**1. Which organization is an international nonprofit organization that offers the CISSP certification?**

* CompTIA
* (ISC)2
* IEEE
* GIAC

**Explanation:** (ISC)2 is an international nonprofit organization that offers the CISSP certification.

**2. What is a benefit to an organization of using SOAR as part of the SIEM system?**

* SOAR was designed to address critical security events and high-end investigation.
* SOAR would benefit smaller organizations because it requires no cybersecurity analyst involvement once installed.
* SOAR automates incident investigation and responds to workflows based on playbooks.
* SOAR automation guarantees an uptime factor of “5 nines”.

**Explanation:** SIEM systems are used for collecting and filtering data, detecting and classifying threats, and analyzing and investigating threats. SOAR technology does the same as SIEMs but it also includes automation. SOAR integrates threat intelligence and automates incident investigation. SOAR also responds to events using response workflows based on previously developed playbooks.

**3. Which personnel in a SOC are assigned the task of hunting for potential threats and implementing threat detection tools?**

* Tier 3 SME
* Tier 2 Incident Reporter
* Tier 1 Analyst
* SOC Manager

**Explanation:** In a SOC, Tier 3 SMEs have expert-level skills in network, endpoint, threat intelligence, and malware reverse engineering (RE). They are deeply involved in hunting for potential security threats and implementing threat detection tools.

**4. Which three technologies should be included in a SOC security information and event management system? (Choose three.)**

* security monitoring
* threat intelligence
* proxy service
* firewall appliance
* intrusion prevention
* log management

**Explanation:** Technologies in a SOC should include the following:  
Event collection, correlation, and analysis  
Security monitoring  
Security control  
Log management  
Vulnerability assessment  
Vulnerability tracking  
Threat intelligence  
Proxy server, VPN, and IPS are security devices deployed in the network infrastructure.

**5. The term cyber operations alert analyst refers to which group of personnel in a SOC?**

* Tier 1 personnel
* Tier 3 personnel
* Tier 2 personnel
* SOC managers

**Explanation:** In a typical SOC, the Tier 1 personnel are called alert analysts, also known as cyberoperations analysts.

**6. How does a security information and event management system (SIEM) in a SOC help the personnel fight against security threats?**

* by analyzing logging data in real time
* by combining data from multiple technologies
* by integrating all security devices and appliances in an organization
* by dynamically implementing firewall rules

**Explanation:** A security information and event management system (SIEM) combines data from multiple sources to help SOC personnel collect and filter data, detect and classify threats, analyze and investigate threats, and manage resources to implement preventive measures.

**7. An SOC is searching for a professional to fill a job opening. The employee must have expert-level skills in networking, endpoint, threat intelligence, and malware reverse engineering in order to search for cyber threats hidden within the network. Which job within an SOC requires a professional with those skills?**

* Incident Responder
* Alert Analyst
* SOC Manager
* Threat Hunter

**Explanation:** Tier 3 professionals called Threat Hunters must have expert-level skills in networking, endpoint, threat intelligence, and malware reverse engineering. They are experts at tracing the processes of malware to determine the impact of the malware and how it can be removed.

**8. Which three are major categories of elements in a security operations center? (Choose three.)**

* technologies
* Internet connection
* processes
* data center
* people
* database engine

**Explanation:** The three major categories of elements of a security operations center are people, processes, and technologies. A database engine, a data center, and an Internet connection are components in the technologies category.

**9. Which KPI metric does SOAR use to measure the time required to stop the spread of malware in the network?**

* MITR
* Time to Control
* MITC
* MTTD

**Explanation:**  
The common key performance indicator (KPI) metrics compiled by SOC managers are as follows:  
• Dwell Time: the length of time that threat actors have access to a network before they are detected and the access of the threat actors stopped  
• Mean Time to Detect (MTTD): the average time that it takes for the SOC personnel to identify that valid security incidents have occurred in the network  
• Mean Time to Respond (MTTR): the average time that it takes to stop and remediate a security incident  
• Mean Time to contain (MTTC): the time required to stop the incident from causing further damage to systems or data  
• Time to Control the time required to stop the spread of malware in the network

**10. What job would require verification that an alert represents a true security incident or a false positive?**

* Alert Analyst
* Threat Hunter
* SOC Manager
* Incident Reporter

**Explanation:** A Cybersecurity Analyst monitors security alert queues and uses a ticketing system to assign alerts to a queue for an analyst to investigate. Because the software that generates alerts can trigger false alarms, one job of the Cybersecurity Analyst would be to verify that an alert represents a true security incident.

**11. When a user turns on the PC on Wednesday, the PC displays a message indicating that all of the user files have been locked. In order to get the files unencrypted, the user is supposed to send an email and include a specific ID in the email title. The message also includes ways to buy and submit bitcoins as payment for the file decryption. After inspecting the message, the technician suspects a security breach occurred. What type of malware could be responsible?**

* Trojan
* spyware
* adware
* ransomware

**Explanation:** Ransomware requires payment for access to the computer or files. Bitcoin is a type of digital currency that does not go through a particular bank.

**12. An employee connects wirelessly to the company network using a cell phone. The employee then configures the cell phone to act as a wireless access point that will allow new employees to connect to the company network. Which type of security threat best describes this situation?**

* rogue access point
* cracking
* spoofing
* denial of service

**Explanation:** Configuring the cell phone to act as a wireless access point means that the cell phone is now a rogue access point. The employee unknowingly breached the security of the company network by allowing a user to access the network without connecting through the company access point. Cracking is the process of obtaining passwords from data stored or transmitted on a network. Denial of service attacks refer to sending large amounts of data to a networked device, such as a server, to prevent legitimate access to the server. Spoofing refers to access gained to a network or data by an attacker appearing to be a legitimate network device or user.

**13. What are two examples of personally identifiable information (PII)? (Choose two.)**

* first name
* IP address
* language preference
* street address
* credit card number

**Explanation:** Personally identifiable information (PII) is any data that could potentially identify and track a specific individual. A credit card number and street address are the best examples of PII.

**14. What is the dark web?**

* It is a website that reports the most recent activities of cybercriminals all over the world.
* It is a website that sells stolen credit cards.
* It is part of the internet where a person can obtain personally identifiable information from anyone for free
* It is part of the internet that can only be accessed with special software.

**Explanation:** One of the more lucrative goals of cybercriminals is obtaining lists of personally identifiable information that can then be sold on the dark web. The dark web can only be accessed with special software and is used by cybercriminals to shield their activities. Stolen PII can be used to create fake accounts, such as credit cards and short-term loans.

**15. A company has just had a cybersecurity incident. The threat actor appeared to have a goal of network disruption and appeared to use a common security hack tool that overwhelmed a particular server with a large amount of traffic. This traffic rendered the server inoperable. How would a certified cybersecurity analyst classify this type of threat actor?**

* terrorist
* hacktivist
* state-sponsored
* amateur

**Explanation:**Amateurs or script kiddies use common, existing tools found on the internet to launch attacks. Hacktivists disrupt services in protest against organizations or governments for a particular political or social idea. State-sponsored threat actors use cyberspace for industrial espionage or interfering with another country in some way. Terrorist groups attack for a specific cause.

**16. A user calls the help desk complaining that the password to access the wireless network has changed without warning. The user is allowed to change the password, but an hour later, the same thing occurs. What might be happening in this situation?**

* rogue access point
* password policy
* weak password
* user error
* user laptop

**Explanation:**Man-in-the-middle attacks are a threat that results in lost credentials and data. These type of attacks can occur for different reasons including traffic sniffing.

**17. Which regulatory law regulates the identification, storage, and transmission of patient personal healthcare information?**

* FISMA
* HIPAA
* PCI-DSS
* GLBA

**Explanation:** The Health Insurance Portability and Accountability Act (HIPAA) requires that all patient personally identifiable healthcare information be stored, maintained, and transmitted in ways that ensure patient privacy and confidentiality.

**18. A worker in the records department of a hospital accidentally sends a medical record of a patient to a printer in another department. When the worker arrives at the printer, the patient record printout is missing. What breach of confidentiality does this situation describe?**

* EMR
* PII
* PSI
* PHI

**Explanation:** Protected Health Information (PHI) includes patient name, addresses, visiting dates and more. The Health Insurance Portability and Accountability Act (HIPAA) regulates and provides severe penalties for breaches of PHI. EMRs (Electronic Medical Records) are documents created and maintained by the medical community that contain PHI. Personally identifiable information (PII) is any information that can be used to positively identify an individual, such as name and social security number. Personal Security Information (PSI) is related to information about an individual such as passwords, access keys, and account details.

**19. What type of cyberwarfare weapon was Stuxnet?**

* botnet
* virus
* worm
* ransomware

**Explanation:**The Stuxnet worm was an excellent example of a sophisticated cyberwarfare weapon. In 2010, it was used to attack programmable logic controllers that operated uranium enrichment centrifuges in Iran.

**20. Which example illustrates how malware might be concealed?**  


* A hacker uses techniques to improve the ranking of a website so that users are redirected to a malicious site.
* An attack is launched against the public website of an online retailer with the objective of blocking its response to visitors.
* A botnet of zombies carry personal information back to the hacker.
* An email is sent to the employees of an organization with an attachment that looks like an antivirus update, but the attachment actually consists of spyware.

**Explanation:** An email attachment that appears as valid software but actually contains spyware shows how malware might be concealed. An attack to block access to a website is a DoS attack. A hacker uses search engine optimization (SEO) poisoning to improve the ranking of a website so that users are directed to a malicious site that hosts malware or uses social engineering methods to obtain information. A botnet of zombie computers is used to launch a DDoS attack.

**21. What websites should a user avoid when connecting to a free and open wireless hotspot?**

* websites to check account fees
* websites to check product details
* websites to check stock prices
* websites to make purchases

**Explanation:** Many free and open wireless hotspots operate with no authentication or weak authentication mechanisms. Attackers could easily capture the network traffic in and out of such a hotspot and steal user information. Therefore, users who use free and open wireless hotspots to connect to websites should avoid giving any personal information to the websites.

**22. In a smart home, an owner has connected many home devices to the Internet, such as the refrigerator and the coffee maker. The owner is concerned that these devices will make the wireless network vulnerable to attacks. What action could be taken to address this issue?**

* Configure mixed mode wireless operation.
* Install the latest firmware versions for the devices.
* Assign static IP addresses to the wireless devices.
* Disable the SSID broadcast.

**Explanation:** The Internet of Things (IoT) is facilitating the connection of different kinds of devices to the internet, like home devices such as coffee makers and refrigerators, and also wearable devices. In order to make these devices secure and not vulnerable to attacks, they have to be updated with the latest firmware.

**24. A group of users on the same network are all complaining about their computers running slowly. After investigating, the technician determines that these computers are part of a zombie network. Which type of malware is used to control these computers?**

* botnet
* spyware
* virus
* rootkit

**Explanation:** A botnet is a network of infected computers called a zombie network. The computers are controlled by a hacker and are used to attack other computers or to steal data.

**25. Which statement describes cyberwarfare?**

* It is Internet-based conflict that involves the penetration of information systems of other nations.
* It is simulation software for Air Force pilots that allows them to practice under a simulated war scenario.
* Cyberwarfare is an attack carried out by a group of script kiddies.
* It is a series of personal protective equipment developed for soldiers involved in nuclear war

**Explanation:** Cyberwarfare is Internet-based conflict that involves the penetration of the networks and computer systems of other nations. Organized hackers are typically involved in such an attack.

**26. Why do IoT devices pose a greater risk than other computing devices on a network?**

* Most IoT devices do not receive frequent firmware updates.
* Most IoT devices do not require an Internet connection and are unable to receive new updates.
* IoT devices cannot function on an isolated network with only an Internet connection.
* IoT devices require unencrypted wireless connections.

**Explanation:** IoT devices commonly operate using their original firmware and do not receive updates as frequently as laptops, desktops, and mobile platforms.

**27. Which cyber-attack involves a coordinated attack from a botnet of zombie computers?**

* DDoS
* MITM
* address spoofing
* ICMP redirect

**Explanation:** DDoS is a distributed denial-of-services attack. A DDoS attack is launched from multiple coordinated sources. The sources of the attack are zombie hosts that the cybercriminal has built into a botnet. When ready, the cybercriminal instructs the botnet of zombies to attack the chosen target.

**28. What is the main purpose of cyberwarfare?**

* to protect cloud-based data centers
* to develop advanced network devices
* to gain advantage over adversaries
* to simulate possible war scenarios among nations

**Explanation:** Cyberwarfare is Internet-based conflict that involves the penetration of the networks and computer systems of other nations. The main purpose of cyberwarfare is to gain advantage over adversaries, whether they are nations or competitors.

**1. Why would a network administrator choose Linux as an operating system in the Security Operations Center (SOC)?**

* It is easier to use than other operating systems.
* More network applications are created for this environment.
* It is more secure than other server operating systems.
* The administrator has more control over the operating system.

**Explanation:** There are several reasons why Linux is a good choice for the SOC.  
Linux is open source.  
The command line interface is a very powerful environment.  
The user has more control over the operating system.  
Linux allows for better network communication control.

**2. Which two methods can be used to harden a computing device? (Choose two.)**

* Allow default services to remain enabled.
* Allow USB auto-detection.
* Enforce the password history mechanism.
* Update patches on a strict annual basis irrespective of release date.
* Ensure physical security.

**Explanation:** The basic best practices for device hardening are as follows:  
Ensure physical security.  
Minimize installed packages.  
Disable unused services.  
Use SSH and disable the root account login over SSH.  
Keep the system updated.  
Disable USB auto-detection.  
Enforce strong passwords.  
Force periodic password changes.  
Keep users from reusing old passwords.  
Review logs regularly.

**3. Which Linux command can be used to display the name of the current working directory?**

* sudo
* ps
* pwd
* chmod

**Explanation:** One of the most important commands in Linux is the pwd command, which stands for print working directory. It shows users the physical path for the directory they are working in.

**4. Consider the result of the ls -l command in the Linux output below. What are the file permissions assigned to the sales user for the analyst.txt file?**

ls –l analyst.txt

-rwxrw-r-- sales staff 1028 May 28 15:50 analyst.txt

* write only
* read, write
* read only
* read, write, execute

**Explanation:** The file permissions are always displayed in the User Group and Other order. In the example displayed, the file has the following permissions:  
The dash ( – ) means that this is a file. For directories, the first dash would replaced with a “d”.  
The first set of characters is for user permission (rwx).  
The user, sales, who owns the file can read, write and execute the file.  
The second set of characters is for group permissions (rw-). The group, staff, who owns the file can read and write to the file.  
The third set of characters is for any other user or group permissions (r–). Any other user or group on the computer can only read the file.

**5. A Linux system boots into the GUI by default, so which application can a network administrator use in order to access the CLI environment?**

* system viewer
* file viewer
* package management tool
* terminal emulator

**Explanation:** A terminal emulator is an application program a user of Linux can use in order to access the CLI environment.

**6. What is the well-known port address number used by DNS to serve requests?**

* 25
* 53
* 110
* 60

**Explanation:** Port numbers are used in TCP and UDP communications to differentiate between the various services running on a device. The well-known port number used by DNS is port 53.

**7. Which user can override file permissions on a Linux computer?**

* any user that has ‘group’ permission to the file
* only the creator of the file
* any user that has ‘other’ permission to the file
* root user

**Explanation:** A user has as much rights to a file as the file permissions allow. The only user that can override file permission on a Linux computer is the root user. Because the root user has the power to override file permissions, the root user can write to any file.

**10. Which type of tool allows administrators to observe and understand every detail of a network transaction?**

* log manager
* malware analysis tool
* ticketing system
* packet capture software

**Explanation:** Network packet capture software is an important tool because it makes it possible to observe and understand the details of a network transaction.

**11. Why is Kali Linux a popular choice in testing the network security of an organization?**

* It is a network scanning tool that prioritizes security risks.
* It is an open source Linux security distribution containing many penetration tools.
* It can be used to test weaknesses by using only malicious software.
* It can be used to intercept and log network traffic.

**Explanation:** Kali is an open source Linux security distribution that is commonly used by IT professionals to test the security of networks.

**14. What are two advantages of the NTFS file system compared with FAT32? (Choose two.)**

* NTFS is easier to configure.
* NTFS supports larger files.
* NTFS allows faster formatting of drives.
* NTFS allows the automatic detection of bad sectors.
* NTFS allows faster access to external peripherals such as a USB drive.
* NTFS provides more security features.

**Explanation:** The file system has no control over the speed of access or formatting of drives, and the ease of configuration is not file system-dependent.

**15. A PC user issues the netstat command without any options. What is displayed as the result of this command?**

* a historical list of successful pings that have been sent
* a list of all established active TCP connections
* a network connection and usage report
* a local routing table

**Explanation:** When used by itself (without any options), the netstat command will display all the active TCP connections that are available.

**16. Which two commands could be used to check if DNS name resolution is working properly on a Windows PC? (Choose two.)**

* nslookup cisco.com
* net cisco.com
* ipconfig /flushdns
* nbtstat cisco.com
* ping cisco.com

**Explanation:** The ping command tests the connection between two hosts. When ping uses a host domain name to test the connection, the resolver on the PC will first perform the name resolution to query the DNS server for the IP address of the host. If the ping command is unable to resolve the domain name to an IP address, an error will result.

Nslookup is a tool for testing and troubleshooting DNS servers.

**17. What is the purpose of using the net accounts command in Windows?**

* to display information about shared network resources
* to show a list of computers and network devices on the network
* to start a network service
* to review the settings of password and logon requirements for users

**Explanation:** These are some common net commands:  
net accounts – sets password and logon requirements for users  
net start – starts a network service or lists running network services  
net use – connects, disconnects, and displays information about shared network resources  
net view – shows a list of computers and network devices on the network  
When used without options, the net accounts command displays the current settings for password, logon limitations, and domain information.

**19. A technician has installed a third party utility that is used to manage a Windows 7 computer. However, the utility does not automatically start whenever the computer is started. What can the technician do to resolve this problem?**

* Set the application registry key value to one.
* Use the Add or Remove Programs utility to set program access and defaults.
* Change the startup type for the utility to Automatic in Services .
* Uninstall the program and then choose Add New Programs in the Add or Remove Programs utility to install the application.

**Explanation:** The Services console in Windows OS allows for the management of all the services on the local and remote computers. The setting of Automatic in the Services console enables the chosen service to start when the computer is started.

**20. Which statement describes the function of the Server Message Block (SMB) protocol?**

* It is used to stream media contents.
* It is used to manage remote PCs.
* It is used to compress files stored on a disk.
* It is used to share network resources.

**Explanation:** The Server Message Block (SMB) protocol is primarily used by Microsoft to share network resources.

**21. A user creates a file with .ps1 extension in Windows. What type of file is it?**

* PowerShell function
* PowerShell cmdlet
* PowerShell documentation
* PowerShell script

**Explanation:** The types of commands that PowerShell can execute include the following:

* cmdlets – perform an action and return an output or object to the next command that will be executed
* PowerShell scripts – files with a .ps1 extension that contain PowerShell commands that are executed
* PowerShell functions – pieces of code that can be referenced in a script

**23. A user logs in to Windows with a regular user account and attempts to use an application that requires administrative privileges. What can the user do to successfully use the application?**

* Right-click the application and choose Run as Priviledge .
* Right-click the application and choose Run as Superuser .
* Right-click the application and choose Run as Administrator .
* Right-click the application and choose Run as root .

**Explanation:** As a security best practice, it is advisable not to log on to Windows using the Administrator account or an account with administrative privileges. When it is necessary to run or install software that requires the privileges of the Administrator, the user can right-click the software in the Windows File Explorer and choose **Run as Administrator** .

**24. An IT technician wants to create a rule on two Windows 10 computers to prevent an installed application from accessing the public Internet. Which tool would the technician use to accomplish this task?**

* Local Security Policy
* Computer Management
* Windows Defender Firewall with Advanced Security
* DMZ

**Explanation:** Windows Firewall with Advanced Security or the Windows 10 Windows Defender Firewall with Advanced Security is used to create inbound and outbound rules, connection security rules such as security traffic between two computers, and monitoring any active connection security rules.

**25. What technology was created to replace the BIOS program on modern personal computer motherboards?**

* UEFI
* MBR
* CMOS
* RAM

**Explanation:** As of 2015, most personal computer motherboards are shipped with UEFI as the replacement for the BIOS program.

**27. What is the outcome when a Linux administrator enters the man man command?**

* The **man man** command configures the network interface with a manual address
* The **man man** command opens the most recent log file
* The **man man** command provides a list of commands available at the current prompt
* The man man command provides documentation about the man command

**Explanation:** The man command is short for manual and is used to obtain documentation about a Linux command. The command man man would provide documentation about how to use the manual.

**29. What are two benefits of using an ext4 partition instead of ext3? (Choose two.)**

* an increase in the number of supported devices
* improved performance
* compatibility with NTFS
* increase in the size of supported files
* decreased load time
* compatibility with CDFS

**Explanation:** Based on the ex3 file system, an ext4 partition includes extensions that improve performance and an increase in the of supported files. An ext4 partition also supports journaling, a file system feature that minimizes the risk of file system corruption if power is suddenly lost to the system.

**30. Consider the result of the ls -l command in the Linux output below. What are the file permissions assigned to the sales user for the analyst.txt file?**

ls -l analyst.txt

-rwxrw-r-- sales staff 1028 May 28 15:50 analyst.txt

* read, write, execute
* write only
* read only
* read, write

**Explanation:** The file permissions are always displayed in the User Group and Other order. In the example displayed, the file has the following permissions:  
The dash ( – ) means that this is a file. For directories, the first dash would replaced with a “d”.  
The first set of characters is for user permission (rwx).  
The user, sales, who owns the file can read, write and execute the file.  
The second set of characters is for group permissions (rw-). The group, staff, who owns the file can read and write to the file.  
The third set of characters is for any other user or group permissions (r–). Any other user or group on the computer can only read the file.

**31. What is the purpose of entering the netsh command on a Windows PC?**

* to configure networking parameters for the PC
* to change the computer name for the PC
* to create user accounts
* to test the hardware devices on the PC

**Explanation:** The **netsh.exe** tool can be used to configure networking parameters for the PC from a command prompt.

**32. Which type of Windows PowerShell command performs an action and returns an output or object to the next command that will be executed?**

* cmdlets
* functions
* routines
* scripts

**Explanation:** The types of commands that PowerShell can execute include the following:

* **cmdlets** – perform an action and return an output or object to the next command that will be executed
* **PowerShell scripts** – files with a .ps1 extension that contain PowerShell commands that are executed
* **PowerShell functions** – pieces of code that can be referenced in a script

**33. A user creates a file with .ps1 extension in Windows. What type of file is it?**

* PowerShell documentation
* PowerShell cmdlet
* PowerShell script
* PowerShell function

**Explanation:** The types of commands that PowerShell can execute include the following:  
**cmdlets** – perform an action and return an output or object to the next command that will be executed  
**PowerShell scripts** – files with a .ps1 extension that contain PowerShell commands that are executed  
**PowerShell functions** – pieces of code that can be referenced in a script

**35. In the Linux shell, which character is used between two commands to instruct the shell to combine and execute these two commands in sequence?**

* $
* #
* %
* |

**Explanation:** In the Linux shell, several commands can be combined to perform a complex task. This technique is known as piping. The piping process is indicated by inserting the character “|” between two consecutive commands.

**36. Why is Linux considered to be better protected against malware than other operating systems?**

* customizable penetration and protection tools
* fewer deployments
* file system structure, file permissions, and user account restrictions
* integrated firewall

**Explanation:** The Linux operating design including how the file system is structured, standard file permissions, and user account restrictions make Linux a better protected operating system. However, Linux still has vulnerabilities and can have malware installed that affects the operating system.

**38. Which Windows tool can be used by a cybersecurity administrator to secure stand-alone computers that are not part of an active directory domain?**

* PowerShell
* Windows Defender
* Windows Firewall
* Local Security Policy

**Explanation:** Windows systems that are not part of an Active Directory Domain can use the Windows Local Security Policy to enforce security settings on each stand-alone system.

**1. When a wireless network in a small office is being set up, which type of IP addressing is typically used on the networked devices?**

* private
* public
* network
* wireless

**Explanation:** In setting up the wireless network in a small office, it is a best practice to use private IP addressing because of the flexibility and easy management it offers.

**2. Which two parts are components of an IPv4 address? (Choose two.)**

* logical portion
* host portion
* broadcast portion
* subnet portion
* network portion
* physical portion

**Explanation:** An IPv4 address is divided into two parts: a network portion – to identify the specific network on which a host resides, and a host portion – to identify specific hosts on a network. A subnet mask is used to identify the length of each portion.

**4. What is the full decompressed form of the IPv6 address 2001:420:59:0:1::a/64?**

* 2001:4200:5900:0:1:0:0:a000
* 2001:0420:0059:0000:0001:0000:000a
* 2001:0420:0059:0000:0001:000a
* 2001:0420:0059:0000:0001:0000:0000:000a
* 2001:420:59:0:1:0:0:a
* 2001:4200:5900:0000:1000:0000:0000:a000

**Explanation:** To decompress an IPv6 address, the two rules of compression must be reversed. Any 16-bit hextet that has less than four hex characters is missing the leading zeros that were removed. An IPv6 address should have a total of 8 groups of 16-bit hextets, a (::) can be replaced with consecutive zeros that were removed.

**5. A cybersecurity analyst believes an attacker is spoofing the MAC address of the default gateway to perform a man-in-the-middle attack. Which command should the analyst use to view the MAC address a host is using to reach the default gateway?**

* route print
* ipconfig /all
* netstat -r
* arp -a

**Explanation:** ARP is a protocol used with IPv4 to map a MAC address to an associated specific IP address. The command arp -a will display the MAC address table on a Windows PC.

**6. A user sends an HTTP request to a web server on a remote network. During encapsulation for this request, what information is added to the address field of a frame to indicate the destination?**

* the network domain of the destination host
* the MAC address of the destination host
* the IP address of the default gateway
* the MAC address of the default gateway

**Explanation:** A frame is encapsulated with source and destination MAC addresses. The source device will not know the MAC address of the remote host. An ARP request will be sent by the source and will be responded to by the router. The router will respond with the MAC address of its interface, the one which is connected to the same network as the source.

**7. What addresses are mapped by ARP?**

* destination IPv4 address to the source MAC address
* destination MAC address to a destination IPv4 address
* destination MAC address to the source IPv4 address
* destination IPv4 address to the destination host name

**Explanation:** ARP, or the Address Resolution Protocol, works by mapping a destination MAC address to a destination IPv4 address. The host knows the destination IPv4 address and uses ARP to resolve the corresponding destination MAC address.

**8. What type of information is contained in an ARP table?**

* domain name to IP address mappings
* switch ports associated with destination MAC addresses
* routes to reach destination networks
* IP address to MAC address mappings

**Explanation:** ARP tables are used to store mappings of IP addresses to MAC addresses. When a network device needs to forward a packet, the device knows only the IP address. To deliver the packet on an Ethernet network, a MAC address is needed. ARP resolves the MAC address and stores it in an ARP table.

**10. What type of information is contained in a DNS MX record?**

* the IP address of an authoritative name server
* the FQDN of the alias used to identify a service
* the domain name mapped to mail exchange servers
* the IP address for an FQDN entry

**Explanation:** MX, or mail exchange messages, are used to map a domain name to several mail exchange servers that all belong to the same domain.

**12. A PC is downloading a large file from a server. The TCP window is 1000 bytes. The server is sending the file using 100-byte segments. How many segments will the server send before it requires an acknowledgment from the PC?**

* 1000 segments
* 100 segments
* 1 segment
* 10 segments

**Explanation:** With a window of 1000 bytes, the destination host accepts segments until all 1000 bytes of data have been received. Then the destination host sends an acknowledgment.

**13. A user issues a ping 192.168.250.103 command and receives a response that includes a code of 1 . What does this code represent?**

* port unreachable
* network unreachable
* protocol unreachable
* host unreachable

**14. Which two commands can be used on a Windows host to display the routing table? (Choose two.)**

* netstat -r
* show ip route
* netstat -s
* route print
* tracert

**Explanation:** On a Windows host, the route print or netstat -r commands can be used to display the host routing table. Both commands generate the same output. On a router, the show ip route command is used to display the routing table. The netstat -s command is used to display per-protocol statistics. The tracert command is used to display the path that a packet travels to its destination.

**15. A user issues a ping 2001:db8:FACE:39::10 command and receives a response that includes a code of 2 . What does this code represent?**

* host unreachable
* port unreachable
* network unreachable
* protocol unreachable

**Explanation:** When a host or gateway receives a packet that it cannot deliver, it can use an ICMP Destination Unreachable message to notify the source that the destination or service is unreachable. The message will include a code that indicates why the packet could not be delivered. These are some of the Destination Unreachable codes for ICMPv4:

0 : net unreachable  
1 : host unreachable  
2 : protocol unreachable  
3 : port unreachable

**16. What message informs IPv6 enabled interfaces to use stateful DHCPv6 for obtaining an IPv6 address?**

* the ICMPv6 Router Solicitation
* the DHCPv6 Advertise message
* the DHCPv6 Reply message
* the ICMPv6 Router Advertisement

**Explanation:** Before an IPv6 enabled interface will use stateful DHCPv6 to obtain an IPv6 address, the interface must receive an ICMPv6 Router Advertisement with the managed configuration flag (M flag) set to 1.

**17. What is the purpose of ICMP messages?**

* to inform routers about network topology changes
* to ensure the delivery of an IP packet
* to provide feedback of IP packet transmissions
* to monitor the process of a domain name to IP address resolution

**Explanation:** The purpose of ICMP messages is to provide feedback about issues that are related to the processing of IP packets.

**19. What network service uses the WHOIS protocol?**

* HTTPS
* DNS
* SMTP
* FTP

**Explanation:** WHOIS is a TCP-based protocol that is used to identify the owners of internet domains through the DNS system.

**20. What action does a DHCPv4 client take if it receives more than one DHCPOFFER from multiple DHCP servers?**

* It sends a DHCPNAK and begins the DHCP process over again.
* It accepts both DHCPOFFER messages and sends a DHCPACK.
* It discards both offers and sends a new DHCPDISCOVER.
* It sends a DHCPREQUEST that identifies which lease offer the client is accepting.

**Explanation:** If there are multiple DHCP servers in a network, it is possible for a client to receive more than one DHCPOFFER. In this scenario, the client will only send one DHCPREQUEST, which includes the server from which the client is accepting the offer.

**21. Refer to the exhibit. From the perspective of users behind the NAT router, what type of NAT address is 209.165.201.1?**

* inside global
* inside local
* outside global
* outside local

**Explanation:** From the perspective of users behind NAT, inside global addresses are used by external users to reach internal hosts. Inside local addresses are the addresses assigned to internal hosts. Outside global addresses are the addresses of destinations on the external network. Outside local addresses are the actual private addresses of destination hosts behind other NAT devices.

**23. What is done to an IP packet before it is transmitted over the physical medium?**

* It is tagged with information guaranteeing reliable delivery.
* It is segmented into smaller individual pieces.
* It is encapsulated in a Layer 2 frame.
* It is encapsulated into a TCP segment.

**Explanation:** When messages are sent on a network, the encapsulation process works from the top of the OSI or TCP/IP model to the bottom. At each layer of the model, the upper layer information is encapsulated into the data field of the next protocol. For example, before an IP packet can be sent, it is encapsulated in a data link frame at Layer 2 so that it can be sent over the physical medium.

**24. Which PDU is processed when a host computer is de-encapsulating a message at the transport layer of the TCP/IP model?**

* segment
* packet
* frame
* bits

**Explanation:** At the transport layer, a host computer will de-encapsulate a segment to reassemble data to an acceptable format by the application layer protocol of the TCP/IP model.

**25. Which networking model is being used when an author uploads one chapter document to a file server of a book publisher?**

* peer-to-peer
* client/server
* master-slave
* point-to-point

**Explanation:** In the client/server network model, a network device assumes the role of server in order to provide a particular service such as file transfer and storage. In the client/server network model, a dedicated server does not have to be used, but if one is present, the network model being used is the client/server model. In contrast, a peer-to-peer network does not have a dedicated server.

**26. Which type of transmission is used to transmit a single video stream such as a web-based video conference to a select number of users?**

* anycast
* broadcast
* unicast
* multicast

**Explanation:** An anycast is used with IPv6 transmissions. A unicast is a transmission to a single host destination. A broadcast is a transmission sent to all hosts on a destination network.

**27. Refer to the exhibit. PC1 attempts to connect to File\_server1 and sends an ARP request to obtain a destination MAC address. Which MAC address will PC1 receive in the ARP reply?**

* the MAC address of the G0/0 interface on R2
* the MAC address of S2
* the MAC address of S1
* the MAC address of File\_server1
* the MAC address of the G0/0 interface on R1

**Explanation:** PC1 must have a MAC address to use as a destination Layer 2 address. PC1 will send an ARP request as a broadcast and R1 will send back an ARP reply with its G0/0 interface MAC address. PC1 can then forward the packet to the MAC address of the default gateway, R1.

**28. What is the result of an ARP poisoning attack?**

* Network clients are infected with a virus.
* Network clients experience a denial of service.
* Client memory buffers are overwhelmed.
* Client information is stolen.

**Explanation:** ARP poisoning is a technique used by an attacker to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway. The attacker, who is effectively doing an MITM attack, pretends to be the default gateway and sends an ARP reply to the transmitter of the ARP request. The receiver of the ARP reply will add the wrong MAC address to the ARP table and will send the packets to the attacker. Therefore, all traffic to the default gateway will funnel through the attacker device.

**29. What is the function of the HTTP GET message?**

* to upload content to a web server from a web client
* to retrieve client email from an email server using TCP port 110
* to request an HTML page from a web server
* to send error information from a web server to a web client

**Explanation:** There are three common HTTP message types:

GET – used by clients to request data from the web server  
POST – used by clients to upload data to a web server  
PUT – used by clients to upload data to a web server

**30. Which protocol is a client/server file sharing protocol and also a request/response protocol?**

* FTP
* UDP
* TCP
* SMB

**Explanation:**The Server Message Block (SMB) is a client/server file sharing protocol that describes the structure of shared network resources such as directories, files, printers, and serial ports. SMB is also a request/response protocol.

**31. How is a DHCPDISCOVER transmitted on a network to reach a DHCP server?**

* A DHCPDISCOVER message is sent with the broadcast IP address as the destination address.
* A DHCPDISCOVER message is sent with a multicast IP address that all DHCP servers listen to as the destination address.
* A DHCPDISCOVER message is sent with the IP address of the default gateway as the destination address.
* A DHCPDISCOVER message is sent with the IP address of the DHCP server as the destination address.

**Explanation:** The DHCPDISCOVER message is sent by a DHCPv4 client and targets a broadcast IP along with the destination port 67. The DHCPv4 server or servers respond to the DHCPv4 clients by targeting port 68.

**32. What is a description of a DNS zone transfer?**

* transferring blocks of DNS data from a DNS server to another server
* the action taken when a DNS server sends a query on behalf of a DNS resolver
* forwarding a request from a DNS server in a subdomain to an authoritative source
* finding an address match and transferring the numbered address from a DNS server to the original requesting client

**Explanation:** When a server requires data for a zone, it will request a transfer of that data from an authoritative server for that zone. The process of transferring blocks of DNS data between servers is known as a zone transfer.

**33. What are the two sizes (minimum and maximum) of an Ethernet frame? (Choose two.)**

* 128 bytes
* 64 bytes
* 1024 bytes
* 56 bytes
* 1518 bytes

**Explanation:** The minimum Ethernet frame is 64 bytes. The maximum Ethernet frame is 1518 bytes. A network technician must know the minimum and maximum frame size in order to recognize runt and jumbo frames.

**34. Which process failed if a computer cannot access the internet and received an IP address of 169.254.142.5?**

* DNS
* IP
* HTTP
* DHCP

**Explanation:** When a Windows computer cannot communicate with an IPv4 DHCP server, the computer automatically assigns itself an IP address in the169.254.0.0/16 range. Linux and Apple computers do not automatically assign an IP address.​

**35. Which statement describes a feature of the IP protocol?**

* IP relies on Layer 2 protocols for transmission error control.
* MAC addresses are used during the IP packet encapsulation.
* IP relies on upper layer services to handle situations of missing or out-of-order packets.
* IP encapsulation is modified based on network media.

**Explanation:** IP protocol is a connection-less protocol, considered unreliable in terms of end-to-end delivery. It does not provide error control in the cases where receiving packets are out-of-order or in cases of missing packets. It relies on upper layer services, such as TCP, to resolve these issues.

**36. What is a basic characteristic of the IP protocol?**

* connectionless
* media dependent
* user data segmentation
* reliable end-to-end delivery

**Explanation:** Internet Protocol (IP) is a network layer protocol that does not require initial exchange of control information to establish an end-to-end connection before packets are forwarded. Thus, IP is connectionless and does not provide reliable end-to-end delivery by itself. IP is media independent. User data segmentation is a service provided at the transport layer.

**37. Which statement describes the ping and tracert commands?**

* Both ping and tracert can show results in a graphical display.
* Ping shows whether the transmission is successful; tracert does not.
* Tracert shows each hop, while ping shows a destination reply only.
* Tracert uses IP addresses; ping does not.

**Explanation:** The ping utility tests end-to-end connectivity between the two hosts. However, if the message does not reach the destination, there is no way to determine where the problem is located. On the other hand, the traceroute utility ( tracert in Windows) traces the route a message takes from its source to the destination. Traceroute displays each hop along the way and the time it takes for the message to get to that network and back.

**38. A large corporation has modified its network to allow users to access network resources from their personal laptops and smart phones. Which networking trend does this describe?**

* cloud computing
* video conferencing
* online collaboration
* bring your own device

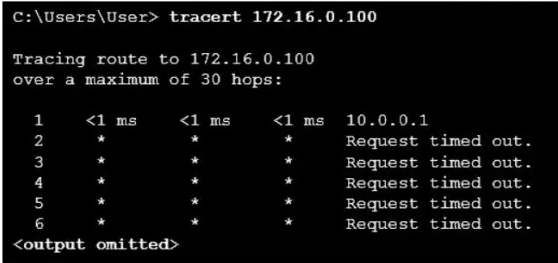
**Explanation:** BYOD allows end users to use personal tools to access the corporate network. Allowing this trend can have major impacts on a network, such as security and compatibility with corporate software and devices.

**40. Which method would an IPv6-enabled host using SLAAC employ to learn the address of the default gateway?**

* router advertisement messages received from the **link router**
* router solicitation messages received from the link router
* neighbor advertisement messages received from link neighbors
* neighbor solicitation messages sent to link neighbors

**Explanation:** When using SLAAC, a host will learn from the router advertisement that is sent by the link router the address to use as a default gateway.

**41. Refer to the exhibit. This PC is unable to communicate with the host at 172.16.0.100. What information can be gathered from the displayed output?**



* The target host is turned off.
* The communication fails after the default gateway.
* 172.16.0.100 is only a single hop away.
* This PC has the wrong subnet configured on its NIC

**Explanation:** The tracert command shows the path a packet takes through the network to the destination. In this example, only a response from the first router in the path is received, and all other responses time out. The first router is the default gateway for this host, and because a response is received from the router, it can be assumed that this host is on the same subnet as the router.

**42. A user issues a ping 192.168.250.103 command and receives a response that includes a code of 1. What does this code represent?**

* network unreachable
* port unreachable
* protocol unreachable
* host unreachable

**43. What are three responsibilities of the transport layer? (Choose three.)**

* identifying the applications and services on the client and server that should handle transmitted data
* conducting error detection of the contents in frames
* meeting the reliability requirements of applications, if any
* directing packets towards the destination network
* formatting data into a compatible form for receipt by the destination devices
* multiplexing multiple communication streams from many users or applications on the same network

**Explanation:** The transport layer has several responsibilities. Some of the primary responsibilities include the following:  
Tracking the individual communication streams between applications on the source and destination hosts  
Segmenting data at the source and reassembling the data at the destination  
Identifying the proper application for each communication stream through the use of port numbers  
Multiplexing the communications of multiple users or applications over a single network  
Managing the reliability requirements of applications

**44. How does network scanning help assess operations security?**

* It can detect open TCP ports on network systems.
* It can detect weak or blank passwords.
* It can simulate attacks from malicious sources.
* It can log abnormal activity.

**Explanation:** Network scanning can help a network administrator strengthen the security of the network and systems by identifying open TCP and UDP ports that could be targets of an attack.

**45. Refer to the exhibit. A network security analyst is examining captured data using Wireshark. The captured frames indicate that a host is downloading malware from a server. Which source port is used by the host to request the download?**

Graphical user interface, text, application

Description automatically generated

* 66
* 1514
* 6666
* 48598

**Explanation:** During the TCP three-way handshake process, the output shows that the host uses source port 48598 to initiate the connection and request the download.

**46. Which two operations are provided by TCP but not by UDP? (Choose two.)**

* retransmitting any unacknowledged data
* acknowledging received data
* reconstructing data in the order received
* identifying the applications
* tracking individual conversations

**Explanation:** Numbering and tracking data segments, acknowledging received data, and retransmitting any unacknowledged data are reliability operations to ensure that all of the data arrives at the destination. UDP does not provide reliability. Both TCP and UDP identify the applications and track individual conversations. UDP does not number data segments and reconstructs data in the order that it is received.

**47. A user is executing a tracert to a remote device. At what point would a router, which is in the path to the destination device, stop forwarding the packet?**

* when the router receives an ICMP Time Exceeded message
* when the RTT value reaches zero
* when the values of both the Echo Request and Echo Reply messages reach zero
* when the host responds with an ICMP Echo Reply message
* when the value in the TTL field reaches zero

**Explanation:** When a router receives a traceroute packet, the value in the TTL field is decremented by 1. When the value in the field reaches zero, the receiving router will not forward the packet, and will send an ICMP Time Exceeded message back to the source.

**48. A network administrator is testing network connectivity by issuing the ping command on a router. Which symbol will be displayed to indicate that a time expired during the wait for an ICMP echo reply message?**

* PC-A
* **router DG**
* DSN server
* router ISP
* web server

The Wireshark capture is of a DNS query from PC-A to the DNS server. Because the DNS server is on a remote network, the PC will send the query to the default gateway router, router DG, using the MAC address of the router G0/0 interface on the router.

**50. At which OSI layer is a source MAC address added to a PDU during the encapsulation process?**

* application layer
* presentation layer
* data link layer
* transport layer

**51. Which value, that is contained in an IPv4 header field, is decremented by each router that receives a packet?**

* Time-to-Live
* Fragment Offset
* Header Length
* Differentiated Services

**Explanation:** When a router receives a packet, the router will decrement the Time-to-Live (TTL) field by one. When the field reaches zero, the receiving router will discard the packet and will send an ICMP Time Exceeded message to the sender.

**52. What are three responsibilities of the transport layer? (Choose three.)**

* identifying the applications and services on the client and server that should handle transmitted data
* conducting error detection of the contents in frames
* meeting the reliability requirements of applications, if any
* directing packets towards the destination network
* formatting data into a compatible form for receipt by the destination devices
* multiplexing multiple communication streams from many users or applications on the same network

**Explanation:** The transport layer has several responsibilities. Some of the primary responsibilities include the following:  
Tracking the individual communication streams between applications on the source and destination hosts  
Segmenting data at the source and reassembling the data at the destination  
Identifying the proper application for each communication stream through the use of port numbers  
Multiplexing the communications of multiple users or applications over a single network  
Managing the reliability requirements of applications

**53. Which two ICMP messages are used by both IPv4 and IPv6 protocols? (Choose two.)​**

* route redirection
* neighbor solicitation
* router solicitation
* router advertisement
* protocol unreachable

**Explanation:** The ICMP messages common to both ICMPv4 and ICMPv6 include: host confirmation, destination (net, host, protocol, port) or service unreachable, time exceeded, and route redirection. Router solicitation, neighbor solicitation, and router advertisement are new protocols implemented in ICMPv6.

**54. What mechanism is used by a router to prevent a received IPv4 packet from traveling endlessly on a network?**

* It checks the value of the TTL field and if it is 100, it discards the packet and sends a Destination Unreachable message to the source host.
* It decrements the value of the TTL field by 1 and if the result is 0, it discards the packet and sends a Time Exceeded message to the source host.
* It checks the value of the TTL field and if it is 0, it discards the packet and sends a Destination Unreachable message to the source host.
* It increments the value of the TTL field by 1 and if the result is 100, it discards the packet and sends a Parameter Problem message to the source host.

**Explanation:** To prevent an IPv4 packet to travel in the network endlessly, TCP/IP protocols use ICMPv4 protocol to provide feedback about issues. When a router receives a packet and decrements the TTL field in the IPv4 packet by 1 and if the result is zero, it discards the packet and sends a Time Exceeded message to the source host.

**55. A device has been assigned the IPv6 address of 2001:0db8:cafe:4500:1000:00d8:0058:00ab/64. Which is the host identifier of the device?**

* 2001:0db8:cafe:4500:1000:00d8:0058:00ab
* 00ab
* 2001:0db8:cafe:4500
* 1000:00d8:0058:00ab

**Explanation:** The address has a prefix length of /64. Thus the first 64 bits represent the network portion, whereas the last 64 bits represent the host portion of the IPv6 address.

**56. What three application layer protocols are part of the TCP/IP protocol suite? (Choose three.)**

* DHCP
* PPP
* FTP
* DNS
* NAT
* ARP

**Explanation:** DNS, DHCP, and FTP are all application layer protocols in the TCP/IP protocol suite. ARP and PPP are network access layer protocols, and NAT is an internet layer protocol in the TCP/IP protocol suite.

**57. A computer can access devices on the same network but cannot access devices on other networks. What is the probable cause of this problem?**

* The computer has an invalid IP address.
* The cable is not connected properly to the NIC.
* The computer has an incorrect subnet mask.
* The computer has an invalid default gateway address.

**Explanation:** The default gateway is the address of the device a host uses to access the Internet or another network. If the default gateway is missing or incorrect, that host will not be able to communicate outside the local network. Because the host can access other hosts on the local network, the network cable and the other parts of the IP configuration are working.

**58. Refer to the exhibit. PC1 issues an ARP request because it needs to send a packet to PC3. In this scenario, what will happen next?**

Diagram

Description automatically generated with low confidence

* RT1 will send an ARP reply with its own Fa0/1 MAC address.
* SW1 will send an ARP reply with its Fa0/1 MAC address.
* RT1 will send an ARP reply with the PC3 MAC address.
* RT1 will forward the ARP request to PC3.
* RT1 will send an ARP reply with its own Fa0/0 MAC address.

**Explanation:** When a network device has to communicate with a device on another network, it broadcasts an ARP request asking for the default gateway MAC address. The default gateway (RT1) unicasts an ARP reply with the Fa0/0 MAC address.

**59. A user who is unable to connect to the file server contacts the help desk. The helpdesk technician asks the user to ping the IP address of the default gateway that is configured on the workstation. What is the purpose for this ping command?**

* to resolve the domain name of the file server to its IP address
* to request that gateway forward the connection request to the file server
* to obtain a dynamic IP address from the server
* to test that the host has the capability to reach hosts on other networks

**Explanation:** The ping command is used to test connectivity between hosts. The other options describe tasks not performed by ping . Pinging the default gateway will test whether the host has the capability to reach hosts on its own network and on other networks.

**60. A user gets an IP address of 192.168.0.1 from the company network administrator. A friend of the user at a different company gets the same IP address on another PC. How can two PCs use the same IP address and still reach the Internet, send and receive email, and search the web?**

* ISPs use Domain Name Service to change a user IP address into a public IP address that can be used on the Internet.
* Both users must be using the same Internet Service Provider.
* Both users must be on the same network.
* ISPs use Network Address Translation to change a user IP address into an address that can be used on the Internet.

**Explanation:** As user traffic from behind an ISP firewall reaches the gateway device, Network Address Translation changes private IP addresses into a public, routable IP address. Private user addresses remain hidden from the public Internet, and thus more than one user can have the same private IP address, regardless of ISP.

**61. How many host addresses are available on the 192.168.10.128/26 network?**

* 30
* 32
* 60
* 62
* 64

**Explanation:** A /26 prefix gives 6 host bits, which provides a total of 64 addresses, because 2 6 = 64. Subtracting the network and broadcast addresses leaves 62 usable host addresses.

**62. What are the three ranges of IP addresses that are reserved for internal private use? (Choose three.)**

* 64.100.0.0/14
* 192.168.0.0/16
* 192.31.7.0/24
* 172.16.0.0/12
* 10.0.0.0/8
* 127.16.0.0/12

**Explanation:** The private IP address blocks that are used inside companies are as follows:10.0.0.0 /8 (any address that starts with 10 in the first octet)  
172.16.0.0 /12 (any address that starts with 172.16 in the first two octets through 172.31.255.255)  
192.168.0.0 /16 (any address that starts with 192.168 in the first two octets)

**63. Refer to the exhibit. A cybersecurity analyst is viewing captured packets forwarded on switch S1. Which device has the MAC address 50:6a:03:96:71:22?**

Diagram

Description automatically generated

* PC-A
* router DG
* DSN server
* router ISP
* web server

The Wireshark capture is of a DNS query from PC-A to the DNS server. Because the DNS server is on a remote network, the PC will send the query to the default gateway router, router DG, using the MAC address of the router G0/0 interface on the router.

**64. A host PC is attempting to lease an address through DHCP. What message is sent by the server to let the client know it is able to use the provided IP information?**

* DHCPDISCOVER
* DHCPOFFER
* DHCPREQUEST
* DHCPACK
* DHCPNACK

**Explanation:** When a host uses DHCP to automatically configure an IP address, the typically sends two messages: the DHCPDISCOVER message and the DHCPREQUEST message. These two messages are usually sent as broadcasts to ensure that all DHCP servers receive them. The servers respond to these messages using DHCPOFFER, DHCPACK, and DHCPNACK messages, depending on the circumstance.

**65. An employee complains that a Windows PC cannot connect to the Internet. A network technician issues the ipconfig command on the PC and is shown an IP address of 169.254.10.3. Which two conclusions can be drawn? (Choose two.)**

* The PC is configured to obtain an IP address automatically.
* The default gateway address is not configured.
* The DNS server address is misconfigured.
* The enterprise network is misconfigured for dynamic routing.
* The PC cannot contact a DHCP server.

**Explanation:** When a Windows PC is configured to obtain an IP address automatically, the PC will try to obtain an IP address from a DHCP server. When the PC cannot contact a DHCP server, Windows will automatically assign an address belonging to the 169.254.0.0/16 range.

**66. What is a function of the tracert command that differs from the ping command when they are used on a workstation?**

* The tracert command is used to test the connectivity between two devices.
* The tracert command reaches the destination faster.
* The tracert command shows the information of routers in the path.
* The tracert command sends one ICMP message to each hop in the path.

**Explanation:** The tracert command sends three pings to each hop (router) in the path toward the destination and displays the domain name and IP address of hops from their responses. Because tracert uses the ping command, the travel time is the same as a standalone ping command. The primary function of a standalone ping command is to test the connectivity between two hosts.

**67. Which two functions or operations are performed by the MAC sublayer? (Choose two.)**

* It is responsible for Media Access Control.
* It performs the function of NIC driver software.
* It adds a header and trailer to form an OSI Layer 2 PDU.
* It handles communication between upper and lower layers.
* It adds control information to network protocol layer data.

**Explanation:** The MAC sublayer is the lower of the two data link sublayers and is closest to the physical layer. The two primary functions of the MAC sublayer are to encapsulate the data from the upper layer protocols and to control access to the media.

**68. Which field in an IPv4 packet header will typically stay the same during its transmission?**

* Flag
* Time-to-Live
* Packet Length
* Destination Address

**Explanation:** The value in the Destination Address field in an IPv4 header will stay the same during its transmission. The other options might change during its transmission.

**1. What is an advantage of HIPS that is not provided by IDS?**

* HIPS protects critical system resources and monitors operating system processes.
* HIPS deploys sensors at network entry points and protects critical network segments.
* HIPS monitors network processes and protects critical files.
* HIPS provides quick analysis of events through detailed logging.

**Explanation:** Network-based IDS (NIDS) sensors are typically deployed in offline mode. They do not protect individual hosts. Host-based IPS (HIPS) is software installed on a single host to monitor and analyze suspicious activity. It can monitor and protect operating system and critical system processes that are specific to that host. HIPS can be thought of as a combination of antivirus software, antimalware software, and a firewall.

**2. Which statement describes a difference between RADIUS and TACACS+?**

* RADIUS separates authentication and authorization whereas TACACS+ combines them as one process.
* RADIUS is supported by the Cisco Secure ACS software whereas TACACS+ is not.
* RADIUS uses TCP whereas TACACS+ uses UDP.
* RADIUS encrypts only the password whereas TACACS+ encrypts all communication.

**Explanation:** TACACS+ uses TCP, encrypts the entire packet (not just the password), and separates authentication and authorization into two distinct processes. Both protocols are supported by the Cisco Secure ACS software.

**3. What are two disadvantages of using an IDS? (Choose two.)**

* The IDS does not stop malicious traffic.
* The IDS works offline using copies of network traffic.
* The IDS has no impact on traffic.
* The IDS analyzes actual forwarded packets.
* The IDS requires other devices to respond to attacks.

**Explanation:** The disadvantage of operating with mirrored traffic is that the IDS cannot stop malicious single-packet attacks from reaching the target before responding to the attack. Also, an IDS often requires assistance from other networking devices, such as routers and firewalls, to respond to an attack. An advantage of an IDS is that by working offline using mirrored traffic, it has no impact on traffic flow.

**4. Which statement describes one of the rules that govern interface behavior in the context of implementing a zone-based policy firewall configuration?**

* An administrator can assign interfaces to zones, regardless of whether the zone has been configured.
* An administrator can assign an interface to multiple security zones.
* By default, traffic is allowed to flow among interfaces that are members of the same zone.
* By default, traffic is allowed to flow between a zone member interface and any interface that is not a zone member.

**Explanation:** An interface can belong to only one zone. Creating a zone is the first step in configuring a zone-based policy firewall. A zone cannot be assigned to an interface if the zone has not been created. Traffic can never flow between an interface that is assigned to a zone and an interface that has not been assigned to a zone.

**5. Which technique is necessary to ensure a private transfer of data using a VPN?**

* encryption
* virtualization
* scalability
* authorization

**Explanation:** Confidential and secure transfers of data with VPNs require data encryption.

**6. What is the function of the distribution layer of the three-layer network design model?**

* providing direct access to the network
* providing secure access to the Internet
* aggregating access layer connections
* providing high speed connection to the network edge

**Explanation:** The function of the distribution layer is to provide connectivity to services and to aggregate the access layer connections

**7. What two components of traditional web security appliances are examples of functions integrated into a Cisco Web Security Appliance? (Choose two.)**

* email virus and spam filtering
* VPN connection
* firewall
* web reporting
* URL filtering

**Explanation:** The Cisco Web Security Appliance is a secure web gateway which combines advanced malware protection, application visibility and control, acceptable use policy controls, reporting, and secure mobility functions. With traditional web security appliances, these functions are typically provided through multiple appliances. It is not a firewall appliance in that it only filters web traffic. It does not provide VPN connections, nor does it provide email virus and spam filtering; the Cisco Email Security Appliance provides these functions.

**8. Which AAA component can be established using token cards?**

* authentication
* accounting
* authorization
* auditing

**Explanation:** The authentication component of AAA is established using username and password combinations, challenge and response questions, and token cards. The authorization component of AAA determines which resources the user can access and which operations the user is allowed to perform. The accounting and auditing component of AAA keeps track of how network resources are used.

**9. Which statement describes a VPN?**

* VPNs use open source virtualization software to create the tunnel through the Internet.
* VPNs use dedicated physical connections to transfer data between remote users.
* VPNs use logical connections to create public networks through the Internet.
* VPNs use virtual connections to create a private network through a public network.

**Explanation:** A VPN is a private network that is created over a public network. Instead of using dedicated physical connections, a VPN uses virtual connections routed through a public network between two network devices.

**10. What is a host-based intrusion detection system (HIDS)?**

* It detects and stops potential direct attacks but does not scan for malware.
* It is an agentless system that scans files on a host for potential malware.
* It identifies potential attacks and sends alerts but does not stop the traffic.
* It combines the functionalities of antimalware applications with firewall protection.

**Explanation:** Accurint HIDS is a comprehensive security application that combines the functionalities of antimalware applications with firewall protection. An HIDS not only detects malware but also prevents it from executing.  
Because the HIDS runs directly on the host, itis considered an agent-based system.

**11. Which two devices would commonly be found at the access layer of the hierarchical enterprise LAN design model? (Choose two.)**

* modular switch
* Layer 3 device
* Layer 2 switch
* firewall
* access point

**Explanation:** While some designs do route at the access layer, the two devices that should always be placed at the access layer of the hierarchical design model are an access point and a Layer 2 switch. A modular switch is commonly used at the core layer. Routing by a Layer 3 device is commonly used in the distribution layer. The firewall is a device in the Internet edge network design.

**12. Which two statements are true about NTP servers in an enterprise network? (Choose two.)**

* There can only be one NTP server on an enterprise network.
* NTP servers at stratum 1 are directly connected to an authoritative time source.
* NTP servers control the mean time between failures (MTBF) for key network devices.
* NTP servers ensure an accurate time stamp on logging and debugging information.
* All NTP servers synchronize directly to a stratum 1 time source.

**Explanation:** Network Time Protocol (NTP) is used to synchronize the time across all devices on the network to make sure accurate timestamping on devices for managing, securing and troubleshooting. NTP networks use a hierarchical system of time sources. Each level in this hierarchical system is called a stratum. The stratum 1 devices are directly connected to the authoritative time sources.

**13. In the data gathering process, which type of device will listen for traffic, but only gather traffic statistics?**

* NetFlow collector
* NMS
* SNMP agent
* syslog server

**Explanation:** A NetFlow collector is the device that receives traffic statistics from networking devices. NetFlow only gathers traffic statistics, unlike syslog and SNMP which can collect various network events.

**14. Which two protocols are link-state routing protocols? (Choose two.)**

* ISIS
* EIGRP
* BGP
* RIP
* OSPF

**Explanation:** ISIS and OSPF are link-state routing protocols. EIGRP and RIP are distance vector routing protocols. BGP is a path vector protocol.

**15. What type of route is created when a network administrator manually configures a route that has an active exit interface?**

* directly connected
* static
* local
* dynamic

**Explanation:** A static route is one that is manually configured by the network administrator.

**16. Which characteristic describes a wireless client operating in active mode?**

* must be configured for security before attaching to an AP
* broadcasts probes that request the SSID
* ability to dynamically change channels
* must know the SSID to connect to an AP

**Explanation:** A wireless client operating in active mode must know the name of the SSID. Probe requests are broadcast by a client across multiple channels and include the SSID name and supported standards. Active mode is used if an AP is configured to not broadcast beacon frames.

**17. What are two types of addresses found on network end devices? (Choose two.)**

* return
* IP
* MAC
* TCP
* UDP

**Explanation:** Intermediary devices use two types of addresses when sending messages to the final destination device, MAC and IP addresses. TCP and UDP are protocols used at Layer 4 to identify what port numbers are being used on the source and destination devices. A return address is used when mailing a letter, not in networking.

**18. What is a characteristic of the WLAN passive discover mode?**

* The client must know the name of the SSID to begin the discover process.
* The client begins the discover process by sending a probe request.
* The beaconing feature on the AP is disabled.
* The AP periodically sends beacon frames containing the SSID.

**Explanation:** In passive mode, the wireless clients learn what networks and APs are available. The client learns this information from beacon frames, sent by the APs, that contain the WLAN SSID, supported standards, and security settings.

**19. What is a characteristic of a routed port that is configured on a Cisco switch?**

* It supports subinterfaces.
* It is associated with a single VLAN.
* It runs STP to prevent loops.
* It is assigned an IP address.

**Explanation:** Routed ports on a Cisco switch behave similarly to those on a router. They are configured with an IP address and forward Layer 3 packets. Unlike Layer 2 switch interfaces, routed ports do not support STP, nor do they support subinterfaces as routers do.

**20. What action does an Ethernet switch take when it receives a frame with an unknown Layer 2 source address?**

* It forwards the frame out all interfaces except the interface on which it was received.
* It forwards the frame to the default gateway.
* It records the source address in the address table of the switch.
* It drops the frame.

**Explanation:** When an Ethernet switch receives a frame with an unknown Layer 2 address, the switch records that address in the address table.

**22. Which routing protocol is used to exchange routes between internet service providers?**

* OSPF
* EIGRP
* ISIS
* BGP
* RIP

**Explanation:** BGP is a path vector routing protocol and it is used by internet service providers to exchange routes.

**23. What is the first step in the CSMA/CA process when a wireless client is attempting to communicate on the wireless network?**

* The client sends an RTS message to the AP.
* The client sends a test frame onto the channel.
* The client listens for traffic on the channel.
* The AP sends a CTS message to the client.

**Explanation:** When a wireless client is attempting to communicate on the network, it will first listen to the channel to be sure it is idle. Next, the client sends an RTS message to the AP to request dedicated access to the network. The AP will then send a CTS message granting access to the client. The client will then transmit data.

**24. What Wi-Fi management frame is regularly broadcast by APs to announce their presence?**

* authentication
* beacon
* probe
* association

**Explanation:** Beacon frames are broadcast periodically by the AP to advertise its wireless networks to potential clients. Probing, association, and authentication frames are only sent when a client is associating to the AP.

**25. What are the three parts of all Layer 2 frames? (Choose three.)**

* source and destination IP address
* payload
* sequence number
* frame check sequence
* time-to-live
* header

**Explanation:** Layer 2 frames have three components: the header, the payload, and a frame check sequence at the end.

**26. What is a function of SNMP?**

* synchronizes the time across all devices on the network
* captures packets entering and exiting the network interface card
* provides a message format for communication between network device managers and agents
* provides statistical analysis on packets flowing through a Cisco router or multilayer switch

**Explanation:** SNMP is an application layer protocol that allows administrators to manage devices on the network by providing a messaging format for communication between network device managers and agents.

**27. Which firewall feature is used to ensure that packets coming into a network are legitimate responses to requests initiated from internal hosts?**

* application filtering
* stateful packet inspection
* packet filtering
* URL filtering

**Explanation:** Stateful packet inspection on a firewall checks that incoming packets are actually legitimate responses to requests originating from hosts inside the network. Packet filtering can be used to permit or deny access to resources based on IP or MAC address. Application filtering can permit or deny access based on port number. URL filtering is used to permit or deny access based on URL or on keywords.

**28. In which memory location is the routing table of a router maintained?**

* ROM
* flash
* NVRAM
* RAM

**Explanation:** The routing table of a router is maintained in RAM, which is volatile memory. If a router loses power or is rebooted, the content of RAM is lost and the routing table must be rebuilt.

**29. Lightweight access points forward data between which two devices on the network? (Choose two.)**

* wireless router
* default gateway
* wireless LAN controller
* autonomous access point
* wireless client

**Explanation:** In a wireless deployment that is using lightweight access points (LWAPs), the LWAP forwards data between the wireless clients and the wireless LAN controller (WLC).

**30. A Cisco router is running IOS 15. What are the two routing table entry types that will be added when a network administrator brings an interface up and assigns an IP address to the interface? (Choose two.)**

* route that is manually entered by a network administrator
* local route interface
* route that is learned via OSPF
* directly connected interface
* route that is learned via EIGRP

**Explanation:** A local route interface routing table entry is found when a router runs IOS 15 or higher or if IPv6 routing is enabled. Whenever an interface is addressed and enabled (made active), a directly connected interface is automatically shown in the routing table.

**33. What is used on WLANs to avoid packet collisions?**

* SVIs
* STP
* CSMA/CA
* VLANs

**Explanation:** WLANs are half-duplex networks which means that only one client can transmit or receive at any given moment. WLANs use carrier sense multiple access with collision avoidance (CSMA/CA) to determine when to send data on the network to avoid packet collisions.

**34. What information within a data packet does a router use to make forwarding decisions?**

* the destination MAC address
* the destination host name
* the destination service requested
* the destination IP address

**Explanation:** A Layer 3 device like a router uses a Layer 3 destination IP address to make a forwarding decision.

**35. What is a characteristic of a hub?**

* operates at Layer 2
* regenerates signals received on one port out all other ports
* subdivides the network into collision domains
* uses CSMA/CA to avoid collisions

**Explanation:** A hub is a Layer 1 device that regenerates signals out all ports other than the ingress port. All ports on a hub belong to the same collision domain. Hubs use CSMA/CD to detect collisions on the network.

**1. Why is asset management a critical function of a growing organization against security threats?**

* It identifies the ever increasing attack surface to threats.
* It allows for a build of a comprehensive AUP.
* It serves to preserve an audit trail of all new purchases.
* It prevents theft of older assets that are decommissioned.

**Explanation:** Asset management is a critical component of a growing organization from a security aspect. Asset management consists of inventorying all assets, and then developing and implementing policies and procedures to protect them. As an organization grows, so does the attack surface in terms of security threats. Each of these assets can attract different threat actors who have different skill levels and motivations. Asset management can help mitigate these threats by inventorying the risks as the attack surface grows.

**2. In a defense-in-depth approach, which three options must be identified to effectively defend a network against attacks? (Choose three.)**

* total number of devices that attach to the wired and wireless network
* assets that need protection
* vulnerabilities in the system
* location of attacker or attackers
* past security breaches
* threats to assets

**Explanation:** In order to prepare for a security attack, IT security personnel must identify assets that need to be protected such as servers, routers, access points, and end devices. They must also identify potential threats to the assets and vulnerabilities in the system or design.

**3. What is the first line of defense when an organization is using a defense-in-depth approach to network security?**

* edge router
* firewall
* proxy server
* IPS

**Explanation:** A defense-in-depth approach uses layers of security measures starting at the network edge, working through the network, and finally ending at the network endpoints. Routers at the network edge are the first line of defense and forward traffic intended for the internal network to the firewall.

**4. What three goals does a BYOD security policy accomplish? (Choose three.)**

* identify all malware signatures and synchronize them across corporate databases
* identify which employees can bring their own devices
* identify safeguards to put in place if a device is compromised
* identify and prevent all heuristic virus signatures
* identify a list of websites that users are not permitted to access
* describe the rights to access and activities permitted to security personnel on the device

**Explanation:** A comprehensive BYOD policy should accomplish the following:  
Identification of which employees can bring their own devices  
Identification of which devices will be supported  
Identification of the level of access employees are granted when using personal devices  
Describe the rights to access and activities permitted to security personnel on the device  
Identification of which regulations must be adhered to when using employee devices  
Identification of safeguards to put in place if a device is compromised

**5. Which two options are security best practices that help mitigate BYOD risks? (Choose two.)**

* Use paint that reflects wireless signals and glass that prevents the signals from going outside the building.
* Keep the device OS and software updated.
* Only allow devices that have been approved by the corporate IT team.
* Only turn on Wi-Fi when using the wireless network.
* Decrease the wireless antenna gain level.
* Use wireless MAC address filtering.

**Explanation:** Many companies now support employees and visitors attaching and using wireless devices that connect to and use the corporate wireless network. This practice is known as a bring-your-own-device policy or BYOD. Commonly, BYOD security practices are included in the security policy. Some best practices that mitigate BYOD risks include the following:

Use unique passwords for each device and account.

Turn off Wi-Fi and Bluetooth connectivity when not being used. Only connect to trusted networks.

Keep the device OS and other software updated.

Backup any data stored on the device.

Subscribe to a device locator service with a remote wipe feature.

Provide antivirus software for approved BYODs.

Use Mobile Device Management (MDM) software that allows IT teams to track the device and implement security settings and software controls.

**6. What is the purpose of mobile device management (MDM) software?**

* It is used to create a security policy.
* It is used to implement security policies, setting, and software configurations on mobile devices.
* It is used to identify potential mobile device vulnerabilities.
* It is used by threat actors to penetrate the system.

**Explanation:** Mobile device management (MDM) software is used with mobile devices so that corporate IT personnel can track the devices, implement security settings, as well as control software configurations.

**7. What does the incident handling procedures security policy describe?**

* It describes how security incidents are handled.
* It describes the procedure for auditing the network after a cyberattack.
* It describes the procedure for mitigating cyberattacks.
* It describes how to prevent various cyberattacks.

**Explanation:** The incident handling procedures security policy describes how security incidents are handled.

**10. What is the primary purpose of the Forum of Incident Response and Security Teams (FIRST)?**

* to enable a variety of computer security incident response teams to collaborate, cooperate, and coordinate information sharing, incident prevention, and rapid reaction strategies
* to provide a security news portal that aggregates the latest breaking news pertaining to alerts, exploits, and vulnerabilities
* to offer 24×7 cyberthreat warnings and advisories, vulnerability identification, and mitigation and incident response
* to provide vendor neutral education products and career services to industry professionals worldwide

**Explanation:** The primary purpose of the Forum of Incident Response and Security Teams (FIRST) is to enable a variety of computer security incident response teams to collaborate, cooperate, and coordinate information sharing, incident prevention, and rapid reaction between the teams.

**11. What is the primary purpose of the Malware Information Sharing Platform (MISP) ?**

* to publish all informational materials on known and newly discovered cyberthreats
* to enable automated sharing of IOCs between people and machines using the STIX and other exports formats
* to provide a set of standardized schemata for specifying and capturing events and properties of network operations
* to exchange all the response mechanisms to known threats

**Explanation:** Malware Information Sharing Platform (MISP) is an open source platform that enables automated sharing of IOCs between people and machines using the STIX and other exports formats.

**12. Which statement describes Trusted Automated Exchange of Indicator Information (TAXII)?**

* It is a set of specifications for exchanging cyber threat information between organizations.
* It is a signature-less engine utilizing stateful attack analysis to detect zero-day threats.
* It is a dynamic database of real-time vulnerabilities.
* It is the specification for an application layer protocol that allows the communication of CTI over HTTPS.

**Explanation:** Trusted Automated Exchange of Indicator Information (TAXII) is the specification for an application layer protocol that allows the communication of CTI over HTTPS. TAXII is designed to support Structured Threat Information Expression (STIX).

**13. Which organization defines unique CVE Identifiers for publicly known information-security vulnerabilities that make it easier to share data?**

* Cisco Talos
* DHS
* FireEye
* MITRE

**Explanation:** The United States government sponsored the MITRE Corporation to create and maintain a catalog of known security threats called Common Vulnerabilities and Exposures (CVE). The CVE serves as a dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities.

**14. How does FireEye detect and prevent zero-day attacks?**

* by establishing an authentication parameter prior to any data exchange
* by addressing all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis
* by keeping a detailed analysis of all viruses and malware
* by only accepting encrypted data packets that validate against their configured hash values

**Explanation:** FireEye uses a three-pronged approach combining security intelligence, security expertise, and technology. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats.

**15. What is the primary function of the Center for Internet Security (CIS)?**

* to maintain a list of common vulnerabilities and exposures (CVE) used by security organizations
* to provide a security news portal that aggregates the latest breaking news pertaining to alerts, exploits, and vulnerabilities
* to offer 24×7 cyberthreat warnings and advisories, vulnerability identification, and mitigation and incident responses
* to provide vendor-neutral education products and career services to industry professionals worldwide

**Explanation:** CIS offers 24×7 cyberthreat warnings and advisories, vulnerability identification, and mitigation and incident responses to state, local, tribal, and territorial (SLTT) governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC).

**16. What is CybOX?**

* It is a specification for an application layer protocol that allows the communication of CTI over HTTPS.
* It is a set of standardized schemata for specifying, capturing, characterizing, and communicating events and properties of network operations.
* It enables the real-time exchange of cyberthreat indicators between the U.S. Federal Government and the private sector.
* It is a catalog of known security threats called Common Vulnerabilities and Exposures (CVE) for publicly known cybersecurity vulnerabilities.

**Explanation:** CybOX is a set of open standards that provide the specifications that aid in the automated exchange of cyberthreat intelligence information in a standardized format. It is a set of standardized schemata for specifying, capturing, characterizing, and communicating events and properties of network operations that support many cybersecurity functions.

**17. A web server administrator is configuring access settings to require users to authenticate first before accessing certain web pages. Which requirement of information security is addressed through the configuration?**

* availability
* integrity
* scalability
* confidentiality

**Explanation:** Confidentiality ensures that data is accessed only by authorized individuals. Authentication will help verify the identity of the individuals.

**18. When designing a prototype network for a new server farm, a network designer chooses to use redundant links to connect to the rest of the network. Which business goal will be addressed by this choice?**

* availability
* manageability
* security
* scalability

**Explanation:** Availability is one of the components of information security where authorized users must have uninterrupted access to important resources and data.

**19. When a security audit is performed at a company, the auditor reports that new users have access to network resources beyond their normal job roles. Additionally, users who move to different positions retain their prior permissions. What kind of violation is occurring?**

* leastprivilege
* network policy
* password
* audit

**Explanation:** Users should have access to information on a need to know basis. When a user moves from job role to job role, the same concept applies.

**20. Which component of the zero trust security model focuses on secure access when an API, a microservice, or a container is accessing a database within an application?**

* workflow
* workforce
* workload
* workplace

**Explanation:** The workload pillar focuses on applications that are running in the cloud, in data centers, and other virtualized environments that interact with one another. It focuses on secure access when an API, a microservice, or a container is accessing a database within an application.

**21. What is the purpose of the network security accounting function?**

* to determine which resources a user can access
* to provide challenge and response questions
* to keep track of the actions of a user
* to require users to prove who they are

**Explanation:** Authentication, authorization, and accounting are network services collectively known as AAA. Authentication requires users to prove who they are. Authorization determines which resources the user can access. Accounting keeps track of the actions of the user.

**22. Which term describes the ability of a web server to keep a log of the users who access the server, as well as the length of time they use it?**

* authentication
* accounting
* assigning permissions
* authorization

**Explanation:** Accounting records what users do and when they do it, including what is accessed, the amount of time the resource is accessed, and any changes that were made. Accounting keeps track of how network resources are used.

**24. What are two characteristics of the RADIUS protocol? (Choose two.)**

* encryption of the entire body of the packet
* encryption of the password only
* the use of UDP ports for authentication and accounting
* the separation of the authentication and authorization processes
* the use of TCP port 49

**Explanation:** RADIUS is an open-standard AAA protocol using UDP port 1645 or 1812 for authentication and UDP port 1646 or 1813 for accounting. It combines authentication and authorization into one process.

**25. Which AAA component can be established using token cards?**

* accounting
* authorization
* authentication
* auditing

**Explanation:** The authentication component of AAA is established using username and password combinations, challenge and response questions, and token cards. The authorization component of AAA determines which resources the user can access and which operations the user is allowed to perform. The accounting and auditing component of AAA keeps track of how network resources are used.

**26. What is a characteristic of the security artichoke, defense-in-depth approach?**

* Threat actors can easily compromise all layers safeguarding the data or systems.
* Threat actors no longer have to peel away each layer before reaching the target data or system.
* Threat actors can no longer penetrate any layers safeguarding the data or system.
* Each layer has to be penetrated before the threat actor can reach the target data or system.

**Explanation:** In the security artichoke, defense-in-depth approach not every layer needs to be penetrated by the threat actor in order to get to the data or systems. Each layer provides a layer of protection while simultaneously providing a path to attack.

**27. What is a characteristic of a layered defense-in-depth security approach?**

* Three or more devices are used.
* Routers are replaced with firewalls.
* One safeguard failure does not affect the effectiveness of other safeguards.
* When one device fails, another one takes over.

**Explanation:** When a layered defense-in-depth security approach is used, layers of security are placed through the organization-at the edge, within the network, and on endpoints. The layers work together to create the security architecture. In this environment, a failure of one safeguard does not affect the effectiveness of other safeguards.

**28. What is the benefit of a defense-in-depth approach?**

* All network vulnerabilities are mitigated.
* The need for firewalls is eliminated.
* Only a single layer of security at the network core is required.
* The effectiveness of other security measures is not impacted when a security mechanism fails.

**Explanation:** The benefit of the defense-in-depth approach is that network defenses are implemented in layers so that failure of any single security mechanism does not impact other secuirty measures.

**30. What is the principle behind the nondiscretionary access control model?**

* It applies the strictest access control possible.
* It allows access decisions to be based on roles and responsibilities of a user within the organization.
* It allows users to control access to their data as owners of that data.
* It allows access based on attributes of the object be to accessed.

**Explanation:** The nondiscretionary access control model used the roles and responsibilities of the user as the basis for access decisions.

**31. Which type of access control applies the strictest access control and is commonly used in military or mission critical applications?**

* Non-discretionary access control
* discretionary access control (DAC)
* attribute-based access control (ABAC)
* mandatory access control (MAC)

**Explanation:** **Access control models are used to define the access controls implemented to protect corporate IT resources. The different types of access control models are as follows:**

Mandatory access control (MAC) – The strictest access control that is typically used in military or mission critical applications.

Discretionary access control (DAC) – Allows users to control access to their data as owners of that data. Access control lists (ACLs) or other security measures may be used to specify who else may have access to the information.

Non-discretionary access control – Also known as role-based access control (RBAC). Allows access based on the role and responsibilities of the individual within the organization.

Attribute-based access control (ABAC) – Allows access based on the attributes of the resource to be accessed, the user accessing the resource, and the environmental factors such as the time of day.

**32. Passwords, passphrases, and PINs are examples of which security term?**

* identification
* access
* authentication
* authorization

**Explanation:** Authentication methods are used to strengthen access control systems. It is important to understand the available authentication methods.

**33. How does AIS address a newly discovered threat?**

* by creating response strategies against the new threat
* by advising the U.S. Federal Government to publish internal response strategies
* by enabling real-time exchange of cyberthreat indicators with U.S. Federal Government and the private sector
* by mitigating the attack with active response defense mechanisms

**Explanation:** AIS responds to a new threat as soon as it is recognized by immediately sharing it with U.S. Federal Government and the private sector to help them protect their networks against that particular threat.

**1. Which type of attack does the use of HMACs protect against?**

* brute force
* DDoS
* DoS
* man-in-the-middle

**Explanation:** Because only the sender and receiver know the secret key, only parties that have access to that key can compute the digest of an HMAC function. This defeats man-in-the-middle attacks and provides authentication of where the data originated.​

**2. Which objective of secure communications is achieved by encrypting data?**

* confidentiality
* integrity
* availability
* authentication

**Explanation:** When data is encrypted, it is scrambled to keep the data private and confidential so that only authorized recipients can read the message. A hash function is another way of providing confidentiality.

**3. Which two statements correctly describe certificate classes used in the PKI? (Choose two.)**

* A class 4 certificate is for online business transactions between companies.
* A class 0 certificate is more trusted than a class 1 certificate.
* A class 0 certificate is for testing purposes.
* The lower the class number, the more trusted the certificate.
* A class 5 certificate is for users with a focus on verification of email.

**Explanation:** A digital certificate class is identified by a number. The higher the number, the more trusted the certificate. The classes include the following:  
Class 0 is for testing purposes in which no checks have been performed.  
Class 1 is for individuals with a focus on verification of email.  
Class 2 is for organizations for which proof of identity is required.  
Class 3 is for servers and software signing for which independent verification and checking of identity and authority is done by the issuing certificate authority.  
Class 4 is for online business transactions between companies.  
Class 5 is for private organizations or governmental security.

**4. A customer purchases an item from an e-commerce site. The e-commerce site must maintain proof that the data exchange took place between the site and the customer. Which feature of digital signatures is required?**

* nonrepudiation of the transaction
* integrity of digitally signed data
* authenticity of digitally signed data
* confidentiality of the public key

**Explanation:** Digital signatures provide three basic security services:  
Authenticity of digitally signed data – Digital signatures authenticate a source, proving that a certain party has seen and signed the data in question.  
Integrity of digitally signed data – Digital signatures guarantee that the data has not changed from the time it was signed.  
Nonrepudiation of the transaction – The recipient can take the data to a third party, and the third party accepts the digital signature as a proof that this data exchange did take place. The signing party cannot repudiate that it has signed the data.

**5. What is the purpose of a digital certificate?**

* It provides proof that data has a traditional signature attached.
* It guarantees that a website has not been hacked.
* It ensures that the person who is gaining access to a network device is authorized.
* It authenticates a website and establishes a secure connection to exchange confidential data.

**Explanation:** Digital signatures commonly use digital certificates that are used to verify the identity of the originator in order to authenticate a vendor website and establish an encrypted connection to exchange confidential data. One such example is when a person logs into a financial institution from a web browser.

**6. In a hierarchical CA topology, where can a subordinate CA obtain a certificate for itself?**

* from the root CA or another subordinate CA at a higher level
* from the root CA or another subordinate CA at the same level
* from the root CA or from self-generation
* from the root CA only
* from the root CA or another subordinate CA anywhere in the tree

**Explanation:** In a hierarchical CA topology, CAs can issue certificates to end users and to subordinate CAs, which in turn issue their certificates to end users, other lower level CAs, or both. In this way, a tree of CAs and end users is built in which every CA can issue certificates to lower level CAs and end users. Only the root CA can issue a self-signing certificate in a hierarchical CA topology.

**7. What is the purpose for using digital signatures for code signing?**

* to establish an encrypted connection to exchange confidential data with a vendor website
* to verify the integrity of executable files downloaded from a vendor website
* to authenticate the identity of the system with a vendor website
* to generate a virtual ID

**Explanation:** Code signing is used to verify the integrity of executable files downloaded from a vendor website. Code signing uses digital certificates to authenticate and verify the identity of a website.

**8. What technology has a function of using trusted third-party protocols to issue credentials that are accepted as an authoritative identity?**

* digital signatures
* hashing algorithms
* PKI certificates
* symmetric keys

**Explanation:** Digital certificates are used to prove the authenticity and integrity of PKI certificates, but a PKI Certificate Authority is a trusted third-party entity that issues PKI certificates. PKI certificates are public information and are used to provide authenticity, confidentiality, integrity, and nonrepudiation services that can scale to large requirements.

**9. In addressing a risk that has low potential impact and relatively high cost of mitigation or reduction, which strategy will accept the risk and its consequences?**

* risk avoidance
* risk reduction
* risk retention
* risk sharing

**Explanation:** There are four potential strategies for responding to risks that have been identified:  
**Risk avoidance** – Stop performing the activities that create risk.  
**Risk reduction** – Decrease the risk by taking measures to reduce vulnerability.  
**Risk sharing** – Shift some of the risk to other parties.  
**Risk retention** – Accept the risk and its consequences.

**10. Which two classes of metrics are included in the CVSS Base Metric Group? (Choose two.)**

* Confidentiality Requirement
* Modified Base
* Exploit Code Maturity
* Exploitability
* Impact metrics

**Explanation:** The Base Metric Group of CVSS represents the characteristics of a vulnerability that are constant over time and across contexts. It contains two classes of metrics, Exploitability and Impact.

**12. A cybersecurity analyst is performing a CVSS assessment on an attack where a web link was sent to several employees. Once clicked, an internal attack was launched. Which CVSS Base Metric Group Exploitability metric is used to document that the user had to click on the link in order for the attack to occur?**

* scope
* integrity requirement
* availability requirement
* user interaction

**Explanation:** The CVSS Base Metric Group has the following metrics: attack vector, attack complexity, privileges required, user interaction, and scope. The user interaction metric expresses the presence or absence of the requirement for user interaction in order for an exploit to be successful.

**13. In network security assessments, which type of test employs software to scan internal networks and Internet facing servers for various types of vulnerabilities?**

* vulnerability assessment
* risk analysis
* strength of network security testing
* penetration testing

**Explanation:** In vulnerability assessment, security analysts use software to scan internal networks and Internet facing servers for various types of vulnerabilities. Tools for vulnerability assessment include the open source OpenVAS platform, Microsoft Baseline Security Analyzer, Nessus, Qualys, and Fireeye Mandiant services.

**14. What are the three outcomes of the NIST Cybersecurity Framework identify core function? (Choose three.)**

* information protection process and procedures
* governance
* mitigation
* risk assessment
* asset management
* recovery planning

**Explanation:** The identify core function is concerned with the development of organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. It involves the following outcomes:  
Asset management  
Business environment  
Governance  
Risk assessment  
Risk management strategy

**15. When a server profile for an organization is being established, which element describes the TCP and UDP daemons and ports that are allowed to be open on the server?**

* critical asset address space
* service accounts
* software environment
* listening ports

**Explanation:** A server profile will often contain the following:  
Listening ports – the TCP and UDP daemons and ports that are allowed to be open on the server  
User accounts – the parameters defining user access and behavior  
Service accounts – the definitions of the type of service that an application is allowed to run on a server  
Software environment – the tasks, processes, and applications that are permitted to run on the server

**16. What is an action that should be taken in the discovery step of the vulnerability management life cycle?**

* documenting the security plan
* assigning business value to assets
* developing a network baseline
* determining a risk profile

**Explanation:** During the discovery step of the vulnerability management life cycle, an inventory of all network assets is made. A network baseline is developed, and security vulnerabilities are identified.

**17. In what order are the steps in the vulnerability management life cycle conducted?**

* discover, assess, prioritize assets, report, remediate, verify
* discover, prioritize assets, assess, remediate, report, verify
* discover, prioritize assets, assess, remediate, verify, report
* discover, prioritize assets, assess, report, remediate, verify

**Explanation:** There are six steps in the vulnerability management life cycle:

* Discover
* Prioritize assets
* Assess
* Report
* Remediate
* Verify

**17. What does the telemetry function provide in host-based security software?**

* It updates the heuristic antivirus signature database.
* It blocks the passage of zero-day attacks.
* It enables updates of malware signatures.
* It enables host-based security programs to have comprehensive logging functions.

**Explanation:** The telemetry function allows for robust logging functionality that is essential to cybersecurity operations. Some host-based security programs will submit logs to a central location for analysis.

**19. A security professional is making recommendations to a company for enhancing endpoint security. Which security endpoint technology would be recommended as an agent-based system to protect hosts against malware?**

* IPS
* HIDS
* blacklisting
* baselining

**Explanation:** A host-based intrusion detection systems (HIDS) is a comprehensive security application that provides antimalware applications, a firewall, and monitoring and reporting.

**20. What is a feature of distributed firewalls?**

* They all use an open sharing standard platform.
* They use only TCP wrappers to configure rule-based access control and logging systems.
* They use only iptables to configure network rules.
* They combine the feature of host-based firewalls with centralized management.

**Explanation:** Distributed firewalls combine features of host-based firewalls with centralized management, which pushes rules to the hosts.

**21. An administrator suspects polymorphic malware has successfully entered the network past the HIDS system perimeter. The polymorphic malware is, however, successfully identified and isolated. What must the administrator do to create signatures to prevent the file from entering the network again?**

* Execute the polymorphic file in the Cisco Threat Grid Glovebox.
* Run the Cisco Talos security intelligence service.
* Use Cisco AMP to track the trajectory of a file through the network.
* Run a baseline to establish an accepted amount of risk, and the environmental components that contribute to the risk level of the polymorphic malware.

**Explanation:** The isolated polymorphic malware file should be run in a sandbox environment like Cisco Threat Grid Glovebox, and the activities of the file documented by the system. This information can then be used to create signatures to prevent the file from entering the network again.

**22. On a Windows host, which tool can be used to create and maintain blacklists and whitelists?**

* Local Users and Groups
* Group Policy Editor
* Task Manager
* Computer Management

**Explanation:** In Windows, blacklisting and whitelisting settings can be managed through the Group Policy Editor.

**23. What is blacklisting?**

* This is an application list that can dictate which user applications are not permitted to run on a computer.
* This is a user list to prevent blacklisted users from accessing a computer.
* This is a network process list to stop a listed process from running on a computer.
* This is a Heuristics-based list to prevent a process from running on a computer.

**Explanation:** Blacklisting can dictate which user applications are not permitted to run on a computer. Windows Local Group Policy Editor can be used to add entries for blacklisted applications.

**24. Which technology is used by Cisco Advanced Malware Protection (AMP) in defending and protecting against known and emerging threats?**

* network admission control
* network profiling
* website filtering and blacklisting
* threat intelligence

**Explanation:** Cisco AMP uses threat intelligence along with known file signatures to identify and block policy-violating file types and exploitations.

**25. Which technique could be used by security personnel to analyze a suspicious file in a safe environment?**

* sandboxing
* baselining
* whitelisting
* blacklisting

**Explanation:** Sandboxing allows suspicious files to be executed and analyzed in a safe environment. There are free public sandboxes that allow for malware samples to be uploaded or submitted and analyzed.

**26. Which statement describes the term iptables?**

* It is a file used by a DHCP server to store current active IP addresses.
* It is a rule-based firewall application in Linux.
* It is a DHCP application in Windows.
* It is a DNS daemon in Linux.

**Explanation:** Iptables is an application that allows Linux system administrators to configure network access rules.

**27. What is the difference between an HIDS and a firewall?**

* An HIDS works like an IPS, whereas a firewall just monitors traffic.
* An HIDS monitors operating systems on host computers and processes file system activity. Firewalls allow or deny traffic between the computer and other systems.
* A firewall performs packet filtering and therefore is limited in effectiveness, whereas an HIDS blocks intrusions.
* An HIDS blocks intrusions, whereas a firewall filters them.
* A firewall allows and denies traffic based on rules and an HIDS monitors network traffic.

**Explanation:** In order to monitor local activity an HIDS should be implemented. Network activity monitors are concerned with traffic and not operating system activity.

**28. Which statement describes the Cisco Threat Grid Glovebox?**

* It is a network-based IDS/IPS.
* It is a host-based intrusion detection system (HIDS) solution to fight against malware.
* It is a sandbox product for analyzing malware behaviors.
* It is a firewall appliance.

**Explanation:** Cisco ThreatGrid Glovebox is a sandbox product for analyzing malware behaviors.

**29. Which statement describes the policy-based intrusion detection approach?**

* It compares the signatures of incoming traffic to a known intrusion database.
* It compares the operations of a host against well-defined security rules.
* It compares the antimalware definitions to a central repository for the latest updates.
* It compares the behaviors of a host to an established baseline to identify potential intrusion.

**Explanation:** With the anomaly-based intrusion detection approach, a set of rules or policies are applied to a host. Violation of these policies is interpreted to be the result of a potential intrusion.

**30. What is the purpose of the DH algorithm?**

* to provide nonrepudiation support
* to generate a shared secret between two hosts that have not communicated before
* to encrypt data traffic after a VPN is established
* to support email data confidentiality

**Explanation:** DH is an asymmetric mathematical algorithm that allows two computers to generate an identical shared secret, without having communicated before. Asymmetric key systems are extremely slow for any sort of bulk encryption. It is common to encrypt the bulk of the traffic using a symmetric algorithm such as DES, 3DES, or AES, and use the DH algorithm to create keys that will be used by the symmetric encryption algorithm.

**31. What is a difference between symmetric and asymmetric encryption algorithms?**

* Symmetric encryption algorithms are used to authenticate secure communications. Asymmetric encryption algorithms are used to repudiate messages.
* Symmetric encryption algorithms are used to encrypt data. Asymmetric encryption algorithms are used to decrypt data.
* Symmetric encryption algorithms use pre-shared keys. Asymmetric encryption algorithms use different keys to encrypt and decrypt data.
* Symmetric algorithms are typically hundreds to thousands of times slower than asymmetric algorithms.

**Explanation:** Asymmetric algorithms can use very long key lengths in order to avoid being hacked. This results in the use of significantly increased resources and time compared to symmetric algorithms.

**32. A company implements a security policy that ensures that a file sent from the headquarters office to the branch office can only be opened with a predetermined code. This code is changed every day. Which two algorithms can be used to achieve this task? (Choose two.)**

* HMAC
* MD5
* 3DES
* SHA-1
* AES

**Explanation:** The task to ensure that only authorized personnel can open a file is data confidentiality, which can be implemented with encryption. AES and 3DES are two encryption algorithms. HMAC can be used for ensuring origin authentication. MD5 and SHA-1 can be used to ensure data integrity.

**33. Which security management plan specifies a component that involves tracking the location and configuration of networked devices and software across an enterprise?**

* asset management
* patch management
* vulnerability management
* risk management

**Explanation:** Asset management involves tracking the location and configuration of networked devices and software across an enterprise.

**34. In addressing an identified risk, which strategy aims to stop performing the activities that create risk?**

* risk retention
* risk avoidance
* risk sharing
* risk reduction

**Explanation:** There are four potential strategies for responding to risks that have been identified:

* Risk avoidance – Stop performing the activities that create risk.
* Risk reduction – Decrease the risk by taking measures to reduce vulnerability.
* Risk sharing – Shift some of the risk to other parties.
* Risk retention – Accept the risk and its consequences.

**35. A company is developing a security policy for secure communication. In the exchange of critical messages between a headquarters office and a branch office, a hash value should only be recalculated with a predetermined code, thus ensuring the validity of data source. Which aspect of secure communications is addressed?**

* data integrity
* data confidentiality
* non-repudiation
* origin authentication

**Explanation:** **Secure communications consists of four elements:**  
**Data confidentiality** – guarantees that only authorized users can read the message  
**Data integrity** – guarantees that the message was not altered  
**Origin authentication** – guarantees that the message is not a forgery and does actually come from whom it states  
**Data nonrepudiation** – guarantees that the sender cannot repudiate, or refute, the validity of a message sent

**37. Which three security services are provided by digital signatures? (Choose three.)**

* provides nonrepudiation using HMAC functions
* guarantees data has not changed in transit
* provides data encryption
* authenticates the source
* provides confidentiality of digitally signed data
* authenticates the destination

**Explanation:** Digital signatures are a mathematical technique used to provide three basic security services. Digital signatures have specific properties that enable entity authentication and data integrity. In addition, digital signatures provide nonrepudiation of the transaction. In other words, the digital signature serves as legal proof that the data exchange did take place.

**1. Which ICMP message type should be stopped inbound?**

* source quench
* echo-reply
* echo
* unreachable

**Explanation:** The echo ICMP packet should not be allowed inbound on an interface. The echo-reply should be allowed so that when an internal device pings an external device, the reply is allowed to return.

**2. How can IMAP be a security threat to a company?**

* Someone inadvertently clicks on a hidden iFrame.
* Encrypted data is decrypted.
* An email can be used to bring malware to a host.
* It can be used to encode stolen data and send to a threat actor.

**Explanation:** IMAP, SMTP, and POP3 are email protocols. SMTP is used to send data from a host to a server or to send data between servers. IMAP and POP3 are used to download email messages and can be responsible for bringing malware to the receiving host.

**3. Which two technologies are primarily used on peer-to-peer networks? (Choose two.)**

* Bitcoin
* BitTorrent
* Wireshark
* Darknet
* Snort

**Explanation:** Bitcoin is used to share a distributed database or ledger. BitTorrent is used for file sharing.

**4. Which protocol is exploited by cybercriminals who create malicious iFrames?**

* HTTP
* ARP
* DHCP
* DNS

**Explanation:** An HTML element known as an inline frame or iFrame allows the browser to load a different web page from another source.

**5. Which method is used by some malware to transfer files from infected hosts to a threat actor host?**

* UDP infiltration
* ICMP tunneling
* HTTPS traffic encryption
* iFrame injection

**Explanation:** ICMP traffic from inside the company is also a threat. Some varieties of malware use ICMP packets to transfer files from infected hosts to threat actors via ICMP tunneling.

**6. Why does HTTPS technology add complexity to network security monitoring?**

* HTTPS dynamically changes the port number on the web server.
* HTTPS uses tunneling technology for confidentiality.
* HTTPS hides the true source IP address using NAT/PAT.
* HTTPS conceals data traffic through end-to-end encryption.

**Explanation:** With HTTPS, a symmetric key is generated by the client after the client verifies the trustworthiness of the web server. The symmetric key is encrypted with the public key of the web server and then sent to the web server. The web server uses its public key to decrypt the key. The key is then used to encrypt the data requested by the client and the data is sent to the client. This end-to-end encryption complicates inline network security monitoring. The HTTPS port number, typically 443, is configured statically on the web server.

**7. Which approach is intended to prevent exploits that target syslog?**

* Use a Linux-based server.
* Use syslog-ng.
* Create an ACL that permits only TCP traffic to the syslog server.
* Use a VPN between a syslog client and the syslog server.

**Explanation:** Hackers may try to block clients from sending data to the syslog server, manipulate or erase logged data, or manipulate the software used to transmit messages between the clients and the server. Syslog-ng is the next generation of syslog and it contains improvements to prevent some of the exploits.

**8. Which type of attack is carried out by threat actors against a network to determine which IP addresses, protocols, and ports are allowed by ACLs?**

* phishing
* denial of service
* reconnaissance
* social engineering

**Explanation:** Packet filtering ACLs use rules to filter incoming and outgoing traffic. These rules are defined by specifying IP addresses, port numbers, and protocols to be matched. Threat actors can use a reconnaissance attack involving port scanning or penetration testing to determine which IP addresses, protocols, and ports are allowed by ACLs.

**9. Which two application layer protocols manage the exchange of messages between a client with a web browser and a remote web server? (Choose two.)**

* HTTP
* HTTPS
* DNS
* DHCP
* HTML

**Explanation:** Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS) are two application layer protocols that manage the content requests from clients and the responses from the web server. HTML (Hypertext Mark-up Language) is the encoding language that describes the content and display features of a web page. DNS is for domain name to IP address resolution. DHCP manages and provides dynamic IP configurations to clients.

**10. What is Tor?**

* a rule created in order to match a signature of a known exploit
* a software platform and network of P2P hosts that function as Internet routers
* a way to share processors between network devices across the Internet
* a type of Instant Messaging (IM) software used on the darknet

**Explanation:** A special browser is used to access the Tor network. This browser allows a user to browse the Internet anonymously.

**11. Which protocol is a name resolution protocol often used by malware to communicate with command-and-control (CnC) servers?**

* IMAP
* DNS
* HTTPS
* ICMP

**Explanation:** Domain Name Service (DNS) is used to convert domain names into IP addresses. Some organizations have less stringent policies in place to protect against DNS-based threats than they have in place for other exploits.

**12. Which technique is necessary to ensure a private transfer of data using a VPN?**

* authorization
* scalability
* encryption
* virtualization

**Explanation:** Confidential and secure transfers of data with VPNs require data encryption.

**13. Which technology would be used to create the server logs generated by network devices and reviewed by an entry level network person who works the night shift at a data center?**

* syslog
* NAT
* ACL
* VPN

**Explanation:** Syslog is a daemon or service run on a server that accepts messages sent by network devices. These logs are frequently examined to detect inconsistencies and issues within the network.

**14. Which function is provided by the Sguil application?**

* It reports conversations between hosts on the network.
* It makes Snort-generated alerts readable and searchable.
* It detects potential network intrusions.
* It prevents malware from attacking a host.

**Explanation:** Applications such as Snorby and Sguil can be used to read and search alert messages generated by NIDS/NIPS.

**15. Which statement describes a Cisco Web Security Appliance (WSA)?**

* It protects a web server by preventing security threats from accessing the server.
* It provides high performance web services.
* It acts as an SSL-based VPN server for an enterprise.
* It functions as a web proxy.

**Explanation:** Cisco Web Security Appliance (WSA) devices provide a wide range of functionalities for security monitoring. WSA effectively acts as a web proxy. It logs all inbound and outbound transaction information for HTTP traffic.

**16. Which statement describes session data in security logs?**

* It can be used to describe or predict network behavior.
* It shows the result of network sessions.
* It is a record of a conversation between network hosts.
* It reports detailed network activities between network hosts.

**Explanation:** Session data is a record of a conversation between two network endpoints.

**17. Which two options are network security monitoring approaches that use advanced analytic techniques to analyze network telemetry data? (Choose two.)**

* NBAD
* Sguil
* NetFlow
* IPFIX
* Snorby
* NBA

**Explanation:** Network behavior analysis (NBA) and network behavior anomaly detection (NBAD) are approaches to network security monitoring that use advanced analytical techniques to analyze NetFlow or IPFIX network telemetry data.

**18. How does a web proxy device provide data loss prevention (DLP) for an enterprise?**

* by functioning as a firewall
* by inspecting incoming traffic for potential exploits
* by scanning and logging outgoing traffic
* by checking the reputation of external web servers

**Explanation:** A web proxy device can inspect outgoing traffic as means of data loss prevention (DLP). DLP involves scanning outgoing traffic to detect whether the data that is leaving the enterprise network contains sensitive, confidential, or secret information.

**19. Which information can be provided by the Cisco NetFlow utility?**

* security and user account restrictions
* IDS and IPS capabilities
* peak usage times and traffic routing
* source and destination UDP port mapping

**Explanation:** NetFlow efficiently provides an important set of services for IP applications including network traffic accounting, usage-based network billing, network planning, security, denial of service monitoring capabilities, and network monitoring. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing.

**20. Which statement describes statistical data in network security monitoring processes?**

* It is created through an analysis of other forms of network data.
* It contains conversations between network hosts.
* It shows the results of network activities between network hosts.
* It lists each alert message along with statistical information.

**Explanation:** Like session data, statistical data is about network traffic. Statistical data is created through the analysis of other forms of network data

**22. Which two tools have a GUI interface and can be used to view and analyze full packet captures? (Choose two.)**

* nfdump
* Wireshark
* Cisco Prime Network Analysis Module
* tcpdump
* Splunk

**Explanation:** The Network Analysis Module of the Cisco Prime Infrastructure system and Wireshark have GUI interfaces and can display full packet captures. The tcpdump tool is a command-line packet analyzer.

**23. Which Windows log contains information about installations of software, including Windows updates?**

* system logs
* application logs
* setup logs
* security logs

**Explanation:** On a Windows host, setup logs record information about the installation of software, including Windows updates.

**25. Which Cisco appliance can be used to filter network traffic contents to report and deny traffic based on the web server reputation?**

* WSA
* AVC
* ASA
* ESA

**Explanation:** The Cisco Web Security Appliance (WSA) acts as a web proxy for an enterprise network. WSA can provide many types of logs related to web traffic security including ACL decision logs, malware scan logs, and web reputation filtering logs. The Cisco Email Security Appliance (ESA) is a tool to monitor most aspects of email delivery, system functioning, antivirus, antispam operations, afnd blacklist and whitelist decisions. The Cisco ASA is a firewall appliance. The Cisco Application Visibility and Control (AVC) system combines multiple technologies to recognize, analyze, and control over 1000 applications.

**26. Which technique would a threat actor use to disguise traces of an ongoing exploit?**

* Create an invisible iFrame on a web page.
* Corrupt time information by attacking the NTP infrastructure.
* Encapsulate other protocols within DNS to evade security measures.
* Use SSL to encapsulate malware.

**Explanation:** The Network Time Protocol (NTP) uses a hierarchy of time sources to provide a consistent time clock to network infrastructure devices. Threat actors may attack the NTP infrastructure in order to corrupt time information that is used in network logs.

**27. A system administrator runs a file scan utility on a Windows PC and notices a file lsass.exe in the Program Files directory. What should the administrator do?**

* Delete the file because it is probably malware.
* Move it to Program Files (x86) because it is a 32bit application.
* Uninstall the lsass application because it is a legacy application and no longer required by Windows.
* Open the Task Manager, right-click on the lsass process and choose End Task .

**Explanation:** On Windows computers, security logging and security policies enforcement are carried out by the Local Security Authority Subsystem Service (LSASS), running as lsass.exe. It should be running from the Windows\System32 directory. If a file with this name, or a camouflaged name, such as 1sass.exe, is running or running from another directory, it could be malware.

**28. Refer to the exhibit. A network administrator is viewing some output on the Netflow collector. What can be determined from the output of the traffic flow shown?**

Graphical user interface

Description automatically generated

* This is a UDP DNS request to a DNS server.
* This is a UDP DNS response to a client machine.
* This is a TCP DNS request to a DNS server.
* This is a TCP DNS response to a client machine.

**Explanation:** The traffic flow shown has a source port of 53 and a destination port of 1025. Port 53 is used for DNS and because the source port is 53, this traffic is responding to a client machine from a DNS server. The IP PROTOCOL is 17 and specifies that UDP is being used and the TCP flag is set to 0.

**29 In a Cisco AVC system, in which module is NetFlow deployed?**

* Management and Reporting
* Control
* Application Recognition
* Metrics Collection

**Explanation:** NetFlow technology is deployed in the Metrics Collection module of a Cisco AVC system to collect network flow metrics and to export to management tools.

**30. What does it indicate if the timestamp in the HEADER section of a syslog message is preceded by a period or asterisk symbol?**

* There is a problem associated with NTP.
* The timestamp represents the round trip duration value.
* The syslog message should be treated with high priority.
* The syslog message indicates the time an email is received.

**Explanation:** The HEADER section of the message contains the timestamp. If the timestamp is preceded by the period (.) or asterisk (\*) symbols, a problem is indicated with NTP.

DFIR

**2. What two shared sources of information are included within the MITRE ATT&CK framework? (Choose two.)**

* collection of digital evidence from most volatile evidence to least volatile
* attacker tactics, techniques, and procedures
* details about the handling of evidence including times, places, and personnel involved
* eyewitness evidence from someone who directly observed criminal behavior
* mapping the steps in an attack to a matrix of generalized tactics

**Explanation:** The MITRE Framework uses stored information on attacker tactics, techniques, and procedures (TTP) as part of threat defense and attack attribution. This is done by mapping the steps in an attack to a matrix of generalized tactics and describing the techniques that are used in each tactic. These sources of information create models that assist in the ability to attribute a threat.

**3. What information is gathered by the CSIRT when determining the scope of a security incident?**

* the networks, systems, and applications affected by an incident
* the amount of time and resources needed to handle an incident
* the strategies and procedures used for incident containment
* the processes used to preserve evidence

**Explanation:** The scoping activity performed by the CSIRT after an incident determines which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring.

**4. According to NIST standards, which incident response stakeholder is responsible for coordinating an incident response with other stakeholders to minimize the damage of an incident?**

* human resources
* legal department
* management
* IT support

**Explanation:** The management team creates the policies, designs the budget, and is in charge of staffing all departments. Management is also responsible for coordinating the incident response with other stakeholders and minimizing the damage of an incident.

**5. According to NIST, which step in the digital forensics process involves drawing conclusions from data?**

* reporting
* collection
* examination
* analysis

**Explanation:** NIST describes the digital forensics process as involving the following four steps:  
Collection – the identification of potential sources of forensic data and acquisition, handling, and storage of that data.  
Examination – assessing and extracting relevant information from the collected data. This may involve decompression or decryption of the data.  
Analysis – drawing conclusions from the data. Salient features, such as people, places, times, events, and so on should be documented.  
Reporting – preparing and presenting information that resulted from the analysis. Reporting should be impartial and alternative explanations should be offered if appropriate.

**6. A cybersecurity analyst has been called to a crime scene that contains several technology items including a computer. Which technique will be used so that the information found on the computer can be used in court?**

* Tor
* rootkit
* unaltered disk image
* log collection

**Explanation:** A normal file copy does not recover all data on a storage device so an unaltered disk image is commonly made. An unaltered disk image preserves the original evidence, thus preventing inadvertent alteration during the discovery phase. It also allows recreation of the original evidence.

**7. In which phase of the NIST incident response life cycle is evidence gathered that can assist subsequent investigations by authorities?**

* postincident activities
* detection and analysis
* preparation
* containment, eradication, and recovery

**Explanation:** NIST defines four phases in the incident response process life cycle. It is in the containment, eradication, and recovery phase that evidence is gathered to resolve an incident and to help with subsequent investigations.

**8. When dealing with security threats and using the Cyber Kill Chain model, which two approaches can an organization use to block a potential back door creation? (Choose two.)**

* Audit endpoints to discover abnormal file creations.
* Establish an incident response playbook.
* Consolidate the number of Internet points of presence.
* Conduct damage assessment.
* Use HIPS to alert or place a block on common installation paths.

**Explanation:** In the installation phase of the Cyber Kill Chain, the threat actor establishes a back door into the system to allow for continued access to the target. Among other measures, using HIPS to alert or block on common installation paths and auditing endpoints to discover abnormal file creations can help block a potential back door creation.

**9. What is defined in the SOP of a computer security incident response capability (CSIRC)?**

* the details on how an incident is handled
* the procedures that are followed during an incident response
* the metrics for measuring incident response capabilities
* the roadmap for increasing incident response capabilities

**Explanation:** A CSIRC will include standard operating procedures (SOPs) that are followed during an incident response. Procedures include following technical processes, filling out forms, and following checklists.

**10. How does an application program interact with the operating system?**

* sending files
* accessing BIOS or UEFI
* making API calls
* using processes

**Explanation:** Application programs interact with an operating system through system calls to the OS application programming interface (API). These system calls allow access to many aspects of system operation such as software process control, file management, device management, and network access.

**11. Which tool included in the Security Onion provides a visual interface to NSM data?**

* Curator
* Beats
* Squert
* OSSEC

**Explanation:** Dashboards provide a combination of data and visualizations designed to improve the access of individuals to large amounts of information. Kibana includes the capability of designing custom dashboards. In addition, other tools that are included in Security Onion, such as Squert, provide a visual interface to NSM data.

**12. Which tool included in the Security Onion includes the capability of designing custom dashboards?**

* Sguil
* Kibana
* Squert
* OSSEC

**Explanation:** Dashboards are usually interactive and provide a combination of data and visualizations designed to improve the access of individuals to large amounts of information. Kibana includes the capability of designing custom dashboards.

**13. How is the hash value of files useful in network security investigations?**

* It is used to decode files.
* It helps identify malware signatures.
* It verifies confidentiality of files.
* It is used as a key for encryption.

**Explanation:** When ELSA is used to investigate downloaded files, the hash value of each file is created and stored with other information about the file. If a cybersecurity analyst is suspicious of the file, the hash value can be submitted to an online malware repository site to determine if the file is known malware.

**14. Which technology is a major standard consisting of a pattern of symbols that describe data to be matched in a query?**

* OSSEC
* POSIX
* Squert
* Sguil

**Explanation:** A regular expression (regex) is a pattern of symbols that describe data to be matched in a query or other operation. Regular expressions are constructed similarly to arithmetic expressions, by using various operators to combine smaller expressions. There are two major standards of regular expression, POSIX and Perl.

**15. Which tool is a Security Onion integrated host-based intrusion detection system?**

* Snort
* OSSEC
* ELK
* Sguil

**Explanation:** OSSEC is a host-based intrusion detection system (HIDS) that is integrated into Security Onion and actively monitors host system operation.

**16. Which term is used to describe the process of converting log entries into a common format?**

* classification
* systemization
* normalization
* standardization

**Explanation:** For processing log entries, data normalization can organize and convert data values in datasets from difference sources into common format. The normalization makes it easy for further data analysis and reporting.

**17. What is the purpose for data normalization?**

* to simplify searching for correlated events
* to reduce the amount of alert data
* to enhance the secure transmission of alert data
* to make the alert data transmission fast

**Explanation:** With data normalization various sources of data are combined into a common display format, which simplifies the searching for similar or relevant events.

**18. Which personnel in a SOC is assigned the task of verifying whether an alert triggered by monitoring software represents a true security incident?**

* SOC Manager
* Tier 3 personnel
* Tier 2 personnel
* Tier 1 personnel

**Explanation:** In a SOC, the job of a Tier 1 Alert Analyst includes monitoring incoming alerts and verifying that a true security incident has occurred.

**19. Refer to the exhibit. A security analyst is reviewing an alert message generated by Snort. What does the number 2100498 in the message indicate?**  
****

* the id of the user that triggers the alert
* the message length in bits
* the Snort rule that is triggered
* the session number of the message

**Explanation:** The sid field in a Snort alert message indicates the Snort security rule that is triggered.

**20. What are security event logs commonly based on when sourced by traditional firewalls?**

* static filtering
* application analysis
* signatures
* 5-tuples

**Explanation:** Traditional firewalls commonly provide security event logs based on the 5-tuples of source IP address and port number, destination IP address and port number, and the protocol in use.

**21. A threat actor has successfully breached the network firewall without being detected by the IDS system. What condition describes the lack of alert?**

* false negative
* true negative
* true positive
* false positive

**Explanation:** A false negative is where no alert exists and exploits are not being detected by the security systems that are in place.

**22. What information is contained in the options section of a Snort rule?**

* direction of traffic flow
* text describing the event
* action to be taken
* source and destination address

**Explanation:** Snort rules consist of two sections, the rules header and the rule options. The rule options section of a snort rule consists of the messages text displayed to describe an alert as well as metadata about the alert.

**23. A network administrator is trying to download a valid file from an internal server. However, the process triggers an alert on a NMS tool. What condition describes this alert?**

* false negative
* false positive
* true negative
* true positive

**Explanation:** Alerts can be classified as follows:

True Positive: The alert has been verified to be an actual security incident.  
False Positive: The alert does not indicate an actual security incident. Benign activity that results in a false positive is sometimes referred to as a benign trigger.  
An alternative situation is that an alert was not generated. The absence of an alert can be classified as:

True Negative: No security incident has occurred. The activity is benign.  
False Negative: An undetected incident has occurred.

**24. What is indicated by a Snort signature ID that is below 3464?**

* The SID was created by Sourcefire and distributed under a GPL agreement.
* This is a custom signature developed by the organization to address locally observed rules.
* The SID was created by the Snort community and is maintained in Community Rules.
* The SID was created by members of EmergingThreats.

**Explanation:** Snort is an open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) developed by Sourcefire. It has the ability to perform real time traffic analysis and packet logging on Internet Protocol (IP) networks and can also be used to detect probes or attacks.

**25. After a security monitoring tool identifies a malware attachment entering the network, what is the benefit of performing a retrospective analysis?**

* A retrospective analysis can help in tracking the behavior of the malware from the identification point forward.
* It can identify how the malware originally entered the network.
* It can calculate the probability of a future incident.
* It can determine which network host was first affected.

**Explanation:** General security monitoring can identify when a malware attachment enters a network and which host is first infected. Retrospective analysis takes the next step and is the tracking of the behavior of the malware from that point forward.

**26. A threat actor collects information from web servers of an organization and searches for employee contact information. The information collected is further used to search personal information on the Internet. To which attack phase do these activities belong according to the Cyber Kill Chain model?**

* action on objectives
* exploitation
* reconnaissance
* weaponization

**Explanation:** According to the Cyber Kill Chain model, in the reconnaissance phase the threat actor performs research, gathers intelligence, and selects targets.

**27. Which HIDS is integrated into the Security Onion and uses rules to detect changes in host-based operating parameters caused by malware through system calls?**

* OSSEC
* Bro
* Snort
* Suricata

**Explanation:** OSSEC is a HIDS integrated into the Security Onion and uses rules to detect changes in host-based parameters like the execution of software processes, changes in user privileges, registry modifications, among many others. OSSEC rules will trigger events that occurred on the host, including indicators that malware may have interacted with the OS kernel. Bro, Snort, and Suricata are examples of NIDS systems.

**28. Which type of events should be assigned to categories in Sguil?**

* false positive
* true positive
* false negative
* true negative

**Explanation:** Sguil includes seven pre-built categories that can be assigned to events that have been identified as true positives.

**29. A cybersecurity analyst is going to verify security alerts using the Security Onion. Which tool should the analyst visit first?**

* Bro
* Sguil
* CapME
* ELK

**Explanation:** The primary duty of a cybersecurity analyst is the verification of security alerts. In the Security Onion, the first place that a cybersecurity analyst will go to verify alerts is Sguil because it provides a high-level console for investigating security alerts from a wide variety of sources.

**30. Refer to the exhibit. Which field in the Sguil application window indicates the priority of an event or set of correlated events?**  
Table

Description automatically generated

* ST
* AlertID
* Pr
* CNT

**Explanation:** The Sguil application window has several fields available that give information about an event. The ST field gives the status of an event that includes a color-coded priority from light yellow to red to indicate four levels of priority.

**32. What is the purpose for data reduction as it relates to NSM?**

* to make the alert data transmission fast
* to remove recurring data streams
* to enhance the secure transmission of alert data
* to diminish the quantity of NSM data to be handled

**Explanation:** The amount of network traffic that is collected by packet captures and the number of log file entries and alerts that are generated by network and security devices can be enormous. For this reason, it is important to identify the NSM-related data that should be gathered. This process is called data reduction.

**33. Why would threat actors prefer to use a zero-day attack in the Cyber Kill Chain weaponization phase?**

* to avoid detection by the target
* to launch a DoS attack toward the target
* to get a free malware package
* to gain faster delivery of the attack on the target

**Explanation:** When a threat actor prepares a weapon for an attack, the threat actor chooses an automated tool (weaponizer) that can be deployed through discovered vulnerabilities. Malware that will carry desired attacks is then built into the tool as the payload. The weapon (tool plus malware payload) will be delivered to the target system. By using a zero-day weaponizer, the threat actor hopes that the weapon will not be detected because it is unknown to security professionals and detection methods are not yet developed.

**34. What is the objective the threat actor in establishing a two-way communication channel between the target system and a CnC infrastructure?**

* to allow the threat actor to issue commands to the software that is installed on the target
* to send user data stored on the target to the threat actor
* to steal network bandwidth from the network where the target is located
* to launch a buffer overflow attack

**Explanation:** In the command and control phase of the Cyber Kill Chain, the threat actor establishes command and control (CnC) with the target system. With the two-way communication channel, the threat actor is able to issue commands to the malware software installed on the target.

**35. Which meta-feature element in the Diamond Model describes information gained by the adversary?**

* methodology
* resources
* results
* direction

**Explanation:** The meta-feature element results are used to delineate what the adversary gained from the intrusion event.

**36. In which step of the NIST incident response process does the CSIRT perform an analysis to determine which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring?**

* incident notification
* attacker identification
* scoping
* detection

**Explanation:** In the detection and analysis phase of the NIST incident response process life cycle, the CSIRT should immediately perform an initial analysis to determine the scope of the incident, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring.

**37. Which classification indicates that an alert is verified as an actual security incident?**

* false negative
* true positive
* false positive
* true negative

**Explanation:**

Alerts can be classified as follows:

True Positive: The alert has been verified to be an actual security incident.  
False Positive: The alert does not indicate an actual security incident. Benign activity that results in a false positive is sometimes referred to as a benign trigger.  
An alternative situation is that an alert was not generated. The absence of an alert can be classified as follows:

True Negative: No security incident has occurred. The activity is benign.  
False Negative: An undetected incident has occurred.

**1. What is the significant characteristic of worm malware?**

* Worm malware disguises itself as legitimate software.
* Once installed on a host system, a worm does not replicate itself.
* A worm must be triggered by an event on the host system.
* A worm can execute independently of the host system.

**Explanation:** Worm malware can execute and copy itself without being triggered by a host program. It is a significant network and Internet security threat.

**2. What are the three major components of a worm attack? (Choose three.)**

* a payload
* a propagation mechanism
* an infecting vulnerability
* a probing mechanism
* an enabling vulnerability
* a penetration mechanism

**Explanation:** A computer can have a worm installed through an email attachment, an executable program file, or a Trojan Horse. The worm attack not only affects one computer, but replicates to other computers. What the worm leaves behind is the payload–the code that results in some action.

**3. A user is curious about how someone might know a computer has been infected with malware. What are two common malware behaviors? (Choose two.)**

* The computer emits a hissing sound every time the pencil sharpener is used.
* The computer beeps once during the boot process.
* The computer gets increasingly slower to respond.
* No sound emits when an audio CD is played.
* The computer freezes and requires reboots.

**Explanation:** Common symptoms of computers infected with malware:  
Appearance of files, applications, or desktop icons  
Security tools such as antivirus software or firewalls turned off or changed  
System crashes  
Emails spontaneously sent to others  
Modified or missing files  
Slow system or browser response  
Unfamiliar processes or services running  
Unknown TCP or UDP ports open  
Connections made to unknown remote devices

**4. Which two types of attacks are examples of reconnaissance attacks? (Choose two.)**

* brute force
* port scan
* ping sweep
* man-in-the-middle
* SYN flood

**Explanation:** Reconnaissance attacks attempt to gather information about the targets. Ping sweeps will indicate which hosts are up and responding to pings, whereas port scans will indicate on which TCP and UDP ports the target is listening for incoming connections. Man-in-the-middle and brute force attacks are both examples of access attacks, and a SYN flood is an example of a denial of service (DoS) attack.

**5. An administrator discovers a vulnerability in the network. On analysis of the vulnerability the administrator decides the cost of managing the risk outweighs the cost of the risk itself. The risk is accepted, and no action is taken. What risk management strategy has been adopted?**

* risk transfer
* risk acceptance
* risk reduction
* risk avoidance

**Explanation:** Risk acceptance is when the cost of risk management options outweighs the cost of the risk itself, the risk is accepted, and no action is taken.

**6. Which protocol is exploited by cybercriminals who create malicious iFrames?**

* HTTP
* DNS
* ARP
* DHCP

**Explanation:** An HTML element known as an inline frame or iFrame allows the browser to load a different web page from another source.

**7. How can a DNS tunneling attack be mitigated?**

* by preventing devices from using gratuitous ARP
* by using a filter that inspects DNS traffic
* by securing all domain owner accounts
* by using strong passwords and two-factor authentication

**Explanation:** To be able to stop DNS tunneling, a filter that inspects DNS traffic must be used. Also, DNS solutions such as Cisco OpenDNS block much of the DNS tunneling traffic by identifying suspicious domains.

**8. What is the function of a gratuitous ARP sent by a networked device when it boots up?**

* to request the netbios name of the connected system
* to request the MAC address of the DNS server
* to request the IP address of the connected network
* to advise connected devices of its MAC address

**Explanation:** A gratuitous ARP is often sent when a device first boots up to inform all other devices on the local network of the MAC address of the new device.

**9. What is the result of a passive ARP poisoning attack?**

* Data is modified in transit or malicious data is inserted in transit.
* Network clients experience a denial of service.
* Confidential information is stolen.
* Multiple subdomains are created.

**Explanation:** ARP poisoning attacks can be passive or active. The result of a passive attack is that cybercriminals steal confidential information. With an active attack, cybercriminals modify data in transit or they inject malicious data.

**10. What are two methods used by cybercriminals to mask DNS attacks? (Choose two.)**

* reflection
* shadowing
* domain generation algorithms
* fast flux
* tunneling

**Explanation:** Fast flux, double IP flux, and domain generation algorithms are used by cybercrimals to attack DNS servers and affect DNS services. Fast flux is a technique used to hide phishing and malware delivery sites behind a quickly-changing network of compromised DNS hosts (bots within botnets). The double IP flux technique rapidly changes the hostname to IP address mappings and the authoritative name server. Domain generation algorithms randomly generate domain names to be used as rendezvous points.

**14. What scenario describes a vulnerability broker?**

* a teenager running existing scripts, tools, and exploits, to cause harm, but typically not for profit
* a threat actor attempting to discover exploits and report them to vendors, sometimes for prizes or rewards
* a threat actor publicly protesting against governments by posting articles and leaking sensitive information
* a State-Sponsored threat actor who steals government secrets and sabotages networks of foreign governments

**Explanation:** Vulnerability brokers typically refers to grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.

**15. In what type of attack is a cybercriminal attempting to prevent legitimate users from accessing network services?**

* DoS
* session hijacking
* MITM
* address spoofing

**Explanation:** In a DoS or denial-of-service attack, the goal of the attacker is to prevent legitimate users from accessing network services.

**16. Which field in the IPv6 header points to optional network layer information that is carried in the IPv6 packet?**

* traffic class
* version
* flow label
* next header

**Explanation:** Optional Layer 3 information about fragmentation, security, and mobility is carried inside of extension headers in an IPv6 packet. The next header field of the IPv6 header acts as a pointer to these optional extension headers if they are present.

**17. Which type of attack is carried out by threat actors against a network to determine which IP addresses, protocols, and ports are allowed by ACLs?**

* social engineering
* denial of service
* phishing
* reconnaissance

**Explanation:** Packet filtering ACLs use rules to filter incoming and outgoing traffic. These rules are defined by specifying IP addresses, port numbers, and protocols to be matched. Threat actors can use a reconnaissance attack involving port scanning or penetration testing to determine which IP addresses, protocols, and ports are allowed by ACLs.

**18. What kind of ICMP message can be used by threat actors to create a man-in-the-middle attack?**

* ICMP echo request
* ICMP unreachable
* ICMP redirects
* ICMP mask reply

**Explanation:**Common ICMP messages of interest to threat actors include the following:  
ICMP echo request and echo reply: used to perform host verification and DoS attacks  
ICMP unreachable: used to perform network reconnaissance and scanning attacks  
ICMP mask reply: used to map an internal IP network  
ICMP redirects: used to lure a target host into sending all traffic through a compromised device and create a man-in-the-middle attack  
ICMP router discovery: used to inject bogus route entries into the routing table of a target host

**19. What are two purposes of launching a reconnaissance attack on a network? (Choose two.)**

* to escalate access privileges
* to prevent other users from accessing the system
* to scan for accessibility
* to gather information about the network and devices
* to retrieve and modify data

**Explanation:** Gathering information about a network and scanning for access is a reconnaissance attack. Preventing other users from accessing a system is a denial of service attack. Attempting to retrieve and modify data, and attempting to escalate access privileges are types of access attacks.

**20. Which type of network attack involves randomly opening many Telnet requests to a router and results in a valid network administrator not being able to access the device?**

* DNS poisoning
* man-in-the-middle
* **SYN flooding**
* spoofing

**Explanation:** The TCP SYN Flood attack exploits the TCP three-way handshake. The threat actor continually sends TCP SYN session request packets with a randomly spoofed source IP address to an intended target. The target device replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet. Those responses never arrive. Eventually the target host is overwhelmed with half-open TCP connections and denies TCP services.

**21. What functionality is provided by Cisco SPAN in a switched network?**

* It mirrors traffic that passes through a switch port or VLAN to another port for traffic analysis.
* It prevents traffic on a LAN from being disrupted by a broadcast storm.
* It protects the switched network from receiving BPDUs on ports that should not be receiving them.
* It copies traffic that passes through a switch interface and sends the data directly to a syslog or SNMP server for analysis.
* It inspects voice protocols to ensure that SIP, SCCP, H.323, and MGCP requests conform to voice standards.
* It mitigates MAC address overflow attacks.

**Explanation:** SPAN is a Cisco technology used by network administrators to monitor suspicious traffic or to capture traffic to be analyzed.

**22. Which statement describes an operational characteristic of NetFlow?**

* NetFlow collects basic information about the packet flow, not the flow data itself.
* NetFlow captures the entire contents of a packet.
* NetFlow flow records can be viewed by the tcpdump tool.
* NetFlow can provide services for user access control.

**Explanation:** NetFlow does not capture the entire contents of a packet. Instead, NetFlow collects metadata, or data about the flow, not the flow data itself. NetFlow information can be viewed with tools such as **nfdump** and FlowViewer.

**24. Which technology is a proprietary SIEM system?**

* StealthWatch
* NetFlow collector
* SNMP agent
* Splunk

**Explanation:** Security Information Event Management (SIEM) is a technology that is used in enterprise organizations to provide real-time reporting and long-term analysis of security events. Splunk is a proprietary SIEM system.

**25. What are three functionalities provided by SOAR? (Choose three.)**

* It automates complex incident response procedures and investigations.
* It provides 24×7 statistics on packets that flow through a Cisco router or multilayer switch.
* It uses artificial intelligence to detect incidents and aid in incident analysis and response.
* It presents the correlated and aggregated event data in real-time monitoring and long-term summaries.
* It provides a complete audit trail of basic information about every IP flow forwarded on a device.
* It provides case management tools that allow cybersecurity personnel to research and investigate incidents.

**Explanation:** SOAR security platforms offer these functionalities:  
• Gather alarm data from each component of the system  
• Provide tools that enable cases to be researched, assessed, and investigated  
• Emphasize integration as a means of automating complex incident response workflows that enable more rapid response and adaptive defense strategies  
• Include predefined playbooks that enable automatic response to specific threats

**26. Which devices should be secured to mitigate against MAC address spoofing attacks?**

* Layer 7 devices
* Layer 4 devices
* Layer 3 devices
* Layer 2 devices

**Explanation:** Layer 2 attacks such as MAC address spoofing can be mitigated by securing Layer 2 devices.

**27. A network administrator is checking the system logs and notices unusual connectivity tests to multiple well-known ports on a server. What kind of potential network attack could this indicate?**

* access
* denial of service
* information theft
* reconnaissance

**Explanation:** A reconnaissance attack is the unauthorized discovery and mapping of systems, services, or vulnerabilities. One of the most common reconnaissance attacks is performed by using utilities that automatically discover hosts on the networks and determine which ports are currently listening for connections.

**28. What is a vulnerability that allows criminals to inject scripts into web pages viewed by users?**

* Cross-site scripting
* XML injection
* buffer overflow
* SQL injection

**Explanation:** Cross-site scripting (XSS) allows criminals to inject scripts that contain malicious code into web applications.

**29. Which cyber attack involves a coordinated attack from a botnet of zombie computers?**

* ICMP redirect
* MITM
* DDoS
* address spoofing

**Explanation:** DDoS is a distributed denial-of-services attack. A DDoS attack is launched from multiple coordinated sources. The sources of the attack are zombie hosts that the cybercriminal has built into a botnet. When ready, the cybercriminal instructs the botnet of zombies to attack the chosen target.

**30. What technique is a security attack that depletes the pool of IP addresses available for legitimate hosts?**

* reconnaissance attack
* DHCP starvation
* DHCP spoofing
* DHCP snooping

**Explanation:** DHCP starvation attacks create a denial of service for network clients. The attacker sends DHCP discovery messages that contain fake MAC addresses in an attempt to lease all of the IP addresses. In contrast, DHCP spoofing occurs when a cybercriminal configures a rogue DHCP server to provide network clients with incorrect IP configuration information.

**31 Which type of Trojan horse security breach uses the computer of the victim as the source device to launch other attacks?**

* proxy
* FTP
* DoS
* data-sending

**Explanation:** The attacker uses a proxy Trojan horse attack to penetrate one device and then use that device to launch attacks on other devices. The Dos Trojan horse slows or halts network traffic. The FTP trojan horse enables unauthorized file transfer services when port 21 has been compromised. A data-sending Trojan horse transmits data back to the hacker that could include passwords.

**32. What are two examples of DoS attacks? (Choose two.)**

* buffer overflow
* SQL injection
* port scanning
* phishing
* ping of death

**Explanation:** The buffer overflow and ping of death DoS attacks exploit system memory-related flaws on a server by sending an unexpected amount of data or malformed data to the server.

**33. Why would a rootkit be used by a hacker?**

* to try to guess a password
* to reverse engineer binary files
* to gain access to a device without being detected
* to do reconnaissance

**Explanation:** Hackers use rootkits to avoid detection as well as hide any software installed by the hacker.

**34. What causes a buffer overflow?**

* sending too much information to two or more interfaces of the same device, thereby causing dropped packets
* attempting to write more data to a memory location than that location can hold
* sending repeated connections such as Telnet to a particular device, thus denying other data sources
* downloading and installing too many software updates at one time
* launching a security countermeasure to mitigate a Trojan horse

**Explanation:** By sending too much data to a specific area of memory, adjacent memory locations are overwritten, which causes a security issue because the program in the overwritten memory location is affected.

**35. Which type of security threat would be responsible if a spreadsheet add-on disables the local software firewall?**

* DoS
* Trojan horse
* buffer overflow
* brute-force attack

**Explanation:** A Trojan horse is software that does something harmful, but is hidden in legitimate software code. A denial of service (DoS) attack results in interruption of network services to users, network devices, or applications. A brute-force attack commonly involves trying to access a network device. A buffer overflow occurs when a program attempts to store more data in a memory location than it can hold.

**36. Which two types of hackers are typically classified as grey hat hackers? (Choose two.)**

* hacktivists
* cyber criminals
* vulnerability brokers
* script kiddies
* state-sponsored hackers

**Explanation:** Grey hat hackers may do unethical or illegal things, but not for personal gain or to cause damage. Hacktivists use their hacking as a form of political or social protest, and vulnerability brokers hack to uncover weaknesses and report them to vendors. Depending on the perspective one possesses, state-sponsored hackers are either white hat or black hat operators. Script kiddies create hacking scripts to cause damage or disruption. Cyber criminals use hacking to obtain financial gain by illegal means.

**37. A white hat hacker is using a security tool called Skipfish to discover the vulnerabilities of a computer system. What type of tool is this?**

* debugger
* fuzzer
* vulnerability scanner
* packet sniffer

**Explanation:** Fuzzers are tools used by threat actors when attempting to discover the vulnerabilities of a computer system. Examples of fuzzers include Skipfish, Wapiti, and W3af.

**38. Which two functions are provided by NetFlow? (Choose two.)**

* It uses artificial intelligence to detect incidents and aid in incident analysis and response.
* It provides a complete audit trail of basic information about every IP flow forwarded on a device.
* It provides 24×7 statistics on packets that flow through a Cisco router or multilayer switch.
* It allows an administrator to capture real-time network traffic and analyze the entire contents of packets.
* It presents correlated and aggregated event data in real-time monitoring and long-term summaries.

**Explanation:** NetFlow is a Cisco IOS technology that provides statistics and complete audit trails on TCP/IP flows on the network. Some of the capabilities of NetFlow include the following: 24×7 network and security monitoring, network planning, traffic analysis, identification of network bottlenecks, and IP accounting for billing purposes.

**39. Which statement describes the function of the SPAN tool used in a Cisco switch?**

* It is a secure channel for a switch to send logging to a syslog server.
* It provides interconnection between VLANs over multiple switches.
* It supports the SNMP trap operation on a switch.
* It copies the traffic from one switch port and sends it to another switch port that is connected to a monitoring device.

**Explanation:** To analyze network traffic passing through a switch, switched port analyzer (SPAN) can be used. SPAN can send a copy of traffic from one port to another port on the same switch where a network analyzer or monitoring device is connected. SPAN is not required for syslog or SNMP. SPAN is used to mirror traffic, while syslog and SNMP are configured to send data directly to the appropriate server.

**40. What are two evasion methods used by hackers? (Choose two.)**

* scanning
* access attack
* resource exhaustion
* phishing
* encryption

**Explanation:** The following methods are used by hackers to avoid detection:Encryption and tunneling – hide or scramble the malware content  
Resource exhaustion – keep the host device too busy to detect the invasion  
Traffic fragmentation – split the malware into multiple packets  
Protocol-level misinterpretation – sneak by the firewall  
Pivot – use a compromised network device to attempt access to another device  
Rootkit – allow the hacker to avoid detection as well as hide software installed by the hacker

**41. Which attack involves threat actors positioning themselves between a source and destination with the intent of transparently monitoring, capturing, and controlling the communication?**

* man-in-the-middle attack
* DoS attack
* ICMP attack
* SYN flood attack

**Explanation:** The man-in-the-middle attack is a common IP-related attack where threat actors position themselves between a source and destination to transparently monitor, capture, and control the communication.

**42. What is the goal of a white hat hacker?**

* validating data
* modifying data
* stealing data
* protectingdata

**Explanation:** White hat hackers are actually “good guys” and are paid by companies and governments to test for security vulnerabilities so that data is better protected.

**43. Once a cyber threat has been verified, the US Cybersecurity Infrastructure and Security Agency (CISA) automatically shares the cybersecurity information with public and private organizations. What is this automated system called?**

* AIS
* NCSA
* ENISA
* NCASM

**Explanation:** Governments are now actively promoting cybersecurity. For instance, the US Cybersecurity Infrastructure and Security Agency (CISA) is leading efforts to automate the sharing of cybersecurity information with public and private organizations at no cost. CISA use a system called Automated Indicator Sharing (AIS). AIS enables the sharing of attack indicators between the US government and the private sector as soon as threats are verified. CISA offers many resources that help to limit the size of the United States attack surface.

**44. A user receives a phone call from a person who claims to represent IT services and then asks that user for confirmation of username and password for auditing purposes. Which security threat does this phone call represent?**

* spam
* anonymous keylogging
* DDoS
* social engineering

**Explanation:** Social engineering attempts to gain the confidence of an employee and convince that person to divulge confidential and sensitive information, such as usernames and passwords. DDoS attacks, spam, and keylogging are all examples of software based security threats, not social engineering.

**45. Which two characteristics describe a worm? (Choose two)**

* is self-replicating
* travels to new computers without any intervention or knowledge of the user
* infects computers by attaching to software code
* hides in a dormant state until needed by an attacker
* executes when software is run on a computer

**Explanation:** Worms are self-replicating pieces of software that consume bandwidth on a network as they propagate from system to system. They do not require a host application, unlike a virus. Viruses, on the other hand, carry executable malicious code which harms the target machine on which they reside.

**46. An attacker is redirecting traffic to a false default gateway in an attempt to intercept the data traffic of a switched network. What type of attack could achieve this?**

* MAC address snoopin
* DHCP snooping
* MAC address starvation
* DHCP spoofing

**Explanation:** In DHCP spoofing attacks, an attacker configures a fake DHCP server on the network to issue DHCP addresses to clients with the aim of forcing the clients to use a false default gateway, and other false services. DHCP snooping is a Cisco switch feature that can mitigate DHCP attacks. MAC address starvation and MAC address snooping are not recognized security attacks. MAC address spoofing is a network security threat.

**47. What would be the target of an SQL injection attack?**

* DHCP
* DNS
* email
* database

**Explanation:** SQL is the language used to query a relational database. Cybercriminals use SQL injections to get information, create fake or malicious queries, or to breach the database in some other way.

**48. The IT department is reporting that a company web server is receiving an abnormally high number of web page requests from different locations simultaneously. Which type of security attack is occurring?**

* social engineering
* adware
* DDoS
* phishing
* spyware

**Explanation:** Phishing, spyware, and social engineering are security attacks that collect network and user information. Adware consists, typically, of annoying popup windows. Unlike a DDoS attack, none of these attacks generate large amounts of data traffic that can restrict access to network services.

**49. Why would an attacker want to spoof a MAC address?**

* so that the attacker can capture traffic from multiple VLANs rather than from just the VLAN that is assigned to the port to which the attacker device is attached
* so that a switch on the LAN will start forwarding frames to the attacker instead of to the legitimate host
* so that a switch on the LAN will start forwarding all frames toward the device that is under control of the attacker (that can then capture the LAN traffic)
* so that the attacker can launch another type of attack in order to gain access to the switch

**Explanation:** MAC address spoofing is used to bypass security measures by allowing an attacker to impersonate a legitimate host device, usually for the purpose of collecting network traffic.

**51. Which two characteristics describe a virus? (Choose two.)**

* Malicious code that can remain dormant before executing an unwanted action.
* Malware that executes arbitrary code and installs copies of itself in memory.
* Malware that relies on the action of a user or a program to activate.
* Program code specifically designed to corrupt memory in network devices.
* A self-replicating attack that is independently launched.

**Explanation:** A virus is malicious code that is attached to legitimate programs or executable files. Most viruses require end user activation, can lie dormant for an extended period, and then activate at a specific time or date. In contrast, a worm executes arbitrary code and installs copies of itself in the memory of the infected computer. The main purpose of a worm is automatic replication to spread quickly across a network. A worm does not require a host program to run.

**52. Which type of security attack would attempt a buffer overflow?**

* ransomware
* reconnaissance
* DoS
* scareware

**Explanation:** Denial of service (DoS) attacks attempt to disrupt service on the network by either sending a particular device an overwhelming amount of data so no other devices can access the attacked device or by sending malformed packets.

Text

Description automatically generated with low confidenceD

Text

Description automatically generated with medium confidenceB