Cisco 200-201

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Version: 1.0

QUESTION NO: 1

Which type of algorithm encrypts data bit by bit?

A.
block

B.
asymmetric

C.
stream

D.
symmetric

Answer: C
Explanation:

Stream ciphers operate bit by rather on a block of data at a time. Stream and block ciphers are the two main types of symmetric algorithms.

Block ciphers process one block of bits, and stream ciphers process one bit at a time. RC5 and RC6 are block ciphers.

Symmetric ciphers are those that use the same key to encrypt as to decrypt. Symmetric ciphers have modes of operation: ECB, CBC, CTM or CTR, and GCM.

Asymmetric cryptography involves the use of different keys to encrypt and decrypt the data. These keys are referred to as private and public keys, respectively. The public encryption key is used to ensure only the intended recipient the cipher text. The public key is shared and used to encrypt information, and the private key is secret and used to decrypt data that was encrypted with the matching public key. ElGamal is an asymmetric public key encryption algorithm based on the Diffie-Hellman key agreement.

Block ciphers operate on a block of data at a time rather than bit by bit.

Objective: Cryptography

Sub-Objective: Compare and contrast symmetric and asymmetric encryption algorithms

Reference: https://www.itprotoday.com/strategy/symmetric-vs-asymmetric-ciphers

QUESTION NO: 2

Which of the following is true of privilege escalation?

A.
vertical movement to a different level

B.
horizontal movement to the same level

C.
obtained without authorization

D.
granted freely

Answer: C

Explanation:

Privilege escalation occurs when someone obtains, without authorization, the rights and privileges of a different user. Privilege escalation usually occurs by logging in to a system using your valid user account and then finding a way to access files that you do not have permissions to access. This often involves invoking a program that can change your permissions, such as Set User ID (SUID), or invoking a program that runs in an administrative context.

There are several methods of dealing with privilege escalation can lead to denial-of-service (DoS) attacks. An example of privilege escalation is gaining access to a file you should not access by changing the permissions of your valid account.

Horizontal escalation is movement to an account on the same level, such as from a regular user another regular user.

Vertical escalation is movement to an account on a different level, such as from a regular user to an administrator.

Privilege escalation is never granted freely. It is an attack.

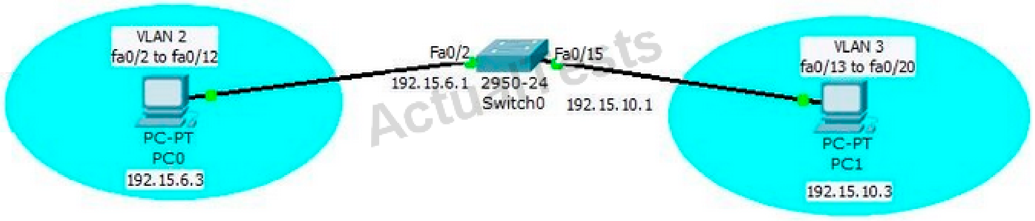
Objective: Attack Methods

Sub-Objective: Define privilege escalation

Reference: https://searchsecurity.techtarget.com/definition/privilege-escalation-attack

QUESTION NO: 3

Examine the diagram below, which contains all devices currently connected to Switch0.



Which of the following statements is true of this scenario?

A.
PC0 can communicate with PC1

B.
is we change the VLAN of Fa0/15 to VLAN 2, PC0 will be able to connect with PC1

C.
if we change the IP address of PC1 to 192.168.6.4, it will be able to connect with PC0

D.
if we change the VLAN of Fa0/2 to VLAN 3 and change the IP address of PC1 to 192.168.6.5, PC1 will be able to connect with PC0

Answer: D
Explanation:

Currently the interfaces to which the two PCs are connected in different VLANs and the PCs have IP addresses in different IP subnets. that is the normal configuration when creating VLANs. The reason they cannot currently connect is because there is NO router in the scenario to route traffic between the VLANs. Therefore, if we place both interfaces in the same VLAN and place both PCs in the same IP subnet, no router will be required to route traffic and the devices can communicate.

PC0 cannot communicate with PC1 in this scenario. Currently the interfaces to which the two PCs are connected in different VLANs, and the PCs have IP addresses in different IP subnets. That is the normal configuration when creating VLANs.

If we change the IP address of PC1 to 192.168.6.4, it will still not be able to connect with PC0 because they will still be in different VLANs. They must be in both the same VLAN and the same IP subnet to communicate in the absence of a router to route between VLANs.

If we change the VLAN of Fa0/15 to VLAN 2, PC0 will till not be to connect with PC1 because they will still be in different IP subnets. They must be in both the same VLAN and the same IP subnet to communicate in the absence of a router to route between VLANs.

Objective: Network Concepts

Sub-Objective: Describe the relationship between VLANs and data visibility

Reference: https://community.spiceworks.com/how_to/55605-how-to-configure-router-on-a-stick

QUESTION NO: 4

Which of the following is deployed on an endpoint as an agent or standalone application?

A.
NIPS

B.
NGFW

C.
HIDS

D.
NIDS

Answer: C
Explanation:

A host-based intrusion detection system (HIDS) monitors individual workstations on a network.

A network intrusion detection system (NIDS) is a system that operated on the network and detects attacks on that network. It monitors real-time traffic over the network, captures the packets, and analyzes them either through a signature database or against the normal traffic pattern behavior to ensure that there are no intrusion attempts or malicious threats. The primary disadvantage of an NIDS is its inability to analyze encrypted information. For example, the packets that traverse through a Virtual Private Network (VPN) tunnel cannot be analyzed by the NIDS. An NIDS would most likely be used to detect, but not react to, behavior on the network.

A network intrusion prevention system (NIPS) is a system that operated on the network and detects attacks on that network while also taking actions to stop the attack. Intrusion prevention system (IPS) and intrusion detection systems (IDS) work together to complement each other. IPS systems can block activities on certain Web sites. Users may be allowed to access the sites but may be prevented from accessing certain features within the site. In other cases, the entire site may be blocked, depending on the security requirements for the organization.

A next generation firewall (NGFW) is one that monitors all layers if the OSI model. It is not deployed on a host.

Objective: Host-Based Analysis

Sub-Objective: Describe the functionality of these endpoint technologies in regards to security monitoring: Host-based intrusion detection, Antimalware and antivirus, Host-based firewall, Application-level whitelisting/blacklisting, Systems-based sandboxing (such as Chrome, Java, Adobe reader).

Reference: https://searchsecurity.techtarget.com/definition/HIDS-NIDS

QUESTION NO: 5

Which of the following represents an exploitable, unpatched, and unmitigated weakness in software?

A.
vulnerability

B.
exploit

C.
threat

D.
breach

Answer: A

Explanation:

A vulnerability is a susceptibility to a threat that exists in a system that has not been mitigated. Patching would be a form of mitigation if it were used to address the vulnerability

When a security weakness or vulnerability exists in a system and threat actor takes advantage, the attack is considered an exploit. An example of a vulnerability is keeping ports open for nonessential services.

A threat is an external danger to which a system may or may not be vulnerable. Is it a potential danger that could take advantage of a system it is vulnerable. An attacker picking the lock of the back entrance to a facility is an example of a threat, not a vulnerability.

A breach is when an exploit is successful in providing unauthorized access to data.

Objective: Security Concepts

Sub-Objective: Compare and contrast these concepts: Risk, Threat, Vulnerability, Exploit

QUESTION NO: 6

Which of the following describes a TCP injection attack?

A.
Many TCP SYN packets are captures with the same sequence number, source, and destination IP address, but different payloads.

B.
there is an abnormally high volume of scanning from numerous sources

C.
many TCP SYN packets are captured with the same sequence number, but different source and destination IP addresses and different payloads

D.
an attacker performs actions slower than normal

Answer: A

Explanation:

A TCP injection attack occurs when the attacker injects data into a TCP packet. Evidence of this attack would be many TCP SYN packets captured with the same sequence number, source and destination IP address but different payloads.

In a resource exhaustion attack, the goal is to overwhelm the IPS or IDS that it cannot keep up. Therefore, it uses an abnormally high volume of scanning from numerous sources. resource exhaustion occurs when a system runs out of limited resources, such as bandwidth, RAM, or hard drive space. Without the required storage space (as an example), the system can no longer perform as expected, and crashes.

Timing attacks are those in which the operations are carried out at a much slower than normal pace to keep the IPS or IDS from assembling the operation in to a recognizable attack.

Capturing many TCP SYN packets captured with the same sequence number, but different source and destination IP address and different payloads, is possible but unlikely. It would not represent a TCP injection attack.

Objective: Attack Methods

Sub-Objective: Describe these evasion methods. Encryption and tunneling, Resource exhaustion, Traffic fragmentation, Protocol-level misinterpretation, traffic substitution and insertion, Pivot.

Reference: http://www.ciscopress.com/articles/article.asp?p=1728833&seqNum=3

QUESTION NO: 7

How are attributes of ownership and control of an object managed in Linux?

A.
permissions

B.
rights

C.
iptables

D.
processes

Answer: A

Explanation:

Just as in Windows, Linux manages ownership and control of an object though the use of permissions. Permissions issues that can be encountered include users being assigned allow permissions that they should not have or being denied access when they need it.

Implementing file auditing will allow you to determine who is accessing files regularly. If a user or group is given access to files and you discover that they are not accessing them, you may want to remove their file permissions. Recertification is the process of examining a user’s permissions and determining if they still need access to what was previously granted.

iptables is a firewall built into Linux. It requires elevated privileges to operate and must be executed by the root user, otherwise it fails to function. On most Linux systems, iptabled is installed as /usr/sbin/iptables.

Rights are network actions granted to a person, such as the right to manage a printer.

A program or service in Linux is called a process, although services are also called daemons. 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.

Objective: Host-Based Analysis

Sub-Objective: Define these terms as they pertain to Linux: Processes, Forks, Permissions, Symlinks, Daemon

Reference: https://www.linux.com/learn/understanding-linux-file-permissions

QUESTION NO: 8

What is the standard for digital certificates?

A.
IEEE 802.3af

B.
IEEE 802.11

C.

X.509

D.
X.500

Answer: C
Explanation:

The standard for digital certificates is X.509. These text documents include identifying information of the holder, the most important being the public key of the holder.

X.500 is the standards for directory services.

Power over Ethernet (PoE) is defined by the IEEE 802.3af and 802.3at standards. PoE allows an Ethernet switch to provide power to an attached device by applying power to the same wires in a UTP cable that are used to transmit and receive data. PoE+ is an enhanced version of PoE that provides more power and better reliability. PoE+ is most commonly deployed in enterprise networks, while PoE is usually sufficient for small business or home networks.

The IEEE 802.11 standard, which is the main standard for wireless LANs (WLANs), specifies using Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) for its media access method. Like an Ethernet network, which uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD), wireless adapter cards “sense”, or listen, for network traffic before transmitting. If the network is free of traffic, the station will send its data. The 802.22 standard also refers to CSMA/CA as Distributed Coordination Function (DCF).

However, unlike an Ethernet network, wireless network cards cannot send and receive transmissions at the same time, which means that they cannot detect a collision. Instead, the sending station will wait for an acknowledgement packet (ACK) to be sent by the destination computer, verifying that the data was received. If, after a random amount of time, an acknowledgement has not been received, the sending station will retransmit the data.

Objective: Cryptography

Sub-Objective: Describe these items in regards to SSL/TLS: Cipher-suite, X.509 certificates, Key exchange, Protocol version, PKCS

Reference: https://searchsecurity.techtarget.com/definition/X509-certificate

QUESTION NO: 9

Which of the following is used to validate and in some cases revoke certificates?

A.
PKI

B.
DHCP

C.
PGP

D.
POP

Answer: A

Explanation:

A public key infrastructure (PKI) contains software hardware and policies that allow digital certificates to be created, validated, or revoked. A digital signature provides integrity, authentication, and non-repudiation in electronic mail. A PKI typically consists of the following components: certificates, a key repository, a method for revoking certificates, and a method to evaluate a certificate chain, which security professionals can use to follow the possession of keys.

Pretty Good Privacy (PGP) is an email encryption system. PGP uses a web of trust to validate public key pairs. In a web of trust model, users sign their own key pairs. If a user wants to receive a file encrypted with PGP, the user must first supply the public key.

Post Office Protocol (POP) is a client email program. It is used to retrieve email from the email server.

Dynamic Host Configuration (DHCP) is a protocol that allows network administrators to centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization’s network. DHCP can automatically assign a new IP address when a computer is plugged into a different location on the network.

Objective: Cryptography

Sub-Objective: Describe the operation of a PKI

Reference: https://searchsecurity.techtarget.com/definition/PKI

QUESTION NO: 10

Which of the following describes a timing attack?

A.
delays attack for an amount of time

B.
waits for an opportune moment

C.
performs actions slower than normal

D.
performs actions faster than normal

Answer: C
Explanation:

Timing attacks are those in which operations carried out are done much slower than normal to keep the IPS or IDS from assembling the operation into a recognizable attack.

Performing actions faster than normal might even make it easier for the IPS or IDS to assemble the parts of the operation into a recognizable attack.

Delaying the attack will have no bearing how easily the IPS may or may not recognize the attack.

Attackers really have no way of recognizing or acting upon an opportune moment.

Objective: Attack Methods

Sub-Objective: Describe these evasion methods: Encryption and tunneling, Resource exhaustion, Traffic fragmentation, Protocol-level misinterpretation, Traffic substitution and insertion, Pivot.

QUESTION NO: 11

Your organization uses both the users location and the time of a day when assessing a connection request.

What type of access control model is this?

A.
RBAC

B.
DAC

C.
ABAC

D.
MAC

Answer: C

Explanation:

This is an example of attribute-based access control (ABAC). In this model, attributes and their combinations are used to control access. There are several classes of attributes that might be included:

Role-based access control (RBAC) provides a specific set of rights and permission based on the job role assigned to the user.

Discretionary access control (DAC) prescribes that the owner of an asset (data) decides the sensitively of the resource and who has access.

Mandatory access control (MAC) creates clearance levels and assigns clearance levels to data assets and to users. Subjects (users) can only access levels to which they have been given clearance and those below.

Objective: Security Concepts

Sub-Objective: Compare and contrast these access control models: Discretionary access control, mandatory access control, Nondiscretionary access control

QUESTION NO: 12

At what layer of the OSI model Internet Protocol (IP) operate?

A.
Layer 3

B.
Layer 1

C.
Layer 2

D.
Layer 4

Answer: A

Explanation:

Both IPv4 and IPv6 operate at the Network Layer 3 of the Open System Interconnection (OSI) model.

The TCP/IP suite of protocols includes Address Resolution Protocol (ARP), Internet Protocol (IP), Internet Control Message (ICMP), Internet Group Management Protocol (IGMP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP).

The TCP/IP suite operates at Layer 2, Layer 3, and Layer 4 of the OSI model follows:

Layer 2, Data Link: ARP

Layer 3, Network: IP, ICMP, IGMP, ARP

Layer 4, Transport: TCP, UDP

The TCP/IP suite operates at layer 2, and layer 3 of the TCP/IP model as follows:

Layer 1, Link: ARP

Layer 2, Internet: IP, ICMP, IGMP, ARP

Layer 3, Transport: TCP, UDP

Objective: Network Concepts

Sub-Objective: Describe the operation of the following: IP, TCP, UDP, ICMP

Reference: http://www.ciscopress.com/articles/article.asp?p=1757634&seqNum=2

QUESTION NO: 13

Which of the following is a compilation of routine procedures and operations that the system administrator or operator carries out?

A.
workflow

B.
script

C.
agenda

D.
runbook

Answer: D
Explanation:

A runbook is a compilation of routine procedures and operations that the system administrator or operator carries out. The runbook is typically divided into routine automated processes and routine manual processes. The effectiveness of a runbook can be measure by these metrics.

Mean time between failures (MTBF) is an estimate of the amount of time a piece of equipment will last and is usually determined by the equipment vendor or third party.

Mean time to repair by the equipment of the amount of time it will take to fix a piece of equipment and return it to production. The owner of the equipment usually determines this amount of time.

An agenda comprises items to be covered in a meeting.

A workflow describes the movement of a piece of work through a process from one operation to another.

While a script may a part of runbook, not all runbook operations are automated. Some are manual.

Objective: Security Concepts

Sun-Objective: Describe these terms. Threat actor, Runbook automation (RBA), Chain of custody (evidentiary), Reverse engineering, Sliding window anomaly detection, PII, PHI.

QUESTION NO: 14

Which of the following occurs at Layer 7 of the OSI model?

A.
VLANs

B.
Packet filtering

C.
Stateful firewall operation

D.
Deep packet inspection

Answer: D
Explanation:

Deep packet inspection is performed by application firewalls, which operate at layer 7 (the Application layer) of the OSI model. This is the examination of the actual data portion of the IP packet. An application firewall is typically integrated into another type of firewall to filter traffic that is traveling at the Application layer of the Open Systems Interconnection (OSI) model. An embedded firewall is typically implemented as a component of a hardware device, such as a switch or a router.

Stateful firewall operation occurs at Layer 3. This type of inspection monitors the TCP three-way handshake which occurs at Layer 3. Stateful firewalls, monitor the state of each TCP connection as well. When traffic is encountered, a stateful firewall first examines a packet to see if it is the result of a previous connection. Information about previous connections is maintained in the state table.

With a stateful firewall, a packet is allowed if it is a response to a previous connection. If the state table holds no information about the packet, the packet is compared to the access control list (ACL). Depending on the ACL, the packet will be forwarded to the appropriate host or dropped completely.

Packer filtering can be done based on IP addresses and port numbers. That means this type of filtering occurs at Layer 3 and 4.

VLANs filter traffic by MAC addresses, and as such operate at Layer 2 of the OSI model.

Objective: Network Concepts

Sub-Objective: Compare and contrast deep packet inspection with packet filtering and stateful firewall operation.

Reference: http://bloggerspath.com/what-is-deep-packet-inspection-and-its-advantages-and-disadvantages/

QUESTION NO: 15

What occurs when you allow specific executable files while denying all others?

A.
whitelisting

B.
blacklisting

C.
greylisting

D.
redlisting

Answer: A

Explanation:

When you whitelisting, you are creating a list of allowed applications while denying all others. Those approved applications are designated as whitelisted. These lists can also be used for domain name allowance with DNS. Several products are available that check for applications that are not on the whitelist, including attempts to install those applications. For example, the logs generated by the whitelisting product would tell you if someone had attempted to install a key logger.

When blacklisting, you create a list of denied applications while allowing all others. These lists can also be used for domain name blocking with DNS. Blacklisting is an allow by default concept, where all software is allowed to execute unless it is on the Deny List.

There is no form of filtering called redlisting or greylisting.

Objective: Security Monitoring

Sub-Objective: Describe these NextGen IPS event types: Connection event, Intrusion event, Host or endpoint event, Network discovery event, NetFlow event.

Reference: https://www.schneier.com/blog/archives/2011/01/whitelisting_vs.html

QUESTION NO: 16

Which operation has as its goal the identification of all available services on a device?

A.
port scan

B.
banner grabbing

C.
OS fingerprinting

D.
ping scan

Answer: A
Explanation:

A port scan identifies the open ports on a device, and thus the services available.

A ping scan has as its goal identification of all live devices in the network. A smurf attack is an attack where a ping request is sent to a broadcast network address with the aim of overwhelming the system.

Operating system (OS) fingerprinting has as its goal the identification of the operating system and version. Banner grabbing is a fingerprinting technique that relies on morphed or empty TCP packets that are sent over to a target machine. Telnet, Netcat, Nmap and other tools can be used to carry out banner grabbing.

Banner grabbing also has as its goal the identification of the operating system and its version. Banner grabbing intercepts a text file sent by a server or a host. The text file includes OS information and in the case of a web server, perhaps the basic configuration info. The attacker can then exploit that information.

Objective: Attack Methods

Sub-Objective: Describe these endpoint-based attacks: Duffer overflows, Command and control (C2), Malware, Rootkit, Port scanning, Host Profiling

Reference: https://www.lifewire.com/introduction-to-port-scanning-2486802

QUESTION NO: 17

Which cross-site scripting attack is sometimes called persistent?

A.
reflected

B.
stored

C.
directed

D.
DOM based

Answer: B

Explanation:

A stored XSS attack is one in which the injected script is stored in the server and received from the server by the user device. Cross-site scripting (XSS) poses the most danger when a user accesses a financial organization’s site using his or her login credentials. The problem is not that the hacker will take over the server. It is more likely that the hacker will take over the client’s session. This will allow the hacker to gain information about the legitimate user that is not publicly available. To prevent XSS, a programmer should validate input to remove hypertext. You can mitigate XSS by preventing the use of HTML tags or JavaScript image tags.

A reflected or non-persistent attack is one that is reflected off the web server and not stored on the server.

Directed is not a term used to describe cross site scripting attacks.

Objective: Attack Methods

Sub-Objective: Describe these web application attacks: SQL injection, Command injections, Cross-site scripting

Reference: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

QUESTION NO: 18

Quantitative and qualitative are two types of which of the following?

A.
risk analysis

B.
business impact analysis

C.
disaster recovery plan

D.
heuristics

Answer: A
Explanation:

Risk analysis come in two basic types. When scoring is used to rate risks rather than dollar figures to potential outcomes.

A business impact analysis (BIA) focuses on critical business systems and the impact if they are lost to an outage. A BIA is created to identify the company's vital functions and prioritize them based on need. It identifies vulnerabilities and threats and calculates the associated risks.

A disaster recovery plan is a short term plan that is implemented when a large disaster event occurs. The plan is created to ensure that your company can resume operations in a timely manner. It mainly focuses on alternative procedures for processing transactions in the short term. it is carries out when the emergency occurs and immediately following the emergency.

Heuristics is an approach that identifies malware based on the behavior it exhibits rather than a signature. A heuristics IDS uses artificial intelligence (AI) to detect intrusions. Analytics are performed on the actions taken, and the IDS takes action based on the logic in the AI.

Objective: Security Concepts

Sub-Objective: Describe these security terms: Principle of least privilege, Risk scoring/risk weighting, Risk reduction, Risk assessment.

Reference: https://www.pmi.org/learning/library/qualitative-risk-assessment-cheaper-faster-3188

QUESTION NO: 19

What is the primary function of routers?

A.
To separate collision domains only

B.
To separate DNS domains

C.
To separate broadcast domains only

D.
To separate collision domains and broadcast domains

Answer: D
Explanation:

Routers create both a broadcast domain for each interface. Routers move traffic from one network to another network, with each interface hosting an IP subnet. A router is a hardware device that transmits data among computers in different networks. Routers use IP addresses to make routing decisions.

A switch is a device that separates collision domains only. Switches make switching decisions based on MAC addresses. A switch is a high-speed networking device that receives incoming data packets from one of its ports and directs them to a destination port for local area network access. A switch will redirect traffic bound outside the local area to a router for forwarding through an appropriate WAN interface.

Neither routers nor switches create only a broadcast domain on each interface. Routers create both a broadcast domain and collision domain for each interface. A switch is a device that separates collision domain only.

DNS servers, not routers, separate DNS domains. A Domain Name Service (DNS) server provides a centralized database of domain name-to-IP address resolutions on a server that other computers on a network can use for name resolution.

Objective: Network Concepts

Sub-Objective: Describe the basic operation of these network device types: Router, Switch, Hub, Bridge, Wireless access point (WAP), Wireless LAN controller (WLC)

Reference: https://ciscoskills.net/2011/03/30/collision-domains-vs-broadcast-domains/

QUESTION NO: 20

OpenDNS is a Cisco security solution designed to protect which component?

A.
LAN

B.
Cloud

C.
WAN

D.
DMZ

Answer: B
Explanation:

OpenDNS is a company and service that hosts a cloud computing security product suite, Umbrella. OpenDNS's business services were renamed as Cisco Umbrella; home products retained the OpenDNS name. It also offers DNS resolution as an alternative to using Internet service providers’ DNS servers or locally installed DNS servers.

Other services offered for cloud protection by Cisco include Cloud lock.

While other products exist for LAN, WAN and DMZ, the Umbrella feature is not one of them.

A local area network (LAN) covers a small geographic area. Typically, a LAN is confined to a campus, a single building, a floor of a building, or an area with in building.

A wide area network (WAN) uses routers (or a collection of routers) to connect LANs that are dispersed over a large geographic area. An example would be a company with office locations in Boston, Miami, Chicago, Dallas, Denver, and San Francisco. Each office has its own LAN, and routers are used to provide connections between the offices. By building the WAN, the offices can share resources and data.

Objective: Network Concepts

Sub-Objective: Describe the functions of these network security systems as deployed on the host, network, or the cloud: Firewall, Cisco Intrusion Prevention System (IPS), Cisco Advanced Malware Protection (AMP), Web Security Appliance (WSA) / Cisco Cloud Web Security (CWS, Email Security Appliance (ESA) / Cisco Cloud Email Security (CES).

Reference: https://www.opendns.com/

QUESTION NO: 21

Which of the following provides non-repudiation?

A.
hashing

B.
redundancy

C.
digital signature

D.
encryption

Answer: C

Explanation:

A digital signature provides non-repudiation, which means the signing cannot be denied at a later time. This is done by hashing the document and then encrypting the hash value with the private key of the sender. The public key of the signer is used to verify a digital signature.

A digital signature provides integrity, authentication, and non-repudiation in electronic mail. Integrity involves providing assurance that a message was not modified during transmission. Authentication is the process of verifying that the sender is who says he is.

Confidentiality means preventing unauthorized access to data. One method of doing that is with encryption. Digital signatures do not provide encryption and cannot ensure availability.

Redundancy, or the use of multiple components, increases availability, the A in CIA. Redundancy ensures that there are multiple ways to control the static environment Redundancy occurs when you have systems in place ready to come when a system fails.

Hashing algorithms generate hash values which can be compared to identify if data has changed. hashing ensures integrity, not non-repudiation. Protecting data from unauthorized change provides integrity. Hashing algorithms include MD2, MD4, MD5, HAVAL, and all of the Secure Hash Algorithm (SHA) variants.

Objective: Cryptography

Sub-Objective: Describe the processes of digital signature creation and verification

References: https://www.assuresign.com/electronic-signatures-vs-digital-signatures/

QUESTION NO: 22

Which of the following is NOT a feature of a next generation firewall?

A.
application visibility and control

B.
stateless firewall

C.
URL filtering

D.
advanced malware protection

Answer: B
Explanation:

Next generation firewalls (NGFW) are stateful firewalls, not stateless firewalls.

Some of the features of the Cisco NGFW are:

With a stateful firewall, a packet is allowed if it is a response to a previous connection. If the table holds no information about the packet, the packet is compared ti the access control list (ACL). Depending on the ACL, the packet will be forwarded to the appropriate host or dropped completely.

Objective: Security Monitoring

Sub-Objective: Describe these types of data used in security monitoring: Full packet capture, Session data, Transaction data, Statistical data, Extracted content, Alert data

References: https://www.cisco.com/c/en/us/products/security/firewalls/index.html

QUESTION NO: 23

A host is sending a ping packet to another host in the same subnet.

For which IP address does the sending host perform an ARP broadcast to resolve?

A.
its own IP address

B.
the IP address of the router

C.
the IP address of the DNS server

D.
the IP address of the destination host

Answer: D
Explanation:

All communication within a subnet is based on MAC addresses. When the destination is in the same subnet, the source device performs an ARP broadcast to learn the MAC address of the destination host.

The Address Resolution Protocol (ARP) is used in TCP/IP to resolve media access control (MAC) addresses to IP addresses. Mac addresses are configured on each NIC on an Ethernet network so that the nodes can be identified on the network. ARP enables the MAC addressing that Ethernet requires to interoperate with the IP addressing that TCP/IP requires. You can use the arp utility to view and manage the ARP cache on a computer. To use the arp utility, you can issue the arp command with various switches at a command prompt. The source device will perform an ARP broadcast to learn the mac address of the router in cases were the destination is in another subnet. Then the router will take over from there.

The source device will never perform an ARP broadcast to learn its own MAC address.

The only time a source device will perform an ARP broadcast to learn the MAC address of the DNS server is when communication is being done by name and not IP address.

Objective: Network Concepts

Sub-Objective: Describe IP subnets and communication within an IP subnet and between IP subnets

Reference: https://www.dummies.com/programming/networking/cisco/network-basics-local-host-arp-requests/

QUESTION NO: 24

At which layer does switching occur in the Cisco modified TCP/IP model?

A.
Internet

B.
Transport

C.
Data Link

D.
Physical

Answer: C

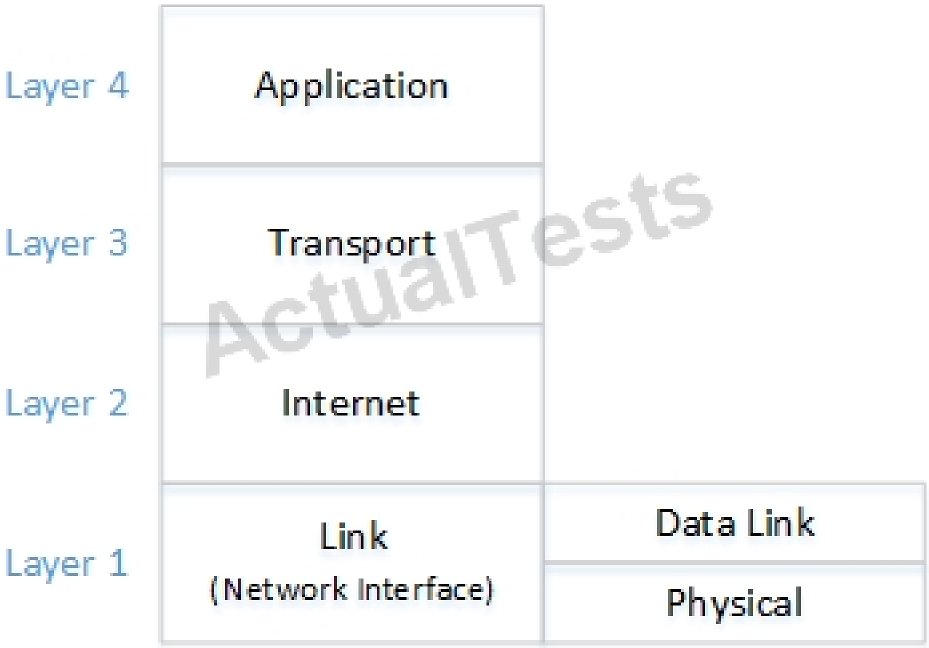
Explanation:

Switches make switching decisions based on MAC addresses. Because MAC address reside in the Data Link layer of the TCP/IP or DoD model, this is the layer where switching occurs. A switch is a high-speed networking device that receives incoming data packets from one of its ports and directs them to a destination port for local area network access. A switch will redirect traffic bound outside the local area to a router for forward through an appropriate WAN interface.

The modified TCP/IP model is a model by Cisco that departs from the DoD model by breaking the bottom layer, the Link layer, into two layers called the Data Link and the Physical layer.

Other versions of the model refer to the Link as the Network Interface layer.

The layers in ascending order are:



Layer 4	Application	
Layer 3	Transport	
Layer 2	Internet	
Layer 1	Link (Network Interface)	Data Link Physical

Switches do not operate on the Internet layer. Routers are an example of devices that operate on this layer, which is where IP addresses are located. A router is a device that examines the contents of data packets transmitted within or across networks. Routers determine if a source and destination are on the same network, or whether data mist be transferred from one network to another, either between locally available network segments, or across a wide-area link to access other, more distant networks.

Switches do not operate on the Transport layer. This is the layer where port numbers are added to the packet.

Switches do not operate on the Physical layer. This is the layer where the information is transmitted as ones and zeros using the underlying technology of the medium.

The Application layer of the TCP/IP model corresponds to the Application, Presentation, and Session layers of the OSI model.

The Transport layer of the TCP/IP model correspond to the Transport layer of the OSI model.

The Internet layer of the TCP/IP model correspond to the Network layer of the OSI model. Internet protocol (IP), address resolution protocol (ARP), and Internet control message protocol (ICMP) operate at the Internet layer.

The Link layer of the TCP/IP model corresponds to the Data Link and Physical layers of the OSI model.

Objective: Network Concepts

Sub-Objective: Describe the function of the network models

Reference: https://converse.org.ua/kak-otliit%27-original%27nye-konversy-ot-poddelki

QUESTION NO: 25

Which of the following is used to prevent malicious software systems?

A.
HIDS

B.
HIPS

C.

network AV

D.
host AV

Answer: C
Explanation:

To protect multiple devices from malware, network antivirus (AV) should be used. These tools can protect an entire network of devices.

A host antivirus (AV) can only protect the device on which it is installed.

A host intrusion prevention system (HIPS) can prevent multiple attack types, but it can only protect the device on which it is installed.

A host intrusion detection system (HIPS) can detect multiple attack types, but it can only detect attacks against the device on which it is installed.

Intrusion prevention systems (IPS) and intrusion detection systems (IDS) work together to complement each other. IPS systems can block activities on certain Web sites. Users may be allowed to access the sites but may be prevented from accessing certain features within the site. In other cases, the entire site may be blocked, depending on the security requirements for the organization.

Objective: Security Concepts

Sub-Objective: Compare and contrast these terms: Network and host antivirus, Agentless and agent-based protections, SIEM and log collection

References: https://www.techrepublic.com/article/pick-an-anti-virus-solution-that-will-grow-with-your-network/

QUESTION NO: 26

What terms represents the leveraging of a security weakness present in a system?

A.

breach

B.
threat

C.
vulnerability

D.
exploit

Answer: D
Explanation:

When a security weakness or vulnerability exists in a system and threat actor takes advantage of it, the attack is considered an exploit.

A vulnerability is a susceptibility to a threat that exists in a system. An example of a vulnerability is keeping ports open for nonessential services.

A threat is an external danger to which a system may or may not be vulnerable. It is a potential danger that could take advantage of a system if it is vulnerable. A hacker is a threat actor. An attacker picking the lock of the back entrance to a facility is an example of a threat, not a vulnerability.

A breach is when an exploit is successful in providing unauthorized access to data.

Objective: Security Concepts

Sub-Objective: Compare and contrast these concepts: Risk, Threat, Vulnerability, Exploit

Reference: https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/

QUESTION NO: 27

Which of the following uses port 443?

A.

DNS

B.
SSH

C.
SSL

D.
Telnet

E.
HTTP

Answer: C
Explanation:

Secure Sockets Layer (SSL) is a security protocol that uses both encryption and authentication to protect data sent in network communications. SSL and HTTPS use port 443.

Port number 22 is reserved for Secure Shell (SSH) remote login.

Telnet uses port 23. Telnet is a terminal emulation protocol. You can use Telnet to establish a remote session with a server and to issue commands on a server. Telnet client software provides you with a text-based interface and a command line from which you can issue commands on a server that supports the Telnet protocol. Telnet works at the Application layer of the OSI model.

HTTP uses port 80. HTTP is used to traverse web pages.

DNS uses port 53. Domain Name System (DNS) is the protocol that will manage the FQDN to IP address mappings.

There are a total of 65,535 ports in the TCP/IP protocol that are vulnerable to attacks. The following are the most commonly used ports and protocols:

Objective: Cryptography

Sub-Objective: Describe the security impact of these commonly used encryption algorithms and secure communications protocols: DES, 3DES, AES, AES256-CTR, RSA, DSA, SSH, SSL/TLS

Reference: http://info.ssl.com/article.aspx?id=10241

QUESTION NO: 28

What is the process of scoring risks by their likelihood and their impact?

A.
quantitative risk analysis

B.
qualitative risk analysis

C.
business impact analysis

D.
disaster recovery

Answer: B
Explanation:

When scoring is used to rate risks by likelihood and impact, it is called qualitative risk analysis. Qualitative risk analysis does not assign monetary values. It is simply a subjective report that is compiled by the risk analysis team that describes the threats, countermeasures, and likelihood an event will occur.

Quantitative risk analysis attempts to attach dollar figures to potential risk outcomes. Quantitative risk analysis attempts to predict the likelihood a threat will occur and assigns a monetary value in the event a loss occurs. The likelihood of risk occurrence is usually based ob subject matter expert opinion and rankings from statistical data.

A business impact analysis (BIA) focuses on critical business systems and the impact if they are lost to an outage. A BIA is created to identify the company’s vital functions and prioritize them based on need. It identifies vulnerabilities and threats and calculates the associated risks.

A disaster recovery plan is a short term plan that is implemented when a large disaster event occurs. The plan is created to ensure that your company can resume operations in a timely manner. It mainly focuses on alternative procedures for processing transactions in the short term. It is carried out when the emergency occurs and immediately following the emergency.

Objective: Security Concepts

Sub-Objective: Describe these security terms: Principle of least privilege, Risk scoring/risk weighting, Risk reduction, Risk assessment

Reference: https://www.pmi.org/learning/library/qualitative-risk-assessment-cheaper-faster-3188

QUESTION NO: 29

Which of the following is not a hashing algorithm?

A.
DES

B.
MD5

C.
SHA-1

D.
SHA-3

Answer: A

Explanation:

Digital encryption standard (DES) is an encryption algorithm, not a hashing algorithm. DES is a private key encryption standard that is used in IPSec to ensure that data packets are confidentially transmitted.

MD5 is a one-way hashing algorithm. One-way hashing inserts a string of variable length into a hashing algorithm and produces a hash value of fixed length. This hash is appended to the end of the message being sent. The receiver recomputes the hash by using the same computational logic. If the recomputed hash value is the same as the generated hash value, the message was not altered during the course of transmission.

Secure Hashing Algorithm 1 (SHA 1) is the first and least secure version of SHA.

Secure Hashing Algorithm 3 (SHA 3) is the first and least secure version of SHA.

Objective: Cryptography

Sub-Objective: Describe the security impact of these commonly used hash algorithms: MD5, SHA-1, SHA-256, SHA-512

Reference: https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard

QUESTION NO: 30

Which of the following is the most widely used public key cipher?

A.
3DES

B.
EI Gamal

C.
RSA

D.
AES

Answer: C
Explanation:

Rivest, Shamir, Adleman (RSA) is the most widely used public key or asymmetric cipher. RSA supports encryption and decryption and secures data with an algorithm that is based on the difficulty of factoring large numbers.

A public key encryption algorithm is sometimes referred to as an asymmetric encryption algorithm. With asymmetric encryption, the public key is shared and used to encrypt information, and the private key is secret and used to decrypt data that was encrypted with the matching public key. Using RSA, messages travelling between two points are encrypted and authenticated. RSA tokens are used to provide a rolling password for one-time use.

Triple DES or 3DES is a symmetric algorithm, which means the key used to encrypt is identical to the key used to decrypt. Triple DES is a later version of Data Encryption Standard (DES) that performs three rounds of encryption. The encryption and decryption process performed by 3ES takes longer due to the higher processing power required.

While EI Gamal is a public key or asymmetric cipher, it is not the most widely used.

AES is a symmetric algorithm that is currently the best encryption algorithm available commercially.

Advanced Encryption Algorithm that is currently the best encryption algorithm available commercially. The Advanced Encryption Standard (AES) uses 128-bit, 192-bit, and 256-bit encryption keys.

Objective: Cryptography

Sub-objective: Describe the security impact of these commonly used encryption algorithms and secure communications protocols: DES, 33DES, AES, AES256-CTR, RSA, DSA, SSH, SSL/TLS.

Reference: https://www.techopedia.com/definition/21852/rsa-encryption

QUESTION NO: 31

Which of the following provides the ability to allow scripting languages to manage Windows computers both locally and remotely?

A.
STP

B.
RMI

C.
EMI

D.
WMI

Answer: D
Explanation:

Windows Management Instrumentation (WMI) consists of a set of extension that allow access to settings and information through the command line, making the scripting of operations possible. The command-line interface to WMI called Windows Management Instrumentation Command-line (WMI).

Electromagnetic interference (EMI) is the inference with data traversing cables by strong electromagnetic energy generated by sources such as machinery. The transformers in fluorescent lighting systems are a common cause of network communications problems. If a network cable that is highly susceptible to EMI, such as unshielded-twisted pair (UTP) cable, is placed near lighting transformers, then the magnetic field produced by the transformers can cause network communications problems. You can replace UTP cable that runs near sources of EMI with shielded cable, such as shielded twisted-pair 9STP) cable or coaxial cable. Fiber-optic cable is immune to EMI.

Radio frequency interference (RFI) occurs near sources of high power radio transmissions. TV stations, radio stations, cellular telephones, and CB radios can be sources of RFI. RFI can cause network communications problems, and intermittent computer problems such as spontaneously rebooting computers and data errors.

Spanning tree protocol (STP) is a loop avoidance protocol used with switches. Switching loops occur when multiple Layer 2 paths to a network cause to flood broadcasts endlessly. This endless broadcast flood is called a “broadcast storm”, and it causes severe network congestion. STP can be used to prevent these problems on a switched or bridged network.

Objective: Host-Based Analysis

Sub-Objective: Define terms as they pertain to Microsoft Windows: Processes, Threads, Memory allocation, Windows Registry, WMI, Handles, Services

Reference: https://docs.microsoft.com/en-us/windows/win32/wmisdk/about-wmi

QUESTION NO: 32

What is the function of ARP?

A.
resolves IP addresses to MAC addresses

B.
resolves host names to IP addresses

C.
resolves MAC addresses to IP addresses

D.
resolves port numbers to IP addresses

Answer: A

Explanation:

Address resolution Protocol (ARP) resolves IP addresses to MAC addresses. It uses a broadcast mechanism to learn the MAC address of a host known only by its address. The media access control (MAC) address uniquely identifies a node on a network segment. ARP tables show the relationship of IP addresses to MAC addresses and are located on most devices.

There is no mechanism for translating port numbers to IP addresses. The IP address and port number combination of a source or destination is called a socket.

Domain Name System (DNS) is the service that translates host names to IP addresses. DNS uses UDP when resolution queries are sent to a server by a client, but its uses TCP for zone transfers between DNS servers. According to RFC 1035, UDP is the recommended method for queries. A DNS server provides a centralized database of domain name-to –IP address resolutions on a server that other computers on a network can use for name resolution.

There is currently no service that resolves MAC addresses to IP addresses.

Objective: Network Concepts

Sub-Objective: Describe the operation of these network services: ARP, DNS, DHCP

Reference: https://www.lifewire.com/address-resolution-protocol-817941

QUESTION NO: 33

Which hashing algorithm is the strongest?

A.
SHA-1

B.
MD5

C.
SHA-256

D.
SHA-512

Answer: D

Explanation:

SHA-512 is a more secure version of SHA-256 and differs only in the number of rounds of computation.

MD5 is the least secure of the listed hashing algorithms. MD5 is a one-way hashing algorithm. One-way hashing inserts a string of variable length into a hashing algorithm and produces a hash value of fixed length. This hash is appended to the end of the message being sent. The receiver recomputes the hash by using the same computational logic. If the recomputed hash value is the same as the generated hash value, the message was not altered during the course of transmission.

SHA-1 is the first version of SHA and is the least secure version of SHA hashing algorithm. The MD5 algorithm produces 128-bit checksums, and SHA produces 160-bit checksums.

The SHA-256 hashing algorithm is part of the SHA-2 family. SHA-256, also referred to as SHA-2, is a newer version of SHA and uses 256-bit checksum.

Objective: Cryptography

Sub-Objective: Describe the security impact of these commonly used hash algorithms: MD5, SHA-1, SHA-256, SHA-512

Reference: https://movable-type.co.uk/scripts/sha256.html

QUESTION NO: 34

Which of the following is NOT an email protocol?

A.
SMTP

B.
IMAP

C.
NTP

D.
POP

Answer: C

Explanation:

Network Time Protocol (NTP) is used to synchronize the clock of computers on the network. Synchronization of time is important in areas such as event logs, billing services, e-commerce, banking and HIPAA Security Rules.

Simple Mail Transport Protocol (SMTP) is an application protocol, so it operates at the top layer of the OSI model. SMTP is the default protocol for sending e-mail in Microsoft operating systems. SMTP provides client and server functions and works with the Internet and UNIX. it is used to send and receive messages.

Post Office Protocol version 3 (POP3) and Internet Mail Access Protocol 4 (IMAP4) are client email programs. They are used to retrieve email from the server. POP3 and IMAP are the most popular protocols for receiving e-mail protocols.

The following is a list of the common ports in use:

Objective: Security Monitoring

Sub-Objective: Describe the function of these protocols in the context of security monitoring: DNS, NTP, SMTP/POP/IMAP, HTTP/HTTPS

Reference: http://www.emailaddressmanager.com/tips/protocol.html

QUESTION NO: 35

Which of the following is Layer 3 attack?

A.
ARP attacks

B.
IP spoofing

C.
VLAN hopping

D.

MAC spoofing

Answer: B

Explanation:

As IP addresses reside on Layer 3 of the OSI model, IP spoofing is considered a Layer 3 attack.

Other types of spoofing attacks apart from IP spoofing are e-mail spoofing and Web spoofing. Do not confuse e-mail spoofing with pharming attacks. While both do involve being redirected to a fake Web site to obtain confidential information, pharming often involves poisoning the DNS cache to ensure the user is redirected to the fake site even if they correctly enter the real site’s URL. E-mail spoofing just involves clicking links in a hoax e-mail. Pharming is considered a more browser-related attack because it is designed to affect browser usage over the long term.

As ARP resolves IP addresses to MAC addresses, and MAC addresses reside on layer2 of the OSI model, ARP attacks are considered a Layer 2 attack.

As MAC addresses reside on layer 2 of the OSI model, MAC spoofing attacks are also considered Layer 2 attacks. MAC addresses are 48-bit addresses in hexadecimal that are permanently attached to the network interface by the manufacturer.

VLANs are Layer 2 concepts, therefore VLAN hopping attacks are considered Layer 2 attacks. Switches are typically deployed to create virtual local area networks (VLNs). The switch isolates the VLAN from the rest of the network to provide better security for the VLAN.

Objective: Attack Methods

Sub-Objective: Describe these attacks: Social engineering, Phishing, Evasion methods

Reference: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-38/104-ip-spoofing.html

QUESTION NO: 36

Which of the following describes a resource exhaustion attack?

A.

receiving an abnormally low volume of scanning from numerous source

B.
performing actions slower than normal

C.
waiting for an opportune moment

D.
receiving an abnormally high volume of scanning from numerous source

Answer: D
Explanation:

In a resource exhaustion attack, the goal is to the IPS or IDS such that it cannot keep up. Therefore, this attack uses an abnormally high volume of scanning from numerous sources. Resource exhaustion occurs when a system runs out of limited resources, such as bandwidth, RAM, or hard drive space. Without the required storage space (as an example), the system can no longer perform as expected, and crashes.

A Distributed Denial of Service (DDoS) is one in which the attacker recruits hundreds or thousands of devices to assist in the attack. The helpers are called zombies and as a group they are called a botnet. A DDoS attack usually involves the hijacking of several computers and routers to use as agents of the attack. Multiple servers and routers involved in the attack often overwhelm the bandwidth of the attack victim. For example, if a server has intermittent connection issues, the logs show repeated connection attempts from the same IP addresses, and the attempts are overloading the server to the point it cannot respond to traffic, then the server is experiencing a DDoS attack.

Timing attacks are those in which the operations carried out are done much slower than normal to keep the IPS or IDS from assembling the operation into a recognizable attack.

Objective: Attack Methods

Sub-Objective: Describe these evasion methods: Encryption and tunneling, Resource exhaustion, Traffic fragmentation, Protocol-level misinterpretation, Traffic substitution and insertion, Pivot.

Reference: http://www.ciscopress.com/articles/article.asp?p=1728833&seqNum=3

QUESTION NO: 37

Which attack requires a botnet?

A.
DDoS

B.
password theft

C.
DoS

D.
man in the middle

Answer: A

Explanation:

A Distributed Denial of Service (DDoS) attack is one in which the attacker recruits hundreds or thousands of devices to assist in the attack. The helpers are called zombies, and as a group they are called a botnet.

A DDoS attack usually involves the hijacking of several computers and routers and routers to use as agents of the attack. Multiple servers and routers overwhelm the bandwidth of the attack victim. For example, if a server has intermittent connection issues, the logs will show repeated connection attempts from the same IP addresses, and the attempts are overloading the server to the point it cannot respond to traffic, then the server is experiencing a DDoS attack.

A man in the middle attack makes use a single attack machine. The intent is to position the attacker between two communicating devices such that they are sending to the attacker rather than sending to one another. Using a packet analyzer to gather packets from a network connection between two computers is a method that can be used to initiate a man in the middle (MITM) attack.

A DoS attack is one that is sourced from a single machine. A denial of service (DoS) attack occurs when attackers overrun a server with requests so that ligitimate users cannot access the server.

Password theft uses a single attack machine as well.

Objective: Attack methods

Sub-Objective: Describe these network attacks: Denial of service, Distributed denial of service, Man-in-the-middle.

Reference: http://www.digitalattackmap.com/understanding-ddos/

QUESTION NO: 38

When the facility has a fence, guards, a locked front door and locked interior doors, it called what?

A.
AUP

B.
separation of duties

C.
defense in depth

D.
piggybacking

Answer: C
Explanation:

A defense in depth strategy prescribes that multiple impediments be presented to a malicious individual. In this case, multiple physical hurdles are presented, but they can also be technical hurdles such as multiple firewalls. Defense in-depth is a multi-layered approach to security that establishes a robust defensive strategy against attackers. This strategy prevents a single attack from being sufficient to breach an environment, forcing attackers to use complex, multi-pronged, daisy-chain attacks that are more likely to fail or be detected during the attempt.

Separation of duties prescribes that any operation susceptible to fraud should be broken into two tasks, with each task given to a different person.

Piggybacking is a social engineering attack in which an unauthorized individual enters a locked door after an authorized individual unlocks the door.

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.

Objective: Security Concepts

Sub-Objective: Describe the principles of the defense in depth strategy

Reference: https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-depth

QUESTION NO: 39

You are reading the output of a Syslog message.

What type of information is contained in the facility section?

A.
message type (UDP or TCP)

B.
process that submitted the message

C.
relationship to other messages

D.
security level

Answer: D
Explanation:

The facility section identifies the process or application that submitted the message.

The relationship to other messages is contained in the priority section.

The security level of the message is contained in the severity section.

The message type is contained in the transport section.

Syslog messages and SNMP traps trigger notification messages that can be sent via email and SMS. A syslog server receives and stores log messages sent from syslog clients. A syslog client sends logging information to a syslog server. A syslog server ensures that a network administrator can review device error information from a central location.

Objective: Host-Based Analysis

Sub-Objective: Interpret these operating system log data to identify an event: Windows security event logs, Unix-based syslog, Apache access logs, IIS access logs

Reference:
http://www.solarwinds.com/documentation/kiwi/help/syslog/index.html?protocol_levels.htm

QUESTION NO: 40

Which of the following is NOT an event category in the Windows Security Log?

A.
Account management

B.
Logoff events

C.
Object access

D.
Directory service access

Answer: B
Explanation:

While there is a category called Logon events (which will also contain logoff vents), there is no Logoff events category. This category records all local logons and logoffs both successful and unsuccessful.

Object access records all attempts to access resources such as files and folders. Account management records all attempts to make changed to user accounts. Directory service access records all attempts to make changes to Active Directory.

Objective: Host-Based Analysis

Sub-Objective: Interpret these operating system log data to identify an event: Windows security event logs, Unix-based syslog, Apache access logs, IIS access logs

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/manage-auditing-and-security-log

QUESTION NO: 41

Which of the following is most likely to be used in a reflected DoS attack?

A.
NTP

B.
STP

C.
ARP

D.
IGMP

Answer: A
Explanation:

Network Time Protocol (NTP) servers are often used in a reflected attack, which if an attack bounced off a third to hit the target. This helps to hide the source of the attack. NTP is used to synchronize the clocks of computers on the network. Time synchronization is important in areas such as event logs, billing services, e-commerce, banking, and HIPAA security rules.

While spanning tree protocol can be used in network attacks on switches, it is not a DoS type attack. STP uses the Spanning Tree Algorithm (STA) to help a switch or bridge by allowing only one active path at a time. STP can prevent network congestion and broadcast storms.

There are two types of STP: spanning tree (802.1d) and rapid spanning tree (802.1w). 802.1d is an older standard that was designed when a minute or more of lost connectively was considered acceptable downtime.

Address resolution protocol (ARP) is also used in attacks, especially man in the middle, but it is not a DoS attack. ARP tables show the relationship of IP address to MAC address. But they cannot be used for DNS and DHCP integration.

Internet Group Messaging Protocol (IGMP) is not typically used in network attacks.

Objective: Attack Methods

Sub-Objective: Describe these network attacks: Denial of service, Distributed denial of service, Man-in-the-middle.

Reference: https://www.imperva.com/learn/application-security/ntp-amplification/?utm_campaign=Incapsula-moved

QUESTION NO: 42

Which of the following represents a single set of sequential machine-code instructions that the processor executes?

A.
forks

B.
processes

C.
threads

D.
handles

Answer: C
Explanation:

A thread represents a single set of sequential machine-code instructions that the processor executes. A thread also may be thought of as a subset of a process, as a process may have multiple threads. Multithreading is when the processor can operate on more than one thread at a time.

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

Handles are logical associations with a shared resource like a file. When a thread opens a file, it establishes a “handle” to the file.

A fork is an operation whereby a process creates a copy of itself. The fork operation creates a separate address space for the child. The child process has an exact copy of all the memory segments of the parent process.

Objective: Host-Based Analysis

Sub-Objective: Define these terms as they pertain to Microsoft Windows: Processes, threads, memory allocation, Windows Registry, WMI, Handles, Services

Reference: https://whatis.techtarget.com/definition/thread

QUESTION NO: 43

Which algorithm is a symmetric cipher?

A.
ECC

B.
EI Gamai

C.
3DES

D.
RSA

Answer: C
Explanation:

Triple DES or 3DES is symmetric algorithm, which means they key used to encrypt is identical to the key used to decrypt. Triple DES is a later version of DES that performs three rounds of encryption. A 3DES takes longer due to the higher processing power required. Data Encryption Standard (DES) is also symmetric.

The other algorithms are all asymmetric. Asymmetric cryptography involves the use of different keys to encrypt and decrypt the data. These keys are referred to as private and public keys, respectively. The public encryption key is used to ensure only the intended recipient can decrypt the cipher text. These algorithms use two keys that do not match, but are mathematically related such that if encryption is performed using one, the other is used for decryption. Asymmetric algorithms include Diffie-Hellman, RSA, EIGamal, Elliptic Curve Cryptosystem (ECC), CAST, and Knapsack.

EIGamal is an asymmetric public key encryption algorithm based on the Diffie-Hellman key agreement. It is used for digital signatures, encryption of data, and key exchange.

Rivest, Shamir, and Adleman (RSA) is used as the worldwide de facto standard for digital signatures. RSA is a public key algorithm that provides both encryption and authentication.

Elliptic Curve Cryptosystem (ECC) serves as an alternative to the RSA algorithm and provides similar functionalities, but ECC has a higher strength per bit than RSA.

Objective: Cryptography

Sub-Objective: Describe the security impact of these commonly used encryption algorithms and secure communications protocols: DES, 3DES, AES, AES256-CTR, RSA, DSA, SSH, SSL/TLS

Reference: https://searchsecurity.techtarget.com/tip/Expert-advice-Encryption-101-Triple-DES-explained

QUESTION NO: 44

Which statement is FALSE with respect to access lists?

A.
every rule is examined before a decision is made

B.
the order of the rules is important

C.
the rule in the list are examined from top to bottom

D.
the first rule match is applied

Answer: A

Explanation:

Every rule is NOT necessarily examined. An access list is a list of rules defined in a specific order. The rules are examined from the top of the list to the bottom. When one of the rules is encountered which matches the traffic type of the packet being examined, the action specified in that rule is taken and no more rules are examined.

The order of the rules is important. For example, examine this set of conceptual rules:

Allow traffic from subnet 192.168.5.0/24

Deny traffic from 192.168.5.5/24

The second rule would never be invoked because the first rule would always match the traffic of 192.168.5.5.

If all of the rules in a set are examined and none match the traffic type, the packet will be disallowed by an implied deny all at the end of each set. To counteract that, most of the time we configure an allow at the end of the set to counteract this implied rule.

Objective: Network Concepts

Sub-Objective: Describe the operation of ACLs applied filters on the interfaces of network devices

Reference: http://www.ciscopress.com/articles/article.asp?p=1697887

QUESTION NO: 45

What type of data is displayed in the following output?

```
Date flow start Duration Proto Scr IP Addr:Port Dst IP Addr: Port Packets Bytes Flows

2010-09-01 00:00:00.459 0.000 UDP 127.0.0.1:24920 -> 192.168.0.1:22126 1 46 1

2010-09-01 00:00:00.363 0.000 UDP 192.168.0.1:22126 > 127.0.0.1:24920 1 80 1
```

A.
firewall log

B.
traffic from a tap

C.
mirrored traffic

D.
NetFlow traffic

Answer: D

Explanation:

The traffic displayed is from a NetFlow capture. NetFlow can collect IP traffic statistics on all interfaces where NetFlow is enabled, and later export those statistics as netFlow records toward at least one NetFlow collector. Each flow is a unidirectional set of communication processes that share the following.

Traffic from a TAP or traffic mirrored to a SPAN port would not be organized in this way. Its output in a capture tool like Wireshark would provide the ability to open the packet and look at its parts.

A network test access points (TAP) is an external monitoring device that mirrors the traffic that passes between two network nodes. A tap (test access point) is a hardware device inserted at a specific point in the network to monitor data.

The SPAN feature, which is sometimes called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer.

A firewall log output would indicate whether traffic was allowed or denied according to the firewall rules, which is not indicated in the output provided.

Objective: Network Concepts

Sub-Objective: Compare and contrast the characteristics of data obtained from taps or traffic mirroring and NetFlow in the analysis of network traffic.

Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

QUESTION NO: 46

Which of the following provides the C in CIA?

A.
redundancy

B.
hashing

C.

encryption

D.
multiple components

Answer: C
Explanation:

CIA stands for Confidentiality, Integrity, and Availability. Confidentiality means preventing unauthorized access to data. One method of doing that is with encryption.

Integrity is a security service that ensures that digital files have not been changed. Digital signatures are an example of an integrity security method. A digital signature provides integrity and non-repudiation. Non-repudiation ensures that the data's origin is known. Availability is a security service that protects hardware and data from loss by ensuring that any needed data is available when necessary. Backups are an example of availability.

Redundancy or the use of multiple components increases availability, the A in CIA. Redundancy ensures that there are multiple components increases multiple ways to control the static environment. Redundancy occurs when you have systems in place ready to come online when a system fails.

Hashing algorithms generate hash values which can be compared to identify if data has changed. Protecting data from unauthorized change provides integrity. Hashing algorithms include MD2, MD4, MD5, HAVAL, and all of the Secure Hash Algorithm (SHA) variants.

Using multiple components is a synonym for redundancy.

Objective: Cryptography

Sub-Objective: Describe the uses of encryption algorithms

Reference: https://www.techopedia.com/definition/25830/cia-triad-of-information-security

QUESTION NO: 47

Which of the following increases when additional functionality is added to an application?

A.
threats

B.
vulnerabilities

C.
risk

D.
attack surface

Answer: B
Explanation:

The attack surface consists of functionalities that a malicious individual might compromise. As you add functionality, you also increase the attack surface. Determining the attack surface will help you identify the different components that can be attacked, and reviewing the architecture one or more new ports to be opened on the firewall, which increases the attack surface of the organization.

A vulnerability is a susceptibility to a threat that exists in a system.

A threat is an external danger. A system may or may not be vulnerable to a specific threat. A threat is a potential danger that could take advantage of a system if it is vulnerable. For example, there might be threat to SQL servers but if you use Oracle, it is not a vulnerability, only a threat. Because threats are external, they are not affected by increasing functionality.

Risk may be increased IF a vulnerability is created but not unless, therefore it is not the best answer. Risk is the likelihood that an external threat leverages an internal vulnerability. We reduce the risk of a breach when we apply controls that mitigate the likelihood or the impact of the threat.

Objective: Attack Methods

Sub-Objective: Compare and contrast an attack surface and vulnerability

Reference: https://www.tripwire.com/state-of-security/featured/understanding-constitutes-attack-surface-2/

QUESTION NO: 48

What is the term for program or service in Linux?

A.
handles

B.
forks

C.
processes

D.
thread

Answer: C
Explanation:

A program or service in Linux is called a process, although services are also called daemons. A process is a single application as seen from the perspective of the processor. Multiprocessing is the operation pf more than one process at a time.

A thread represents a single set of sequential machine-code instructions that the processor executes. A thread also may be thought of as a subset of a process as a process may have multiple threads.

Handles are logical associations with a process creates a copy of itself. The fork operation creates a separate address space for the child. The child process has an exact copy of all the memory segments of the parent process.

Objective: Host-Based Analysis

Sub-Objective: Define these terms as they pertain to Linux: Processes, Forks, Permissions, Daemon

Reference: http://www.basicconfig.com/linux/process

QUESTION NO: 49

Which of the following is the technique used by Java that prevents certain functions when the applet is sent as part of a Web page?

A.
segmentation

B.
process isolation

C.
sandboxing

D.
reference monitor

Answer: C
Explanation:

Sandboxing is a technique used by Java as well as other applications to prevent the operation of the program from interfering with any other programs running.

Sandboxing also refers to developing an application outside of the production environment. Sandboxing can also be useful to test a legacy operation system that may not have security patches. Virtual machines are often used to create the sandbox. Memory allocation issues may be discovered during sandbox testing, but are not directly a part of the sandbox functionality.

Process isolation is a technique used by operating systems to isolate one running process from any other. It is not done in memory but in the processor queue.

Reference monitor is an abstract concept implemented by the security kernel of the operating system. It manages access from untrusted component to those that are part of the trusted computer base.

Segmentation is not a term used to discuss Java activities and operation.

Objective: Host-Based Analysis

Sub-Objective: Describe the functionality of these endpoint technologies in regards to security monitoring: Host-based intrusion detection, Antimalware and antivirus, Host-based firewall, Application-level whitelisting/blacklisting, Systems-based sandboxing (such as Chrome, Java, Adobe reader).

Reference: https://www.webopedia.com/TERM/S/sandbox.html

QUESTION NO: 50

Which of the following would one NOT expect to find in a packet capture of an HTTP packet?

A.
referrer header

B.
SYN flag

C.
user agent

D.
host

Answer: B

Explanation:

SYN flags are seen in TCP packets that are part of the three-way TCP handshake. Once the connection setup is complete, the HTTP packets will not have this element.

Among the elements in an HTTP packets are the following:

Objective: Security Monitoring

Sub-Objective: Describe the function of these protocols in the context of security monitoring: DNS, NTP, SMTP/POP/IMAP, HTTP/HTTPS

QUESTION NO: 51

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

A.
a packet with the SYN and ACK flags set

B.
a packet with an RST flag

C.
no response

D.
a packet with the ACK flag set

Answer: A
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”).

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 YSN 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: Network Concepts

Sub-Objective: Describe the operation of the following: IP, TCP, UDP, ICMP

References: https://www.techopedia.com/definition/10339/three-way-handshake

QUESTION NO: 52

Which of the following is a file that contains a reference to another file or directory in the form of an absolute or relative path?

A.
symlink

B.
handle

C.
thread

D.
fork

Answer: A
Explanation:

A symbolic link in Linux (also symlink or soft link) is a term for any file that contains a reference to another file or directory in the form of an absolute or relative path.

A thread represents a single set of sequential machine-code instructions that the processor executes. A thread also may be thought of as a subset of a process as a process may have multiple threads.

handles are logical associations with a shared resource like a file. When a thread opens a file, it establishes a “handle” to the file.

A fork is an operation whereby a process creates a copy of itself. The fork operation creates a separate address space for the child. The child process has an exact copy of all the memory segments of the parent process.

Objective: Host-Based Analysis

Sub-Objective: Define these terms as they pertain to Linux: Processes, Forks, Permissions, Symlinks, Daemon

Reference: https://kb.iu.edu/d/abbe

QUESTION NO: 53

You have been tasked with protecting user’s medical records.

What type of information are you protecting?

A.
PCI-DSS

B.
PII

C.
PHI

D.
HIPAA

Answer: C
Explanation:

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

Personally identifiable (PII) is any piece of information that can be used to uniquely 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 Concepts

Sub-Objective: Describe these terms: Threat actor, Run Book Automation (RBA), Chain of custody (evidentiary), reverse engineering, Sliding windows anomaly detection, PII, PHI

Reference: https://www.getfilecloud.com/blog/2015/03/what-is-pii-and-phi-why-is-it-important/#.XSRUDf5S-Uk

QUESTION NO: 54

What is DNS poisoning?

A.
the practice of dispending IP addresses and host names with the goal of traffic diversion

B.
the practice of many computers transmitting malformed packets to the DNS server to cause the server to crash

C.
the practice of one computer transmitting malformed packets to the DNS server to cause the server to crash

D.
the practice of continually sending a DNS server synchronization messages with spoofed packets

Answer: A

Explanation:

DNS poisoning is the practice of dispensing IP addresses and host names with the goal of traffic diversion. Properly configured DNS security (DNSSES) on the server can provide message validation, which. in turn, would prevent DNS poisoning.

A SYN flood is the practice of continually sending a DNS server synchronization messages with spoofed packets. A SYN flood can transpire when a high number of half-open connections are established to a single computer.

A DNS denial-of-service (DoS) attack is the practice of one computer transmitting malformed packets to the DNS server to cause the server to crash. A DNS distributed DoS (DDoS) attack is the practice of many computers transmitting malformed packets to the DNS server to cause the server to crash.

Address resolution Protocol (ARP) poisoning is similar to DNS poisoning. In this attack, a malicious actor sends falsified ARP messages over a local area network.

In a domain hijacking attack, the registration of a domain name is changed without the permission of the original registrant.

Objective: Security Monitoring

Sub-Objective: Describe the function of these protocols in the context of security monitoring: DNS, NTP, SMTP/POP/IMAP, HTTP/HTTPS

Reference: https://adventuresinsecurity.com/Papers/DNS_Cache_Poisoning.pdf

QUESTION NO: 55

Which of the following is defined by the NIST in the FIPS 180-4 standard?

A.
SHA-1

B.
MD5

C.
SHA-256

D.
SHA-512

Answer: C
Explanation:

The SHA-256 hashing algorithm is defined in the FIPS 180-4 standard by the NIST. It is part of the SHA-2 family. The purpose of Secure Hash Algorithm (SHA) is to protect message integrity.

SHA-256, also referred to as SHA-2, is a newer version of SHA and uses 256-bit checksums. SHA-256 should be used with a disk image to protect the image's integrity so that image can be retained for forensic purposes.

MD5 is hashing algorithm but it is not defined in the FIPS 180-4 standard by the NIST. MD5 is the least secure of the listed hashing algorithms. MD5 is a one-way hashing algorithm. One-way hashing refers to inserting a string of variable length into a hashing algorithm and producing a hash value of fixed length. This hash is appended to the end of the message being sent. This hash value is recomputed at the receivers end in the same fashion in which it was created by using the same computational logic. If the recomputed hash value is the same as the generated hash value, the message was not altered during the course of transmission.

Secure hash algorithm (SHA)-1 is the first version of SHA, and is the least secure version of SHA hashing algorithm. SHA-1 is a hashing algorithm that creates a message digest, which can be used to determine whether a file has been changed since the message digest was created. An unchanged message should create the same message digest on multiple passes through a hashing algorithm. it is not defined in the FIPS 180-4 standard by the NIST.

SHA-512 is a more secure version of SHA-256 and differs only in the number of rounds of computation. It is not defined in the FIPS 180-4 standard by the NIST.

Objective: Cryptography

Sub-Objective: Describe the uses of a hash algorithm

Reference: https://movable-type.co.uk/scripts/sha256.html

QUESTION NO: 56

You are examining NetFlow records.

What is the state of the connection when you receive a packet with the RST flag set in response to a packet with the SYN flag set?

A.
the port is open

B.
the port is blocked by the firewall

C.
the connection is set up

D.
the port is closed

Answer: D

Explanation:

Receiving a packet with the RST flag in response to a packet with the SYN flag means the port is closed. When a port is closed, the device answers back with a TCP packet with the RST flag set.

If the port were open, the response packet would have 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”).

Were the connection successfully set up, the response packet would have the ACK flag set.

If the port were blocked by the firewall, there would be no response. Firewalls do not send diagnostic or error messages when blocking a transmission.

Objective: Security Monitoring

Sub-Objective: Identify the types of data provided by these technologies: TCP Dump, NetFlow, Next-Gen firewall, Traditional stateful firewall, Application visibility and control, Web content filtering, Email content filtering.

Reference: https://www.lifewire.com/introduction-to-port-scanning-2486802

QUESTION NO: 57

In which access control model does the owner of the resource decide who has access to the resource?

A.
MAC

B.
RBAC

C.
DAC

D.
NDAC

Answer: C
Explanation:

Discretionary access control is used when the data owner configures the appropriate permission for each user.

In the mandatory access control model (MAC), a central assigns a sensitivity label to each document, such as secret, top secret, and so on. Users can access sensitivity levels to which they have been given access. The least privilege principle is most commonly associated with mandatory access control. Under MAC, only an administrator can change the category or classification of a subject or object.

In the non-discretionary access control (NDAC) model, a central body decides which users have access to which documents.

In role-based access control (RBAC), access is based on the job roles to which a user belongs.

Objective: Security Concepts

Sub-Objective: Compare and contrast these access control models: Discretionary access control, mandatory access control, Nondiscretionary access control

Reference: https://pdfs.semanticscholar.org/45a2/775770d870b8675fb1301919224c9bcb7361.pdf

QUESTION NO: 58

Which of the following makes a command injection possible?

A.
unneeded service ports left open

B.
input is accepted without bounds checking

C.
web server that accepts input from the user and passes it to a bash shell

D.
two passwords that hash to the same value

Answer: C
Explanation:

When a web server accepts input and passes it to a bash shell (command line), an attacker might input a command as part of the input that might be accepted and processes by the web server.

Two passwords that hash to the same value is called a hash collision, and can lead to either or both passwords being cracked. A Birthday attack captures hashed passwords from the network and uses brute force to try out different text strings using the same hashing algorithm, hoping to end up with a matching pair of hash values, referred to as a collision.

When input is accepted without bounds checking an integer overflow can occur, which is when a value is entered that is larger than expected leading to the integer overflow, a type of buffer overflow. IT occurs when a mathematic operation attempts to create a numeric value that is too large for the available storage space.

When unneeded service ports are left open, the attack surface of the device is increased. Increasing the attack surface makes more attacks possible, but does not make you more susceptible to command injection.

Other injection attacks include SQL injection, LDAP injection, XML injection, and file injection.

Objective: Attack Methods

Sub-Objective: Describe these web application attacks: SQL injection, Command injection, Cross-site scripting

Reference: https://www.owasp.org/index.php/Command_Injection

QUESTION NO: 59

What is the recommended range of setting for virtual memory allocation in Windows?

A.
4 times the installed RAM

B.
half of the installed RAM

C.
1 to 3 times installed RAM

D.
the same as the installed RAM

Answer: C
Explanation:

While Windows can handle virtual memory allocation automatically and usually does a good job, increasing the allocation can improve performance. The virtual memory allocation should be between 1 and 3 times the size of the RAM.

Virtual memory is space on the hard drive used as memory is maxed out. When memory contention arises, the virtual memory manager moves items out of memory to the hard drive to free up more memory. When that bit of information is found to missing in memory, the VMM goes back to the page file on the hard drive and moves it back into memory. This process of moving items back and forth from real memory to virtual memory is called paging.

Objective: Host-based Analysis

Sub-Objective: Define these terms as they pertain to Microsoft Windows: Processes, Threads, Memory allocation, Windows Registry, WMI, handles, Services

Reference: https://technastic.com/change-virtual-memory-allocation-size-windows-10/

QUESTION NO: 60

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.
MTTF

B.
MTBF

C.
MTTR

D.
FIT

Answer: C
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 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 Monitoring

Sub-Objective: Describe these NextGen IPS event types: Connection event, Intrusion event, Host or endpoint event, Network discovery event, NetFlow event.

Reference: http://www.bb-elec.com/Learning-Center/All-White-Papers/Fiber/MTBF,-MTTR,-MTTF,-FIT-Explanation-of-Terms/MTBF-MTTR-MTTF-FIT-10262012-pdf.pdf

QUESTION NO: 61

Which of the following represents an attack source?

A.
threat actor

B.
attack vector

C.
action on objectives

D.
host file

Answer: A
Explanation:

A threat actor is anyone posing a threat through malicious activity. Some well-known threat actors globally are:

A host file is a file on a Windows machine that can contain manual IP address to name mappings.

The attack vector is not the individual. It is the method used by the threat actor. Attack vectors include:

Action on objectives refers to the goal of the hacker. For example, it might be to deliver a ransomware letter.

Reference: https://www.recordedfuture.com/threat-actor-types/

QUESTION NO: 62

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

A.
organizational mission

B.
organizational approach

C.
siloed approach to communication

D.
strategies and goals

Answer: C
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:

1. Preparation

2. Detection and analysis

3. Containment, eradication, and recovery

4. Post incident analysis

The NIST’s incident response plan elements are:

Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

QUESTION NO: 63

Which of the following Cisco tools makes retrospective analysis possible?

A.
Cisco AMP

B.
Cisco Ironport

C.
Cisco Talos

D.
Cisco ASA

Answer: A
Explanation:

Cisco Advanced Malware Protection (AMP) comes in a Network version and an Endpoint version. It can use threat intelligence to perform retrospective (looking back in time) analysis. This would allow an administrator to do something like determine when malware entered your network, as in many cases it enters long before you discover it.

Cisco Advanced Security Appliance (ASA) is the standard Cisco firewall product and does not do retrospective analysis.

Cisco Ironport comes in a web version and email version, and is designed to protect those types of systems. It does not perform retrospective analysis.

Although Cisco Talos feeds are sometimes used in the process of performing retrospective analysis, it is not the component that does it. Cisco Talos is the threat intelligence sharing system that Cisco uses for all customers of the feature. The Talos team protects data, and infrastructure. Its researchers, data scientists, and engineers collect information about existing and developing threats. They then deliver protection against attacks and malware. Talos underpins the entire Cisco security ecosystem.

Reference: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html

QUESTION NO: 64

What is the first step in establishing an internal CSIRT?

A.
Defining the CSIRT constituency

B.
Developing the process and policies for the CSIRT

C.
Making sure that the proper budget is allocated

D.
Deciding where the CSIRT will reside within the organization’s hierarchy

Answer: A

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

Reference: https://www.thegfce.com/good-practices/documents/publications/2016/04/01/best-practices-for-establishing-a-national-csirt

QUESTION NO: 65

Which section of the IP header defines the entire packet size in bytes, including header and data?

A.
Identification

B.
Total length

C.
IP address

D.
Version

Answer: B
Explanation:

The total length field in the IP header indicates the entire packet size in bytes, including header and data. While this is not the most useful field in intrusion analysis, it is good to know what it describes.

The first header field in an IP packet is the four-bit version field. For Pv4, this is always equal to 4. The source and destination IP address fields contain the source and destination IP addresses. The identification field is primarily used for uniquely identifying the group of fragments of a single IP datagram.

Reference: http://www.ciscopress.com/articles/article.asp?p=348253&seqNum=4

QUESTION NO: 66

In the HTTP header, which of the following header fields indicates the domain name of the server (for virtual hosting) and the TCP port number on which the server is listening?

A.
urgent pointer

B.
referrer

C.
authorization

D.
date

E.
host

Answer: E
Explanation:

The host field indicates the domain name of the server (for virtual hosting) and the TCP port number on which the server is listening.

Other examples of HHTP header fields are:

There is no urgent pointer field in an HTTP header. This field is found in TCP headers. The following lists the fields found in a TCP header:

Reference: https://en.wikipedia.org/wiki/List_of_HTTP_header_fields

QUESTION NO: 67

The IDS alerted you there was an attack when there was none.

What is called?

A.
True negative

B.
False positive

C.
False negative

D.
True positive

Answer: B
Explanation:

A false positive means the IDS mistakenly (False) identified an attack (positive). A true positive means the IDS correctly (True) detected an issue positive). A false negative means the system made a mistake (False) and missed (negative) an issue. A true negative means the IDS correctly (True) did not detect an issue (negative).

Reference: https://www.livescience.com/32767-what-are-false-positives-and-false-negatives.html

QUESTION NO: 68

Which netstat command displays Ethernet statistics?

A.
netstat –a

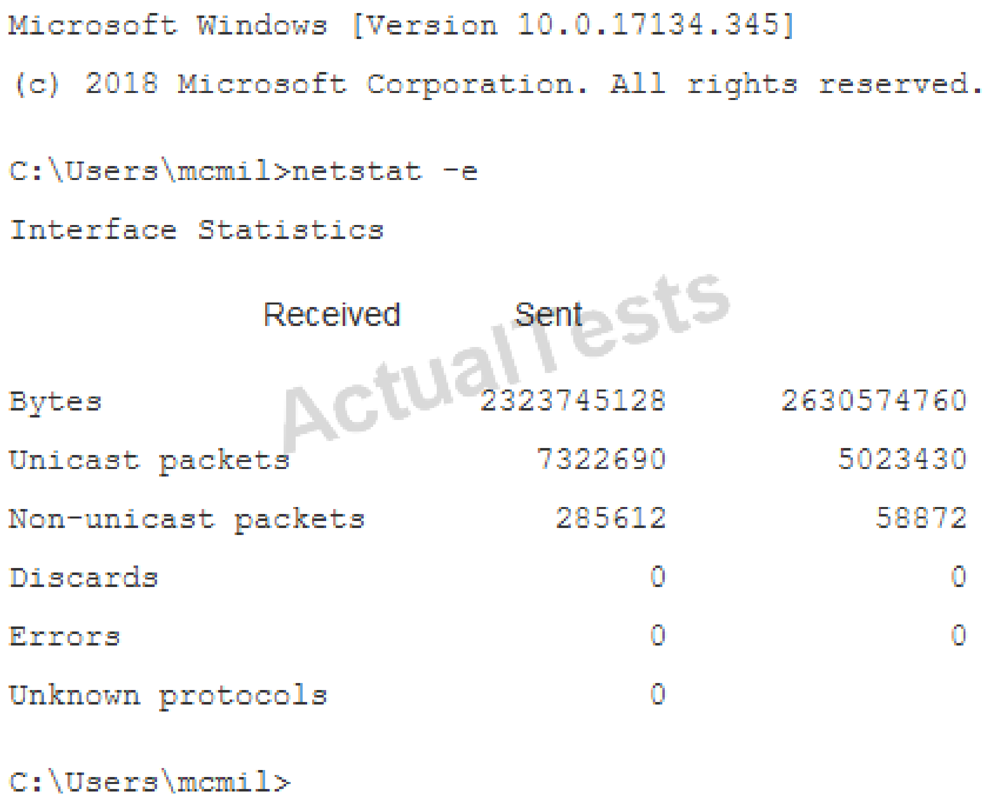
B.
netstat –b

C.
netstat –f

D.
netstat –e

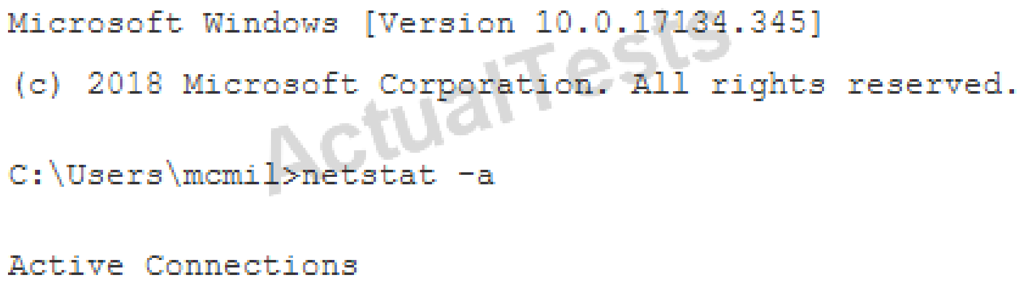
Answer: D
Explanation:

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

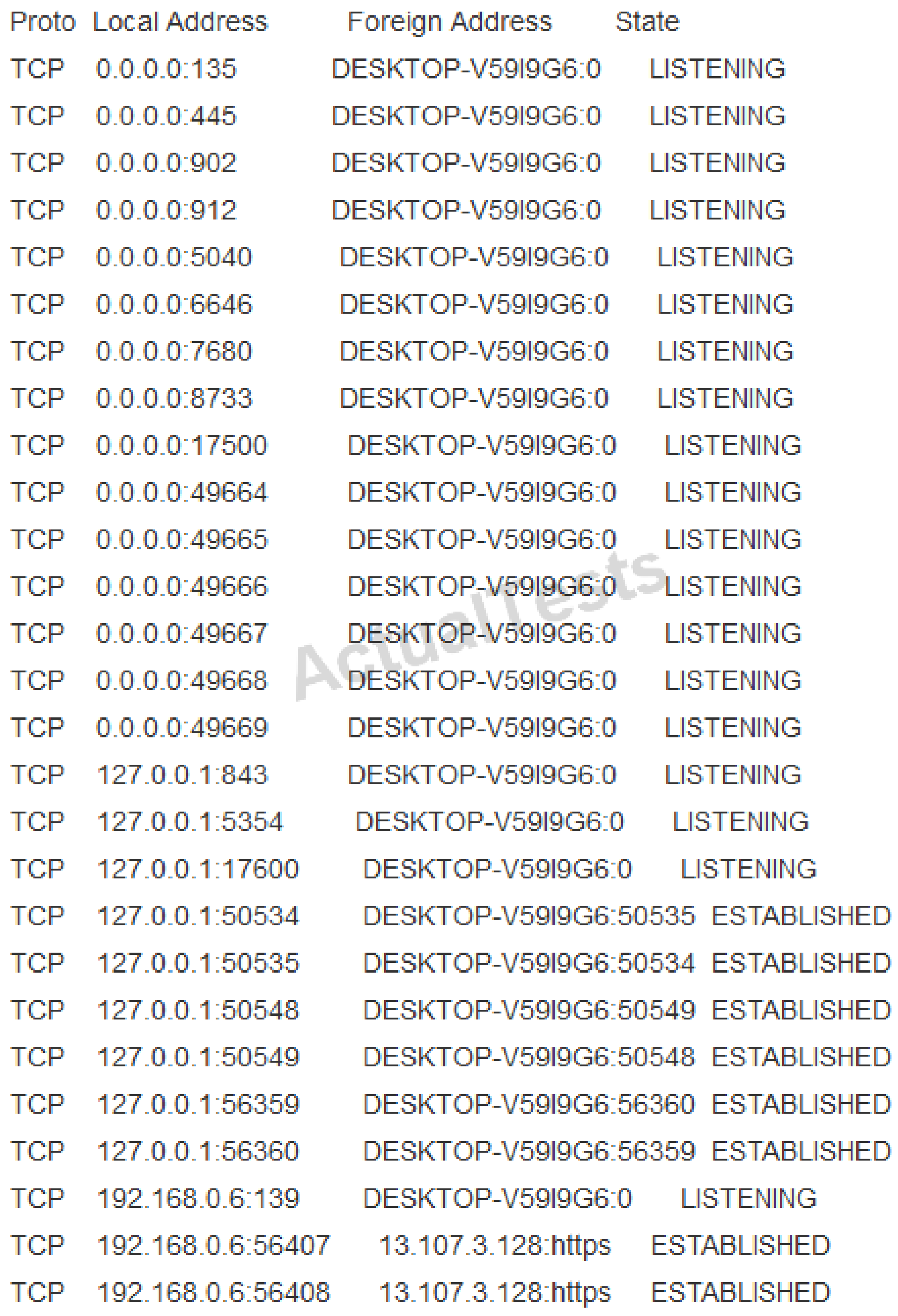


```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

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:

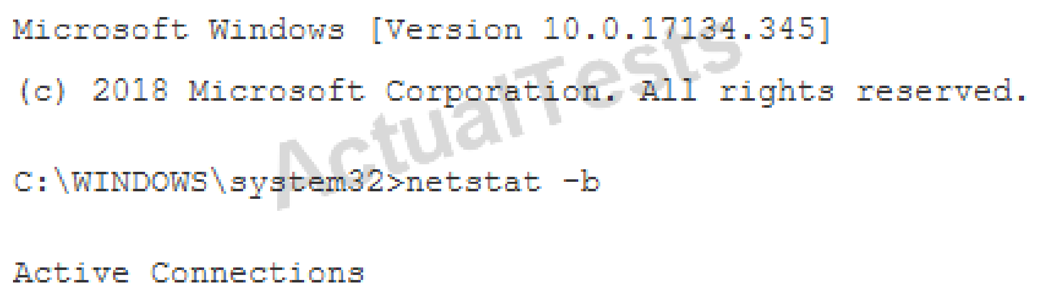


```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\mcmil>netstat -a

Active Connections
```

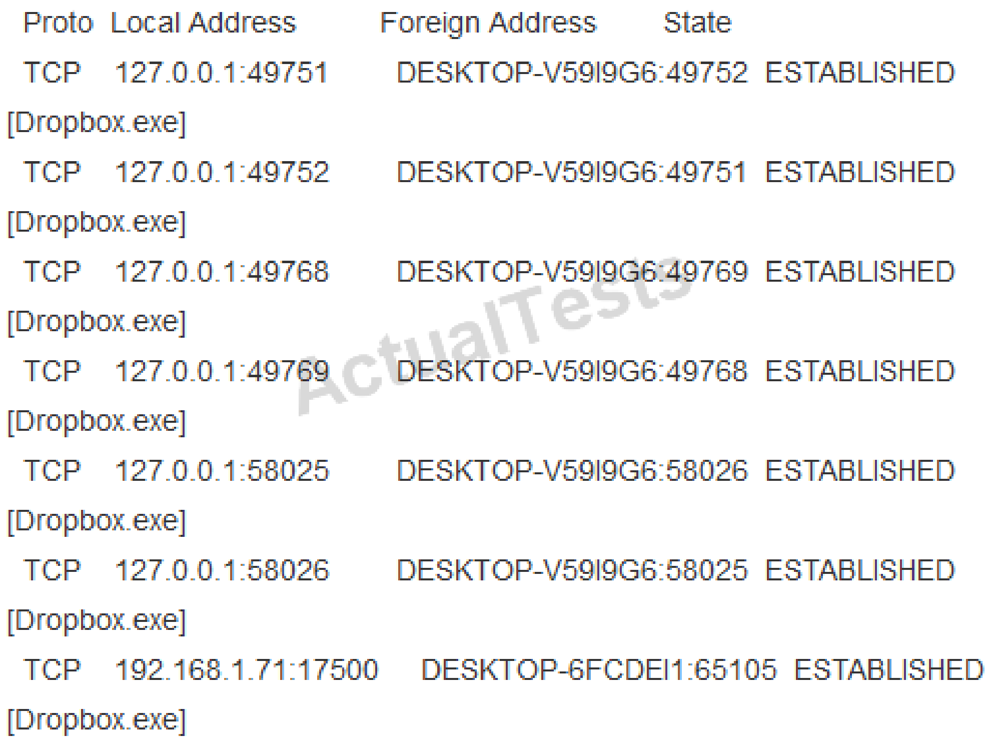


```
Proto  Local Address          Foreign Address        State
TCP    0.0.0.0:135            DESKTOP-V59I9G6:0      LISTENING
TCP    0.0.0.0:445            DESKTOP-V59I9G6:0      LISTENING
TCP    0.0.0.0:902            DESKTOP-V59I9G6:0      LISTENING
TCP    0.0.0.0:912            DESKTOP-V59I9G6:0      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

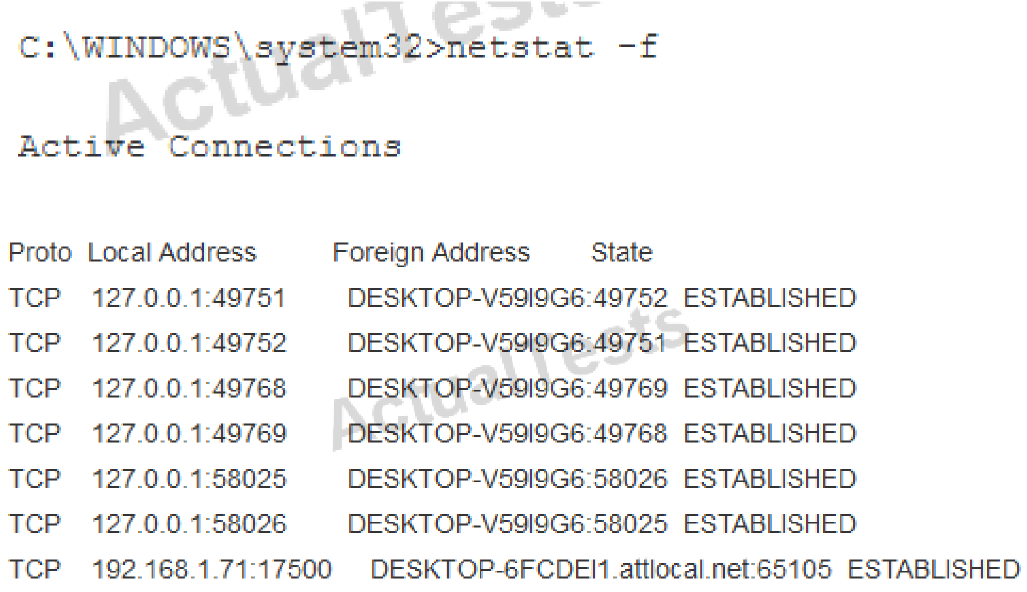


```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

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]
```

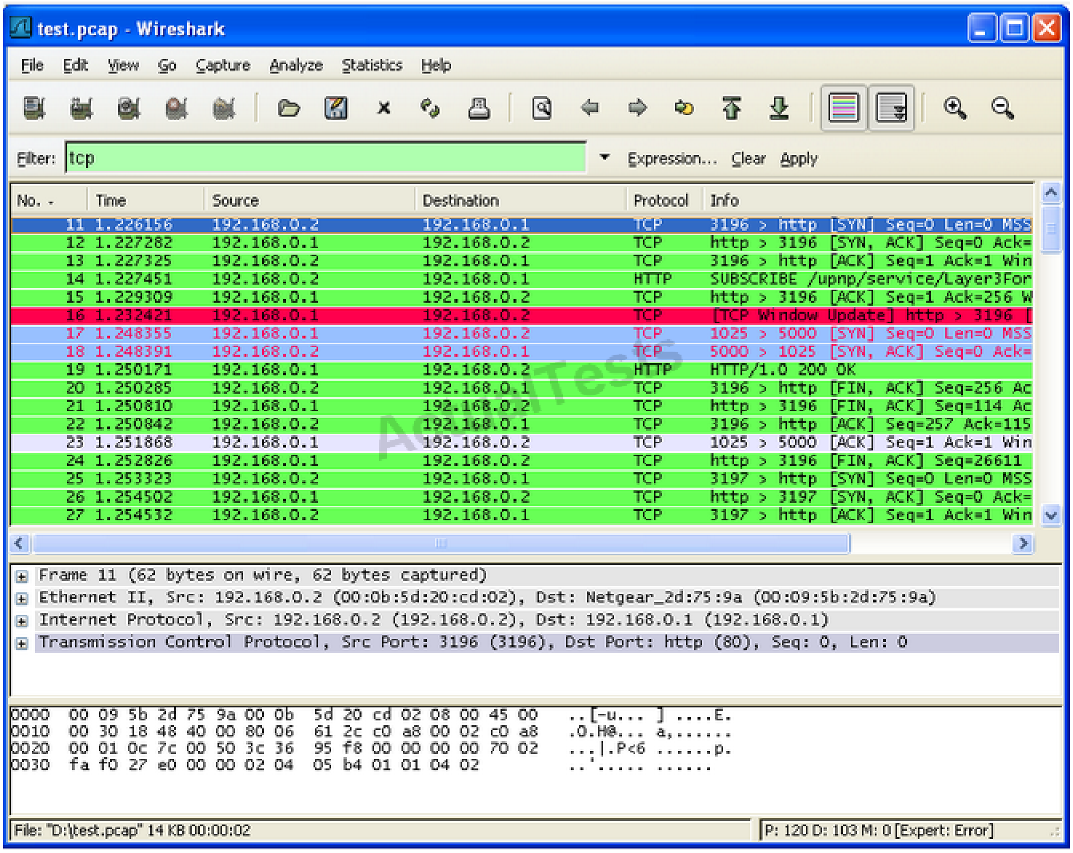
The netstat –f command displays fully qualified domain names for foreign addresses.



```
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
```

QUESTION NO: 69

What application protocol is in use in this capture?


test.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: tcp
Expression... Clear Apply

```
No. -  Time       Source        Destination   Protocol  Info
   11 1.226156   192.168.0.2   192.168.0.1   TCP       3196 > http [SYN] Seq=0 Len=0 MSS
   12 1.227282   192.168.0.1   192.168.0.2   TCP       http > 3196 [SYN, ACK] Seq=0 Ack=
   13 1.227325   192.168.0.2   192.168.0.1   TCP       3196 > http [ACK] Seq=1 Ack=1 Win
   14 1.227451   192.168.0.2   192.168.0.1   HTTP      SUBSCRIBE /upnp/service/Layer3For
   15 1.229309   192.168.0.1   192.168.0.2   TCP       http > 3196 [ACK] Seq=1 Ack=256 W
   16 1.232421   192.168.0.1   192.168.0.2   TCP       [TCP Window Update] http > 3196 [
   17 1.248355   192.168.0.1   192.168.0.2   TCP       1025 > 5000 [SYN] Seq=0 Len=0 MSS
   18 1.248391   192.168.0.2   192.168.0.1   TCP       5000 > 1025 [SYN, ACK] Seq=0 Ack=
   19 1.250171   192.168.0.1   192.168.0.2   HTTP      HTTP/1.0 200 OK
   20 1.250285   192.168.0.2   192.168.0.1   TCP       3196 > http [FIN, ACK] Seq=256 Ac
   21 1.250810   192.168.0.1   192.168.0.2   TCP       http > 3196 [FIN, ACK] Seq=114 Ac
   22 1.250842   192.168.0.2   192.168.0.1   TCP       3196 > http [ACK] Seq=257 Ack=115
   23 1.251868   192.168.0.1   192.168.0.2   TCP       1025 > 5000 [ACK] Seq=1 Ack=1 Win
   24 1.252826   192.168.0.1   192.168.0.2   TCP       http > 3196 [FIN, ACK] Seq=26611
   25 1.253323   192.168.0.2   192.168.0.1   TCP       3197 > http [SYN] Seq=0 Len=0 MSS
   26 1.254502   192.168.0.1   192.168.0.2   TCP       http > 3197 [SYN, ACK] Seq=0 Ack=
   27 1.254532   192.168.0.2   192.168.0.1   TCP       3197 > http [ACK] Seq=1 Ack=1 Win
```

```
⊞ Frame 11 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊞ Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

File: "D:\test.pcap" 14 KB 00:00:02

P: 120 D: 103 M: 0 [Expert: Error]

A.
HTTP

B.
DHCP

C.
SSL

D.
DNS

Answer: A

Explanation:

The application protocol is indicated in the details section as the destination port of 80, which is HTTP.

The application protocol is not DHCP. Were that the case, the destination port numbers in the details section would be 67 and 68.

DNS is not the protocol in use. Were it in use, the destination port number in the details section would be 53.

If SSL were the application protocol, the destination would have been port 443.

You should be familiar with the following common protocols and their ports:

Reference: https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

QUESTION NO: 70

You suspect there is a threat against your DNS server that makes use of the query process.

What type of traffic should you monitor?

A.
UDP

B.
ARP

C.
TCP

D.
HTTP

Answer: A
Explanation:

You should monitor UDP traffic. DNS servers communicate queries using UDP. 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 that 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.

Using DNS server logs, you can identify this type of communication by performing retrospective analysis to determine when the malware file entered the network.

Many security products maintain a list of communication by performing retrospective analysis to determine when the malware file entered the network.

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.

TCP is not used by DNS for queries. Query traffic will fit into a UDP packet. Because UDP is much faster than TCP, it was chosen as the transport protocol for queries. Reliability is provided by DNS at the application layer.

ARP is used to resolve IP addresses to MAC addresses. It is not a protocol used in DNS query communication.

HTTP is a protocol used by web servers and would be of no use in mapping to find a threat actor that involves DNS servers. However, HTTP headers can be used to map HTTP attacks to their source.

HTTP logs and DNS logs can be correlated to one another. The DNS log will show the domain name and IP address and by matching those to the HTTP log we can identify the contents of the HTTP header to identify the attack type.

Reference: https://securelist.com/use-of-dns-tunneling-for-cc-communications/78203/

QUESTION NO: 71

Which statement is FALSE with respect to open ports?

A.
If it is listening, it is open

B.
Ports use values that range between 1 and 65535.

C.
Port 23 is FTP

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

Answer: C

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 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.

Reference: https://support.rackspace.com/how-to/checking-listening-ports-with-netstat/

QUESTION NO: 72

Which of the following CVSS scores measures the extent to which the information resource can be changed due to an attack?

A.
Availability

B.
Confidentiality

C.
Integrity

D.
Attack vector

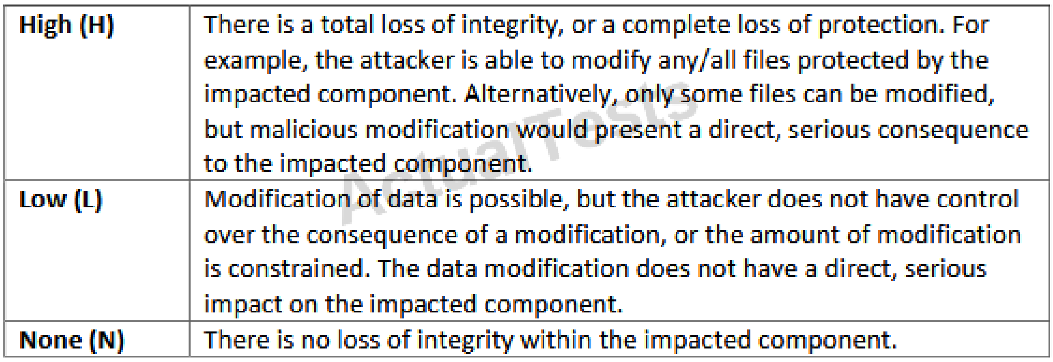
Answer: C
Explanation:

Integrity is the extent to which the information resource can be changed due to an attack.

Confidentiality is the secrecy of an information resource managed by a software component due to an exploited vulnerability.

Availability measures the extent to which availability is at risk due to an attack.

Attack vector describe the nature of the vulnerability. Version 3.0 of CVSS sets the possible values for the confidentiality, integrity, and availability metrics to none, low, and high. These are explained below for integrity:



High (H)	There is a total loss of integrity, or a complete loss of protection. For example, the attacker is able to modify any/all files protected by the impacted component. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.
Low (L)	Modification of data is possible, but the attacker does not have control over the consequence of a modification, or the amount of modification is constrained. The data modification does not have a direct, serious impact on the impacted component.
None (N)	There is no loss of integrity within the impacted component.

Reference: https://www.first.org/cvss/

QUESTION NO: 73

You are assessing application or service availability with a port scan. All services use default ports.

This is an example of what type of exploit analysis?

A.
deterministic

B.
predictive

C.
probabilistic

D.
intuitive

Answer: A

Explanation:

In deterministic analysis, all data used for analysis is known beforehand. An example of this type of analysis is port scanning because we clearly understand the rules of the TCP three-way handshake beforehand and we know the default port numbers.

In probabilistic analysis don’t have all data beforehand and works on probabilities. Predictive analysis is not a term that is used when describing exploit analysis. Intuitive is also not a term used when describing exploit analysis.

Reference: https://www.quora.com/What-is-the-difference-between-probabilistic-and-deterministic-models

QUESTION NO: 74

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 malware data

D.
collect hard drive data first

Answer: A

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

QUESTION NO: 75

Which of the following is NOT one of the five tuples?

A.
source Ip address

B.
source port number

C.
destination IP address

D.
device name

Answer: D
Explanation:

The 5-tuple is a term used to describe the five significant parts of each TCP connection. The five elements which make each conversation unique are:

By using the 5-tuple to uniquely identify each communication, you can map data from various sources that refer to the same communication.

In a TCP connection, the source device creates the connection, the TCP three-way handshake occurs, and the destination accepts the connection. This handshake involves three TCP packets. The first packet has the SYN flag set, indicating a desire to make a connection. The destination answers back with a TCP packet with the SYN and ACK flags set, indicating a willingness to create the connection. Finally, the source finalizes the connection. Finally, the source finalizes the connection with a TCP packet with only the ACK flag set.

Device name is not one of the five tuples.

Reference: https://blog.packet-foo.com/2015/03/tcp-analysis-and-the-five-tuple/

QUESTION NO: 76

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

A.
hibernation file

B.
slack space

C.
network configuration

D.
network connections

Answer: A
Explanation:

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

Reference: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

QUESTION NO: 77

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

A.
System and network administrators

B.
CEO

C.

CISO

D.
CSIRT team

Answer: A
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.

QUESTION NO: 78

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

A.
MSSP

B.
PSIRT

C.
Coordination centers

D.
National CSIRT

Answer: A
Explanation:

Managed Security Service Providers (MSSPs) provide incident response and managed security services to their customers. The Cisco 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).

QUESTION NO: 79

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

A.
exploitation

B.
command and control

C.
action on objectives

D.
installation

Answer: C
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 server.

The seven steps in the kill chain are:

QUESTION NO: 80

Which of the following is the latest Linux file system?

A.
ext3

B.
ext2

C.
ext4

D.
ext5

Answer: C
Explanation:

Ext4 is the latest Linux file system. One of the improvements over ext3 is support for unlimited subdirectories. Ext4 modifies important data structures of the filesystem, such as the ones destined to store the file data. The result is a filesystem with an improved design, better performance, reliability, and features. Other improvements are:

Ext2 was the first commercial-grade file system for Linux. It is no longer in use. The ext2 filesystem does not support journaling, which would help in recovery after a crash. Ext3 is the second version of the file system. The journaling feature in filesystems helps in recovery after a crash. The ext3 filesystem provides journaling capability.

There is no Ext5.

Reference: https://www.ibm.com/developerworks/library/l-lpic1-v3-104-1/

QUESTION NO: 81

Which of the following activities would be a part of retrospective analysis?

A.
scanning for vulnerabilities with NESSUS

B.
using historical data to identify an infected host

C.
using nmap to determine open ports

D.
attempting to exploit a vulnerability you found

Answer: B
Explanation:

Whenever you use historical data from logs to help identify a breach of any sort, you are engaged in retrospective analysis. A retrospective analysis is permed when the outcome of an event is already known, such as attempting to discover when identified malware first entered your system. GigaStor Security Forensics is another example of a tool that performs retrospective analysis.

Using nmap to determine open ports is a part of network discovery stage of a penetration test. by identifying the open ports, potential attacks may be identified before they occur.

Scanning for vulnerabilities with NESSUS is a part of a vulnerability test. Attempting to exploit a vulnerability is a later stage in the penetration test.

QUESTION NO: 82

What is the term for an operation that purges redundant data while maintaining data integrity?

A.
modularization

B.
aggregation

C.
warehousing

D.
normalization

Answer: D
Explanation:

Normalization is the process of eliminating redundancy and protecting integrity of the data. When data normalization is utilized with IPS systems, the IPS manages multiple incoming streams of data and ensures that all data exists only in one form. This eliminates redundant data. Normalization is the part of the security analysis process that reduces the sheer amount of data and makes the process cleaner and more efficient.

Modularization is the breaking of a process into modules. A great example is the OSI model, which breaks the communication process down into seven modules or layers.

Aggregation is the process of taking data from multiple sources, such as IPS, firewall and router, and combining into a single integrated log file. A Security Information and Event (SIEM) system collects data from the different security devices in the system, such as firewalls and IPSs, and then aggregates the log files for analysis.

Data warehousing is the combination of data from multiple data sources or databases into a single repository for analysis and manipulation.

References: https://www.helpnetsecurity.com/2013/01/07/the-importance-of-data-normalization-in-ips/

https://support.microsoft.com/en-us/help/283878/description-of-the-database-normalization-basics

QUESTION NO: 83

Which statement is FALSE with respect to listening ports?

A.
Port 443, when set to default, is encrypted.

B.
Ports can be numbered 1 to 65535.

C.
The port number does not always identify the service.

D.
They are closed.

Answer: D

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 as their defaults are:

Port 443 is SSL over HTTP, which is encrypted.

QUESTION NO: 84

Which evidence is always considered the best evidence?

A.
hearsay

B.
indirect

C.
direct

D.
corroborative

Answer: C
Explanation:

Direct evidence is always considered the best because it does not require any reasoning or inference to arrive at the conclusion to be drawn from the evidence. An eyewitness account is direct evidence.

Hearsay is never admissible in court. This is when someone testifies they heard someone else say something they witnessed (also called second hand). Corroborative evidence is that which supports other evidence. For example, is someone testifies they saw it raining and another said they heard rain, that is considered corroborative evidence. Indirect evidence suggests but does not prove anything. For example, if a man is accused of gambling and has been seen with gamblers, that is indirect evidence.

Reference: https://legal-dictionary.thefreedictionary.com/direct+evidence

QUESTION NO: 85

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

A.
Coordination centers

B.
MISSP

C.
PSIRT

D.
national CSIRT

Answer: B
Explanation:

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

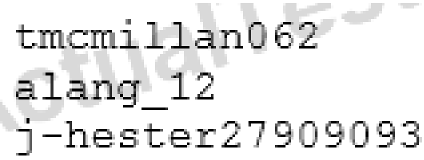
Coordination centers around the world also help with the coordination of security vulnerability disclosures to vendors, hardware and software providers, and security researchers. One of the best examples is the CERT Division of the Software Engineering Institute (SEI).

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.

Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

QUESTION NO: 86

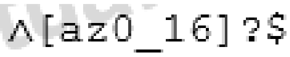
You have been asked to collect all the usernames from an access log. According to policy, usernames must be at least six characters and no more than sixteen characters. Usernames can only include lowercase letters, numbers, underscores, and hyphens, such as the following:



```
tmcmillan062
alang_12
j-hester27909093
```

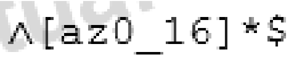
Which regular expression will locate all valid usernames?

A.



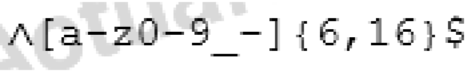
```
^[az0_16]?$
```

B.



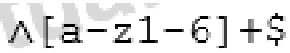
```
^[az0_16]*$
```

C.



```
^[a-z0-9_-]{6,16}$
```

D.



```
^[a-z1-6]+$
```

Answer: C

Explanation:

The regular expression [a-z0-9_-]{6,16}$ will locate all valid usernames. The and $ indicate the beginning and end of the pattern, respectively. The characters inside of the square brackets [] specify what is allowable, being a lowercase letter (a-z), number (0-9), underscore (_), or hyphen (-). The values in the curly braces {} specifies the minimum number of occurrences, being at least six, but no more than sixteen characters.

The regular expression [az0_16]?$ only finds usernames with a single characters a, z, 0, 1, _, or 6. Also, the question mark (?) will match these characters zero or one time, returning empty matches.

The regular expression [a-z1-6]+$ will locate only usernames that contain one or more lowercase letters or the digits 1 through 6. The plus sign (+) will match one or more occurrence.

The regular expression [az0_16]*$ will locate only usernames that contain the characters 1, z, 0, _, 1 or 6. Also, the asterisk (*) will match zero or more occurrences, returning empty matches.

QUESTION NO: 87

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.
Reconnaissance

B.
Exploitation

C.
Installation

D.
Weaponization

Answer: C

Explanation:

It is the installation step. Installation comes after exploitation and involves the installation 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.

QUESTION NO: 88

Which of the following represents the software that is acting on behalf of a user?

A.
representative agent field

B.
cookie

C.
type field

D.
host field

E.
user agent

Answer: E
Explanation:

The user agent is an HTTP header inside the software that is acting on behalf of a user. For example, it might indicate the browser type and capability. The User-Agent (UA) string is intended to identify devices requesting online content, which helps with intrusion analysis.

The host field indicates the domain name of the server (for virtual hosting), and the TCP port number on which the server is listening.

Other examples of HTTP header fields are:

Cookies are text files with information with stored information about the user. They are not HTTP header fields. There is no representative agent field in the HTTP header. There is no type field in the HTTP header. The type field is the first field in an Internet Control Message Protocol (ICMP) header, and is used to indicate the function or purpose of the communication. A control message is the function or purpose of the ICMP communication.

Common examples of Types are:

There are about sixteen formally defined Types for ICMP. The remaining fields in the ICMP header are Code, Checksum, and Rest of Header. The Code field is used to define or reference a sub-type (i.e., a more specific sub-meaning of the indicated control message). The Checksum field is used to verify that the ICMP communication was not corrupted in transit. The Rest of Header field may hold values when needed based on the Type, or is set to all zeros when unused. For example, a Type 5 Redirect will place an IP address in the Rest of Header field.

Reference: https://en.wikipedia.org/wiki/List_of_HTTP_header_fields

QUESTION NO: 89

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

A.
volatility

B.
time involved

C.
likely value

D.
effort required

Answer: B

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):

Reference: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

QUESTION NO: 90

Which statement is true with regard to evidence collection?

A.
Allow full access to the crime scene.

B.
Always shut the computer down first.

C.
Always call police.

D.
Always protect the integrity of the evidence.

Answer: D

Explanation:

You should always protect the confidentiality and the integrity of all evidence collected and ensure that a proper chain of custody is maintained. You should never shut the computer down until all volatile (memory) evidence is collected. You should tightly control access to the crime scene. You should always consider calling the police carefully as they will take control of the investigation.

In summary, guidelines for evidence collection are:

Reference: https://www.journals.elsevier.com/digital-investigation/

QUESTION NO: 91

Which of the following is NOT reconnaissance?

A.
scanning without completing the three way handshake

B.
installation of a RAT

C.
searching for the robots.txt file

D.
communicating over social media

Answer: B
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.

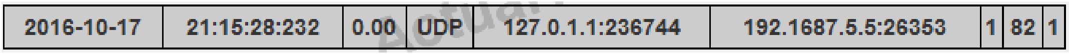
The first and most important step is reconnaissance when information is gathered that helps penetrate the network. For example, consider an exploit takes advantage of an injection vulnerability in an exploitable Hypertext Preprocessor php file by sending an HTTP POST with specific variables. If the hacker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

QUESTION NO: 92

Examine the following NetFlow entry:



2016-10-17	21:15:28:232	0.00	UDP	127.0.1.1:236744	192.1687.5.5:26353	1	82	1

Which statement is FALSE?

A.
The destination port is 236744.

B.
The bytes are 82.

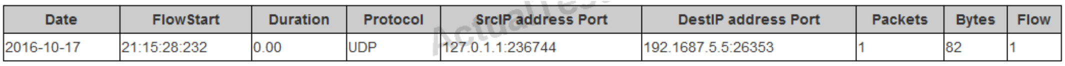
C.
This is a single packet.

D.
The protocol is UDP

Answer: A

Explanation:

The destination port is 236353, not 236744. The number of bytes is 82. This entry represents a single packet. The entry with the missing column heading are as follows:



Date	FlowStart	Duration	Protocol	SrcIP address Port	DestIP address Port	Packets	Bytes	Flow
2016-10-17	21:15:28:232	0.00	UDP	127.0.1.1:236744	192.1687.5.5:26353	1	82	1

Reference: https://www.flowmon.com/en/solutions/use-case/netflow-ipfix?msclkid=7aa92f29a1561b55d6e7749d573ad74c&utm_source=bing&utm_medium=cpc&utm_campaign=2017%20BING%20SEA%20Netflow-IPFIX%20[p%2Be]&utm_term=netflow&utm_content=Netflow

QUESTION NO: 93

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

A.
lessons learned

B.
containment

C.
scoping

D.
identification

Answer: C
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:

Reference: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

QUESTION NO: 94

Which of the following is NOT one of the 5 tuples?

A.
source port number

B.
source Ip address

C.
destination IP address

D.
netflow record ID

Answer: D
Explanation:

The Netflow ID appears in the NetFlow header when using NetFlow to capture what is called a flow. This compromises all packets that are part of the same conversation as defined by the 5-tuple that all packets share. However, the NetFlow ID is not one of the five tuples.

By using the 5-tuple uniquely identify each communication you can match up data from various sources that refer to the same communication.

The 5 tuple is a term to describe the 5 significant parts of each TCP connection. These 5 elements which make each conversation unique are:

The source device created the connection and the destination accepts the connection following the TCP three way handshake. this handshake involves three TCP packets. The forst packet has the SYN flag set, indicating a desire to make a connection. The destination answers back with TCP packet with the SYN and ACK flags set, indicating a willingness to create the connection. Finally, the source finalizes the connection with a TCP packet with only the ACK flag set.

Reference: https://blog.packet-foo.com/2015/03/tcp-analysis-and-the-five-tuple/

QUESTION NO: 95

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

A.
integrity

B.
availability

C.
confidentiality

D.
authentication

Answer: A
Explanation:

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

QUESTION NO: 96

You are investigating suspicious communication between two devices in your environment. The source socket is 205.16.3.74:5696 and the destination socket is 192.168.5.3:53.

What service should you suspect is under attack?

A.
DHCP

B.
NTP

C.
DNS

D.
HTTP

Answer: C

Explanation:

You should suspect a DNS attack, mist likely an at attempt at an unauthored zone transfer. The destination port is port 53. Unless there is a non-default service running on that port, that port is used for DNS.

You should not suspect DHCP. By default, DHCP uses ports 67 and 68, not 53.

You should not suspect HTTP. By default, HTTP uses port 80.

You should not suspect NTP. By default, NTP uses port 123.

Reference: https://whatis.techtarget.com/definition/sockets

QUESTION NO: 97

You have discovered a vulnerability to your web service that if leveraged would cause data to be changed in the attack.

Which CVSS metric will increase if this attack is realized?

A.
complexity

B.
confidentiality

C.
Availability

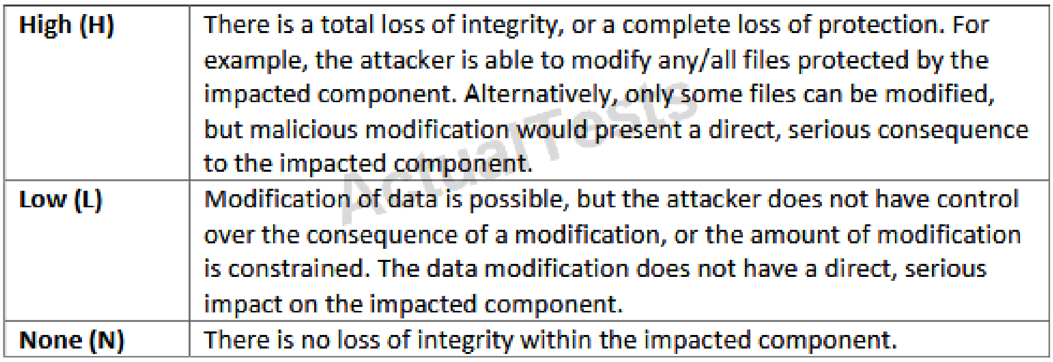
D.
integrity

Answer: D
Explanation:

The integrity metric increases when data is changed in the attack.

When a service is rendered unable to do its job as in this case, its availability has been decreased resulting in an increase in the availability metric. The confidentiality metric increases when there is a data disclosure or breach.

Attack vector describe the nature of the vulnerability. The new version of CVSS (3.0) set the possible values for the confidentiality, integrity and availability metrics to none, low, and high. These are explained below for integrity:



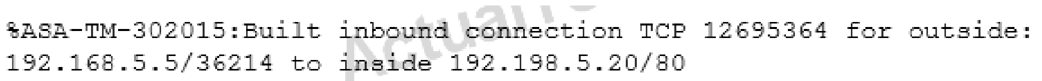
High (H)	There is a total loss of integrity, or a complete loss of protection. For example, the attacker is able to modify any/all files protected by the impacted component. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.
Low (L)	Modification of data is possible, but the attacker does not have control over the consequence of a modification, or the amount of modification is constrained. The data modification does not have a direct, serious impact on the impacted component.
None (N)	There is no loss of integrity within the impacted component.

The complexity metric is a measure of the difficulty of succeeding in the attack. Low and high are values for attack complexity, which has replaced access complexity in version 3.0, and measures the difficulty of the attack. It has two possible values:

Reference: https://www.first.org/cvss/

QUESTION NO: 98

Examine the following ASA system message:



```
%ASA-TM-302015:Built inbound connection TCP 12695364 for outside:
192.168.5.5/36214 to inside 192.198.5.20/80
```

Which statement is FALSE?

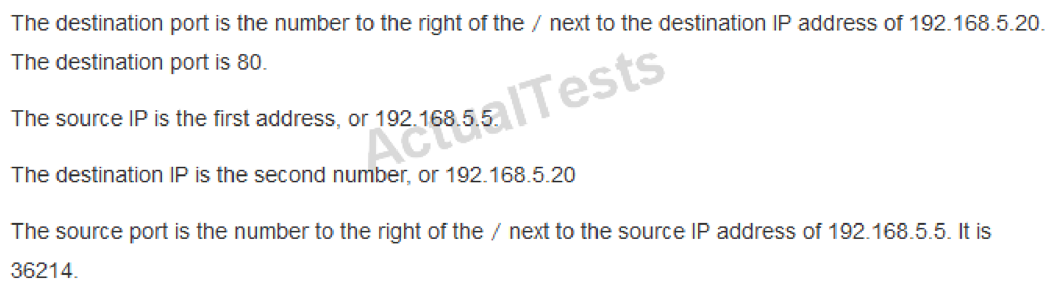
A.
The destination port is 302015.

B.
The destination IP is 192.168.5.20

C.
The source IP is 192.168.5.5

D.
The source port is 36214.

Answer: A
Explanation:



The destination port is the number to the right of the / next to the destination IP address of 192.168.5.20. The destination port is 80.

The source IP is the first address, or 192.168.5.5.

The destination IP is the second number, or 192.168.5.20

The source port is the number to the right of the / next to the source IP address of 192.168.5.5. It is 36214.

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/syslog/b_syslog.html

QUESTION NO: 99

What statement is FALSE about probabilistic analysis?

A.
The answer is not definitive.

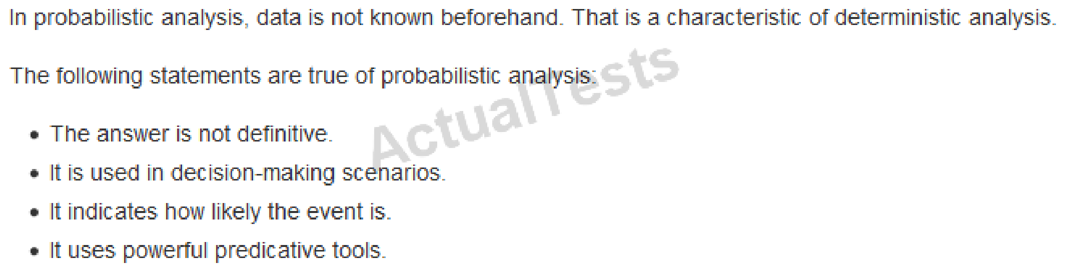
B.
All data is known beforehand.

C.
It is used in decision-making scenarios.

D.
It indicates how likely the event is.

Answer: B

Explanation:



In probabilistic analysis, data is not known beforehand. That is a characteristic of deterministic analysis.

The following statements are true of probabilistic analysis:

- The answer is not definitive.
- It is used in decision-making scenarios.
- It indicates how likely the event is.
- It uses powerful predicative tools.

QUESTION NO: 100

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

A.
nbtstat

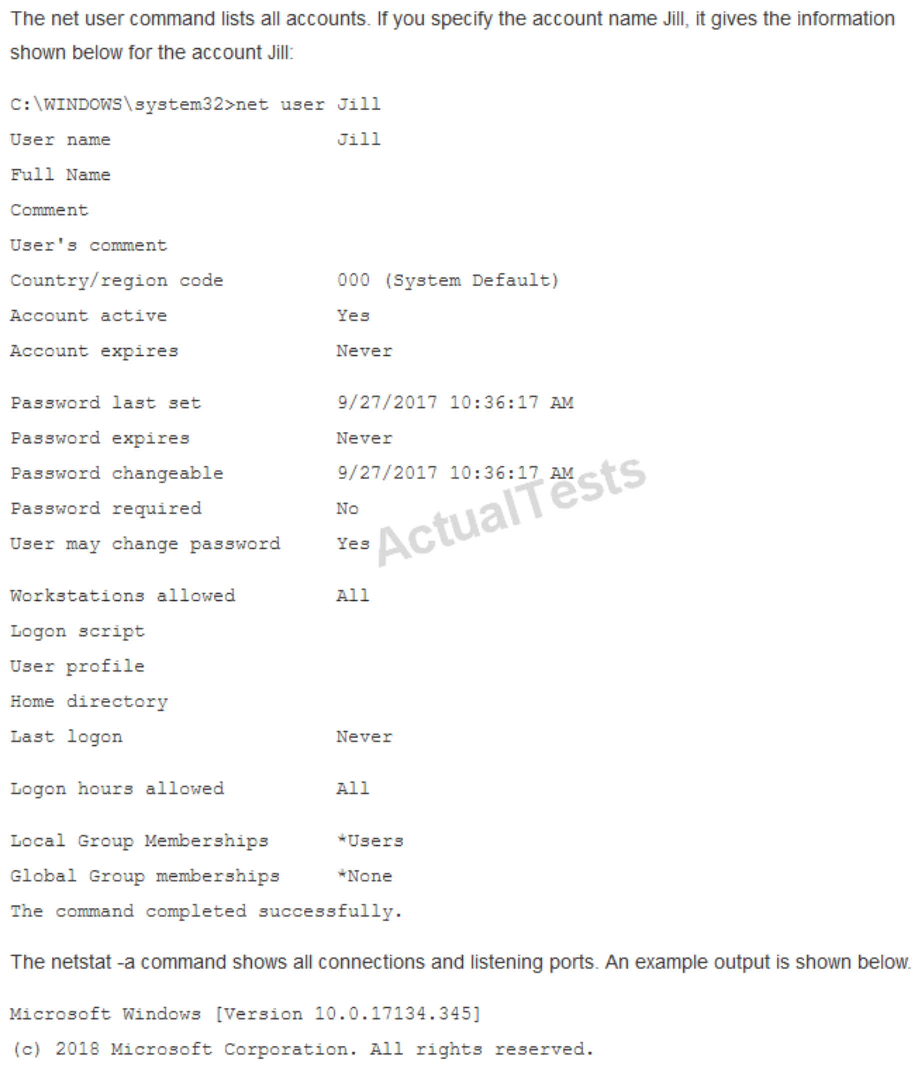
B.
Task Manager

C.
netstat –a

D.
net user

Answer: D

Explanation:

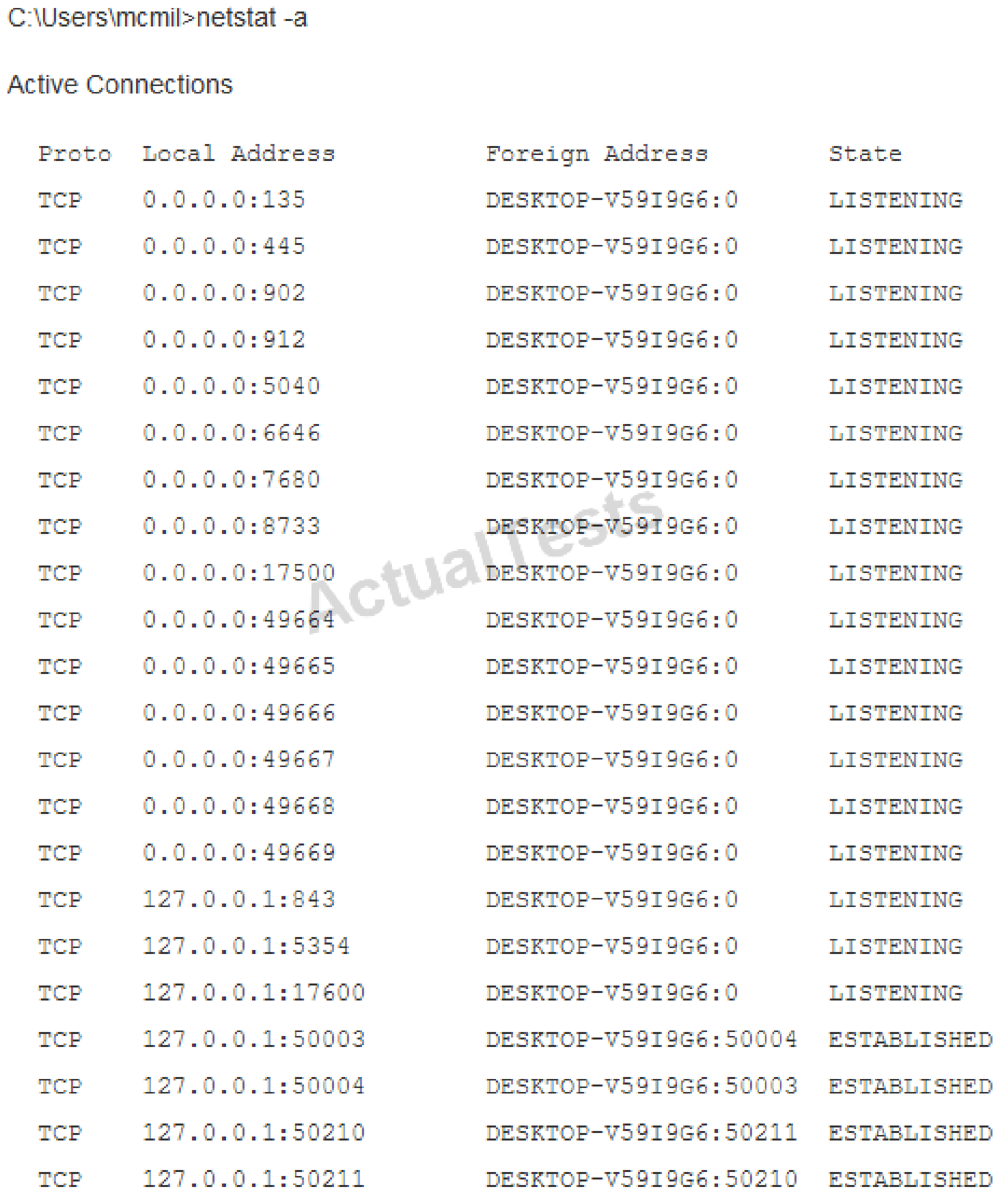


The net user command lists all accounts. If you specify the account name Jill, it gives the information shown below for the account Jill:

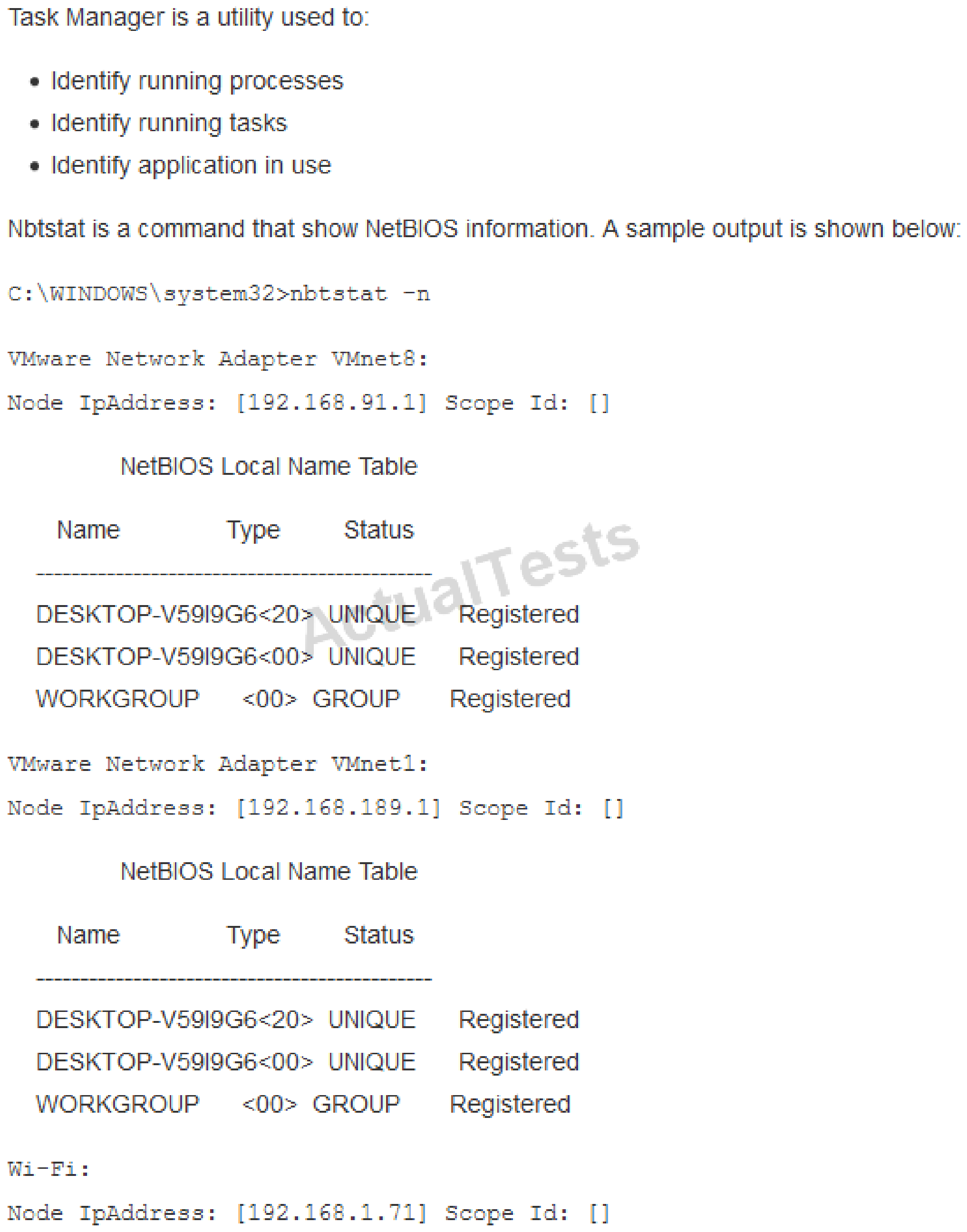
```
C:\WINDOWS\system32>net user Jill
User name                    Jill
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

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
```

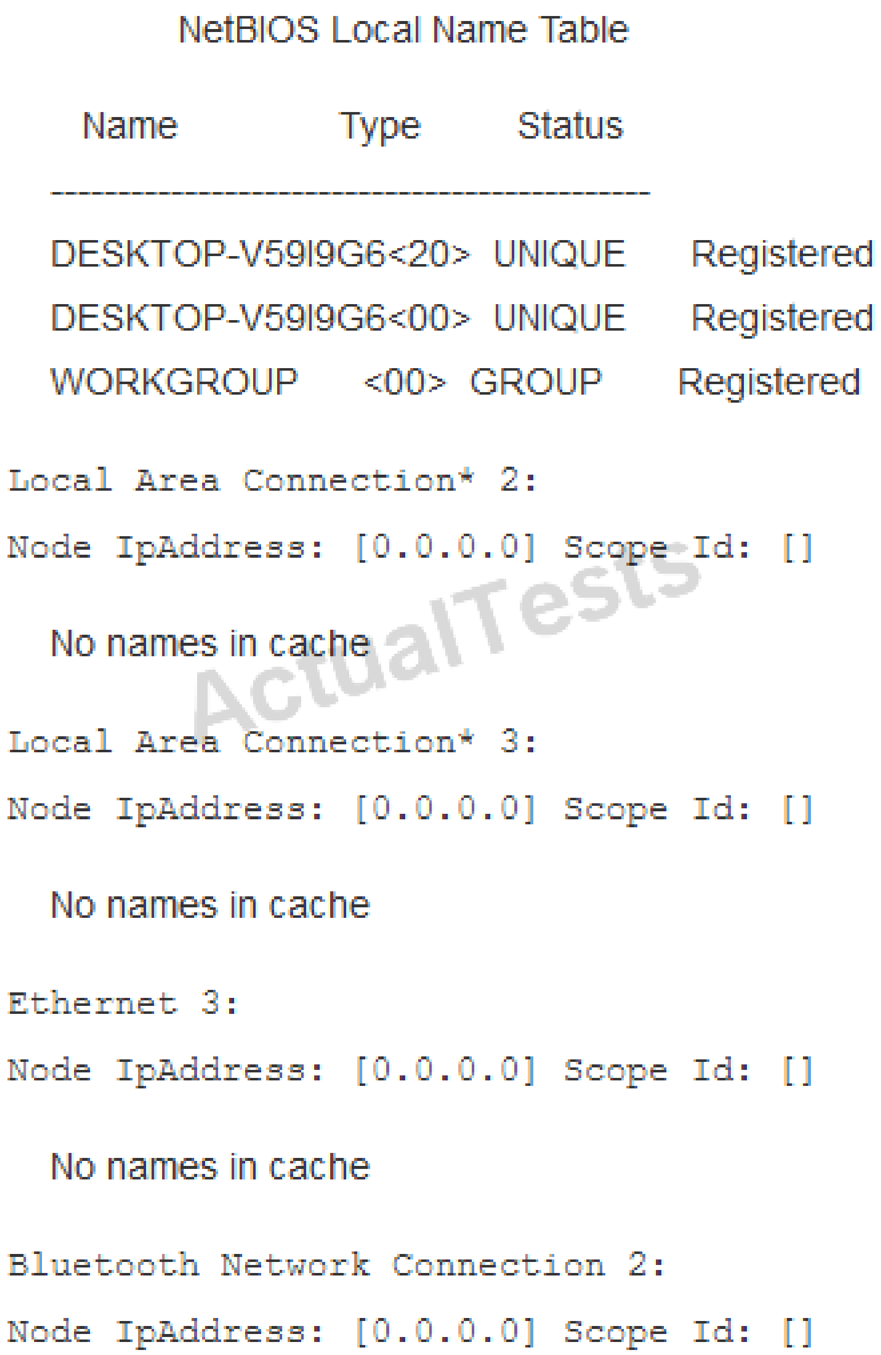


Task Manager is a utility used to:

- 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: []
```

Reference: https://www.lifewire.com/net-user-command-2618097

QUESTION NO: 101

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

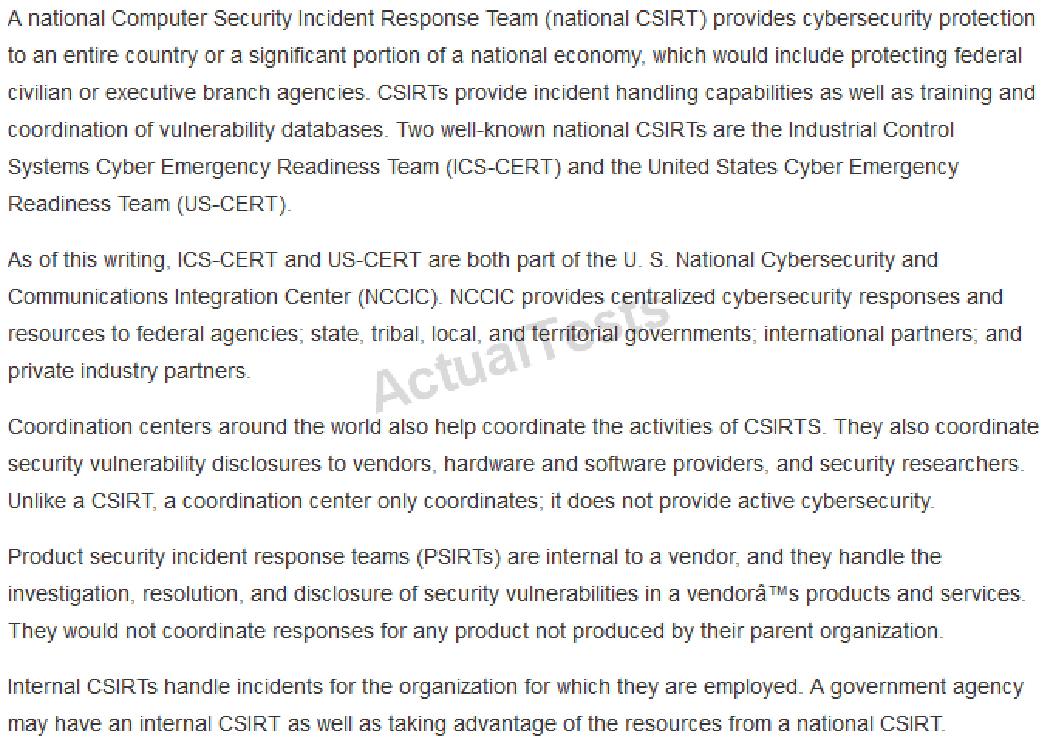
A.
National CSIRT

B.
Coordination center

C.
Internal CSIRT

D.
PSIRT

Answer: A
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 vendorâ™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.

Reference:

https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/national-csirts/

https://www.us-cert.gov/about-us

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

QUESTION NO: 102

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

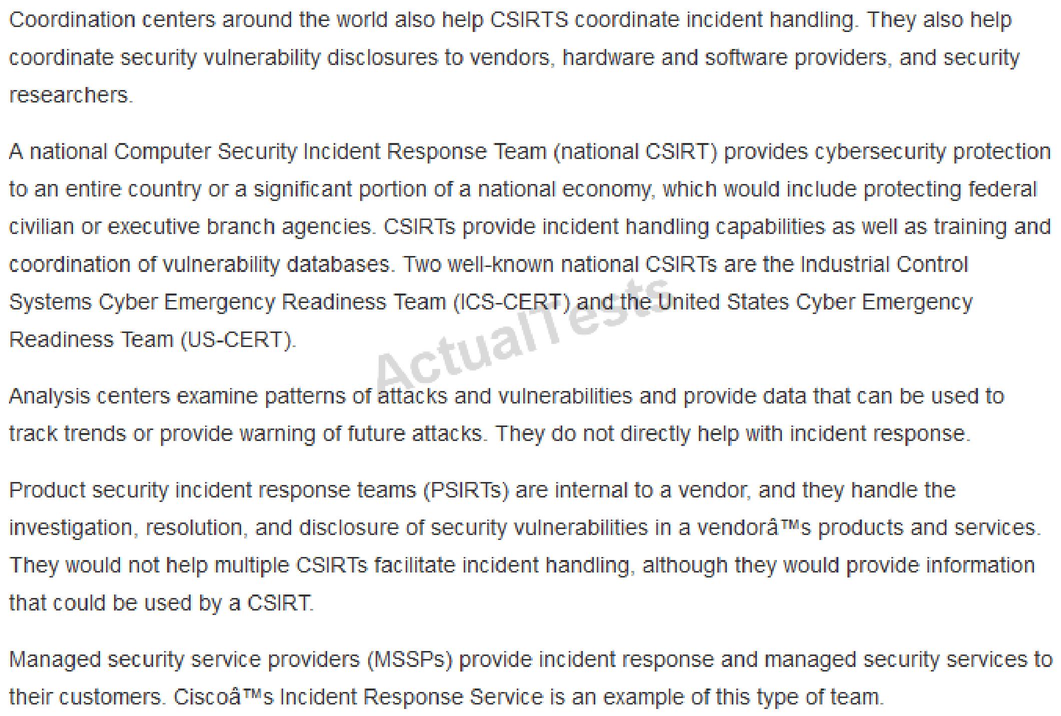
A.
MSSP

B.
national CSIRT

C.
Coordination center

D.
Analysis center

Answer: C
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 vendorâ™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. Ciscoâ™s Incident Response Service is an example of this type of team.

Reference: https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485654.pdf

QUESTION NO: 103

Which of the following represents a step in the second normal form in the process of normalization?

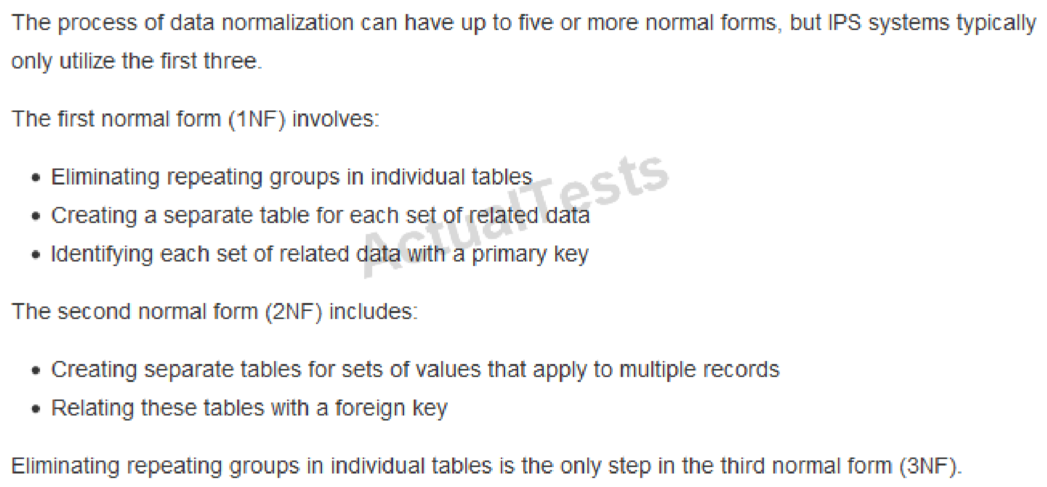
A.
Create a separate table for each set of related data.

B.
Eliminate repeating groups in individual tables.

C.
Create separate tables for sets of values that apply to multiple records.

D.
Eliminate fields that do not depend on the key.

Answer: C
Explanation:



The process of data normalization can have up to five or more normal forms, but IPS systems typically only utilize the first three.

The first normal form (1NF) involves:

- Eliminating repeating groups in individual tables
- Creating a separate table for each set of related data
- Identifying each set of related data with a primary key

The second normal form (2NF) includes:

- Creating separate tables for sets of values that apply to multiple records
- Relating these tables with a foreign key

Eliminating repeating groups in individual tables is the only step in the third normal form (3NF).

QUESTION NO: 104

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

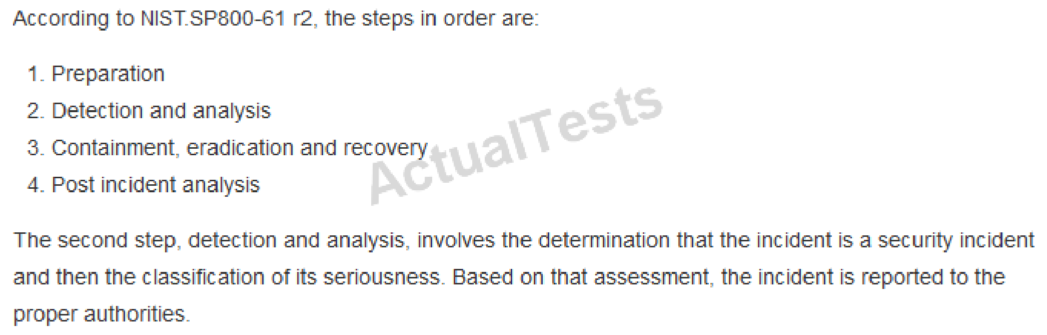
A.
detection and analysis

B.
post incident analysis

C.
preparation

D.
containment, eradication, and recovery

Answer: A
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.

QUESTION NO: 105

What information can be discovered from the user agent field in an HTTP packet?

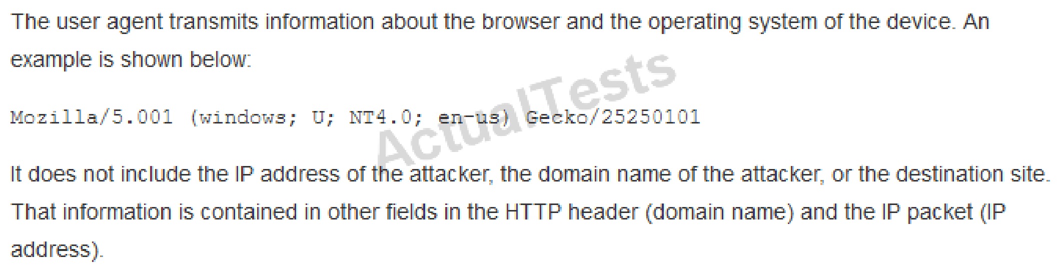
A.
IP address of attacker

B.
domain name of attacker

C.
browser version

D.
destination site

Answer: C
Explanation:



The user agent transmits information about the browser and the operating system of the device. An example is shown below:

```
Mozilla/5.001 (windows; U; NT4.0; en-us) Gecko/25250101
```

It does not include the IP address of the attacker, the domain name of the attacker, or the destination site. That information is contained in other fields in the HTTP header (domain name) and the IP packet (IP address).

Reference: https://whatismyipaddress.com/user-agent

QUESTION NO: 106

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

A.
remediation

B.
Identification

C.
containment

D.
lesson-based hardening

Answer: A

Explanation:

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

Reference:

https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

QUESTION NO: 107

What is the term for any evasion attempt where the attacker splits malicious traffic to avoid detection or filtering?

A.
fragmentation

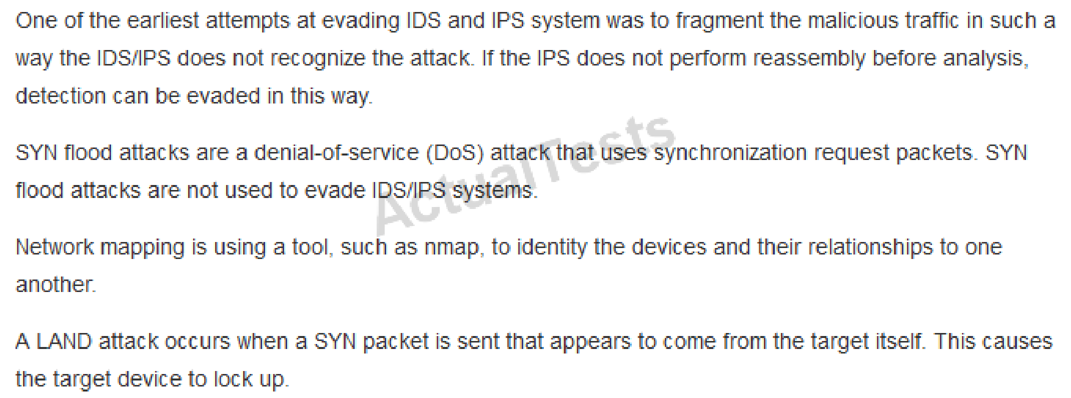
B.
SYN flood

C.
LAND attack

D.
network mapping

Answer: A

Explanation:



One of the earliest attempts at evading IDS and IPS system was to fragment the malicious traffic in such a way the IDS/IPS does not recognize the attack. If the IPS does not perform reassembly before analysis, detection can be evaded in this way.

SYN flood attacks are a denial-of-service (DoS) attack that uses synchronization request packets. SYN flood attacks are not used to evade IDS/IPS systems.

Network mapping is using a tool, such as nmap, to identity the devices and their relationships to one another.

A LAND attack occurs when a SYN packet is sent that appears to come from the target itself. This causes the target device to lock up.

Reference: http://www.ciscopress.com/articles/article.asp?p=1728833&seqNum=3

QUESTION NO: 108

Actors and actions are part of which VERIS schema category?

A.
discovery and response

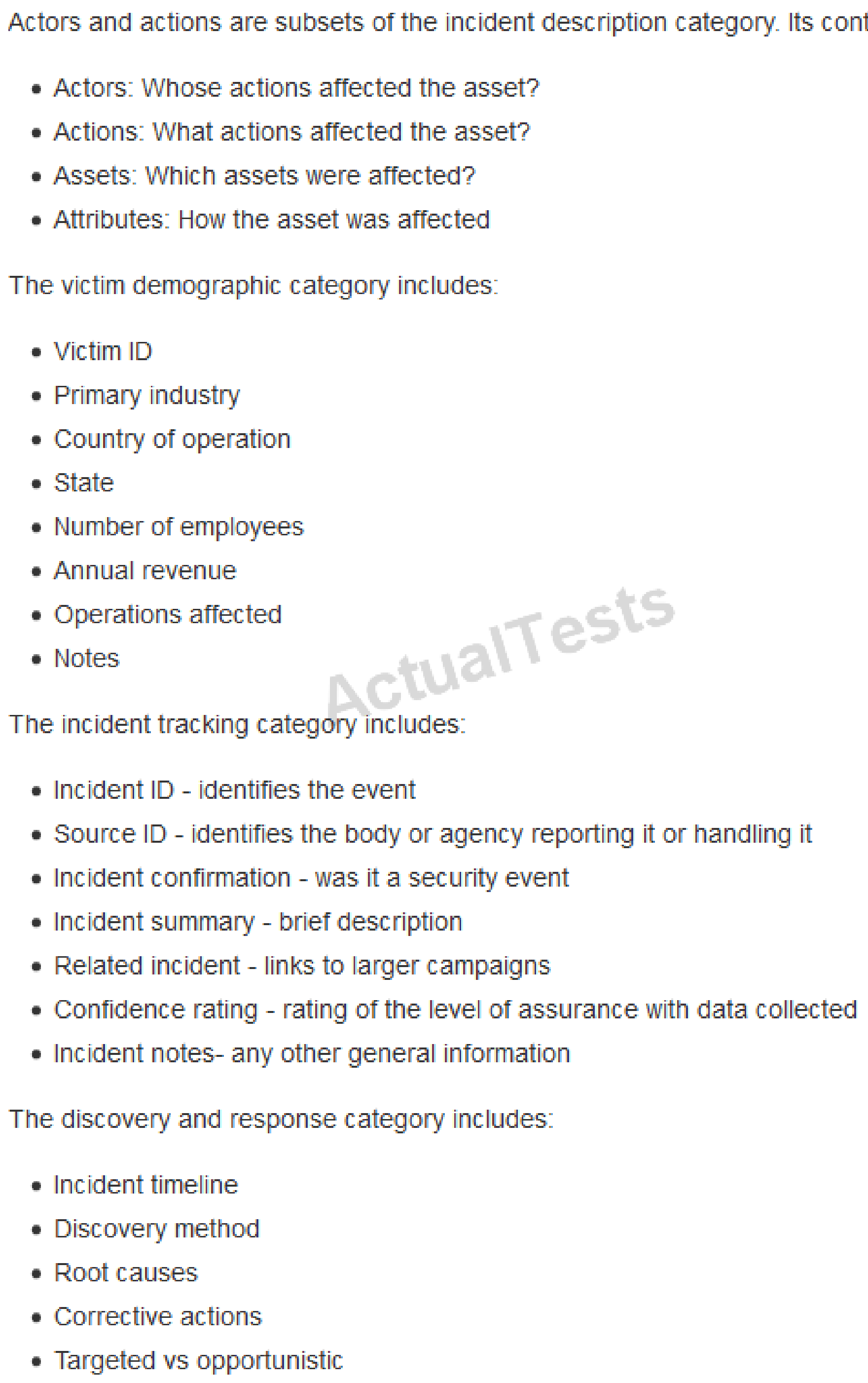
B.
incident tracking

C.
victim demographics

D.
incident description

Answer: D

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

Reference: http://veriscommunity.net/index.html

QUESTION NO: 109

When discontinuous free space is created by the adding and removing of data on a hard drive, what has occurred?

A.
steganography

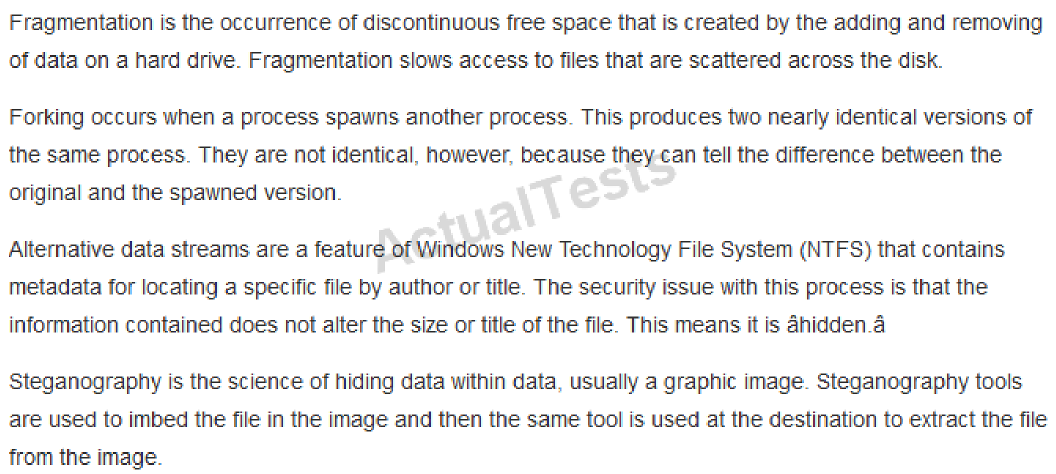
B.
alternative data streams

C.
forking

D.
fragmentation

Answer: D

Explanation:



Fragmentation is the occurrence of discontinuous free space that is created by the adding and removing of data on a hard drive. Fragmentation slows access to files that are scattered across the disk.

Forking occurs when a process spawns another process. This produces two nearly identical versions of the same process. They are not identical, however, because they can tell the difference between the original and the spawned version.

Alternative data streams are a feature of Windows New Technology File System (NTFS) that contains metadata for locating a specific file by author or title. The security issue with this process is that the information contained does not alter the size or title of the file. This means it is âhidden.â

Steganography is the science of hiding data within data, usually a graphic image. Steganography tools are used to imbed the file in the image and then the same tool is used at the destination to extract the file from the image.

Reference: https://www.remosoftware.com/faq/what-is-fragmentation

QUESTION NO: 110

Which process is used to increase data accuracy and integrity and to support data visualization?

A.
data aggregation

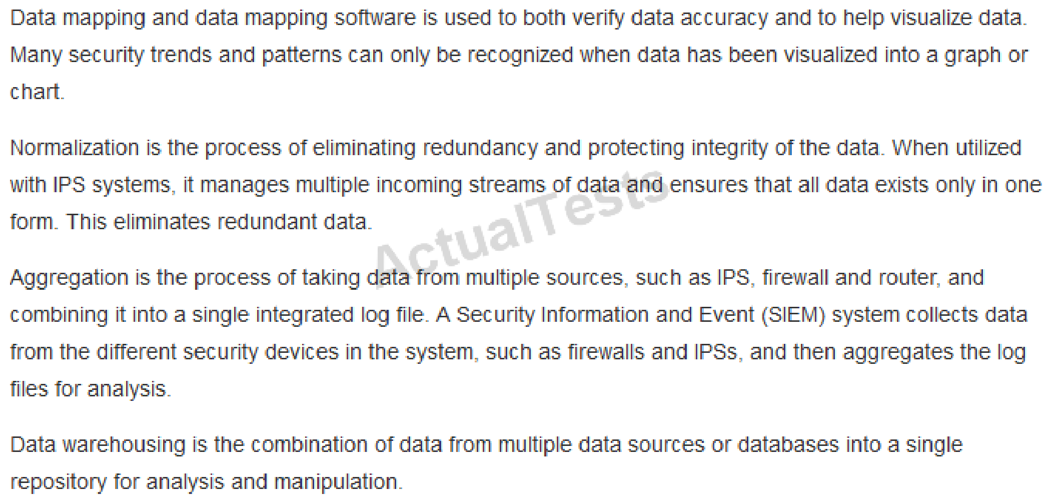
B.
data warehousing

C.
data normalization

D.
data mapping

Answer: D

Explanation:



Data mapping and data mapping software is used to both verify data accuracy and to help visualize data. Many security trends and patterns can only be recognized when data has been visualized into a graph or chart.

Normalization is the process of eliminating redundancy and protecting integrity of the data. When utilized with IPS systems, it manages multiple incoming streams of data and ensures that all data exists only in one form. This eliminates redundant data.

Aggregation is the process of taking data from multiple sources, such as IPS, firewall and router, and combining it into a single integrated log file. A Security Information and Event (SIEM) system collects data from the different security devices in the system, such as firewalls and IPSs, and then aggregates the log files for analysis.

Data warehousing is the combination of data from multiple data sources or databases into a single repository for analysis and manipulation.

Reference: https://www.bridging-the-gap.com/what-is-data-mapping/

QUESTION NO: 111

Which of the following is a standard for port-based access control?

A.
X.509

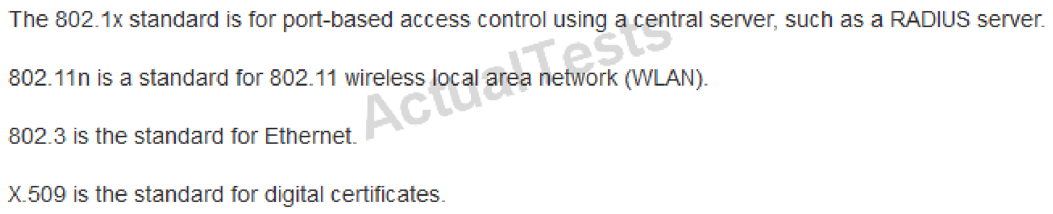
B.
802.11n

C.
802.3

D.
802.1x

Answer: D

Explanation:



The 802.1x standard is for port-based access control using a central server, such as a RADIUS server.

802.11n is a standard for 802.11 wireless local area network (WLAN).

802.3 is the standard for Ethernet.

X.509 is the standard for digital certificates.

Reference: https://searchmobilecomputing.techtarget.com/definition/8021X

QUESTION NO: 112

You discover several client machines are infected with malware that begins to make outbound calls (connection attempts) to a remote server after infection. You run a malware analysis tool.

What information could you derive from any domain names and host IP addresses in the malware analysis report?

A.
the next machine that will be infected

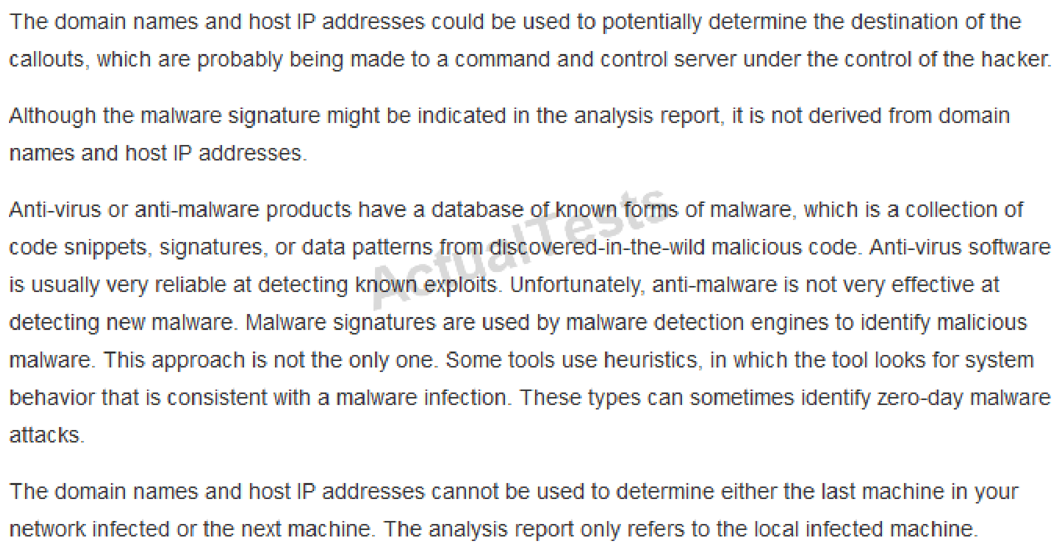
B.
destination of the callouts

C.
signature of the malware

D.
the first machine infected

Answer: B

Explanation:



The domain names and host IP addresses could be used to potentially determine the destination of the callouts, which are probably being made to a command and control server under the control of the hacker.

Although the malware signature might be indicated in the analysis report, it is not derived from domain names and host IP addresses.

Anti-virus or anti-malware products have a database of known forms of malware, which is a collection of code snippets, signatures, or data patterns from discovered-in-the-wild malicious code. Anti-virus software is usually very reliable at detecting known exploits. Unfortunately, anti-malware is not very effective at detecting new malware. Malware signatures are used by malware detection engines to identify malicious malware. This approach is not the only one. Some tools use heuristics, in which the tool looks for system behavior that is consistent with a malware infection. These types can sometimes identify zero-day malware attacks.

The domain names and host IP addresses cannot be used to determine either the last machine in your network infected or the next machine. The analysis report only refers to the local infected machine.

Reference:

https://www.networkworld.com/article/2235842/cisco-asa-innovation-tracks-botnet-malicious-activity.html

QUESTION NO: 113

Which of the following Wireshark filters excludes an IP address?

A.
gateway host <host>

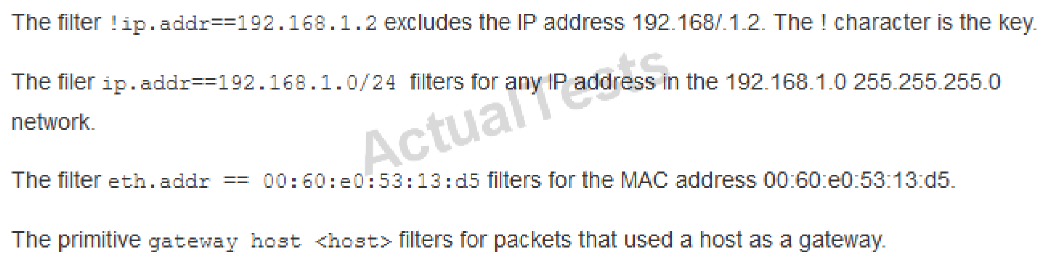
B.
!ip.addr ==192.168.1.2

C.
eth.addr == 00:60:0e:53:13:d5

D.
ip.addr==192.168.1.0/24

Answer: B

Explanation:



The filter `!ip.addr==192.168.1.2` excludes the IP address 192.168/.1.2. The ! character is the key.

The filer `ip.addr==192.168.1.0/24` filters for any IP address in the 192.168.1.0 255.255.255.0 network.

The filter `eth.addr == 00:60:e0:53:13:d5` filters for the MAC address 00:60:e0:53:13:d5.

The primitive `gateway host <host>` filters for packets that used a host as a gateway.

Reference: https://networksecuritytools.com/list-wireshark-display-filters/

QUESTION NO: 114

What is the main purpose of data normalization?

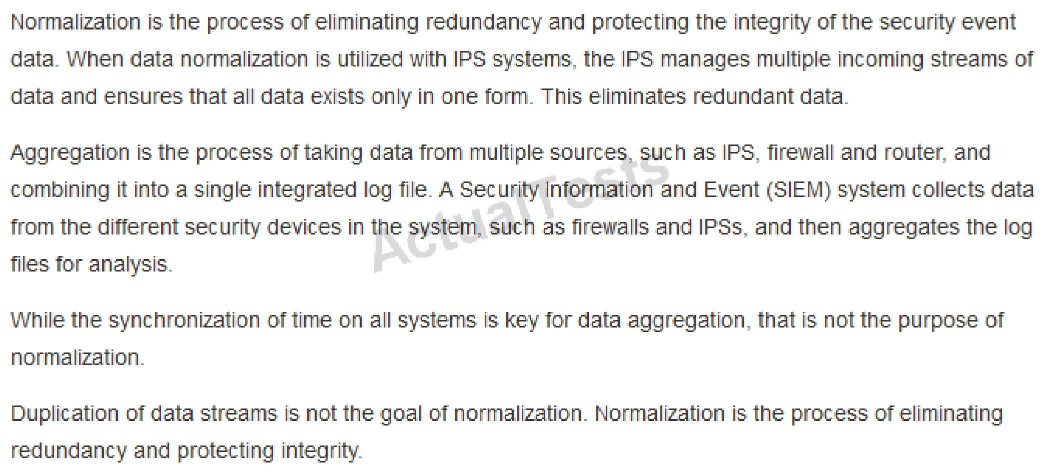
A.
synchronize of time stamps

B.
duplicate data streams

C.
eliminate redundancy

D.
aggregate data

Answer: C
Explanation:



Normalization is the process of eliminating redundancy and protecting the integrity of the security event data. When data normalization is utilized with IPS systems, the IPS manages multiple incoming streams of data and ensures that all data exists only in one form. This eliminates redundant data.

Aggregation is the process of taking data from multiple sources, such as IPS, firewall and router, and combining it into a single integrated log file. A Security Information and Event (SIEM) system collects data from the different security devices in the system, such as firewalls and IPSs, and then aggregates the log files for analysis.

While the synchronization of time on all systems is key for data aggregation, that is not the purpose of normalization.

Duplication of data streams is not the goal of normalization. Normalization is the process of eliminating redundancy and protecting integrity.

Reference: https://www.helpnetsecurity.com/2013/01/07/the-importance-of-data-normalization-in-ips/

QUESTION NO: 115

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

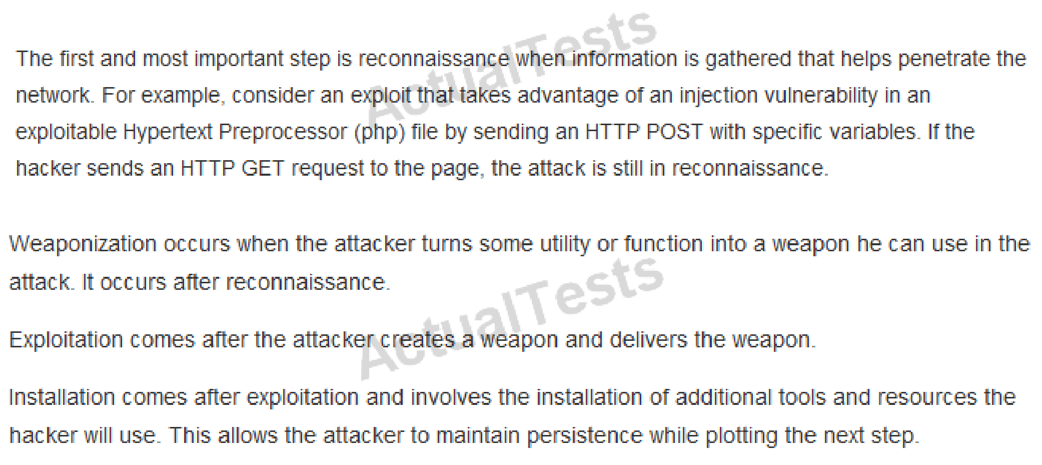
A.
exploitation

B.
weaponization

C.
reconnaissance

D.
installation

Answer: C
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.

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.

QUESTION NO: 116

Which of the following is part of the 5 tuple?

A.

web software

B.
NetFlow record ID

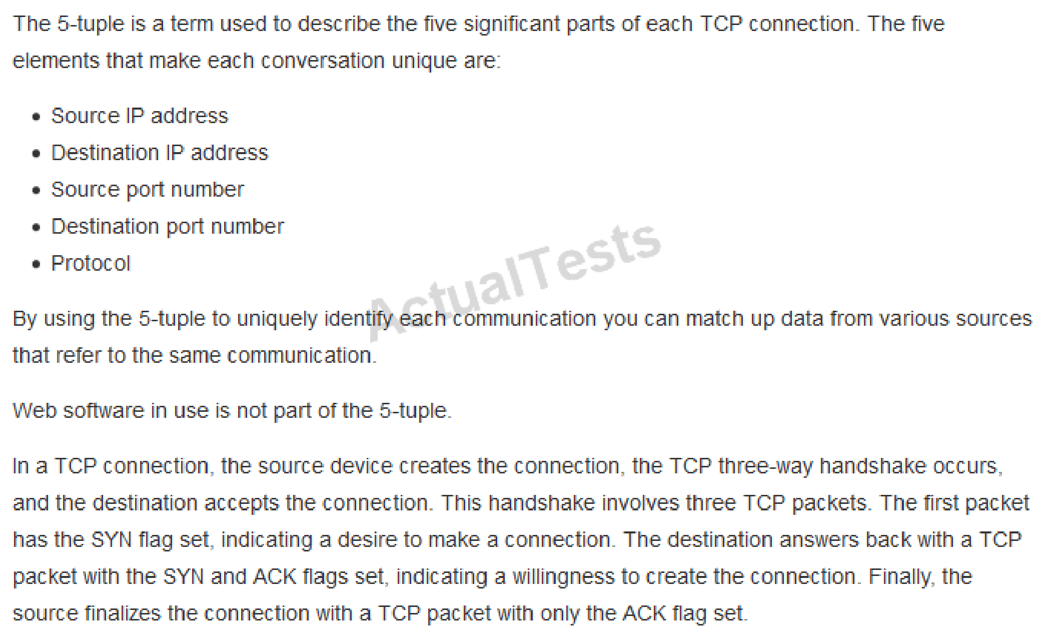
C.
source IP address

D.
operating system

E.
device name

Answer: C

Explanation:



The 5-tuple is a term used to describe the five significant parts of each TCP connection. The five elements that make each conversation unique are:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Protocol

By using the 5-tuple to uniquely identify each communication you can match up data from various sources that refer to the same communication.

Web software in use is not part of the 5-tuple.

In a TCP connection, the source device creates the connection, the TCP three-way handshake occurs, and the destination accepts the connection. This handshake involves three TCP packets. The first packet has the SYN flag set, indicating a desire to make a connection. The destination answers back with a TCP packet with the SYN and ACK flags set, indicating a willingness to create the connection. Finally, the source finalizes the connection with a TCP packet with only the ACK flag set.

Reference: https://blog.packet-foo.com/2015/03/tcp-analysis-and-the-five-tuple/

QUESTION NO: 117

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

A.
Reconnaissance

B.
Exploitation

C.
Weaponization

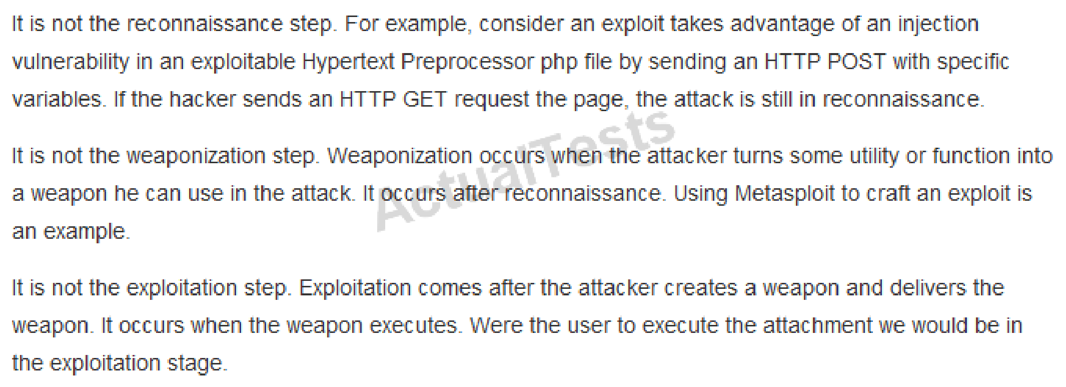
D.
Delivery

Answer: D

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:



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.

QUESTION NO: 118

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

A.
Applications

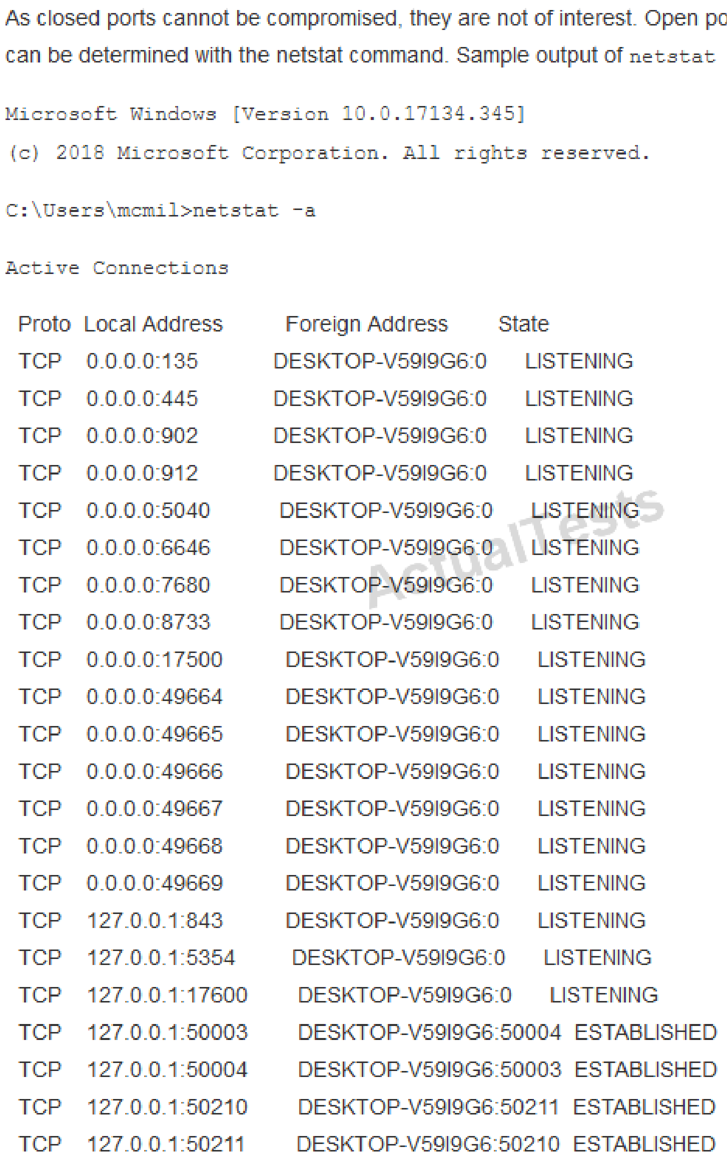
B.
Logged-in Users/Service Accounts

C.
Running Processes

D.
Closed ports

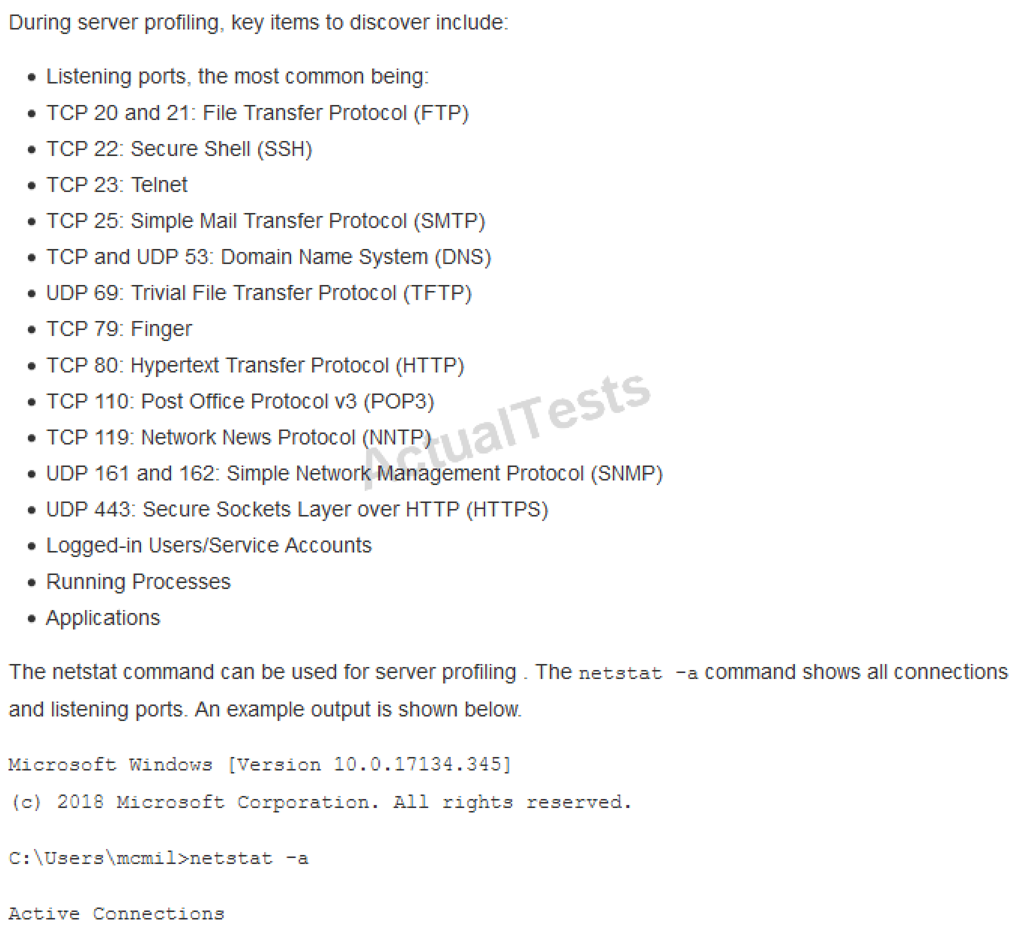
Answer: D

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
```

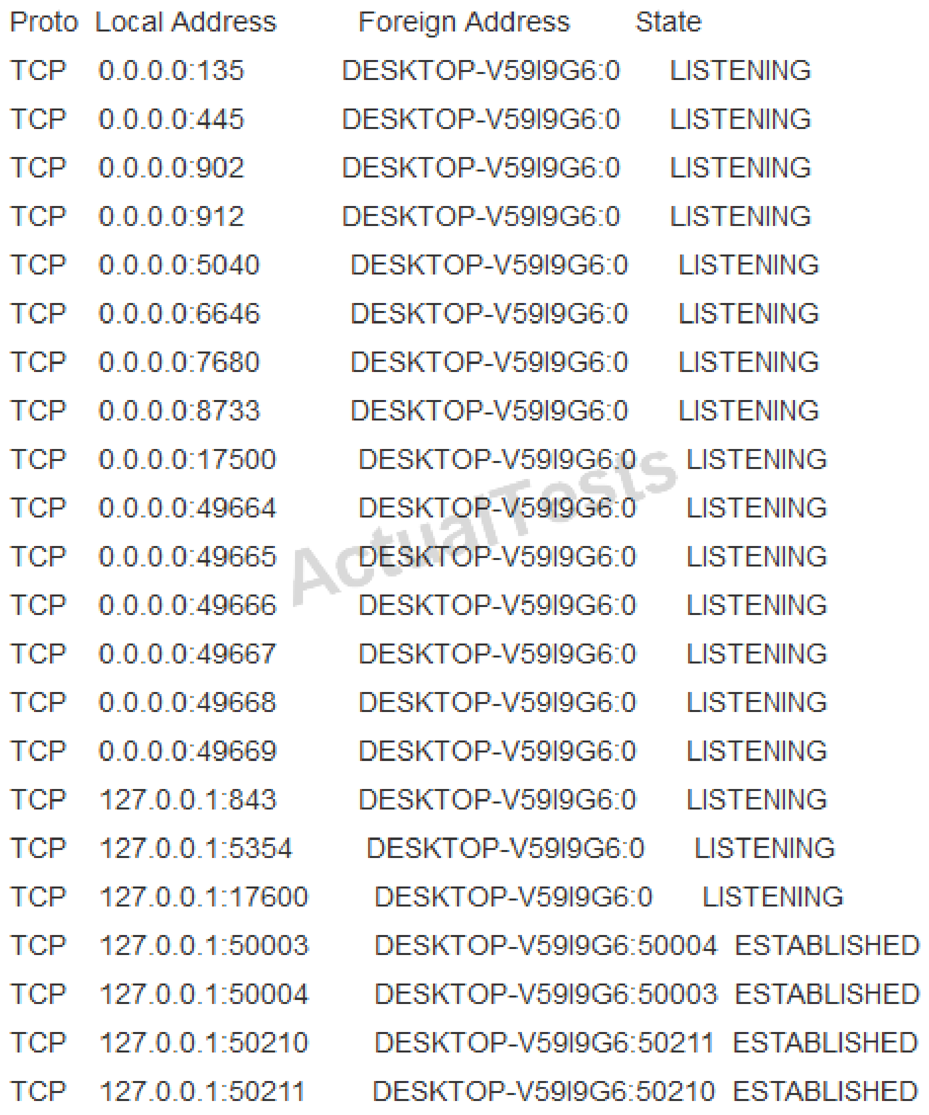


During server profiling, key items to discover include:

- 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
```

Reference: https://www.lifewire.com/netstat-command-2618098

QUESTION NO: 119

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

A.
Exactly what happened and at what time?

B.
How could information sharing with other organizations be improved?

C.
Whose fault was the attack?

D.
Were any steps or actions taken that might have inhibited the recovery?

Answer: C

Explanation:

Blame placing is not port o the post mortem.