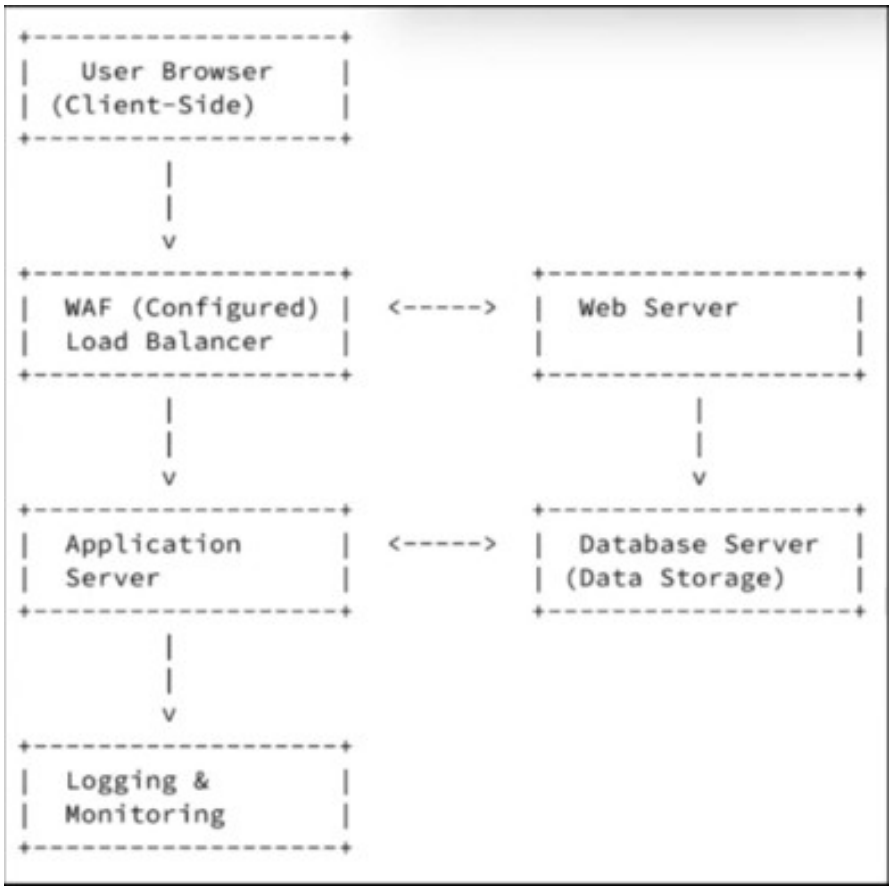
Vendor: Cisco

Exam Code: 350-201

Exam Name: Performing CyberOps Using Core Security Technologies

Version: DEMO

QUESTION 1
Refer to the exhibit. A security architect must develop a threat model for a new web application. Which two components should be prioritized for analysis to identify potential security risks? (Choose two.)



A. web server
B. load balancer
C. external APIs
D. application server
E. database server

Answer: DE
Explanation:
The application server contains the core business logic where most vulnerabilities such as injection and authentication flaws occur. The database server stores sensitive data, making it a primary target for data breaches, so both must be prioritized in threat modeling.

QUESTION 2
An organization plans to become ISO 27001 compliant and asked a compliance team to complete the initial implementation project. Which type of information is appropriate to present to executive stakeholders during the presentation?

A. technical specifications of hardware and software required for implementation
B. gaps between unpatched systems and requirements

C. estimated budget required for implementation
D. servers and software asset databases affected by the project

Answer: C
Explanation:
Executive stakeholders require high-level, strategic information for decision-making. Presenting the estimated budget provides insight into resource allocation and financial impact, which is most relevant at the executive level.

QUESTION 3
What are hardened images?

A. full backup images of a system that is secure, encrypted, and archived for system recovery
B. virtual machine images that are preconfigured to meet security standards
C. incremental backups of a system configuration and setup used for system recovery
D. secure "golden" images used to set up software on network laptops and desktops

Answer: B
Explanation:
Hardened images are preconfigured system or virtual machine images that have been secured according to established security standards and best practices, reducing vulnerabilities before deployment.

QUESTION 4
What is a core limitation of Network Intrusion Detection Systems?

A. IDS needs tuning after it is installed in the infrastructure.
B. IDS could block legitimate traffic and cause false positives.
C. IDS has a significant negative impact on bandwidth.
D. IDS cannot detect threats in encrypted data.

Answer: D
Explanation:
Network IDS typically inspects packet contents, but encrypted traffic cannot be analyzed without decryption, limiting its ability to detect threats hidden within encrypted communications.

QUESTION 5
Drag and Drop Question

Drag and drop the cyber risk insurance concepts from the left onto their descriptions on the right.

Answer Area

network security	cyber risk insurance against cyber attacks and hacking attacks
theft and fraud	services necessary to assess whether a cyber attack has occurred and to stop an attack
forensic investigation	lost income from being unable to conduct business due to a cyber event
business interruption	destruction or loss of data result from a criminal or fraudulent cyber event

Answer:

Answer Area

network security	network security
theft and fraud	forensic investigation
forensic investigation	business interruption
business interruption	theft and fraud

QUESTION 6
In a scenario where a large healthcare provider is revamping its cybersecurity strategy, it faces potential risks from sophisticated cyber threats like targeted ransomware, insider threats, and patient data breaches. The network includes diverse digital health records, interconnected medical devices, and remote patient portals. Which approach should be adopted for a risk analysis considering the provider's complex assets, varied vulnerabilities, and the severe threat landscape?

A. Limit analysis to prevalent threats, overlooking specific system or device risks.
B. Perform a general health sector risk review, not tailored to the provider's unique profile.
C. Map ransomware and insider threat patterns to EHR systems and device vulnerabilities.
D. Focus on high-cost medical equipment, assuming baseline security for digital records.

Answer: C
Explanation:
Mapping specific threat patterns such as ransomware and insider threats to critical assets like EHR systems and medical devices enables a tailored and comprehensive risk analysis that reflects the organization’s unique environment and threat landscape.

QUESTION 7
A new threat was discovered that is distributed with legitimate software across the internet. Management asked for an organizational risk assessment to understand the threat and impact. The asset management team provided a list of all the assets within the organization and an existing incident response plan. Which two elements does the asset management team need to conduct the risk assessment? (Choose two.)

A. list of assets affected by the vulnerability within the organization
B. business-critical assets and services
C. likelihood and severity of occurrence for the vulnerability
D. threat modeling and countermeasures approved by my senior management
E. revised incident response plan for the newly discovered vulnerability

Answer: BC
Explanation:
Risk assessment requires identifying business-critical assets and services to understand impact, along with evaluating the likelihood and severity of the vulnerability to determine overall risk and prioritize mitigation.

QUESTION 8
An organization is conducting a vulnerability triage and risk analysis. The security team wants to prioritize vulnerabilities effectively using industry scoring systems. Which method should the team use to ensure a thorough assessment?

A. Use the CVSS base score and correlate with the number of network vulnerabilities found.
B. Assign a CVSS environmental score and analyze historical exploitation trend data.
C. Calculate the CVSS base score and integrate asset criticality and threat intelligence insights.
D. Determine the CVSS temporal score and focus on immediate patch deployment decisions.

Answer: C
Explanation:
Combining the CVSS base score with asset criticality and threat intelligence provides a contextualized risk assessment, enabling accurate prioritization based on both severity and business impact.

QUESTION 9
A global financial organization is conducting a risk analysis for their critical database server, which hosts sensitive customer information, PII, and financial transactions. The server operates within a hybrid cloud environment, connecting with third-party services for data sharing, while maintaining stringent compliance with financial regulations like PCI-DSS. Recently, the organization faced a breach attempt on its cloud infrastructure, which exposed potential vulnerabilities in its external communication channels. As part of the risk analysis, the team must prioritize security risks that could lead to unauthorized access, data breaches, or noncompliance penalties. Which combination of factors should the team prioritize to effectively identify and mitigate critical security risks?

A. exposure, third-party risk management, patch management, and regulatory compliance
B. data sensitivity, compliance with financial regulations, encryption protocols, and cloud configurations
C. human factors risk, control effectiveness risk, vulnerability management, and physical security risk
D. patch management, change management, user training, and legal and regulatory changes

Answer: B
Explanation:
Prioritizing data sensitivity, regulatory compliance, encryption, and secure cloud configurations directly addresses risks related to unauthorized access, data breaches, and compliance requirements in a hybrid cloud financial environment.

QUESTION 10
A cybersecurity team is building a cloud-based storage system in a multinational corporation. Which approaches should be undertaken, in line with the concept of "data at rest" to protect sensitive corporate data across multiple jurisdictions with varying data protection laws, while ensuring high availability and rapid access for global teams?

A. Enforce strict role-based access control systems for data in use, tailored to comply with the most stringent international data protection standards, and conduct regular internal audits.
B. Implement encryption standards like AES-256 for all stored data, conduct frequent key rotations, and use compliance measures adhering to the relevant local data protection laws.
C. Focus primarily on encrypting data transfers between global locations, using high-standard encryption protocols like SSL/TLS, which are in line with multiple global jurisdictions.
D. Segment data of each country into its own separate storage in line with GDPR and encrypt it using AES-4096, rotate keys frequently and ensure every company employee can access it.

Answer: B
Explanation:
Data at rest protection requires strong encryption of stored data, secure key management with rotation, and compliance with local regulations. This ensures confidentiality across jurisdictions while maintaining accessibility and availability.

QUESTION 11
A threat research lab is analyzing malware that employs polymorphic techniques to constantly modify its code structure. Which sequence of actions should the cybersecurity experts follow to gain a comprehensive understanding of it?

A. Analyze network, dissect code, and observe behavior.
B. Execute dynamic analysis, examine code, and check network.
C. Use dynamic analysis, inspect code, and assess network.
D. Perform static code analysis, multiple sandbox runs, and pattern identification.

Answer: D
Explanation:
Polymorphic malware continuously changes its code, making static signatures unreliable. Starting with static analysis provides an initial understanding, followed by multiple sandbox executions to observe different mutated variants. Pattern identification then enables analysts to detect consistent behavioral or structural traits across variants, which is essential for understanding polymorphic behavior comprehensively.

QUESTION 12
A SOC analyst detects malware that is destined for a Linux-based OS. After using fully automated tools, the analyst used automated inspection tools but also decides to examine the static properties of the suspicious file on a local Linux computer. The analyst wants to find information on the IP address, error messages, and comments of the file. Which step must the SOC analyst take next to find this information?

A. Examine the malware using antivirus scanners.
B. Examine the malware hash types.
C. Perform portable executable header analysis.
D. Perform malware string analysis.

Answer: D
Explanation:
String analysis extracts human-readable content embedded in a binary, such as IP addresses, error messages, and developer comments. This aligns directly with the requirement to inspect static properties of the file and identify readable indicators without executing the malware.

QUESTION 13
An engineer receives multiple events on the Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) showing that an "Unknown" file was detected and caused an incident alert to be triggered. The engineer must determine if this event is malware or a legitimate file. Which action must be taken to check the reputation of the file?

A. Deploy Cisco Secure Malware Analysis (ThreatGrid).
B. Upload the hash into Talos File Reputation Checker.
C. View the identifier of the triggered action in Cisco Secure Firewall Threat Defense Manager (Firepower Management Center).
D. Scan the file using Cisco Secure Endpoint (AMP) customer scan.

Answer: B
Explanation:
Checking the file reputation requires submitting the file hash to a reputation service. The Cisco Talos File Reputation Checker provides known intelligence about whether a file is malicious or benign based on global threat data, making it the correct method to verify the file's reputation quickly.

QUESTION 14
Refer to the exhibit. What is occurring within the exhibit?

```
<body topmargin="0" leftmargin="0" rightmargin="0" bottommargin="0" marginwidth="0"

<iframe src="http://xxxyyy135.cc:8080/index.php" width=135 height=101 style"visibility:hidden"></iframe>
```

A. A CSS script is forcing visitors to click ads and popups.
B. An unknown file is downloaded.
C. A malicious IFRAME is inside the HTML code.
D. A suspicious redirect occurs to another website with an insecure connection.

Answer: C
Explanation:
The HTML snippet shows an <iframe> element loading content from an external URL with its visibility set to hidden. This indicates a malicious iframe embedded in the page, commonly used to silently load harmful content or execute attacks without user awareness.

QUESTION 15
An engineer must mitigate a recent zero-day vulnerability affecting RDP service where an

attacker connects to a targeted system and sends crafted requests, followed by an arbitrary code execution. The organization's management does not want to disable RDP because several services are dependent on it. Which action must the engineer take?

A. Configure blocking modes for session hijacking violations.
B. Configure Network Level Authentication for Remote Desktop Services Connections.
C. Implement IDS to detect similar attacks in the future.
D. Configure MAC Address Consistency Check in an ARP Packet.

Answer: B
Explanation:
Enabling Network Level Authentication requires users to authenticate before establishing a full RDP session, reducing exposure to unauthenticated exploitation attempts such as crafted request attacks and mitigating the risk of remote code execution without disabling the service.

QUESTION 16
An organization's network infrastructure consists of four quiet rooms, two meeting rooms, and a diverse array of network-connected devices. A security engineer must enhance network protection by ensuring that employees have access to internal resources while restricting visitors' access to the internet only. Which type of network segmentation should the security engineer recommend?

A. multiple VPNs with strict access control policies
B. layered VLANs with 802.1X authentication
C. IPsec-based network isolation for each room
D. separate DMZs for employees and visitors

Answer: B
Explanation:
Using VLAN segmentation combined with 802.1X authentication enables dynamic network access control based on user identity. Employees can be placed into VLANs with access to internal resources, while visitors are assigned to restricted VLANs with internet-only access, providing effective and scalable segmentation within the same infrastructure.

QUESTION 17
An analyst is investigating a potentially malicious program. Static analysis showed suspicious header details, hashes, and strings embedded within the executable file. The analyst cannot determine the indicators of compromise and other file characteristics. Which set of steps should an analyst take next?

A. Analyze the static properties of the file as a part of the incident triage effort, summarize the results, and report to management that the file is suspicious, but indicators of compromise were not defined.
B. Analyze the program in antivirus engines and compare the file to the known malware to determine the attack vector of the file and define its attributes.
C. Perform interactive behavior analysis to understand how the file uses memory and connectivity to reveal behavioral characteristics.
D. Use a limited guest account and production environment to determine the connectivity to reveal if the file uses the host as a command-and-control server.

Answer: C
Explanation:

When static analysis is inconclusive, the next step is dynamic or behavioral analysis. Interactive behavior analysis allows the analyst to observe how the program executes, interacts with memory, and communicates over the network, which helps uncover indicators of compromise and hidden malicious characteristics.

QUESTION 18
An organization had a recent breach with a man-in-the-middle attack. Attackers were able to intercept traffic and steal customer's data. The organization has asked a security engineer to make its systems better at stopping similar attacks from happening in the future. What recommendations should the security engineer provide to enhance security and protect against future man-in-the-middle attacks?

A. Configure a secure cookie attribute.
B. Implement HTTP authentication.
C. Implement session timeouts.
D. Configure the HTTP Strict Transport Security.

Answer: D
Explanation:
HTTP Strict Transport Security enforces the use of HTTPS by preventing browsers from connecting over insecure HTTP. This protects against man-in-the-middle attacks by ensuring encrypted communication and eliminating protocol downgrade opportunities.

QUESTION 19
An engineer is analyzing a case of an employee receiving a seemingly trustworthy email that included a link to a management feedback request. The employee opened the link and was redirected to a malicious website that downloaded ransomware and encrypted files onto their computer. Which security product would have prevented this attack?

A. network security solution
B. intrusion detection system
C. email security solution
D. intrusion prevention system

Answer: C
Explanation:
An email security solution analyzes inbound messages, detects phishing attempts, and blocks malicious links or attachments before they reach the user, preventing the initial compromise that led to the ransomware infection.

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**