CCNA Cyber Ops (Version 1.1) – Chapter 13 Exam Answers Full

itexamanswers.net/ccna-cyber-ops-chapter-13-exam-answers-full.html

May 13, 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. 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

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

2. Which NIST incident response life cycle phase includes continuous monitoring by the CSIRT to quickly identify and validate an incident?

- **Detection and analysis**
- Preparation
- Containment, eradication, and recovery
- Post-incident activities

A. It is in the detection and analysis phase of the NIST incident response life cycle that the CSIRT identifies and validates incidents through continuous monitoring. The NIST defines four stages of the incident response life cycle.

3. Which NIST incident response life cycle phase includes training for the computer security incident response team on how to respond to an incident?

- Post-incident activities
- Containment, eradication, and recovery
- Detection and analysis
- **Preparation**

D. It is in the preparation phase of the NIST incident response life cycle phase that the CSIRT is trained on how to respond to an incident.

4. Which three aspects of a target system are most likely to be exploited after a weapon is delivered? (Choose three.)

- **Applications**
- **User accounts**
- **OS vulnerabilities**
- Existing backdoors
- Domain name space
- DHCP configurations

A, B, C. The most common exploit targets, once a weapon is delivered, are applications, operating system vulnerabilities, and user accounts. Threat actors will use an exploit that gains the effect they desire, does it quietly, and avoids detection.

5. Which meta-feature element in the Diamond Model describes tools and information (such as software, black hat knowledge base, and username and password) that the adversary uses for the intrusion event?

- Results
- Direction
- **Resources**
- Methodology

C. The resources element in the Diamond Model is used to describe one or more external resources used by the adversary for the intrusion event. The resources include software, knowledge gained by the adversary, information (e.g., username/passwords), and assets to carry out the attack.

6. Which activity is typically performed by a threat actor in the installation phase of the Cyber Kill Chain?

- Harvest email addresses of user accounts.
- Obtain an automated tool to deliver the malware payload.
- Open a two-way communication channel to the CnC infrastructure.
- **Install a web shell on the target web server for persistent access.**

D. In the installation phase of the Cyber Kill Chain, the threat actor establishes a backdoor into the system to allow for continued access to the target.

7. Which top-level element of the VERIS schema would allow a company to document the incident timeline?

- **Discovery and Response**
- Incident Description
- Incident Tracking
- Victim Demographics

8. When dealing with a security threat and using the Cyber Kill Chain model, which two approaches can an organization use to help block potential exploitations on a system? (Choose two.)

- Conduct full malware analysis.
- **Train web developers to secure code.**
- Collect email and web logs for forensic reconstruction.
- Build detections for the behavior of known weaponizers.
- **Perform regular vulnerability scanning and penetration testing.**

B, E. The most common exploit targets, once a weapon is delivered, are applications, operating system vulnerabilities, and user accounts. Amongother measures, such as regular vulnerability scanning and penetration testing, training web developers in securing code can help block potential exploitations on systems.

9. What is a chain of custody?

- **The documentation surrounding the preservation of evidence related to an incident**
- A list of all of the stakeholders that were exploited by an attacker
- The disciplinary measures an organization may perform if an incident is caused by an employee
- A plan ensuring that each party involved in an incident response understands how to collect evidence

A. A chain of custody refers to the documentation of evidence collected about an incident that is used by authorities during an investigation.

10. What type of CSIRT organization is responsible for determining trends to help predict and provide warning of future security incidents?

- **Analysis center**
- Vendor team
- Coordination center

- National CSIRT

A. There are many different types of CSIRTs and related information security organizations. Analysis centers use data from many sources to determine security incident trends that can help predict future incidents and provide early warning. This helps to mitigate the damages that incidents can cause.

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

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

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

12. According to NIST standards, which incident response stakeholder isresponsible for coordinating an incident response with other stakeholders to minimize the damage of an incident?

- IT support
- **Management**
- Legal department
- Human resources

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

13. After a threat actor completes a port scan of the public web server of an organization and identifies a potential vulnerability, what is the next phase for the threat actor in order to prepare and launch an attack as defined in the Cyber Kill Chain?

- Exploitation
- **Weaponization**
- Reconnaissance
- Action on objectives

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

14. When dealing with security threats and using the Cyber Kill Chain model, which two approaches can an organization use to help block potential exploitations of a system? (Choose two.)

- Collect email and web logs for forensic reconstruction.
- Analyze the infrastructure path used for delivery.
- **Audit endpoints to forensically determine origin of exploit.**
- Conduct full malware analysis.
- **Conduct employee awareness training and email testing.**

The most common exploit targets, once a weapon is delivered, are applications, operating system vulnerabilities, and user accounts. Among other measures, conducting employee awareness training and email testing and auditing endpoints to forensically determine the origin of an exploit can help block future exploitations of systems.

15. Which action should be included in a plan element that is part of a computer security incident response capability (CSIRC)?

- Detail how incidents should be handled based on the mission and functions of an organization.
- **Develop metrics for measuring the incident response capability and its effectiveness.**
- Create an organizational structure and definition of roles, responsibilities, and levels of authority.
- Prioritize severity ratings of security incidents.

NIST recommends creating policies, plans, and procedures for establishing and maintaining a CSIRC. A purpose of the plan element is to develop metrics for measuring the incident response capability and its effectiveness.

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

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

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

17. After containment, what is the first step of eradicating an attack?

- Hold meetings on lessons learned.
- Change all passwords.
- Patch all vulnerabilities.
- **Identify all hosts that need remediation.**

Once an attack is contained, the next step is to identify all hosts that will need remediation so that the effects of the attack can be eliminated.

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

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

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

19. A school has a web server mainly used for parents to view school events, access student performance indicators, and communicate with teachers. The network administrator suspects a security-related event has occurred and is reviewing what steps should be taken.

a. The threat actor has already placed malware on the server causing its performance to slow. The network administrator has found and removed the malware as well as patched the security hole where the threat actor gained access. The network administrator can find no other security issue. What stage of the Cyber Kill Chain did the threat actor achieve?

- **actions on objectives**
- command and control
- delivery
- exploitation
- installation

During the installation step, the threat actor installed a server backdoor in order to install the malware (installation step), and an outside server command channel was created to manipulate the target (CnC step). The final step is used to access the server to achieve the objective of the attack.
The Cyber Kill Chain has seven steps:

1. reconnaissance
2. weaponization
3. delivery
4. exploitation
5. installation
6. command and control (CnC)
7. actions on objectives

b. If the web server runs Microsoft IIS, which Windows tool would the network administrator use to view the access logs?

- **Event Viewer**
- net command
- PowerShell
- Task Manager

Information provided in the IIS access log includes the date, time, client IP address, username, port number, requested action, bytes sent, bytes received, and content of the cookie sent or received.

c. Reports of network slowness lead the network administrator to review server alerts. The administrator confirms that an alert was an actual security incident. Which type of security alert classification would this be?

- false negative
- false positive

- true negative
- **true positive**

A positive alert of any type means that the system generated a system alert. A true positive indicates the incident occurred. A false positive is that no incident occurred (the system alerted, but there was no problem). A negative alert of any type means there was no alert generated. A true negative indicates that there wasn't any incident (thus no alert). A false negative indicates that there was an incident, but an alert was not generated.

d. The network administrator believes that the threat actor used a commonly available tool to slow the server down. The administrator concludes that based on the source IP address identified in the alert, the threat actor was probably one of the students. What type of hacker would the student be classified as?

- **black hat**
- gray hat
- red hat
- white hat

Three classifications of hackers are black hat, gray hat, and white hat. White hat hackers use their security skills for good, ethical, legal purposes. Gray hat hackers do not compromise the network for personal gain or to cause damage such as when users leave their computers logged into the corporate network and walk away. Black hat hackers penetrate computers or servers for malicious reasons, such as to slow down system performance.

20. What is the goal of an attack in the installation phase of the Cyber Kill Chain?

- **Create a back door in the target system to allow for future access.**
- Establish command and control (CnC) with the target system.
- Use the information from the reconnaissance phase to develop a weapon against the target.
- Break the vulnerability and gain control of the target.

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.

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

- resources
- methodology
- direction
- **results**

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

22. What is a benefit of using the VERIS community database?

- **It can be used to discover how other organizations dealt with a particular type of security incident.**
- Companies who pay to contribute and access the database are protected from security threats.
- It can be used to discover the name of known threat actors.
- The database can be easily compressed.

The VERIS community database is free. It can be used as a tool for risk management, to document security incidents, to discover over incidents, and to compare how other organizations dealt with a particular type of security incident.

23. 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.)

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

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

24. 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.

One tactic of weaponization used by a threat actor after the vulnerability is identified is to obtain an automated tool to deliver the malware payload through the vulnerability.

25. Which action is taken in the postincident phase of the NIST incident response life cycle?

- **Document the handling of the incident.**
- identify and validate incidents.
- Conduct CSIRT response training.
- Implement procedures to contain threats.

It is in the post-incident phase of the NIST incident response life cycle phase that the CSIRT documents how incidents are handled. Recommended changes for future response are also made to avoid reoccurrences.

26. Which top-level element of the VERIS schema would allow a company to log who the actors were, what actions affected the asset, which assets were affected, and how the asset was affected?

- **incident description**
- incident tracking
- discovery and response
- victim demographics

Explanation: The incident description top-level element uses the 4A model (actors, actions, assets, and attributes). Each section has subsections to further document the incident.

27. What is the role of vendor teams as they relate to CSIRT?

- Coordinate incident handling across multiple CSIRTs.
- **Handle customer reports concerning security vulnerabilities.**
- Use data from many sources to determine incident activity trends.
- Provide incident handling to other organizations as a fee-based service.

There are many different types of CSIRTs and related information security organizations. Vendor CSIRT teams provide remediation for vulnerabilities in the software or hardware of an organization and often handle customer reports concerning security vulnerabilities.

28. 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.

Threat actors may use port scanning toward a web server of an organization and identify vulnerabilities on the server. They may visit the web server to collect information about the organization. The web server logging should be enabled and the logging data should be analyzed to identify possible reconnaissance threats. Building playbooks by filtering and combining related web activities by visitors can sometimes reveal the intentions of threat actors.

29. To ensure that the chain of custody is maintained, what three items should be logged about evidence that is collected and analyzed after a security incident has occurred? (Choose three.)

- measures used to prevent an incident
- **time and date the evidence was collected**
- extent of the damage to resources and assets
- vulnerabilities that were exploited in an attack
- **serial numbers and hostnames of devices used as evidence**
- **location of all evidence**

A chain of custody refers to the proper accounting of evidence collected about an incident that is used as part of an investigation. The chain of custody should include the location of all evidence, the identifying information of all evidence such as serial numbers and hostnames, identifying information about all persons handing the evidence, and the time and date that the evidence was collected.

30. Which schema or model was created to anonymously share quality information about security events to the security community?

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

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.

31. What is the purpose of the policy element in a computer security incident response capability of an organization, as recommended by NIST?

- It provides a roadmap for maturing the incident response capability.
- It provides metrics for measuring the incident response capability and effectiveness.

- It defines how the incident response teams will communicate with the rest of the organization and with other organizations.
- **It details how incidents should be handled based on the organizational mission and functions.**

NIST recommends creating policies, plans, and procedures for establishing and maintaining a CSIRC. A purpose of the policy element is to detail how incidents should be handled based on the mission and functions of an organization.

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

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

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

33. 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.

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

34. Which term is used in the Diamond Model of intrusion to describe a tool that a threat actor uses toward a target system?

- infrastructure
- **capability**
- weaponization
- adversary

The Diamond Model of intrusion contains four parts:

- Adversary – the parties responsible for the intrusion

- Capability – a tool or technique that the adversary uses to attack the victim
- Infrastructure – the network path or paths that the adversaries use to establish and maintain command and control over their capabilities
- Victim – the target of the attack

35. What is the role of a Computer Emergency Response Team?

- Receive, review, and respond to security incidents in an organization.
- Provide national standards as a fee-based service.
- Coordinate security incident handling across multiple CSIRTs.
- **Provide security awareness, best practices, and security vulnerability information to a specific population.**

A Computer Emergency Response Team (CERT) provides security awareness, best practices, and security vulnerability information to populations. A CERT does not respond directly to security incidents.

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

- exploitation
- weaponization
- **reconnaissance**
- action on objectives

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

37. Match the security incident stakeholder with the role.

management

IT support

legal department

human resources

information assurance

performs disciplinary measures

changes firewall rules

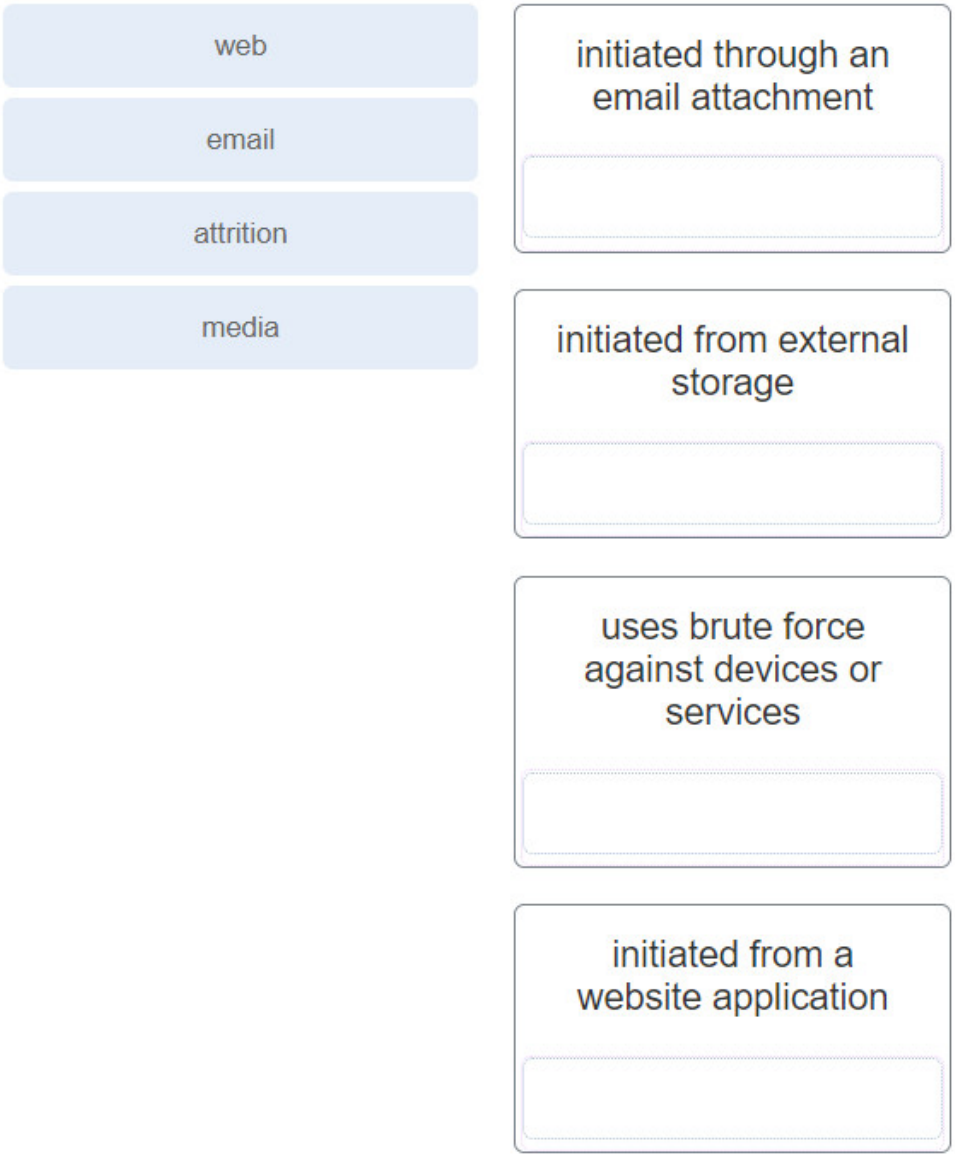
preserves attack evidence

designs the budget

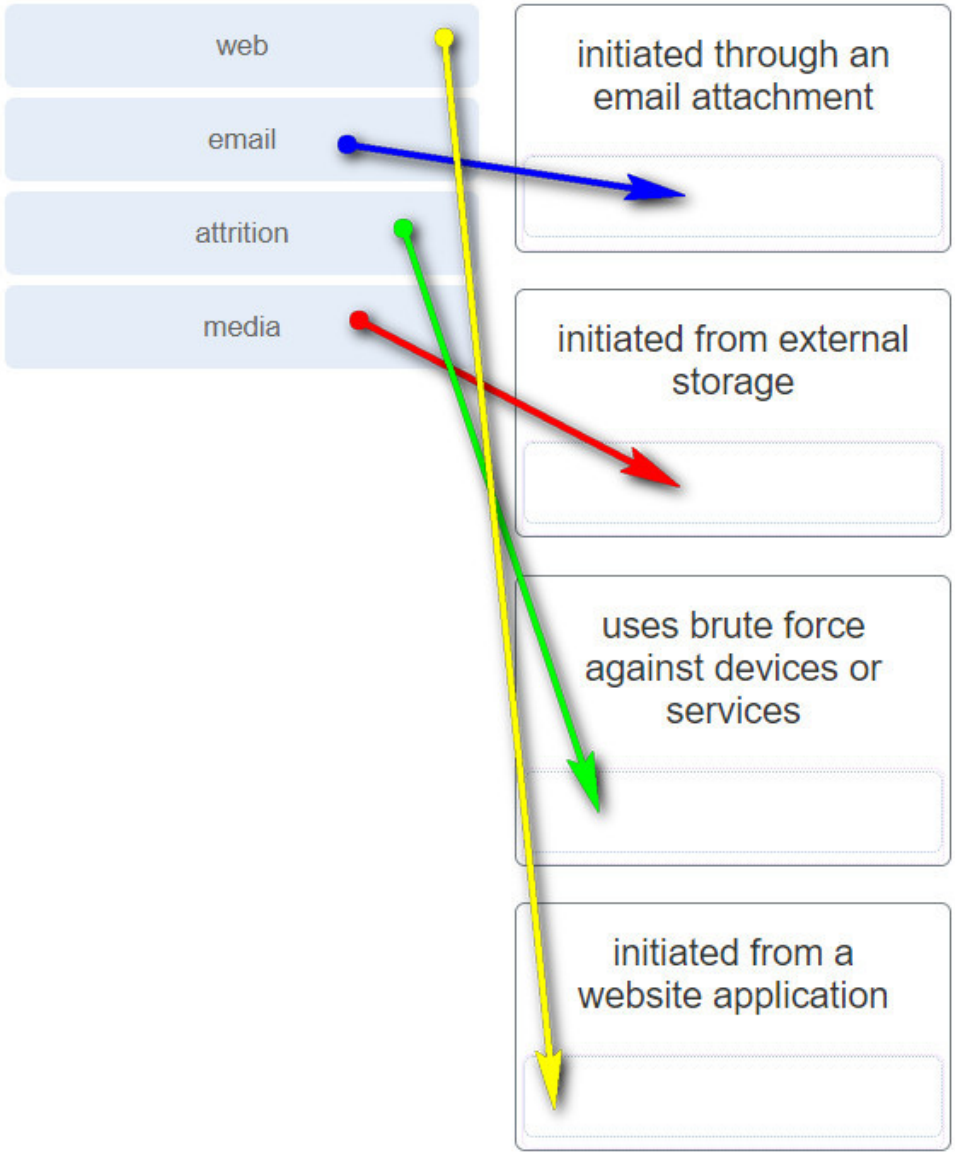
reviews policies for local or federal guideline violations

Answer

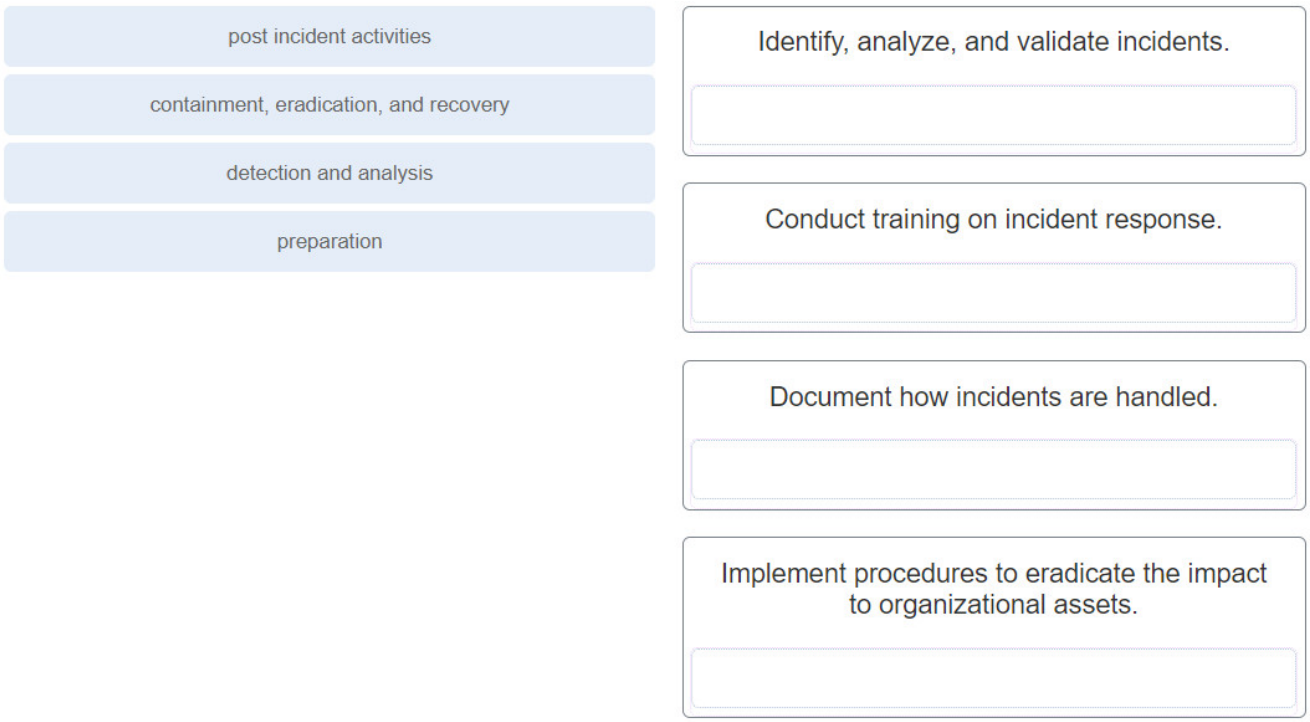
38. Match the attack vector with the description.


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

Answer



39. Match the NIST incident response life cycle phase with the description.

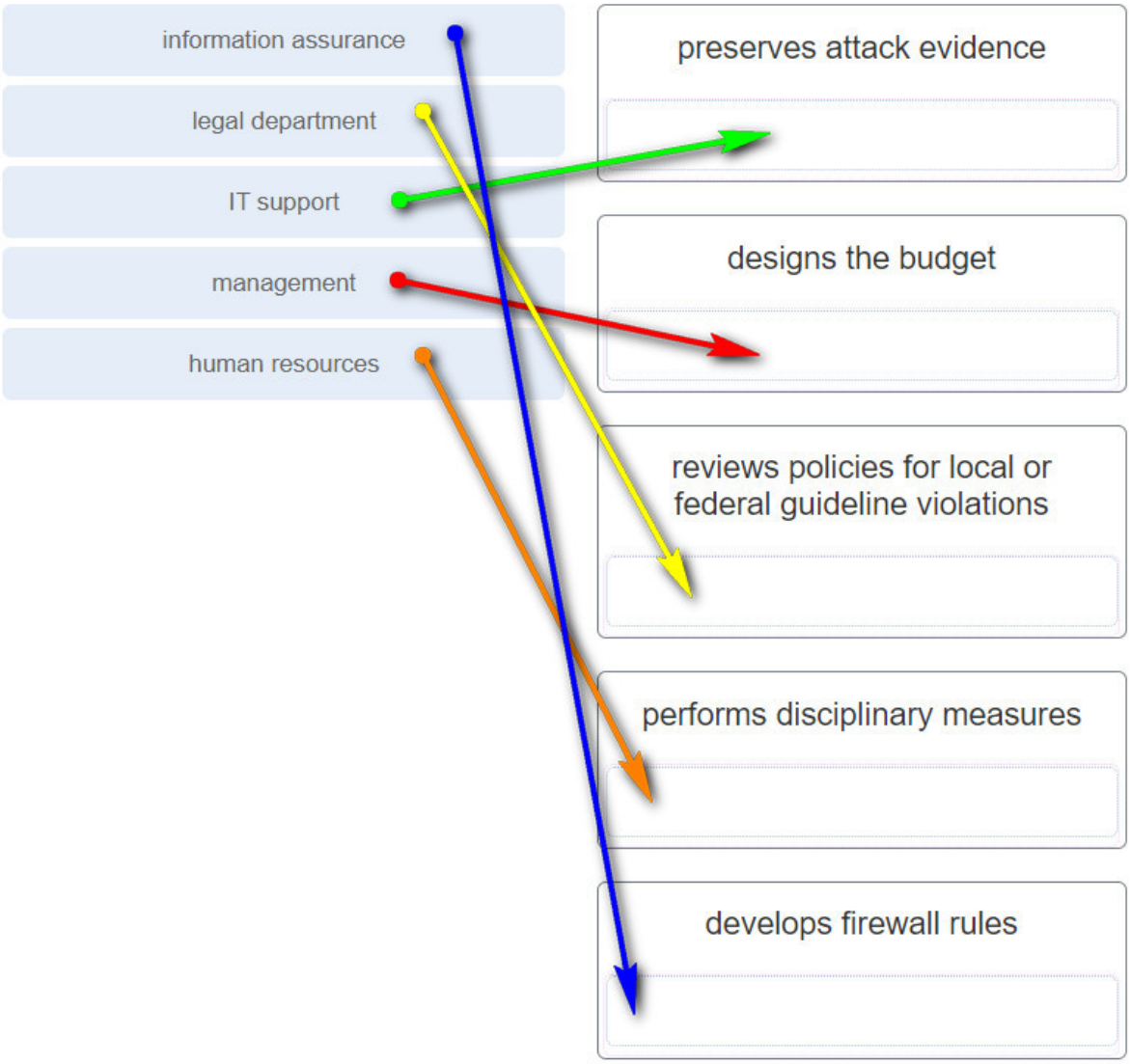


Answer

40. Match the NIST incident response stakeholder with the role.

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

Answer



Download PDF File below:

[sociallocker id="54558"]

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 13 Exam Answers.pdf 380.60 KB 1065 downloads

...

Download

[/sociallocker]