QBank Quiz Domain 5

Test ID: 178834797

Question #1 of 84

Question ID: 1323080

Which organizational stakeholders are responsible for installing anti-malware software?

- **A)** CISO
- **B)** CEO
- **C)** System and network administrators
- **D)** CSIRT team

Explanation

The proper way to address malware, according to the NIST SP800-61 r2, is to install anti-malware software. The stakeholder group responsible for that is the system and network administrators. It is part of their duties to keep it up to date.

It is not the responsibility of the Computer Security Incident Response Team (CSIRT). Their job is to identify and handle security incidents.

It is not the responsibility of the Chief Information Security Officer. This role’s job is to manage security from a much higher level and to support all security efforts.

It is not the responsibility of the Chief Executive Officer. His job is to manage the entire organization, although this role’s support of all security efforts is critical.

Objective:
Security Policies and Procedures

Sub-Objective:
Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (Preparation; Detection and analysis; Containment, eradication, and recovery; Post-incident analysis (lessons learned))

References:

HYPERLINK "https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf"NIST > Computer Security Incident Handling Guide (PDF)

Question #2 of 84

Question ID: 1323118

Which step in the Cyber Kill Chain framework comes just after weaponization?

- **A)** installation
- **B)** delivery
- **C)** command and control
- **D)** exploitation

Explanation

Weaponization occurs when the attacker turns some utility or function into a weapon he can use in the attack. It occurs after reconnaissance. Using Metasploit to craft an exploit is an example of weaponization.

In the Delivery step, the attacker transmits the crafted exploit to the target.

The seven steps in the kill chain are:

1. Reconnaissance – the attacker gathers information to aid in penetrating the network
2. Weaponization – the attacker turns a legitimate utility or function into a weapon that can be used in the attack
3. Delivery – the attacker transmits the crafted exploit to the target
4. Exploitation – the exploit is executed
5. Installation – the hacker installs additional tools and resources on the target device or in the target network
6. Command and control (C2 – the attacker takes remote control of the target device from the Command and control (CnC) server
7. Actions on objectives – the attacker takes action (deletes data, steals data, defaces website)

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

The Cyber Kill Chain frameworkLockheed Martin > The Cyber Kill Chain®

Question #3 of 84

Question ID: 1323060

According to NIST SP 800-61 r2, what is a precursor?

A) the attacker

B) a sign that an incident may have occurred or may be occurring now

C) the methods used in the attack

D) a sign that an incident may occur in the future

Explanation

In the NIST SP 800-61 r2 publication, a precursor is something that indicates an incident may occur in the future. NIST SP 800-61 r2 is the Computer Security Incident Handling Guide. According to this publication, the four major phases of the incident response lifecycle are:

- Preparation
- Detection and Analysis
- Containment Eradication and Recovery
- Post-Incident Activity

Precursors are usually found in computer security software alerts, logs (such as SIEM logs), social media, and public sources of information, like security blogs. Precursors could include a tweet from a hacktivist group stating that they plan to target a specific organization, anomalous NetFlow activity, or the announcement of a vulnerability that affects a key server in your organization.

The attacker is called the instigator.

A sign that an incident may have occurred or may be occurring now is called an indicator.

The methods used in the attack are attack vectors.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe the elements in an incident response plan as stated in NIST.SP800-61

References:

NIST > Computer Security Incident Handling Guide (PDF)

Question #4 of 84

Question ID: 1323104

When a TCP packet is sent to an open port with the SYN flag set, what response would be expected from the open port?

A) no response
B) a packet with the ACK flag set
C) a packet with the SYN and ACK flags set
D) a packet with an RST flag

Explanation

When the port is open, the receiver will send back a packet with the SYN and ACK flags set.

Transmission Control Protocol (TCP) is a session-oriented or connection-based protocol. It uses a three-way handshake to ensure that every packet sent is successfully received and acknowledged by the destination. The handshake is performed at the start of each session by TCP, and contains a set of three segments (TCP "packets").

- The sender sends the first segment to the receiver with the Synchronization (SYN) flag enabled.
- Step two: The receiver sends the second segment back to the sender with both the Acknowledgement flag (ACK) and the Synchronization (SYN) flag enabled.
- Step three: The sender sends the third segment back to the receiver with just the Acknowledgement (ACK) flag enabled (in response to the server's Synchronization request).

A packet with the RST flag would be received if the port were closed. An open port responds with a SYN/ACK segment, while a closed port responds with a RST (reset) flagged segment.

A packet with the ACK flag set would only follow a packet with the SYN and ACK flags set. The first step is to send a SYN packet. When the port is open, the receiver will send back a packet the SYN and ACK flags set.

No response would occur only if the port were blocked on the firewall. Firewalls do not send diagnostic or error messages when blocking a transmission.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for server profiling (Listening ports; Logged in users/service accounts; Running processes; Running tasks; Applications)

References:

Techopedia > Three-Way Handshake

Question #5 of 84

Question ID: 1323115

Which of the following is an example of reconnaissance?

A) stealing future plans

B) installing a RAT

C) communicating with well-known malicious IP address

D) scanning without completing the three-way handshake

Explanation

Scanning without completing the three-way handshake is done to determine open ports and potential vulnerabilities. Another example would be sourcing for the Robots.txt file. The first and most important step in hacking or pen testing is reconnaissance when information is gathered that helps penetrate the network.

Installation of a remote access Trojan (RAT) would be part of the installation step.

Theft of future is part of the Action on objectives step

Communication with well-known malicious IP address is part of the Command and Control step since the remote device is quite likely a command and control (CnC) server.

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

The Cyber Kill Chain frameworkLockheed Martin > The Cyber Kill Chain®

Question #6 of 84

Question ID: 1323076

According to NIST.SP800-61 r2, which of the following is NOT a question to ask during post mortem?

A) Were any steps or actions taken that might have inhibited the recovery?

B) Exactly what happened and at what time?

C) Whose fault was the attack?

D) How could information sharing with other organizations be improved?

Explanation

Blame placing is not part of the post mortem. The idea is to discover what can be done better in a supportive atmosphere. Questions that should be answered include:

- Exactly what happened, and at what times?
- How well did the staff and management perform while dealing with the incident?
- Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations be improved?

- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Objective:
Security Policies and Procedures

Sub-Objective:
Map elements to these steps of analysis based on the NIST.SP800-61 (Preparation: Detection and analysis; Containment, eradication, and recovery; Post-incident analysis (lessons learned))

References:

NIST > Computer Security Incident Handling Guide (PDF)

Question #7 of 84

Question ID: 1323106

Which of the following standards or regulations covers e-PHI? (Choose all that apply.)

A) HIPAA
B) GDPR
C) SOX
D) PCI

Explanation

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) prescribes requirements for handling medical records and applies to any entity that handles them in the process of doing business. Personal health information (PHI) should be protected from unauthorized disclosure as per HIPAA privacy rules. Electronic personal health information (e-PHI) should be protected at rest and during transmission as per HIPAA security rules.

The Payment Card Industry Data Security Standards (PCI-DSS) prescribes requirements for handling credit card data. It applies to both cardholder data (such as names) and authentication data (such as magnetic stripes).

The Sarbanes-Oxley (SOX) Act of 2002 is legislation that covers financial reporting, and is intended to prevent companies from committing fraud by knowingly providing inaccurate financial reports to shareholders and the public. It is mainly concerned with corporate accounting practices. Section 404 of this act specifically addresses information technology. It applies to all publically held or traded U.S. companies and to some reporting practices of privately held companies.

The General Data Protection Regulation (GDPR) is new set of regulations designed to safeguard personal information in the European Union. It applies to personal data of EU citizens that is stored or exported out of the EU, including electronic health information. Personal data that is regulated is defined as “any information that relates to an identified or identifiable living individual,” including information that can identify a particular person only after it is assembled with other pieces of information. Examples of covered personal data include a name, an IP address, geo-location information, an email address, a national identification number, and health data.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify protected data in a network (PII; PSI; PHI; Intellectual property)

References:

U.S. Department of Health & Human Services > HIPAA Home > For Professionals > The Security Rule

TrustArc > Essential Guide to the GDPR

U.S. Securities and Exchange Commission > Sarbanes-Oxley Act

Question #8 of 84

Question ID: 1323113

Which of the following is NOT a meta feature of the Diamond model?

A) response

B) date

C) result

D) timestamp

Explanation

Response is not one of the meta features of the Diamond model. The Diamond model is designed to represent an incident, also called an event, and is made up of four parts: adversary, infrastructure, capabilities, and victims. The meta features of this model are:

- Timestamp
- Phase
- Result
- Direction
- Methodology
- Resources

An example of each of these meta features filled out for an attack is as follows.

- Timestamp - 6/3/2018 8:45
- Phase - delivery
- Result - success
- Direction - toward victim
- Methodology - phishing
- Resources - target email

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

Threat Connect > Diamond Model of Intrusion Analysis

Question #9 of 84

Question ID: 1323062

In which stage of incident handling is the environment returned to a secure state?

A) lessons-based hardening

B) containment

C) remediation

D) Identification

Explanation

Returning the environment to a secure state occurs during the remediation stage. There are six steps in the incident handling process:

1. Identification – determining whether there is an incident
2. Scoping – determining the extent of the incident and identifying the attackers
3. Containment – halting the spread of the incident and minimizing the impact
4. Remediation – returning the environment to secure state
5. Lesson-based hardening – preventing future incidents
6. Reporting – documenting the incident and reporting it

Objective:
Security Policies and Procedures

Sub-Objective:
Describe the elements in an incident response plan as stated in NIST.SP800-61

References:

NIST > SP 800-61 Rev. 2 Computer Security Incident Handling Guide

---

Question #10 of 84

Question ID: 1323063

In which stage of incident handling does the verification that an incident exists occur?

A) lessons-based hardening

B) identification

C) remediation

Explanation

In the identification phase, there is a determination if there is a security incident. There are six steps in the incident handling process:

1. Identification – determining whether there is an incident
2. Scoping – determining the extent of the incident and identifying the attackers
3. Containment – halting the spread of the incident and minimizing the impact
4. Remediation – returning the environment to secure state
5. Lesson-based hardening – preventing future incidents
6. Reporting – documenting the incident and reporting it

Objective:
Security Policies and Procedures

Sub-Objective:
Describe the elements in an incident response plan as stated in NIST.SP800-61

References:

NIST > SP 800-61 Rev. 2 Computer Security Incident Handling Guide

Question #11 of 84

Question ID: 1323131

Which of the following would help multiple CSIRTS facilitate incident handling?

A) national CSIRT

B) MSSP

C) Analysis center

D) Coordination center

Explanation

Coordination centers around the world also help CSIRTS coordinate incident handling. They also help coordinate security vulnerability disclosures to vendors, hardware and software providers, and security researchers.

A national Computer Security Incident Response Team (national CSIRT) provides cybersecurity protection to an entire country or a significant portion of a national economy, which would include protecting federal civilian or executive branch agencies. CSIRTs provide incident handling capabilities as well as training and coordination of vulnerability databases. Two well-known national CSIRTs are the Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT) and the United States Cyber Emergency Readiness Team (US-CERT).

Analysis centers examine patterns of attacks and vulnerabilities and provide data that can be used to track trends or provide warning of future attacks. They do not directly help with incident response.

Product security incident response teams (PSIRTs) are internal to a vendor, and they handle the investigation, resolution, and disclosure of security vulnerabilities in a vendor's products and services. They would not help multiple CSIRTs facilitate incident handling, although they would provide information that could be used by a CSIRT.

Managed security service providers (MSSPs) provide incident response and managed security services to their customers. Cisco's Incident Response Service is an example of this type of team.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

References:

NIST > Computer Security Incident Handling Guide (PDF)

Carnegie Mellon University > Software Engineering Institute > CSIRT FREQUENTLY ASKED QUESTIONS (FAQ) (PDF)

Question #12 of 84

Question ID: 1323089

According to SP 800-86, which of the following is NOT an important factor when prioritizing potential data sources of evidence?

A) effort required

B) volatility

C) time involved

D) likely value

Explanation

The amount of time involved in the collection is NOT one of the three considerations covered by SP 800-86. They are (quoted directly from SP 800-86):

- Likely Value. Based on the analysts understanding of the situation and previous experience in similar situations, the analyst should be able to estimate the relative likely value of each potential data source.
- Volatility. Volatile data refers to data on a live system that is lost after a computer is powered down or due to the passage of time. Volatile data may also be lost as a result of other actions performed on the system. In many cases, acquiring volatile data should be given priority over non-volatile data. However, non-volatile data may also be somewhat dynamic in nature (e.g., log files that are overwritten as new events occur).
- Amount of Effort Required. The amount of effort required to acquire different data sources may vary widely. The effort involves not only the time spent by analysts and others within the organization (including legal advisors) but also the cost of equipment and services (e.g., outside experts). For example, acquiring data from a network router would probably require much less effort than acquiring data from an ISP.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe concepts as documented in NIST.SP800-86 (Evidence collection order; Data integrity; Data preservation; Volatile data collection)

References:

NIST > Guide to Integrating Forensic Techniques into Incident Response (PDF)

Question #13 of 84

Question ID: 1323079

The CERT division of the Software Engineering Institute (SEI).is an example of which of the following?

A) MSSP

B) national CSIRT

C) PSIRT

D) Coordination centers

Explanation

Coordination centers around the world also help CSIRTS coordinate incident handling. They also help coordinate security vulnerability disclosures to vendors, hardware and software providers, and security researchers. One of the best examples is the CERT Division of the Software Engineering Institute (SEI).

Product security incident response teams (PSIRTs) handle the investigation, resolution, and disclosure of security vulnerabilities in their products and services. These fixes are provided as a free service to protect the users and the company’s reputation.

Managed security service providers (MSSPs) provide incident response and managed security services to their customers. Cisco’s Incident Response Service is an example of this type of team.

National CSIRTS provide incident handling for a country. Examples include the US-CERT.

Objective:
Security Policies and Procedures

Sub-Objective:
Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (Preparation; Detection and analysis; Containment, eradication, and recovery; Post-incident analysis (lessons learned))

References:

Exabeam > The Complete Guide to CSIRT Organization: How to Build an Incident Response Team

---

Question #14 of 84

Question ID: 1323098

What tool or command can be used to determine details of a user account?

A) `netstat -a`

B) `nbtstat`

C) Task Manager

D) `net user`

Explanation

The net user command lists all accounts. If you specify the account name Jill, it gives the information shown below for the account Jill:

```
C:\WINDOWS\system32>net user Jill
User name                    Jill
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            9/27/2017 10:36:17 AM
Password expires             Never
Password changeable          9/27/2017 10:36:17 AM
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.
```

The netstat -a command shows all connections and listening ports. An example output is shown below.

```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\mcmil>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:902            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:912            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:6646           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:8733           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:17500          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:843          DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:5354         DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:17600        DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:50003        DESKTOP-V59I9G6:50004  ESTABLISHED
  TCP    127.0.0.1:50004        DESKTOP-V59I9G6:50003  ESTABLISHED
  TCP    127.0.0.1:50210        DESKTOP-V59I9G6:50211  ESTABLISHED
  TCP    127.0.0.1:50211        DESKTOP-V59I9G6:50210  ESTABLISHED
```

Task Manager is a utility used to:

Identify running processes

Identify running tasks

Identify application in use

Nbtstat is a command that show NetBIOS information. A sample output is shown below:

```
C:\WINDOWS\system32>nbtstat -n

VMware Network Adapter VMnet8:
Node IpAddress: [192.168.91.1] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    DESKTOP-V59I9G6<20>  UNIQUE      Registered
    DESKTOP-V59I9G6<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

VMware Network Adapter VMnet1:
Node IpAddress: [192.168.189.1] Scope Id: []

                NetBIOS Local Name Table
       Name               Type         Status
    ---------------------------------------------
    DESKTOP-V59I9G6<20>  UNIQUE      Registered
    DESKTOP-V59I9G6<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

Wi-Fi:
Node IpAddress: [192.168.1.71] Scope Id: []

                 NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    DESKTOP-V59I9G6<20>  UNIQUE      Registered
    DESKTOP-V59I9G6<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

Local Area Connection* 2:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Local Area Connection* 3:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Ethernet 3:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Bluetooth Network Connection 2:
Node IpAddress: [0.0.0.0] Scope Id: []
```

Objective:

Security Policies and Procedures

Sub-Objective:

Identify these elements used for server profiling (Listening ports; Logged in users/service accounts; Running processes; Running tasks; Applications)

References:

Lifewire > Net User Command

Question #15 of 84

Question ID: 1323081

Cisco Active Threat Analysis is an example of which if the following?

- **A)** PSIRT
- **B)** MSSP
- **C)** Coordination centers
- **D)** National CSIRT

Explanation

Managed Security Service Providers (MSSPs) provide incident response and managed security services to their customers. The Cisco’s Incident Response Service is an example. Another example is Cisco Active Threat Analysis.

Coordination centers around the world also help CSIRTS coordinate incident handling. They also help coordinate security vulnerability disclosures to vendors, hardware and software providers, and security researchers. One of the best examples is the CERT Division of the Software Engineering Institute (SEI).

Product security incident response teams (PSIRTs) handle the investigation, resolution, and disclosure of security vulnerabilities in their products and services.

A national Computer Security Incident Response Team (national CSIRT) provides cybersecurity protection to an entire country or a significant portion of a national economy, which would include protecting federal civilian or executive branch agencies. CSIRTs provide incident handling capabilities as well as training and coordination of vulnerability databases. Two well-known national CSIRTs are the Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT) and the United States Cyber Emergency Readiness Team (US-CERT).

Objective:
Security Policies and Procedures

Sub-Objective:
Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (Preparation; Detection and analysis; Containment, eradication, and recovery; Post-incident analysis (lessons learned))

References:

NIST > Computer Security Incident Handling Guide (PDF)

Question #16 of 84

Question ID: 1323090

According to SP 800-86, which of the following is NOT volatile data?

A) slack space

B) hibernation file

C) network configuration

D) network connections

Explanation

Hibernation files are created when a system hibernates or sleeps and are still there after rebooting.

Slack space is space in memory where no data is located normally but can contain evidence. It goes way when rebooting.

When a host received dynamic network configurations (DHCP) these configuration are lost when rebooting.

Evidence of all current network connections will be lost when rebooting.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe concepts as documented in NIST.SP800-86 (Evidence collection order; Data integrity; Data preservation; Volatile data collection)

References:

NIST > Guide to Integrating Forensic Techniques into Incident Response (PDF)

Question #17 of 84

Question ID: 1323110

Of which of the following is a Social security number an example?

A) PHI

B) HIPAA

C) PS-DSS

D) PII

Explanation

Personally identifiable information (PII) is any piece of information that can be used to uniquely identify a person, such as full name, account name, phone number, license number, date of birth, social security number, or any other personal attribute.

Medical records are considered Personal Health Information (PHI) and must be protected from unauthorized disclosure.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the act governs the handling of PHI.

The Payment Card Industry Data Security Standard (PCI DSS) protects credit card information.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify protected data in a network (PII; PSI; PHI; Intellectual property)

References:

File Cloud > What is PII and PHI? Why is it Important?

Question #18 of 84

Question ID: 1323120

Which step in the Cyber Kill Chain framework occurs LAST among the following options?

- Reconnaissance
- Delivery
- Weaponization
- Exploitation

A) Reconnaissance

B) Exploitation

C) Delivery

D) Weaponization

Explanation

Exploitation comes after the attacker creates a weapon and delivers the weapon. It occurs when the weapon executes.

The first and most important step is reconnaissance when information is gathered that helps penetrate the network. For example, consider an exploit takes advantage of an injection vulnerability in an exploitable Hypertext Preprocessor (php) file by sending an HTTP POST with specific variables. If the hacker sends an HTTP GET request the page, the attack is still in reconnaissance. The steps are:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and control (C2)
7. Actions on objectives

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

The Cyber Kill Chain frameworkLockheed Martin > The Cyber Kill Chain®

Question #19 of 84

Question ID: 1323132

Which of the following provides incident response and managed security services to its customers?

A) Coordination center

B) MSSP

C) PSIRT

D) National CSIRT

Explanation

Managed security service providers (MSSPs) provide incident response and managed security services to their customers. Cisco's Incident Response Service is an example of this type of team.

Product security incident response teams (PSIRTs) are internal to a vendor, and they handle the investigation, resolution, and disclosure of security vulnerabilities in a vendor's products and services.

Coordination centers around the world also help CSIRTS coordinate incident handling. They also help coordinate security vulnerability disclosures to vendors, hardware and software providers, and security researchers.

A national Computer Security Incident Response Team (national CSIRT) provides cybersecurity protection to an entire country or a significant portion of a national economy, which would include protecting federal civilian or executive branch agencies. CSIRTs provide incident handling capabilities as well as training and coordination of vulnerability databases. Two well-known national CSIRTs are the Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT) and the United States Cyber Emergency Readiness Team (US-CERT).

Objective:
Security Policies and Procedures

Sub-Objective:
Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

References:

NIST > Computer Security Incident Handling Guide (PDF)

Carnegie Mellon University > Software Engineering Institute > Education and Outreach > Computer Security Incident Response Teams > National CSIRTs

Cybersecurity and Infrastructure Security Agency (CISA) > About Us

---

Question #20 of 84

Question ID: 1323066

Which document prescribes that an issue tracking system should be able to identify incidents related to a selected incident?

A) PCI-DSS
B) SP 800-61
C) SP 800-66
D) IOC 27005

Explanation

NIST SP 800-61 covers the handling of security incidents and managing the response to such incidents. It prescribes that an issue tracking system should be able to identify incidents related to a selected incident.

The IOC 27005 covers risk management and does not address incident handling.

The SP 800-66 is an introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

Payment Card Industry Data Security Standard (PCI-DSS) is a standard for handling credit card information and does not address incident handling

Objective:
Security Policies and Procedures

Sub-Objective:
Apply the incident handling process (such as NIST.SP800-61) to an event

References:

NIST > SP 800-61 Rev. 2 Computer Security Incident Handling Guide

---

Question #21 of 84

Question ID: 1323126

Which of the following is an example of a VERIS main schema category?

A) source ID
B) threat actors
C) incident ID
D) incident description

Explanation

The VERIS model views incidents as a series of events that adversely affect assets. The schema has the following schema categories:

- Incident Tracking - contains items related to capturing information about the incident
- Victim Demographics - information about the victim
- Incident Description - brief outline of the event
- Discovery & Response - how long did it take to identify and what was our response?
- Impact Assessment - what was the final impact on the organization

Threat actors is one of the subset of incident description.

Incident ID and Source ID are subsets of incident tracking.

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

VERIS > The Vocabulary for Event Recording and Incident Sharing

---

Question #22 of 84

Question ID: 1323099

Which netstat command displays Ethernet statistics?

A) `netstat -b`

B) `netstat -a`

C) `netstat -f`

D) `netstat --e`

Explanation

The `netstat -e` command displays Ethernet statistics. An example output is shown below:

```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\mcmil>netstat -e
Interface Statistics

                      Received          Sent

Bytes                       2323745128      2630574760
Unicast packets                7322690         5023430
Non-unicast packets             285612           58872
Discards                             0               0
Errors                               0               0
Unknown protocols                    0

C:\Users\mcmil>
```

The netstat -a command shows all connections and listening ports:

```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\mcmil>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:902            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:912            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:6646           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:8733           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:17500          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:843          DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:5354         DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:17600        DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:50534        DESKTOP-V59I9G6:50535  ESTABLISHED
  TCP    127.0.0.1:50535        DESKTOP-V59I9G6:50534  ESTABLISHED
  TCP    127.0.0.1:50548        DESKTOP-V59I9G6:50549  ESTABLISHED
  TCP    127.0.0.1:50549        DESKTOP-V59I9G6:50548  ESTABLISHED
  TCP    127.0.0.1:56359        DESKTOP-V59I9G6:56360  ESTABLISHED
  TCP    127.0.0.1:56360        DESKTOP-V59I9G6:56359  ESTABLISHED
  TCP    192.168.0.6:139        DESKTOP-V59I9G6:0      LISTENING
  TCP    192.168.0.6:56407      13.107.3.128:https     ESTABLISHED
  TCP    192.168.0.6:56408      13.107.3.128:https     ESTABLISHED
```

The `netstat -b` command displays the executable involved in creating the connection

```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -b

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49751        DESKTOP-V59I9G6:49752  ESTABLISHED
[Dropbox.exe]
  TCP    127.0.0.1:49752        DESKTOP-V59I9G6:49751  ESTABLISHED
[Dropbox.exe]
  TCP    127.0.0.1:49768        DESKTOP-V59I9G6:49769  ESTABLISHED
[Dropbox.exe]
  TCP    127.0.0.1:49769        DESKTOP-V59I9G6:49768  ESTABLISHED
[Dropbox.exe]
```

```
  TCP    127.0.0.1:58025        DESKTOP-V59I9G6:58026  ESTABLISHED
[Dropbox.exe]
  TCP    127.0.0.1:58026        DESKTOP-V59I9G6:58025  ESTABLISHED
[Dropbox.exe]
  TCP    192.168.1.71:17500     DESKTOP-6FCDEI1:65105  ESTABLISHED
[Dropbox.exe]
```

The `netstat - f` command displays fully qualified domain names for foreign addresses.

```
C:\WINDOWS\system32>netstat -f

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49751        DESKTOP-V59I9G6:49752  ESTABLISHED
  TCP    127.0.0.1:49752        DESKTOP-V59I9G6:49751  ESTABLISHED
  TCP    127.0.0.1:49768        DESKTOP-V59I9G6:49769  ESTABLISHED
  TCP    127.0.0.1:49769        DESKTOP-V59I9G6:49768  ESTABLISHED
  TCP    127.0.0.1:58025        DESKTOP-V59I9G6:58026  ESTABLISHED
  TCP    127.0.0.1:58026        DESKTOP-V59I9G6:58025  ESTABLISHED
  TCP    192.168.1.71:17500     DESKTOP-6FCDEI1.attlocal.net:65105  ESTABLISHED
```

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for server profiling (Listening ports; Logged in users/service accounts; Running processes; Running tasks; Applications)

References:

HYPERLINK "https://www.lifewire.com/netstat-command-2618098"Lifewire > How to Use the Netstat Command

Question #23 of 84

Question ID: 1323100

What would be the key reason to perform server profiling?

A) to find which ports are connected

B) to determine if a compromise exists

C) troubleshooting

D) performance issues

Explanation

One of the key reasons for server profiling is to identify what ports are currently listening though certainly not the only point of interest. Key items include:

- Listening ports, the most common being:
    - TCP 20 and 21: File Transfer Protocol (FTP)
    - TCP 22: Secure Shell (SSH)
    - TCP 23: Telnet
    - TCP 25: Simple Mail Transfer Protocol (SMTP)
    - TCP and UDP 53: Domain Name System (DNS)
    - UDP 69: Trivial File Transfer Protocol (TFTP)

    - TCP 79: Finger
    - TCP 80: Hypertext Transfer Protocol (HTTP)
    - TCP 110: Post Office Protocol v3 (POP3)
    - TCP 119: Network News Protocol (NNTP)
    - UDP 161 and 162: Simple Network Management Protocol (SNMP)
    - UDP 443: Secure Sockets Layer over HTTP (HTTPS)
- Logged-in Users/Service Accounts
- Running Processes
- Applications

The `netstat` command can be used for this process. The `netstat -a` command shows all connections and listening ports. An example output is shown below.

```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\mcmil>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:902            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:912            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:6646           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:8733           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:17500          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:843          DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:5354         DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:17600        DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:50003        DESKTOP-V59I9G6:50004  ESTABLISHED
  TCP    127.0.0.1:50004        DESKTOP-V59I9G6:50003  ESTABLISHED
  TCP    127.0.0.1:50210        DESKTOP-V59I9G6:50211  ESTABLISHED
  TCP    127.0.0.1:50211        DESKTOP-V59I9G6:50210  ESTABLISHED
```

Server profiling does not have troubleshooting or assessing performance as its main goal. Although ultimately we want to determine a compromise, the profiling process should occur before an attack.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for server profiling (Listening ports; Logged in users/service accounts; Running processes; Running tasks; Applications)

References:

HYPERLINK "https://www.lifewire.com/netstat-command-2618098" Lifewire > How to Use the Netstat Command

Question #24 of 84

Question ID: 1323105

From the perspective of the processor, what is the term used to describe a running program in Windows?

A) procedure

B) object

C) process

D) instance

Explanation

A process is a single application as seen from the perspective of the processor. Multiprocessing is the operation of more than one process at a time.

Procedures are sets of tasks and the term is not used when describing a running program in Windows.

An instance is one running process, while a duplicate process would be called another instance.

Objects are metrics that can be chosen to monitor in the performance tool and the term is not used when describing a running program in Windows.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for server profiling (Listening ports; Logged in users/service accounts; Running processes; Running tasks; Applications)

References:

Microsoft Docs > Windows > Apps > System Services > Processes and Threads

Question #25 of 84

Question ID: 1323078

Which of the following offers incident handling services for a fee to other organizations?

A) national CSIRT

B) PSIRT

C) Coordination centers

D) MISSP

Explanation

Managed Security Service Providers (MSSPs) provide incident response and managed security services to their customers. The Cisco's Incident Response Service is an example. Another example is Cisco Active Threat Analysis.

Coordination centers around the world also help with the coordination of security vulnerability disclosures to vendors, hardware and software providers, and security researchers. One of the best examples is the CERT Division of the Software Engineering Institute (SEI).

Product security incident response teams (PSIRTs) handle the investigation, resolution, and disclosure of security vulnerabilities in their products and services.

National CSIRTS provide incident handling for a country. Examples include the US-CERT.

Objective:
Security Policies and Procedures

Sub-Objective:
Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (Preparation; Detection and analysis; Containment, eradication, and recovery; Post-incident analysis (lessons learned))

References:

NIST > Computer Security Incident Handling Guide (PDF)

Question #26 of 84

Question ID: 1323084

What is the first step in establishing an internal CSIRT?

A) Deciding where the CSIRT will reside within the organization’s hierarchy
B) Developing the process and policies for the CSIRT
C) Defining the CSIRT constituency
D) Making sure that the proper budget is allocated

Explanation

Establishing a CSIRT involves the following steps:

Step 1. Define the CSIRT constituency
Step 2. Ensure management and executive support
Step 3. Allocate the proper budget
Step 4. Decide where the CSIRT will reside within the organization’s hierarchy
Step 5. Determine whether the team will be central, distributed, or virtual
Step 6. Develop the process and policies for the CSIRT

Objective:
Security Policies and Procedures

Sub-Objective:
Describe concepts as documented in NIST.SP800-86 (Evidence collection order; Data integrity; Data preservation; Volatile data collection)

References:

Best Practices for Establishing a National CSIRT by the Organisation of American States (OAS)

Question #27 of 84

Question ID: 1323065

Which of the following is NOT an element of the NIST.SP800-61 r2 incident response plan?

A) organizational mission

B) strategies and goals

C) organizational approach

D) siloed approach to communication

Explanation

Rather than a siloed approach, the incident response approach should encourage and specify communication between the team and the organization and other organizations. In a siloed approach, the team has little communication with the organization and other organizations during the response.

NIST SP 800-61 v2 is the Computer Security Incident Handling Guide. According to this publication, the four major phases of the incident response lifecycle are:

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

The NIST's incident response plan elements are:

- Incident response plan's mission
- Strategies and goals of the incident response plan
- Senior management approval of the incident response plan
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization

Objective:
Security Policies and Procedures

Sub-Objective:
Apply the incident handling process (such as NIST.SP800-61) to an event

References:

NIST > Computer Security Incident Handling Guide (PDF)

Question #28 of 84

Question ID: 1323087

Which action would be supportive of the concept of volatile data collection as describe in SP 800-86?

A) collect memory data first

B) collect volatile data after rebooting

C) collect hard drive data first

D) collect malware data

Explanation

According to the concept of volatile data collection as covered in NIST 800-86, volatile data, meaning data that is gone after rebooting, should be collected first as it is fragile. Memory data should be collected first.

All volatile data should be collected before, not after, rebooting while it still exists.

You should not collect hard drive data first. This is not volatile data.

The concept of volatile data does not concern itself with the data content, such as malware data. It is only concerned with the volatile data.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe concepts as documented in NIST.SP800-86 (Evidence collection order; Data integrity; Data preservation; Volatile data collection)

References:

HYPERLINK "https://csrc.nist.gov/publications/detail/sp/800-86/final"NIST > SP 800-86 Guide to Integrating Forensic Techniques into Incident Response

---

Question #29 of 84

Question ID: 1323095

You have an extremely high volume of outgoing email. What should you suspect?

A) malware outbreak
B) Land attack
C) spam relay
D) SYN flood

Explanation

When your email severs are used to relay spam, it can cause this. It can be prevented by disallowing your server from doing open relay.

A malware outbreak does not cause an increase in email. It may cause an increase in traffic of other types.

A SYN flood is an attack in which zombies are recruited to overwhelm a target with unanswered TCP packets with the SYN flag set. When the target uses all its memory to reserve space for the never received ACK packets it freezes. It does not cause an increase in email.

In a land attack, a TCP packet is sent with the SYN flag set, but the packet is malformed in such a way that it appears to come from the target. This confuses the target and locks it up.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for network profiling (Total throughput; Session duration; Ports used; Critical asset address space)

References:

Techopedia > Open Relay

Question #30 of 84

Question ID: 1323074

Which of the following is NOT part of the considerations for a contaminant strategy, according to NIST SP 800-61 r2?

A) attack vector used

B) need for evidence preservation

C) time and resources required

D) potential for damage and theft

Explanation

Once the attack has taken place, the manner in which it was delivered (attack vector) is not a consideration during containment.

NIST Special Publication 800-61 defines the following criteria for determining the appropriate containment, eradication, and recovery strategy:

- The potential damage to and theft of resources
- The need for evidence preservation
- Service availability (for example, network connectivity as well as services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (for example, partial containment or full containment)
- Duration of the solution (for example, emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, or permanent solution)

Objective:
Security Policies and Procedures

Sub-Objective:
Map elements to these steps of analysis based on the NIST.SP800-61 (Preparation: Detection and analysis; Containment, eradication, and recovery; Post-incident analysis (lessons learned))

References:

NIST > Computer Security Incident Handling Guide (PDF)

Question #31 of 84

Question ID: 1323124

You have discovered that a compromised host in your network is communicating with an IP address that is well known to be malicious. Which step of the Cyber Kill Chain framework are you most likely in?

A) action on objectives

B) installation

C) command and control

D) exploitation

Explanation

It is the command and control step. Communication with a well-known malicious IP address is part of the Command and Control step, since the remote device is quite likely a Command and control (CnC) server designed to control the target.

It is not the exploitation step. Exploitation comes after the attacker creates a weapon and delivers the weapon. It occurs when the weapon executes. Were the user to execute the attachment, we would be in the exploitation stage.

It is not the installation step. Installation comes after exploitation and involves the installation of additional tools and resources the hacker will use. These tools allow the attacker to maintain persistence while plotting the next step.

Installation of a remote access Trojan (RAT) would be part of the installation step.

It is not the action on objectives step. During the action on objectives step, the attacker achieves the long-term goal. For example, it could be defacing a website or it could be stealing money.

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

The Cyber Kill Chain frameworkLockheed Martin > The Cyber Kill Chain®

Question #32 of 84

Question ID: 1323071

Which of the following is the second step in incident handling, according to NIST.SP 800-61 r2?

A) preparation
B) containment, eradication and recovery
C) detection and analysis
D) post incident analysis

Explanation

According to NIST.SP800-61 r2, the steps in order are:

1. Preparation
2. Detection and analysis
3. Containment, eradication and recovery
4. Post incident analysis

The second step, detection and analysis, involves the determination that the incident is a security incident and then the classification of its seriousness. Based on that assessment, the incident is reported to the proper authorities.

Objective:
Security Policies and Procedures

Sub-Objective:
Map elements to these steps of analysis based on the NIST.SP800-61 (Preparation: Detection and analysis; Containment, eradication, and recovery; Post-incident analysis (lessons learned))

References:

NIST > Computer Security Incident Handling Guide (PDF)

Question #33 of 84

Question ID: 1323085

Which of the following handle the investigation, resolution, and disclosure of security vulnerabilities in their products and services?

A) Coordination centers

B) National CSIRT

C) MSSP

D) PSIRT

Explanation

Product security incident response teams (PSIRTs) handle the investigation, resolution, and disclosure of security vulnerabilities in their products and services.

Managed security service providers (MSSPs) provide incident response and managed security services to their customers. Cisco's Incident Response Service is an example of this type of team.

National CSIRTS provide incident handling for a country.

Coordination centers around the world also help CSIRTS coordinate incident handling. They also help coordinate security vulnerability disclosures to vendors, hardware and software providers, and security researchers.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe concepts as documented in NIST.SP800-86 (Evidence collection order; Data integrity; Data preservation; Volatile data collection)

References:

Exabeam > The Complete Guide to CSIRT Organization: How to Build an Incident Response Team

Question #34 of 84

Question ID: 1323133

Which of the following is responsible for incident classification and handling on behalf of a single corporation?

A) MSSP

B) Coordination center

C) CSIRT

D) PSIRT

Explanation

The CSIRT works hand in hand with the information security team (in many cases, it's the same team) and is responsible for corporate incident classification and handling. A CSIRT would protect the corporation's infrastructure.

Product security incident response teams (PSIRTs) are internal to a vendor, and they handle the investigation, resolution, and disclosure of security vulnerabilities in a vendor's products and services. A PSIRT would be responsible for fixing the vendor's products for customers who use the products. The PSIRT would not respond to incidents that affect its own organization's infrastructure.

Managed security service providers (MSSPs) provide incident response and managed security services to their customers. Cisco's Incident Response Service is an example of this type of team. The CSIRT would respond to incidents that affect the MSSP's own infrastructure.

Coordination centers around the world also help CSIRTS coordinate incident handling. They also help coordinate security vulnerability disclosures to vendors, hardware and software providers, and security researchers.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

References:

Exabeam > The Complete Guide to CSIRT Organization: How to Build an Incident Response Team

Carnegie Mellon University > Software Engineering Institute > Education and Outreach > Computer Security Incident Response Teams > National CSIRTs

---

Question #35 of 84

Question ID: 1323121

When an email with a malicious attachment is delivered to a mailbox, what step in the Cyber Kill Chain framework has occurred?

A) Delivery
B) Exploitation
C) Weaponization
D) Reconnaissance

Explanation

When an email with a malicious attachment is delivered to a mailbox, the delivery step has occurred. This occurs when the exploit is delivered to the target.

The seven steps in the kill chain are:

1. Reconnaissance – the attacker gathers information to aid in penetrating the network
2. Weaponization – the attacker turns a legitimate utility or function into a weapon that can be used in the attack
3. Delivery – the attacker transmits the crafted exploit to the target
4. Exploitation – the exploit is executed
5. Installation – the hacker installs additional tools and resources on the target device or in the target network
6. Command and control (C2 – the attacker takes remote control of the target device from the Command and control (CnC) server
7. Actions on objectives – the attacker takes action (deletes data, steals data, defaces website)

It is not the reconnaissance step. For example, consider an exploit takes advantage of an injection vulnerability in an exploitable Hypertext Preprocessor php file by sending an HTTP POST with specific variables. If the hacker sends an HTTP GET request the page, the attack is still in reconnaissance.

It is not the weaponization step. Weaponization occurs when the attacker turns some utility or function into a weapon he can use in the attack. It occurs after reconnaissance. Using Metasploit to craft an exploit is an example.

It is not the exploitation step. Exploitation comes after the attacker creates a weapon and delivers the weapon. It occurs when the weapon executes. Were the user to execute the attachment we would be in the exploitation stage.

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

HYPERLINK "https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html"The Cyber Kill Chain frameworkLockheed Martin > The Cyber Kill Chain®

Question #36 of 84

Question ID: 1323059

What would you use to identify, remove, and mitigate system vulnerabilities?

- **A)** port scan
- **B)** network discovery
- **C)** service discovery
- **D)** vulnerability management framework

Explanation

The purpose of a vulnerability management framework is to identify, remove, and mitigate system vulnerabilities. In some cases, the vulnerability cannot be removed, but its impact or likelihood might be lessened.

The other three options might be a part of a vulnerability management framework, but alone they do not identify, remove, and mitigate system vulnerabilities.

Port scans locate open ports on devices that can represent security vulnerabilities.

Network discovery is the process of identifying live devices and IP addresses.

Service discovery is another term for port scan.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe management concepts (Asset management; Configuration management; Mobile device management; Patch management; Vulnerability management)

References:

Cisco > Vulnerability Management

Question #37 of 84

Question ID: 1323068

What occurs in the containment stage of incident handling?

- **A)** determining whether there is an incident
- **B)** minimizing the impact
- **C)** documenting the incident and reporting
- **D)** determining the extent

Explanation

In the containment stage, halting the spread of the incident and minimizing the impact is the goal. There are six steps in the incident handling process:

1. Identification – determining whether there is an incident
2. Scoping – determining the extent of the incident and identifying the attackers
3. Containment – halting the spread of the incident and minimizing the impact
4. Remediation – returning the environment to secure state
5. Lesson-based hardening – preventing future incidents
6. Reporting – documenting the incident and reporting it

Objective:
Security Policies and Procedures

Sub-Objective:
Apply the incident handling process (such as NIST.SP800-61) to an event

References:

NIST > SP 800-61 Rev. 2 Computer Security Incident Handling Guide

---

Question #38 of 84

Question ID: 1323136

Which of the following metrics used to measure the effectiveness of a run book represents the average time to recover a system from a hardware failure?

A) FIT

B) MTTF

C) MTTR

D) MTBF

Explanation

Mean time to recover (MTTR) is average time to recover a system from a hardware failure. Should a component or an entire system fail, it is important to know how long it would take to repair it, or how long it would be before a replacement could be up and running.

The mean time between failures (MTBF) is the estimated amount of time that a piece of equipment should remain operational before failure. The MTBF is usually supplied by the hardware vendor or a third party. MTBF can also be referred to as mean time to failure (MTTF).

Mean time to failure (MTTF) is the average time until the first failure occurs in a piece of equipment.

Failure in time (FIT) is another way of reporting MTBF. FIT reports the number of expected failures per one billion hours of operation for a device.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

References:

B+B > MTBF, MTTR, MTTF & FIT Explanation of Terms (PDF)

Question #39 of 84

Question ID: 1323101

Which statement is FALSE with respect to listening ports?

A) The port number does not always identify the service.

B) They are closed.

C) Port 443, when set to default, is encrypted.

D) Ports can be numbered 1 to 65535.

Explanation

Ports can be open, closed, or filtered. When they are open, they are said to be listening. When closed they are not listening.

While ports do have default port numbers, it is possible to run a service on a non-default port number.

Software ports can be numbered from 1 to 65535. The first 1024 or so are called well known. Some of these well-known port numbers at their defaults are:

- TCP 20 and 21: File Transfer Protocol (FTP)
- TCP 22: Secure Shell (SSH)
- TCP 23: Telnet
- TCP 25: Simple Mail Transfer Protocol (SMTP)
- TCP and UDP 53: Domain Name System (DNS)
- UDP 69: Trivial File Transfer Protocol (TFTP)
- TCP 79: Finger
- TCP 80: Hypertext Transfer Protocol (HTTP)
- TCP 110: Post Office Protocol v3 (POP3)
- TCP 119: Network News Protocol (NNTP)
- UDP 161 and 162: Simple Network Management Protocol (SNMP)
- UDP 443: Secure Sockets Layer over HTTP (HTTPS)

Port 443 is SSL over HTTP, which is encrypted.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for server profiling (Listening ports; Logged in users/service accounts; Running processes; Running tasks; Applications)

References:

Meridian Outpost > What are the TCP/IP Well Known Port Numbers (0 to 1023)

Question #40 of 84

Question ID: 1323123

After compromising a host and escalating privileges, the attacker installs a remote access Trojan (RAT). What step of the Cyber Kill Chain framework has just occurred?

A) Installation

B) Weaponization

C) Reconnaissance

D) Exploitation

Explanation

It is the installation step. Installation comes after exploitation and involves the installation of additional tools and resources the hacker will use. These tools allow the attacker to maintain persistence while plotting the next step. Installation of a remote access Trojan (RAT) would be part of the installation step.

It is not the reconnaissance step when information is gathered. For example, consider an exploit takes advantage of an injection vulnerability in an exploitable php by sending an HTTP POST with specific variables. If the hacker sends an HTTP GET request the page, the attack is still in reconnaissance.

It is not the weaponization step. Weaponization occurs when the attacker turns some utility or function into a weapon he can use in the attack. It occurs after reconnaissance. Using Metasploit to craft an exploit is an example.

It is not the exploitation step. Exploitation comes after the attacker creates a weapon and delivers the weapon. It occurs when the weapon executes. Were the user to execute the attachment we would be in the exploitation stage.

The seven steps in the kill chain are:

1. Reconnaissance – the attacker gathers information to aid in penetrating the network
2. Weaponization – the attacker turns a legitimate utility or function into a weapon that can be used in the attack
3. Delivery – the attacker transmits the crafted exploit to the target
4. Exploitation – the exploit is executed
5. Installation – the hacker installs additional tools and resources on the target device or in the target network
6. Command and control (C2 – the attacker takes remote control of the target device from the Command and control (CnC) server
7. Actions on objectives – the attacker takes action (deletes data, steals data, defaces website)

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

The Cyber Kill Chain frameworkLockheed Martin > The Cyber Kill Chain®

Question #41 of 84

Question ID: 1323088

According to NIST, what goal are you supporting when you hash both evidence data and backup of the data and compare the hashes?

A) authentication

B) confidentiality

C) availability

D) integrity

Explanation

Hashing is used to prove integrity or prove that the data has not changed since the original hash values were generated.

Confidentiality is provided by applying access controls or encryption. The goal is to prevent unauthorized viewing of data.

Availability is provided by redundancy. The goal is to maintain access to the data at all times.

Authentication is provided by assessing credentials. The goal is to only allow credentialed entities to log in.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe concepts as documented in NIST.SP800-86 (Evidence collection order; Data integrity; Data preservation; Volatile data collection)

References:

SP 800-86 Guide to Integrating Forensic Techniques into Incident Response

---

Question #42 of 84

Question ID: 1323127

According to VERIS schema, which of the following is NOT one of the subsets of incident tracking?

A) incident confirmation

B) source ID

C) victim demographics

D) incident ID

Explanation

Victim demographics is one of the main categories in the VERIS schema and is not a subset of the Incident tracking category.

The Incident tracking category contains items related to capturing information about the incident. Items included are

- Incident ID - identifies the event
- Source ID - identifies the body or agency reporting it or handling it
- Incident confirmation - was it a security event
- Incident summary - brief description
- Related incident - links to larger campaigns
- Confidence rating - rating of the level of assurance with data collected
- Incident notes- any other general information

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

VERIS > The Vocabulary for Event Recording and Incident Sharing

---

Question #43 of 84

Question ID: 1323072

In which stage of the NIST SP 800-61 r2 incident handling method do you ensure that the organization has appropriate incident analysis hardware and software as well as incident mitigation software?

A) detection and analysis
B) preparation
C) containment, eradication, and recovery
D) post-incident activity

Explanation

The preparation phase includes:

- Creating processes for incident handler communications and the facilities that will host the security operation center (SOC) and incident response team
- Making sure that the organization has appropriate incident analysis hardware and software as well as incident mitigation software
- Creating risk assessment capabilities within the organization
- Making sure the organization has appropriately deployed host security, network security, and malware prevention solutions
- Developing user awareness training
- Post incident activity covers lessons learned.

Containment eradication and recovery includes evidence gathering and handling, identifying the attacking hosts and choosing a containment strategy.

The detection and analysis phase covers analysis of the evidence found.

Objective:
Security Policies and Procedures

Sub-Objective:
Map elements to these steps of analysis based on the NIST.SP800-61 (Preparation: Detection and analysis; Containment, eradication, and recovery; Post-incident analysis (lessons learned))

References:

NIST > Computer Security Incident Handling Guide (PDF)

Question #44 of 84

Question ID: 1323069

What is the third step in the incident handling procedure?

A) Identification
B) Reporting
C) Scoping
D) Containment

Explanation

There are six major phases in incident handling. The roadmap for implementing the incident response plan is defined by these incident handling procedures.

1. Identification – determining whether there is an incident
2. Scoping – determining the extent of the incident and identifying the attackers
3. Containment – halting the spread of the incident and minimizing the impact
4. Remediation – returning the environment to secure state
5. Lesson-based hardening – preventing future incidents
6. Reporting – documenting the incident and reporting it

Objective:
Security Policies and Procedures

Sub-Objective:
Apply the incident handling process (such as NIST.SP800-61) to an event

References:

Broadcom > An Introduction to Incident Handling

Question #45 of 84

Question ID: 1323122

A penetration tester is hired and succeeds in attacking a vulnerability. What step of the Cyber Kill Chain framework is the test performing?

A) action on objectives
B) installation
C) exploitation
D) command and control

Explanation

When the attacker either successfully attacks a vulnerability or executes a delivered payload, the test is in the exploitation step. Exploitation comes after the attacker creates a weapon and delivers the weapon. It occurs when the weapon executes.

It is not the installation step. Installation comes after exploitation and involves the installation of additional tools and resources the hacker will use. These tools allow the attacker to maintain persistence while plotting the next step. Installation of a remote access Trojan (RAT) would be part of the installation step.

It is not the command and control step. Communication with a well-known malicious IP address is part of the Command and Control step, since the remote device is quite likely a command and control (CnC) server designed to control the target.

It is not the action on objectives step. During the action on objectives step, the attacker achieves the long-term goal. For example, it could be defacing a website or it could be stealing money.

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

The Cyber Kill Chain frameworkLockheed Martin > The Cyber Kill Chain®

Question #46 of 84

Question ID: 1323053

What characteristic of a vulnerability scanner would allow you to determine all devices affected by an attack?

A) trend analysis

B) low false positives

C) retrospective analysis

D) ability to perform multiple scans

Explanation

Some scanners can use threat intelligence to perform retrospective (looking back in time) analysis. This would allow it to do something like determine when malware entered your network, as in many cases it enters long before you discover it.

While low false positives is a good thing, it is not the characteristic that would allow you to determine all devices affected by an attack. A false positive occurs when the scanner identifies a vulnerability that does not exist.

Trend analysis uses historical data to chart trends in traffic flows or in events frequency. It would not allow you to determine all devices affected by an attack.

The ability to perform multiple scans is a value-added feature, but it is not the characteristic that would allow you to determine all devices affected by an attack.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe management concepts (Asset management; Configuration management; Mobile device management; Patch management; Vulnerability management)

References:

Cisco > Support > Product Support > Security > Cisco Firepower Management Center > Configuration Guides > Firepower Management Center Configuration Guide, Version 6.0 > Chapter: File/Malware Events and Network File Trajectory

Question #47 of 84

Question ID: 1323094

Which statement is FALSE with respect to open ports?

A) If you send a TCP packet with the SYN flag set, you will receive one with the SYN and ACK flags back

B) Port 23 is FTP

C) If it is listening, it is open

D) Ports use values that range between 1 and 65535.

Explanation

Port 23 is not used by FTP. It is used by Telnet. Although port numbers do have defaults set for well-known services, you can always change the port on which a service is running.

An open port is also called a “listening” port in some instances. Open or listening ports have an available service running on them. It may or may not be the default service for that port. If the port is closed, it means a service is not available on that port.

Ports use values that range between 1 and 65535.

If you send a TCP packet with the SYN flag set, you will receive one with the SYN and ACL flags back if it is open. If it is closed, you will receive a packet with the RST flag set. If you receive no response, the port is filtered or blocked on the firewall.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for network profiling (Total throughput; Session duration; Ports used; Critical asset address space)

References:

Rackspace > Check listening ports with netstat

Question #48 of 84

Question ID: 1323057

In which policy would one find the procedures to be followed for equipment after an employee is terminated?

A) physical security
B) asset return
C) AUP
D) data classification

Explanation

The asset return policy dictates at which times a laptop must be turned in after an employee is terminated, and how that process occurs.

An acceptable use policy defines the manner in which employees are allowed to use a company's network equipment and resources, such as bandwidth, Internet access, and e-mail services.

The data classification policy dictates the process for classifying data by sensitivity.

The physical security plan covers the protection of the facility and all physical assets, but does not address returning equipment following a termination.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe management concepts (Asset management; Configuration management; Mobile device management; Patch management; Vulnerability management)

References:

Fiix > A complete guide to building an asset management policy

---

Question #49 of 84

Question ID: 1323114

What is the first step in the Cyber Kill Chain framework?

A) reconnaissance

B) installation

C) exploitation

D) weaponization

Explanation

The first and most important step is reconnaissance when information is gathered that helps penetrate the network. For example, consider an exploit that takes advantage of an injection vulnerability in an exploitable Hypertext Preprocessor (php) file by sending an HTTP POST with specific variables. If the hacker sends an HTTP GET request to the page, the attack is still in reconnaissance.

The seven steps in the kill chain are:

- Reconnaissance – the attacker gathers information to aid in penetrating the network
- Weaponization – the attacker turns a legitimate utility or function into a weapon that can be used in the attack
- Delivery – the attacker transmits the crafted exploit to the target
- Exploitation – the exploit is executed
- Installation – the hacker installs additional tools and resources on the target device or in the target network
- Command and control (C2 – the attacker takes remote control of the target device from the Command and control (CnC) server
- Actions on objectives – the attacker takes action (deletes data, steals data, defaces website)

Weaponization occurs when the attacker turns some utility or function into a weapon he can use in the attack. It occurs after reconnaissance.

Exploitation comes after the attacker creates a weapon and delivers the weapon.

Installation comes after exploitation and involves the installation of additional tools and resources the hacker will use. This allows the attacker to maintain persistence while plotting the next step.

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

The Cyber Kill Chain frameworkLockheed Martin > The Cyber Kill Chain®

Question #50 of 84

Question ID: 1323112

You have been tasked with protecting user’s medical records. What type of information are you protecting?

A) PCI-DSS

B) HIPAA

C) PHI

D) PII

Explanation

Medical records are considered Personal Health Information (PHI) and must be protected from unauthorized disclosure.

Personally identifiable information (PII) is any piece of information that can be used to uniquely identify a person, such as full name, account name, phone number, license number, date of birth, social security number, or any other personal attribute.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the act governs the handling of PHI.

The Payment Card Industry Data Security Standard (PCI DSS) protects credit card information, not medical records.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify protected data in a network (PII; PSI; PHI; Intellectual property)

References:

File Cloud > What is PII and PHI? Why is it Important?

Question #51 of 84

Question ID: 1323082

Which of the following would provide cybersecurity training and incident response to both a federal executive branch agency and a foreign company?

A) National CSIRT
B) Coordination center
C) Internal CSIRT
D) PSIRT

Explanation

A national Computer Security Incident Response Team (national CSIRT) provides cybersecurity protection to an entire country or a significant portion of a national economy, which would include protecting federal civilian or executive branch agencies. CSIRTs provide incident handling capabilities as well as training and coordination of vulnerability databases. Two well-known national CSIRTs are the Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT) and the United States Cyber Emergency Readiness Team (US-CERT).

As of this writing, ICS-CERT and US-CERT are both part of the U. S. National Cybersecurity and Communications Integration Center (NCCIC). NCCIC provides centralized cybersecurity responses and resources to federal agencies; state, tribal, local, and territorial governments; international partners; and private industry partners.

Coordination centers around the world also help coordinate the activities of CSIRTS. They also coordinate security vulnerability disclosures to vendors, hardware and software providers, and security researchers. Unlike a CSIRT, a coordination center only coordinates; it does not provide active cybersecurity.

Product security incident response teams (PSIRTs) are internal to a vendor, and they handle the investigation, resolution, and disclosure of security vulnerabilities in a vendor’s products and services. They would not coordinate responses for any product not produced by their parent organization.

Internal CSIRTs handle incidents for the organization for which they are employed. A government agency may have an internal CSIRT as well as taking advantage of the resources from a national CSIRT.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe concepts as documented in NIST.SP800-86 (Evidence collection order; Data integrity; Data preservation; Volatile data collection)

References:

Carnegie Mellon University > Software Engineering Institute > Education and Outreach > Computer Security Incident Response Teams > National CSIRTs

Cybersecurity and Infrastructure Security Agency (CISA) > About Us

NIST > Computer SecurityIncident Handling Guide (PDF)

Question #52 of 84

Question ID: 1323129

Actors and actions are part of which VERIS schema category?

A) victim demographics

B) incident tracking

C) discovery and response

D) incident description

Explanation

Actors and actions are subsets of the incident description category. Its contents include:

- Actors: Whose actions affected the asset?
- Actions: What actions affected the asset?
- Assets: Which assets were affected?
- Attributes: How the asset was affected

The victim demographic category includes:

- Victim ID
- Primary industry
- Country of operation
- State
- Number of employees
- Annual revenue
- Operations affected
- Notes

The incident tracking category includes:

- Incident ID - identifies the event
- Source ID - identifies the body or agency reporting it or handling it
- Incident confirmation - was it a security event
- Incident summary - brief description
- Related incident - links to larger campaigns
- Confidence rating - rating of the level of assurance with data collected
- Incident notes- any other general information

The discovery and response category includes:

- Incident timeline
- Discovery method
- Root causes
- Corrective actions
- Targeted vs opportunistic

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

VERIS > The Vocabulary for Event Recording and Incident Sharing

---

Question #53 of 84

Question ID: 1323061

Which publication from the NIST covers the incident handling process?

A) IOC 27001:2013

B) IEEE 802.2

C) SP 800-61

D) SP 800-65

Explanation

The NIST SP 800-61 covers the handling of security incidents and managing the response to such incidents. That process includes:

- Preparation - actually having a plan for responding to incidents
- Detection and analysis - defining what type of incident is it
- Containment Eradication and Recovery - eliminating the threat and returning the environment to normal
- Post-incident activity - applying lesson learned to new threats

IOC 27001:2013 is a guideline document for establishing an information security management system.

SP-800-65 covers Integrating IT Security into the Capital Planning and Investment Control Process and has been withdrawn.

IEEE 802.2 is the standard for Ethernet.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe the elements in an incident response plan as stated in NIST.SP800-61

References:

NIST > SP 800-61 Rev. 2 Computer Security Incident Handling Guide

---

Question #54 of 84

Question ID: 1323119

What is the final step in the Cyber Kill Chain framework?

A) installation

B) exploitation

C) command and control

D) action on objectives

Explanation

During the action on objectives step, the attacker achieves the long term goal. For example it could be defacing a website or it could be stealing money.

Exploitation comes after the attacker creates a weapon and delivers the weapon. It occurs when the weapon executes.

Installation comes after exploitation and involves the installation of additional tools and resources the hacker will use. These tools allow the attacker to maintain persistence while plotting the next step. Installation of a remote access Trojan (RAT) would be part of the installation step.

Communication with well-known malicious IP address is part of the Command and Control step, since the remote device is quite likely a command and control (CnC) server.

The seven steps in the kill chain are:

1. Reconnaissance – the attacker gathers information to aid in penetrating the network
2. Weaponization – the attacker turns a legitimate utility or function into a weapon that can be used in the attack
3. Delivery – the attacker transmits the crafted exploit to the target
4. Exploitation – the exploit is executed
5. Installation – the hacker installs additional tools and resources on the target device or in the target network
6. Command and control (C2 – the attacker takes remote control of the target device from the Command and control (CnC) server
7. Actions on objectives – the attacker takes action (deletes data, steals data, defaces website)

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

The Cyber Kill Chain frameworkLockheed Martin > The Cyber Kill Chain®

Question #55 of 84

Question ID: 1323096

What do hackers target when they want to identify open services on a device?

A) port numbers

B) IP addresses

C) IVs

D) MAC addresses

Explanation

Well known services reside on software ports. Hackers probe these ports to identity is of they are open. If they are the hacker well attempt well known attacks on these services.

IP addresses are part of the probing process but not the element that identifies a service. They identify the device.

MAC addresses are sometimes used in attacks but are not the element that identifies a service. They identify the device.

Initialization vectors (IVs) are used with cryptographic algorithm and have nothing to do with port numbers or identifying open services on a device.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for server profiling (Listening ports; Logged in users/service accounts; Running processes; Running tasks; Applications)

References:

Rackspace > Check listening ports with netstat

Question #56 of 84

Question ID: 1323086

When the device used to store evidence is part of the evidence what has occurred?

A) scoping
B) cross contamination
C) lessons -based hardening
D) chain of custody

Explanation

Evidentiary cross contamination occurs when the device used to store evidence is part of the evidence. Any drives that store evidence should not be altered in any way and should not be used to store evidence of any other incident.

Chain of custody is the recording of the location and status of evidence during all time periods between collection and presentation.

Lesson-based hardening is a step in the incident handling process in which future incidents are prevented by making changes.

Scoping is a step in the incident handling process in which the extent of the incident and identification of attackers takes place.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe concepts as documented in NIST.SP800-86 (Evidence collection order; Data integrity; Data preservation; Volatile data collection)

References:

NIST > SP 800-61 Rev. 2 Computer Security Incident Handling Guide

Question #57 of 84

Question ID: 1323128

Which of the following is NOT one of the milestones in the incident timeline according to VERIS schema?

A) first malicious action

B) data destruction

C) data exfiltration

D) containment/restoration

Explanation

While the destruction of data is always of interest, it is not one of the milestones in the incident timeline, according to VERIS schema. These milestones are (quoted from the VERIS site):

- First malicious action: Beginning of the threat actor's malicious actions against the victim. Port scans, initiating a brute-force attack, and even physical recon, are a few examples. This is only relevant to intentional and malicious actions.
- Initial compromise: First point at which a security attribute (C/P, I/A, A/U) of an information asset was compromised.
- Data exfiltration: First point at which non-public data was taken from the victim environment. Only applicable to data compromise events.
- Incident discovery: When the organization first learned the incident had occurred.
- Containment/restoration: Point at which the incident is contained (e.g., the “bleeding is stopped”) or restored (e.g., fully functional)”.

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

HYPERLINK "http://veriscommunity.net/index.html" VERIS > The Vocabulary for Event Recording and Incident Sharing

Question #58 of 84

Question ID: 1323056

Which of the following is least likely to be a part of patch management?

A) research significant updates

B) manage automatic updates

C) install patches

D) remove patches

Explanation

While installing patches is typically a part of patch management, removing patches is not. Only in rare cases where a deployed patch breaks something would this be required.

While many updates are automatic, some are not. It is incumbent on the security professional to research updates they may need that are not automatically applied.

Automatic updates make the process easier, but these updates still have to be managed.

Installing patches is one of the prime operations in patch management.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe management concepts (Asset management; Configuration management; Mobile device management; Patch management; Vulnerability management)

References:

Itarian > Patch Management

Question #59 of 84

Question ID: 1323108

Which data elements must be protected by the PCI-DSS standard? (Choose all that apply.)

A) last payment amount

B) mailing address

C) last charge amount

D) primary account number

E) full cardholder’s name

Explanation

PCI-DSS requires the full name and primary account number to be protected because the full name and account number are both unique to a user. Because PCI-DSS is a contract, its requirements are a contractual obligation rather than a law or regulation. But they still have to be implemented and followed. Violations of a contract can result in legal complications.

The PCI-DSS standard specifies these requirements for compliance:

- Install and maintain a firewall configuration to protect cardholder data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect stored cardholder data.
- Encrypt transmission of cardholder data across open, public networks.
- Use and regularly update antivirus software.
- Develop and maintain secure systems and applications.
- Restrict access to cardholder data by business need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify protected data in a network (PII; PSI; PHI; Intellectual property)

References:

PCI Document Library

Question #60 of 84

Question ID: 1323116

In which step of the Cyber Kill Chain framework does an attacker use Metasploit to craft an exploit?

A) Installation
B) Delivery
C) Exploitation
D) Weaponization

Explanation

Weaponization occurs when the attacker turns some utility or function into a weapon he can use in the attack. It occurs after reconnaissance. Using Metasploit to craft an exploit is an example.

In the Delivery step, the attackers transmits the crafted exploit to the target.

Exploitation comes after the attacker creates a weapon and delivers the weapon. It occurs when the weapon executes.

Installation comes after exploitation and involves the installation of additional tools and resources the hacker will use. These tools allow the attacker to maintain persistence while plotting the next step. Installation of a remote access Trojan (RAT) would be part of the installation step.

The seven steps in the kill chain are:

- Reconnaissance – the attacker gathers information to aid in penetrating the network
- Weaponization – the attacker turns a legitimate utility or function into a weapon that can be used in the attack
- Delivery – the attacker transmits the crafted exploit to the target
- Exploitation – the exploit is executed
- Installation – the hacker installs additional tools and resources on the target device or in the target network
- Command and control (C2 – the attacker takes remote control of the target device from the Command and control (CnC) server
- Actions on objectives – the attacker takes action (deletes data, steals data, defaces website)

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

The Cyber Kill Chain frameworkLockheed Martin > The Cyber Kill Chain®

Question #61 of 84

Question ID: 1323070

In which stage of incident handling would you identify the exploit used and the financial impact?

A) remediation

B) lessons-based hardening

C) reporting

D) identification

Explanation

In the reporting step, the following items are recorded:

- Exploit or vulnerability used
- Impact or financial loss
- Detection method

There are six steps in the incident handling process:

1. Identification – determining whether there is an incident
2. Scoping – determining the extent of the incident and identifying the attackers
3. Containment – halting the spread of the incident and minimizing the impact
4. Remediation – returning the environment to secure state
5. Lesson-based hardening – preventing future incidents
6. Reporting – documenting the incident and reporting it

Objective:
Security Policies and Procedures

Sub-Objective:
Apply the incident handling process (such as NIST.SP800-61) to an event

References:

NIST > SP 800-61 Rev. 2 Computer Security Incident Handling Guide

Question #62 of 84

Question ID: 1323075

Which of the following is NOT an element of the NIST.SP800-61 r2 incident response plan?

A) metrics

B) organizational approach to security

C) disaster recovery

D) communications with other organizations

E) senior management approval

Explanation

Disaster recovery is NOT a part of incident response and should have a separate team and set of policy elements.

NIST SP 800-61 v2 is the Computer Security Incident Handling Guide. According to this publication, the four major phases of the incident response lifecycle are:

1. Preparation
2. Detection and analysis
3. Containment, eradication, and recovery
4. Post incident analysis

The incident response plan elements include:

- Incident response plan’s mission
- Strategies and goals of the incident response plan
- Senior management approval of the incident response plan
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization

Objective:
Security Policies and Procedures

Sub-Objective:
Map elements to these steps of analysis based on the NIST.SP800-61 (Preparation: Detection and analysis; Containment, eradication, and recovery; Post-incident analysis (lessons learned))

References:

NIST > Computer Security Incident Handling Guide (PDF)

Question #63 of 84

Question ID: 1323097

Which netstat command displays all connections and listening ports?

A) `netstat -f`

B) `netstat --e`

C) `netstat -a`

D) `netstat -b`

Explanation

The netstat -a command shows all connections and listening ports. An example output is shown below.

```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\mcmil>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:902            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:912            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:6646           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:8733           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:17500          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:843          DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:5354         DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:17600        DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:50003        DESKTOP-V59I9G6:50004  ESTABLISHED
  TCP    127.0.0.1:50004        DESKTOP-V59I9G6:50003  ESTABLISHED
  TCP    127.0.0.1:50210        DESKTOP-V59I9G6:50211  ESTABLISHED
  TCP    127.0.0.1:50211        DESKTOP-V59I9G6:50210  ESTABLISHED
```

The `netstat -b` command displays the executable involved in creating the connection.

```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -b

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49751        DESKTOP-V59I9G6:49752  ESTABLISHED
[Dropbox.exe]
  TCP    127.0.0.1:49752        DESKTOP-V59I9G6:49751  ESTABLISHED
[Dropbox.exe]
  TCP    127.0.0.1:49768        DESKTOP-V59I9G6:49769  ESTABLISHED
[Dropbox.exe]
  TCP    127.0.0.1:49769        DESKTOP-V59I9G6:49768  ESTABLISHED
[Dropbox.exe]
  TCP    127.0.0.1:58025        DESKTOP-V59I9G6:58026  ESTABLISHED
[Dropbox.exe]
  TCP    127.0.0.1:58026        DESKTOP-V59I9G6:58025  ESTABLISHED
[Dropbox.exe]
  TCP    192.168.1.71:17500     DESKTOP-6FCDEI1:65105  ESTABLISHED
[Dropbox.exe]
```

The `netstat -e` command displays Ethernet statistics.

```
C:\WINDOWS\system32>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     764479693       179105700
Unicast packets              914545          604183
Non-unicast packets          209808           24887
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

The `netstat - f` command displays fully qualified domain names for foreign addresses.

```
C:\WINDOWS\system32>netstat -f

Active Connections
```

```
Proto  Local Address          Foreign Address        State
TCP    127.0.0.1:49751        DESKTOP-V59I9G6:49752  ESTABLISHED
TCP    127.0.0.1:49752        DESKTOP-V59I9G6:49751  ESTABLISHED
TCP    127.0.0.1:49768        DESKTOP-V59I9G6:49769  ESTABLISHED
TCP    127.0.0.1:49769        DESKTOP-V59I9G6:49768  ESTABLISHED
TCP    127.0.0.1:58025        DESKTOP-V59I9G6:58026  ESTABLISHED
TCP    127.0.0.1:58026        DESKTOP-V59I9G6:58025  ESTABLISHED
TCP    192.168.1.71:17500     DESKTOP-6FCDEI1.attlocal.net:65105  ESTABLISHED
```

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for server profiling (Listening ports; Logged in users/service accounts; Running processes; Running tasks; Applications)

References:

Lifewire > How to Use the Netstat Command

Question #64 of 84

Question ID: 1323083

Which of the following discloses vulnerabilities in a single organization’s products and services?

- **A)** National CSIRT
- **B)** MSSP
- **C)** PSIRT
- **D)** Coordination centers

Explanation

Product security incident response teams (PSIRTs) are internal to a vendor, and they handle the investigation, resolution, and disclosure of security vulnerabilities in a vendor’s products and services.

Coordination centers around the world also help CSIRTS coordinate incident handling. They also help coordinate security vulnerability disclosures to vendors, hardware and software providers, and security researchers. They would disclose vulnerabilities in the products of multiple organizations, not just a single organization or vendor.

A national Computer Security Incident Response Team (national CSIRT) provides cybersecurity protection to an entire country or a significant portion of a national economy, which would include protecting federal civilian or executive branch agencies. CSIRTs provide incident handling capabilities as well as training and coordination of vulnerability databases. Two well-known national CSIRTs are the Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT) and the United States Cyber Emergency Readiness Team (US-CERT).

Managed security service providers (MSSPs) provide incident response and managed security services to their customers. Cisco’s Incident Response Service is an example of this type of team.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe concepts as documented in NIST.SP800-86 (Evidence collection order; Data integrity; Data preservation; Volatile data collection)

References:

First Learning > PSIRT Training

Carnegie Mellon University > Software Engineering Institute > CSIRT FREQUENTLY ASKED QUESTIONS (FAQ) (PDF)

Question #65 of 84

Question ID: 1323103

Which of the following is NOT of interest during server profiling?

A) Applications

B) Running Processes

C) Closed ports

D) Logged-in Users/Service Accounts

Explanation

As closed ports cannot be compromised, they are not of interest. Open ports are of interest, however, and can be determined with the netstat command. Sample output of `netstat -a` is shown below:

```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\mcmil>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:902            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:912            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:6646           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:8733           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:17500          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:843          DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:5354         DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:17600        DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:50003        DESKTOP-V59I9G6:50004  ESTABLISHED
  TCP    127.0.0.1:50004        DESKTOP-V59I9G6:50003  ESTABLISHED
  TCP    127.0.0.1:50210        DESKTOP-V59I9G6:50211  ESTABLISHED
  TCP    127.0.0.1:50211        DESKTOP-V59I9G6:50210  ESTABLISHED
```

During server profiling, key items to discover include:

- Listening ports, the most common being:

  - TCP 20 and 21: File Transfer Protocol (FTP)
  - TCP 22: Secure Shell (SSH)
  - TCP 23: Telnet
  - TCP 25: Simple Mail Transfer Protocol (SMTP)
  - TCP and UDP 53: Domain Name System (DNS)
  - UDP 69: Trivial File Transfer Protocol (TFTP)
  - TCP 79: Finger
  - TCP 80: Hypertext Transfer Protocol (HTTP)
  - TCP 110: Post Office Protocol v3 (POP3)
  - TCP 119: Network News Protocol (NNTP)
  - UDP 161 and 162: Simple Network Management Protocol (SNMP)
  - UDP 443: Secure Sockets Layer over HTTP (HTTPS)
- Logged-in Users/Service Accounts
- Running Processes
- Applications

The **netstat** command can be used for server profiling . The `netstat -a` command shows all connections and listening ports. An example output is shown below.

```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\mcmil>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:902            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:912            DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:6646           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:8733           DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:17500          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-V59I9G6:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:843          DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:5354         DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:17600        DESKTOP-V59I9G6:0      LISTENING
  TCP    127.0.0.1:50003        DESKTOP-V59I9G6:50004  ESTABLISHED
  TCP    127.0.0.1:50004        DESKTOP-V59I9G6:50003  ESTABLISHED
  TCP    127.0.0.1:50210        DESKTOP-V59I9G6:50211  ESTABLISHED
  TCP    127.0.0.1:50211        DESKTOP-V59I9G6:50210  ESTABLISHED
```

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for server profiling (Listening ports; Logged in users/service accounts; Running

processes; Running tasks; Applications)

References:

HYPERLINK "https://www.lifewire.com/netstat-command-2618098" Lifewire > How to Use the Netstat Command

Question #66 of 84

Question ID: 1323058

Which of the following would be included in a CMDB?

A) vendor list

B) organizational chart

C) settings of a router

D) perimeter fence diagram

Explanation

A configuration management database (CMDB) contains information on the settings or configuration of the devices in the network.

A premier fence diagram, while desirable, would not be found in a CMDB.

An organizational chart is not included in a CMDB, but should be available to all organization members.

A vendor list would not be in a CMDB.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe management concepts (Asset management; Configuration management; Mobile device management; Patch management; Vulnerability management)

References:

Cherwell > The Essential Guide to the Configuration Management Database

Question #67 of 84

Question ID: 1323125

Your website was defaced last night with hate speech attacking the company. What stage of the Cyber Kill Chain framework has occurred?

A) Installation

B) Exploitation

C) Action on objectives

D) Reconnaissance

Explanation

It is the action on objectives step. During the action on objectives step, the attacker achieves the long-term goal. For example, it could be defacing a website or it could be stealing money.

It is not the reconnaissance step. For example, consider an exploit takes advantage of an injection vulnerability in an exploitable Hypertext Preprocessor php file by sending an HTTP POST with specific variables. If the hacker sends an

HTTP GET request the page, the attack is still in reconnaissance.

It is not the installation step. Installation comes after exploitation and involves the installation of additional tools and resources the hacker will use. These tools allow the attacker to maintain persistence while plotting the next step. Installation of a remote access Trojan (RAT) would be part of the installation step.

It is not the exploitation step. Exploitation comes after the attacker creates a weapon and delivers the weapon. It occurs when the weapon executes. Were the user to execute the attachment, it would be in the exploitation stage.

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

The Cyber Kill Chain frameworkLockheed Martin > The Cyber Kill Chain®

Question #68 of 84

Question ID: 1323091

The following output is displayed over a network map after running a vulnerability scan:

IP address	Hostname	Last day	Type
45.66.120.8	Roc2.mydomain.com	3.1	Malware
203.156.84.6	MIC3.mydomain.com	8.3	Spam

Which statement is FALSE with respect to this output?

A) The device at 203.156.84.6 is sending traffic identified as malware.

B) You may have issues connecting to the device at 203.156.84.6.

C) You should have no issues connecting to 45.66.120.8.

D) The device at 45.66.120.8 is sending traffic identified as malware.

Explanation

The device at 203.156.84.6 is not sending traffic identified as malware. It is sending traffic identified as spam, as indicated by the `Type` column in the chart.

The device at 203.156.84.6 is sending spam as indicted by the traffic type column in the chart. The device at 45.66.120.8 is sending traffic identified as malware.

You may have issues connecting to the device at 203.156.84.6 because it is eating bandwidth by sending spam, as indicated by the value of 8.3 in the `Last day` column. This value is just a numerical system indicating level of traffic in a scale of 1 to 10. This value could also indicate a DoS attack attempt.

You should have no issues connecting to 45.66.120.8, as the traffic level is only 3.1. However, you might not want to because it is sending malware.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for network profiling (Total throughput; Session duration; Ports used; Critical asset

address space)

References:

CSO > What are vulnerability scanners and how do they work?

Question #69 of 84

Question ID: 1323111

Which of the following is NOT considered PII?

- **A)** gender
- **B)** social security number
- **C)** driver's license number
- **D)** credit card number

Explanation

Personally identifiable information (PII) is information that can be uniquely tied to the individual only. Gender is not in that category as it is shared by many.

Social security numbers, driver's license numbers, and credit card numbers will be unique to an individual, and thus would be PII.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify protected data in a network (PII; PSI; PHI; Intellectual property)

References:

LifeLock > What Is Personally Identifiable Information (PII)?

Question #70 of 84

Question ID: 1323117

Which of the following is NOT reconnaissance?

- **A)** scanning without completing the three way handshake
- **B)** searching for the robots.txt file
- **C)** installation of a RAT
- **D)** communicating over social media

Explanation

Installation comes after exploitation and involves the installation of additional tools and resources the hacker will use. These tools allow the attacker to maintain persistence while plotting the next step. Installation of a remote access Trojan (RAT) would be part of the installation step.

The first and most important step is reconnaissance when information is gathered that helps penetrate the network. For example, consider an exploit takes advantage of an injection vulnerability in an exploitable Hypertext Preprocessor php file by sending an HTTP POST with specific variables. If the hacker sends an HTTP GET request to the page, the attack is still in reconnaissance.

Other examples of reconnaissance include obtaining IP blocks, researching social media accounts and obtaining DNS records.

The seven steps in the kill chain are:

1. Reconnaissance – the attacker gathers information to aid in penetrating the network
2. Weaponization – the attacker turns a legitimate utility or function into a weapon that can be used in the attack
3. Delivery – the attacker transmits the crafted exploit to the target
4. Exploitation – the exploit is executed
5. Installation – the hacker installs additional tools and resources on the target device or in the target network
6. Command and control (C2 – the attacker takes remote control of the target device from the Command and control (CnC) server
7. Actions on objectives – the attacker takes action (deletes data, steals data, defaces website)

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

The Cyber Kill Chain frameworkLockheed Martin > The Cyber Kill Chain®

Question #71 of 84

Question ID: 1323102

Which metric or tool can be used to determine the role of a server in a network?

A) running processes

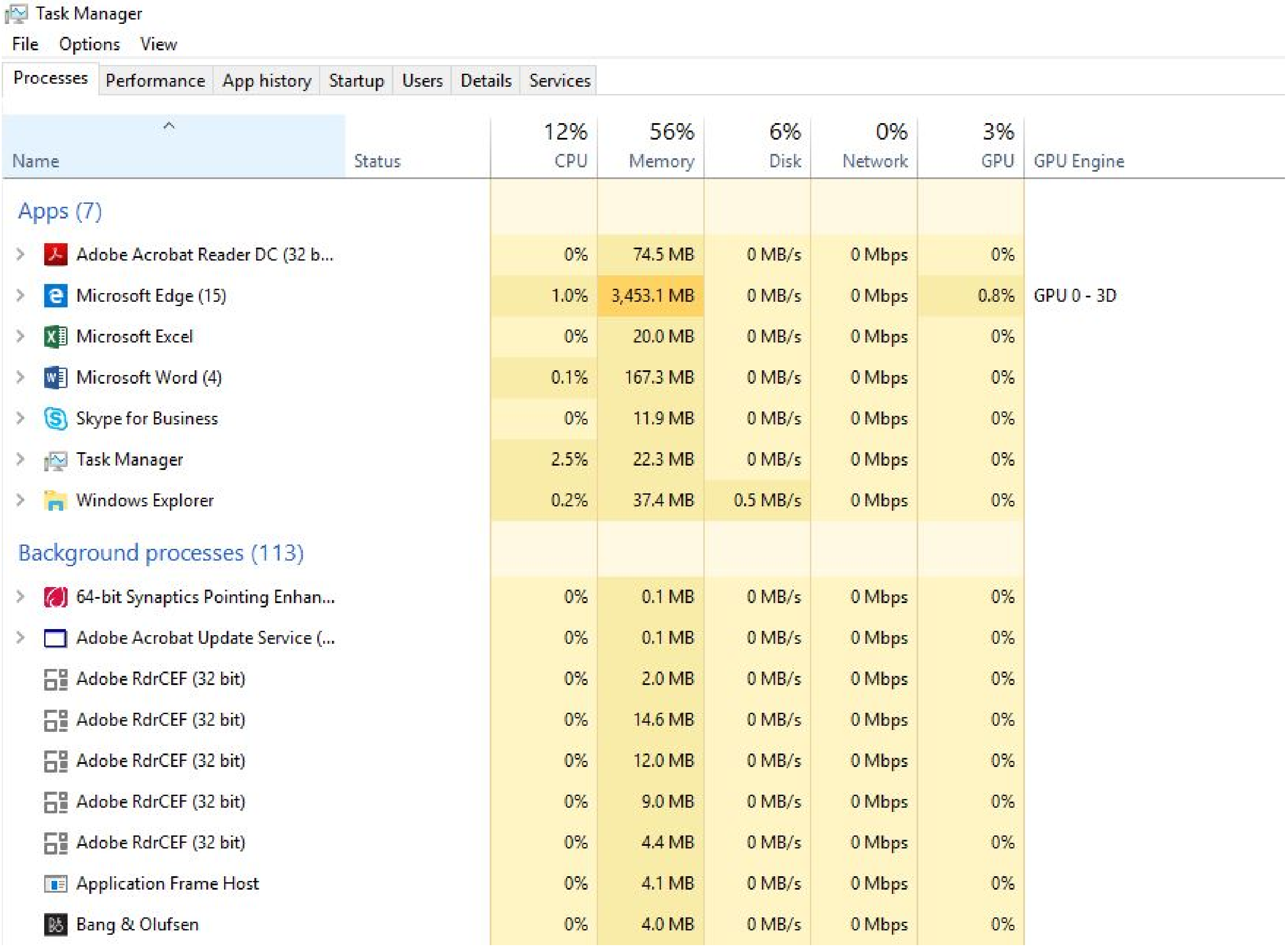
B) IP address

C) operating system version

D) `tracert`

Explanation

By identifying the running processes, you can identify the service and applications in use, and thereby derive the role of the server. Deriving the role of the server will identity potential attacks. This can be done with Task Manager as shown below. The device below appears not be a server because most of the processes and apps that are running are user applications and services.



Name	Status	12% CPU	56% Memory	6% Disk	0% Network	3% GPU	GPU Engine
Apps (7)							
Adobe Acrobat Reader DC (32 b...		0%	74.5 MB	0 MB/s	0 Mbps	0%	
Microsoft Edge (15)		1.0%	3,453.1 MB	0 MB/s	0 Mbps	0.8%	GPU 0 - 3D
Microsoft Excel		0%	20.0 MB	0 MB/s	0 Mbps	0%	
Microsoft Word (4)		0.1%	167.3 MB	0 MB/s	0 Mbps	0%	
Skype for Business		0%	11.9 MB	0 MB/s	0 Mbps	0%	
Task Manager		2.5%	22.3 MB	0 MB/s	0 Mbps	0%	
Windows Explorer		0.2%	37.4 MB	0.5 MB/s	0 Mbps	0%	
Background processes (113)							
64-bit Synaptics Pointing Enhan...		0%	0.1 MB	0 MB/s	0 Mbps	0%	
Adobe Acrobat Update Service (...		0%	0.1 MB	0 MB/s	0 Mbps	0%	
Adobe RdrCEF (32 bit)		0%	2.0 MB	0 MB/s	0 Mbps	0%	
Adobe RdrCEF (32 bit)		0%	14.6 MB	0 MB/s	0 Mbps	0%	
Adobe RdrCEF (32 bit)		0%	12.0 MB	0 MB/s	0 Mbps	0%	
Adobe RdrCEF (32 bit)		0%	9.0 MB	0 MB/s	0 Mbps	0%	
Adobe RdrCEF (32 bit)		0%	4.4 MB	0 MB/s	0 Mbps	0%	
Application Frame Host		0%	4.1 MB	0 MB/s	0 Mbps	0%	
Bang & Olufsen		0%	4.0 MB	0 MB/s	0 Mbps	0%	

Tracert is used to determine the route used to arrive at a destination. A sample is shown below:

```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\mcmil>tracert nascar.com

Tracing route to nascar.com [52.216.227.210]
over a maximum of 30 hops:

  1    50 ms     1 ms     1 ms  192.168.0.1
  2    18 ms    13 ms    30 ms  075-183-032-001.res.spectrum.com [75.183.32.1]
  3   173 ms    36 ms    31 ms  174.111.102.69
  4    13 ms    13 ms    11 ms  24.28.254.32
  5    15 ms    14 ms    15 ms  be34.drhmncev01r.southeast.rr.com [24.93.64.196]
  6    23 ms    30 ms    29 ms  bu-ether15.asbnva1611w-bcr00.tbone.rr.com [66.109.6.80]
  7    25 ms    30 ms    28 ms  bu-ether12.vinnva0510w-bcr00.tbone.rr.com [66.109.6.31]
  8    27 ms    26 ms    23 ms  0.ae0.pr1.dca20.tbone.rr.com [107.14.17.208]
  9    21 ms    22 ms    25 ms  24.27.236.46
 10    26 ms    26 ms    26 ms  54.239.110.0
 11    23 ms    20 ms    30 ms  54.239.110.27
 12     *        *        *     Request timed out.
 13    27 ms    31 ms    23 ms  72.21.197.243
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17
```

While the operating system can be used to identify potential attacks, it does not identify the role of the server.

The IP address can actually shed little light during server profiling. It cannot help identify the role of the server.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for server profiling (Listening ports; Logged in users/service accounts; Running processes; Running tasks; Applications)

References:

PCWorld > How to Use Task Manager

Question #72 of 84

Question ID: 1323054

Which of the following is NOT one of the three broad categories of cybersecurity investigations?

A) individual
B) private
C) public
D) corporate

Explanation

Corporate is not a term used when describing the three broad categories of cybersecurity investigations. The three categories are:

- Public - investigations resolved in a court of law
- Private - corporate investigations
- Individual - investigations that take the form of eDiscovery

Therefore, all corporate investigation fall into the public category.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe management concepts (Asset management; Configuration management; Mobile device management; Patch management; Vulnerability management)

References:

NIST > Cybersecurity Framework

Question #73 of 84

Question ID: 1323093

Which of the following is another term for an open port?

A) listening port
B) positive port
C) ingress port
D) egress port

Explanation

An open port is also called a “listening” port in some instances. Open or listening ports have an available service running on them. It may or may not be the default service for that port.

An ingress port is one that is accepting data inbound.

Positive is not a word used to discuss ports. .

An egress port is one that is sending data out.

For this exam, you will need to understand the following as it as it relates to network profiling.

Total throughput - the rate of successful message delivery over a communication channel

Session duration - the amount of time that has elapsed between the first packets in the session and the last

Critical asset address space - the IP address range or the individual IP addresses of hosts holding key or critical enterprise information

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for network profiling (Total throughput; Session duration; Ports used; Critical asset address space)

References:

Rackspace > Check listening ports with netstat

Question #74 of 84

Question ID: 1323073

When you are trying to identify communications to Command and Control (CnC) servers, security events are usually correlated with which data?

A) HTTP logs
B) SMTP logs
C) SNMP logs
D) DNS logs

Explanation

As many attacks come through the DNS server, it can be helpful to correlate DNS intelligence with security events. In one example of a DNS attack type that makes use of UDP (but not the only one), a malicious individual queries your DNS server for a record unknown to the DNS server. The server then does what it is designed to do which is forward that query to the domain name listed in the record. In this attack, the listed domain is a malicious domain and the malicious DNS server responds with a record, but within the record is hidden malware that infects the DNS server.

By mapping DNS data to the data found in other intelligence gathering utilities, one can correlate the two and use the DNS data to identify the threat actor.

Many security products maintain a list of known problematic DNS domains. They scan the DNS records (which can be huge in size) for matches and alert you to any communication with a known problem domain.

HTTP logs gather information regarding transactions with the HTTP server, and will be little help in this scenario. On the other hand, if the target was a web server, the data in the HTTP headers could be correlated with data from other security utilities to identify the source of the attack.

SMTP logs contain email events and are not usually helpful in identifying communication to CnC servers.

SNMP logs contain information about the operation of Simple Network Monitoring and are not usually helpful in identifying communication to CnC servers.

Objective:
Security Policies and Procedures

Sub-Objective:
Map elements to these steps of analysis based on the NIST.SP800-61 (Preparation: Detection and analysis; Containment, eradication, and recovery; Post-incident analysis (lessons learned))

References:

HYPERLINK "https://securelist.com/use-of-dns-tunneling-for-cc-communications/78203/" Kapersky > Use of DNS Tunneling for C&C Communications

---

Question #75 of 84

Question ID: 1323130

According to the VERIS schema, when an entrusted user takes malicious actions, it is in what category of threat actions?

A) social

B) hacking

C) malware

D) misuse

Explanation

There are six categories of threat actions. The difference between hacking and misuse is whether or not the individual is abusing privileges and is a trusted user. If the user is a trusted user, that is misuse not hacking. The six categories are:

- Malware -used malicious software
- Hacking - involved outsiders
- Social - involved a social engineering attack
- Misuse - involves trusted users
- Physical - involved a physical breach
- Error - was the result of misconfigurations or human error
- Environmental - includes natural events like tornadoes

Objective:
Security Policies and Procedures

Sub-Objective:
Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

References:

VERIS > The Vocabulary for Event Recording and Incident Sharing

---

Question #76 of 84

Question ID: 1323135

The Cisco's Incident Response Service is an example of which of the following?

A) PSIRT

B) MISSP

C) national CSIRT

D) Coordination centers

Explanation

Managed Security Service Providers (MSSPs) provide incident response and managed security services to its customers. The Cisco's Incident Response Service is an example. Another example is Cisco Active Treat Analysis.

Coordination centers around the world also help CSIRTS coordinate incident handling. They also help coordinate security vulnerability disclosures to vendors, hardware and software providers, and security researchers. One of the best examples is the CERT Division of the Software Engineering Institute (SEI).

Product security incident response teams (PSIRTs) are internal to a vendor, and they handle the investigation, resolution, and disclosure of security vulnerabilities in a vendor's products and services.

National CSIRTS provide incident handling for a country. Examples include the US-CERT.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

References:

HYPERLINK "https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf"NIST > Computer Security Incident Handling Guide (PDF)

Question #77 of 84

Question ID: 1323107

Which of the following is a European agreement that attempts to enhance privacy protections?

A) PCI-DSS

B) PSIRT

C) Wassenaar Agreement

D) GDPR

Explanation

The General Data Protection Regulation (GDPR) is an agreement designed to provide privacy protections in Europe, but the requirements are generally being adopted globally.

The Wassenaar Agreement is an agreement concerning the transfer of dual use goods, that is, those that have a commercial and military use.

The Payment Card Industry Data Security Standard (PCI-DSS) is a standard for protecting credit card information.

Product security incident response teams (PSIRTs) handle the investigation, resolution, and disclosure of security vulnerabilities in their products and services.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify protected data in a network (PII; PSI; PHI; Intellectual property)

References:

TrustArc > Essential Guide to the GDPR

Question #78 of 84

Question ID: 1323092

Which of the following elements used in network profiling can potentially indicate malicious behavior if the value is extremely high?

A) ports used
B) critical address space
C) services in use
D) session duration

Explanation

If the session duration is extremely long, it can indicate malicious activity. This is the amount of time from the setup of the three-way TCP handshake until the session is ended.

A high number of services in use would not necessarily be indicative of malicious behavior, although it could indicate a vulnerability on the target.

A high value for the port in use would not indicate malicious behavior. High port numbers are used as the source for a device seeking access to a well-known port as the destination. The ports in use when profiling identity the potential survives and applications running on the host.

A high value for the critical address space would not be an indicator of malicious activity. The critical address space is the part of an IP network that contains sensitive hosts.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify these elements used for network profiling (Total throughput; Session duration; Ports used; Critical asset address space)

References:

Rackspace > Check listening ports with netstat

Question #79 of 84

Question ID: 1323077

Which stakeholder group is responsible for establishing the incident response process?

A) Information assurance

B) Management

C) IT support

D) Legal

Explanation

Management establishes the incident response policy, budget, and staffing.

Information assurance staff members may be needed during certain stages of incident handling (prevention, containment, eradication, and recovery), but they do not establish the incident response process.

IT support staff (e.g. system and network administrators) have the needed skills to assist, but also usually have the best understanding of the technology they manage daily.

Legal experts should review incident response plans, policies, and procedures to ensure their compliance with legal guidelines.

Objective:
Security Policies and Procedures

Sub-Objective:
Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (Preparation; Detection and analysis; Containment, eradication, and recovery; Post-incident analysis (lessons learned))

References:

NIST > Computer Security Incident Handling Guide (PDF)

Question #80 of 84

Question ID: 1323134

Which of the following help with the dissemination of security vulnerability disclosures to vendors, hardware and software providers, and security researchers?

A) Coordination centers

B) PSIRT

C) MISSP

D) National CSIRT

Explanation

Coordination centers around the world also help CSIRTS coordinate incident handling. They also help coordinate security vulnerability disclosures to vendors, hardware and software providers, and security researchers.

Product security incident response teams (PSIRTs) handle the investigation, resolution, and disclosure of security vulnerabilities in their products and services.

Managed security service providers (MSSPs) provide incident response and managed security services to their customers. Cisco’s Incident Response Service is an example of this type of team.

National CSIRTS provide incident handling for a country.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

References:

Exabeam > The Complete Guide to CSIRT Organization: How to Build an Incident Response Team

---

Question #81 of 84

Question ID: 1323067

In which stage of incident handling is the extent of the incident determined?

A) lessons learned
B) Identification
C) Scoping
D) containment

Explanation

Determining the extent of the incident involves determining how widespread it is and what devices are involved. There are six steps in the incident handling process:

1. Identification – determining whether there is an incident
2. Scoping – determining the extent of the incident and identifying the attackers
3. Containment – halting the spread of the incident and minimizing the impact
4. Remediation – returning the environment to secure state
5. Lesson-based hardening – preventing future incidents
6. Reporting – documenting the incident and reporting it

Objective:
Security Policies and Procedures

Sub-Objective:
Apply the incident handling process (such as NIST.SP800-61) to an event

References:

NIST > SP 800-61 Rev. 2 Computer Security Incident Handling Guide

---

Question #82 of 84

Question ID: 1323064

In incident handling, which of the following is not considered a precursor?

A) a host with a changed configuration
B) the discovery of a malware infection
C) a changed root password
D) a port scan against a host

Explanation

The discovery of a malware infection is not a precursor of a security event. It is an indicator of a security event, meaning it has definitely happened. Precursors are signs that someone MAY be preparing an attack. Precursors include:

- a root password has been changed
- a port scan against a host
- a host with a changed configuration

Objective:
Security Policies and Procedures

Sub-Objective:
Describe the elements in an incident response plan as stated in NIST.SP800-61

References:

NIST > SP 800-61 Rev. 2 Computer Security Incident Handling Guide

---

Question #83 of 84

Question ID: 1323055

Which tool provides the ability to remotely wipe a stolen smart phone?

A) MDM

B) HIPS

C) HIDS

D) network AV

Explanation

Mobile device management (MDM) software is used to control and manage mobile devices that may or may not belong to the enterprise.

A host intrusion prevention system (HIPS) can prevent multiple attack types but can only protect the device on which it is installed. It is not capable of remote wipe.

A host intrusion detection system (HIDS) can detect multiple attack types but can only protect the device on which it is installed. It is not capable of remote wipe.

To protect multiple devices from malware, network antivirus (AV) should be used. These tools can protect an entire network of devices, but are not capable of remote wipe.

Objective:
Security Policies and Procedures

Sub-Objective:
Describe management concepts (Asset management; Configuration management; Mobile device management; Patch management; Vulnerability management)

References:

PC Mag > The Best Mobile Device Management (MDM) Solutions for 2020

Question #84 of 84

Question ID: 1323109

According to the PCI-DSS framework, which data element can only be stored in an unreadable format?

A) expiration date

B) PIN

C) cardholder name

D) primary account number

E) credit card type

Explanation

The primary account number can only be stored in an unreadable format.

The cardholder name, service code, and expiration date can be stored in a readable format.

The PIN, magnetic stripe data, chip data, and security codes (such as CIDs) cannot be stored by the payment processor in any format, whether readable or unreadable.

The credit card type is not a protected data element under PCI DSS.

Elements that are included are:

- Primary account number
- Magnetic stripe data
- Chip data
- Expiration date
- Full name
- The CVV Number ("Card Verification Value")

The PCI-DSS standard specifies requirements for compliance:

- Install and maintain a firewall configuration to protect cardholder data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect stored cardholder data.
- Encrypt transmission of cardholder data across open, public networks.
- Use and regularly update antivirus software.
- Develop and maintain secure systems and applications.
- Restrict access to cardholder data by business need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security.

Objective:
Security Policies and Procedures

Sub-Objective:
Identify protected data in a network (PII; PSI; PHI; Intellectual property)

References:

PCI Document Library