

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

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.**

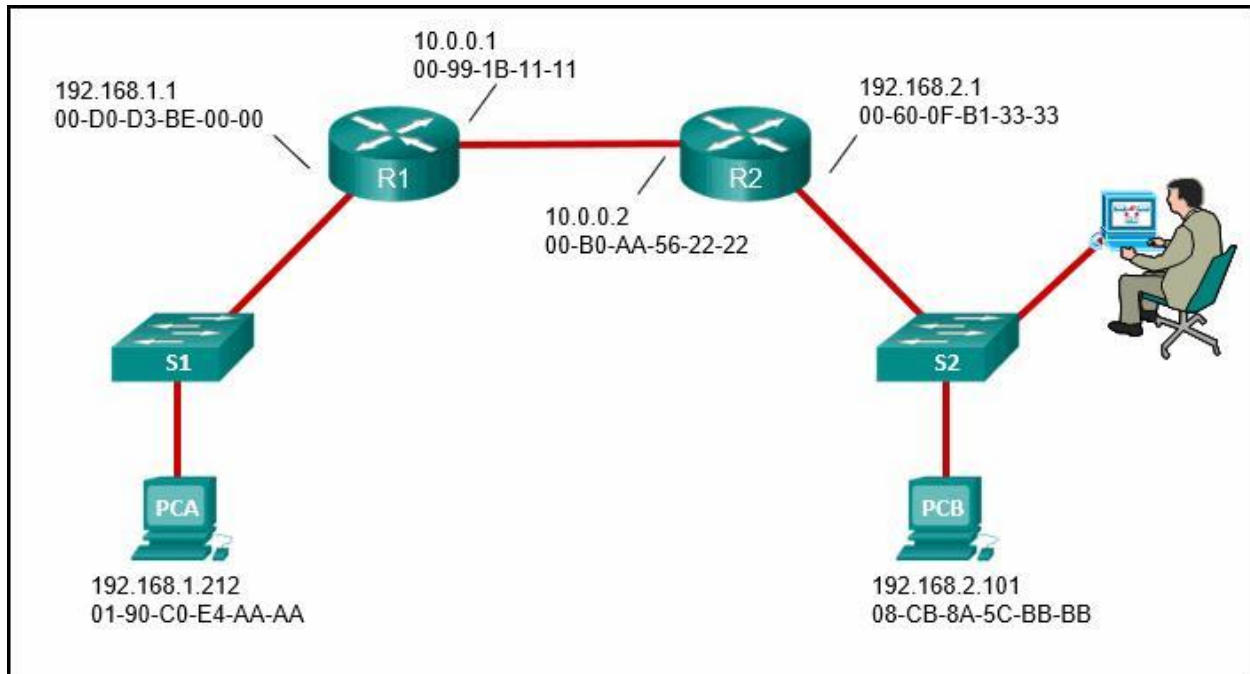
3. What technique is used in social engineering attacks?

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

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.

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?



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

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.

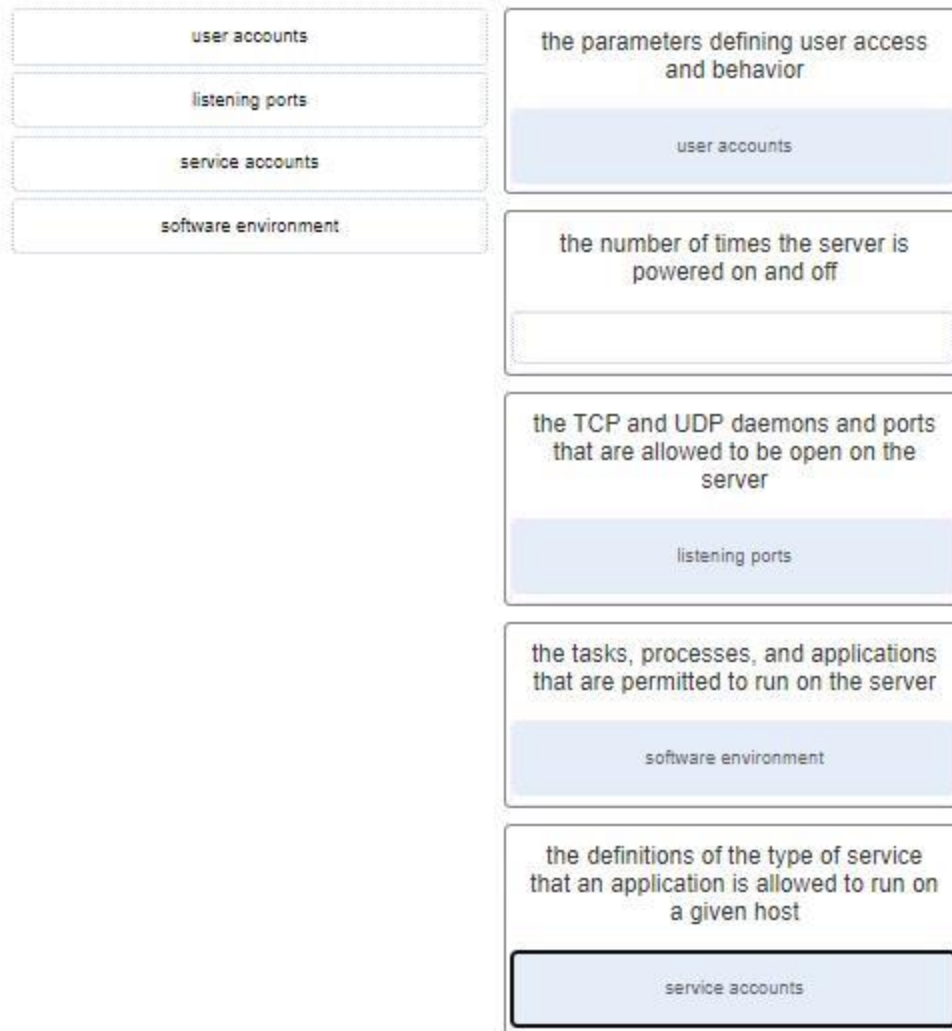
Match the Security Onion tool with the description.

Snort	network-based intrusion detection system
OSSEC	Snort
Sguil	packet capture application
Wireshark	Wireshark
	host-based intrusion detection system
	OSSEC
	high-level cybersecurity analysis console
	Sguil

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.)



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**

12. Match the monitoring tool to the definition.

NetFlow	presents real-time reporting and long-term analysis of security events
Wireshark	
SNMP	SIEM
SIEM	
	provides statistics on packets flowing through a Cisco router or multilayer switch
	NetFlow
	captures packets and saves them in a PCAP file
	Wireshark
	retrieves information on the operation of network devices
	SNMP

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.

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.

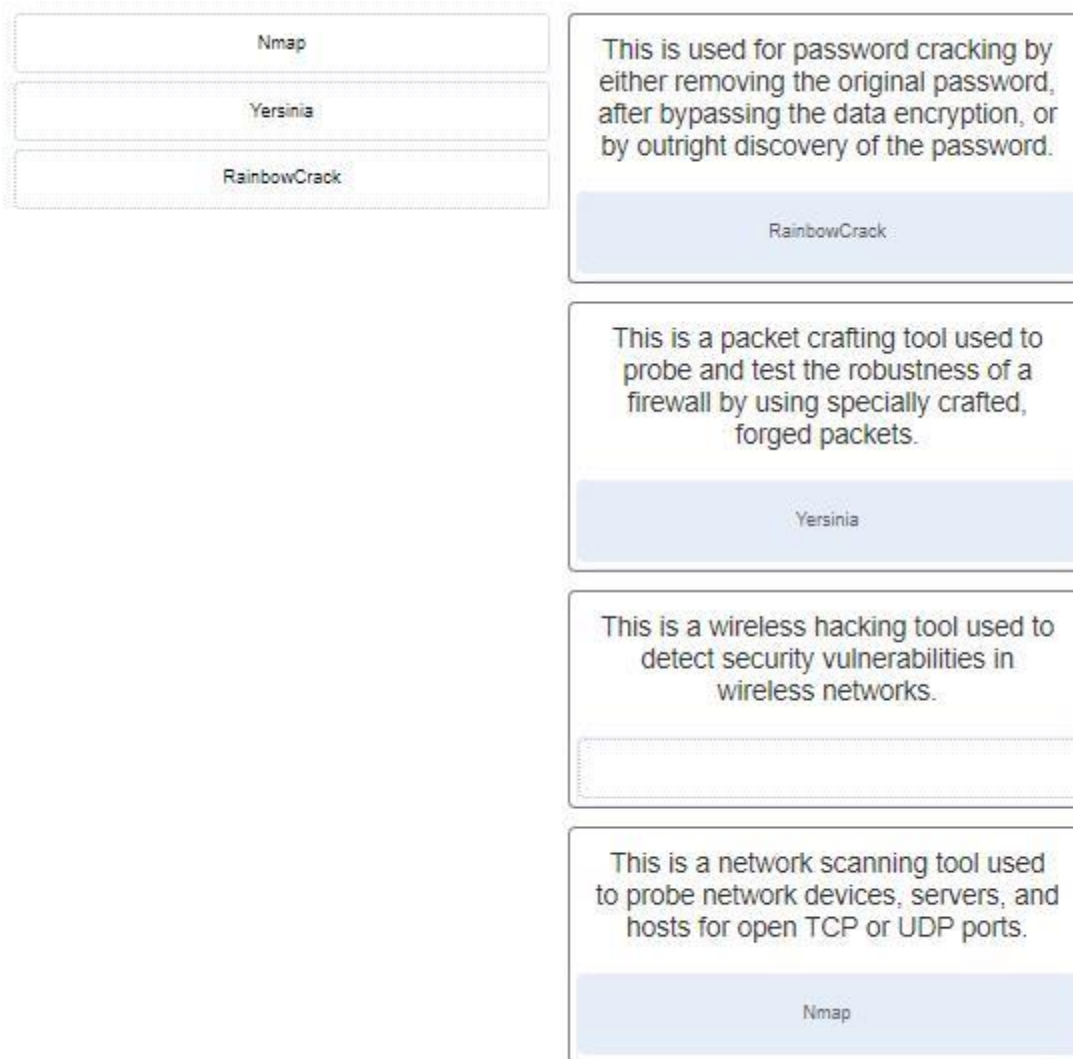
15. What is an advantage for small organizations of adopting IMAP instead of POP?

- 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.**

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.

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

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.**

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

- nfdump
- Wireshark
- NBAR2
- **tcpdump**

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**

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.

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.

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

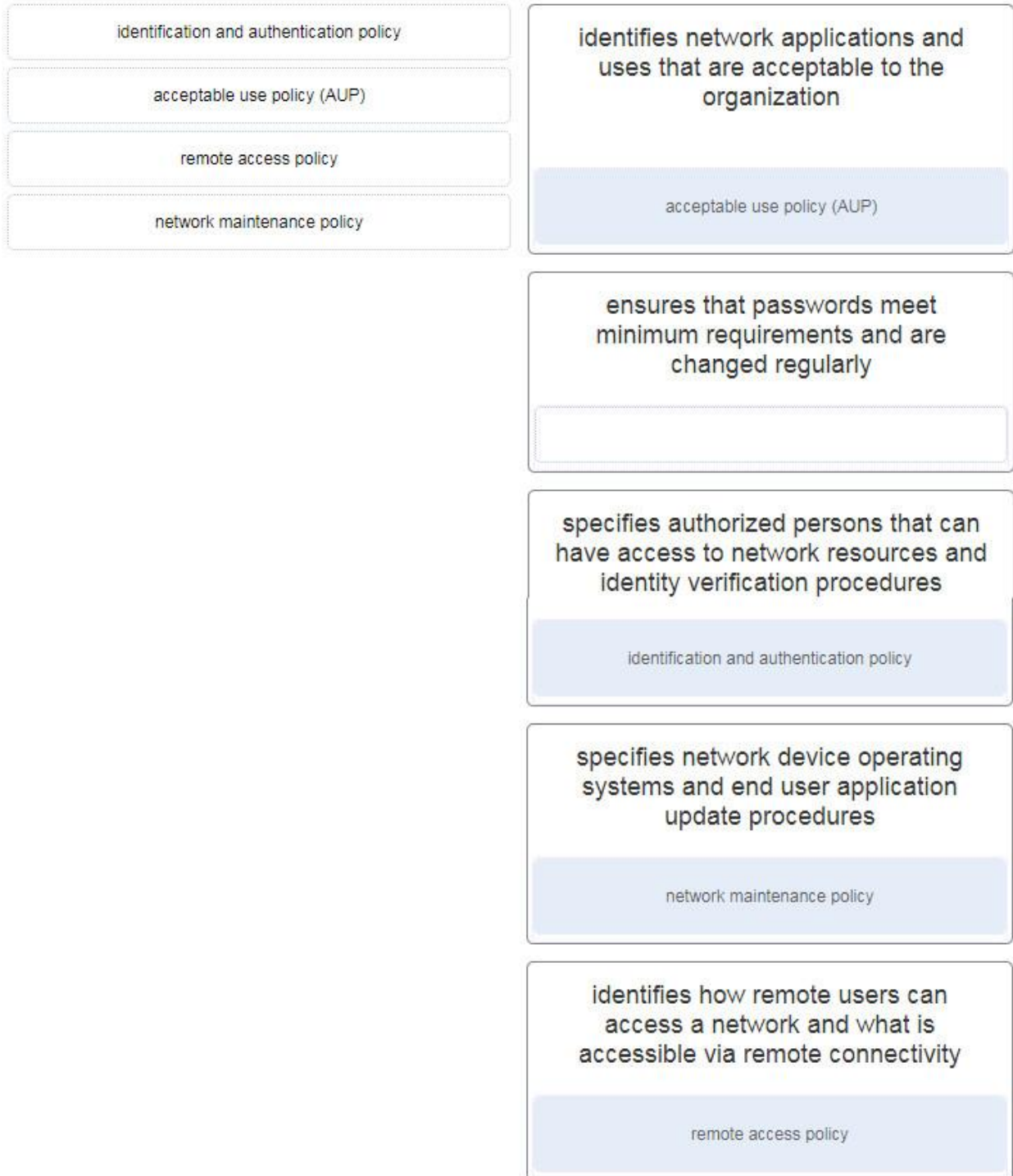
30. Which measure can a security analyst take to perform effective security monitoring against network traffic encrypted by SSL technology?

- 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.)

attacker sends falsified information to redirect users to malicious sites	domain generation
attacker uses open resolvers to increase the volume of attacks and mask the true source of the attack	
attacker sends multiple packets that consume server resources	resource utilization attack
	attacker sends multiple packets that consume server resources
	ARP cache poisoning
	attacker sends falsified information to redirect users to malicious sites
	amplification and reflection
	attacker uses open resolvers to increase the volume of attacks and mask the true source of the attack

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**

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**

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

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

40. Which tool included in the Security Onion is a series of software plugins that send different types of data to the Elasticsearch data stores?

- Curator
- **Beats**
- OSSEC
- ElastAlert

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

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.

management	performs disciplinary measures
IT support	human resources
legal department	changes firewall rules
human resources	information assurance
information assurance	preserves attack evidence
	IT support
	designs the budget
	management
	reviews policies for local or federal guideline violations
	legal department

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

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

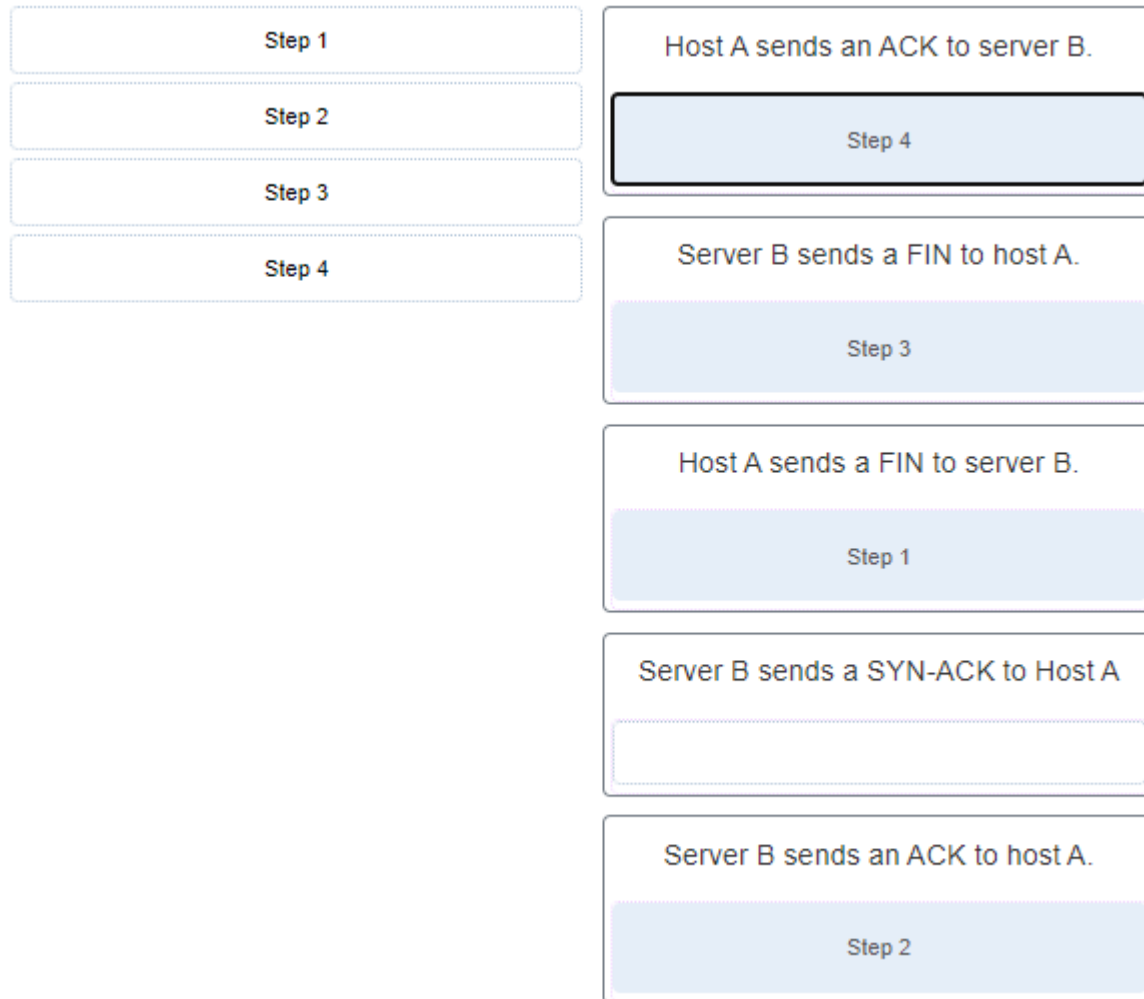
Match the security organization with its security functions. (Not all options are used.)

SANS	It maintains and supports the Internet Storm Center and also develops security courses.
MITRE	
FIRST	SANS
	It maintains a list of common vulnerabilities and exposures (CVE).
	MITRE
	It provides vendor neutral educational products and career services to industry professionals globally.
	It brings together a variety of computer security incident response teams from government, commercial, and educational organizations to foster cooperation and coordination in information sharing, incident prevention and rapid reaction.
	FIRST

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**

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

- **fragment offset**
- protocol
- **flag**
- TTL
- **identification**
- version

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

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

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

HKKEY_LOCAL_MACHINE	all of the configuration settings for the hardware and software configured on the computer for all users
HKEY_CURRENT_USER	
HKEY_CLASSES_ROOT	HKEY_USERS
HKEY_USERS	
HKEY_CURRENT_CONFIG	settings about the file system, file associations, shortcuts used when you ask Windows to run a file, or view a directory
	HKEY_CLASSES_ROOT
	data about the preferences of the currently logged on user, including personalization settings, default devices, and programs, etc
	HKEY_CURRENT_USER
	information about the current hardware profile of the machine
	HKEY_CURRENT_CONFIG

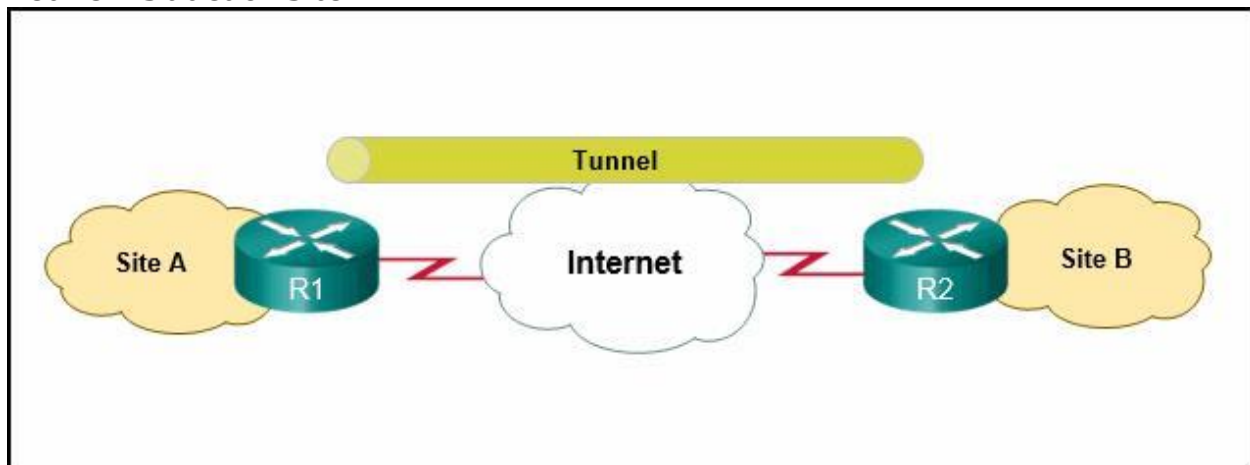
52. Which PDU format is used when bits are received from the network medium by the NIC of a host?

- segment
- file
- packet
- **frame**

53. A user is executing a traceroute 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

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?

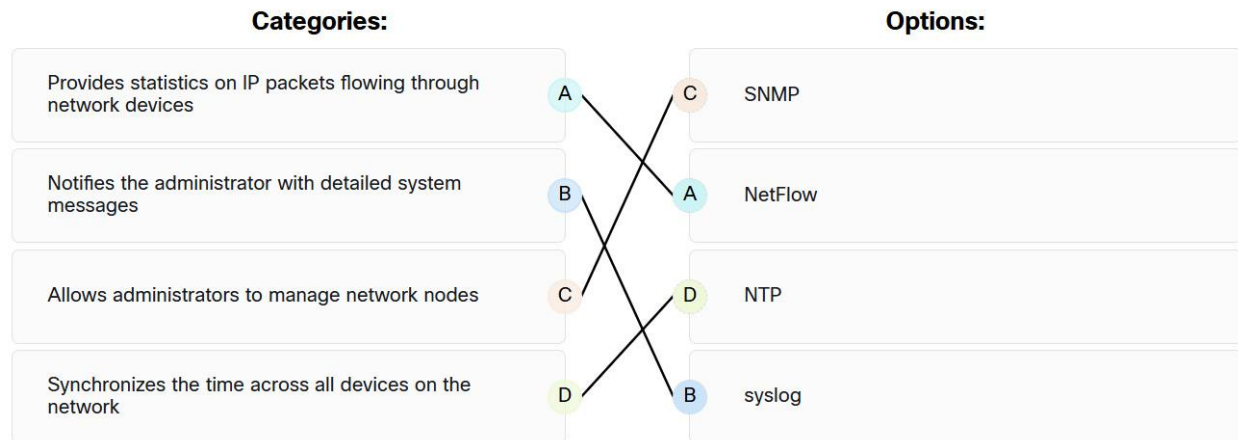


- an IPsec tunnel
- Cisco SSL VPN
- **a GRE tunnel**
- a remote access tunnel

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.



Endpoint Security (ESec) Final Exam Answers 19

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. (Not 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.)

step 1	client sends ACK
step 2	step 4
step 3	client sends FIN
step 4	step 1
	client sends SYN
	server sends ACK
	step 2
	server sends FIN
	step 3
	server sends SYN

58. Match the attack surface with attack exploits.

Match the attack surface with attack exploits.

Network Attack Surface

Software Attack Surface

Human Attack Surface

These attacks are delivered through exploitation of vulnerabilities in web, cloud, or host-based software applications.

Software Attack Surface

These attacks include conventional wired and wireless network protocols, as well as other wireless protocols used by smartphones or IoT devices. The attacks target vulnerabilities at the transport layer.

Network Attack Surface

These attacks include social engineering, malicious behaviour by trusted insiders, and user error.

Human Attack Surface

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

iptables	<p>This is a rule-based access control and logging system for Linux Packet filtering based on IP addresses and network services.</p> <p>TCP Wrappers</p>
nftables	
TCP Wrappers	

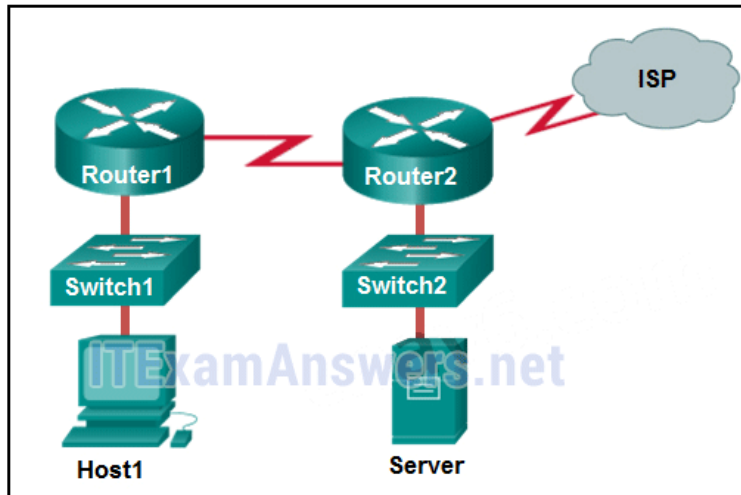
<p>This is an application that allows Linux system administrators to configure network access rules that are part of the Linux kernel Netfilter modules.</p> <p>iptables</p>
--

<p>This application uses a simple virtual machine in the Linux kernel where code is executed and network packets are inspected.</p> <p>nftables</p>

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

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

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

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

directly connected interface	found only in routers running IOS 15+ or IPv6 routing
dynamic route	local route interface
local route interface	automatically added when an interface is configured and active
static route	directly connected interface
	added when a protocol such as OSPF or EIGRP discovers a route
	dynamic route
	manually configured by a network administrator
	static route

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

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

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

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

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.

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**

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

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

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.

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.

statistical data	includes device-specific server and host logs
transaction data	transaction data
session data	generated by IPS or IDS devices when suspicious traffic is detected
alert data	alert data
	used to describe and analyze network flow or performance data
	statistical data
	contains details of network flows including the 5-tuples, the amount of data transmitted, and the duration of data transmission
	session data

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

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.

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

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.

83. 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

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

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

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.

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.

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

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

- Trojan horse
- **pivot**

- **rootkit**
- reconnaissance
- phishing

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.**

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

delivery	Step 1
installation	reconnaissance
exploitation	Step 2
weaponization	weaponization
reconnaissance	Step 3
action on objectives	delivery
command and control	Step 4
	exploitation
	Step 5
	installation
	Step 6
	command and control
	Step 7
	action on objectives

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

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

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

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

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.)

Category	Description
sniffer attack	It can crash applications or network services. It can also flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
MITM	It constructs an IP packet that appears to originate from a valid address inside a corporate network.
DoS	It occurs when threat actors have positioned themselves between a source and a destination and can actively monitor, capture, and control the communication transparently.
	It uses an application or device that can read, monitor, and capture network data exchanges and read network packets.

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**

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

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

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**

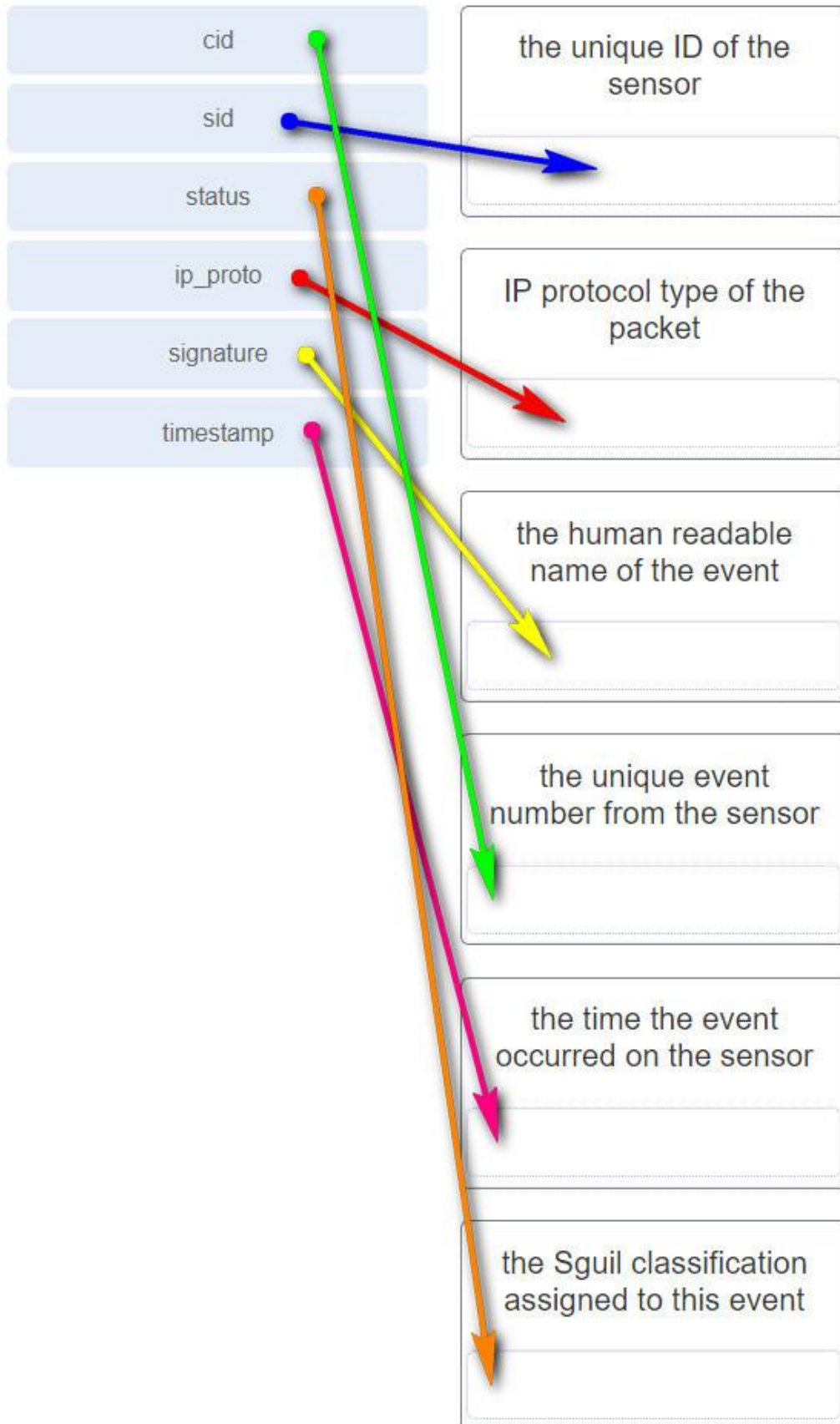
102. What is the primary objective of a threat intelligence platform (TIP)?

- **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

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.

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 in the 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**

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

113. Match the SIEM function to the description.

Match the SIEM function to the description.

forensic analysis	reduces the volume of event data by consolidating duplicate event records
correlation	aggregation
aggregation	presents event data in real-time monitoring and long-time summaries
reporting	reporting
	speeds detection of and reaction to security threats by examining logs and events from different systems
	correlation
	searches logs and events from sources throughout the organization for complete information analysis
	forensic analysis

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

- **amplification and reflection**
- fast flux
- ARP poisoning
- **resource utilization**
- cushioning

115. 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

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

- HTTP
- FTP

- **DNS**
- SMTP

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.**

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**

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


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

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

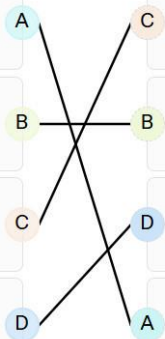
124. Which method is used to make data unreadable to unauthorized users?

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

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

Categories:  **Options:**

Displays resource utilization information for CPU, memory, network, disk, and others	A	C	Services
Allows programs that are running on system startup to be disabled	B	B	Startup
Allows for a start, stop or restart of a particular service	C	D	Details
Allows for a process to have its affinity set	D	A	Performance



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**

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

NTP	uses application protocols that are commonly responsible for bringing malware to a host
Syslog	
ICMP	
DNS	uses a hierarchy of authoritative time sources to send time information between devices on the network
	NTP
	used by attackers to exfiltrate data in traffic disguised as normal client queries
	DNS
	uses UDP port 514 for logging event messages from network devices and endpoints
	Syslog
	used by attackers to identify hosts on a network and the structure of the network
	ICMP

**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

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

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**

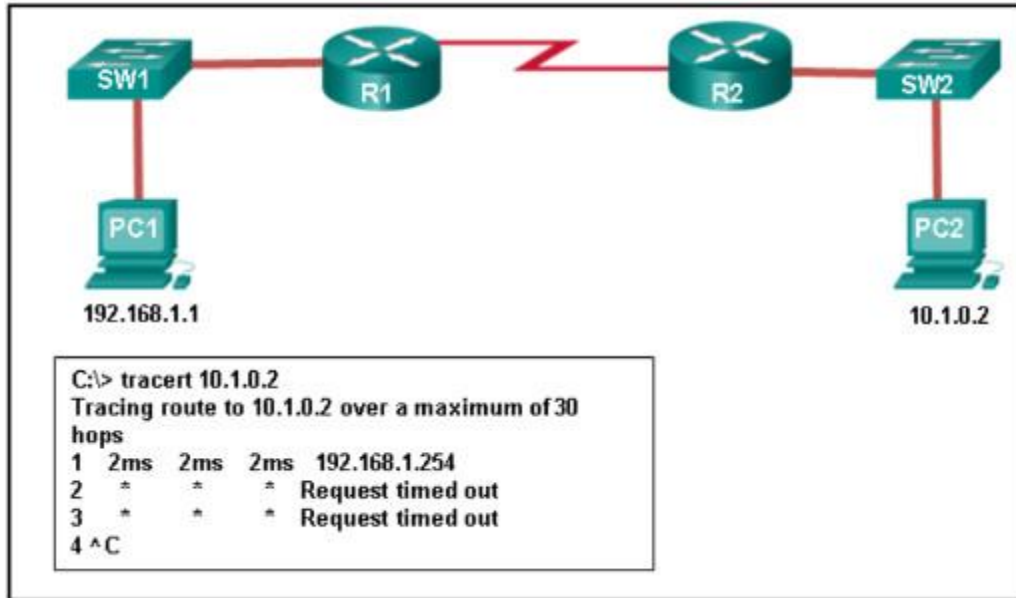
131. Which type of data would be considered an example of volatile data?

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

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.

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

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

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

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

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

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

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

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.**

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

MTTD	The average time that it takes for the SOC personnel to identify that valid security incidents have occurred in the network.
MTTC	The time required to stop the incident from causing further damage to systems or data.
MTTR	The average time that it takes to stop and remediate a security incident.
	The average length of time that threat actors have access to a network before they are detected and their access is stopped.

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**

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?

- Ask the user to stop immediately and inform the user that this constitutes grounds for dismissal.
- Create a firewall rule blocking the respective website.

- **Revise the AUP immediately and get all users to sign the updated AUP.**
- Immediately suspend the network privileges of the user.

147. Which two tasks can be performed by a local DNS server? (Choose two.)

- allowing data transfer between two network devices
- retrieving email messages
- providing IP addresses to local hosts
- **forwarding name resolution requests between servers**
- **mapping name-to-IP addresses for internal hosts**

148. Which type of event is logged in Cisco Next-Generation IPS devices (NGIPS) using FirePOWER Services when changes have been detected in the monitored network?

- intrusion
- connection
- host or endpoint
- **network discovery**

149. Which two actions should be taken during the preparation phase of the incident response life cycle defined by NIST? (Choose two.)

- **Acquire and deploy the tools that are needed to investigate incidents.**
- Detect all the incidents that occurred.
- Meet with all involved parties to discuss the incident that took place.
- **Create and train the CSIRT.**
- Fully analyze the incident.

150. What subnet mask is represented by the slash notation /20?

- 255.255.255.0
- 255.255.255.248
- 255.255.255.192
- **255.255.240.0**
- 255.255.224.0

151. What is the benefit of converting log file data into a common schema?

- creates a data model based on fields of data from a source
- creates a set of regex-based field extractions
- allows the implementation of partial normalization and inspection
- **allows easy processing and analysis of datasets**

152. Which Cisco sponsored certification is designed to provide the first step in acquiring the knowledge and skills to work with a SOC team?

- **CCNA CyberOps Associate**
- CCNA Cloud
- CCNA Security
- CCNA Data Center

153. Which three IP addresses are considered private addresses? (Choose three.)

- 198.168.6.18
- **192.168.5.29**
- 172.68.83.35
- 128.37.255.6
- **172.17.254.4**
- **10.234.2.1**

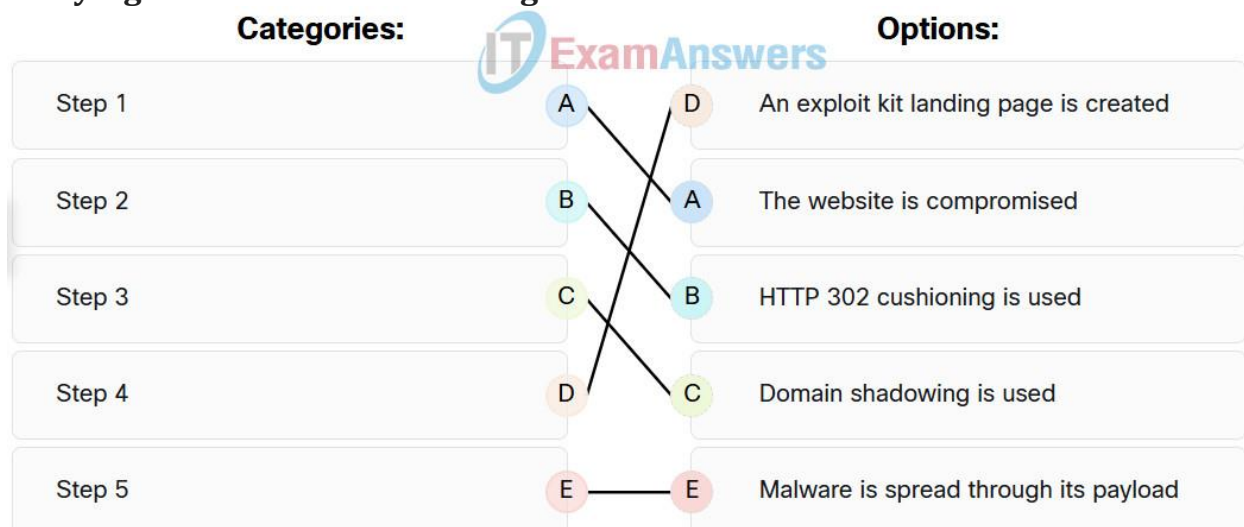
154. When establishing a network profile for an organization, which element describes the time between the establishment of a data flow and its termination?

- bandwidth of the Internet connection
- routing protocol convergence
- **session duration**
- total throughput

155. What are the stages that a wireless device completes before it can communicate over a wireless LAN network?

- **discover a wireless AP, authenticate with the AP, associate with the AP**
- discover a wireless AP, associate with the AP, authorize with the AP
- discover a wireless AP, associate with the AP, authenticate with the AP
- discover a wireless AP, authorize with the AP, associate with the AP

156. Match the correct sequence of steps typically taken by a threat actor carrying out a domain shadowing attack.

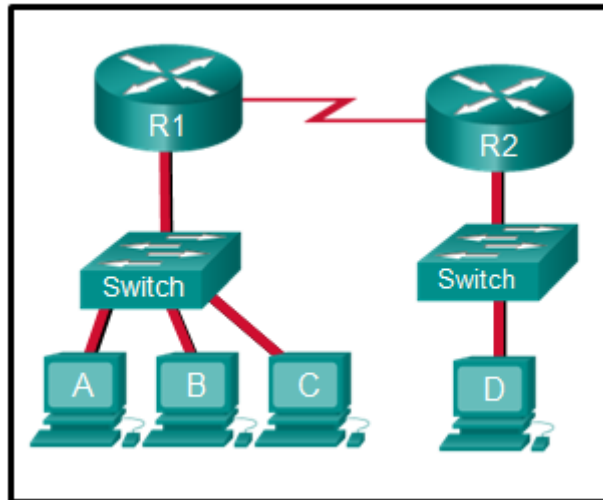


157. What are two properties of a cryptographic hash function? (Choose two.)

- Complex inputs will produce complex hashes.
- **The output is a fixed length.**
- **The hash function is one way and irreversible.**

- Hash functions can be duplicated for authentication purposes.
- The input for a particular hash algorithm has to have a fixed size.

158. Refer to the exhibit. The switches have a default configuration. Host A needs to communicate with host D, but host A does not have the MAC address for the default gateway. Which network devices will receive the ARP request sent by host A?



i360201v3n1_275353.png

- only host D
- only hosts A, B, C, and D
- only hosts B and C
- **only hosts B, C, and router R1**
- only hosts A, B, and C
- only router R1

159. Which type of evidence cannot prove an IT security fact on its own?

- hearsay
- corroborative
- best
- **indirect**

160. What is a characteristic of a probabilistic analysis in an alert evaluation?

- each event an inevitable result of antecedent causes
- precise methods that yield the same result every time by relying on predefined conditions
- **random variables that create difficulty in knowing the outcome of any given event with certainty**
- analysis of applications that conform to application/networking standards

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

- It is easier to use than other server operating systems.
- **It can be acquired at no charge.**

- More network applications are created for this environment.
- The administrator has control over specific security functions, but not standard applications.

162. A technician needs to verify file permissions on a specific Linux file. Which command would the technician use?

- cd
- sudo
- **ls -l**
- vi

163. Which two protocols may devices use in the application process that sends email? (Choose two.)

- HTTP
- POP
- POP3
- **DNS**
- IMAP
- **SMTP**

164. Which file system type was specifically created for optical disk media?

- ext3
- HFS+
- **CDFS**
- ext2

165. A piece of malware has gained access to a workstation and issued a DNS lookup query to a CnC server. What is the purpose of this attack?

- to check the domain name of the workstation
- **to send stolen sensitive data with encoding**
- to masquerade the IP address of the workstation
- to request a change of the IP address

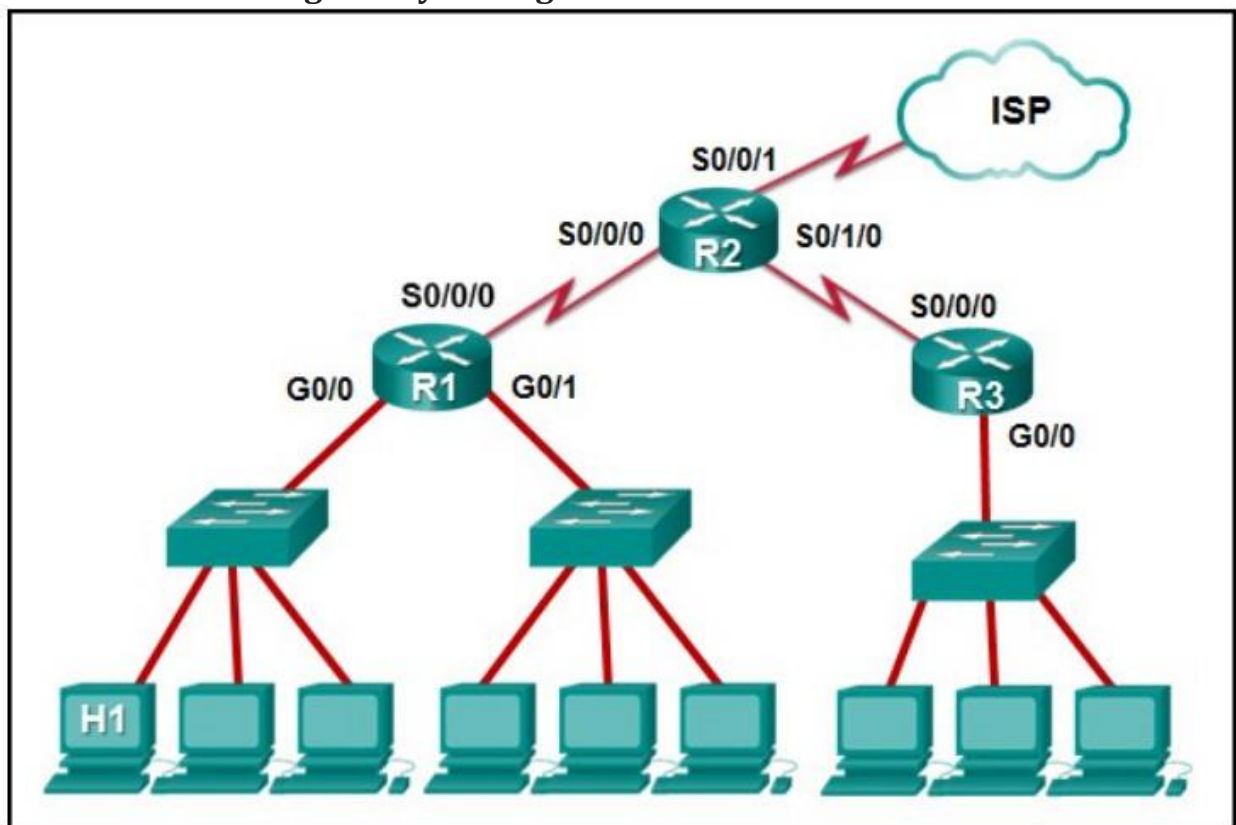
166. Refer to the exhibit. Which field in the Sguil event window indicates the number of times an event is detected for the same source and destination IP

address?

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	8	seconion-ossec	1.13	2017-06-19 23:10:40	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checks
RT	232	seconion-ossec	1.24	2017-06-19 23:18:28	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packe
RT	6	seconion-ossec	1.3	2017-06-19 23:08:51	0.0.0.0		0.0.0.0		0	[OSSEC] Interface entere
RT	1	seconion-ossec	1.41	2017-06-30 14:34:56	0.0.0.0		0.0.0.0		0	[OSSEC] User login failed
RT	3	seconion-ossec	1.42	2017-06-30 14:39:31	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checks
RT	3	seconion-ossec	1.52	2017-06-30 15:04:27	0.0.0.0		0.0.0.0		0	[OSSEC] Host-based anoa
RT	1	seconion-ossec	1.7	2017-06-19 23:09:11	0.0.0.0		0.0.0.0		0	[OSSEC] New group adde
RT	16	seconion-ossec	1.8	2017-06-19 23:09:26	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checks
RT	6	seconion-eth1-1	5.1	2017-06-19 23:18:22	209.165.200.235		192.168.0.1		1	GPL ICMP_INFO PING B
RT	10	seconion-eth1-1	5.13	2017-06-19 23:38:49	209.165.200.226		209.165.200.235		1	GPL ICMP_INFO PING *N
RT	6	seconion-eth1-1	5.2	2017-06-19 23:18:22	209.165.200.235		192.168.0.1		1	GPL ICMP_INFO PING *N
RT	1	seconion-eth1-1	5.23	2017-06-19 23:51:12	209.165.201.17	40599	209.165.200.235	21	6	ET EXPLOIT VSFTPD Back
RT	1	seconion-eth1-1	5.24	2017-06-19 23:51:12	209.165.200.235	6200	209.165.201.17	34057	6	GPL ATTACK_RESPONSE
RT	106	seconion-eth2-1	7.1	2017-06-19 23:19:00	209.165.201.17		192.168.0.1		1	GPL ICMP_INFO PING *N
RT	51	seconion-eth2-1	7.6	2017-06-19 23:39:03	209.165.201.21		209.165.201.17		1	GPL ICMP_INFO PING *N
RT	1	seconion-eth2-1	7.90	2017-06-19 23:51:12	209.165.201.17	40599	209.165.200.235	21	6	ET EXPLOIT VSFTPD Back
RT	1	seconion-eth2-1	7.91	2017-06-19 23:51:12	209.165.200.235	6200	209.165.201.17	34057	6	GPL ATTACK_RESPONSE

- CNT
- Pr
- ST
- AlertID

167. Refer to the exhibit. The IP address of which device interface should be used as the default gateway setting of host H1?



- R1: G0/0

- R2: S0/0/0
- R2: S0/0/1
- R1: S0/0/0

168. According to information outlined by the Cyber Kill Chain, which two approaches can help identify reconnaissance threats? (Choose two.)

- **Analyze web log alerts and historical search data.**
- Audit endpoints to forensically determine origin of exploit.
- **Build playbooks for detecting browser behavior.**
- Conduct full malware analysis.
- Understand targeted servers, people, and data available to attack.

169. Which two ICMPv6 messages are used during the Ethernet MAC address resolution process? (Choose two.)

- router solicitation
- router advertisement
- **neighbor solicitation**
- **neighbor advertisement**
- echo request

170. What best describes the destination IPv4 address that is used by multicasting?

- **a single IP multicast address that is used by all destinations in a group**
- an IP address that is unique for each destination in the group
- a group address that shares the last 23 bits with the source IPv4 address
- a 48 bit address that is determined by the number of members in the multicast group

171. What is the result of using security devices that include HTTPS decryption and inspection services?

- The devices require continuous monitoring and fine tuning.
- **The devices introduce processing delays and privacy issues.**
- The devices must have preconfigured usernames and passwords for all users.
- Monthly service contracts with reputable web filtering sites can be costly.

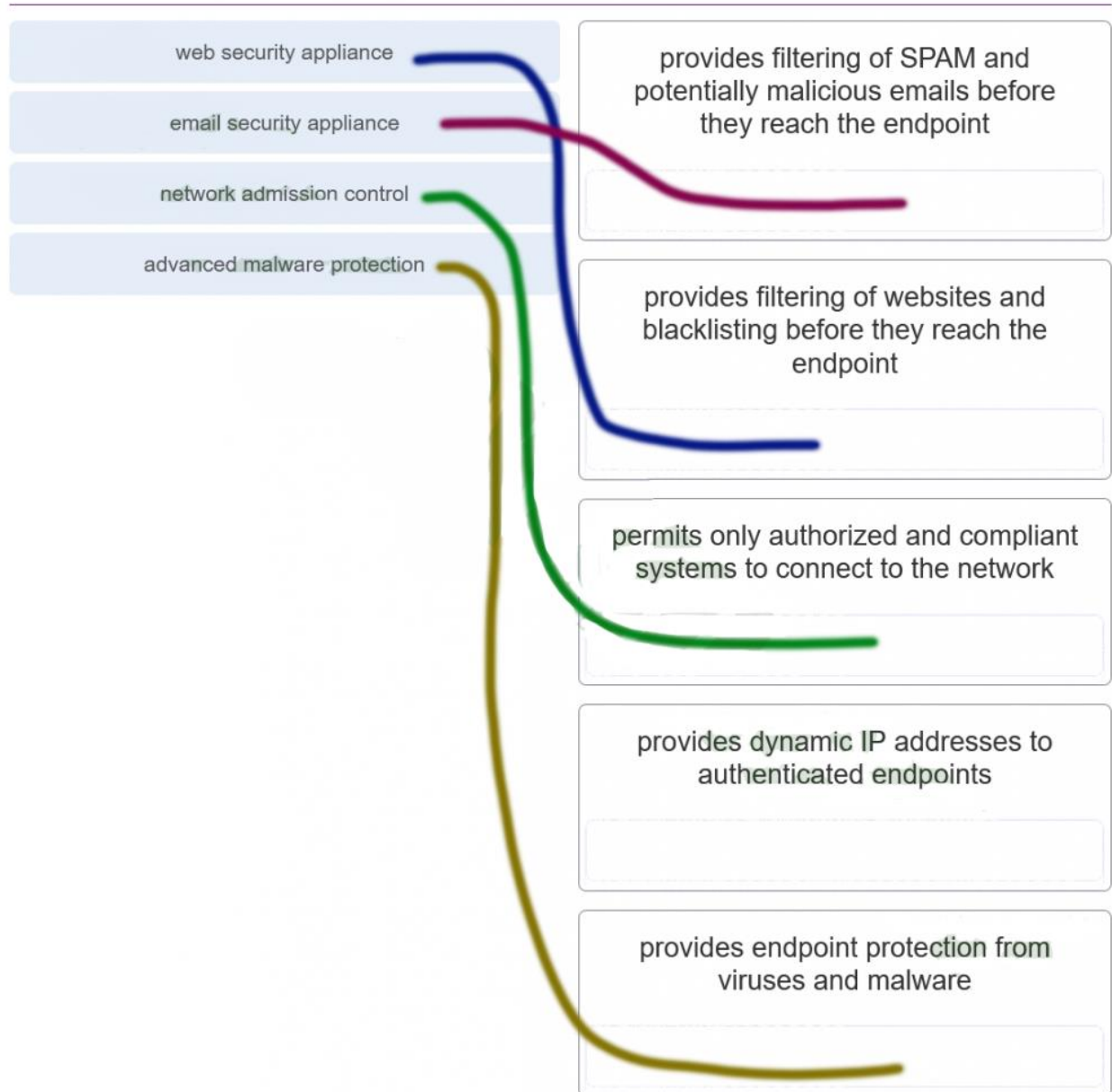
172. What is a disadvantage of DDNS?

- DDNS is considered malignant and must be monitored by security software.
- DDNS is unable to co-exist on a network subdomain that also uses DNS.
- **Using free DDNS services, threat actors can quickly and easily generate subdomains and change DNS records.**

- Using DDNS, a change in an existing IP address mapping can take over 24 hours and could result in a disruption of connectivity.

173. Match the network-based antimalware solution to the function. (Not all options are used.)

Match the network-based antimalware solution to the function. (Not all options are used.)



174. A threat actor has identified the potential vulnerability of the web server of an organization and is building an attack. What will the threat actor possibly do to build an attack weapon?

- Obtain an automated tool in order to deliver the malware payload through the vulnerability.**
- Install a webshell on the web server for persistent access.

- Create a point of persistence by adding services.
- Collect credentials of the web server developers and administrators.

175. Which tool included in the Security Onion is a series of software plugins that send different types of data to the Elasticsearch data stores?

- OSSEC
- Curator
- **Beats**
- ElastAlert

176. Which term is used to describe the process of identifying the NSM-related data to be gathered?

- data archiving
- data normalization
- **data reduction**
- data retention

177. Match the alert classification with the description.

Match the alert classification with the description.

false positive	malicious traffic is correctly identified as a threat
false negative	normal traffic is incorrectly identified as a threat
true positive	malicious traffic is not identified as a threat
true negative	normal traffic is not identified as a threat

178. According to NIST, which step in the digital forensics process involves preparing and presenting information that resulted from scrutinizing data?

- examination
- collection
- **reporting**
- analysis

179. Refer to the exhibit. A cybersecurity analyst is using Sguil to verify security alerts. How is the current view sorted?

ST	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	seconion...	5.55	2017-07-05 18:38:17	209.165.201.17	36606	209.165.200.235	80	6	ET SCAN Nmap Scripting Engin...
RT	seconion...	7.121	2017-07-05 18:38:17	209.165.201.17	36606	209.165.200.235	80	6	ET SCAN Nmap Scripting Engin...
RT	seconion...	5.56	2017-07-05 18:38:17	209.165.201.17	36606	209.165.200.235	80	6	ET SCAN Possible Nmap User...
RT	seconion...	7.122	2017-07-05 18:38:17	209.165.201.17	36606	209.165.200.235	80	6	ET SCAN Possible Nmap User...
RT	seconion...	1.23	2017-06-19 23:18:28	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packets in ...
RT	seconion...	7.1	2017-06-19 23:19:00	209.165.201.17		192.168.0.1		1	GPL ICMP_INFO PING *NIX
RT	seconion...	7.6	2017-06-19 23:39:03	209.165.201.21		209.165.201.17		1	GPL ICMP_INFO PING *NIX
RT	seconion...	1.8	2017-06-19 23:09:26	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum c...
RT	seconion...	5.25	2017-06-20 15:02:27	209.165.201.17		209.165.200.235		1	GPL ICMP_INFO PING *NIX
RT	seconion...	5.13	2017-06-19 23:38:49	209.165.200.226		209.165.200.235		1	GPL ICMP_INFO PING *NIX
RT	seconion...	1.13	2017-06-19 23:10:40	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum c...
RT	seconion...	5.99	2017-07-05 18:38:18	209.165.201.17	37354	209.165.200.235	80	6	ET WEB_SERVER ColdFusion a...
RT	seconion...	5.100	2017-07-05 18:38:18	209.165.201.17	37354	209.165.200.235	80	6	ET WEB_SERVER ColdFusion p...

- by sensor number
- by source IP
- by date/time
- **by frequency**

180. Which two options are window managers for Linux? (Choose two.)

- File Explorer
- Kali
- **Gnome**
- PenTesting
- **KDE**

181. What are the two methods that a wireless NIC can use to discover an AP? (Choose two.)

- **transmitting a probe request**
- sending an ARP request broadcast
- initiating a three-way handshake
- **receiving a broadcast beacon frame**
- sending a multicast frame

182. A client device has initiated a secure HTTP request to a web browser. Which well-known port address number is associated with the destination address?

- 110
- 80
- **443**
- 404

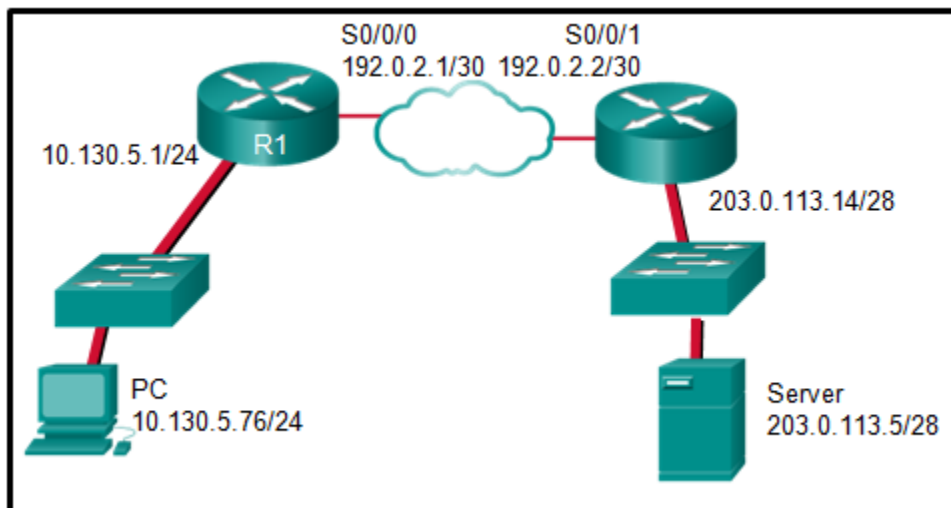
183. Which term describes evidence that is in its original state?

- Corroborating evidence
- **Best evidence**
- Indirect evidence
- Direct evidence

184. Which three statements describe a DHCP Discover message? (Choose three.)

- The source MAC address is 48 ones (FF-FF-FF-FF-FF-FF).
- **The destination IP address is 255.255.255.255.**
- The message comes from a server offering an IP address.
- **The message comes from a client seeking an IP address.**
- **All hosts receive the message, but only a DHCP server replies.**
- Only the DHCP server receives the message.

185. Refer to the exhibit. The PC is sending a packet to the Server on the remote network. Router R1 is performing NAT overload. From the perspective of the PC, match the NAT address type with the correct IP address. (Not all options are used.)

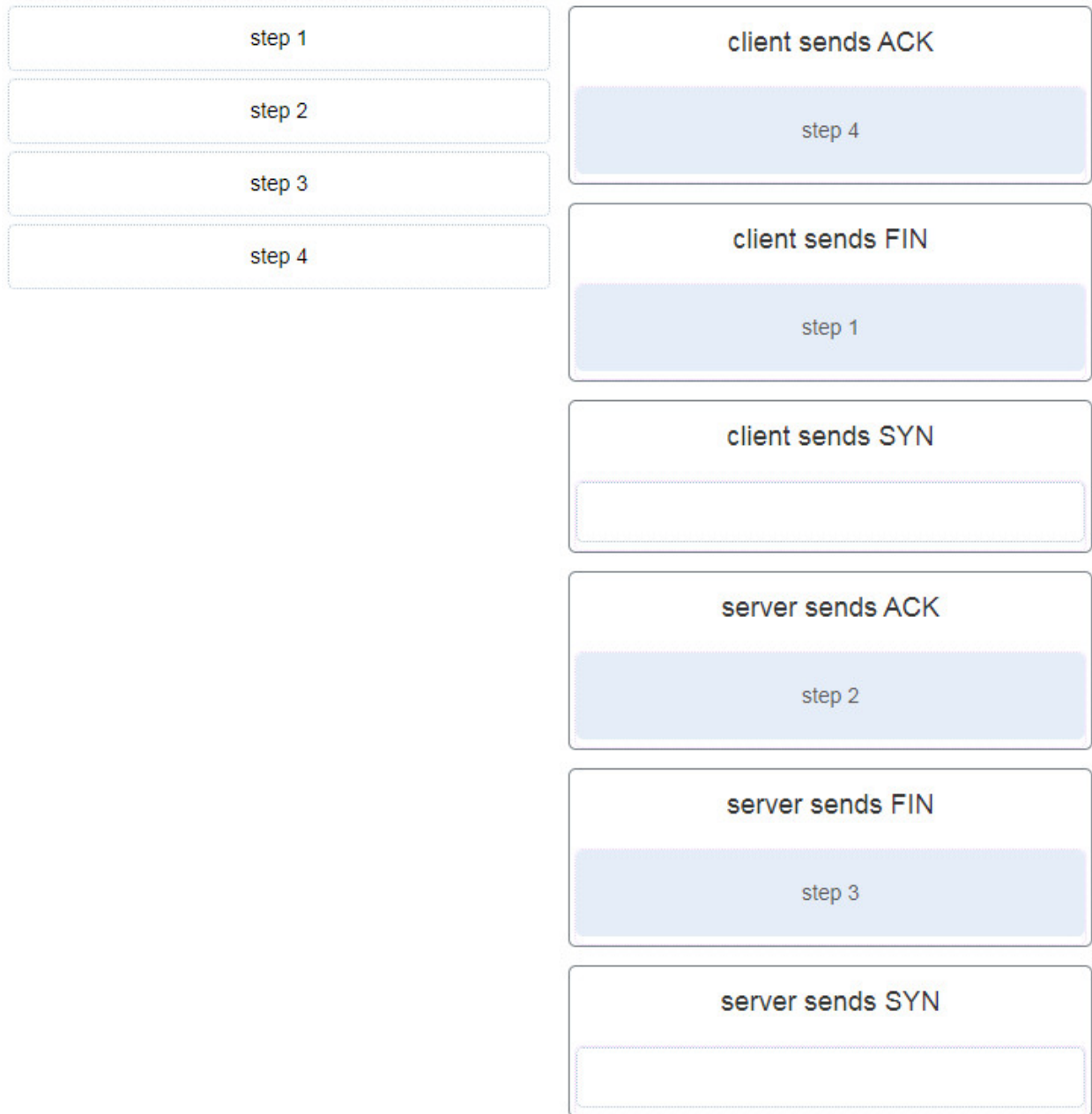




186. Which step in the Vulnerability Management Life Cycle categorizes assets into groups or business units, and assigns a business value to asset groups based on their criticality to business operations?

- remediate
- **prioritize assets**
- report
- assess

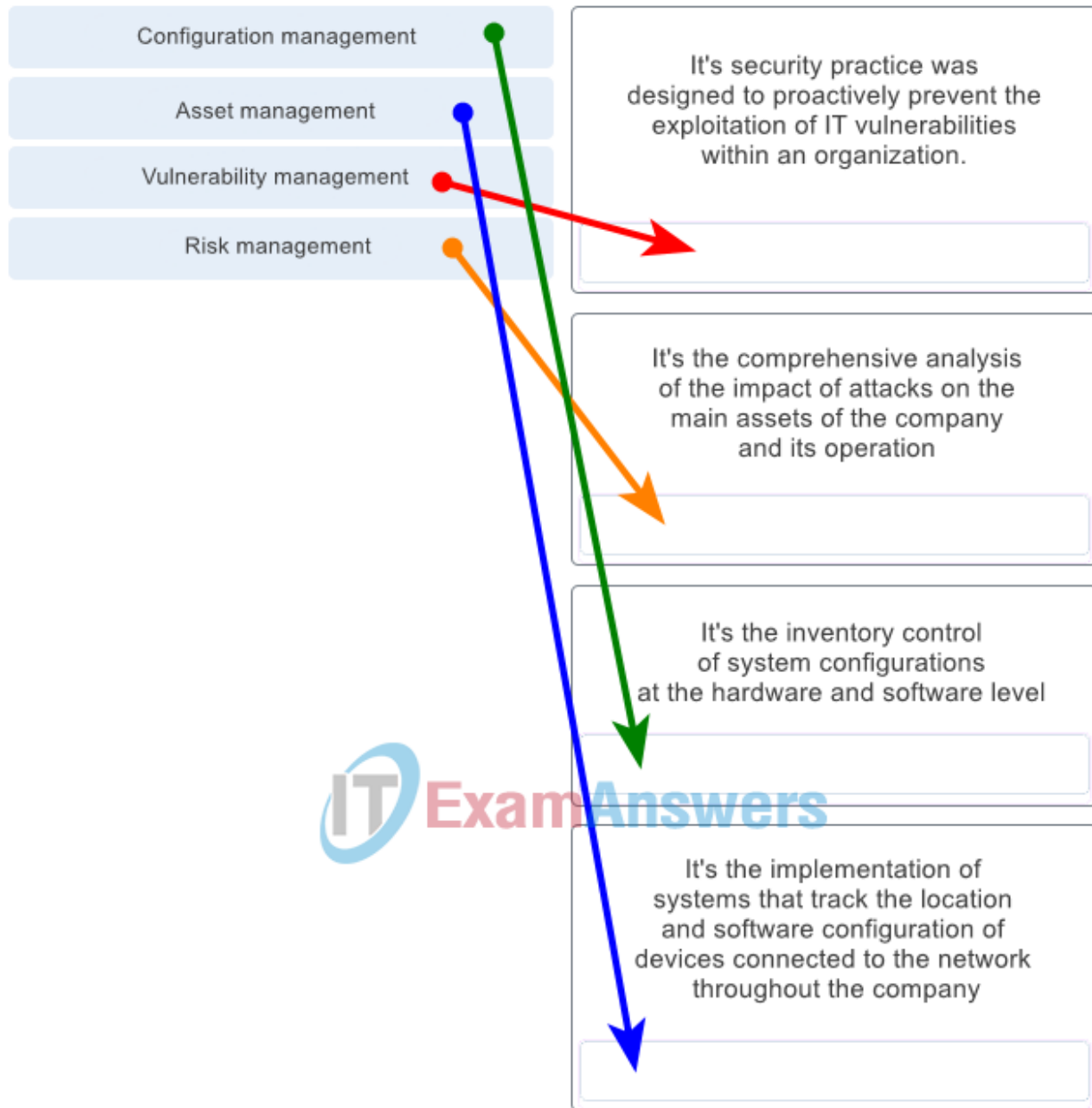
187. A client application needs to terminate a TCP communication session with a server. Place the termination process steps in the order that they will occur. (Not all options are used.)



188. Match the attack vector with the description.

web	initiated through an email attachment
email	email
attrition	initiated from external storage
media	media
	uses brute force against devices or services
	attrition
	initiated from a website application
	web

189. Match the security management function with the description.



CyberOps Associate (Version 1.0) – CyberOps Associate 1.0 Final exam answers
Q189

190. What are two functions that are provided by the network layer? (Choose two.)

- directing data packets to destination hosts on other networks
- placing data on the network medium
- carrying data between processes that are running on source and destination hosts
- providing dedicated end-to-end connections
- providing end devices with a unique network identifier

191. Match the phase in the NIST incident response life cycle to the action.

preparation	Document incident handling.
detection and analysis	post-incident activities
containment, eradication, and recovery	Conduct CSIRT response training.
post-incident activities	preparation
	Identify, analyze, and validate an incident.
	detection and analysis
	Implement procedures to contain the threat.
	containment, eradication, and recovery

- Document incident handling. → post-incident activities
- Conduct CSIRT response training. → preparation
- Identify, analyze, and validate an incident. → detection and analysis
- Implement procedures to contain the threat. → containment, eradication, and recovery

192. Match the Linux CLI commands to their function. (Not all options are used.)

rm	copies files from source to destination
man	
ls	
cd	changes the current directory
mkdir	cd
	removes files
	rm
	creates a directory under the current directory
	mkdir
	displays the files inside a directory
	ls
	moves files to a different directory
	displays the documentation for a specific command
	man