CCNA Cyber Ops (Version 1.1) – FINAL Exam Answers Full

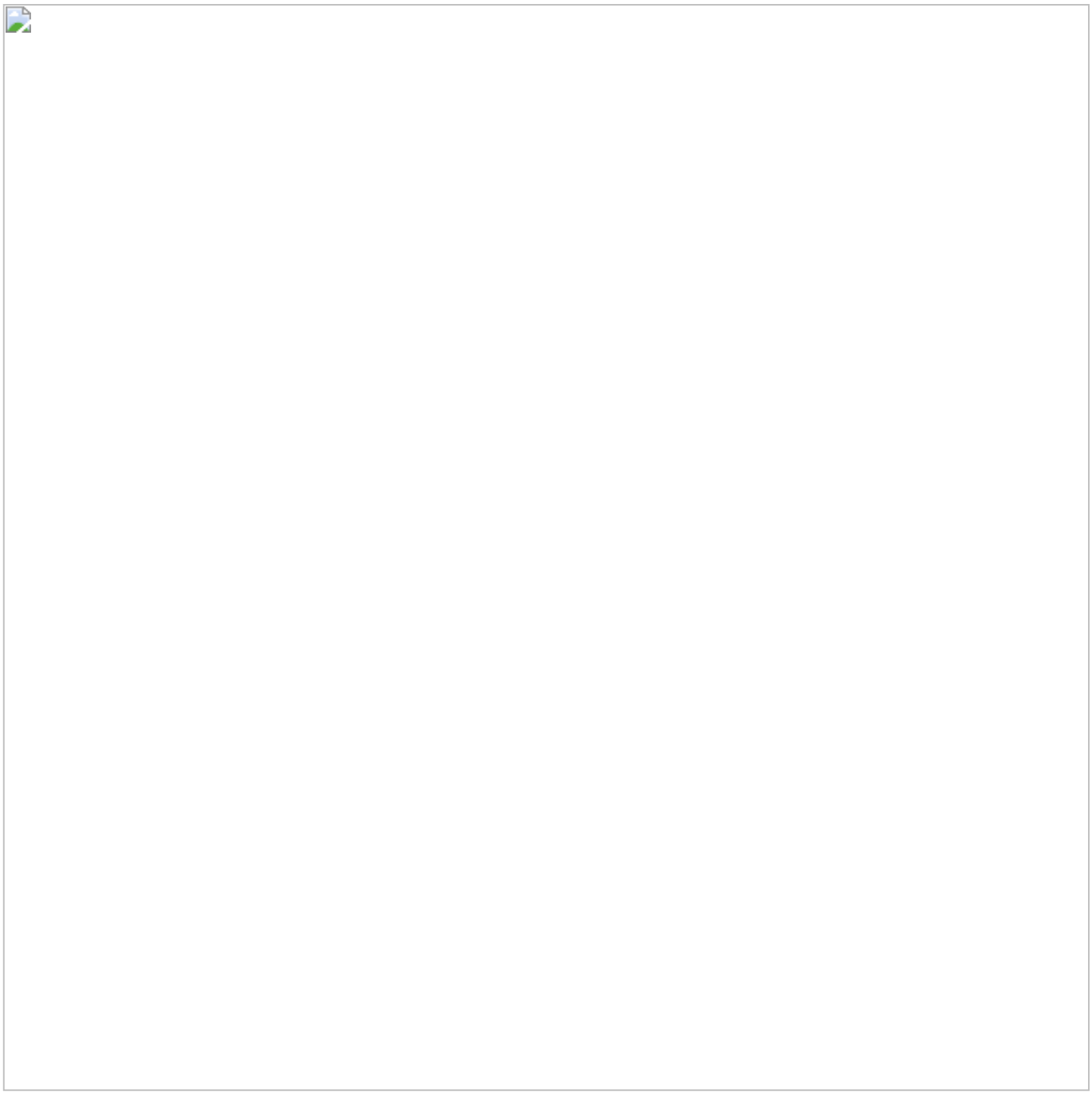
itexamanswers.net/ccna-cyber-ops-version-1-1-final-exam-answers-full.html

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.

1. Refer to the exhibit. A network security specialist issues the command `tcpdump` to capture events. What does the number 6337 indicate?



- the number of transactions currently captured
- **the process id of the tcpdump command**
- the port that tcpdump is listening to
- the Snort signature id that tcpdump will watch and capture

After the tcpdump command is issued, the device displays the message, [1] 6337. The message indicates that the process with PID 6337was sent to the background.

2. How do cybercriminals make use of a malicious iFrame?

- The iFrame allows multiple DNS subdomains to be used.
- The attacker embeds malicious content in business appropriate files.

- **The iFrame allows the browser to load a web page from another source.**
- The attacker redirects traffic to an incorrect DNS server.

An inline frame or iFrame is an HTML element that allows the browser to load a different web page from another source.

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

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

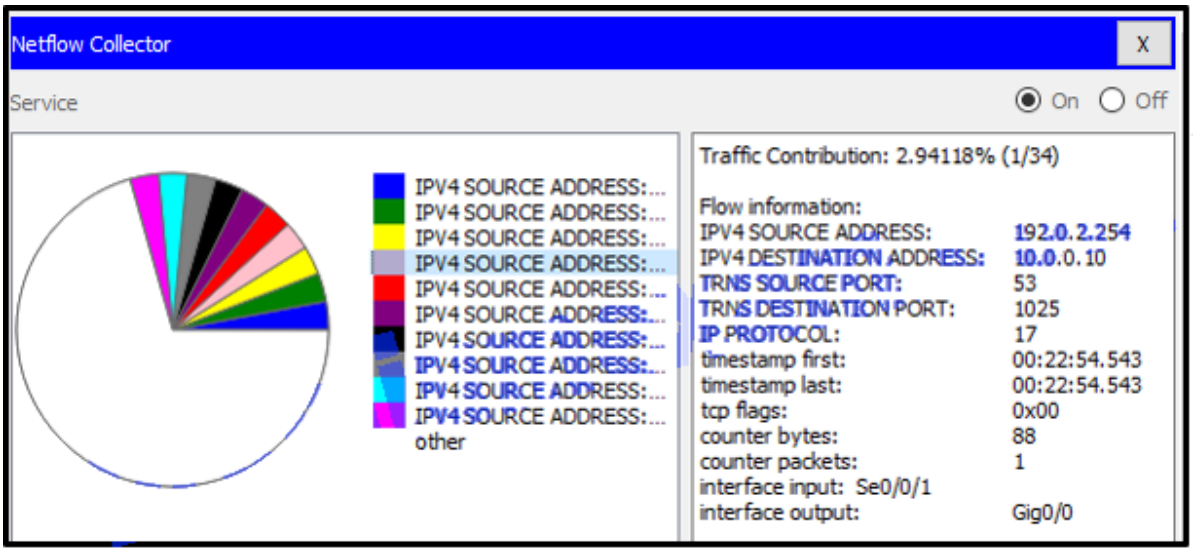
Asymmetric algorithms can use very long key lengths in order to avoid being hacked. This results in the use of significantly increased resources and time compared to symmetric algorithms.

4. What is a network tap?

- a Cisco technology that provides statistics on packets flowing through a router or multilayer switch
- a technology used to provide real-time reporting and long-term analysis of security events
- 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**

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

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



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

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

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

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

NIST describes the digital forensics process as involving the following four steps:

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

7. 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**

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

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

- firewall appliance
- **threat intelligence**
- VPN connection
- **security monitoring**
- **vulnerability tracking**
- intrusion prevention

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

9. In which situation is an asymmetric key algorithm used?

- An office manager encrypts confidential files before saving them to a removable device.
- Two Cisco routers authenticate each other with CHAP.
- User data is transmitted across the network after a VPN is established.
- **A network administrator connects to a Cisco router with SSH.**

The SSH protocol uses an asymmetric key algorithm to authenticate users and encrypt data transmitted. The SSH server generates a pair of public/private keys for the connections. Encrypting files before saving them to a storage device uses a symmetric key algorithm because the same key is used to encrypt and decrypt files. The router authentication with CHAP uses a

symmetric key algorithm. The key is pre-configured by the network administrator. A VPN may use both an asymmetric key and a symmetric encryption algorithm. For example in an IPSec VPN implementation, the data transmission uses a shared secret (generated with an asymmetric key algorithm) with a symmetric encryption algorithm used for performance.

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

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

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

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

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

By default Windows keeps four types of host logs:

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

12. What is the responsibility of the human resources department when handling a security incident?

- Perform actions to minimize the effectiveness of the attack and preserve evidence.
- Review the incident policies, plans, and procedures for local or federal guideline violations.
- Coordinate the incident response with other stakeholders and minimize the damage of the incident.
- **Apply disciplinary measures if an incident is caused by an employee.**

The human resources department may be called upon to perform disciplinary measures if an incident is caused by an employee.

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

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

14. A network security professional has applied for a Tier 2 position in a SOC. What is a typical job function that would be assigned to a new employee?

- monitoring incoming alerts and verifying that a true security incident has occurred
- hunting for potential security threats and implementing threat detection tools
- **further investigating security incidents**
- serving as the point of contact for a customer

In a typical SOC, the job of a Tier 2 incident responder involves deep investigation of security incidents.

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

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

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

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

- scalability
- authorization

- virtualization
- **encryption**

Confidential and secure transfers of data with VPNs require data encryption.

17. As described by the SANS Institute, which attack surface includes the use of social engineering?

- Internet attack surface
- software attack surface
- **human attack surface**
- network attack surface

The SANS Institute describes three components of the attack surface:

- **Network Attack Surface –** exploitation of vulnerabilities in networks
- **Software Attack Surface –** exploitation of vulnerabilities in web, cloud, or host-based software applications
- **Human Attack Surface –** exploitation of weaknesses in user behavior

18. Refer to the exhibit. A network administrator is showing a junior network engineer some output on the server. Which service would have to be enabled on the server to receive such output?

	Time	HostName	Message
1	10.22.2017 02:50:27.292 PM	192.168.30.1	ICMP; echo reply sent, src 209.165.200.226, dst 209.165.200.225
2	10.22.2017 02:50:28.404 PM	192.168.30.1	ICMP; echo reply sent, src 209.165.200.226, dst 209.165.200.225
3	10.22.2017 02:50:29.503 PM	192.168.30.1	ICMP; echo reply sent, src 209.165.200.226, dst 209.165.200.225
4	10.22.2017 02:50:30.609 PM	192.168.30.1	ICMP; echo reply sent, src 209.165.200.226, dst 209.165.200.225

- **SNMP**
- ICMP
- debug
- AAA

The Simple Network Management Protocol is used by network devices to send and log messages to a syslog server in order to monitor traffic and network device events. The syslog service must be enabled on the server or a syslog server application must be installed in order to receive such traffic.

19. Which scenario is probably the result of activities by a group of hacktivists?

- The major power grid in a country is experiencing frequent attacks from another country.
- The central database of student grades is accessed and a few grades are modified illegally.
- The sales record files of recent years in a large company suddenly cannot be opened and an offer comes forward promising that the data could be restored for a hefty fee.

- **The internal emails related to the handling of an environmental disaster by a petroleum company appear on multiple websites.**

Hacktivists are typically hackers who protest against a variety of political and social ideas. Hacktivists publicly protest against organizations or governments by posting articles and leaking sensitive information. Accessing school database and changing grades is probably made by a few script kiddies. Offers from someone to restore data for a hefty fee is a ransomware attack. Attacking the major power grid is typically conducted by a government.

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

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

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

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

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

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

22. Which statement identifies an important difference between the TACACS+ and RADIUS protocols?

- TACACS+ provides extensive accounting capabilities when compared to RADIUS.
- RADIUS can cause delays by establishing a new TCP session for each authorization request.
- The RADIUS protocol encrypts the entire packet transmission.

- **The TACACS+ protocol allows for separation of authentication from authorization.**

One key difference between TACACS+ and RADIUS protocols is that TACACS+ provides flexibility by separating authentication and authorization processes. RADIUS, on the other hand, combines authentication and authorization as one process.

23. What is a function of SNMP?

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

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

24. What commonly motivates cybercriminals to attack networks as compared to hactivists or state-sponsored hackers?

- fame seeking
- **financial gain**
- status among peers
- political reasons

Cybercriminals are commonly motivated by money. Hackers are known to hack for status. Cyberterrorists are motivated to commit cybercrimes for religious or political reasons.

25. In a networking class, the instructor tells the students to ping the other computers in the classroom from the command prompt. Why do all pings in the class fail?

- Port 25 is blocked and preventing the echo request from being transmitted.
- The computers are on different networks.
- A virus is on the classroom computers.
- **The Windows firewall is blocking the ping.**

Unsuccessful pings usually indicate a network problem which eliminates the virus option. In this case computers in the same classroom would also be on the same network. Port 25 is used used by the email SMTP protocol, not by ping.

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

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

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.

27. Because of implemented security controls, a user can only access a server with FTP. Which AAA component accomplishes this?

- auditing
- **authorization**
- accessibility
- accounting
- authentication

One of the components in AAA is authorization. After a user is authenticated through AAA, authorization services determine which resources the user can access and which operations the user is allowed to perform.

28. Which protocol translates a website name such as www.cisco.com into a network address?

- **DNS**
- HTTP
- FTP
- DHCP

Domain Name Service translates names into numerical addresses, and associates the two. DHCP provides IP addresses dynamically to pools of devices. HTTP delivers web pages to users. FTP manages file transfers.

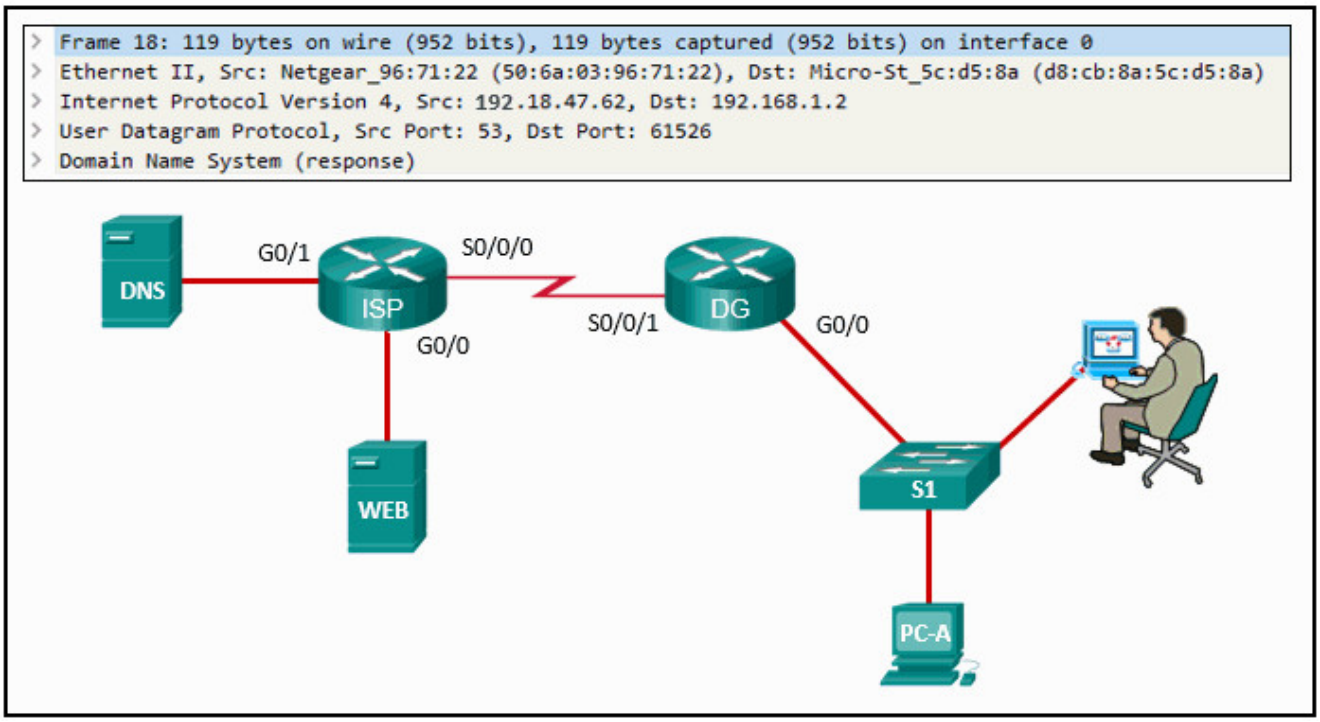
29. How might DNS be used by a threat actor to create mayhem?

- Change the timestamp on network messages in order to conceal the cyberattack.

- Surveil or deny service from outside the corporate network.
- **Collect personal information and encode the data in outgoing DNS queries.**
- Intercept and decrypt network traffic.

Malware could be used by a threat actor to collect stolen encoded data, decode it, and then gain access to corporate data such as a username/password database.

30. Refer to the exhibit. A cybersecurity analyst is viewing captured packets forwarded on switch S1. Which device has the MAC address d8:cb:8a:5c:d5:8a?



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

The Wireshark capture is a DNS response from the DNS server to PC-A. Because the packet was captured on the LAN that the PC is on, router DG would have encapsulated the response packet from the ISP router into an Ethernet frame addressed to PC-A and forwarded the frame with the MAC address of PC-A as the destination.

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

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

- It compares the signatures of incoming traffic to a known intrusion database.

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

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

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

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

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

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

NetFlow efficiently provides an important set of services for IP applications including network traffic accounting, usage-based network billing, network planning, security, denial of service monitoring capabilities, and network monitoring.

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

- The administrator has control over specific security functions, but not standard applications.
- It is easier to use than other server operating systems.
- More network applications are created for this environment.
- **It can be acquired at no charge.**

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

35. Which two statements describe access attacks? (Choose two.)

- **Buffer overflow attacks write data beyond the allocated buffer memory to overwrite valid data or to exploit systems to execute malicious code.**
- Port redirection attacks use a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN.
- Trust exploitation attacks often involve the use of a laptop to act as a rogue access point to capture and copy all network traffic in a public location, such as a wireless hotspot.
- To detect listening services, port scanning attacks scan a range of TCP or UDP port numbers on a host.
- **Password attacks can be implemented by the use of brute-force attack methods, Trojan horses, or packet sniffers.**

An access attack tries to gain access to a resource using a hijacked account or other means. The five types of access attacks include the following:password – a dictionary is used for repeated login attempts
trust exploitation – uses granted privileges to access unauthorized material
port redirection – uses a compromised internal host to pass traffic through a firewall
man-in-the-middle – an unauthorized device positioned between two legitimate devices in order to redirect or capture traffic
buffer overflow – too much data sent to a memory location that already contains data

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

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

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

37. Which Linux command could be used to discover the process ID (PID) for a specific process before using the *kill* command?

- **ps**
- ls
- chkrootkit
- grep

38. Which two characteristics describe a worm? (Choose two.)

- infects computers by attaching to software code
- **travels to new computers without any intervention or knowledge of the user**
- hides in a dormant state until needed by an attacker

- executes when software is run on a computer
- **is self-replicating**

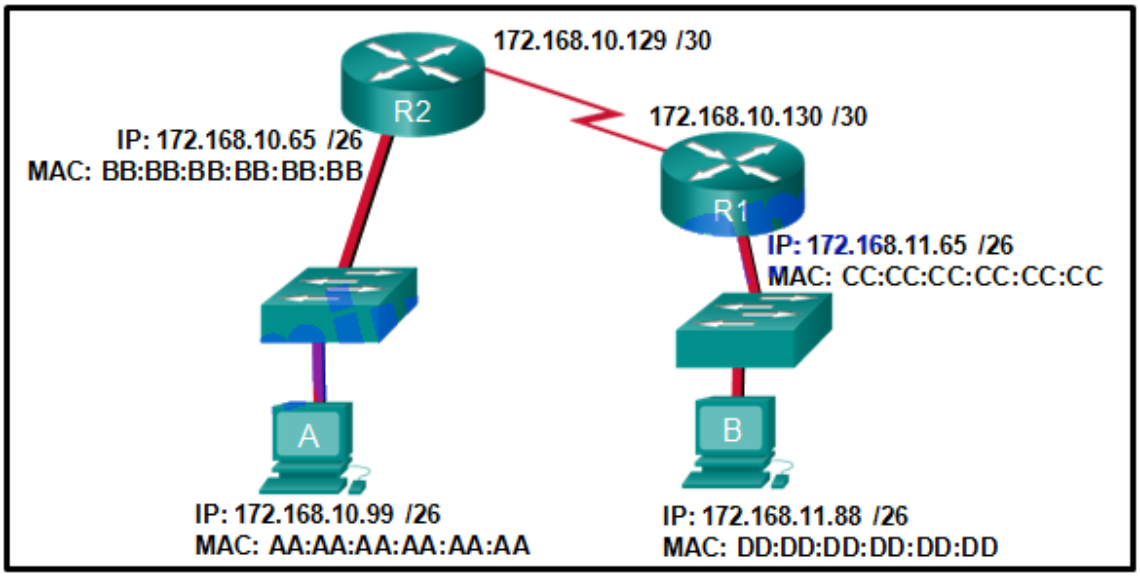
Worms are self-replicating pieces of software that consume bandwidth on a network as they propagate from system to system. They do not require a host application, unlike a virus. Viruses, on the other hand, carry executable malicious code which harms the target machine on which they reside.

39. Which two roles are typically performed by a wireless router that is used in a home or small business? (Choose two.)

- WLAN controller
- RADIUS authentication server
- **Ethernet switch**
- **access point**
- repeater

In addition to its roles as router, a typical SOHO wireless router acts as both a wireless access point and an Ethernet switch. RADIUS authentication is provided by an external server. A WLAN controller is used in enterprise deployments to manage groups of lightweight access points. A repeater is a device that enhances an incoming signal and retransmits it.

40. Refer to the exhibit. If host A sends an IP packet to host B, what will the destination address be in the frame when it leaves host A?



- AA:AA:AA:AA:AA:AA
- CC:CC:CC:CC:CC:CC
- DD:DD:DD:DD:DD:DD
- 172.168.10.65

- 172.168.10.99
- **BB:BB:BB:BB:BB:BB**

When a host sends information to a distant network, the Layer 2 frame header will contain a source and destination MAC address. The source address will be the originating host device. The destination address will be the router interface that connects to the same network. In the case of host A sending information to host B, the source address is AA:AA:AA:AA:AA:AA and the destination address is the MAC address assigned to the R2 Ethernet interface, BB:BB:BB:BB:BB:BB.

41. A threat actor has gained administrative access to a system and achieved the goal of controlling the system for a future DDoS attack by establishing a communication channel with a CnC owned by the threat actor. Which phase in the Cyber Kill Chain model describes the situation?

- delivery
- exploitation
- command and control
- **action on objectives**

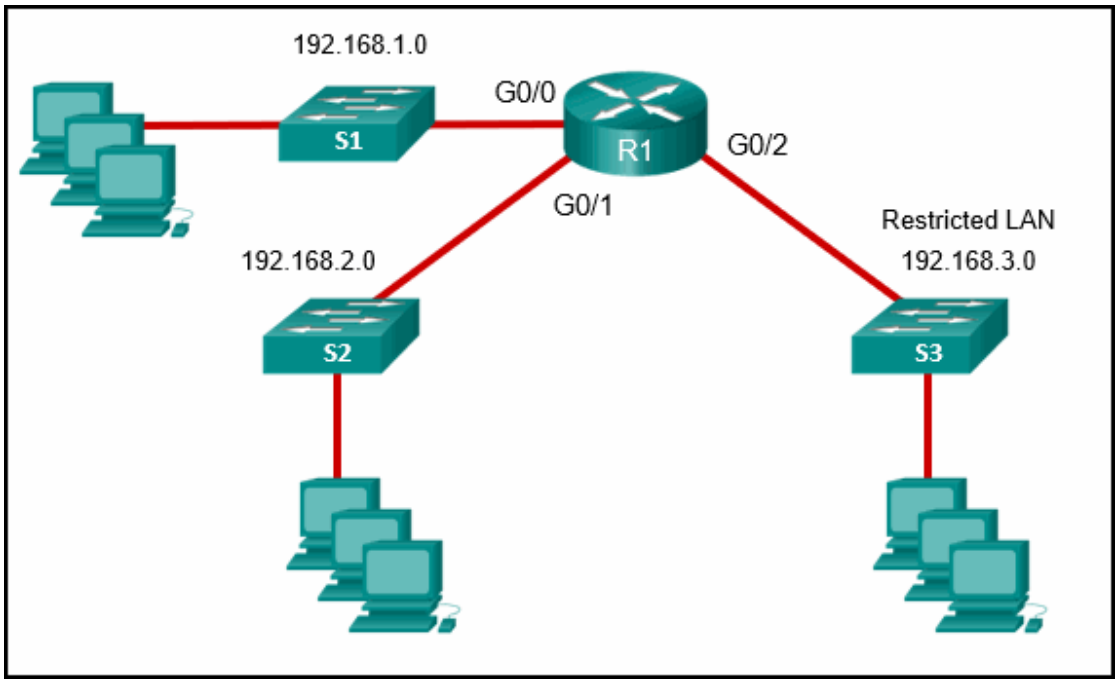
The Cyber Kill Chain specifies seven steps (or phases) and sequences that a threat actor must complete to accomplish an attack:
Reconnaissance – The threat actor performs research, gathers intelligence, and selects targets.
Weaponization – The threat actor uses the information from the reconnaissance phase to develop a weapon against specific targeted systems.
Delivery – The weapon is transmitted to the target using a delivery vector.
Exploitation – The threat actor uses the weapon delivered to break the vulnerability and gain control of the target.
Installation – The threat actor establishes a back door into the system to allow for continued access to the target.
Command and Control (CnC) – The threat actor establish command and control (CnC) with the target system.
Action on Objectives – The threat actor is able to take action on the target system, thus achieving the original objective.

42. How is a source IP address used in a standard ACL?

- It is used to determine the default gateway of the router that has the ACL applied.
- It is the address that is unknown, so the ACL must be placed on the interface closest to the source address.
- It is the address to be used by a router to determine the best path to forward packets.
- **It is the criterion that is used to filter traffic.**

The only filter that can be applied with a standard ACL is the source IP address. An extended ACL is used to filter on such traffic as the source IP address, destination IP address, type of traffic, and type of message.

43. Refer to the exhibit. Which access list configuration on router R1 will prevent traffic from the 192.168.2.0 LAN from reaching the Restricted LAN while permitting traffic from any other LAN?



R1(config-std-nacl)# permit any
R1(config-std-nacl)# deny 192.168.2.0
R1(config)# interface G0/2
R1(config-if)# ip access-group BLOCK_LAN2 out
R1(config-std-nacl)# deny 192.168.2.0
R1(config-std-nacl)# permit any
R1(config)# interface G0/2
R1(config-if)# ip access-group BLOCK_LAN2 out

R1(config-std-nacl)# deny 192.168.3.0
R1(config-std-nacl)# permit any
R1(config)# interface G0/2
R1(config-if)# ip access-group BLOCK_LAN2 in

R1(config-std-nacl)# permit any
R1(config-std-nacl)# deny 192.168.3.0
R1(config)# interface G0/2
R1(config-if)# ip access-group BLOCK-LAN2 in

The correct access list syntax requires that the deny source IP address (192.168.2.0) statement come before the permit statement so that only traffic sourced from the 192.168.2.0 LAN is denied. Then the access list must be applied on interface G0/2 in the outbound direction.

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

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

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

45. 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.

HTTPS adds extra overhead to the HTTP-formed packet. HTTPS encrypts using Secure Sockets Layer (SSL). Even though some devices can perform SSL decryption and inspection, this can present processing and privacy issues.

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

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

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

47. What are two advantages of using the community VERIS database? (Choose two.)

- **Data is in a format that allows for manipulation.**
- The data sets are compact for easy download.
- **The data is open and free to the public.**
- The access fee is minimal.
- The database is sponsored and backed by governments.

The VERIS community database (VCDB) is open and free to the public. The VCDB uses metrics to describe incidents in a structured and repeatable way, thus allowing for data manipulation.

48. 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?

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

A firewall is typically a second line of defense in a layered defense-in-depth approach to network security. The firewall typically connects to an edge router that connects to the service provider. The firewall tracks connections initiated within the company going out of the company and denies initiation of connections from external untrusted networks going to internal trusted networks.

49. Based on the command output shown, which file permission or permissions have been assigned to the other user group for the data.txt file?

```
ls –l data.txt
-rwxrw-r-- sales staff 1028 May 28 15:50 data.txt
```

- read, write
- read, write, execute
- **read**
- full access

The file permissions are always displayed in the user, group and other order. In the example displayed, the file has the following permissions:
The dash (-) means that this is a file. For directories, the first dash would be replaced with a “d”.
The first set of characters is for user permission (rwx). The user, sales, who owns the file can read, write and execute the file.
The second set of characters is for group permissions (rw-). The group, staff, who owns the file

can read and write to the file.
The third set of characters is for any other user or group permissions (r–). Any other user or group on the computer can only read the file.

50. What is indicated by a true negative security alert classification?

- **Normal traffic is correctly ignored and erroneous alerts are not being issued.**
- An alert is verified to be an actual security incident.
- Exploits are not being detected by the security systems that are in place.
- An alert is incorrectly issued and does not indicate an actual security incident.

True negative classifications are desirable because they indicate that normal traffic is correctly not being identified as malicious traffic by security measures.

51. Which metric class in the CVSS Basic Metric Group identifies the impacts on confidentiality, integrity, and availability?

- Exploitability
- Modified Base
- **Impact**
- Exploit Code Maturity

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

- **Exploitability metrics –** features of the exploit such as the vector, complexity, and user interaction required by the exploit
- **Impact metrics –** the impacts of the exploit rooted in the CIA triad of confidentiality, integrity, and availability

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

- **pivot**
- reconnaissance
- **rootkit**
- Trojan horse
- phishing

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

53. Which technology might increase the security challenge to the implementation of IoT in an enterprise environment?

- CPU processing speed
- data storage
- **cloud computing**
- network bandwidth

With cloud computing, boundaries of enterprise networks are expanded to include locations on the Internet for which the enterprises are not responsible. Malicious software might access the internal network endpoints to attack internal networks.

54. Which type of security threat would be responsible if a spreadsheet add-on disables the local software firewall?

- brute-force attack
- **Trojan horse**
- buffer overflow
- DoS

A Trojan horse is software that does something harmful, but is hidden in legitimate software code. A denial of service (DoS) attack results in interruption of network services to users, network devices, or applications. A brute-force attack commonly involves trying to access a network device. A buffer overflow occurs when a program attempts to store more data in a memory location than it can hold.

55. Why is Diffie-Hellman algorithm typically avoided for encrypting data?

- DH requires a shared key which is easily exchanged between sender and receiver.
- Most data traffic is encrypted using asymmetrical algorithms.
- DH runs too quickly to be implemented with a high level of security.
- **The large numbers used by DH make it too slow for bulk data transfers.**

Diffie-Hellman (DH) is an asymmetric mathematical algorithm that is too slow for encrypting large amounts of data. The longer key length and complexity of DH make it ideal for generating the keys used by symmetric algorithms. Symmetric algorithms typically encrypt the data, whereas DH creates the keys they use.

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

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

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

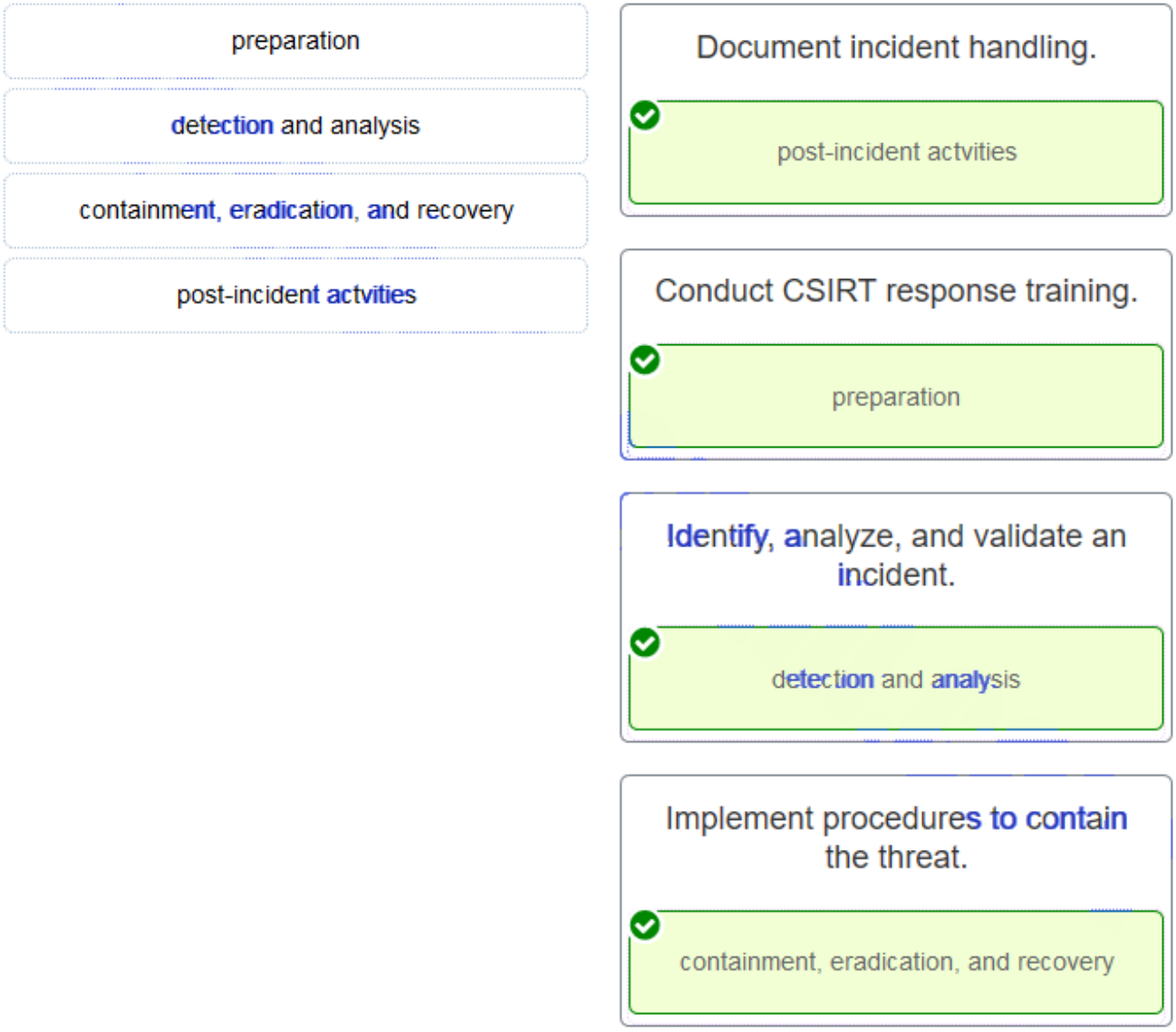
- `net accounts` – sets password and logon requirements for users
- `net session` – lists or disconnects sessions between a computer and other computers on the network
- `net share` – creates, removes, or manages shared resources
- `net start` – starts a network service or lists running network services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

57. Which Linux command could be used to discover the process ID (PID) for a specific process before using the kill command?

- chkrootkit
- grep
- ls
- **ps**

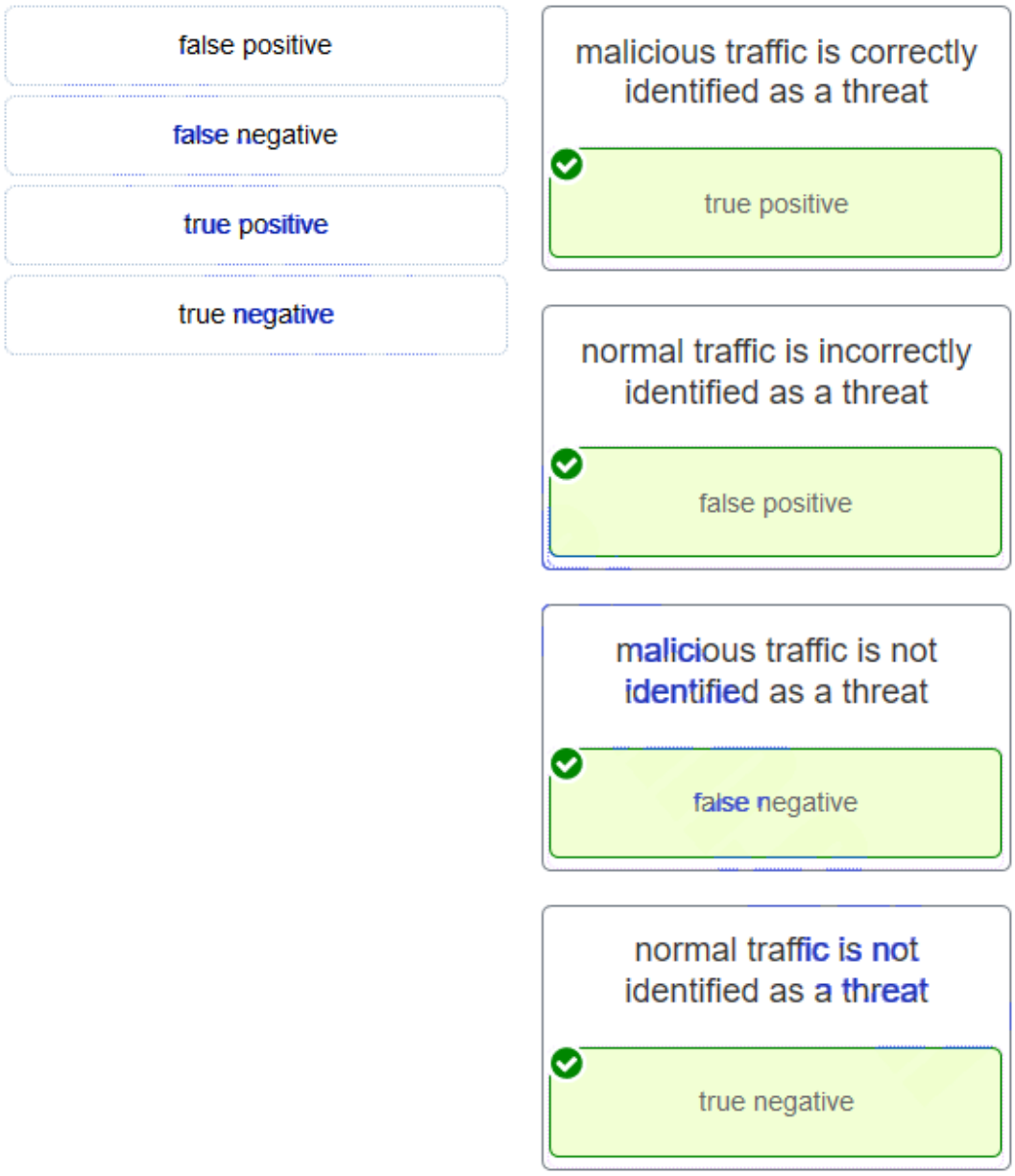
The ps command is used before the kill command to discover the PID for the specific process. The kill command requires root privileges, but listing the processes that use the ps command does not.

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



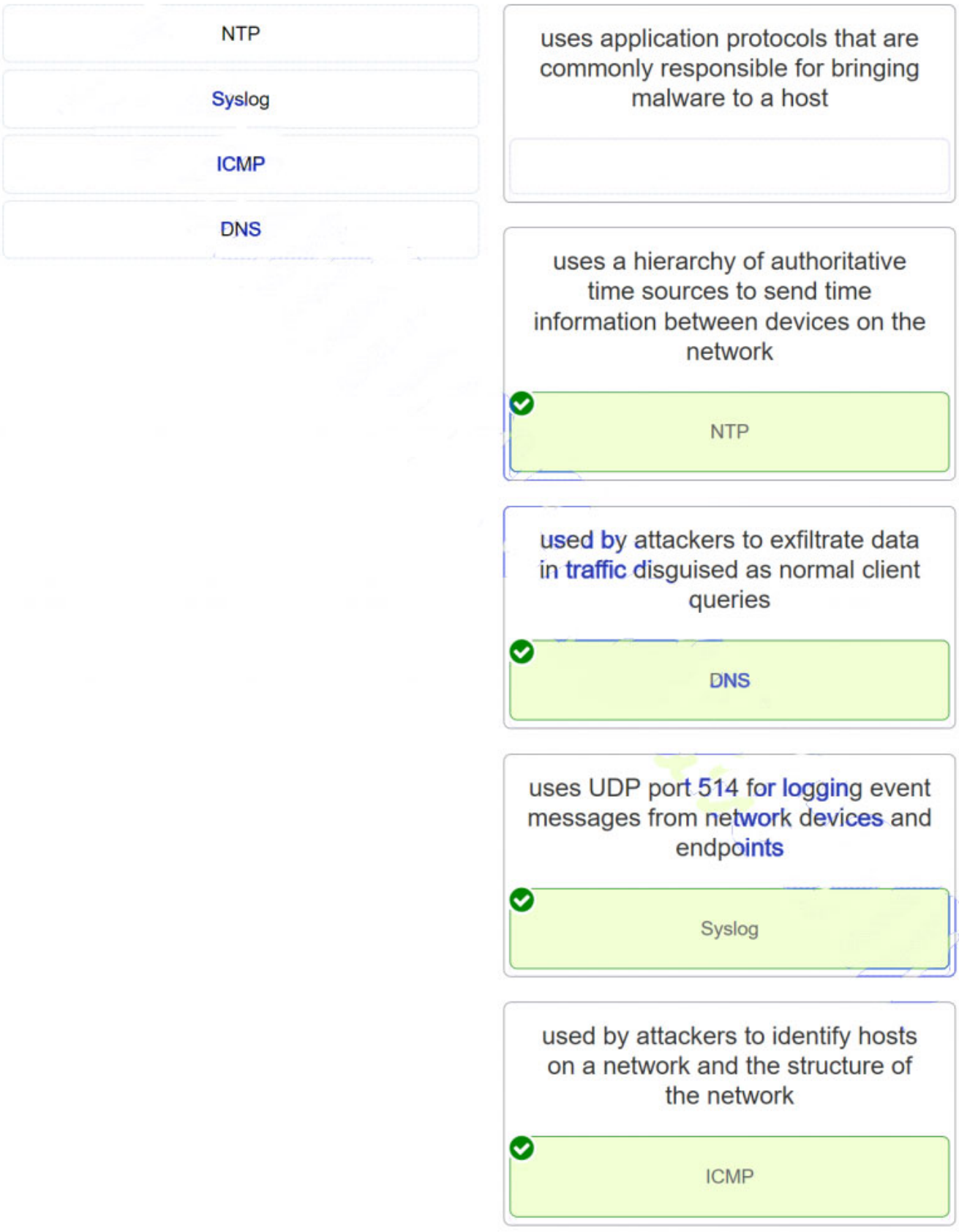
- Document incident handling. –> post-incident actvities
- Conduct CSIRT response training. –> preparation
- Identify, analyze, and validate an incident. –> detection and analysis
- Implement procedures to contain the threat. –> containment, eradication, and recovery

59. Match the alert classification with the description.



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

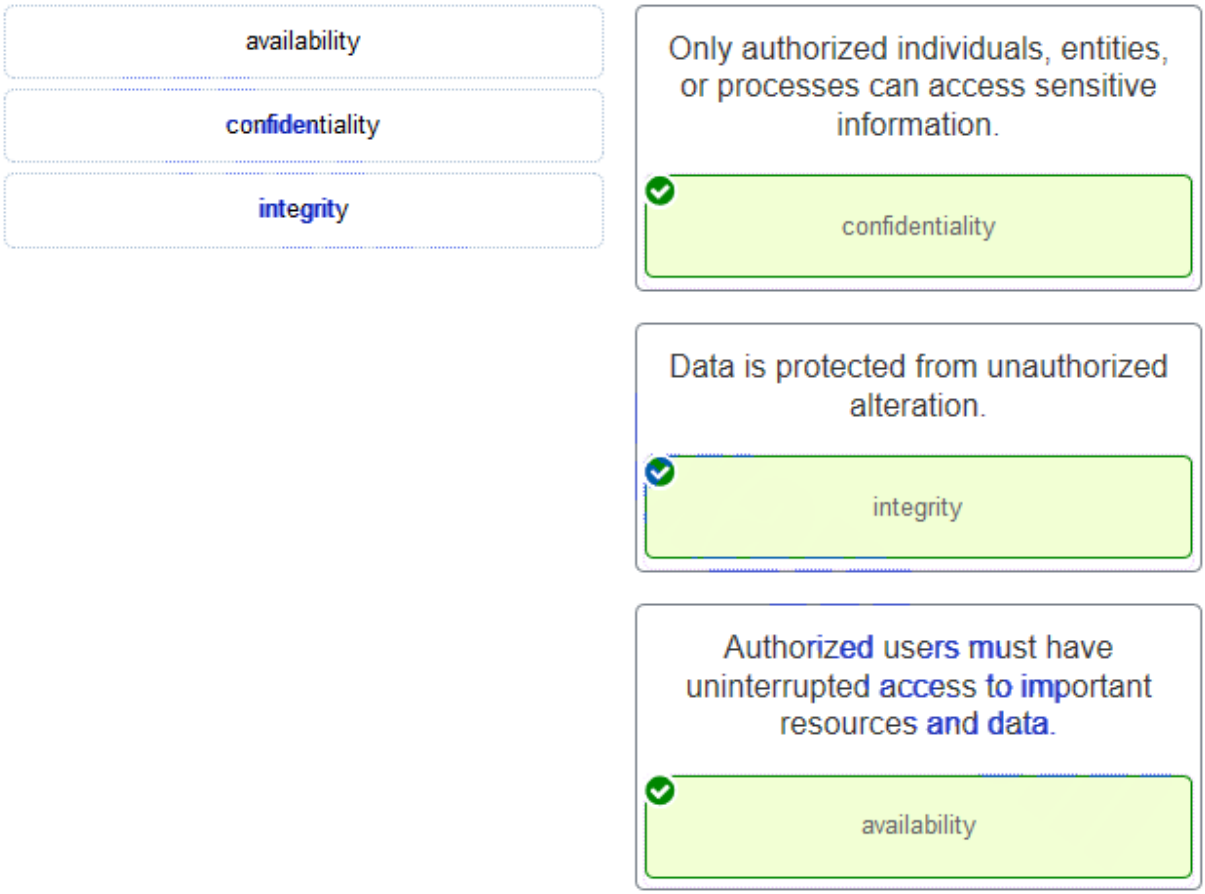
60. Match the common network technology or protocol with the description. (Not all options are used.)



- NTP –> uses a hierarchy of authoritative time sources to send time information between devices on the network
- DNS –> used by attackers to exfiltrate data in traffic disguised as normal client queries

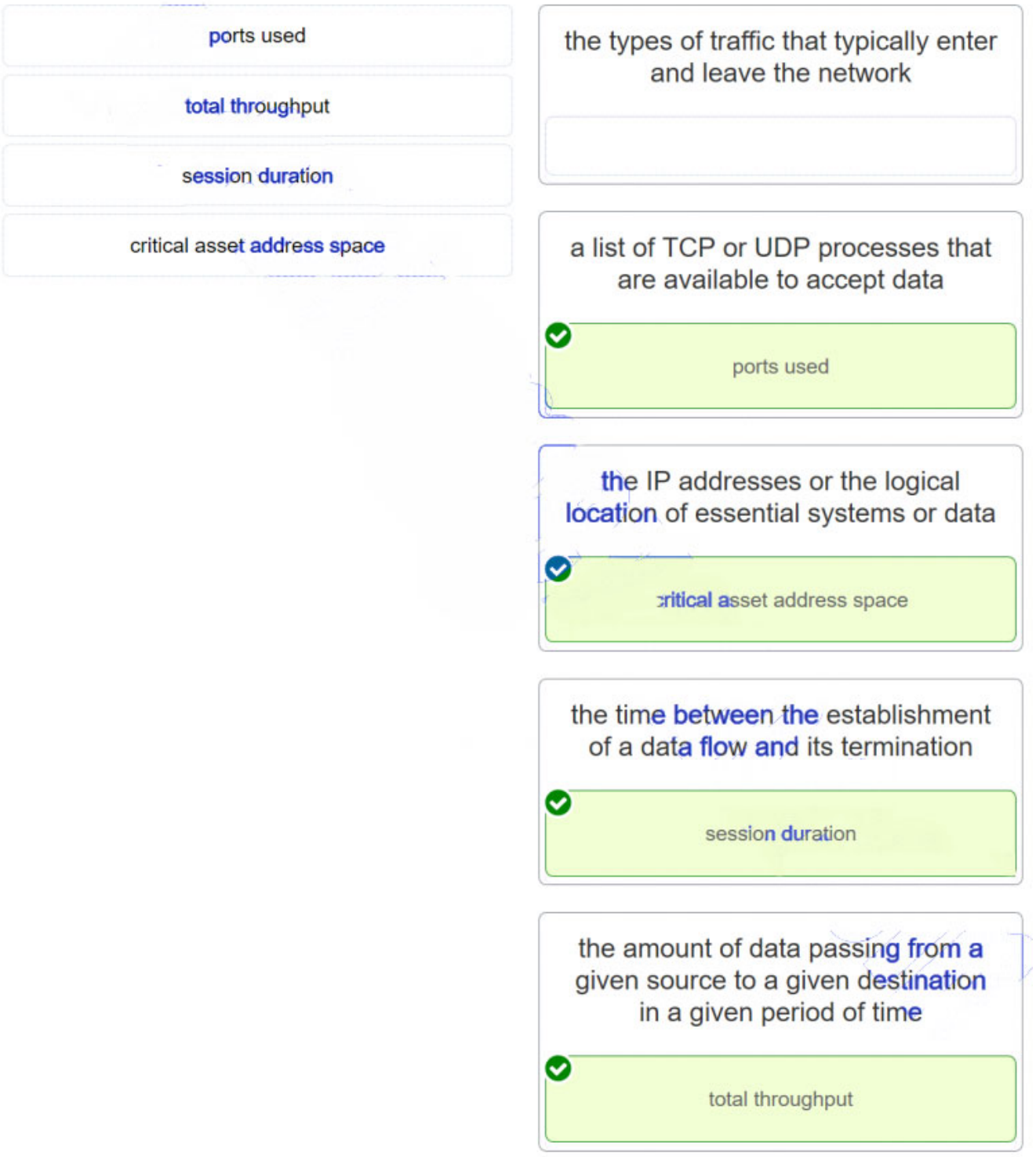
- Syslog –> uses UDP port 514 for logging event messages from network devices and endpoints
- ICMP –> used by attackers to identify hosts on a network and the structure of the network

61. Match the information security component with the description.



Only authorized individuals, entities, or processes can access sensitive information –> confidentiality
Data is protected from unauthorized alteration. –> integrity
Authorized users must have uninterrupted access to important resources and data. –> availability

62. Match the network profile element to the description. (Not all options are used.)



Important elements of a network profile include:

- **Total throughput** – the amount of data passing from a given source to a given destination in a given period of time
- **Session duration** – the time between the establishment of a data flow and its termination

- **Ports used –** a list of TCP or UDP processes that are available to accept data
- **Critical asset address space –** the IP addresses or the logical location of essential systems or data