NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

CyberOps Associate (Version 1.0) – CyberOps Associate 1.0 Final exam

1. Which two statements are characteristics of a virus? (Choose two.)

- A virus typically requires end-user activation.
- A virus can be dormant and then activate at a specific time or date.
- A virus replicates itself by independently exploiting vulnerabilities in networks.
- A virus has an enabling vulnerability, a propagation mechanism, and a payload.
- A virus provides the attacker with sensitive data, such as passwords

Explanation: The type of end user interaction required to launch a virus is typically opening an application, opening a web page, or powering on the computer. Once activated, a virus may infect other files located on the computer or other computers on the same network.

2. What is a characteristic of a Trojan horse as it relates to network security?

- Too much information is destined for a particular memory block, causing additional memory areas to be affected.
- Extreme quantities of data are sent to a particular network device interface.
- An electronic dictionary is used to obtain a password to be used to infiltrate a key network device.
- Malware is contained in a seemingly legitimate executable program.

Explanation: A Trojan horse carries out malicious operations under the guise of a legitimate program. Denial of service attacks send extreme quantities of data to a particular host or network device interface. Password attacks use electronic dictionaries in an attempt to learn passwords. Buffer overflow attacks exploit memory buffers by sending too much information to a host to render the system inoperable.

3. What technique is used in social engineering attacks?

- sending junk email
- buffer overflow
- phishing
- man-in-the-middle

Explanation: A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information.

4. What is a purpose of implementing VLANs on a network?

- They can separate user traffic.
- They prevent Layer 2 loops.
- They eliminate network collisions.
- They allow switches to forward Layer 3 packets without a router.

Explanation: VLANs are used on a network to separate user traffic based on factors such as function, project team, or application, without regard for the physical location of the user or device.

5. Refer to the exhibit. A cybersecurity analyst is viewing packets forwarded by switch S2. What addresses will identify frames containing data sent from PCA to PCB?

Assessment

Practice Final Exam Answers

CyberOps Associate (Version 1.0) – FINAL EXAM ANSWERS

Recent Comments

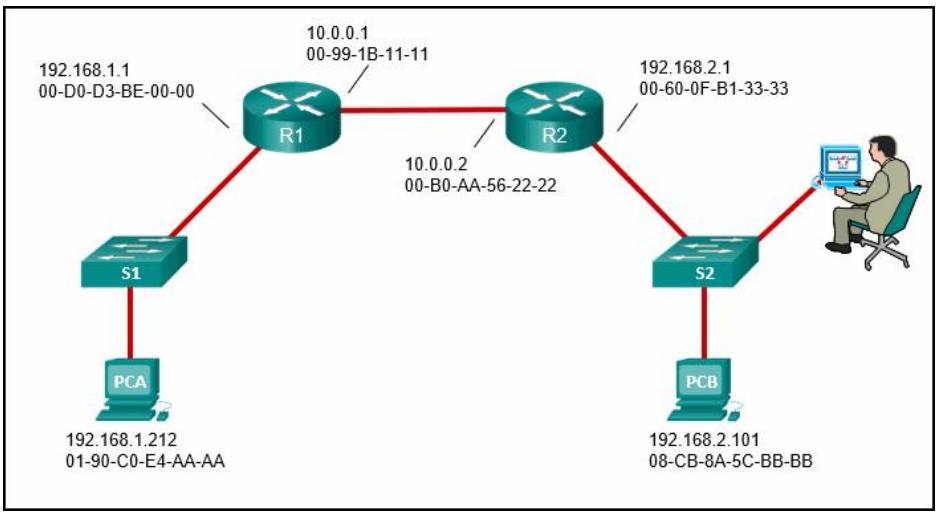
Krishna Gaggara on CCNA 200-301 Dumps Full Questions – Exam Study Guide & Free

Mohammed on CCNA 200-301 Dumps Full Questions – Exam Study Guide & Free

Mohammed on CCNA 200-301 Dumps Full Questions – Exam Study Guide & Free

Kmotso on CCNA 200-301 Dumps Full Questions – Exam Study Guide & Free

Mohammed on CCNA 200-301 Dumps Full Questions – Exam Study Guide & Free



Src IP: 192.168.2.1
Src MAC: 00-60-0F-B1-33-33
Dst IP: 192.168.2.101
Dst MAC: 08-CB-8A-5C-BB-BB

Src IP: 192.168.1.212
Src MAC: 01-90-C0-E4-AA-AA
Dst IP: 192.168.2.101
Dst MAC: 08-CB-8A-5C-BB-BB

Src IP: 192.168.1.212
Src MAC: 00-60-0F-B1-33-33
Dst IP: 192.168.2.101
Dst MAC: 08-CB-8A-5C-BB-BB

Src IP: 192.168.1.212
Src MAC: 00-60-0F-B1-33-33
Dst IP: 192.168.2.101
Dst MAC: 00-D0-D3-BE-00-00

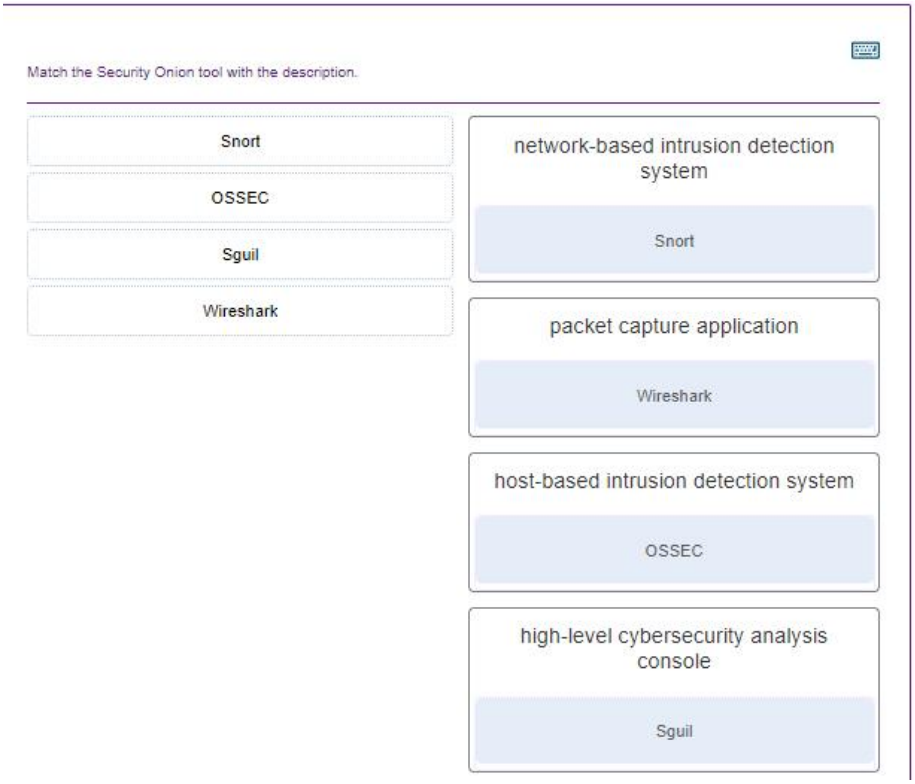
Explanation: When a message sent from PCA to PCB reaches router R2, some frame header fields will be rewritten by R2 before forwarding to switch S2. The frames will contain the source MAC address of router R2 and the destination MAC address of PCB. The frames will retain the original IPv4 addressing applied by PCA which is the IPv4 address of PCA as the source address and the IPv4 address of PCB as the destination.

6. A cybersecurity analyst needs to collect alert data. What are three detection tools to perform this task in the

Security Onion architecture? (Choose three.)

- CapME
- Wazuh
- Kibana
- Zeek
- Sguil
- Wireshark

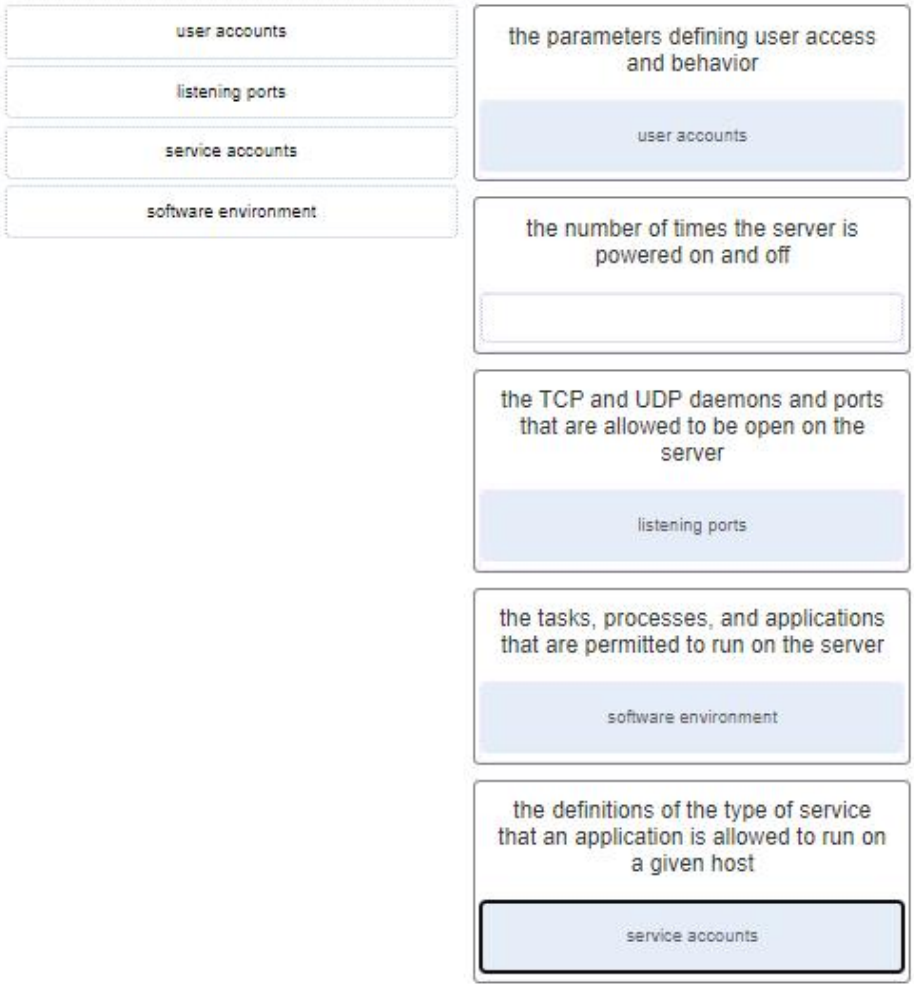
7. Match the Security Onion tool with the description.



8. In network security assessments, which type of test is used to evaluate the risk posed by vulnerabilities to a specific organization including assessment of the likelihood of attacks and the impact of successful exploits on the organization?

- port scanning
- risk analysis
- penetration testing
- vulnerability assessment

9. Match the server profile element to the description. (Not all options are used.)



Explanation: The elements of a server profile include 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 given host
Software environment – the tasks, processes, and applications that are permitted to run on the server

10. In addressing an identified risk, which strategy aims to shift some of the risk to other parties?

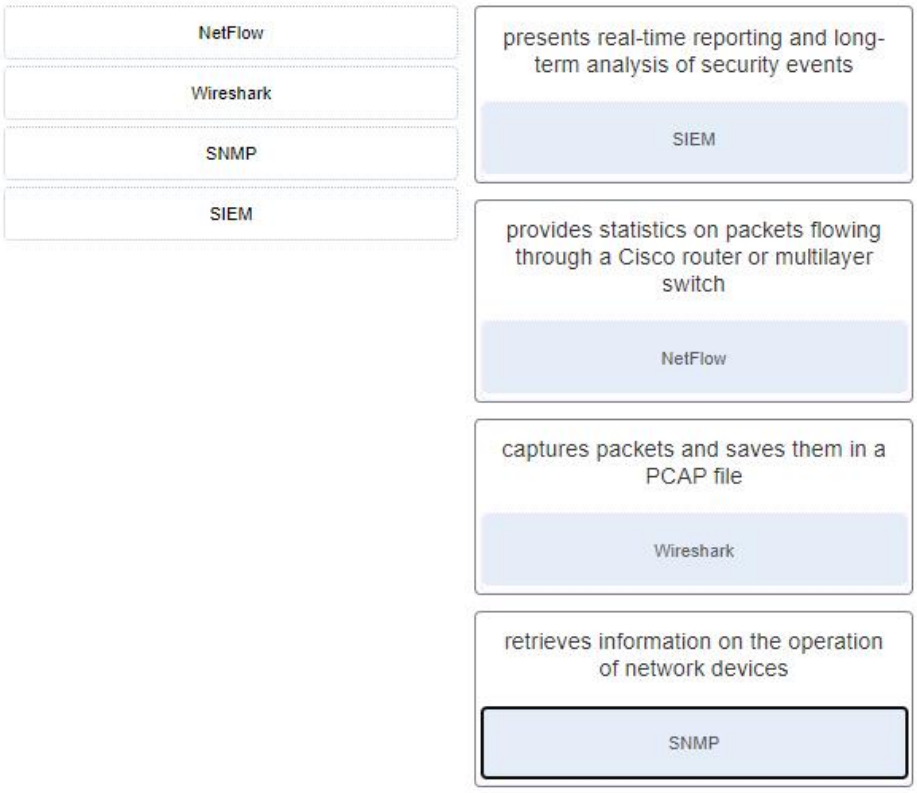
- risk avoidance
- risk sharing
- risk retention
- risk reduction

11. What is a network tap?

- a technology used to provide real-time reporting and long-term analysis of security events
- a Cisco technology that provides statistics on packets flowing through a router or multilayer switch
- a feature supported on Cisco switches that enables the switch to copy frames and forward them to an analysis device
- a passive device that forwards all traffic and physical layer errors to an analysis device

Explanation: A network tap is used to capture traffic for monitoring the network. The tap is typically a passive splitting device implemented inline on the network and forwards all traffic, including physical layer errors, to an analysis device.

12. Match the monitoring tool to the definition.



13. If a SOC has a goal of 99.999% uptime, how many minutes of downtime a year would be considered within its goal?

- Approximately 5 minutes per year.
- Approximately 10 minutes per year

- Approximately 20 minutes per year.
- Approximately 30 minutes per year.

Explanation: Within a year, there are 365 days x 24 hours a day x 60 minutes per hour = 525,600 minutes. With the goal of uptime 99.999% of time, the downtime needs to be controlled under 525,600 x (1-0.99999) = 5.256 minutes a year.

14. The HTTP server has responded to a client request with a 200 status code. What does this status code indicate?

- The request is understood by the server, but the resource will not be fulfilled.
- The request was completed successfully.
- The server could not find the requested resource, possibly because of an incorrect URL.
- The request has been accepted for processing, but processing is not completed.

15. What is an advantage for small organizations of adopting IMAP instead of POP?

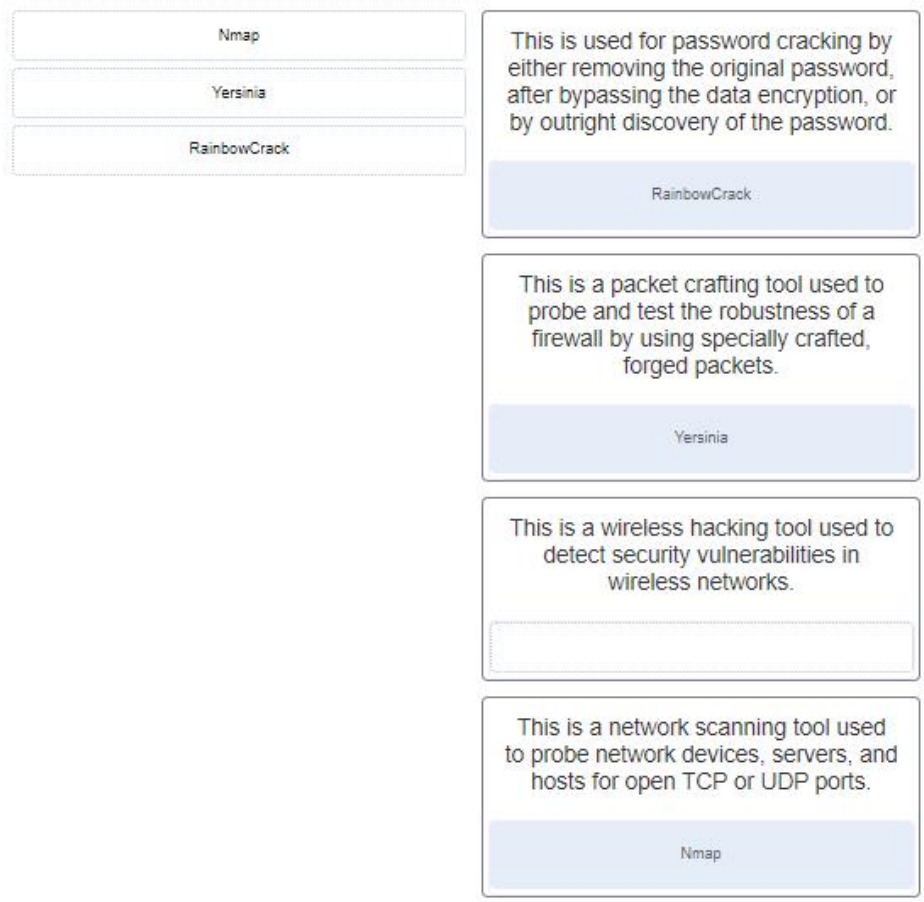
- POP only allows the client to store messages in a centralized way, while IMAP allows distributed storage.
- IMAP sends and retrieves email, but POP only retrieves email.
- When the user connects to a POP server, copies of the messages are kept in the mail server for a short time, but IMAP keeps them for a long time.
- Messages are kept in the mail servers until they are manually deleted from the email client.

Explanation: IMAP and POP are protocols that are used to retrieve email messages. The advantage of using IMAP instead of POP is that when the user connects to an IMAP-capable server, copies of the messages are downloaded to the client application. IMAP then stores the email messages on the server until the user manually deletes those messages.

16. What debugging security tool can be used by black hats to reverse engineer binary files when writing exploits?

- WinDbg
- Firesheep
- Skipfish
- AIDE

17. Match the attack tools with the description. (Not all options are used.)



18. What are two features of ARP? (Choose two.)

- When a host is encapsulating a packet into a frame, it refers to the MAC address table to determine the mapping of IP addresses to MAC addresses.
- If a host is ready to send a packet to a local destination device and it has the IP address but not the MAC address of the destination, it generates an ARP broadcast.
- If a device receiving an ARP request has the destination IPv4 address, it responds with an ARP reply.
- If no device responds to the ARP request, then the originating node will broadcast the data packet to all

devices on the network segment.

- An ARP request is sent to all devices on the Ethernet LAN and contains the IP address of the destination host and the multicast MAC address.

Explanation: When a node encapsulates a data packet into a frame, it needs the destination MAC address. First it determines if the destination device is on the local network or on a remote network. Then it checks the ARP table (not the MAC table) to see if a pair of IP address and MAC address exists for either the destination IP address (if the destination host is on the local network) or the default gateway IP address (if the destination host is on a remote network). If the match does not exist, it generates an ARP broadcast to seek the IP address to MAC address resolution. Because the destination MAC address is unknown, the ARP request is broadcast with the MAC address FFFF.FFFF.FFFF. Either the destination device or the default gateway will respond with its MAC address, which enables the sending node to assemble the frame. If no device responds to the ARP request, then the originating node will discard the packet because a frame cannot be created.

19. What is a property of the ARP table on a device?

- Entries in an ARP table are time-stamped and are purged after the timeout expires.
- Every operating system uses the same timer to remove old entries from the ARP cache.
- Static IP-to-MAC address entries are removed dynamically from the ARP table.
- Windows operating systems store ARP cache entries for 3 minutes.

20. What is the purpose of Tor?

- to allow users to browse the Internet anonymously
- to securely connect to a remote network over an unsecure link such as an Internet connection
- to donate processor cycles to distributed computational tasks in a processor sharing P2P network

- to inspect incoming traffic and look for any that violates a rule or matches the signature of a known exploit

Explanation: Tor is a software platform and network of peer-to-peer (P2P) hosts that function as routers. Users access the Tor network by using a special browserthat allows them to browse anonymously.

21. Which two network protocols can be used by a threat actor to exfiltrate data in traffic that is disguised as normal network traffic? (Choose two.)

- NTP
- DNS
- HTTP
- syslog
- SMTP

22. What is a key difference between the data captured by NetFlow and data captured by Wireshark?

- NetFlow data shows network flow contents whereas Wireshark data shows network flow statistics.
- NetFlow data is analyzed by tcpdump whereas Wireshark data is analyzed by nfdump.
- NetFlow provides transaction data whereas Wireshark provides session data.
- NetFlow collects metadata from a network flow whereas Wireshark captures full data packets.

Explanation: Wireshark captures the entire contents of a packet. NetFlow does not. Instead, NetFlow collects metadata, or data about the flow.

23. Which tool captures full data packets with a command-line interface only?

- nfdump
- Wireshark
- NBAR2
- tcpdump

Explanation: The command-line tool tcpdump is a packet analyzer. Wireshark is a packet analyzer with a GUI interface.

24. Which method can be used to harden a device?

- maintain use of the same passwords
- allow default services to remain enabled
- allow USB auto-detection
- use SSH and disable the root account access over SSH

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 re-using old passwords.
Review logs regularly.

25. In a Linux operating system, which component interprets user commands and attempts to execute them?

- GUI
- daemon
- kernel
- shell

26. A network administrator is configuring an AAA server to manage RADIUS authentication. Which two features are included in RADIUS authentication? (Choose two.)

- encryption for all communication
- encryption for only the data
- single process for authentication and authorization
- separate processes for authentication and authorization
- hidden passwords during transmission

27. What is privilege escalation?

- Vulnerabilities in systems are exploited to grant higher levels of privilege than someone or some process should have.
- Everyone is given full rights by default to everything and rights are taken away only when someone abuses privileges.
- Someone is given rights because she or he has received a promotion.
- A security problem occurs when high ranking corporate officials demand rights to systems or files that they should not have.

Explanation: With privilege escalation, vulnerabilities are exploited to grant higher levels of privilege. After the privilege is granted, the threat actor can access sensitive information or take control of the system.

28. What two assurances does digital signing provide about code that is downloaded from the Internet? (Choose two.)

- The code contains no viruses.
- The code has not been modified since it left the software publisher.
- The code is authentic and is actually sourced by the publisher.
- The code contains no errors.
- The code was encrypted with both a private and public key.

Explanation: Digitally signing code provides several assurances about the code:
The code is authentic and is actually sourced by the publisher.
The code has not been modified since it left the software publisher.
The publisher undeniably published the code. This provides nonrepudiation of the act of publishing.

29. An IT enterprise is recommending the use of PKI applications to securely exchange information between the employees. In which two cases might an organization use PKI applications to securely exchange information between users? (Choose two.)

- HTTPS web service
- 802.1x authentication
- local NTP server
- FTP transfers
- file and directory access permission

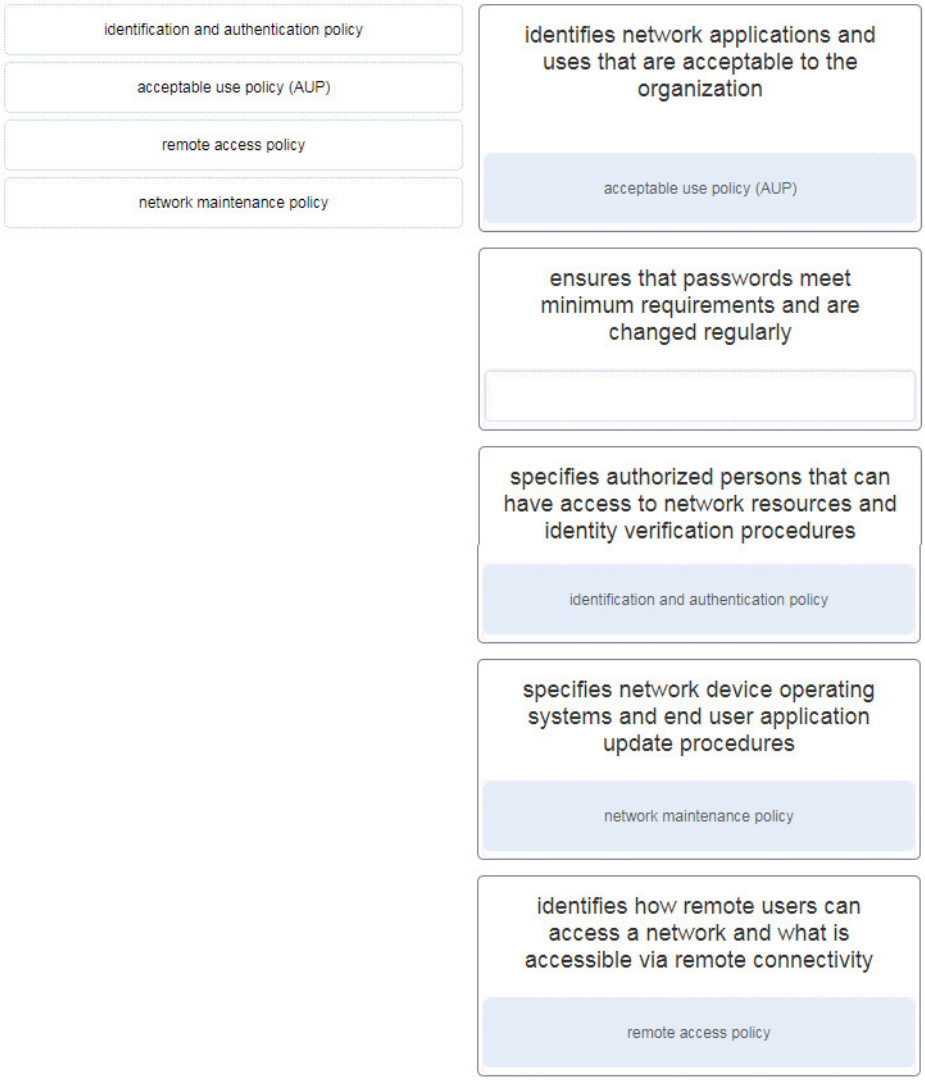
30. Which measure can a security analyst take to perform effective security monitoring against network traffic encrypted by SSL technology?

- Use a Syslog server to capture network traffic.
- Deploy a Cisco SSL Appliance.
- Require remote access connections through IPsec VPN.
- Deploy a Cisco ASA.

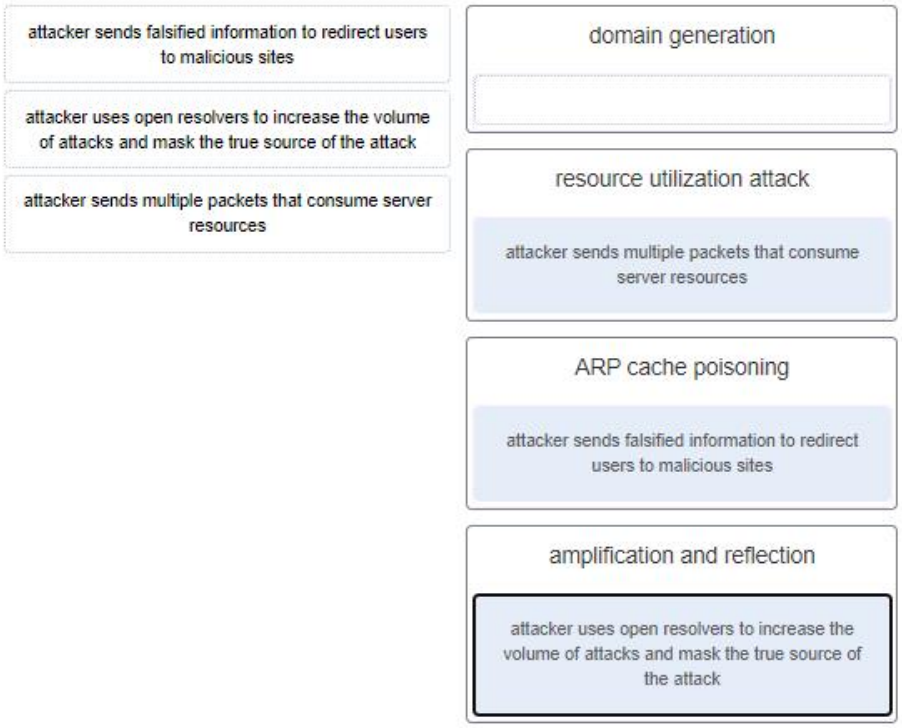
31. An administrator is trying to develop a BYOD security policy for employees that are bringing a wide range of devices to connect to the company network. Which three objectives must the BYOD security policy address? (Choose three.)

- All devices must be insured against liability if used to compromise the corporate network.
- All devices must have open authentication with the corporate network.
- Rights and activities permitted on the corporate network must be defined.
- Safeguards must be put in place for any personal device being compromised.
- The level of access of employees when connecting to the corporate network must be defined.
- All devices should be allowed to attach to the corporate network flawlessly.

32. Match the security policy with the description. (Not all options are used.)



33. Match the attack to the definition. (Not all options are used.)



34. What type of attack targets an SQL database using the input field of a user?

- XML injection
- buffer overflow
- Cross-site scripting
- SQL injection

Explanation: A criminal can insert a malicious SQL statement in an entry field on a website where the system does not filter the user input correctly.

35. What are two characteristics of Ethernet MAC addresses? (Choose two.)

- MAC addresses use a flexible hierarchical structure.
- They are expressed as 12 hexadecimal digits.
- They are globally unique.
- They are routable on the Internet.
- MAC addresses must be unique for both Ethernet and serial interfaces on a device.

36. A user calls to report that a PC cannot access the internet. The network technician asks the user to issue the command `ping 127.0.0.1` in a command prompt window. The user reports that the result is four positive

replies. What conclusion can be drawn based on this connectivity test?

- The IP address obtained from the DHCP server is correct.
- The PC can access the network. The problem exists beyond the local network.
- The PC can access the Internet. However, the web browser may not work.
- The TCP/IP implementation is functional.

37. What characterizes a threat actor?

- They are all highly-skilled individuals.
- They always use advanced tools to launch attacks.
- They always try to cause some harm to an individual or organization.
- They all belong to organized crime.

38. A computer is presenting a user with a screen requesting payment before the user data is allowed to be accessed by the same user. What type of malware is this?

- a type of logic bomb
- a type of virus
- a type of worm
- a type of ransomware

Explanation: Ransomware commonly encrypts data on a computer and makes the data unavailable until the computer user pays a specific sum of money

39. Which ICMPv6 message type provides network addressing information to hosts that use SLAAC?

- router solicitation
- neighbor advertisement
- neighbor solicitation
- router advertisement

40. A client is using SLAAC to obtain an IPv6 address for the interface. After an address has been generated and applied to the interface, what must the client do before it can begin to use this IPv6 address?

- It must wait for an ICMPv6 Router Advertisement message giving permission to use this address.
- It must send an ICMPv6 Router Solicitation message to determine what default gateway it should use.
- It must send an ICMPv6 Neighbor Solicitation message to ensure that the address is not already in use on the network.
- It must send an ICMPv6 Router Solicitation message to request the address of the DNS server.

41. Which two types of unreadable network traffic could be eliminated from data collected by NSM? (Choose two.)

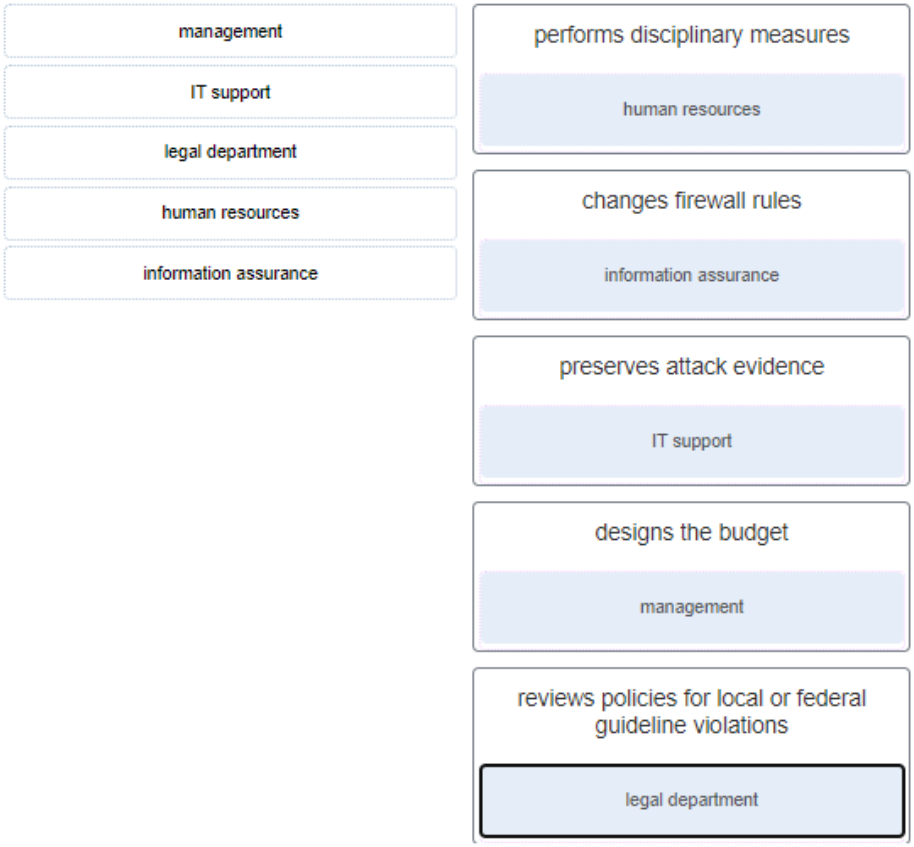
- STP traffic
- IPsec traffic
- routing updates traffic
- SSL traffic
- broadcast traffic

Explanation: To reduce the huge amount of data collected so that cybersecurity analysts can focus on critical threats, some less important or unusable data could be eliminated from the datasets. For example, encrypted data, such as IPsec and SSL traffic, could be eliminated because it is unreadable in a reasonable time frame.

42. Which core open source component of the Elastic-stack is responsible for accepting the data in its native format and making elements of the data consistent across all sources?

- Logstash
- Kibana
- Beats
- Elasticsearch

43. Match the security incident stakeholder with the role.

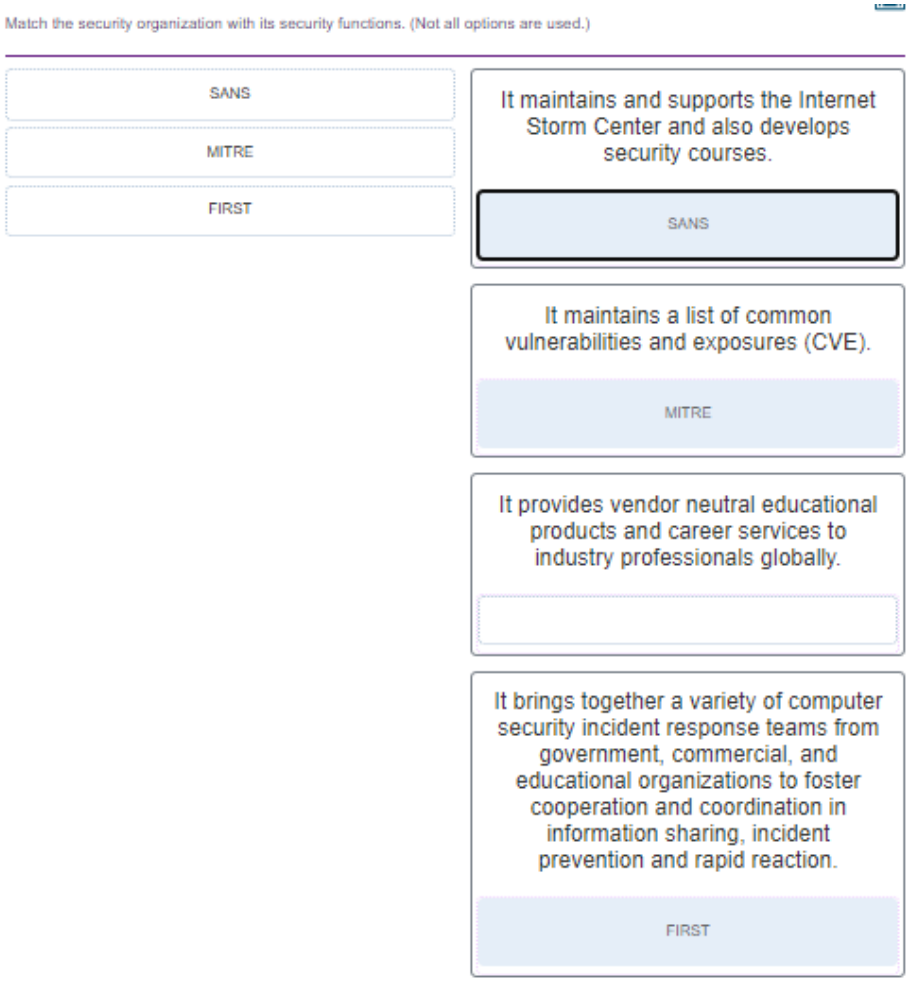


44. In the NIST incident response process life cycle, which type of attack vector involves the use of brute force against devices, networks, or services?

- media
- impersonation
- attrition
- loss or theft

Explanation: Common attack vectors include media, attrition, impersonation, and loss or theft. Attrition attacks are any attacks that use brute force. Media attacks are those initiated from storage devices. Impersonation attacks occur when something or someone is replaced for the purpose of the attack, and loss or theft attacks are initiated by equipment inside the organization.

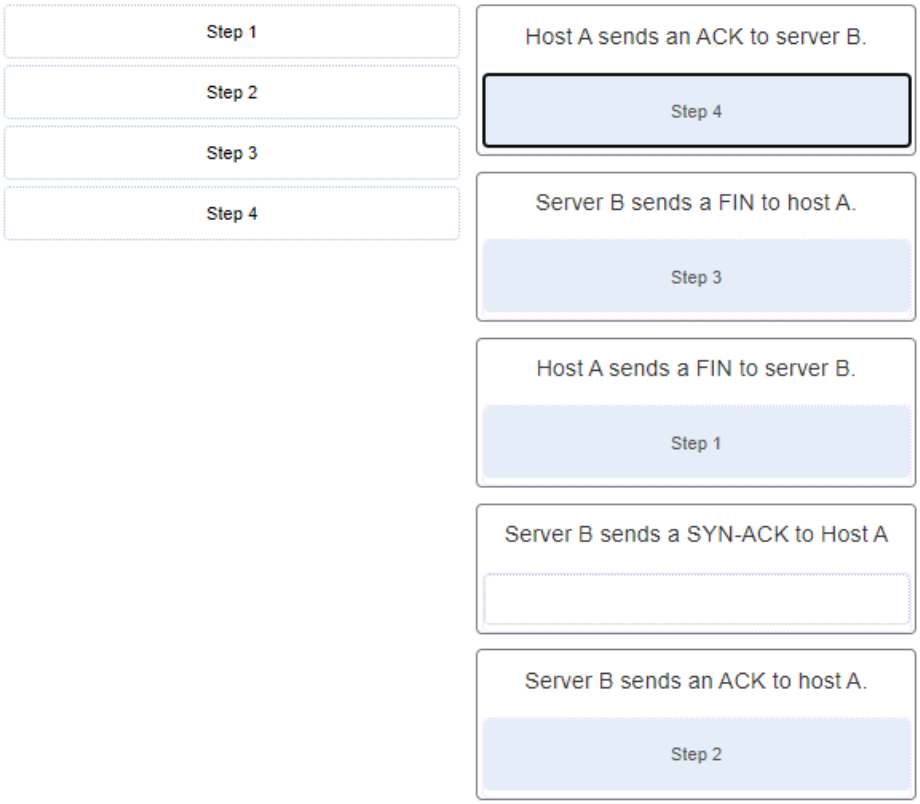
45. Match the security organization with its security functions. (Not all options are used.)



46. What is a characteristic of CybOX?

- 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 set of specifications for exchanging cyberthreat information between organizations.
- It is the specification for an application layer protocol that allows the communication of CTI over HTTPS.

47. After host A receives a web page from server B, host A terminates the connection with server B. Match each step to its correct option in the normal termination process for a TCP connection. (Not all options are used.)



48. What are two ways that ICMP can be a security threat to a company? (Choose two.)

- by collecting information about a network
- by corrupting data between email servers and email recipients
- by the infiltration of web pages
- by corrupting network IP data packets
- by providing a conduit for DoS attacks

Explanation: ICMP can be used as a conduit for DoS attacks. It can be used to collect information about a network such as the identification of hosts and network structure, and by determining the operating systems being used on the network.

49. Which three IPv4 header fields have no equivalent in an IPv6 header? (Choose three.)

- fragment offset
- protocol
- flag
- TTL
- identification

- version

Explanation: Unlike IPv4, IPv6 routers do not perform fragmentation. Therefore, all three fields supporting fragmentation in the IPv4 header are removed and have no equivalent in the IPv6 header. These three fields are fragment offset, flag, and identification. IPv6 does support host packet fragmentation through the use of extension headers, which are not part of the IPv6 header.

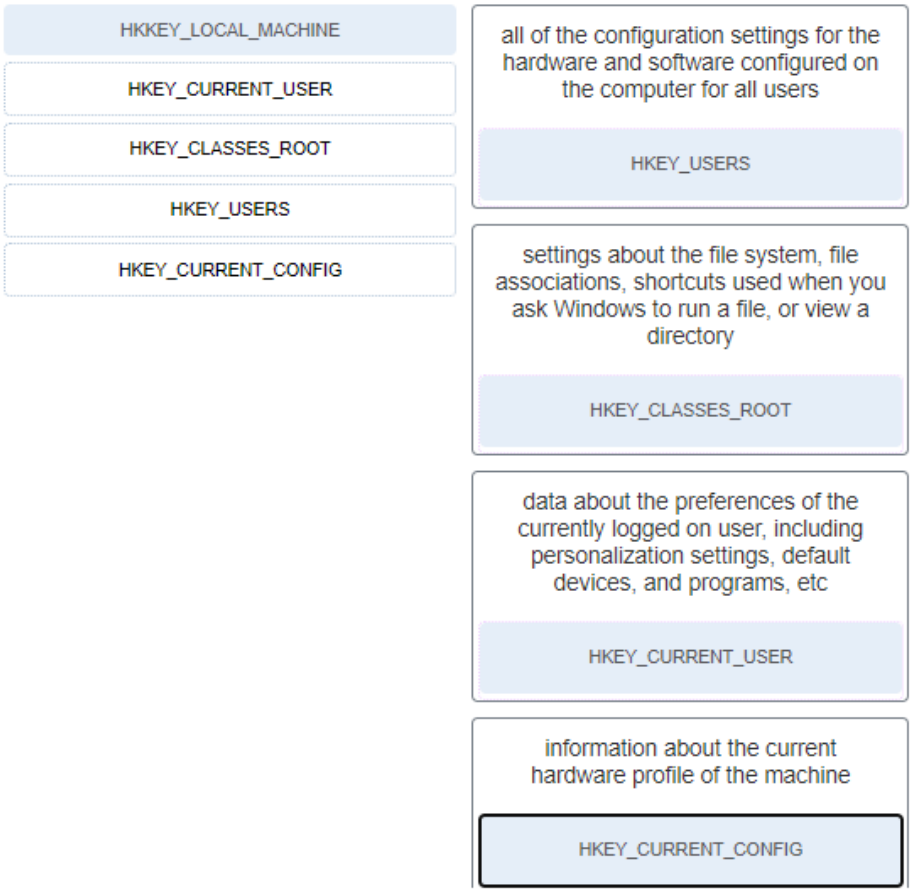
50. Which two `net` commands are associated with network resource sharing? (Choose two.)

- net start
- net accounts
- net share
- net use
- net stop

Explanation:
The `net` command is a very important command. Some common `net` commands include these:

- `net accounts` – sets password and logon requirements for users
- `net session` – lists or disconnects sessions between a computer and other computers on the network
- `net share` – creates, removes, or manages shared resources
- `net start` – starts a network service or lists running network services
- `net stop` – stops a network service
- `net use` – connects, disconnects, and displays information about shared network resources
- `net view` – shows a list of computers and network devices on the network

51. Match the Windows 10 Registry key with its description. (Not all options are used)



52. Which PDU format is used when bits are received from the network medium by the NIC of a host?

- segment
- file
- packet
- frame

Explanation: When received at the physical layer of a host, the bits are formatted into a frame at the data link layer. A packet is the PDU at the network layer. A segment is the PDU at the transport layer. A file is a data structure that may be used at the application layer.

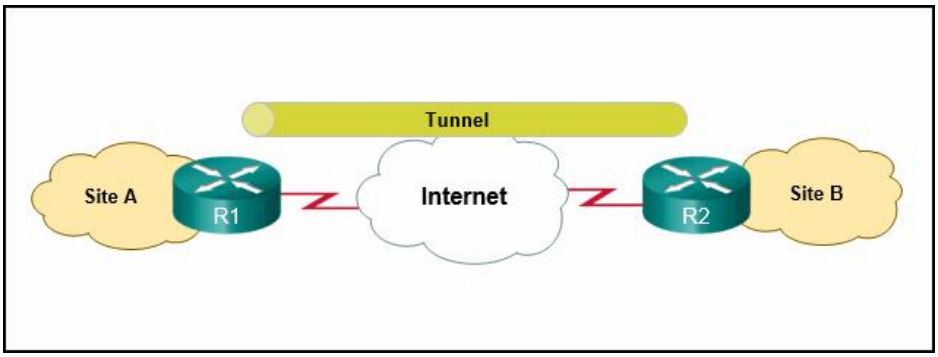
53. A user is executing a tracert to a remote device. At what point would a router, which is in the path to the destination device, stop forwarding the packet?

- when the router receives an ICMP Time Exceeded message
- when the values of both the Echo Request and Echo Reply messages reach zero

- when the RTT value reaches zero
- when the value in the TTL field reaches zero
- when the host responds with an ICMP Echo Reply message

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.

54. Refer to the exhibit. What solution can provide a VPN between site A and site B to support encapsulation of any Layer 3 protocol between the internal networks at each site?



- an IPsec tunnel
- Cisco SSL VPN
- a GRE tunnel
- a remote access tunnel

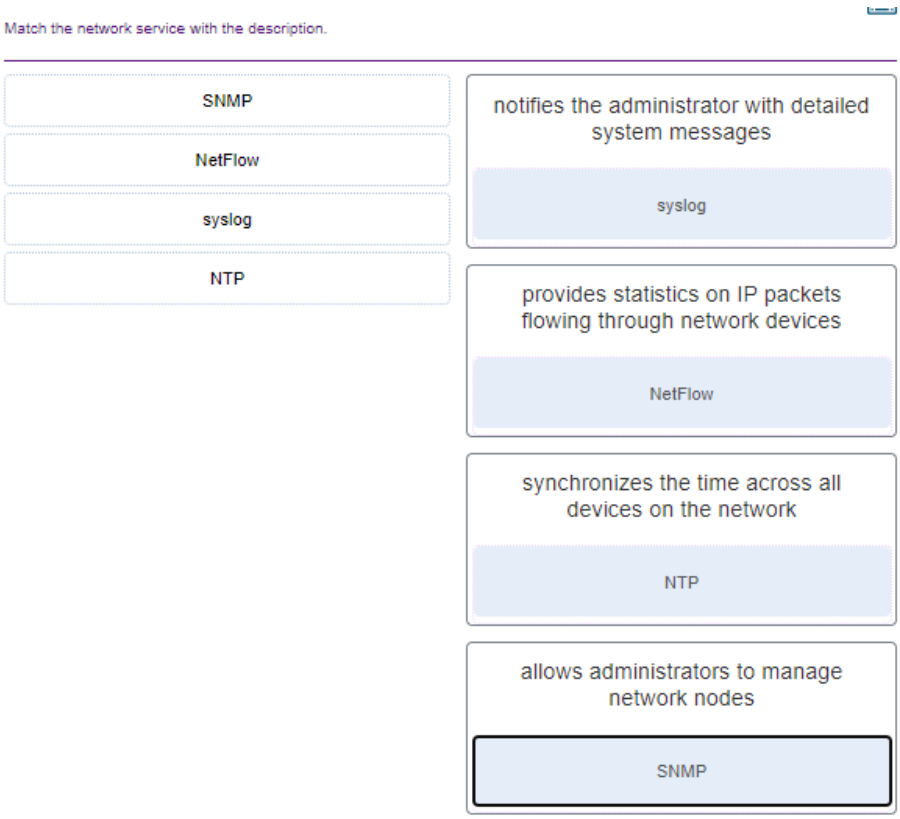
Explanation: A Generic Routing Encapsulation (GRE) tunnel is a non-secure, site-to-site VPN tunneling solution that is capable of encapsulating any Layer 3 protocol between multiple sites across over an IP internetwork.

55. For what purpose would a network administrator use the Nmap tool?

- protection of the private IP addresses of internal hosts
- identification of specific network anomalies
- collection and analysis of security alerts and logs

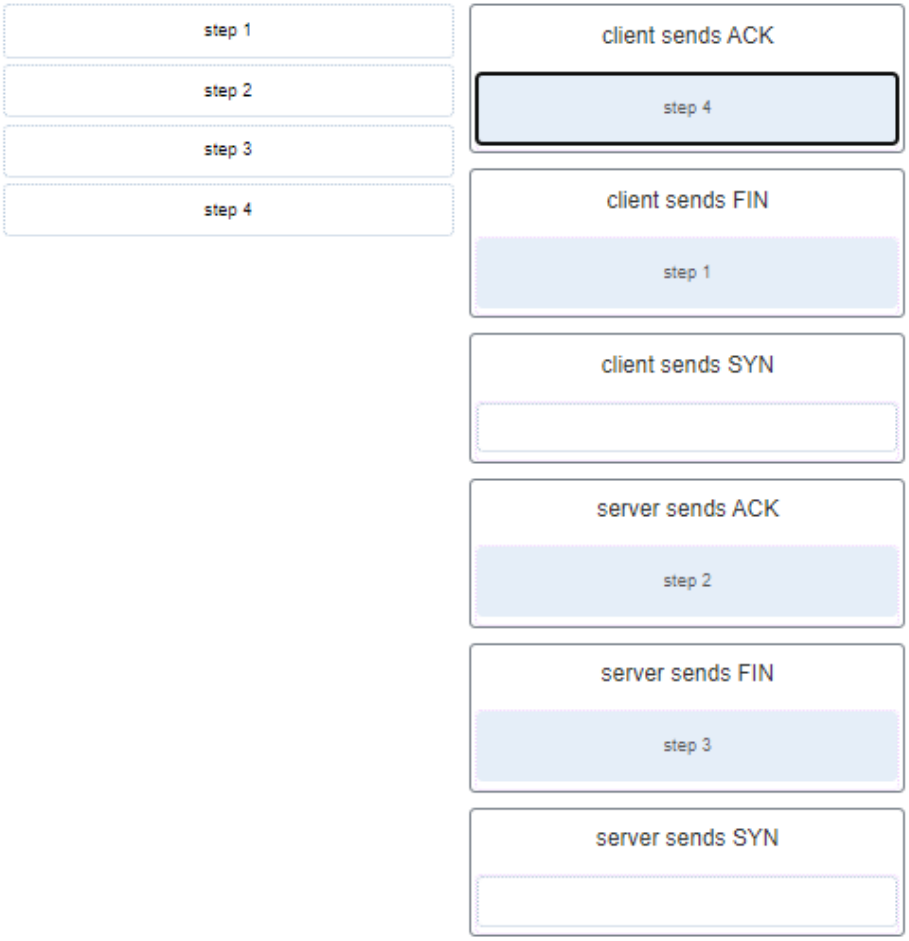
- detection and identification of open ports

56. Match the network service with the description.



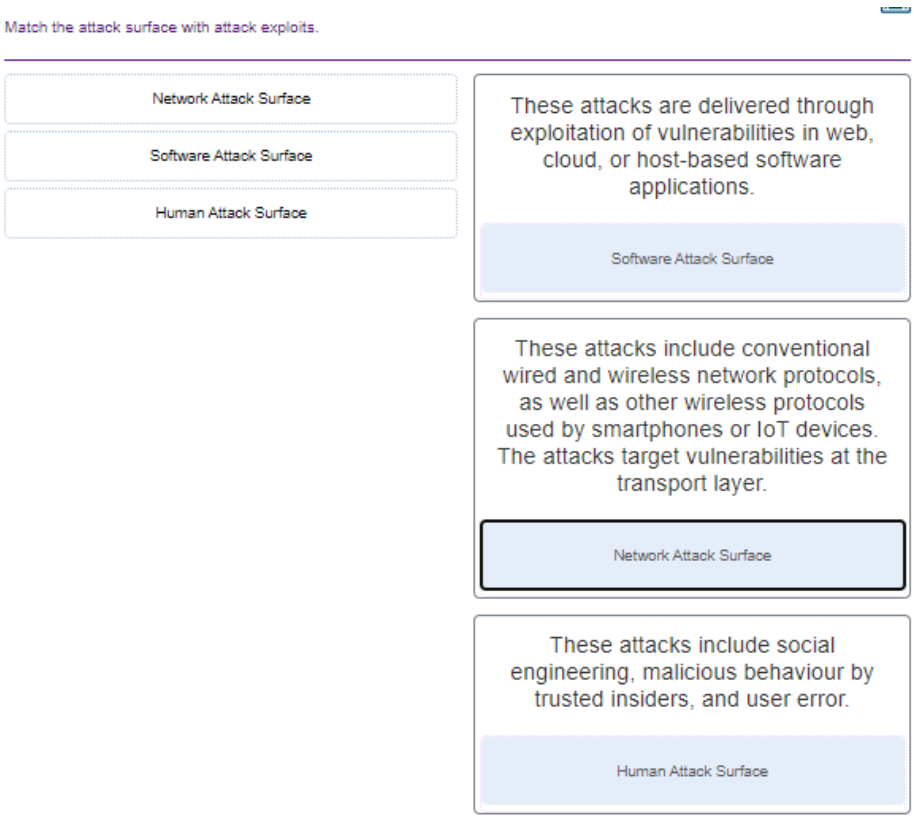
57. A client application needs to terminate a TCP communication session with a server. Place the termination process steps in the order that they will occur. (Nat all options are used.)

A client application needs to terminate a TCP communication session with a server. Place the termination process steps in the order that they will occur. (Not all options are used.)

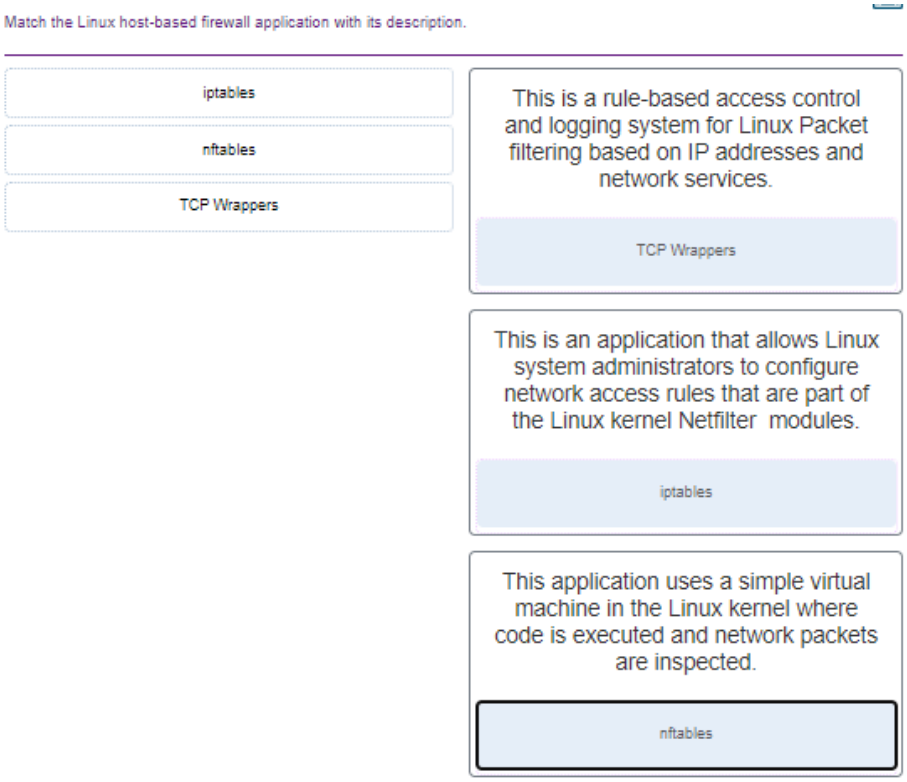


58. Match the attack surface with attack exploits.

Match the attack surface with attack exploits.



59. Match the Linux host-based firewall application with its description.

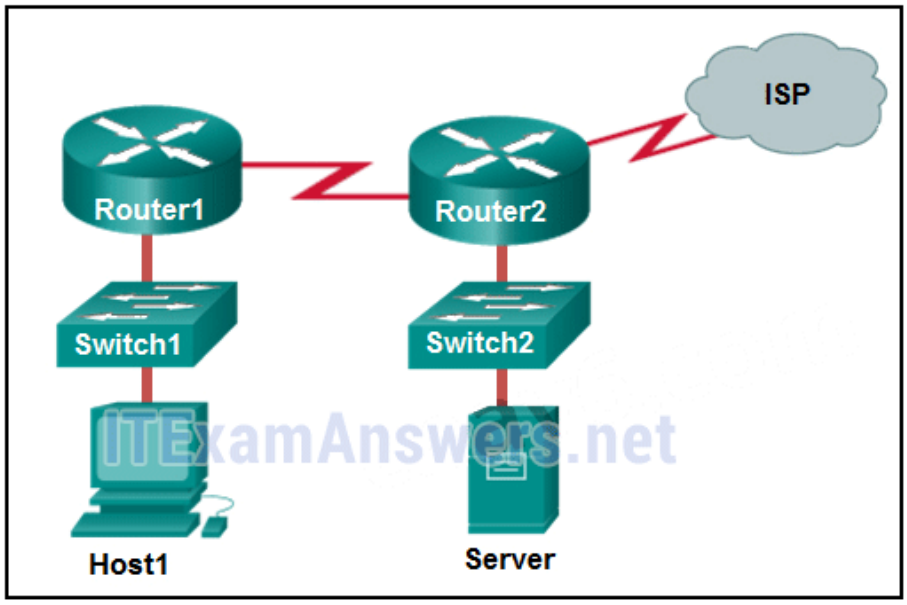


60. What network attack seeks to create a DoS for clients by preventing them from being able to obtain a DHCP lease?

- **DHCP starvation**
- IP address spoofing
- DHCP spoofing
- CAM table attack

Explanation: DCHP starvation attacks are launched by an attacker with the intent to create a DoS for DHCP clients. To accomplish this goal, the attacker uses a tool that sends many DHCPDISCOVER messages in order to lease the entire pool of available IP addresses, thus denying them to legitimate hosts.

61. Refer to the exhibit. If Host1 were to transfer a file to the server, what layers of the TCP/IP model would be used?



- only application and Internet layers
- **application, transport, Internet, and network access layers**
- only Internet and network access layers
- only application, transport, network, data link, and physical layers
- only application, Internet, and network access layers
- application, session, transport, network, data link, and physical layers

Explanation: The TCP/IP model contains the application, transport, internet, and network access layers. A file transfer uses the FTP application layer protocol. The data would move from the application layer through all of the layers of the model and across the network to the file server.

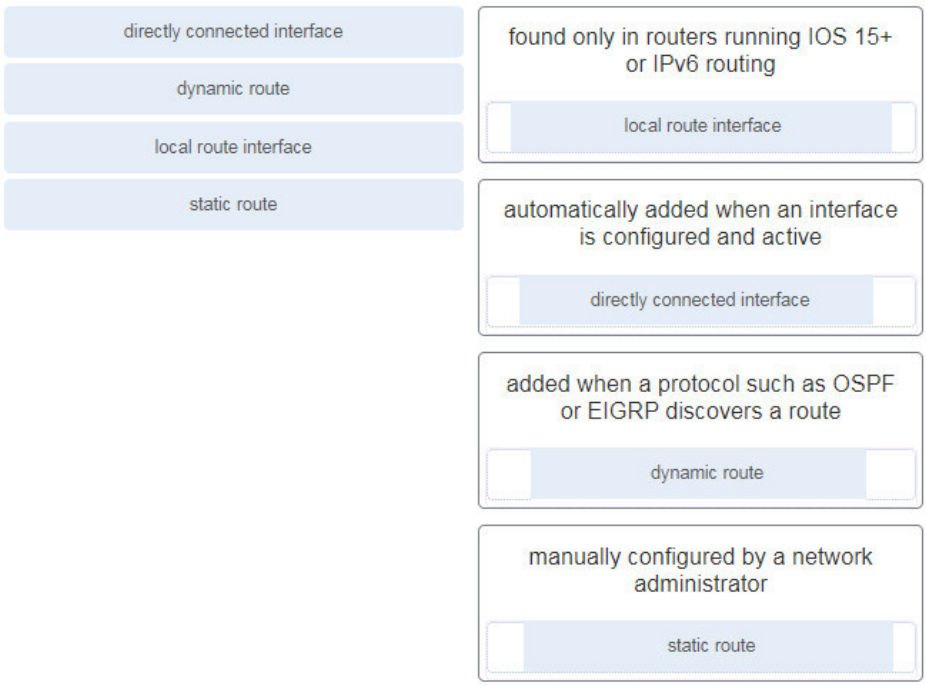
62. A company has a file server that shares a folder named Public. The network security policy specifies that the Public folder is assigned Read-Only rights to anyone who can log into the server while the Edit rights are assigned only to the network admin group. Which component is addressed in the AAA network service framework?

- automation
- authentication

- **authorization**
- accounting

Explanation: After a user is successfully authenticated (logged into the server), the authorization is the process of determining what network resources the user can access and what operations (such as read or edit) the user can perform.

63. Match the destination network routing table entry type with a defintion.



64. A person coming to a cafe for the first time wants to gain wireless access to the Internet using a laptop. What is the first step the wireless client will do in order to communicate over the network using a wireless management frame?

- associate with the AP
- authenticate to the AP
- **discover the AP**
- agree with the AP on the payload

Explanation: In order for wireless devices to communicate on a wireless network, management frames are used to complete a three-stage process:

Discover the AP
Authenticate with the AP
Associate with the AP

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

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

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.

66. An administrator wants to create four subnetworks from the network address 192.168.1.0/24. What is the network address and subnet mask of the second useable subnet?

subnetwork 192.168.1.64
subnet mask 255.255.255.192

subnetwork 192.168.1.64
subnet mask 255.255.255.240

subnetwork 192.168.1.32
subnet mask 255.255.255.240

subnetwork 192.168.1.128
subnet mask 255.255.255.192

subnetwork 192.168.1.8
subnet mask 255.255.255.224

67. What term describes a set of software tools designed to increase the privileges of a user or to grant access to the user to portions of the operating system that should not normally be allowed?

- compiler

- **rootkit**
- package manager
- penetration testing

Explanation: A rootkit is used by an attacker to secure a backdoor to a compromised computer, grant access to portions of the operating system normally not permitted, or increase the privileges of a user.

68. The IT security personnel of an organization notice that the web server deployed in the DMZ is frequently targeted by threat actors. The decision is made to implement a patch management system to manage the server. Which risk management strategy method is being used to respond to the identified risk?

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

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.

69. What are three characteristics of an information security management system? (Choose three.)

- It involves the implementation of systems that track the location and configuration of networked devices and software across an enterprise.
- **It is a systematic and multilayered approach to cybersecurity.**
- It addresses the inventory and control of hardware and software configurations of systems.

- **It consists of a set of practices that are systematically applied to ensure continuous improvement in information security.**
- **It consists of a management framework through which an organization identifies, analyzes, and addresses information security risks.**
- It is based on the application of servers and security devices.

Explanation: An Information Security Management System (ISMS) consists of a management framework through which an organization identifies, analyzes, and addresses information security risks. ISMSs are not based in servers or security devices. Instead, an ISMS consists of a set of practices that are systematically applied by an organization to ensure continuous improvement in information security. ISMSs provide conceptual models that guide organizations in planning, implementing, governing, and evaluating information security programs.
ISMSs are a natural extension of the use of popular business models, such as Total Quality Management (TQM) and Control Objectives for Information and Related Technologies (COBIT), into the realm of cybersecurity.
An ISMS is a systematic, multi-layered approach to cybersecurity. The approach includes people, processes, technologies, and the cultures in which they interact in a process of risk management.

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

- **event collection, correlation, and analysis**
- **security monitoring**
- user authentication
- proxy service
- intrusion prevention
- **threat intelligence**

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.

71. What part of the URL, http://www.cisco.com/index.html, represents the top-level DNS domain?

- http
- www
- **.com**
- index

Explanation: The components of the URL http://www.cisco.com/index.htm are as follows:
http = protocol
www = part of the server name
cisco = part of the domain name
index = file name
com = the top-level domain

72. What best describes the security threat of spoofing?

- sending bulk email to individuals, lists, or domains with the intention to prevent users from accessing email
- **sending abnormally large amounts of data to a remote server to prevent user access to the server services**
- intercepting traffic between two hosts or inserting false information into traffic between two hosts
- making data appear to come from a source that is not the actual source

73. A newly created company has fifteen Windows 10 computers that need to be installed before the company can open for business. What is a best practice that the technician should implement when configuring the Windows Firewall?

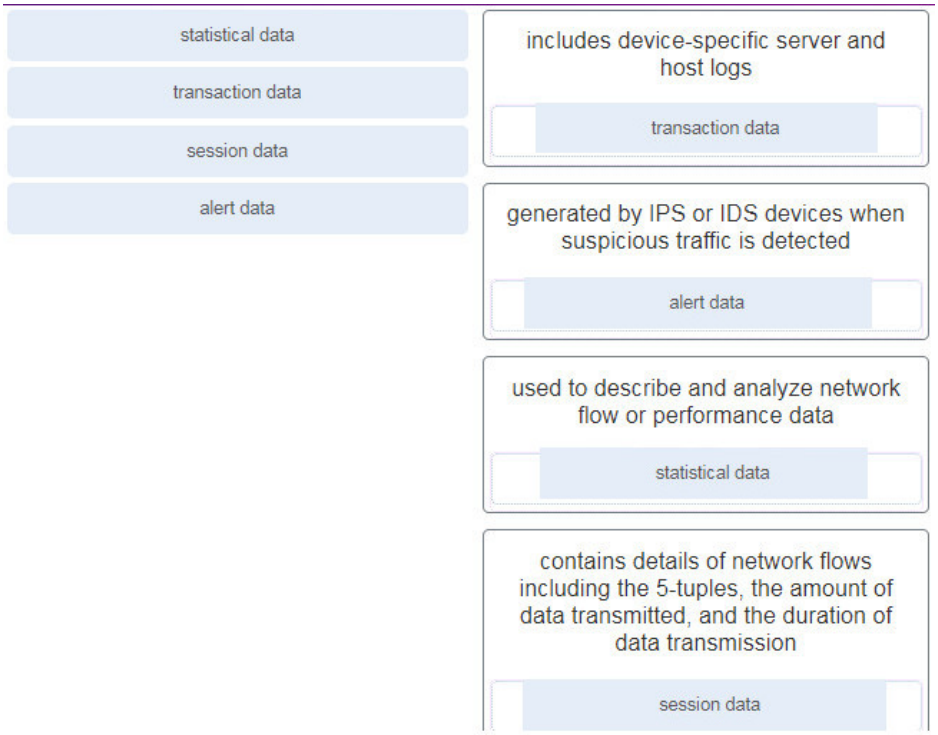
- The technician should remove all default firewall rules and selectively deny traffic from reaching the company network.
- **After implementing third party security software for the company, the technician should verify that the Windows Firewall is disabled.**
- The technician should create instructions for corporate users on how to allow an app through the WIndows Firewall using the Administrator account.
- The technician should enable the Windows Firewall for inbound traffic and install other firewall software for outbound traffic control.

Explanation: Only disable Windows Firewall if other firewall software is installed. Use the Windows Firewall (Windows 7 or 8) or the Windows Defender Firewall (Windows 10) Control Panel to enable or disable the Windows Firewall.

74. Which statement defines the difference between session data and transaction data in logs?

- Session data analyzes network traffic and predicts network behavior, whereas transaction data records network sessions.
- Session data is used to make predictions on network behaviors, whereas transaction data is used to detect network anomalies.
- **Session data records a conversation between hosts, whereas transaction data focuses on the result of network sessions.**
- Session data shows the result of a network session, whereas transaction data is in response to network threat traffic.

75. Match the network monitoring data type with the description.



76. Which device supports the use of SPAN to enable monitoring of malicious activity?

- **Cisco Catalyst switch**
- Cisco IronPort
- Cisco NAC
- Cisco Security Agent

77. Which term is used for describing automated queries that are useful for adding efficiency to the cyberoperations workflow?

- cyber kill chain
- **playbook**
- chain of custody
- rootkit

Explanation: A playbook is an automated query that can add efficiency to the cyberoperations workflow.

78. When ACLs are configured to block IP address spoofing and DoS flood attacks, which ICMP message should be allowed both inbound and outbound?

- echo reply
- unreachable
- source quench

- **echo**

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

- It can identify how the malware originally entered the network.
- **A retrospective analysis can help in tracking the behavior of the malware from the identification point forward.**
- 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.

80. Which two data types would be classified as personally identifiable information (PII)? (Choose two.)

- house thermostat reading
- average number of cattle per region
- **vehicle identification number**
- hospital emergency use per region
- **Facebook photographs**

81. A help desk technician notices an increased number of calls relating to the performance of computers located at the manufacturing plant. The technician believes that botnets are causing the issue. What are two purposes of botnets? (Choose two.)

- **to transmit viruses or spam to computers on the same network**
- to record any and all keystrokes
- **to attack other computers**
- to withhold access to a computer or files until money has been paid
- to gain access to the restricted part of the operating system

Explanation: Botnets can be used to perform DDoS attacks, obtain data, or transmit malware to other devices on the network.

82. Which two statements describe the use of asymmetric algorithms? (Choose two.)

- Public and private keys may be used interchangeably.
- **If a public key is used to encrypt the data, a private key must be used to decrypt the data.**
- If a public key is used to encrypt the data, a public key must be used to decrypt the data.
- **If a private key is used to encrypt the data, a public key must be used to decrypt the data.**
- If a private key is used to encrypt the data, a private key must be used to decrypt the data.

Explanation: Asymmetric algorithms use two keys: a public key and a private key. Both keys are capable of the encryption process, but the complementary matched key is required for decryption. If a public key encrypts the data, the matching private key decrypts the data. The opposite is also true. If a private key encrypts the data, the corresponding public key decrypts the data.

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

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

84. What are two methods to maintain certificate revocation status? (Choose two.)

- **CRL**
- DNS
- subordinate CA
- **OCSP**

- LDAP

Explanation: A digital certificate might need to be revoked if its key is compromised or it is no longer needed. The certificate revocation list (CRL) and Online Certificate Status Protocol (OCSP), are two common methods to check a certificate revocation status.

85. What are two uses of an access control list? (Choose two.)

- **ACLs provide a basic level of security for network access.**
- **ACLs can control which areas a host can access on a network.**
- Standard ACLs can restrict access to specific applications and ports.
- ACLs assist the router in determining the best path to a destination.
- ACLs can permit or deny traffic based upon the MAC address originating on the router.

Explanation: ACLs can be used for the following:Limit network traffic in order to provide adequate network performance
Restrict the delivery of routing updates
Provide a basic level of security
Filter traffic based on the type of traffic being sent
Filter traffic based on IP addressing

86. A client is using SLAAC to obtain an IPv6 address for the interface. After an address has been generated and applied to the interface, what must the client do before it can begin to use this IPv6 address?

- It must send an ICMPv6 Router Solicitation message to determine what default gateway it should use.
- It must send an ICMPv6 Router Solicitation message to request the address of the DNS server.
- **It must send an ICMPv6 Neighbor Solicitation message to ensure that the address is not already in**

use on the network.

- It must wait for an ICMPv6 Router Advertisement message giving permission to use this address.

Explanation: Stateless DHCPv6 or stateful DHCPv6 uses a DHCP server, but Stateless Address Autoconfiguration (SLAAC) does not. A SLAAC client can automatically generate an address that is based on information from local routers via Router Advertisement (RA) messages. Once an address has been assigned to an interface via SLAAC, the client must ensure via Duplicate Address Detection (DAD) that the address is not already in use. It does this by sending out an ICMPv6 Neighbor Solicitation message and listening for a response. If a response is received, then it means that another device is already using this address.

87. A technician is troubleshooting a network connectivity problem. Pings to the local wireless router are successful but pings to a server on the Internet are unsuccessful. Which CLI command could assist the technician to find the location of the networking problem?

- **tracert**
- ipconfig
- msconfig
- ipconfig/renew

Explanation: The tracert utlility (also known as the tracert command or tracert tool) will enable the technician to locate the link to the server that is down. The ipconfig command displays the computer network configuration details. The ipconfig/renew command requests an IP address from a DHCP server. Msconfig is not a network troubleshooting command.

88. What are two evasion techniques that are used by hackers? (Choose two.)

- Trojan horse

- **pivot**
- **rootkit**
- reconnaissance
- phishing

Explanation: The following methods are used by hackers to avoid detection:Encryption and tunneling – hide or scramble the malware content
Resource exhaustion – keeps the host device too busy to detect the invasion
Traffic fragmentation – splits the malware into multiple packets
Protocol-level misinterpretation – sneaks by the firewall
Pivot – uses a compromised network device to attempt access to another device
Rootkit – allows the hacker to be undetected and hides software installed by the hacker

89. When a security attack has occurred, which two approaches should security professionals take to mitigate a compromised system during the Actions on Objectives step as defined by the Cyber Kill Chain model? (Choose two.)

- **Perform forensic analysis of endpoints for rapid triage.**
- Train web developers for securing code.
- Build detections for the behavior of known malware.
- Collect malware files and metadata for future analysis.
- **Detect data exfiltration, lateral movement, and unauthorized credential usage.**

Explanation: When security professionals are alerted about the system compromises, forensic analysis of endpoints should be performed immediately for rapid triage. In addition, detection efforts for further attacking activities such as data exfiltration, lateral movement, and unauthorized credential usage should be enhanced to reduce damage to the minimum.

90. Place the seven steps defined in the Cyber Kill Chain in the correct order.

What are three goals of a port scan attack? (Choose three.)

- to identify peripheral configurations
- **to determine potential vulnerabilities**
- to disable used ports and services
- **to identify operating systems**
- **to identify active services**
- to discover system passwords

91. Which field in the TCP header indicates the status of the three-way handshake process?

- **control bits**
- window
- reserved
- checksum

Explanation: The value in the control bits field of theTCP header indicates the progress and status of the connection.

92. A user opens three browsers on the same PC to access www.cisco.com to search for certification course information. The Cisco web server sends a datagram as a reply to the request from one of the web browsers. Which information is used by the TCP/IP protocol stack in the PC to identify which of the three web browsers should receive the reply?

- the source IP address
- **the destination port number**
- the destination IP address
- the source port number

Explanation: Each web browser client application opens a randomly generated port number in the range of the registered ports and uses this number as the source port number in the datagram that it sends to a server. The server then uses this port number as the destination port number in the reply datagram that it sends to the web browser. The PC that is running the web browser application receives the datagram and uses the destination port number that is contained in this datagram to identify the client application.

93. What are two scenarios where probabilistic security analysis is best suited? (Choose two.)

- when applications that conform to application/networking standards are analyzed
- **when analyzing events with the assumption that they follow predefined steps**
- when random variables create difficulty in knowing with certainty the outcome of any given event
- **when analyzing applications designed to circumvent firewalls**
- when each event is the inevitable result of antecedent causes

94. Which tool is a web application that provides the cybersecurity analyst an easy-to-read means of viewing an entire Layer 4 session?

- Snort
- Zeek
- **CapME**
- OSSEC

95. Match the category of attacks with the description. (Not all options are used.)

96. What are two characteristics of the SLAAC method for IPv6 address configuration? (Choose two.)

- **The default gateway of an IPv6 client on a LAN will be the link-local address of the router interface attached to the LAN.**
- This stateful method of acquiring an IPv6 address requires at least one DHCPv6 server.
- Clients send router advertisement messages to routers to request IPv6 addressing.

- **IPv6 addressing is dynamically assigned to clients through the use of ICMPv6.**
- Router solicitation messages are sent by the router to offer IPv6 addressing to clients.

97. A technician notices that an application is not responding to commands and that the computer seems to respond slowly when applications are opened. What is the best administrative tool to force the release of system resources from the unresponsive application?

- Event Viewer
- System Restore
- Add or Remove Programs
- **Task Manager**

Explanation: Use the Task Manager Performance tab to see a visual representation of CPU and RAM utilization. This is helpful in determining if more memory is needed. Use the Applications tab to halt an application that is not responding.

98. How can statistical data be used to describe or predict network behavior?

- **by comparing normal network behavior to current network behavior**
- by recording conversations between network endpoints
- by listing results of user web surfing activities
- by displaying alert messages that are generated by Snort

Explanation: Statistical data is created through the analysis of other forms of network data. Statistical characteristics of normal network behavior can be compared to current network traffic in an effort to detect anomalies. Conclusions resulting from analysis can be used to describe or predict network behavior.

99. Which metric in the CVSS Base Metric Group is used with an attack vector?

- **the proximity of the threat actor to the vulnerability**

- the presence or absence of the requirement for user interaction in order for an exploit to be successful
- the determination whether the initial authority changes to a second authority during the exploit
- the number of components, software, hardware, or networks, that are beyond the control of the attacker and that must be present in order for a vulnerability to be successfully exploited

Explanation: This is a metric that reflects the proximity of the threat actor to the vulnerable component. The more remote the threat actor is to the component, the higher the severity. Threat actors close to your network or inside your network are easier to detect and mitigate.

100. Which NIST Cybersecurity Framework core function is concerned with the development and implementation of safeguards that ensure the delivery of critical infrastructure services?

- respond
- detect
- identify
- recover
- **protect**

101. Which two techniques are used in a smurf attack? (Choose two.)

- session hijacking
- resource exhaustion
- botnets
- **amplification**
- **reflection**

102. What is the primary objective of a threat intelligence platform (TIP)?

- to aggregate the data in one place and present it in a comprehensible and usable format
- to provide a specification for an application layer protocol that allows the communication of CTI over HTTPS
- to provide a standardized schema for specifying, capturing, characterizing, and communicating events and

properties of network operations

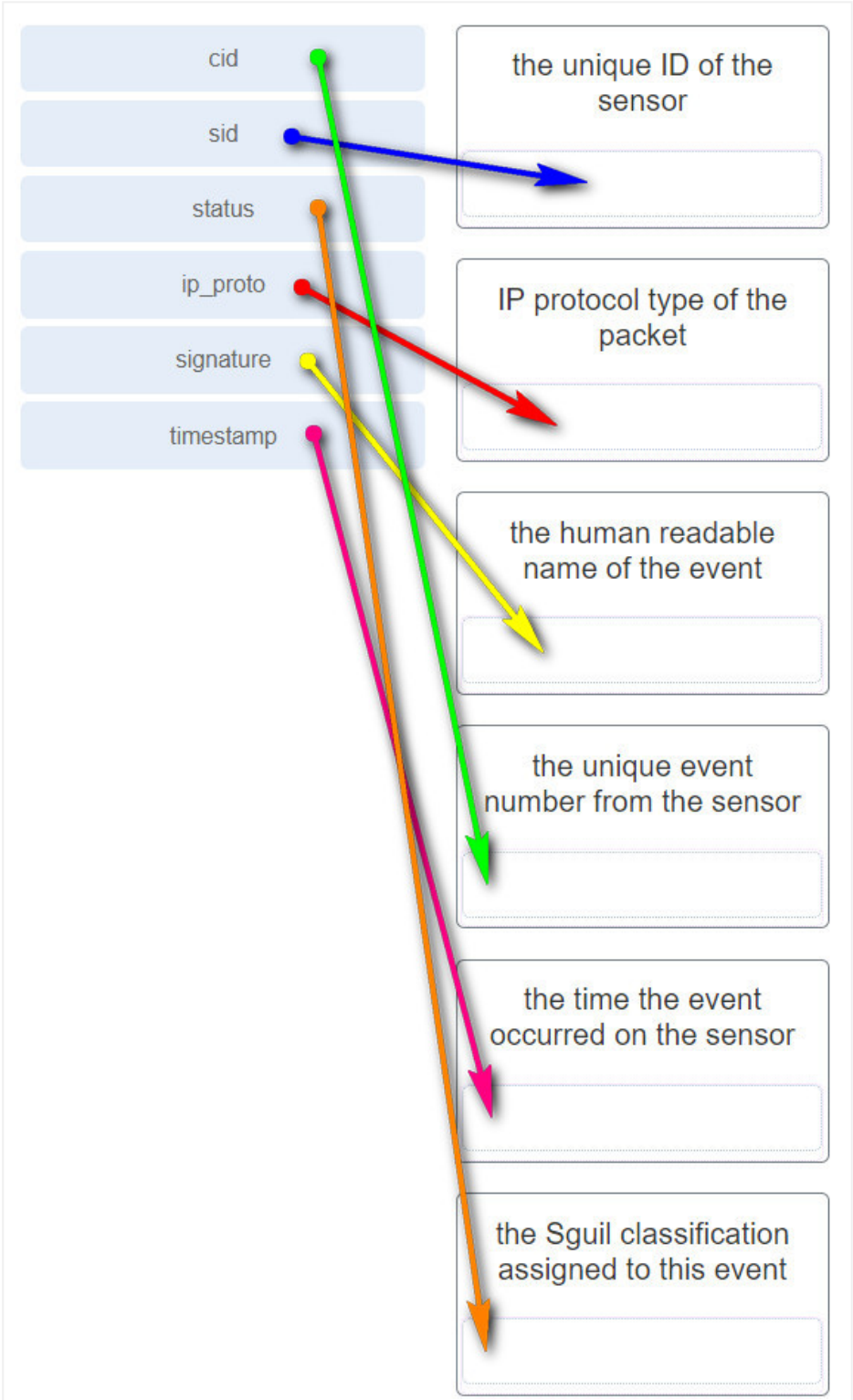
- **to provide a security operations platform that integrates and enhances diverse security tools and threat intelligence**

103. Which wireless parameter is used by an access point to broadcast frames that include the SSID?

- security mode
- active mode
- **passive mode**
- channel setting

Explanation: The two scanning or probing modes an access point can be placed into are passive or active. In passive mode, the AP advertises the SSID, supported standards, and security settings in broadcast beacon frames. In active mode, the wireless client must be manually configured for the same wireless parameters as the AP has configured.

104. Match the field in the Event table of Sguil to the description.



Match the field in the Event table of Sguil to the description

105. 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
- denial of service
- spoofing

106. What information is required for a WHOIS query?

- outside global address of the client
- ICANN lookup server address
- link-local address of the domain owner
- **FQDN of the domain**

107. Which two statements describe the characteristics of symmetric algorithms? (Choose two.)

- **They are referred to as a pre-shared key or secret key.**
- They use a pair of a public key and a private key.
- **They are commonly used with VPN traffic.**
- They provide confidentiality, integrity, and availability.

Explanation: Symmetric encryption algorithms use the same key (also called shared secret) to encrypt and decrypt the data. In contrast, asymmetric encryption algorithms use a pair of keys, one for encryption and another for decryption.

108. What are two drawbacks to using HIPS? (Choose two.)

- With HIPS, the success or failure of an attack cannot be readily determined.
- **With HIPS, the network administrator must verify support for all the different operating systems used inthe network.**
- **HIPS has difficulty constructing an accurate network picture or coordinating events that occur across the entire network.**
- If the network traffic stream is encrypted, HIPS is unable to access unencrypted forms of the traffic.
- HIPS installations are vulnerable to fragmentation attacks or variable TTL attacks

109. What are three functions provided by the syslog service? (Choose three.)

- **to select the type of logging information that is captured**
- to periodically poll agents for data
- to provide statistics on packets that are flowing through a Cisco device
- to provide traffic analysis
- **to gather logging information for monitoring and troubleshooting**
- **to specify the destinations of captured messages**

Explanation: There are three primary functions provided by the syslog service:

1. gathering logging information
2. selection of the type of information to be logged
3. selection of the destination of the logged information

110. Which consideration is important when implementing syslog in a network?

- Enable the highest level of syslog available to ensure logging of all possible event messages.
- **Synchronize clocks on all network devices with a protocol such as Network Time Protocol.**
- Log all messages to the system buffer so that they can be displayed when accessing the router.
- Use SSH to access syslog information

111. What are the two ways threat actors use NTP? (Choose two.)

- They place an attachment inside an email message.
- **They attack the NTP infrastructure in order to corrupt the information used to log the attack.**
- They place iFrames on a frequently used corporate web page.
- They encode stolen data as the subdomain portion where the nameserver is under control of an attacker.
- **Threat actors use NTP systems to direct DDoS attacks.**

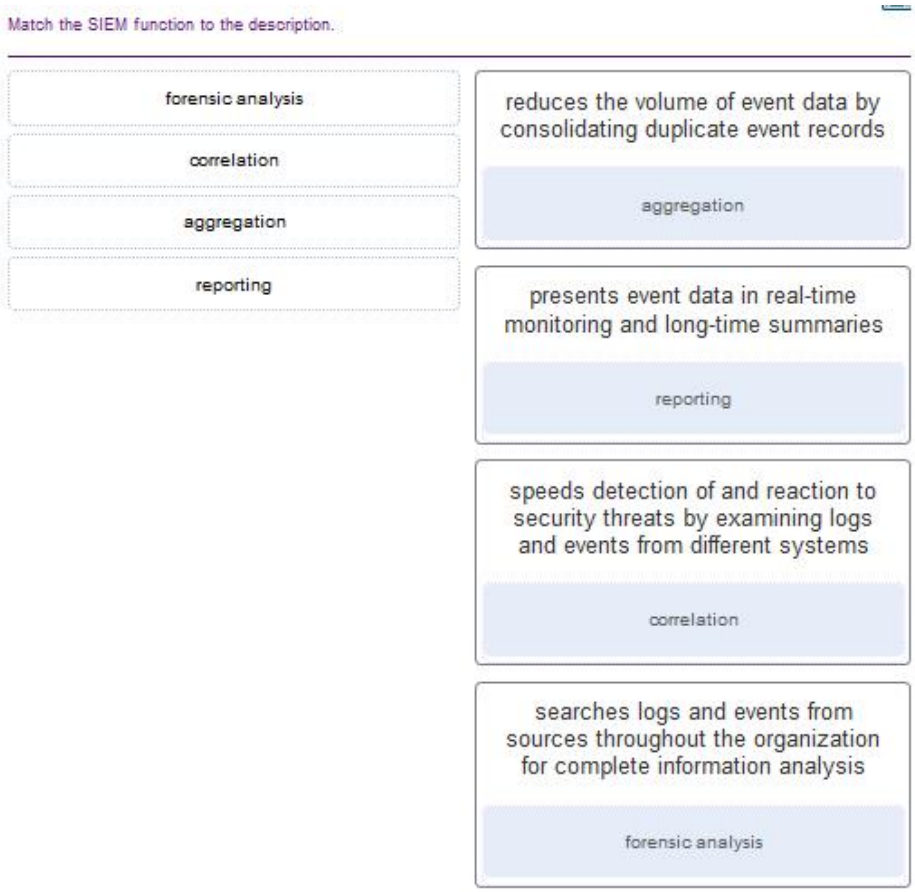
112. Which two features are included by both TACACS+ and RADIUS protocols? (Choose two.)

- password encryption

- **separate authentication and authorization processes**
- SIP support
- **utilization of transport layer protocols**
- 802.1X support

Explanation: Both TACACS+ and RADIUS support password encryption (TACACS+ encrypts all communication) and use Layer 4 protocol (TACACS+ uses TCP and RADIUS uses UDP). TACACS+ supports separation of authentication and authorization processes, while RADIUS combines authentication and authorization as one process. RADIUS supports remote access technology, such as 802.1x and SIP; TACACS+ does not.

113. Match the SIEM function to the description.



114. What are two types of attacks used on DNS open resolvers? (Choose two.)

- **amplification and reflection**
- fast flux

- ARP poisoning
- **resource utilization**
- cushioning

Explanation: Three types of attacks used on DNS open resolvers are as follows:DNS cache poisoning – attacker sends spoofed falsified information to redirect users from legitimate sites to malicious sites
DNS amplification and reflection attacks – attacker sends an increased volume of attacks to mask the true source of the attack
DNS resource utilization attacks – a denial of service (DoS) attack that consumes server resources

115. Which host-based firewall uses a three-profile approach to configure the firewall functionality?

- iptables
- Windows Firewall
- **nftables**
- TCP Wrapper

116. Which protocol or service uses UDP for a client-to-server communication and TCP for server-to-server communication?

- HTTP
- FTP
- **DNS**
- SMTP

Explanation: Some applications may use both TCP and UDP. DNS uses UDP when clients send requests to a DNS server, and TCP when two DNS serves directly communicate.

117. What is one difference between the client-server and peer-to-peer network models?

- Only in the client-server model can file transfers occur.
- A data transfer that uses a device serving in a client role requires that a dedicated server be present.

- A peer-to-peer network transfers data faster than a transfer using a client-server network.
- **Every device in a peer-to-peer network can function as a client or a server.**

118. Which statement is correct about network protocols?

- **They define how messages are exchanged between the source and the destination.**
- They all function in the network access layer of TCP/IP.
- They are only required for exchange of messages between devices on remote networks.
- Network protocols define the type of hardware that is used and how it is mounted in racks.

119. Which approach can help block potential malware delivery methods, as described in the Cyber Kill Chain model, on an Internet-faced web server?

- Build detections for the behavior of known malware.
- Collect malware files and metadata for future analysis.
- Audit the web server to forensically determine the origin of exploit.
- **Analyze the infrastructure storage path used for files.**

Explanation: A threat actor may send the weapon through web interfaces to the target server, either in file uploads or coded web requests. By analyzing the infrastructure storage path used for files, security measures can be implemented to monitor and detect malware deliveries through these methods.

120. Which meta-feature element in the Diamond Model classifies the general type of intrusion event?

- phase
- **results**
- methodology
- direction

121. Which Linux command is used to manage processes?

- chrootkit
- ls
- grep
- **kill**

Explanation: The kill command is used to stop, restart, or pause a process. The chrootkit command is used to check the computer for rootkits, a set of software tools that can increase the privilege level of a user or grant access to portions of software normally not allowed. The grep command is used to look for a file or text within a file. The ls command is used to list files, directories, and file information.

122. Which tool can be used in a Cisco AVC system to analyze and present the application analysis data into dashboard reports?

- NetFlow
- NBAR2
- **Prime**
- IPFIX

Explanation: A management and reporting system, such as Cisco Prime, can be used to analyze and present the application analysis data into dashboard reports for use by network monitoring personnel.

123. Which Windows Event Viewer log includes events regarding the operation of drivers, processes, and hardware?

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

By default Windows keeps four types of host logs:

- **Application logs –** events logged by various applications

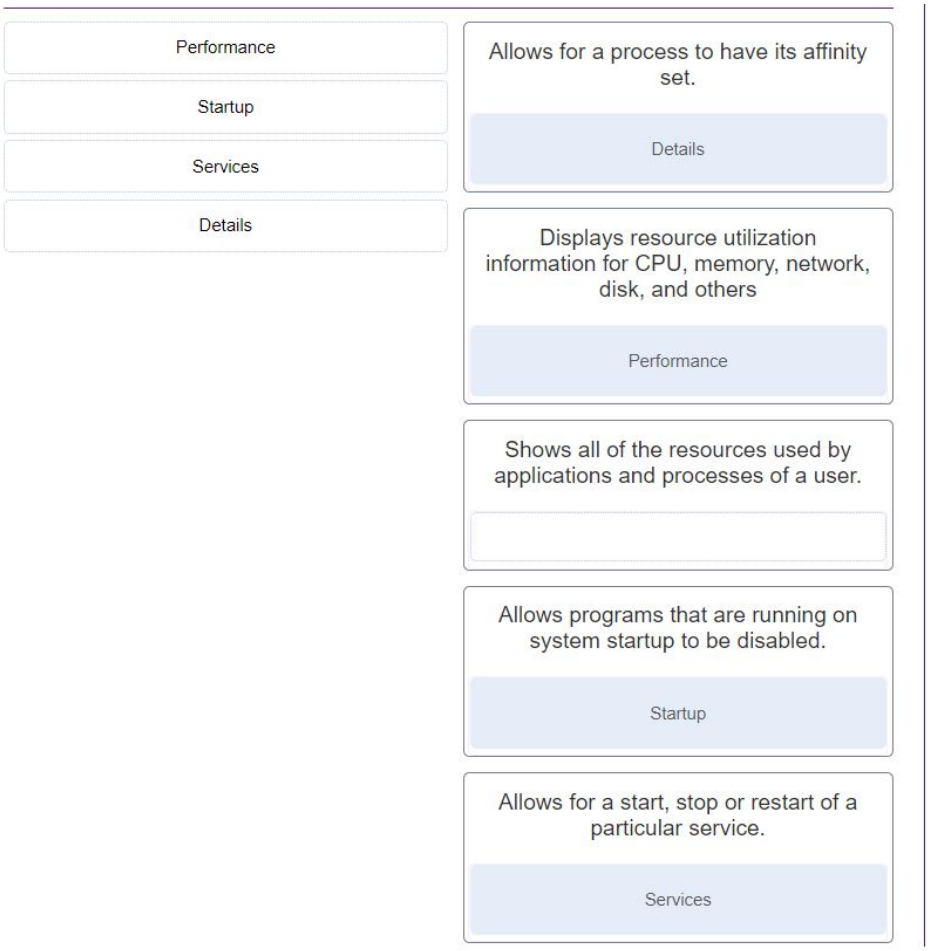
- **System logs –** events about the operation of drivers, processes, and hardware
- **Setup logs –** information about the installation of software, including Windows updates
- **Security logs –** events related to security, such as logon attempts and operations related to file or object management and access

124. Which method is used to make data unreadable to unauthorized users?

- **Encrypt the data.**
- Fragment the data.
- Add a checksum to the end of the data.
- Assign it a username and password.

Explanation: Network data can be encrypted using various cryptography applications so that the data is made unreadable to unauthorized users. Authorized users have the cryptography application so the data can be unencrypted.

125. Match the tabs of the Windows 10 Task Manager to their functions. (Not all options are used.)

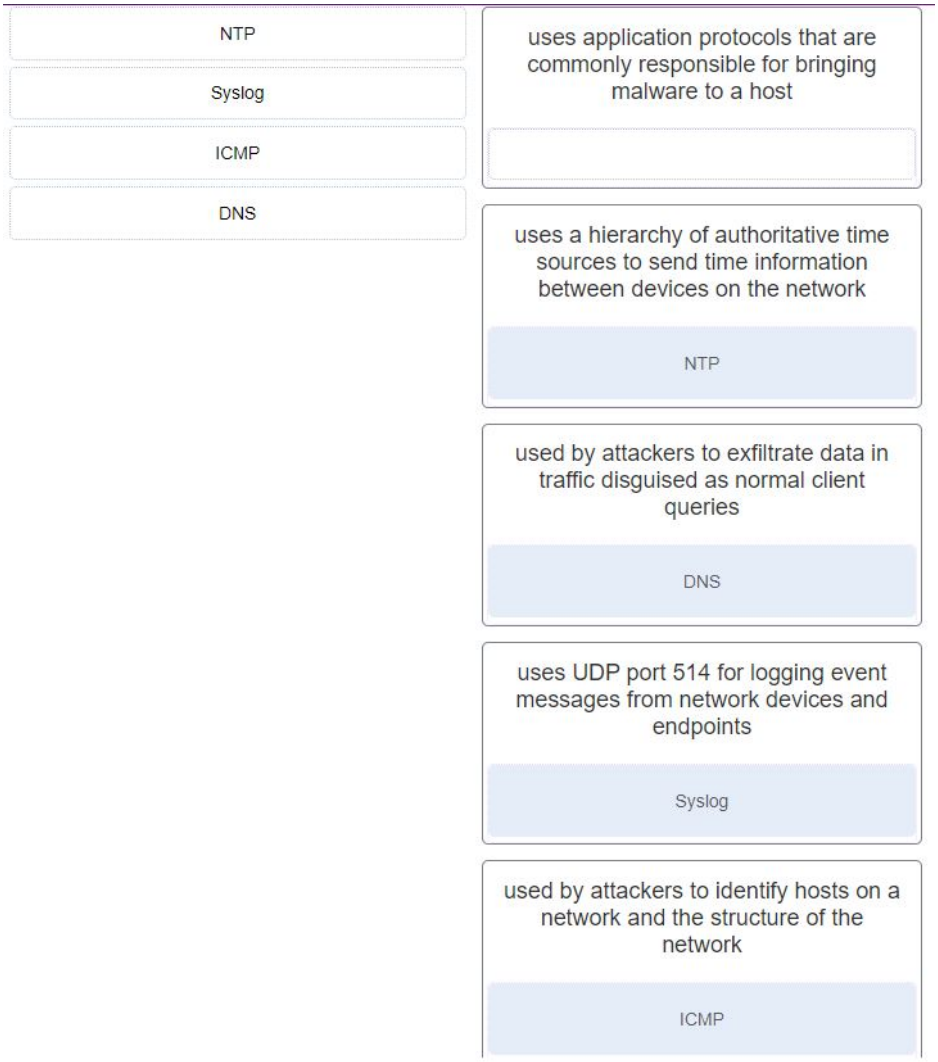


126. For network systems, which management system addresses the inventory and control of hardware and software configurations?

- asset management
- vulnerability management
- risk management
- **configuration management**

Explanation: Configuration management addresses the inventory and control of hardware and software configurations of network systems.

127. Match the common network technology or protocol with the description. (Not all options are used.)



128. What are the three core functions provided by the Security Onion? (Choose three.)

- business continuity planning
- **full packet capture**
- **alert analysis**
- **intrusion detection**
- security device management
- threat containment

Explanation: Security Onion is an open source suite of Network Security Monitoring (NSM) tools for evaluating cybersecurity alerts. For cybersecurity analysts the Security Onion provides full packet capture, network-based and host-based intrusion detection systems, and alert analysis tools.

129. In NAT terms, what address type refers to the globally routable IPv4 address of a destination host on the Internet?

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

Explanation: From the perspective of a NAT device, 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.

130. Which two fields or features does Ethernet examine to determine if a received frame is passed to the data link layer or discarded by the NIC? (Choose two.)

- CEF
- source MAC address
- **minimum frame size**
- auto-MDIX
- **Frame Check Sequence**

131. Which type of data would be considered an example of volatile data?

- web browser cache
- **memory registers**
- log files
- temp files

Explanation: Volatile data is data stored in memory such as registers, cache, and RAM, or it is data that exists in transit. Volatile memory is lost when the computer loses power.

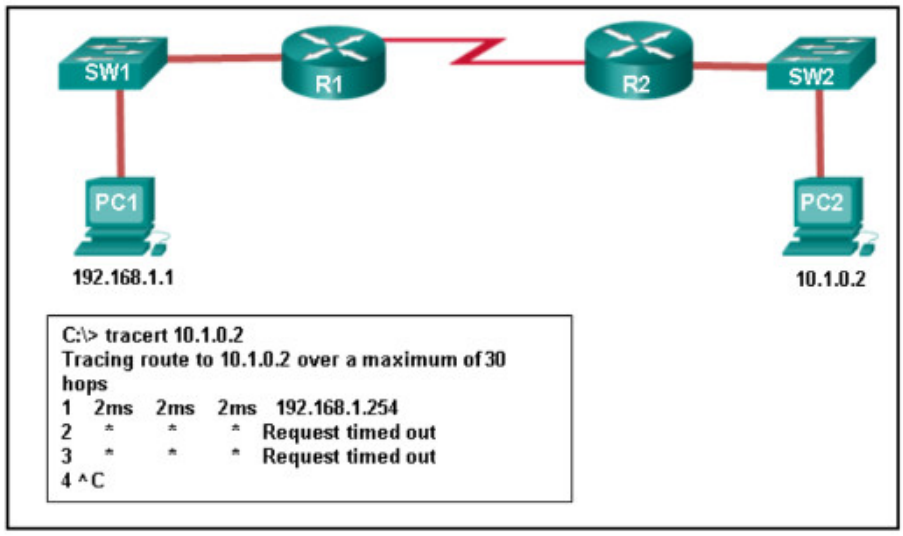
132. What is the main purpose of exploitations by a threat actor through the weapon delivered to a target during the

Cyber Kill Chain exploitation phase?

- Launch a DoS attack.
- Send a message back to a CnC controlled by the threat actor.
- **Break the vulnerability and gain control of the target.**
- Establish a back door into the system.

Explanation: After the weapon has been delivered, the threat actor uses it to break the vulnerability and gain control of the target. The threat actor will use an exploit that gains the effect desired, does it quietly, and avoids detections. Establishing a back door in the target system is the phase of installation.

133. Refer to the exhibit. An administrator is trying to troubleshoot connectivity between PC1 and PC2 and uses the tracert command from PC1 to do it. Based on the displayed output, where should the administrator begin troubleshooting?



CyberOps Associate 1.0 Final exam

- **R1**
- PC2
- SW2
- R2
- SW1

Explanation: Tracert is used to trace the path a packet takes. The only successful response was from the first device along the path on the same LAN as the sending host. The first device is the default gateway on router R1. The administrator should therefore start troubleshooting at R1.

134. What three security tools does Cisco Talos maintain security incident detection rule sets for? (Choose three.)

- **Snort**
- NetStumbler
- Socat
- **SpamCop**
- **ClamAV**

135. Which host-based firewall uses a three-profile approach to configure the firewall functionality?

- **Windows Firewall**
- iptables
- TCP Wrapper
- nftables

Explanation: Windows Firewall uses a profile-based approach to configuring firewall functionality. It uses three profiles, Public, Private, and Domain, to define firewall functions.

136. When a user visits an online store website that uses HTTPS, the user browser queries the CA for a CRL. What is the purpose of this query?

- **to verify the validity of the digital certificate**
- to request the CA self-signed digital certificate
- to check the length of key used for the digital certificate
- to negotiate the best encryption to use

Explanation: A digital certificate must be revoked if it is invalid. CAs maintain a certificate revocation list (CRL), a list of revoked certificate serial numbers that have been

invalidated. The user browser will query the CRL to verify the validity of a certificate.

137. Which step in the Vulnerability Management Life Cycle determines a baseline risk profile to eliminate risks based on asset criticality, vulnerability threat, and asset classification?

- discover
- **assess**
- prioritize assets
- verify

Explanation: The steps in the Vulnerability Management Life Cycle include these:

- Discover – inventory all assets across the network and identify host details, including operating systems and open services, to identify vulnerabilities
- Prioritize assets – categorize assets into groups or business units, and assign a business value to asset groups based on their criticality to business operations
- Assess – determine a baseline risk profile to eliminate risks based on asset criticality, vulnerability threats, and asset classification
- Report – measure the level of business risk associated with assets according to security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities.
- Remediate – prioritize according to business risk and fix vulnerabilities in order of risk
- Verify – verify that threats have been eliminated through follow-up audits

138. Which management system implements systems that track the location and configuration of networked devices and software across an enterprise?

- **asset management**
- vulnerability management
- risk management
- configuration management

Explanation: Asset management involves the implementation of systems that track the location and configuration of networked devices and software across an enterprise.

139. A network administrator is reviewing server alerts because of reports of network slowness. The administrator confirms that an alert was an actual security incident. What is the security alert classification of this type of scenario?

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

140. Which application layer protocol is used to provide file-sharing and print services to Microsoft applications?

- SMTP
- HTTP
- **SMB**
- DHCP

Explanation: SMB is used in Microsoft networking for file-sharing and print services. The Linux operating system provides a method of sharing resources with Microsoft networks by using a version of SMB called SAMBA.

141. Which device in a layered defense-in-depth approach denies connections initiated from untrusted networks to internal networks, but allows internal users within an organization to connect to untrusted networks?

- access layer switch
- **firewall**
- internal router
- IPS

Explanation: A firewall is typically a second line of defense in a layered defense-in-depth approach to

network security. The firewall typically connects to an edge router that connects to the service provider. The firewall tracks connections initiated within the company going out of the company and denies initiation of connections from external untrusted networks going to internal trusted networks.

142. What are two potential network problems that can result from ARP operation? (Choose two.)

- Large numbers of ARP request broadcasts could cause the host MAC address table to overflow and prevent the host from communicating on the network.
- On large networks with low bandwidth, multiple ARP broadcasts could cause data communication delays.
- **Network attackers could manipulate MAC address and IP address mappings in ARP messages with the intent of intercepting network traffic.**
- Multiple ARP replies result in the switch MAC address table containing entries that match the MAC addresses of hosts that are connected to the relevant switch port.
- Manually configuring static ARP associations could facilitate ARP poisoning or MAC address spoofing.

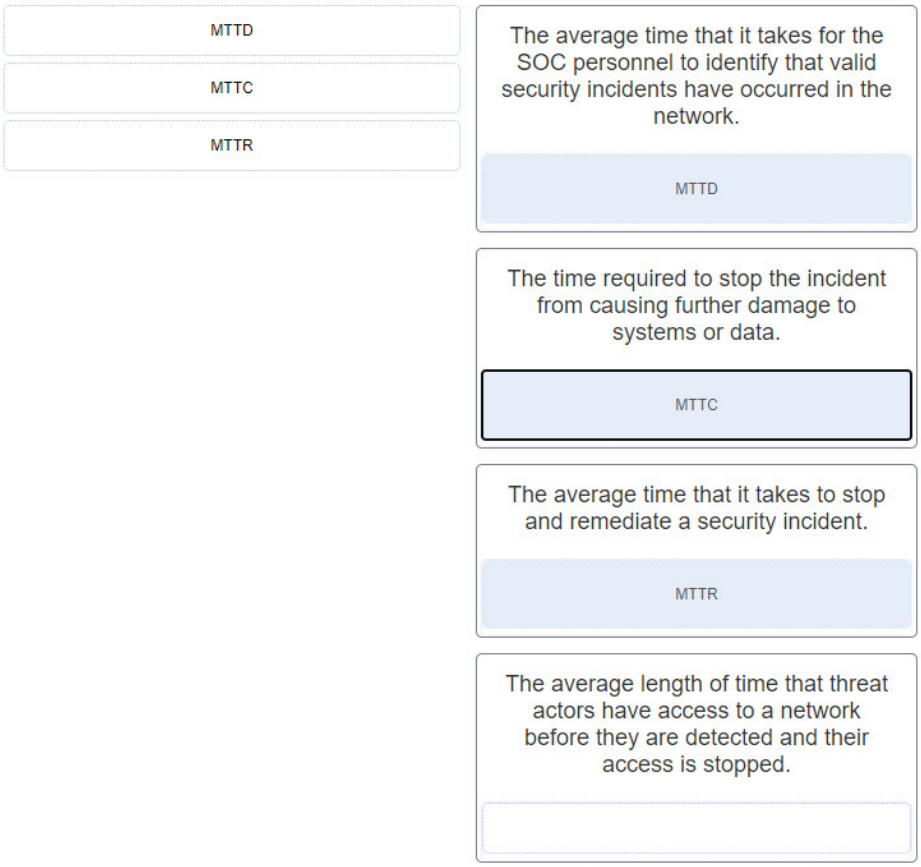
143. Which three procedures in Sguil are provided to security analysts to address alerts? (Choose three.)

- **Escalate an uncertain alert.**
- Correlate similar alerts into a single line.
- **Categorize true positives.**
- Pivot to other information sources and tools.
- Construct queries using Query Builder.
- **Expire false positives.**

Explanation: Sguil is a tool for addressing alerts. Three tasks can be completed in Sguil to manage alerts:

- Alerts that have been found to be false positives can be expired.
- An alert can be escalated if the cybersecurity analyst is uncertain how to handle it.
- Events that have been identified as true positives can be categorized.

144. Match the SOC metric with the description. (Not all options apply.)



145. Which two services are provided by the NetFlow tool? (Choose two.)

- QoS configuration
- **usage-based network billing**
- log analysis
- access list monitoring
- **network monitoring**

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.

146. An administrator discovers that a user is accessing a newly established website that may be detrimental to company security. What action should the administrator take first in terms of the security policy?