200-201.exam

Number: 200-201
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Cisco 200-201

https://www.gratisexam.com/

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Exam A

QUESTION 1
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 2
Which of the following is not a hashing algorithm?

A. DES
B. MD5
C. SHA-1
D. SHA-3

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 3
Which of the following is the most widely used public key cipher?

A. 3DES
B. El Gamal
C. RSA
D. AES

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 4
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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
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 5
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 6
Which hashing algorithm is the strongest?

A. SHA-1
B. MD5
C. SHA-256
D. SHA-512

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 7
Which of the following is NOT an email protocol?

A. SMTP
B. IMAP
C. NTP
D. POP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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:

- TCP Port 20 – FTP (File transfer Protocol) data
- TCP Port 21 – FTP
- TCP Port 22 – Secure Shell (ssh), Secure Copy (scp), or Secure FTP (SFTP)
- TCP Port 23 – Telnet
- TCP Port 25 – Simple Mail Transfer Protocol (SMTP)
- TCP/UDP Port 53 – Domain Name System (DNS)
- UDP Port 67 Dynamic Host Configuration Protocol (DHCP) Server
- UDP Port 68 Dynamic Host Configuration Protocol (DHCP) Client
- TCP Port 80 HyperText Transfer Protocol (HTTP)

- TCP Port 110 – Post Office Protocol version 3 (POP3)
- TCP Port 123 – Network Time Protocol (NTP)
- TCP Port 143 – Internet Mail Access Protocol

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 8
Which of the following is Layer 3 attack?

A. ARP attacks
B. IP spoofing
C. VLAN hopping
D. MAC spoofing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 9
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 10
Which attack requires a botnet?

A. DDoS

B. password theft
C. DoS
D. man in the middle

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 11
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 12
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 13
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 14

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

A. NTP
B. STP
C. ARP
D. IGMP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 15
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 16
Which algorithm is a symmetric cipher?

A. ECC
B. El Gamai
C. 3DES
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 17
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 18
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

- Ingress interface
- Source IP address
- Destination IP address
- IP protocol
- Source port for UDP or TCP, 0 for other protocols
- Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
- IP Type of Service

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 19
Which of the following provides the C in CIA?

A. redundancy
B. hashing
C. encryption
D. multiple components

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 20
Which of the following increases when additional functionality is added to an application?

A. threats
B. vulnerabilities
C. risk
D. attack surface

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 21
What is the term for program or service in Linux?

A. handles
B. forks
C. processes
D. thread

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 22
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 23
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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:

- user agent – software (a software agent) that is acting on behalf of a user
- referrer header – URL data from an HTTP header field identifying the Web link used to direct users to a Web page
- host – sending device

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 24
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

Correct Answer: A
Section: (none)
Explanation

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

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

- The sender sends the first segment to the receiver with the Synchronization (SYN) flag enabled.

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

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

A packet with the ACK flag set would only follow a packet with the SYN and ACK flags set. The first step is to send a SYN packet. When the port is open, the receiver will send back a packet the 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 25
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 26
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 27
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 28
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

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
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 29
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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").

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

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 30
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 31
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 32
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 33
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 34
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 35
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 36
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 37
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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:

- 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 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 38
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 39
Which organizational stakeholders are responsible for installing anti-malware software?

A. System and network administrators
B. CEO
C. CISO
D. CSIRT team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 40
Cisco Active Threat Analysis is an example of which of the following?

A. MSSP
B. PSIRT
C. Coordination centers
D. National CSIRT

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 41
What is the final step in the Cyber Kill Chain framework?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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:

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

QUESTION 42
Which of the following is the latest Linux file system?

A. ext3
B. ext2
C. ext4
D. ext5

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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:

- Supports volumes with sizes up to 1 exibyte (EiB) and files with sizes up to 16 terabytes (TiB)
- Supports extens
- Is backwards compatible with ext3 and ext2
- Uses extents to replace the traditional block mapping scheme used by ext2 and ext3

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 43
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 44
What is the term for an operation that purges redundant data while maintaining data integrity?

A. modularization
B. aggregation
C. warehousing
D. normalization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 45
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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:

- TCP 20 and 21: File transfer Protocol (FTP)
- TCP 22: Secure Shell (SSH)
- TCP 23: Telnet
- TCP 25: Simple mail Transfer Protocols (SMTP)

- TCP and UDP 53: Domain Name System (DNS)
- UDP 69: Trivial File Transfer Protocol (TFTP)
- TCP 79: Finger
- TCP 80: Hypertext Transfer Protocol (HTTP)
- TCP 110: Post Office Protocol v3 (POP3)
- TCP 119: Network News Protocol (NNTP)
- UDP 161 and 162: Simple Network Management Protocol (SNMP)
- UDP 443: Secure Sockets Layer over HTTP (HTTPS)

Port 443 is SSL over HTTP, which is encrypted.

QUESTION 46
Which evidence is always considered the best evidence?

A. hearsay
B. indirect
C. direct
D. corroborative

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 47
Which of the following offers incident handling services for a fee to other organizations?

A. Coordination centers
B. MISSP

C. PSIRT
D. national CSIRT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 48
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}$`
D. `^[a-z1-6]+$`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The regular expression Щ[a-z0-9_-]{6,16}$ will locate all valid usernames. The Щ 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 Щ[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 Щ[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 Щ[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 49
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 50
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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
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:
- Accept – Media type(s) that is(are) acceptable for the response
- Content-Length – The length of the request body in octets (8-bit bytes)
- From – The email address of the user making the request
- Referrer – The address of the previous web page from which a link to the currently requested page was followed
- Host – The domain name of the server (for virtual hosting), and the TCP port number on which the server is listening
- Date – The date and time that the message was originated
- Authorization – Authentication credentials for HTTP authentication

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:
- 8 for Echo Request
- 0 for Echo Reply
- 11 for Timeout Exceeded
- 3 for Destination Unreachable

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 51
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

QUESTION 52
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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:

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

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

QUESTION 53
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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:

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

QUESTION 54
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 55
In which stage of incident handling is the extent of the incident determined?

A. lessons learned
B. containment
C. scoping
D. identification

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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:

- Identification - determining whether there is an incident

- Scoping - determining the extent of the incident and identifying the attackers
- Containment - halting the spread of the incident and minimizing the impact
- Remediation – returning the environment to secure state
- Lesson-based hardening preventing future incidents
- reporting – documenting the incident and reporting it

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

QUESTION 56
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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:

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

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 57
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 58
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 59
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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:

- Low (L) – the attacker can perform the attack at will
- High (H) – the attack depends on conditions beyond the control of the attacker

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

QUESTION 60
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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