because these databases can contain sensitive information, they are a frequent target of attacks. Code injection and SQL injection attacks exploit insufficiently validated input fields to send commands to databases or other applications in order to gain access to private information. Cross-Site Scripting (XSS) attacks occur when browsers execute malicious scripts on the client and provide threat actors with access to sensitive information on the local host.

The OWASP Top 10 Web Application Security Risks is designed to help organizations create secure web applications. It is a useful list of potential vulnerabilities that are commonly exploited by threat actors.

Enterprise Services

Mitigating Common Network Attacks

The following best practices are used for securing a network: develop a written security policy, educate employees, control physical access to systems, use strong passwords, encrypt and password- protect sensitive data, implement security hardware and software, perform backups and test the back up files, shut down unnecessary services and ports, keep patches up-to-date, and perform security audits and tests.

The primary means of mitigating virus and Trojan horse attacks is antivirus software. A network security professional must be aware of the major viruses and keep track of security updates regarding emerging viruses.

Worms are more network-based than viruses. The response to a worm attack can be broken down into four phases: containment, inoculation, quarantine, and treatment.

Reconnaissance attacks can be mitigated in several ways: implement authentication to ensure proper access, use encryption to render packet sniffer attacks useless, use anti-sniffer tools to detect packet sniffer attacks, implement a switched infrastructure, and use a firewall and IPS. Encryption is also effective for mitigating packet sniffer attacks. Several techniques are available for mitigating access attacks: strong password security, principle of minimum trust, cryptography, and applying operating system and application patches.

To minimize the number of DoS attacks, a network utilization software package should be running at all times. DoS attacks could be a component of a larger offensive. DoS attacks can lead to problems in the network segments of the computers being attacked. Historically, many DoS attacks were sourced from spoofed addresses.

5.4.1 What did I learn in this module?

Click the headings to see a summary of the topics covered in this module.

Wireless Communications

Wireless networking devices connect to an Access Point (AP) or Wireless LAN Controller (WLC) suing the 802.11 standard. The 802.11 frame format is similar to the Ethernet frame format, except that it contains additional fields. WLAN devices use carrier sense multiple access with collision avoidance (CSMA/CA) as the method to determine how and when to send data on the network. To connect to the WLAN, wireless devices complete a three-stage process to discover a wireless AP, to authenticate with the AP, and to associate with the AP. APs can be configured autonomously (individually) or by using a WLC to simplify the configuration and monitoring of numerous access points.

WLAN Threats

Secure WLANs

Click the headings to see a summary of the topics covered in this module.

Wireless Communications

WLAN Threats

Wireless networks are susceptible to threats, including: data interception, wireless intruders, DoS attacks, and rogue APs. Wireless DoS attacks can be the result of: improperly configured devices, a malicious user intentionally interfering with the wireless communication, and accidental interference. A rogue AP is an AP or wireless router that has been connected to a corporate network without explicit authorization. When connected, a threat actor can use the rogue AP to capture MAC addresses, capture data packets, gain access to network resources, or launch a MITM attack. In a MITM attack, the threat actor is positioned in between two legitimate entities to read or modify the data that passes between the two parties. A popular wireless MITM attack is called the “evil twin AP” attack, where a threat actor introduces a rogue AP and configures it with the same SSID as a legitimate AP. To prevent the installation of rogue APs, organizations must configure WLCs with rogue AP policies.

Secure WLANs

5.4.1 What did I learn in this module?

Wireless Communications

WLAN Threats

Secure WLANs

To keep wireless intruders out and protect data, two early security features are still available on most routers and APs: SSID cloaking and MAC address filtering. There are four shared key authentication techniques available: WEP, WPA, WPA2, and WPA3 (Devices with WPA3 are not yet readily available.). Home routers typically have two choices for authentication: WPA and WPA2. WPA2 is the stronger of the two. Encryption is used to protect data. The WPA and WPA2 standards use the following encryption protocols: TKIP and AES. In networks that have stricter security requirements, an additional authentication or login is required to grant wireless clients access. The Enterprise security mode choice requires an Authentication, Authorization, and Accounting (AAA) RADIUS server.

6.3.1 What Did I Learn in this Module?

Click the headings to see a summary of the topics covered in this module.

Security Devices

There are several different types of firewalls. Packet filtering (stateless) firewalls provide Layer 3 and sometimes Layer 4 filtering. Firewall design is primarily about device interfaces permitting or denying traffic based on the source, the destination, and the type of traffic. A stateful inspection firewall allows or blocks traffic based on state, port, and protocol. Application gateway firewalls (proxy firewall) filter information at Layers 3, 4, 5, and 7. Next-generation firewalls provide additional services beyond application gateways such as Integrated intrusion prevention, application awareness and control to see and block risky apps, access to future information feeds, and techniques to address evolving security threats. Intrusion prevention systems (IPS) and intrusion detection systems (IDS) are used to detect potential security risks and alert/stop unsafe traffic. IDS/IPS can be implemented as host-based or network based with specific advantages and disadvantages to each implementation. Specialized security appliances are available including Cisco Advanced Malware Protection (AMP), Cisco Web Security Appliance (WSA), and Cisco Email Security Appliance (WSA). These security appliances utilize the services of the Cisco Talos Security Intelligence and Research Group. Talos detects and correlates threats in real time using the largest threat-detection network in the world.

6.3.1 What Did I Learn in this Module?

Click the headings to see a summary of the topics covered in this module.

Security Devices

Security Services

Network security services include the following technologies. ACLs are a series of statements that control whether a device forwards or drops packets based on information found in the packet header. NTP synchronizes the system time across all devices on the network to ensure accurate and consistent timestamping of system messages. Syslog servers compile and provide access to the system messages generated by networking devices. SNMP enables network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth. NetFlow provides statistics on packets that are flowing through a Cisco router or multilayer switch. Port mirroring is a feature that allows a switch to make duplicate copies of traffic that is passing through the switch, and then send it out a port that has a network monitor attached. AAA is a framework for configuring user authentication, authorization, and accounting services. AAA typically uses a TACACS+ or RADIUS server for this purpose. VPNs are private networks that are created between two endpoints across a public network.

7.5.1 What Did I Learn in this Module?

Click the headings to see a summary of the topics covered in this module.

Windows History

The first computers required a Disk Operating System (DOS) to create and manage files. Microsoft developed MS-DOS as a command line interface (CLI) to access the disk drive and load the operating system files. Early versions of Windows consisted of a Graphical User Interface (GUI) that ran over MS-DOS. However, modern Windows versions are in direct control of the computer and its hardware and support multiple user processes. This is much different than the single process, single user MS-DOS. Since 1993, there have been more than 20 releases of Windows that are based on the NT operating system. Users use a Windows GUI to work with data files and software. The GUI has a main area that is known as the Desktop and a Task Bar situated below the desktop. The Task Bar includes the Start menu, quick launch icons, and a notification area. Windows has many vulnerabilities. Recommendations to secure the Windows OS include use of virus or malware protection, use of strong passwords, use of firewall, and limited use of the administrator account, among others.

Windows Architecture and Operations

7.5. The Windows Operating System Summary

EN

Windows consists of a hardware abstraction layer (HAL) that is software that handles all of the communication between the hardware and the kernel. The kernel has control over the entire computer and handles input and output requests, memory, and all of the peripherals connected to the computer. Windows operates in two different modes. The first is user mode. Most Windows programs run in user mode. The second is kernel mode. It allows operating system code direct access to the computer hardware. Windows supports several different file systems, but NTFS is the most widely used. NTFS volumes include the partition boot sector, master file table, system files and the file area. When a computer boots, it first accesses system information and code that is stored in BIOS hardware. The BIOS boot code performs a system self-test called POST, locates and loads the Windows OS, and loads other associated programs to start the operating system. Windows should always be shutdown properly.

A computer works by storing instructions in RAM until the CPU processes them. Each process in a 32-bit Windows computer supports a virtual address space that enables addressing up to 4 gigabytes. Each process in a 64-bit Windows computer supports a virtual address space of up to 8 terabytes. Windows stores all of the information about hardware, applications, users, and system settings in a large database known as the registry. The registry is a hierarchical database where the highest level is known as a hive, below that there are keys, followed by subkeys. There are five registry hives that contain data regarding the configuration and operation of Windows. There are hundreds of keys and subkeys.

Windows Configuration and Monitoring

For security reasons, it is not advisable to log on to Windows using the Administrator account or an account with administrative privileges. Do not give standard users administrative privileges. Do not enable the Guests account unless the computer is going to be used by many different people who do not have accounts. Use Windows groups to make administration of users easier. Local users and groups are managed with the lusrmgr.msc control panel applet.

You can use the CLI or the Windows PowerShell to execute commands. PowerShell can be used to create scripts to automate tasks that the regular CLI is unable to automate. Windows Management Instrumentation (WMI) is used to manage remote computers. The **net** command can be combined with switches to focus on specific output. Task Manager provides a lot of information about what is running, and the general performance of the computer. The Resource Monitor provides more detailed information about resource usage. The Network and Sharing Center is used to configure Windows networking properties and test networking settings. The Server Message Block (SMB) protocol is used to share network resources such as files on remote hosts. The Universal Naming Convention (UNC) format is used to connect to resources. Windows Server is an edition of Windows that is mainly used in data centers. It provides network, file, web, and management services to a Windows network or domain.

7.5. The Windows Operating System Summary

EN

Windows Architecture and Operations

Windows Configuration and Monitoring

Windows Security

Malware can open communication ports to communicate and spread. The Windows **netstat** command displays all open communication ports on a computer and can also display the software processes that are associated with the ports. This enables unknown potentially malicious software to be identified and shutdown. Windows Event Viewer provides access to numerous logged events regarding the operation of a computer. Windows logs Windows events and applications and services events. Logged event severity levels range through the information, warning, error, or critical levels. It is very important to keep Windows up to date to guard against new security threats. Software patches, updates, and service packs address security vulnerabilities as they are discovered. Windows should be configured to automatically download and install updates as they become available. Windows can be configured to only install and restart a computer at specified times of day.

8.8.1 What Did I Learn in this Module?

Click the headings to see a summary of the topics covered in this module.

Linux Basics

Linux is a fast, reliable, and small open-source operating system. It requires few hardware resources to run and is highly customizable. It is designed to be used on networks. The Linux kernel is distributed by different organizations with different tools and software packages. A customized version of Linux that is called Security Onion contains software and tools that are designed for use in network security monitoring by cybersecurity analysts. Kali Linux is another customized Linux distribution that has numerous tools that are designed for network security penetration testing.

Working in the Linux Shell

In Linux, the user communicates with the operating system through a GUI or a command-line interface (CLI), or shell. If a GUI is running, the shell is accessed through at terminal application such as xterm or gnome terminal. Linux commands are programs that perform a specific task. The man command, followed by a specific command, provides documentation for that command. It is important to know at least basic Linux commands, file and directory commands, and commands for working with text files. In Linux everything is treated is if it were a file, including the memory, disks, monitor, and directories.

Linux Servers and Clients

Basic Server Administration

Linux Basics

Working in the Linux Shell

Linux Servers and Clients

Servers are computers that have software installed that enables them to provide services to client computers across the network. Some services provide access to external resources such as files, email, and web pages, to clients upon request. Other services run internally and perform tasks such as log management, memory management, or disk scanning. To enable a computer to provide multiple services, ports are used. A port is a reserved network resource that “listens” for requests by clients. While the port number that is used by a service can be configured, most services listen on default “well-known” ports. Client software applications are designed to communicate with specific types of servers. Web browsers are designed to communicate with web servers by using the HTTP protocol on port 80. FTP clients communicate with FTP servers to transfer files.

Basic Server Administration

8.8.1 What Did I Learn in this Module?

EN

Linux Servers and Clients

Basic Server Administration

In Linux, servers are managed by using configuration files. Various settings can be modified and saved in configuration files. When a service is started, it looks at its configuration file(s) to know how it should run. There is no rule for the way configuration files are written. Configuration file formatting depends on the creator of the server software. Linux devices should be secured by using proven methods to protect the device and administrative access. This is known as hardening devices. One way to harden a device is to maintain passwords, configure enhanced login features, and implement secure remote login with SSH. It is also very important to keep the operating system up to date. Other ways to harden a device are to force periodic password changes, enforce strong passwords, and to prevent reuse of passwords. Finally, Linux clients and servers use logfiles to record the operation of the system and important events. A number of different logfiles are maintained including application logs, event logs, service logs, and system logs. Server logs record activities that are conducted by remote users who access system services. It is important to know the location of different logs in the Linux file system so that they can be accessed and monitored for problems.

The Linux File System

Linux supports a number of different file systems that vary by speed, flexibility, security, size, structure, logic, and more. Some of the file systems that are supported by Linux are ext2, ext3, ext4, NFS, and CDFS. File systems are mounted on partitions and accessed through mounting points, or directories. Windows drive letters are examples of mounting points. The mount command can be used to display details of the file systems that are currently mounted on a Linux computer. The root file system is represented by the "/" symbol. It contains all of the files in the computer by default. Linux uses file permissions to control who is permitted to have different types of access to files and directories. Permissions include read (r), write (w), and execute (x). Files and directories have permissions that are assigned for users, groups, and others. The permissions for files and folders are displayed with the ls -l command. This command also displays the links for a file. Hard links create another file with a different name that is linked to the same place in the file system. The owner of the file and the group for the file are also displayed along with the date and time of the last modification to the file. File permissions are powerful features of the Linux file system and can't be violated. Only the root user can override file permissions. Because of the power of the root user, root access should be carefully controlled. Hard links are created with the ln command. Changes to one of the hard-linked files are also made to the original file. Symbolic links, or symlinks, are similar to hard links in that a change to the linked file is reflected in the original file. Symbolic links have several advantages over hard links.

8.8.1 What Did I Learn in this Module?

The Linux File System

Working with Linux GUI

The X Windows, or X11, system is a basic software framework that includes functions for creating, controlling, and configuring a windows GUI in a point-and-click interface. Different vendors use the X Windows system to create different windows manager GUIs for Linux. Examples of windows managers are Gnome and KDE. The Ubuntu Linux distribution uses Gnome 3 by default. The Gnome 3 desktop consists of the Apps Menu, Ubuntu Dock, Top Bar, Calendar and System Message tray, the Activities area, and the Status Menu.

Working on a Linux Host

8.8.1 What Did I Learn in this Module?

In order to install applications on Linux hosts, programs called package managers are used. Packages are software applications and all of their supporting files. Package managers are extremely helpful for installing complex software applications from centralized package repositories that are accessible over the internet. Different Linux distributions use different package managers. For example, Arch Linux uses pacman, Debian uses dpkg as the base package manager and apt to communicate with dpkg. Ubuntu also uses apt. Package manager CLI commands are used to install, remove, and update software packages. Upgrade commands upgrade all currently installed packages. Package management can also be performed in a GUI. Software processes are instances of computer programs that are running. Multitasking operating systems can run many processes at the same time. Forking is a method that the kernel uses to allow a running process to copy itself. The ps command lists the running processes, top displays information about running processes dynamically, and kill is used to remove, restart, or pause running processes. While Linux is considered to be better protected against malicious software (malware) than other operating systems, it is still susceptible to Trojan horses, worms, and other types of malware. Linux is usually attacked through its services and processes. Out of date software is often vulnerable to attack. Threat actors can probe a device for open ports that are linked to out of date server processes. With this knowledge, attacks can be launched. It is important to keep the operating system and its components and applications up to date. The chkrootkit program is designed to detect rootkit malware. Rootkits are deep level malware programs that are very difficult to detect and remove. They can change the fundamental operation of the operating system itself and can be used to create unauthorized access to systems. Piping commands uses the "|" symbol to chain different commands together by using the output of one command as the input for another.

9.5.1 What Did I Learn in this Module?

Click the headings to see a summary of the topics covered in this module.

Defending Systems and Devices

To secure an operating system, administrators should remove any unnecessary programs and services, and ensure that security patches and updates are installed. An organization should establish procedures for monitoring security-related information, evaluate updates, and install updates using a documented plan. Additionally, they should identify potential vulnerabilities by establishing a baseline to compare how a system is performing.

Malware includes viruses, worms, Trojan horses, keyloggers, spyware and adware. They invade privacy, steal information, damage the system or delete and corrupt data. Use reputable antimalware software. Fileless viruses use scripting languages such as Windows PowerShell and are hard to detect. Scripting languages such as Python, Bash, or VBA can be used to create malware. Remove non-compliant software immediately.

Patches are code updates that prevent a new virus, worm, or other malware from making a successful attack. Patches and upgrades are often combined into a service pack. A patch management tool can be used to manage patches locally. It is also important to update third-party applications such as Adobe Acrobat, Java and Chrome to address vulnerabilities. A host-based firewall runs on a device to restrict incoming and outgoing network activity for that device. HIDS software monitor system calls and file system access to detect malicious requests. HIPS monitors a device for known attacks and anomalies. EDR continuously monitors and collects data from an endpoint device, and then analyzes the data and responds to any threats. DLP tools ensure that sensitive data is not lost or accessed by unauthorized users. NGFW combines a traditional firewall with other network-device-filtering functions. Encryption is a tool used to protect data by using an algorithm to transform data and make it unreadable.

The Windows Encrypting File System (EFS) feature allows users to encrypt files, folders, or an entire hard drive. Boot integrity ensures that the system can be trusted and has not been altered while the operating system loads. Secure Boot is a security standard to ensure that a device boots using trusted software. Measured Boot can identify untrusted applications trying to load, and it also allows antimalware to load earlier.

unreadable.

The Windows Encrypting File System (EFS) feature allows users to encrypt files, folders, or an entire hard drive. Boot integrity ensures that the system can be trusted and has not been altered while the operating system loads. Secure Boot is a security standard to ensure that a device boots using trusted software. Measured Boot can identify untrusted applications trying to load, and it also allows antimalware to load earlier.

Administrators should have policies and countermeasures in place for unpatched software, unauthorized user downloads, malware, unattended devices, acceptable use policy violations, and unauthorized media. Protect physical equipment with cable locks, ciphered door locks, Faraday cages to block electromagnetic fields, and RFID tags to identify and track items.
Antimalware Protection

Endpoints are hosts on the network that can access (or be accessed by) other hosts on the network. With the IoT, other types of devices are now endpoints. Each endpoint is a potential opening for malware to access the network. Not all endpoints are within the network. Many endpoints connect to networks remotely over VPN. The network perimeter is always expanding. Various network security devices are required to protect the network perimeter from outside access. Many attacks originate from inside the network; therefore, securing an internal LAN is also important. After an internal host is infiltrated, it can become a starting point for an attacker to gain access to critical system devices. There are two internal LAN elements to secure: endpoints and network infrastructure.

Antivirus/Antimalware software is installed on a host to detect and mitigate viruses and malware. It does this using signature-based (using various characteristics of known malware files), heuristics-based (using general features shared by various types of malware), and behavior-based (using an analysis of suspicious behavior). Many antivirus programs are able to provide real-time protection by analyzing data as it is used by the endpoint. A host-based firewall restricts incoming and outgoing connections to connections initiated by that host only. Some firewall software can also prevent a host from becoming infected and stop infected hosts from spreading malware to other hosts. Most host-based security software includes logging functionality that is essential to cybersecurity operations. To protect endpoints in a borderless network use network-based, as well as host-based techniques.

Host-based Intrusion Prevention

9.5.1 What Did I Learn in this Module?

Click the headings to see a summary of the topics covered in this module.

Defending Systems and Devices

Host-based Intrusion Prevention

Host-based firewalls may use a set of predefined policies, or profiles, to control packets entering and leaving a computer. They may also have rules that can be directly modified or created to control access based on addresses, protocols, and ports. They can also be configured to issue alerts if suspicious behavior is detected. Logging varies depending on the firewall application. It typically includes date and time of the event, whether the connection was allowed or denied, information about the source or destination IP addresses of packets, and the source and destination ports of the encapsulated segments. (Distributed firewalls combine features of host-based firewalls with centralized management.)

Some examples of host-based firewalls include Windows Defender Firewall, iptables, nftables, and TCP Wrappers. A HIDS protects hosts against known and unknown malware. It can perform detailed monitoring and reporting on the system configuration and application activity, log analysis, event correlation, integrity checking, policy enforcement, rootkit detection, and alerting. A HIDS will frequently include a management server endpoint. Because the HIDS software must run directly on the host, it is considered an agent-based system. A HIDS uses both proactive and reactive strategies. A HIDS can prevent intrusion because it uses signatures to detect known malware and prevent it from infecting a system.

Signatures are not effective against new, or zero day, threats. In addition, some malware families exhibit polymorphism. Additional strategies to detect the possibility of successful attacks include anomaly-based detection and policy-based detection.

Application Security

Defending Systems and Devices

Host-based Intrusion Prevention

Application Security

An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker. It may consist of open ports on servers or hosts, software that is running on internet-facing servers, wireless network protocols, remote devices, and even users. The attack surface is continuing to expand. More devices are connecting to networks through the IoT and BYOD.

The SANS Institute describes three components of the attack surface: Network Attack Surface, Software Attack Surface, and Human Attack Surface. One way of decreasing the attack surface is to limit access to potential threats by creating lists of prohibited applications. Similarly, an organization can create lists of allowed programs in accordance with a security baseline that has been established by an organization. Sandboxing is a technique that allows suspicious files to be executed and analyzed in a safe environment. Automated malware analysis sandboxes offer tools that analyze malware behavior. These tools observe the effects of running unknown malware so that features of malware behavior can be determined and then used to create defenses against it. Polymorphic malware changes frequently and new malware appears regularly. Malware will enter the network despite the most robust perimeter and host-based security systems. HIDS and other detection systems can create alerts on suspected malware that may have entered the network and executed on a host.

Click the headings to see a summary of the topics covered in this module.

The Three Dimensions

The first dimension of the cybersecurity cube identifies the goals to protect cyberspace. Data **confidentiality** prevents the disclosure of information to unauthorized people, resources, or processes. Data **integrity** refers to the accuracy, consistency, and trustworthiness of data. Data **availability** ensures that information is accessible by authorized users when needed. You can use the acronym CIA to remember these three principles. The second dimension of the cybersecurity cube represents the three possible data states: data in **transit**, data at **rest** or in storage, and data in **process**.

The third dimension of the cybersecurity cube defines the pillars on which to base your cybersecurity defenses. These are: 1. technology, 2. policies and practices, and 3. improving education, training and awareness in people.

To accomplish confidentiality without using encryption, tokenization is a substitution technique that can isolate data elements from exposure to other data systems. Rights management covers both digital rights management (DRM) and information rights management (IRM). Both protect data from unauthorized access by using encryption. Types of sensitive information fall into three categories: personal information, business information and classified information. Some organizations deploy privacy enhancement technologies including anonymization, data minimization and tokenization to help resolve data privacy concerns.

Integrity is the accuracy, consistency and trustworthiness of data across its entire lifecycle. Methods used to ensure data integrity include hashing, data validation checks, data consistency checks and access controls. Availability ensures that information can be accessed whenever it is needed. Actions that help ensure availability include equipment maintenance, OS and software updates and patches, backup testing, disaster planning, new technology implementations, activity monitoring, and availability testing.

States of Data

Information security requires data to be protected in all three states: at rest, in transit and in process. Data is at rest when no user or process is accessing, requesting, or amending it. Data can be stored in DAS, RAID, NAS, SAN, or in the cloud. Direct-attached storage is vulnerable to malicious attacks on the local host. Data at rest also includes backup data (when it is not being written or in transit). Backups can be manual or automatic. Network storage systems including RAID, SAN and NAS provide greater performance and redundancy. They handle a lot of data, posing a greater risk to the organization if the device fails. The unique challenges of network storage systems include configuring, testing and monitoring the system.

Data in transit is data which is being transmitted – it is not at rest nor in use. A sneaker net uses removable media to physically move data from one computer to another. Wired networks include copper and fiber optic media and can serve a local area network (LAN) or span great distances in wide area networks (WAN). Both wired and wireless networks use packets or data units. Standard protocols such as the Internet Protocol (IP) and Hypertext Transfer Protocol (HTTP) define the structure and formation of data packets. Cybercriminals can capture, save and steal data in transit. Cybersecurity professionals can implement VPNs, using SSLs, IPsec and various other methods of encryption. Cybercriminals can intercept and alter data in transit. Cybersecurity professionals deploy data integrity systems that test the integrity and authenticity of transmitted data to counter these actions. These systems include hashing and data redundancy. Cybercriminals can use rogue or unauthorized devices to interrupt data availability, capturing it in transit. Mutual authentication systems require the user to authenticate to the server and requests the server to authenticate to the user.

Data in process refers to data during initial input, modification, computation, or output.

Protection of data integrity starts with the initial input of data. Organizations use several methods to collect data, each posing a potential threat to data integrity: data entry, scanning forms, file uploads and data collected from sensors.

Corruption during the input process may include mislabeling and incorrect or mismatched data formats, data entry errors or disconnected and/or malfunctioning or inoperable system sensors. When data is modified in a way that stops it from being readable or usable, this is often referred to as data corruption. Examples of output data corruption include the incorrect use of data delimiters, incorrect communication configurations and improperly configured printers. Invalid data modification during processing can have an adverse impact, and mitigating against such cases is important.

10.4.1 What Did I Learn in this Module?

States of Data

Cybersecurity Countermeasures

Administrators can install the following software-based countermeasures or safeguards on individual hosts or servers: software firewalls, network and port scanners, protocol analyzers, vulnerability scanners, and host-based IDS. A security awareness program and solid, comprehensive security policies are extremely important. Make security awareness training a part of an organization's onboarding process. Tie security awareness to job requirements or performance evaluations. Conduct in-person training sessions using gamification and activities. Complete online modules and courses.

An active security awareness program depends on the organization's environment and network, the level of threat, and the nature and demands of the data the organization holds. Developing security awareness should be an ongoing process because new threats and techniques are always emerging.

A comprehensive security policy demonstrates an organization's commitment to security. It sets the rules for expected behavior and ensures consistency in system operations and software and hardware acquisition, use, and maintenance. It defines the legal consequences of violations, and it gives security staff the backing of management. Types of security policies include identification and authentication, passwords, acceptable use, remote access, network maintenance, and incident handling.

Standards documents provide the technologies that specific users or programs need. In addition, they specifiy program requirements or criteria that an organization must follow. This helps IT staff improve efficiency and simplicity in design, maintenance, and troubleshooting. In addition to an organization's defined best practices, guidelines are also available from the following: the National Institute of Standards and Technology (NIST) Computer Security Resource Center, the National Security Agency (NSA) Security Configuration Guides, and the Common Criteria standard.

Procedure documents are longer and more detailed than standards and guidelines. They include implementation details that usually contain step-by-step instructions and graphics.

11.4.1 What Did I Learn in this Module?

Defense-in-Depth

To prepare for any type of attack, cybersecurity technicians must first identify assets, vulnerabilities, and threats. The collection of all the devices and information owned or managed by the organization are assets. The assets constitute the attack surface that threat actors could target. There are four steps to asset identification and classification: 1. Determine the proper asset identification category., 2. Establish asset accountability by identifying the owner of each information asset and each piece of software., 3. Determine the criteria for classification., and 4. Implement a classification schema. Asset standards identify specific hardware and software products used by an organization. The stages of an assets lifecycle are procurement, deployment, utilization, maintenance, and disposal. Identifying vulnerabilities on a network requires an understanding of the important applications that are used, as well as the different vulnerabilities of that application and hardware. Organizations must use a defense-in-depth approach to identify threats and secure vulnerable assets. This approach uses multiple layers of security at the network edge, within the network, and on network endpoints. There are two common analogies that are used to describe a defense-in-depth approach: the Security Onion and the Security Artichoke. To make sure data and infrastructure remain secure, an organization should create different layers of protection including layering, limiting, diversity, obscurity, and simplicity.

Cybersecurity Operations Management

Security Policies, Regulations, and Standards

11.4.1 What Did I Learn in this Module?

11.4.1 What Did I Learn in this Module?

Defense-in-Depth

Cybersecurity Operations Management

Configuration management refers to identifying, controlling, and auditing the implementation and any changes made to a system's established baseline. Documented configuration resources can include network maps, cabling/wiring diagrams, app configuration standards, naming conventions and an IP schema. Configuring log files along with auditing, changing default account names and passwords, and implementing account policies and file-level access control are all used to create a secure OS. Management of computer security log data should determine the procedures for the following: generating, transmitting, and storing log files, as well as analyzing and disposing of log data. Operating system logs record events that are linked to actions that have to do with the OS. Organizations use network-based and/or system-based security software to detect malicious activity. This software generates security logs which are useful for performing auditing analysis and identifying trends and long-term problems. Logs also enable an organization to provide documentation showing that it complies with laws and regulatory requirements. Packet analyzers, otherwise known as packet sniffers, intercept and log network traffic. Packet analyzers perform the following functions: traffic logging, network problem analysis, detection of network misuse, detection of network intrusion attempts, and isolation of exploited systems.

Security Policies, Regulations, and Standards

Defense-in-Depth

Cybersecurity Operations Management

Security Policies, Regulations, and Standards

Business policies define standards of correct behavior for the business and its employees. In networking, policies define the activities that are allowed on the network, setting a baseline of acceptable use. If behavior that violates business policy is detected on the network, it is possible that a security breach has occurred. Most organizations will have company policies, employee policies, and security policies. Security policies are made up of a variety of policies including: Identification and authentication, passwords, Acceptable Use, remote access, network maintenance, and incident handling. BYOD policies are made up of best practices including: password protected access, manual control of wireless connectivity, patches and updates are current, backups are current, enable “Find my Device”, use antivirus software, and use MDM. There are also external regulations regarding network security. Network security professionals must be familiar with the laws and codes of ethics that are binding on Information Systems Security (INFOSEC) professionals.

12.8.1 What Did I Learn in this Module?

Physical Security

Barricades or fencing are the two most common types of physical security. Biometrics are the physiological or behavioral characteristics of an individual. Biometric authentication systems can include measurements of the face, fingerprint, hand geometry, iris, retina, signature, and voice. The most common metric to describe the overall accuracy of a biometric authentication system is the Crossover Error Rate (CER). An access badge allows an individual to gain access to an area with automated entry points. Security guards are a great solution for access control requiring an instantaneous and appropriate response. Video and electronic surveillance can supplement or, in some cases, replace security guards. RFID asset tags can track any asset that physically leaves a secure area. New RFID asset tag systems can read multiple tags simultaneously.

Application Security

Physical Security

Application Security

To maintain security at all stages of application development, follow a process that includes: developing and testing, staging and production, and provisioning and deprovisioning. When coding applications, developers use techniques to validate that all security requirements have been met including: normalization, stored procedure, obfuscation and camouflage, code reuse and SDKs. Controlling the data input process is key to maintaining database integrity. Many attacks run against a database and insert malformed data. A validation rule checks that data falls within the parameters defined by the database designer. This helps to ensure the completeness, accuracy, and consistency of data. The integrity check performs a hash function to take a snapshot of data and then uses this snapshot to ensure data has remained unchanged. A checksum is an example of a hash function. Code signing helps prove that a piece of software is authentic. Using secure cookies protects information. Organizations can implement various measures including access policies, business continuity and disaster recovery plans, application and OS patches and updates policies, MFA and log file monitoring, data classification standards and backup procedures, and software testing prior to launch.

12.8.1 What Did I Learn in this Module?

Physical Security

Application Security

Network Hardening: Services and Protocols

Cybercriminals use vulnerable network services to attack a device, or to use it as part of an attack. Use a port scanner to detect open ports on a device. A port scanner sends a message to each port and waits for a response, which indicates how the port is used and whether it is open. Securing network services ensures that only necessary ports are exposed and available. DHCP uses a server to assign an IP address and other configuration information to network devices. DHCP snooping prevent rogue DHCP servers from providing IP addresses to clients by validating messages from sources that are not trusted. DNSSEC uses digital signatures to strengthen authentication and protect against threats to the DNS. The ping command is a network utility that uses ICMP to test the reachability of a host on a network. Cybercriminals can alter the use of ICMP to run reconnaissance, DoS, and covert channel attacks. Filter ICMP requests to prevent such attacks. RIP calculates the best route based on hop count, but cybercriminals can also target routers and the RIP protocol. Use secure services with authentication and implement system patching and updates to protect routing services. NTP allows network devices to synchronize their time settings with an NTP server. Use NTP Authentication to verify that the server is trusted. Secure Shell (SSH) is a protocol that provides a secure (encrypted) remote connection to a device. Telnet is an older protocol that uses unsecure plaintext when authenticating a device and transmitting data. Wherever possible, use SSH rather than Telnet to manage connections. SSH uses TCP port 22. Telnet uses TCP port 23. SCP uses SSH for data transfer and authentication, ensuring the authenticity and confidentiality of the data in transit. SNMP collects statistics from TCP/IP devices to monitor network and computer equipment. SNMPv3 is the current standard – it uses cryptography to prevent eavesdropping and make sure data hasn't been tampered with while in transit. HTTP provides basic web connectivity and uses port 80. Use SSL or TLS for better security.

Network Hardening: Segmentation

Application Security

Network Hardening: Services and Protocols

Network Hardening: Segmentation

VLANs provide a way to group devices within a LAN and on individual switches. VLANs are based on logical connections, while LANs are based on physical connections. Individual ports on a switch can be assigned to a specific VLAN. Other ports (trunks) can be used to physically interconnect switches and allow multiple VLAN traffic between switches. VLANs allow an administrator to segment a network. A VLAN can separate groups of devices that host sensitive data from the rest of the network, decreasing the chances of confidential information breaches. Trunks allow individuals on the HR VLAN to be physically connected to multiple switches. To protect the VLAN, monitor its performance, use advanced configurations, and regularly install patches and updates.

A DMZ is a small network between a trusted private network and the internet. Web servers and mail servers are usually placed within the DMZ to allow users to access an untrusted network, such as the internet, without compromising the internal network. Most networks have two to four zones of risk: the trusted private LAN, the DMZ, the internet, and an extranet. To protect its network, an organization can implement a Zero Trust model. Automatically trusting users and endpoints within the organization can put any network at risk, as trusted users can move throughout the network to access data. Zero Trust networking constantly monitors all users on the network regardless of their status or role.

Hardening Wireless and Mobile Devices

12.8.1 What Did I Learn in this Module?

Network Hardening: Services and Protocols

Network Hardening: Segmentation

Hardening Wireless and Mobile Devices

WEP was the first security protocol used for wireless networks. This was replaced by WPA, which improved the security of wireless connections. The evolution of WPA includes WPA2, WPA3 and WPS. Open system authentication is where any wireless device can connect to the wireless network. Shared key authentication provides mechanisms to authenticate and encrypt data between a wireless client and AP or wireless router. EAP is an authentication framework used in wireless networks. EAP includes EAP-TLS, PEAP, EAP-TTLS and EAP-FAST. The rogue access point will often imitate an authorized access point, allowing users to connect to the wireless network and potentially stealing their data. Mutual authentication is two-way authentication in which both entities in a communications link authenticate each other before they connect. Mobile devices can use wireless signals such as Wi-Fi and Bluetooth. NFC allows contactless communication between devices. IR provides short-range communication using an IR receiver. USB communication is the only type of communication on this list that is wired. It allows you to use your smartphone for data or audio storage. Storage segmentation and containerization allow you to separate personal and work content on a device. It provides an authenticated, encrypted area that separates sensitive company information from the user's personal data. There are security risks involved in using applications that share data (e.g., Dropbox, Box, Google Drive, and iCloud). An identity-management security system can be used to control what data a user can access. the allow list allows you to digitally sign applications so that you can authorize which applications users can install. Jailbreaking, rooting and sideloading are ways of bypassing a device's limitations to do things that the device is restricted from doing. Safeguards include screen locks, biometric authentication, context-aware authentication, remote wiping, and full device encryption. GPS uses satellites and computers to determine the location of a device.

Hardening Wireless and Mobile Devices

Cybersecurity Resilience

High availability systems typically are based on three design principles: eliminating single points of failure, providing for reliable crossover, and detecting failures as they occur. A popular high availability goal is called 'five nines.' It gets its name from its aim to achieve an availability rate of 99.999%. Systems standardization provides for systems that use the same components. Clustering is multiple devices grouped together provide a service that, to users, appears to be a single entity. Shared component systems are built so that a complete system can stand in for one that failed. A single point of failure can be a specific piece of hardware, a process, a specific piece of data, or even an essential utility. Generally, the solution to a single point of failure is to modify the critical operation so that it does not rely on any single element. Build redundant components into the operation to take over the process should one of these points fail. N+1 redundancy helps ensure system availability in the event of a component failure. It means that components (N) need to have at least one backup component (+1). RAID takes data that is normally stored on a single disk and spreads it out among several drives. Except for RAID 0, if any single disk is lost, the user can recover data from the other disks where the data also resides. STP's basic function is to prevent loops on a network when switches interconnect via multiple paths. STP ensures that redundant physical links are loop-free and only one logical path runs between all destinations on the network. The default gateway is typically the router that provides devices access to the rest of the network and/or to the internet. If there is only one router serving as the default gateway, it is a single point of failure. Install a standby router. Use location redundancy including: synchronous and asynchronous replication, and point-in-time replication. Resilient design is more than just adding redundancy. There are three availability solutions to address application resilience: fault tolerant hardware, cluster architecture, and backup and restore. A sound security policy should include regular data backups. Backups are usually stored off-site to protect the data if anything happens to the main facility. Protecting information systems includes electrical power systems and power considerations. A continuous supply of electrical power is essential for today's massive server and data storage facilities. HVAC systems control the ambient environment, including the temperature, humidity, and airflow. This must be managed along with data components such as hardware, cabling, data storage, fire protection, physical security systems and power, and their needs. Environmental requirements are detailed in product specifications documentation and/or physical planning guides.

12.8.1 What Did I Learn in this Module?

Embedded and Specialized Systems

Cyber attacks like Stuxnet proved that malware attacks could successfully destroy or interrupt critical infrastructures. To prevent attacks on these systems, segregate internal and external networks to separate the SCADA network from the organization's LAN. The IoT is the collection of technologies that enable various devices to connect to the internet. Most IoT devices connect to a network via wireless technology. IoT applications use RTOS. This data expansion created a new area in technology and business called 'Big Data.' Embedded systems capture, store and access data. They are susceptible to timing attacks, whereby attackers discover vulnerabilities by studying how long it takes the system to respond to different inputs. SoC technology is an SFF hardware module – customer-grade examples include devices such as Raspberry Pi and Arduino. These devices are single-board computers that can be implemented using an FGPA, which is an integrated circuit that can be programmed or modified in the field. Using an IoT scanner such as Shodan is an easy way to tell whether a home automation device is vulnerable to attack. IoT devices communicate using short-range, medium-range or long-range methods and include cellular (4G, 5G), radio You need an internet connection and a phone for VoIP. VoIP security is only as reliable as the underlying network security. There are several ways to protect your VoIP service. Two of these measures are: encrypt voice message packets to protect against eavesdropping, and use SSH to protect gateways and switches. Devices such as pacemakers, insulin pumps, medical implants and defibrillators are capable of wireless connectivity, remote monitoring, and NFC. Vulnerabilities in these medical devices can lead to patient safety issues, medical record leaks, or the risk of granting access to the network to cybercriminals. In-vehicle systems produce and store the data necessary for the operation of the vehicle along with its maintenance, safety protection and emergency contact transmission. Typically, a wireless interface connects to the internet and to a diagnostic interface on board. Encrypt all communication between controllers and use a firewall. An aircraft has many embedded control systems such as its flight control system and communication system. Security issues include the use of hard-coded logon credentials, insecure protocols, and backdoors. UAVs, more commonly called drones, have been used in military, agricultural and cartography applications, among others. Drones are very useful for aerial photography, surveillance, and surveying. However, drones are susceptible to hijacking, Wi-Fi attacks, GPS spoofing attacks, jamming and de-authentication attacks. Organizations use deception technologies to distract attackers from production networks. They also use them to learn an attacker's methods and to warn of potential attacks that could be launched against the network. Deception adds a fake layer to the organization's infrastructure. A honeypot is a decoy system that is configured to mimic a server in the organization's network. It is purposefully left exposed, to lure attackers. When an attacker goes after the honeypot, their activities are logged and monitored for later review. A honeynet is a collection of honeypots. A DNS sinkhole prevents the resolution of hostnames for specified URLs and can push users away from malicious resources.

13.5.1 What Did I Learn in this Module?

Access Controls

There are many types of access controls. This topic covered physical, logical, and administrative controls. Physical access controls are actual barriers deployed to prevent direct physical contact with systems. Examples include guards to monitor the facility, motion detectors, and mantraps. Logical access controls are the hardware and software solutions used to manage access resources and systems. Examples include encryption, ACLs, and intrusion detection systems. The concept of administrative access controls involves three security services: authentication, authorization, and accounting. Identification enforces the rules established by the authorization process. Multi-factor authentication uses at least two methods of verification. Authorization controls what a user can and cannot do on the network after successful authentication. Accountability traces an action back to a person or process making the change to the system.

13.5.1 What Did I Learn in this Module?

13.5.1 What Did I Learn in this Module?

Access Controls

Access Control Concepts

The CIA triad consists of the primary three components of information security: confidentiality, integrity, and availability. Network data can be encrypted (made unreadable to unauthorized users) using a variety of cryptography applications. The trend is that all data be encrypted. Zero trust is a comprehensive approach to securing all access across networks, applications, and environments. The principle of zero trust is “never trust, always verify”. Traditionally, the network perimeter, or edge, was the boundary between inside and outside, or trusted and untrusted. In a zero trust approach, any place at which an access control decision is required should be considered a perimeter. This means that although a user or other entity may have successfully passed access control previously, they are not trusted to access another area or resource until they are authenticated. The pillars of trust are zero trust for workforce, zero trust for workloads, and zero trust for workplace. Access control methods include discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), attribute-based control (ABAC), rule-based access (RBAC), and time-based access control (TAC). A common exploit is known as privilege escalation. In this exploit, vulnerabilities in servers or access control systems are exploited to grant access to an unauthorized user or software process.

Access Controls

Access Control Concepts

Account Management

Account types can include administrator accounts, user accounts, service accounts, and guest accounts. In addition to granting users no more access than is required, it is also important to disable accounts that are no longer needed. The principle of least privilege is closely connected to the concept of “need to know” access. Permission levels can be assigned to files and folders to include full control, modify, read and execute, write, and read. On a Windows computer, an administrator configures a domain security policy that applies to all domain members. Privileged accounts are used by administrators to deploy and manage operating systems, applications, and network devices. Robust practices for securing privileged accounts must be taken because they are often the target of cybercriminals. Authentication management aims to ensure secure sign in while still providing ease of use. Methods include SSO, Oath, a password vault, and KBA. HMAC uses an encryption key with a hash function to authenticate a web user. An authentication protocol authenticates data between two entities to prevent unauthorized access. Secure protocols include EAP, PAP, CHAP, 802.1x, RADIUS, TACACS+, and Kerberos.

13.5.1 What Did I Learn in this Module?

Access Control Concepts

Account Management

AAA usage and operation

A network must be designed to control who is allowed to connect to it and what they are allowed to do when they are connected. These design requirements are identified in the network security policy. The policy can also mandate the implementation of an accounting system that tracks who logged and when and what they did when they were logged in. Authentication, Authorization, and Accounting (AAA) systems provide the necessary framework to enable scalable security. AAA authentication can be used to authenticate users for local access, or it can be used to authenticate users for remote network access. Cisco provides two common methods of implementing AAA services: Local AAA Authentication and Server-based AAA Authentication. Centralized AAA is more scalable and manageable than local AAA and is the preferred AAA implementation. A centralized AAA system can leverage Active Directory or Lightweight Directory Access Protocol (LDAP) for user authentication and group membership, while maintaining its own authorization and accounting databases. Devices communicate with the centralized AAA server using with the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control Systems (TACACS+) protocols. Centralized AAA also enables the use of the accounting method. AAA accounting collects and reports usage data in AAA logs. Various types of accounting information that can be collected are network accounting, connection accounting, EXEC accounting, system accounting, command accounting, and resource accounting.