CCNA Cyber Ops (Version 1.1) – Practice Final Exam Answers Full

itexamanswers.net/ccna-cyber-ops-practice-final-exam-answers-full.html

May 14, 2019

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

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.

CCNA Cybersecurity Operations (Version 1.1) – CyberOps Practice Final Exam

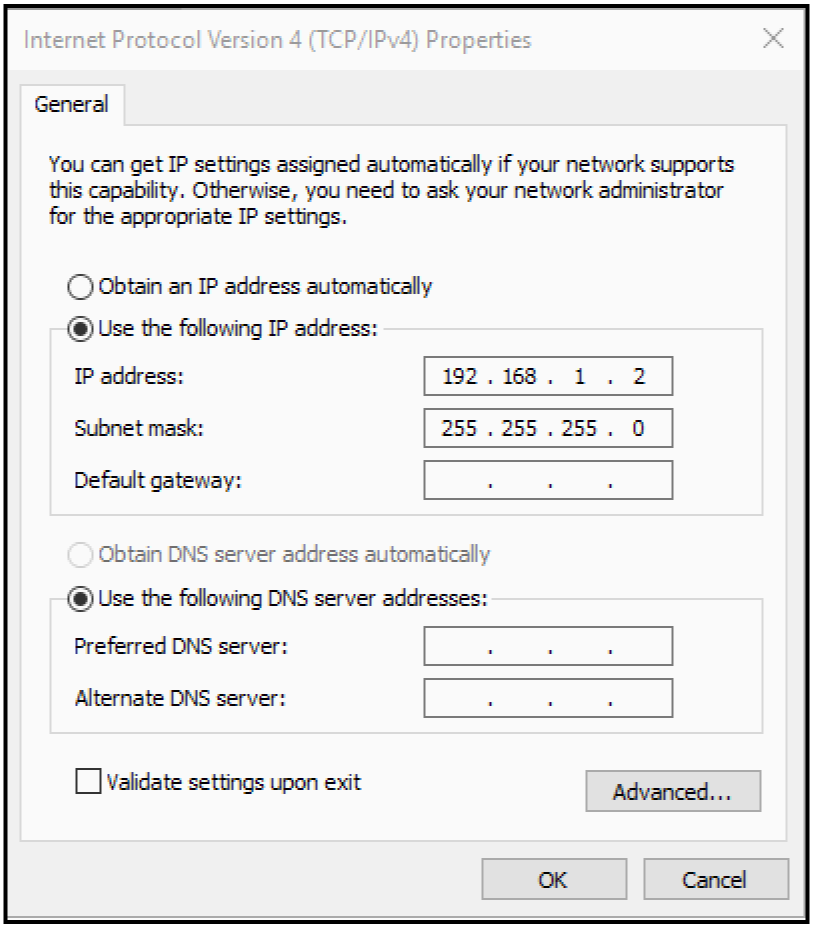
1. A person coming to a cafe for the first time wants to gain wireless access to the Internet using a laptop. What is the first step the wireless client will do in order to communicate over the network using a wireless management frame?

- 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

2. Refer to the exhibit. What is a valid address on the PC for the default gateway?



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

- 192.168.255.1
- 192.168.2.1
- **192.168.1.1**
- 192.168.0.1

Explanation: The default gateway setting is the IP address of the router to which the host will send packets in order to reach remote networks. The default gateway address setting must be on the same logical network as the host IP address. In this case, the network of the host is 192.168.1.0 so the default gateway must also be on the 192.168.1.0 network.

3. A cybersecurity analyst believes that an attacker is announcing a forged MAC address to network hosts in an attempt to spoof the default gateway. Which command could the analyst use on the network hosts to see what MAC address the hosts are using to reach the default gateway?

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

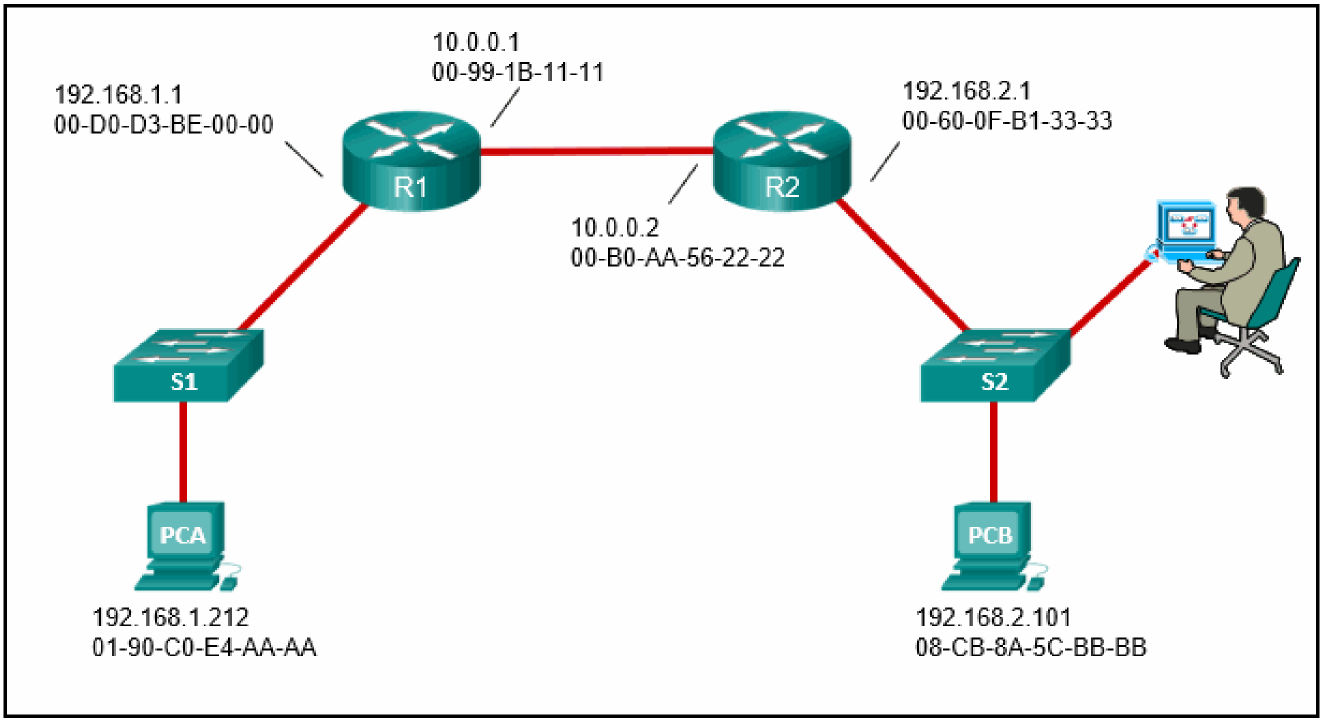
Explanation: The command arp -a will display the MAC address table on a PC.

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

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

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

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

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

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. 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.

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

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

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

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

- to provide statistics on packets that are flowing through a Cisco device
- **to select the type of logging information that is captured**
- **to specify the destinations of captured messages**

- to periodically poll agents for data
- **to gather logging information for monitoring and troubleshooting**
- to provide traffic analysis

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

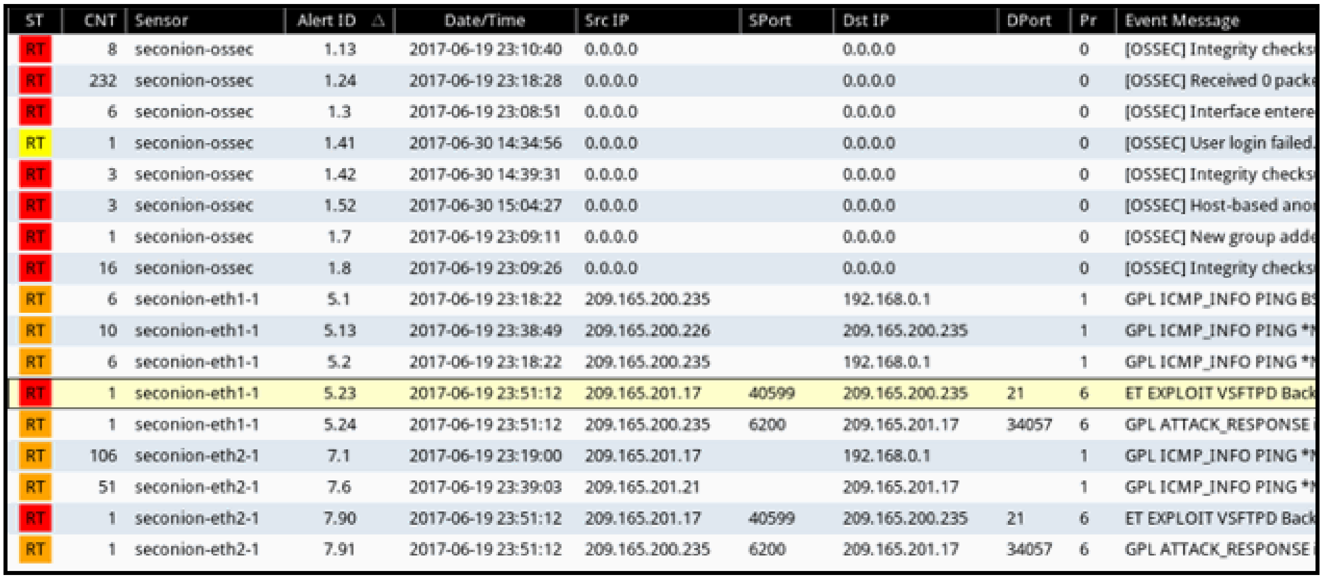
1. gathering logging information
2. selection of the type of information to be logged
3. selection of the destination of the logged information

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

- Allow users to re-use old passwords.
- **Force periodic password changes.**
- Allow USB auto-detection.
- Allow default services to remain enabled.

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.

10. 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 pack
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 ano
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 *
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 *
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 *
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 *
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

- Pr
- **CNT**
- AlertID
- ST

Explanation: The CNT field indicates the number of times an event is detected from the same source and destination IP address. Having a high number of events can indicated a problem with event signatures.

11. A user successfully logs in to a corporate network via a VPN connection. Which part of the AAA process records that a certain user performed a specific operation at a particular date and time?

- access
- **accounting**
- authorization
- authentication

Explanation: The three parts of the AAA process are authentication, authorization, and accounting. The accounting function records information such as who logged in, when the user logged in and out, and what the user did with network resources.

12. What is the responsibility of the IT support group when handling a security incident?

- Coordinate the incident response with other stakeholders and minimize the damage of the incident.
- Review the incident policies, plans, and procedures for local or federal guideline violations.

- **Perform actions to minimize the effectiveness of the attack and preserve evidence.**
- Perform disciplinary measures if an incident is caused by an employee.

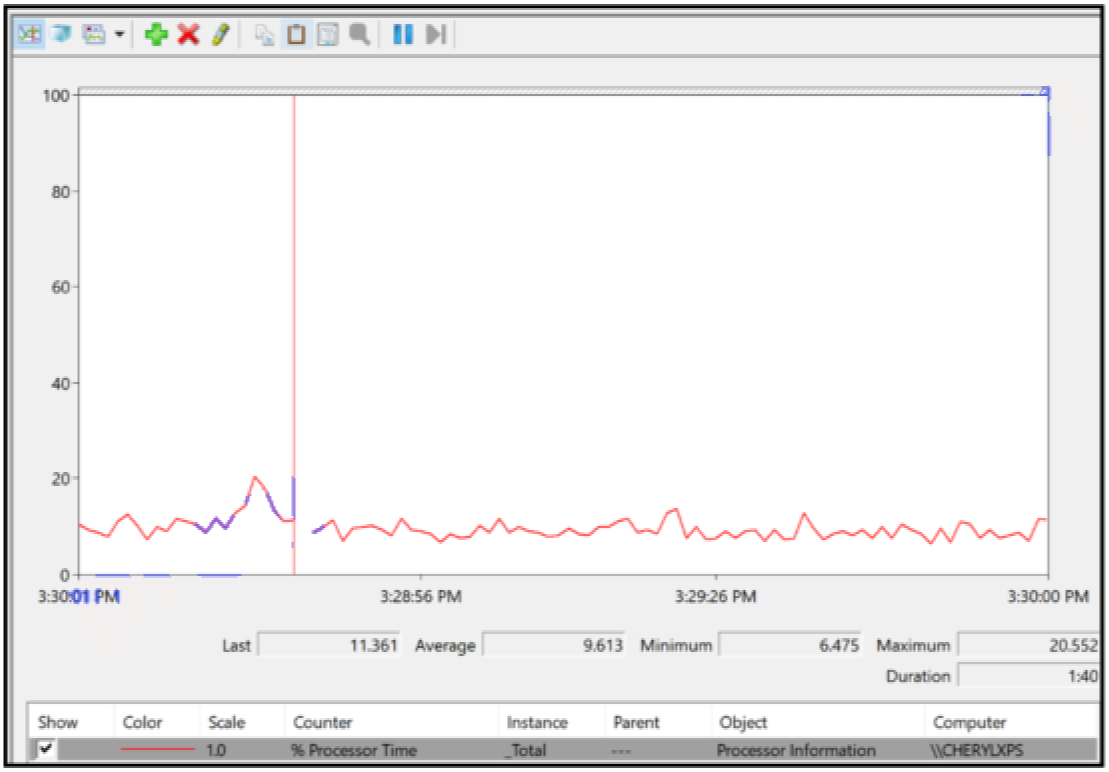
Explanation: IT support best understands the technology used in the organization and can perform the correct actions to minimize the effectiveness of the attack and preserve evidence.

13. Which Linux program is going to be used when installing an application?

- X Window System
- launcher
- **package manager**
- penetration tool

Explanation: A package is a specific program and all of the files needed to run that program. A package manager is used to install a package and place all the associated files in the correct location within the operating system.

14. Refer to the exhibit. Which security issue would a cybersecurity analyst use the displayed tool?



Last 11.361 Average 9.613 Minimum 6.475 Maximum 20.552
Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
✓	—	1.0	% Processor Time	_Total	---	Processor Information	\\CHERYLXPS

- ARP cache poisoning
- DNS attack
- TCP attack

- **malware**

Explanation: Windows Performance Monitor is used to evaluate the performance of individual components on a Windows host computer. Commonly monitored components include the processor, hard drive, network, and memory. Windows Task Manager and Performance Monitor are used when malware is suspected and a component is not performing the way it should.

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

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

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

16. What would be the target of an SQL injection attack?

- **database**
- DHCP
- email
- DNS

Explanation: SQL is the language used to query a relational database. Cybercriminals use SQL injections to get information, create fake or malicious queries, or to breach the database in some other way.

17. What is the result of a DHCP starvation attack?

- Clients receive IP address assignments from a rogue DHCP server.
- **Legitimate clients are unable to lease IP addresses.**
- The IP addresses assigned to legitimate clients are hijacked.
- The attacker provides incorrect DNS and default gateway information to clients.

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 to lease the entire pool of available IP addresses, thus denying them to legitimate hosts.

18. Users report to the helpdesk that icons usually seen on the menu bar are randomly appearing on their computer screens. What could be a reason that computers are displaying these random graphics?

- A DoS attack has been launched against the network.
- The computers are subject to a reconnaissance attack.
- **A virus has infected the computers.**
- An access attack has occurred.

Explanation: A virus such as this is harmless, but still needs to be removed. Other viruses can be destructive in that they modify or delete files on the local computer and possibly other computers on the network.

19. A disgruntled employee is using Wireshark to discover administrative Telnet usernames and passwords. What type of network attack does this describe?

- trust exploitation
- port redirection
- **reconnaissance**
- denial of service

Explanation: Wireshark is a free download that allows network packet inspection. Someone using this tool for malicious intent would be performing a reconnaissance attack. Through the capture of network packets, weak security network connectivity protocols such as Telnet can be caught, inspected, and then analyzed for detailed network information, including passwords.

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

- Darknet
- Snort
- **Bitcoin**
- **BitTorrent**
- Wireshark

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

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

- Header Length

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

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

22. What are two elements that form the PRI value in a syslog message? (Choose two.)

- **facility**
- **severity**
- header
- hostname
- timestamp

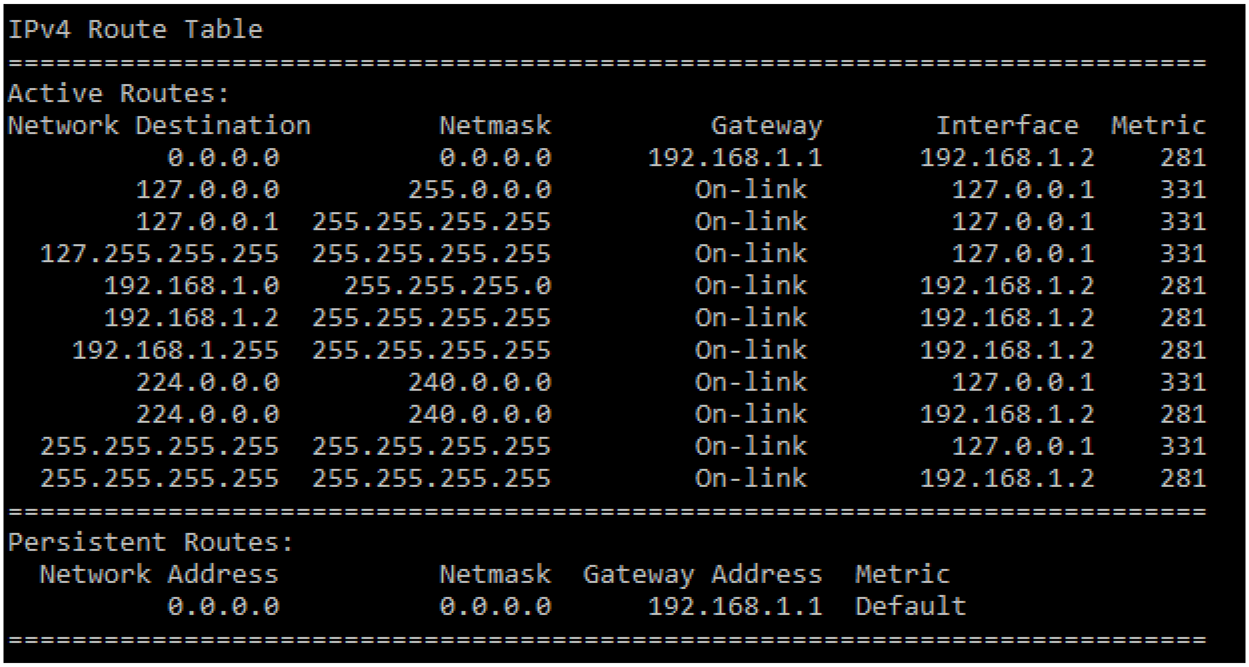
Explanation: The PRI in a syslog message consists of two elements, the facility and severity of the message.

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

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

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

24. Refer to the exhibit. Which IPv4 address does the PC use for sending traffic to remote networks?



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.2    281
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link       192.168.1.2    281
      192.168.1.2  255.255.255.255         On-link       192.168.1.2    281
    192.168.1.255  255.255.255.255         On-link       192.168.1.2    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       192.168.1.2    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link       192.168.1.2    281
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      192.168.1.1  Default
===========================================================================
```

- 127.0.0.1
- 192.168.1.2
- **192.168.1.1**
- 192.168.1.255

Explanation: The default gateway setting is the IP address of the router to which the host will send packets that are destined for remote networks. In the routing table of a PC, the gateway address is the default gateway and must be on the same logical network as the host IP address, in this case 192.168.1.0. Thus the gateway address, which must be on the 192.168.1.0 network, is 192.168.1.1.

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

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

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

Turn off Wi-Fi and Bluetooth connectivity when not being used. Only connect to trusted networks.
Keep the device OS and other software updated.
Backup any data stored on the device.
Subscribe to a device locator service with a remote wipe feature.
Provide antivirus software for approved BYODs.
Use Mobile Device Management (MDM) software that allows IT teams to track the device and implement security settings and software controls.

26. What is an essential function of SIEM?

- forwarding traffic and physical layer errors to an analysis device
- providing 24×7 statistics on packets flowing through a Cisco router or multilayer switch
- monitoring traffic and comparing it against the configured rules
- **providing reporting and analysis of security events**

Explanation: SIEM provides real-time reporting and analysis of security events. SIEM provides administrators with details on sources of suspicious activity such as user information, device location, and compliance with security policies.

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

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

28. Which statement describes the Cyber Kill Chain?

- **It identifies the steps that adversaries must complete to accomplish their goals.**
- It specifies common TCP/IP protocols used to fight against cyberattacks.

- It is a set of metrics designed to create a way to describe security incidents in a structured and repeatable way.
- It uses the OSI model to describe cyberattacks at each of the seven layers.

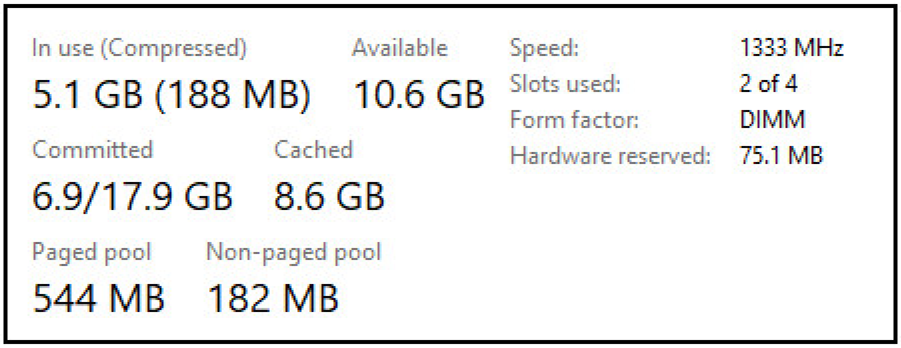
Explanation: The Cyber Kill Chain was developed to identify and prevent cyber intrusions by specifying what threat actors must complete to accomplish their goals.

29. Why does a worm pose a greater threat than a virus poses?

- **Worms are more network-based than viruses are.**
- Worms are not detected by antivirus programs.
- Worms run within a host program.
- Worms directly attack the network devices.

Explanation: One major component of a worm is the propagation mechanism which replicates the worm and targets unprotected network devices. A virus requires a host program, but worms do not.

30. Refer to the exhibit. Approximately what percentage of the physical memory is in use on this Windows system?



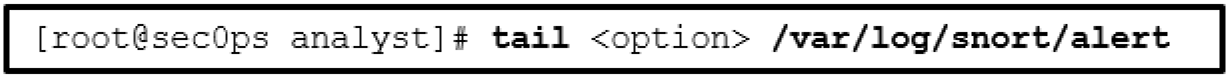
In use (Compressed): 5.1 GB (188 MB)
Available: 10.6 GB
Committed: 6.9/17.9 GB
Cached: 8.6 GB
Paged pool: 544 MB
Non-paged pool: 182 MB

Speed: 1333 MHz
Slots used: 2 of 4
Form factor: DIMM
Hardware reserved: 75.1 MB

- **33%**
- 53%
- 67%
- 90%

Explanation: The graphic shows that there is 5.0 GB (187 MB) of memory in use with 10.7 GB still available. Together this adds up to 16 GB of total physical memory. 5 GB is approximately 33% of 16 GB.

31. Refer to the exhibit. A network security specialist is issuing the tail command to monitor the Snort alert in real time. Which option should be used in the command line to watch the file for changes?



```
[root@secOps analyst]# tail <option> /var/log/snort/alert
```

- -c
- -q
- **-f**
- -n

Explanation: For the Linux tail command, the option -f is used to monitor a file for changes. The -c option is used to limit the number of bytes shown. The -n option is used to set the number of lines to display. The -q option is used to suppress the header line.

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

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

Explanation: Digital signatures provide three basic security services:Authenticity of digitally signed data – Digital signatures authenticate a source, proving that a certain party has seen and signed the data in question.
Integrity of digitally signed data – Digital signatures guarantee that the data has not changed from the time it was signed.

Nonrepudiation of the transaction – The recipient can take the data to a third party, and the third party accepts the digital signature as a proof that this data exchange did take place. The signing party cannot repudiate that it has signed the data.

33. A network security specialist is tasked to implement a security measure that monitors the status of critical files in the data center and sends an immediate alert if any file is modified. Which aspect of secure communications is addressed by this security measure?

- origin authentication
- **data integrity**
- nonrepudiation
- data confidentiality

Explanation: Secure communications consists of four elements:

Data confidentiality – guarantees that only authorized users can read the message

Data integrity – guarantees that the message was not altered

Origin authentication – guarantees that the message is not a forgery and does actually come from whom it states

Data nonrepudiation – guarantees that the sender cannot repudiate, or refute, the validity of a message sent

34. What is the most common use of the Diffie-Helman algorithm in communications security?

- **to secure the exchange of keys used to encrypt data**
- to create password hashes for secure authentication
- to encrypt data for secure e-commerce communications
- to provide routing protocol authentication between routers

Explanation: Diffie-Helman is not an encryption mechanism and is not typically used to encrypt data. Instead, it is a method to securely exchange the keys used to encrypt the data.

35. In threat intelligence communications, which sharing standard is a specification for an application layer protocol that allows communication of cyberthreat intelligence over HTTPS?

- **Trusted automated exchange of indicator information (TAXII)**
- Structured threat information expression (STIX)
- Common vulnerabilities and exposures (CVE)
- Automated indicator sharing (AIS)

Explanation: The two common threat intelligence sharing standards are as follows:

Structured Threat Information Expression (STIX) – This is a set of specifications for exchanging cyberthreat information between organizations. The Cyber Observable Expression (CybOX) standard has been incorporated into STIX.

Trusted Automated Exchange of Indicator Information (TAXII) – This is the specification for an application layer protocol that allows the communication of CTI over HTTPS. TAXII is designed to support STIX.

36. Which schema or model allows security professionals to enter data about a particular incident, such as victim demographics, incident description, discovery method and response, and impact assessment, and share that data with the security community anonymously?

- Diamond

- Cyber Kill Chain
- CSIRT
- **VERIS**

Explanation: Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designed to create a way to describe security incidents in a structured or repeatable way. A Computer Security Incident response Team (CSIRT) is an internal organizational group that provides services and functions to secure assets. Cyber Kill Chain contains seven steps which help analysts understand the techniques, tools, and procedures of threat actors. The Diamond Model of intrusion has four parts that represent a security incident.

37. Which component in Linux is responsible for interacting directly with the device hardware?

- shell
- command interpreter
- **kernel**
- command line interface

Explanation: A Linux OS can be divided into kernel and shell. The shell, also called the command line interface, is a command interpreter that parses the inputs (or commands) from a user and interacts with the kernel. The kernel, in turn, interacts with the hardware components of a device.

38. 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?

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

Explanation: Port numbers are used in TCP and UDP communications to differentiate between the various services running on a device. The well-known port number used by HTTPs is port 443.

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

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

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

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

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

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.

41. A law office uses a Linux host as the firewall device for the network. The IT administrator is configuring the firewall iptables to block pings from Internet devices to the Linux host. Which iptables chain should be modified to achieve the task?

- INTERNET
- **INPUT**
- OUTPUT
- FORWARD

Explanation: The firewall iptables uses the concepts of chains and rules to filter traffic:

INPUT chain – handles traffic entering the firewall and destined to the firewall device itself

OUTPUT chain – handles traffic originating within the firewall device itself and destined to somewhere else

FORWARD chain – handles traffic originated somewhere else and passing through the firewall device

42. What is the main purpose of cyberwarfare?

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

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

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

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.

44. Which statement describes the state of the administrator and guest accounts after a user installs Windows desktop version to a new computer?

- By default, both the administrator and guest accounts are enabled.
- **By default, both the administrator and guest accounts are disabled.**
- By default, the administrator account is enabled but the guest account is disabled.
- By default, the guest account is enabled but the administrator account is disabled.

Explanation: When a user installs Windows desktop version, two local user accounts are created automatically during the process, administrator and guest. Both accounts are disabled by default.

45. Which two characteristics describe a virus? (Choose two.)

- Malware that executes arbitrary code and installs copies of itself in memory.
- A self-replicating attack that is independently launched.
- **Malware that relies on the action of a user or a program to activate.**
- Program code specifically designed to corrupt memory in network devices.
- **Malicious code that can remain dormant before executing an unwanted action.**

Explanation: A virus is malicious code that is attached to legitimate programs or executable files. Most viruses require end user activation, can lie dormant for an extended period, and then activate at a specific time or date. In contrast, a worm executes arbitrary code and installs copies of itself in the memory of the infected computer. The main purpose of a worm is automatic replication to spread quickly across a network. A worm does not require a host program to run.

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

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

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

47. A security incident has been filed and an employee believes that someone has been on the computer since the employee left last night. The employee states that the computer was turned off before the employee left for the evening. The computer is running slowly and applications are acting strangely. Which Microsoft Windows tool would be used by the security analyst to determine if and when someone logged on to the computer after working hours?

- Task Manager
- **Event Viewer**
- PowerShell
- Performance Monitor

Explanation: Event Viewer is used to investigate the history of application, security, and system events. Events show the date and time that the event occurred along with the source of the event. If a cybersecurity analyst has the address of the Windows computer targeted or the date and time that a security breach occurred, the analyst could use Event Viewer to document and prove what occurred on the computer.

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

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

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

49. What information does an Ethernet switch examine and use to forward a frame?

- **destination MAC address**
- destination IP address
- source MAC address
- source IP address

Explanation: A switch is a Layer 2 device that uses source MAC addresses to build a MAC address table (a CAM table) and destination MAC addresses to forward frames.

50. In threat intelligence communications, which sharing standard is a specification for an application layer protocol that allows communication of cyberthreat intelligence over HTTPS?

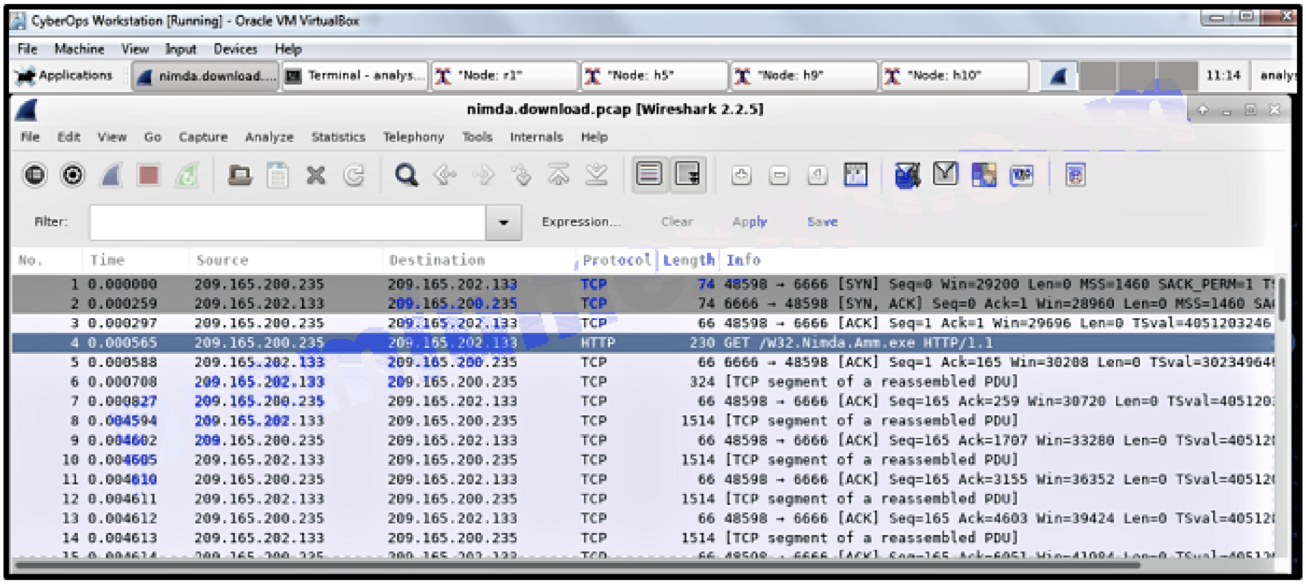
- **Trusted automated exchange of indicator information (TAXII)**
- Structured threat information expression (STIX)
- Common vulnerabilities and exposures (CVE)
- Automated indicator sharing (AIS)

Explanation: The two common threat intelligence sharing standards are as follows:

Structured Threat Information Expression (STIX) – This is a set of specifications for exchanging cyberthreat information between organizations. The Cyber Observable Expression (CybOX) standard has been incorporated into STIX.

Trusted Automated Exchange of Indicator Information (TAXII) – This is the specification for an application layer protocol that allows the communication of CTI over HTTPS. TAXII is designed to support STIX.

51. Refer to the exhibit. A network security analyst is examining captured data using Wireshark. What is represented by the first three frames?


CyberOps Workstation [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
nimda.download...
Terminal - analys...
"Node: r1"
"Node: h5"
"Node: h9"
"Node: h10"
11:14
analys
nimda.download.pcap [Wireshark 2.2.5]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save

```
No.   Time       Source            Destination       Protocol Length Info
    1 0.000000   209.165.200.235   209.165.202.133   TCP        74 48598 → 6666 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 T
    2 0.000259   209.165.202.133   209.165.200.235   TCP        74 6666 → 48598 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA
    3 0.000297   209.165.200.235   209.165.202.133   TCP        66 48598 → 6666 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=4051203246
    4 0.000565   209.165.200.235   209.165.202.133   HTTP      230 GET /W32.Nimda.Amn.exe HTTP/1.1
    5 0.000588   209.165.202.133   209.165.200.235   TCP        66 6666 → 48598 [ACK] Seq=1 Ack=165 Win=30208 Len=0 TSval=30234964
    6 0.000708   209.165.202.133   209.165.200.235   TCP       324 [TCP segment of a reassembled PDU]
    7 0.000827   209.165.200.235   209.165.202.133   TCP        66 48598 → 6666 [ACK] Seq=165 Ack=259 Win=30720 Len=0 TSval=405120
    8 0.004594   209.165.202.133   209.165.200.235   TCP      1514 [TCP segment of a reassembled PDU]
    9 0.004602   209.165.200.235   209.165.202.133   TCP        66 48598 → 6666 [ACK] Seq=165 Ack=1707 Win=33280 Len=0 TSval=40512
   10 0.004605   209.165.202.133   209.165.200.235   TCP      1514 [TCP segment of a reassembled PDU]
   11 0.004610   209.165.200.235   209.165.202.133   TCP        66 48598 → 6666 [ACK] Seq=165 Ack=3155 Win=36352 Len=0 TSval=40512
   12 0.004611   209.165.202.133   209.165.200.235   TCP      1514 [TCP segment of a reassembled PDU]
   13 0.004612   209.165.200.235   209.165.202.133   TCP        66 48598 → 6666 [ACK] Seq=165 Ack=4603 Win=39424 Len=0 TSval=40512
   14 0.004613   209.165.202.133   209.165.200.235   TCP      1514 [TCP segment of a reassembled PDU]
   15 0.004614   209.165.200.235   209.165.202.133   TCP        66 48598 → 6666 [ACK] Seq=165 Ack=6051 Win=41984 Len=0 TSval=40512
```

- request of a file from the client
- **TCP three-way handshake**
- UDP DNS request
- connectivity test between two hosts

Explanation: The first three frames consist of the SYN, SYN/ACK, and ACK exchanges that constitute the TCP three-way handshake between the two hosts.

52. The IT department is reporting that a company web server is receiving an abnormally high number of web page requests from different locations simultaneously. Which type of security attack is occurring?

- social engineering
- adware
- phishing
- **DDoS**
- spyware

Explanation: Phishing, spyware, and social engineering are security attacks that collect network and user information. Adware consists, typically, of annoying popup windows. Unlike a DDoS attack, none of these attacks generate large amounts of data traffic that can restrict access to network services.

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

- 30
- 32
- 60
- **62**

- 64

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

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

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

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

55. What are three access control security services? (Choose three.)

- **authentication**
- repudiation
- availability
- **accounting**
- **authorization**
- access

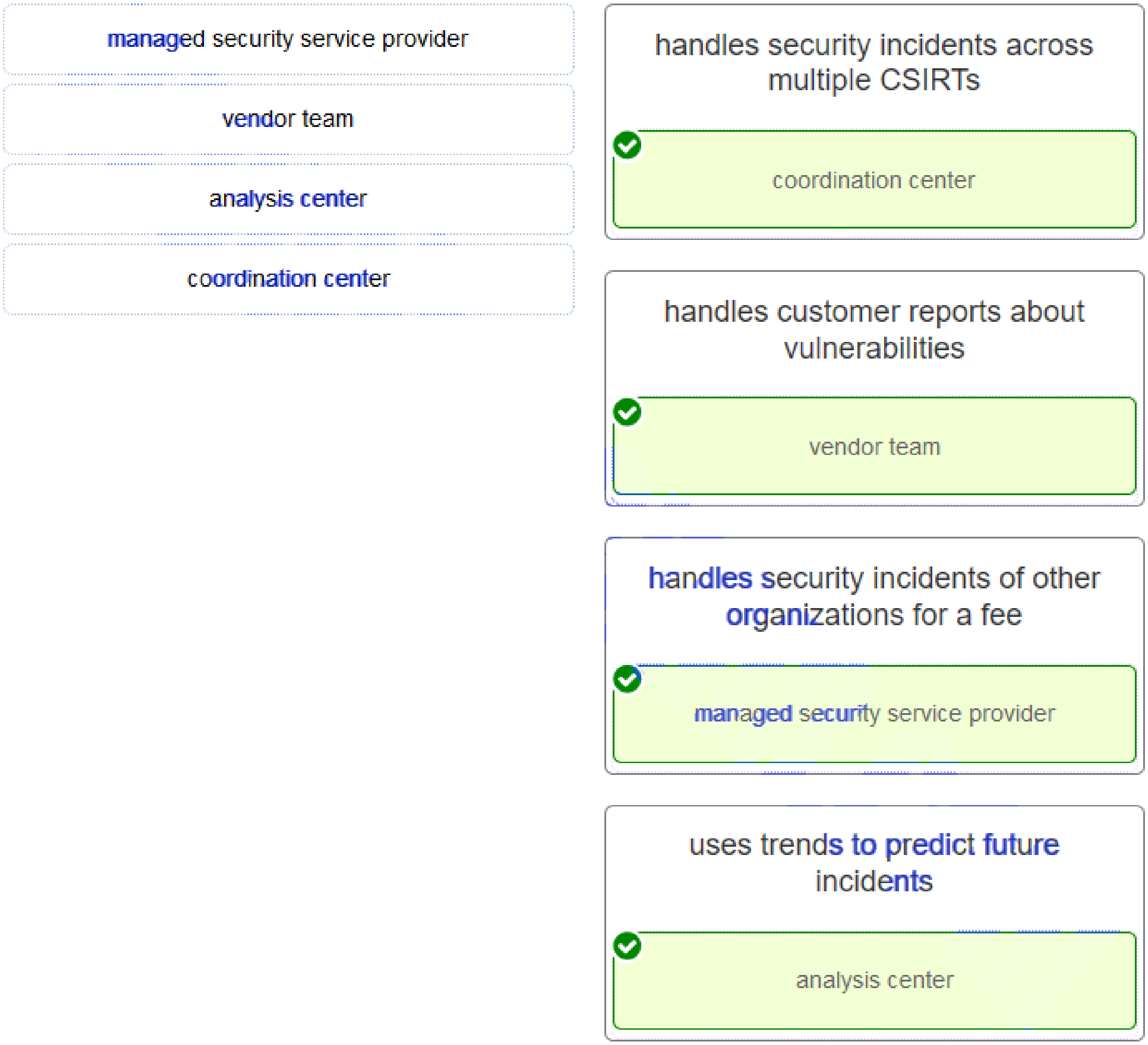
Explanation: This question refers to AAA authentication, authorization, and accountability.

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

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

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

57. Match the type of CSIRT with the description.



managed security service provider

vendor team

analysis center

coordination center

handles security incidents across multiple CSIRTs

✓ coordination center

handles customer reports about vulnerabilities

✓ vendor team

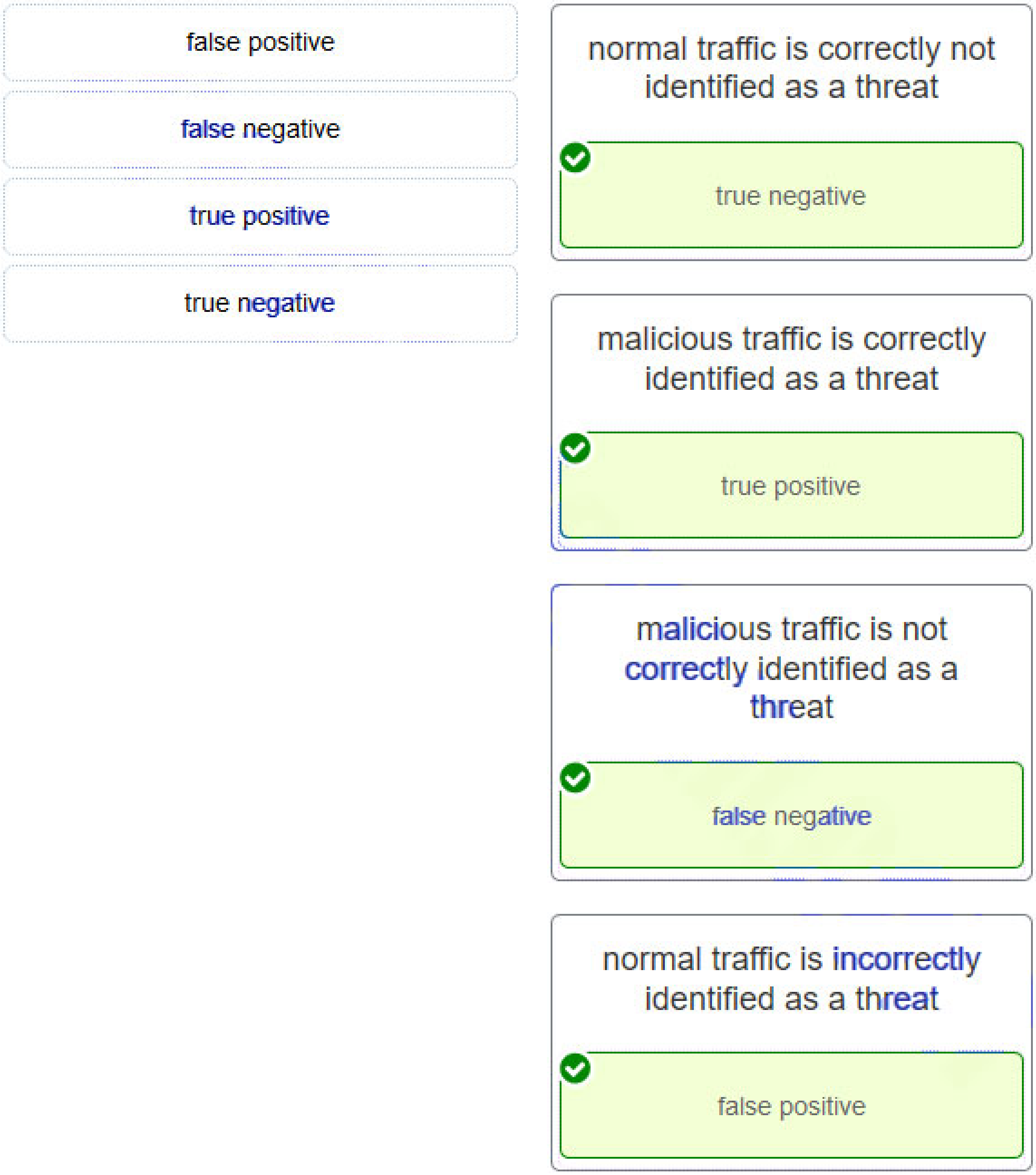
handles security incidents of other organizations for a fee

✓ managed security service provider

uses trends to predict future incidents

✓ analysis center

58. Match the IPS alarm with the description.



false positive

false negative

true positive

true negative

normal traffic is correctly not identified as a threat

✓ true negative

malicious traffic is correctly identified as a threat

✓ true positive

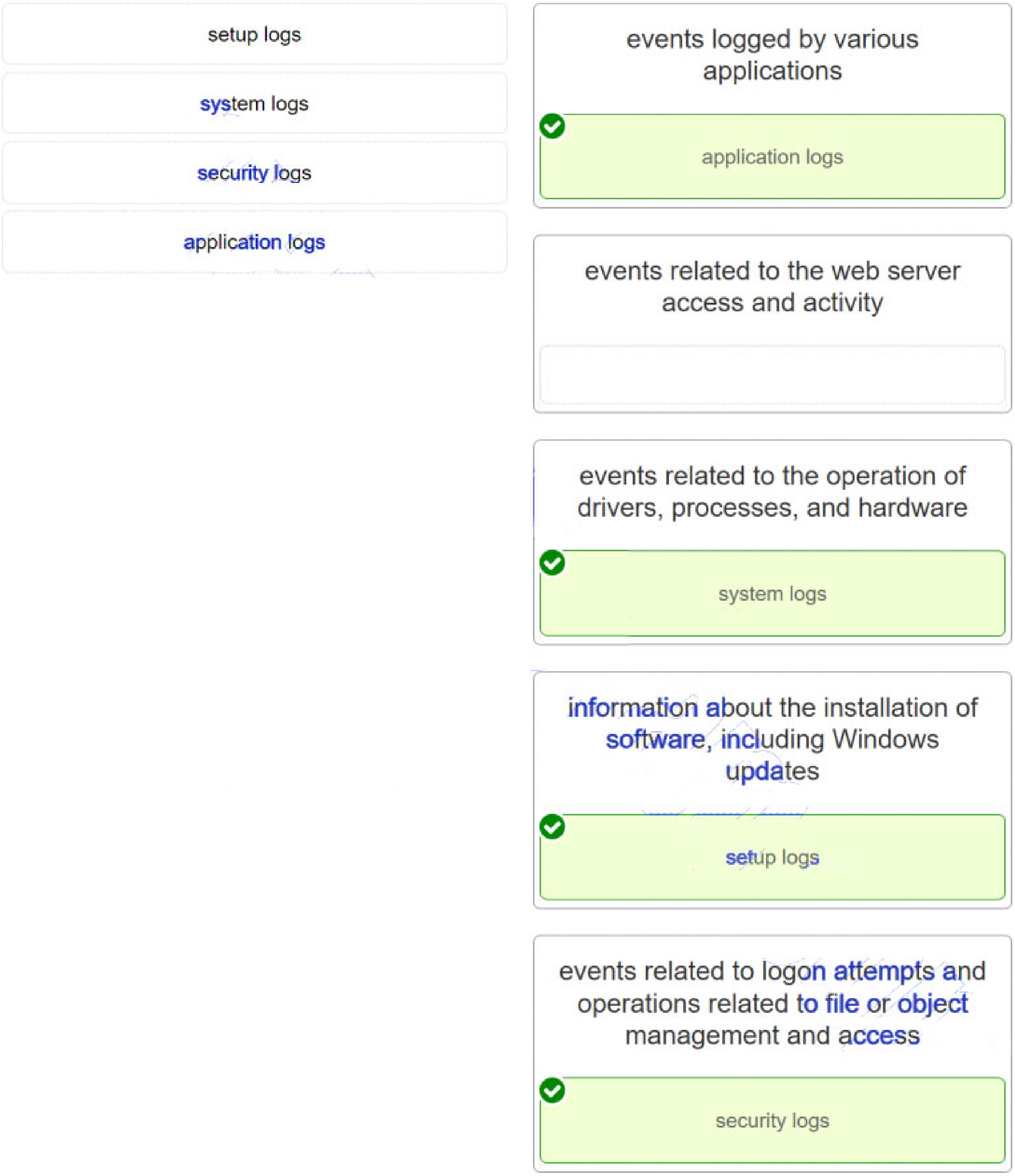
malicious traffic is not correctly identified as a threat

✓ false negative

normal traffic is incorrectly identified as a threat

✓ false positive

59. Match the Windows host log to the messages contained in it. (Not all options are used.)



setup logs

system logs

security logs

application logs

events logged by various applications

✓ application logs

events related to the web server access and activity

events related to the operation of drivers, processes, and hardware

✓ system logs

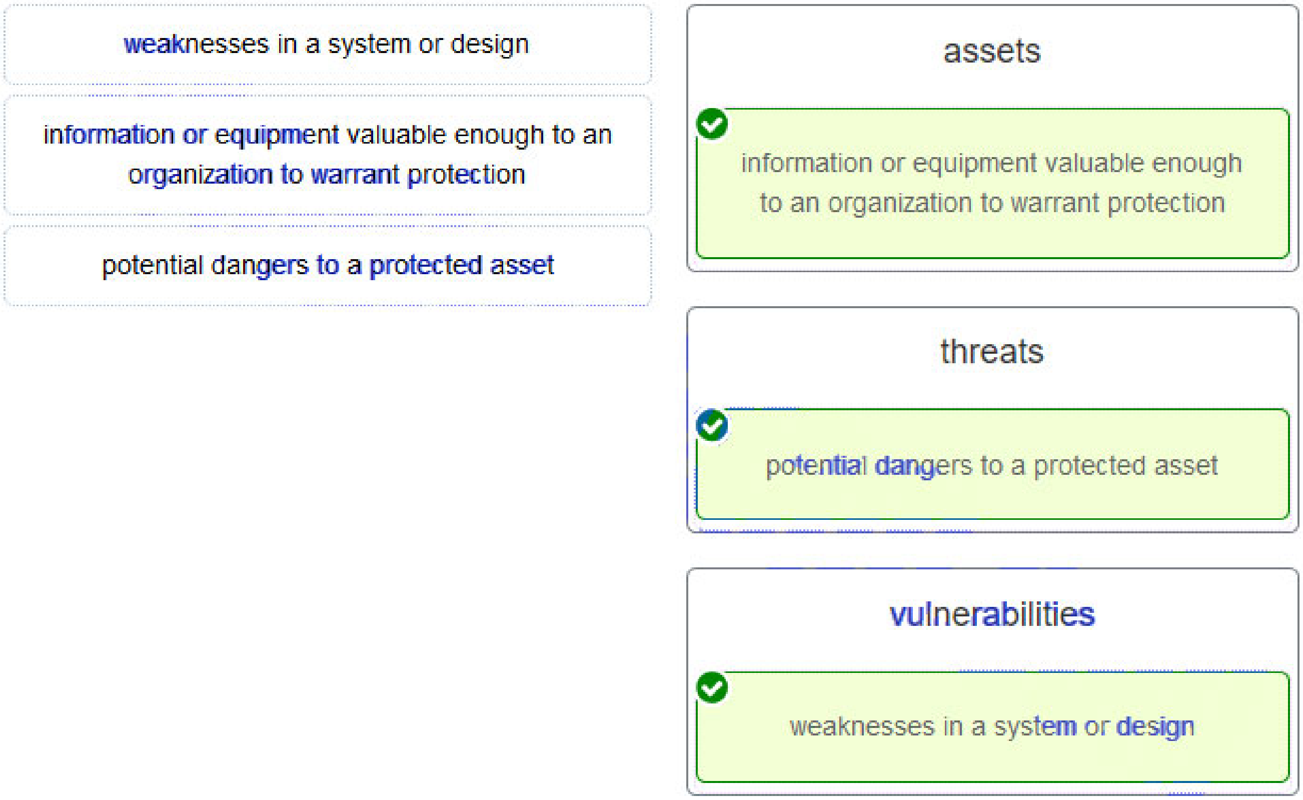
information about the installation of software, including Windows updates

✓ setup logs

events related to logon attempts and operations related to file or object management and access

✓ security logs

60. Match the term to the description.



weaknesses in a system or design

information or equipment valuable enough to an organization to warrant protection

potential dangers to a protected asset

assets

✓ information or equipment valuable enough to an organization to warrant protection

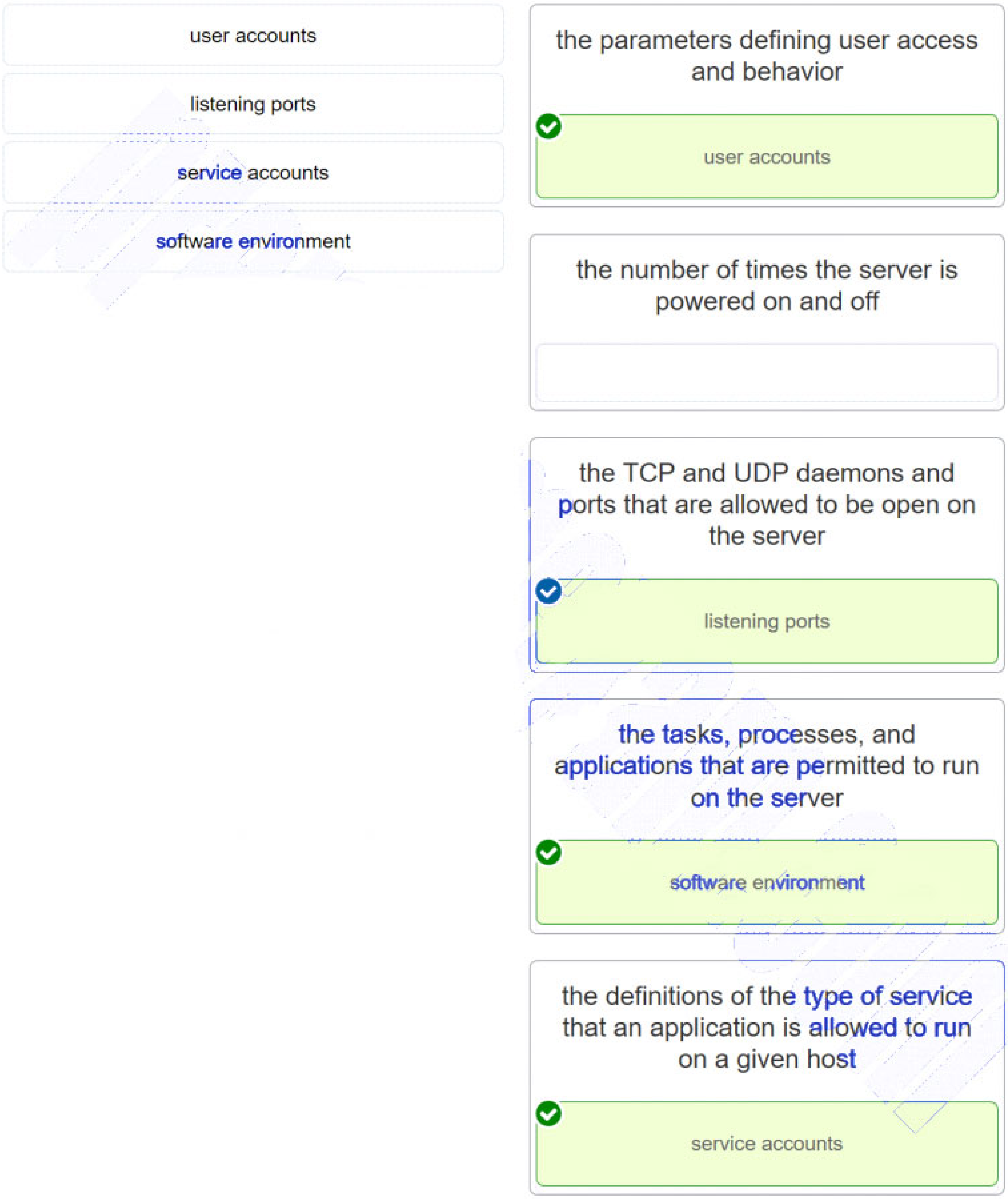
threats

✓ potential dangers to a protected asset

vulnerabilities

✓ weaknesses in a system or design

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



user accounts

listening ports

service accounts

software environment

the parameters defining user access and behavior

✓ user accounts

the number of times the server is powered on and off

the TCP and UDP daemons and ports that are allowed to be open on the server

✓ listening ports

the tasks, processes, and applications that are permitted to run on the server

✓ software environment

the definitions of the type of service that an application is allowed to run on a given host

✓ service accounts

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