Vendor: Cisco

Exam Code: 200-201

Exam Name: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Version: DEMO

QUESTION 1
Which action matches the weaponization step of the Cyber Kill Chain model?

A. Research data on a specific vulnerability.
B. Test and construct the appropriate malware to launch the attack.
C. Scan a host to find open ports and vulnerabilities.
D. Construct the appropriate malware and deliver it to the victim.

Answer: B
Explanation:
Weaponization in the Cyber Kill Chain refers to the phase where attackers craft or develop the specific exploit or malicious payload designed to carry out the attack. This phase involves constructing, refining, and testing the malware or exploit to ensure its effectiveness in achieving the attacker's objectives. Therefore, "Test and construct the appropriate malware to launch the attack" aligns with the weaponization step.

QUESTION 2
Which process represents the application-level allow list?

A. allowing everything and denying specific executable files
B. allowing everything and denying specific applications protocols
C. allowing specific files and deny everything else
D. allowing specific format files and deny executable files

Answer: C
Explanation:
An application-level allow list involves permitting specific files, applications, or software while denying access to everything else. This approach focuses on explicitly specifying and permitting certain trusted applications or files, ensuring that only approved or authorized items are allowed to execute or run within a system or network. All other files or applications not listed in the allow list are automatically restricted or denied from executing or accessing resources.

QUESTION 3
According to CVSS, what is a description of the attack vector score?

A. It depends on how far away the attacker is located and the vulnerable component.
B. The metric score will be larger when a remote attack is more likely.
C. It depends on how many physical and logical manipulations are possible on a vulnerable component.
D. The metric score will be larger when it is easier to physically touch or manipulate the vulnerable component.

Answer: B
Explanation:
The Attack Vector metric assesses the different ways an attacker could exploit a vulnerability, considering the level of proximity required for the attack.
A higher score is given when the vulnerability can be exploited remotely without the need for physical access to the vulnerable system, indicating a higher risk compared to attacks that require physical access or user interaction. Therefore, the Attack Vector score is larger when the possibility of a remote attack is more feasible, as remote attacks often pose a higher risk due to their accessibility and potential for exploitation by a wider range of threat actors.

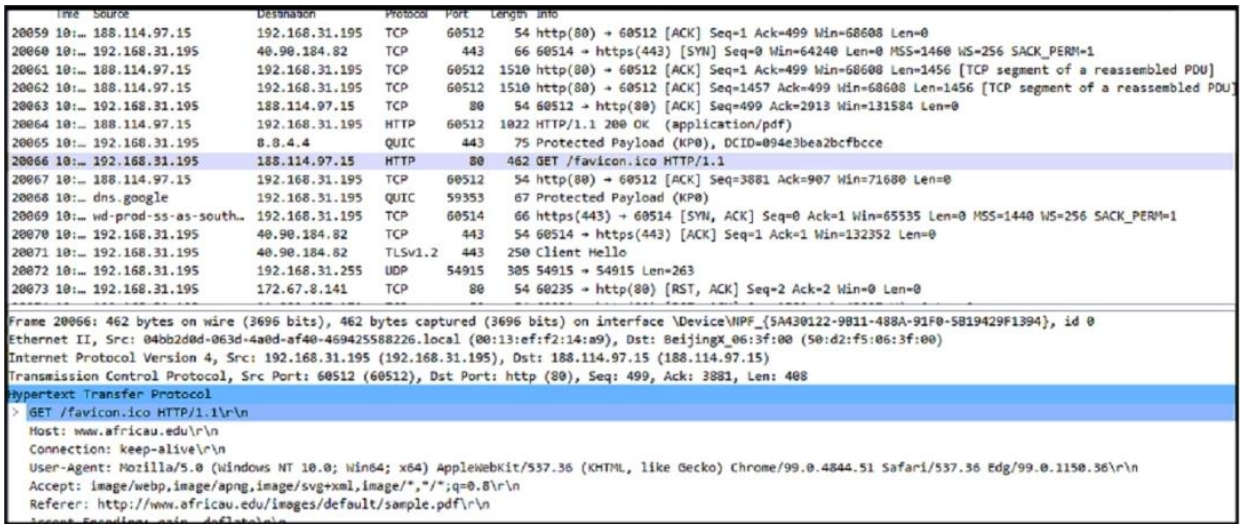
QUESTION 4
Refer to the exhibit. An attacker gained initial access to the company's network and ran an Nmap scan to advance with the lateral movement technique and to search the sensitive data. Which two elements can an attacker identify from the scan? (Choose two.)

```
nmap 10.19.140.2

Starting Nmap 6.40 ( http://nmap.org ) at 2019-07-21 16:39 EDT
Nmap scan report for 10.19.140.2
Host is up (0.061s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
199/tcp   open  smux
443/tcp   open  https
8000/tcp  open  http-alt
8181/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.18 seconds
```

A. workload and the configuration details
B. functionality and purpose of the server
C. number of users and requests that the server is handling
D. running services
E. user accounts and SID

Answer: BD

QUESTION 5
Refer to the exhibit. Which frame numbers contain a file that is extractable from Wireshark PCAP?



A. Frames No. 20064 and 20066
B. Frame No. 20064

C. Frame No. 20086
D. All Frames from No. 20061 to 20064

Answer: D

QUESTION 6
Which two measures are used by the defense-in-depth strategy? (Choose two.)

A. Bridge the single connection into multiple.
B. Divide the network into parts.
C. Split packets into pieces.
D. Implement the patch management process.
E. Reduce the load on network devices.

Answer: BD
Explanation:
Divide the network into parts: This measure involves segmenting or dividing the network into separate zones or segments with different security controls based on sensitivity, functionality, or user access requirements. Segmentation helps contain potential threats, limits lateral movement, and mitigates the impact of security incidents by compartmentalizing network areas.
Implement the patch management process: Patch management is crucial in maintaining the security of systems. It involves regularly applying updates, patches, or fixes provided by software vendors to address vulnerabilities or weaknesses in software or systems. Implementing a robust patch management process ensures that systems are up-to-date with the latest security patches, reducing the risk of exploitation of known vulnerabilities.

QUESTION 7
Which example represents the defense-in-depth principle?

A. implementing a CMDB
B. creating a separate VLAN to isolate networks
C. creating a privileged group in AD
D. implementing new security policy within the organization

Answer: B
Explanation:
Defense-in-depth is a cybersecurity strategy that involves implementing multiple layers of security controls to protect systems and networks. Creating a separate VLAN (Virtual Local Area Network) to isolate and segment networks is an application of this principle. VLANs help in segregating network traffic, controlling access between different network segments, and mitigating the impact of potential security breaches by limiting the spread of unauthorized access or attacks across the network. This segmentation adds an additional layer of security to the overall network infrastructure.

QUESTION 8
What is the purpose of a SIEM solution?

A. to collect and forward event logs to another log collection device to evaluate security threats
B. to collect and correlate event log data to provide holistic views of the security posture of an environment
C. to collect and categorize indicators of compromise to evaluate and search for potential security

threats
D. to monitor and manage firewall access control lists for duplicate firewall filtering

Answer: B
Explanation:
SIEM systems are designed to aggregate and analyze data from various sources such as logs, event records, and security-related information across an organization's network infrastructure. The primary function is to collect, store, normalize, and analyze this data to provide comprehensive insights into the security posture of an environment. It correlates events, identifies patterns, detects anomalies, and generates alerts or reports that help security teams in threat detection, incident response, compliance monitoring, and overall security management. This holistic view aids in understanding the overall security status, identifying potential threats, and enabling proactive measures to mitigate risks.

QUESTION 9
Which evasion method is being used when TLS is observed between two endpoints?

A. encryption
B. obfuscation
C. X.509 certificate authentication
D. traffic insertion

Answer: A
Explanation:
TLS (Transport Layer Security) is a cryptographic protocol designed to provide secure communication between two endpoints over a network. It encrypts the data transmitted between these endpoints, ensuring confidentiality, integrity, and authenticity of the data. The encryption of data in transit using TLS helps in preventing eavesdropping or tampering by unauthorized entities, thereby securing the communication channel.

QUESTION 10
What is a comparison between rule-based and statistical detection?

A. Statistical is based on measured data while rule-based uses the evaluated probability approach.
B. Statistical uses the probability approach while rule-based is based on measured data.
C. Rule-based is based on assumptions and statistical uses data known beforehand.
D. Rule-based uses data known beforehand and statistical is based on assumptions.

Answer: B
Explanation:
Rule-Based Detection: Relies on predefined rules or signatures that identify known patterns or characteristics of attacks or threats. It involves a set of explicit rules that detect specific patterns or behaviors within the data. These rules are typically based on known attack patterns, signatures, or indicators of compromise (IoCs) and are static in nature.
Statistical Detection: Utilizes statistical models or algorithms to analyze patterns in data and identify anomalies or deviations from normal behavior. It involves analyzing data for unusual patterns or deviations from expected behavior based on statistical models, behavioral baselines, or machine learning algorithms.

QUESTION 11
What are the two differences between vulnerability and exploit? (Choose two.)

A. Vulnerabilities can be found in hardware and software, and exploits can be used only for software-based vulnerabilities.
B. Zero-day exploit can be used to take advantage of a vulnerability until the vulnerable software or hardware is patched.
C. Known vulnerabilities are assigned special CVE numbers, and exploits are using process to take advantage of vulnerabilities.
D. Zero-day exploit can be used for taking advantage of a known vulnerability, and cyber-attack can be performed on company assets.
E. Vulnerabilities are usually populated in the dark web, and exploit tools and methods can be found in the public web.

Answer: AB
Explanation:
Vulnerabilities refer to weaknesses or flaws present in hardware, software, or configurations that can be exploited. They can exist in both hardware and software. Exploits, however, are methods, scripts, or tools that leverage vulnerabilities to gain unauthorized access, execute commands, or perform malicious actions. While many exploits target software vulnerabilities, there are also exploits that target vulnerabilities in hardware or system configurations.
Zero-day exploits are exploits that take advantage of vulnerabilities that are unknown to the software vendor or the public. Attackers use zero-day exploits until the vulnerability is discovered and patched, providing a window of opportunity for attacks.

QUESTION 12
What are two differences of deep packet inspection compared to stateful firewall inspection? (Choose two.)

A. static lists for maintaining a strict access control level
B. different rule configurations based on payload pattern
C. quality of service capabilities based on list definitions
D. offers application-level monitoring
E. inspection of only the first packet during a connection attempt

Answer: BD
Explanation:
Deep packet inspection involves examining packet contents, including payloads, to apply rules and policies based on the specific patterns found within the packet payloads. This allows for more granular and detailed rule configurations compared to stateful firewall inspection, which typically focuses on broader rules based on connection states and header information.
Deep packet inspection offers application-level monitoring by delving into the actual contents of packets up to the application layer (Layer 7 of the OSI model). It can understand and analyze specific application-layer protocols, enabling the inspection and control of traffic based on application-specific characteristics or signatures. Stateful firewall inspection primarily focuses on monitoring and controlling traffic based on the state of connections and header information, usually operating at lower OSI layers (Layers 3 and 4).

QUESTION 13
What is used to maintain persistent control of an exploited device?

A. encryption
B. ARP spoof
C. rootkit

D. DDoS

Answer: C
Explanation:
A rootkit is a type of malicious software designed to gain unauthorized access to a computer system and maintain persistent control over it while concealing its presence from users and security tools. Rootkits are specifically crafted to enable continued access or control over a compromised system without being detected. They can be employed to carry out various malicious activities, such as spying on user activities, stealing sensitive information, or allowing unauthorized access for further exploitation.

QUESTION 14
According to CVSS, which metric group does user interaction belong to?

A. temporal
B. temporary
C. base
D. environmental

Answer: C
Explanation:
There are three metric groups that make up every CVSS score - Base, Temporal, and Environmental. Every component has several subcomponents.

QUESTION 15
What is the impact of a ransomware infection?

A. Data on infected endpoints is encrypted.
B. Encrypted data cannot be restored from backup.
C. Multiple connections are made to external C&C servers.
D. User must pay ransom to decrypt data.

Answer: A
Explanation:
Ransomware is a type of malware that encrypts files or systems, making them inaccessible to users unless a ransom is paid to the attacker. When a system gets infected with ransomware, the malware encrypts the data on the compromised machine or network, rendering it unusable or inaccessible to the user without the decryption key held by the attacker. This encryption process is the primary impact of a ransomware infection, causing data loss or inaccessibility until the ransom is paid or alternative solutions are found.

QUESTION 16
Which piece of information is needed for attribution in an investigation?

A. attack surface and the threat posing the risk
B. attack vector and exploited vulnerability
C. asset value and an asset owner
D. threat actor and associated behavior

Answer: D
Explanation:

Attribution in investigations involves identifying and linking the actions or behaviors of threat actors (individuals, groups, or entities) to a particular incident or attack. Understanding the behavior patterns, techniques, or tactics associated with known threat actors can assist in attributing an attack to a specific group or individual. Associating the observed behaviors with a known threat actor's profile aids in establishing the source or identity of the attacker, contributing to attribution efforts in security investigations.

QUESTION 17
What are two types of cross site scripting attacks? (Choose two.)

A. directed
B. encoded
C. reflected
D. stored
E. cascaded

Answer: CD
Explanation:
Reflected XSS: In a reflected XSS attack, the malicious script is injected into a web application and reflected back to the user as part of the request, often through URLs or input fields. The injected script is then executed within the victim's browser.
Stored XSS: Stored XSS, also known as persistent XSS, occurs when the malicious script is permanently stored on the target server, such as in a database or in user-generated content. When other users access the compromised data, the malicious script executes in their browsers.

QUESTION 18
What is a Heartbleed vulnerability?

A. denial of service
B. information disclosure
C. buffer overflow
D. command injection

Answer: B
Explanation:
Heartbleed is a security vulnerability found in the OpenSSL cryptographic software library. It allows an attacker to retrieve memory contents from servers running affected versions of OpenSSL. This information disclosure vulnerability could potentially expose sensitive data, including usernames, passwords, cryptographic keys, and other confidential information from the server's memory. Heartbleed does not enable direct execution of commands or cause a denial of service (DoS) by itself; instead, it facilitates the retrieval of potentially sensitive data from affected systems.

QUESTION 19
What is the difference between the ACK flag and the RST flag?

A. The ACK flag validates the next packets to be sent to a destination, and the RST flag is what the RST returns to indicate that the destination is reachable.
B. The RST flag establishes the communication, and the ACK flag cancels spontaneous connections that were not specifically sent to the expecting host.
C. The RST flag identifies the connection as reliable and trustworthy within the handshake process,

and the ACK flag prepares a response by opening a session between the source and destination.

D. The ACK flag validates the receipt of the previous packet in the stream, and the same session is being closed by the RST flag.

Answer: D
Explanation:
ACK (Acknowledgment) Flag: The ACK flag in the TCP header acknowledges the successful receipt of data by confirming the receipt of a packet or segment. It validates that the receiver has received a particular sequence number and acknowledges the next expected sequence number. It does not close sessions but rather acknowledges data within an ongoing session.
RST (Reset) Flag: The RST flag, on the other hand, is used in TCP to immediately terminate a connection. When a device receives a packet with the RST flag set, it indicates an abnormal condition or an attempt to reset or abort an ongoing connection. The RST flag is used to forcefully close a session and reset the connection.

QUESTION 20
Where is a host-based intrusion detection system located?

A. on a dedicated proxy server monitoring egress traffic
B. on a tap switch port
C. on a span switch port
D. on an end-point as an agent

Answer: D
Explanation:
Host-based intrusion detection systems (HIDS) are installed on individual endpoints or hosts (such as servers, workstations, or laptops) as software agents. These agents monitor and analyze activities occurring on the specific host where they are installed. HIDS are designed to detect suspicious activities, unauthorized access attempts, or security policy violations on the host itself, providing insights into potential security threats or breaches occurring at the endpoint level.

QUESTION 21
Which SOC metric represents the time to stop the incident from causing further damage to systems or data?

A. Mean Time to Respond (MTTR)
B. Mean Time to Acknowledge (MTTA)
C. Mean Time to Contain (MTTC)
D. Mean Time to Detect (MTTR)

Answer: C
Explanation:
Mean Time to Contain (MTTC) measures the average time taken by a Security Operations Center (SOC) or incident response team to contain or mitigate a security incident after it has been detected. It signifies the duration between the detection of an incident and successfully implementing measures to prevent further damage or spread of the incident within the environment.

QUESTION 22
Which technique obtains information about how the system works without knowing it's design

details?

A. DNS spoofing
B. DDOS attack
C. malware analysis
D. reverse engineering

Answer: D
Explanation:
Reverse engineering involves analyzing a system, software, or hardware to understand its functionality, design principles, or architecture without relying on specific knowledge of the system's internal workings. This process typically involves disassembling, decompiling, or analyzing the system to gain insight into its structure and behavior.

QUESTION 23
Which risk approach eliminates activities posing a risk exposure?

A. risk acknowledgment
B. risk reduction
C. risk retention
D. risk avoidance

Answer: D
Explanation:
Risk avoidance involves taking actions to completely remove or avoid activities, processes, or situations that could potentially lead to risks or threats.
This approach aims to steer clear of situations where potential risks might occur, thereby eliminating the chance of exposure to those risks entirely.

QUESTION 24
What is session data used for in network security?

A. It contains the set of parameters used for fetching logs.
B. It tracks cookies within each session initiated from user.
C. It is the transaction log between monitoring software.
D. It is the summary of the transmission between two network devices.

Answer: D
Explanation:
Session data is a record of a conversation between two network endpoints, which are often a client and a server.

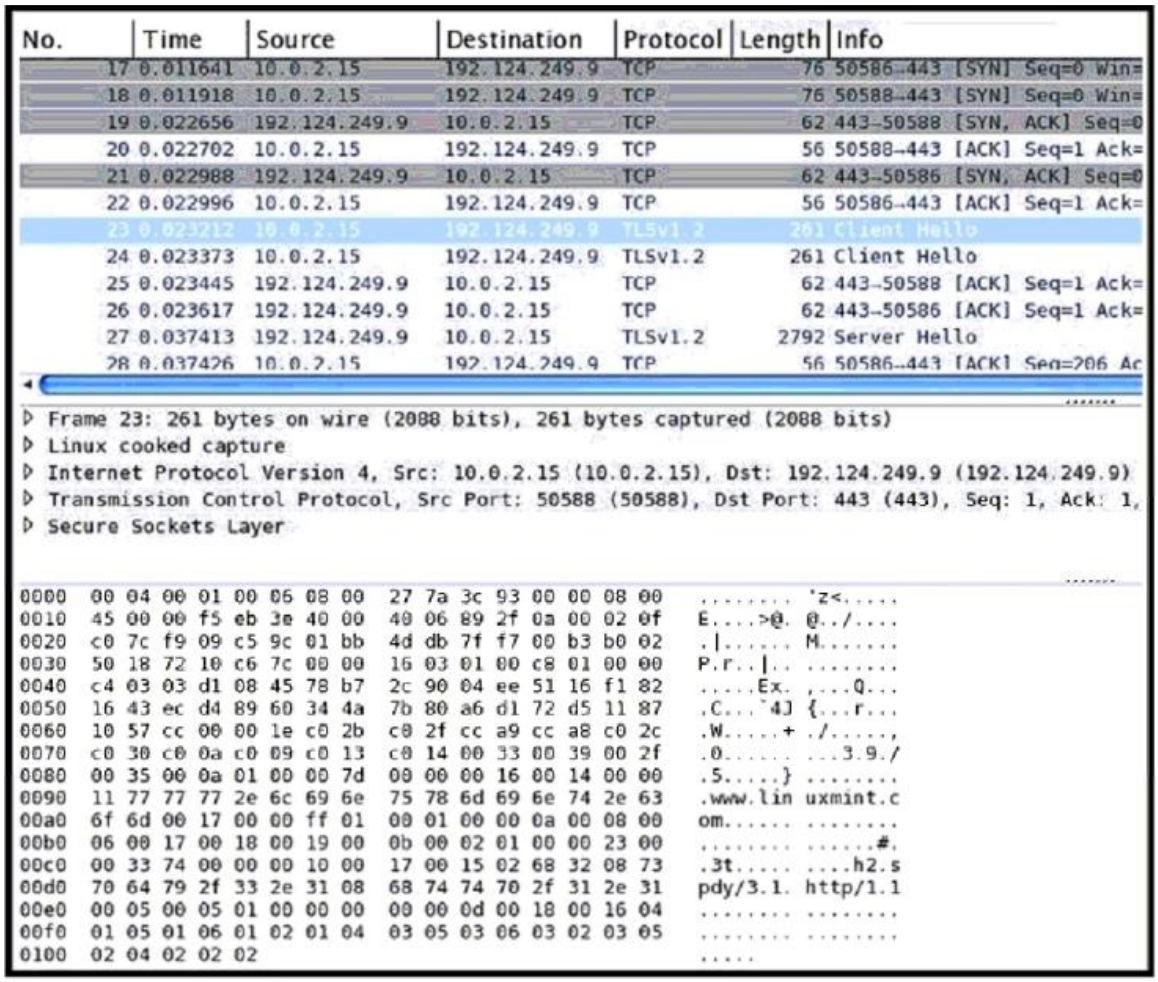
QUESTION 25
What is the principle of defense-in-depth?

A. Agentless and agent-based protection for security are used.
B. Several distinct protective layers are involved.
C. Access control models are involved.
D. Authentication, authorization, and accounting mechanisms are used.

Answer: B
Explanation:
Defense-in-depth is a cybersecurity strategy that involves the implementation of multiple layers of security controls, mechanisms, and safeguards throughout an organization's IT infrastructure. The principle aims to create a layered defense approach, where various security measures are employed at different levels within the network, systems, applications, and data to mitigate risks and protect against diverse threats. This strategy involves using a combination of technical, administrative, and physical controls, such as firewalls, intrusion detection systems, antivirus software, access controls, encryption, employee training, and more, to provide redundancy and enhance overall security posture.

QUESTION 26
Drag and Drop Question

Refer to the exhibit. Drag and drop the element names from the left onto the corresponding pieces of the PCAP file on the right.



Answer Area

source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	TCP
Transport Protocol	Internet Protocol v4
Application Protocol	TLS v1.2

Answer:

Answer Area

	source address
	source port
	destination port
	destination address
	Transport Protocol
	Network Protocol
	Application Protocol

QUESTION 27
What is the relationship between a vulnerability and a threat?

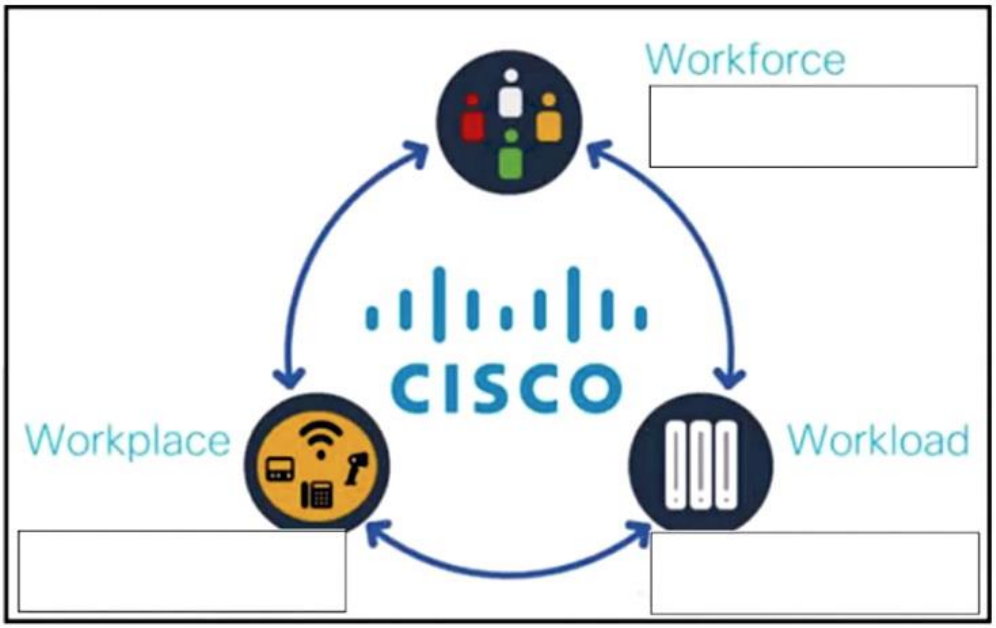
A. A threat exploits a vulnerability
B. A vulnerability is a calculation of the potential loss caused by a threat
C. A vulnerability exploits a threat
D. A threat is a calculation of the potential loss caused by a vulnerability

Answer: A
Explanation:
A vulnerability represents a weakness or flaw in a system, application, or network that could potentially be exploited by a threat actor or an external entity. Meanwhile, a threat refers to anything that has the potential to cause harm, exploit vulnerabilities, or compromise the security of a system or organization. Threats exploit vulnerabilities, taking advantage of the weaknesses present in systems or networks to cause damage, gain unauthorized access, or carry out malicious activities.

QUESTION 28
Drag and Drop Question

Cisco's Zero Trust Architecture simplifies the Zero Trust journey into three critical areas. Drag the definitions onto the graphic to describe Zero Trust from the Cisco perspective.

Answer Area



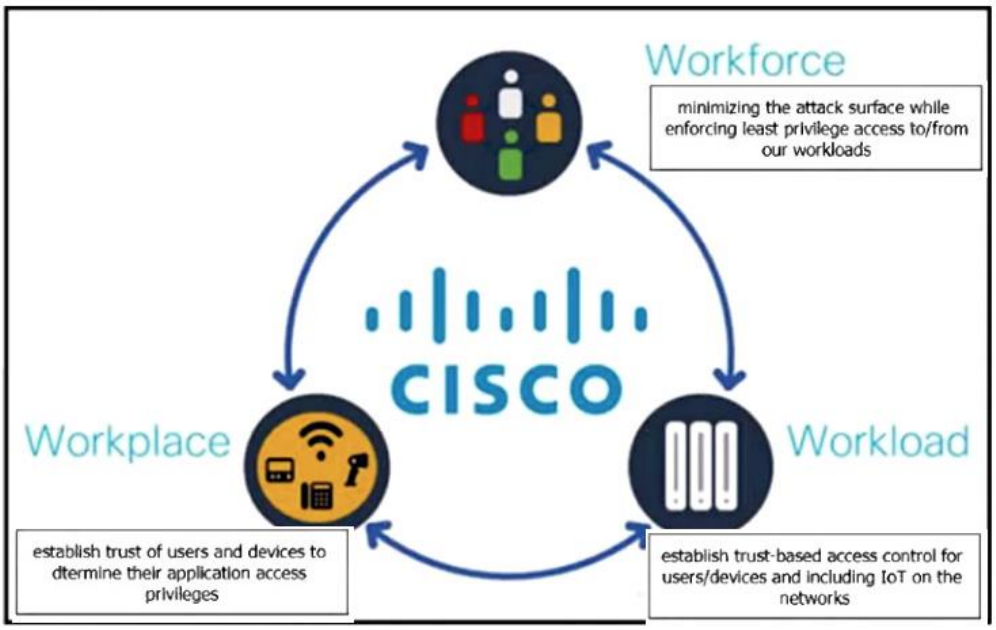
minimizing the attack surface while enforcing least privilege access to/from our workloads

establish trust-based access control for users/devices and including IoT on the networks

establish trust of users and devices to dtermine their application access privileges

Answer:

Answer Area



QUESTION 29
What is the difference between attack surface and vulnerability management?

A. Vulnerability management is to create strong user access protocols, and the attack surface is to defend against buffer overflow attacks.
B. Attack surface reduction is to block all ports except port 80, and vulnerability management is to correct programming bugs in a code.
C. Vulnerability management is to protect backups, and attack surface is to find critical OS drawback that results in remote code execution.
D. Attack surface reduction is to defend against SQL injection attacks, and vulnerability management is to use strong authentication policies.

Answer: B
Explanation:
The attack surface refers to all the possible entry points (e.g., open ports, services, exposed APIs, applications) through which an attacker could exploit a system. Attack surface reduction involves minimizing these entry points to reduce the risk of an attack. For example, blocking all unnecessary ports except essential ones (like port 80 for HTTP traffic) reduces the avenues an attacker can use.
Vulnerability management is the process of identifying, assessing, and mitigating vulnerabilities (weaknesses or flaws) in a system, such as software bugs, configuration issues, or outdated systems. Correcting programming bugs, such as fixing buffer overflow vulnerabilities or patching software, is part of vulnerability management.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**