



CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and It has continues to evade detection. Which of the following should administrator implement to protect the environment from this malware?

- A. Install a definition-based antivirus.
- B. Implement an IDS/IPS
- C. Implement a heuristic behavior-detection solution.
- D. Implement CASB to protect the network shares.

Answer: C

NEW QUESTION 2

A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

- A. CVE
- B. SIEM
- C. SOAR
- D. CVSS

Answer: D

NEW QUESTION 3

The concept of connecting a user account across the systems of multiple enterprises is BEST known as:

- A. federation.
- B. a remote access policy.
- C. multifactor authentication.
- D. single sign-on.

Answer: D

NEW QUESTION 4

In which of the following risk management strategies would cybersecurity insurance be used?

- A. Transference
- B. Avoidance
- C. Acceptance
- D. Mitigation

Answer: A

NEW QUESTION 5

A desktop support technician recently installed a new document-scanning software program on a computer However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

- A. A new firewall rule is needed to access the application.
- B. The system was quarantined for missing software updates
- C. The software was not added to the application whitelist.
- D. The system was isolated from the network due to infected software.

Answer: C

NEW QUESTION 6

A security analyst is configuring a large number of new company-issued laptops. The analyst received the following requirements:

- The devices will be used internationally by staff who travel extensively.
- Occasional personal use is acceptable due to the travel requirements.
- Users must be able to install and configure sanctioned programs and productivity suites.
- The devices must be encrypted
- The devices must be capable of operating in low-bandwidth environments.

Which of the following would provide the GREATEST benefit to the security posture of the devices?

- A. Configuring an always-on VPN
- B. Implementing application whitelisting
- C. Requiring web traffic to pass through the on-premises content filter
- D. Setting the antivirus DAT update schedule to weekly

Answer: A

NEW QUESTION 7

A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string Which of the following would be BEST to use to accomplish the task? (Select TWO).

- A. head
- B. Tcpdump
- C. grep
- D. rail
- E. curl
- F. openssi
- G. dd

Answer: AB

NEW QUESTION 8

Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

- A. An ARO
- B. An MOU
- C. An SLA
- D. A BPA

Answer: B

NEW QUESTION 9

An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner's account. Which of the following would be BEST to minimize this risk?

- A. Require a complex, eight-character password that is updated every 90 days.
- B. Perform only non-intrusive scans of workstations.
- C. Use non-credentialed scans against high-risk servers.
- D. Log and alert on unusual scanner account logon times.

Answer: D

NEW QUESTION 10

A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control. Which of the following BEST describes this process?

- A. Continuous delivery
- B. Continuous integration
- C. Continuous validation
- D. Continuous monitoring

Answer: B

NEW QUESTION 10

Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic. Which of the following attacks is MOST likely occurring?

- A. DDoS
- B. Man-in-the-middle
- C. MAC flooding
- D. Domain hijacking

Answer: A

NEW QUESTION 13

An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:

- A. business continuity plan
- B. communications plan.
- C. disaster recovery plan.
- D. continuity of operations plan

Answer: C

NEW QUESTION 18

A security analyst is investigating a vulnerability in which a default file permission was set incorrectly. The company uses non-credentialed scanning for vulnerability management.

Which of the following tools can the analyst use to verify the permissions?

- A. ssh
- B. chmod
- C. 1s
- D. setuid
- E. nessus
- F. nc

Answer: B

NEW QUESTION 21

A smart retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:

* Protection from power outages

* Always-available connectivity In case of an outage

The owner has decided to implement battery backups for the computer equipment Which of the following would BEST fulfill the owner's second need?

A. Lease a point-to-point circuit to provide dedicated access.

B. Connect the business router to its own dedicated UPS.

C. Purchase services from a cloud provider for high availabilityD Replace the business's wired network with a wireless network.

Answer: C

NEW QUESTION 25

A500 is implementing an insider threat detection program, The primary concern is that users may be accessing confidential data without authorization. Which of the following should be deployed to detect a potential insider threat?

A. A honeypot

B. A DMZ

C. ULF

D. File integrity monitoring

Answer: A

NEW QUESTION 29

A security manager for a retailer needs to reduce the scope of a project to comply with PCI DSS. The PCI data is located in different offices than where credit cards are accepted. All the offices are connected via MPLS back to the primary datacenter. Which of the following should the security manager implement to achieve the objective?

A. Segmentation

B. Containment

C. Geofencing

D. Isolation

Answer: A

NEW QUESTION 30

To reduce costs and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would BEST meet the needs of the organization?

A. MaaS

B. IaaS

C. SaaS

D. PaaS

Answer: D

NEW QUESTION 34

A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

A. IPSec

B. Always On

C. Split tunneling

D. L2TP

Answer: B

NEW QUESTION 39

An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?

A. Date of birth

B. Fingerprints

C. PIN

D. TPM

Answer: B

NEW QUESTION 40

Which of the following often operates in a client-server architecture to act as a service repository, providing enterprise consumers access to structured threat intelligence data?

- A. STIX
- B. CIRT
- C. OSINT
- D. TAXII

Answer: B

NEW QUESTION 41

Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

- A. DLP
- B. HIDS
- C. EDR
- D. NIPS

Answer: C

NEW QUESTION 44

A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

- A. perform attribution to specific APTs and nation-state actors.
- B. anonymize any PII that is observed within the IoC data.
- C. add metadata to track the utilization of threat intelligence reports.
- D. assist companies with impact assessments based on the observed data.

Answer: B

NEW QUESTION 45

After entering a username and password, an administrator must gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

- A. Multifactor authentication
- B. Something you can do
- C. Biometric
- D. Two-factor authentication

Answer: D

NEW QUESTION 50

While reviewing the wireless router, the systems administrator of a small business determines someone is spoofing the MAC address of an authorized device. Given the table below:

Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administrator's NEXT step to detect if there is a rogue system without impacting availability?

- A. Conduct a ping sweep.
- B. Physically check each system.
- C. Deny Internet access to the "UNKNOWN" hostname.
- D. Apply MAC filtering.

Answer: D

NEW QUESTION 52

A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

- A. Security information and event management
- B. A web application firewall
- C. A vulnerability scanner
- D. A next-generation firewall

Answer: A

NEW QUESTION 53

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

INSTRUCTIONS

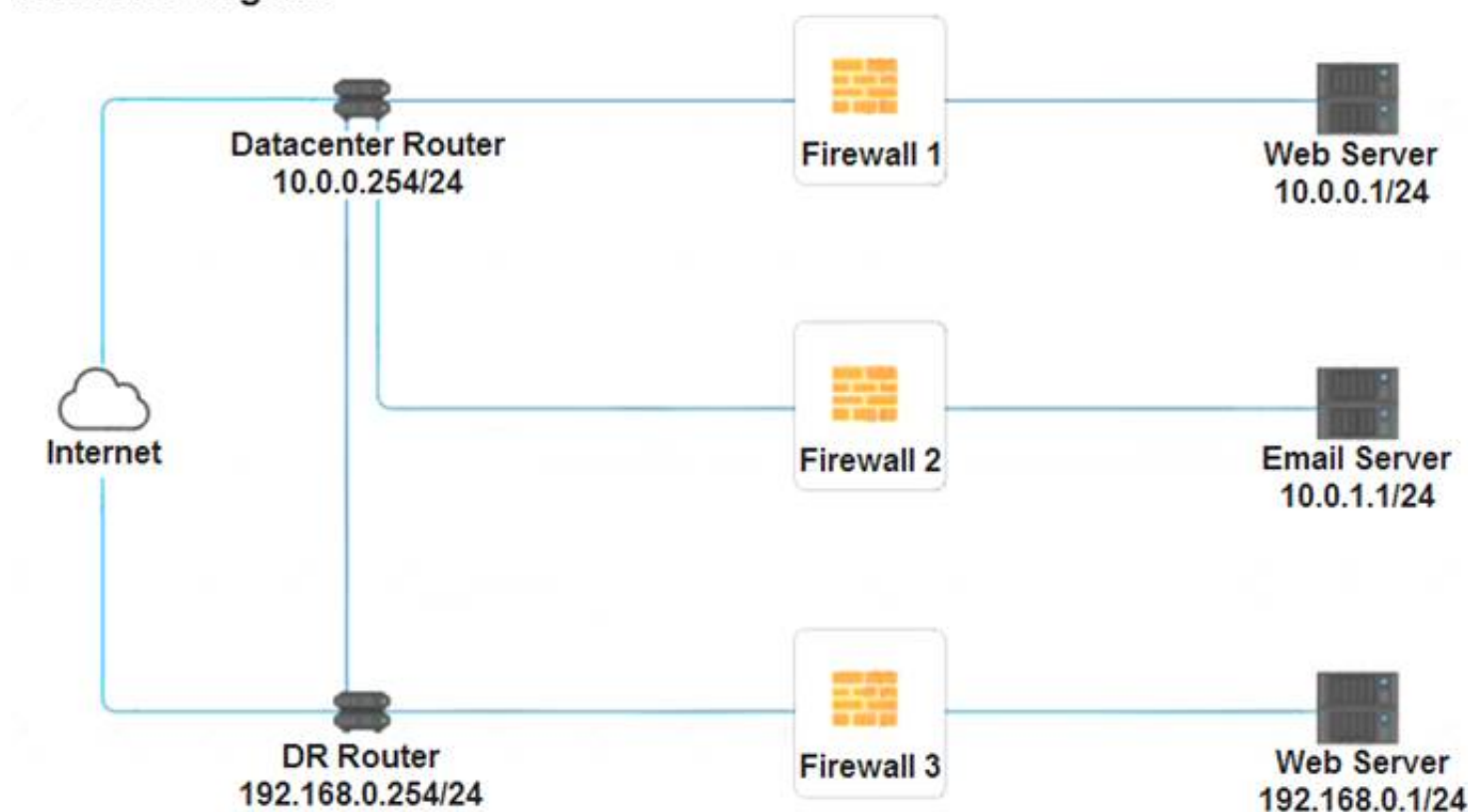
Click on each firewall to do the following:

- Deny cleartext web traffic.
- Ensure secure management protocols are used.
- Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram



Firewall 1

Rule Name	Source	Destination	Service	Action
DNS Rule	<div> <div>▼</div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div>▼</div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div>▼</div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div> <div>▼</div> <div> PERMIT DENY </div> </div>
HTTPS Outbound	<div> <div>▼</div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div>▼</div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div>▼</div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div> <div>▼</div> <div> PERMIT DENY </div> </div>
Management	<div> <div>▼</div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div>▼</div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div>▼</div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div> <div>▼</div> <div> PERMIT DENY </div> </div>
HTTPS Inbound	<div> <div>▼</div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div>▼</div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div>▼</div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div> <div>▼</div> <div> PERMIT DENY </div> </div>
HTTP Inbound	<div> <div>▼</div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div>▼</div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div> <div>▼</div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div> <div>▼</div> <div> PERMIT DENY </div> </div>

Reset Answer
Save
Close

Firewall 3 ✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> PERMIT DENY </div> </div>
HTTPS Outbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> PERMIT DENY </div> </div>
Management	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> PERMIT DENY </div> </div>
HTTPS Inbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> PERMIT DENY </div> </div>
HTTP Inbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div> PERMIT DENY </div> </div>

Reset Answer
Save
Close

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Firewall 1:

Firewall 1 ✕

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	10.0.0.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 10.0.0.1/24	• SSH	• PERMIT
HTTPS Inbound	ANY	• 10.0.0.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 10.0.0.1/24	• HTTP	• DENY

Reset Answer
Save
Close

Firewall 1				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY

Reset Answer Save Close

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

Firewall 2:

Firewall 2				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Reset Answer Save Close

Firewall 2				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Reset Answer Save Close

Firewall 3:

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	192.168.0.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 192.168.0.1/24	• SSH	• PERMIT
HTTPS Inbound	ANY	• 192.168.0.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 192.168.0.1/24	• HTTP	• DENY

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	192.168.0.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 192.168.0.1/24	• SSH	• PERMIT
HTTPS Inbound	ANY	• 192.168.0.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 192.168.0.1/24	• HTTP	• DENY

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

NEW QUESTION 54

A company is concerned about its security after a red-team exercise. The report shows the team was able to reach the critical servers due to the SMB being exposed to the Internet and running NTLMV1. Which of the following BEST explains the findings?

- A. Default settings on the servers
- B. Unsecured administrator accounts
- C. Open ports and services
- D. Weak Data encryption

Answer: C

NEW QUESTION 59

A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

- A. Default system configuration
- B. Unsecure protocols
- C. Lack of vendor support
- D. Weak encryption

Answer: B

NEW QUESTION 64

A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic. Which of the following should the analyst use?

- A. openssl
- B. hping
- C. netcat
- D. tcpdump

Answer: A

NEW QUESTION 68

A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?

- A. Developing an incident response plan
- B. Building a disaster recovery plan
- C. Conducting a tabletop exercise
- D. Running a simulation exercise

Answer: C

NEW QUESTION 71

In which of the following situations would it be BEST to use a detective control type for mitigation?

- A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
- B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
- C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
- D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
- E. A company purchased liability insurance for flood protection on all capital assets.

Answer: D

NEW QUESTION 74

A nationwide company is experiencing unauthorized logins at all hours of the day. The logins appear to originate from countries in which the company has no employees. Which of the following controls should the company consider using as part of its IAM strategy? (Select TWO).

- A. A complex password policy
- B. Geolocation
- C. An impossible travel policy
- D. Self-service password reset
- E. Geofencing
- F. Time-based logins

Answer: AB

NEW QUESTION 76

An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

- A. Voice
- B. Gait
- C. Vein
- D. Facial
- E. Retina
- F. Fingerprint

Answer: BD

NEW QUESTION 81

An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?

- A. The theft of portable electronic devices
- B. Geotagging in the metadata of images
- C. Bluesnarfing of mobile devices
- D. Data exfiltration over a mobile hotspot

Answer: D

NEW QUESTION 82

An incident, which is affecting dozens of systems, involves malware that reaches out to an Internet service for rules and updates. The IP addresses for the Internet host appear to be different in each case. The organization would like to determine a common IoC to support response and recovery actions. Which of the following sources of information would BEST support this solution?

- A. Web log files
- B. Browser cache
- C. DNS query logs
- D. Antivirus

Answer: C

NEW QUESTION 86

To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

- A. A password reuse policy
- B. Account lockout after three failed attempts

- C. Encrypted credentials in transit
- D. A geofencing policy based on login history

Answer: C

NEW QUESTION 87

During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

- A. 1a
- B. chflags
- C. chmod
- D. leof
- E. setuid

Answer: D

NEW QUESTION 90

A financial analyst has been accused of violating the company's AUP and there is forensic evidence to substantiate the allegation. Which of the following would dispute the analyst's claim of innocence?

- A. Legal hold
- B. Order of volatility
- C. Non-repudiation
- D. Chain of custody

Answer: D

NEW QUESTION 94

A cloud administrator is configuring five compute instances under the same subnet in a VPC. Three instances are required to communicate with one another, and the other two must be logically isolated from all other instances in the VPC. Which of the following must the administrator configure to meet this requirement?

- A. One security group
- B. Two security groups
- C. Three security groups
- D. Five security groups

Answer: B

NEW QUESTION 99

A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

- A. Implement open PSK on the APs
- B. Deploy a WAF
- C. Configure WIPS on the APs
- D. Install a captive portal

Answer: D

NEW QUESTION 104

A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plain text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

- A. Create DLP controls that prevent documents from leaving the network
- B. Implement salting and hashing
- C. Configure the web content filter to block access to the forum.
- D. Increase password complexity requirements

Answer: A

NEW QUESTION 105

A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select TWO).

- A. The order of volatility
- B. A checksum
- C. The location of the artifacts
- D. The vendor's name
- E. The date and time
- F. A warning banner

Answer: AE

NEW QUESTION 107

An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

- A. It allows for the sharing of digital forensics data across organizations
- B. It provides insurance in case of a data breach
- C. It provides complimentary training and certification resources to IT security staff.
- D. It certifies the organization can work with foreign entities that require a security clearance
- E. It assures customers that the organization meets security standards

Answer: E

NEW QUESTION 112

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned if servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

- A. 135
- B. 139
- C. 143
- D. 161
- E. 443
- F. 445

Answer: BF

NEW QUESTION 114

An organization has implemented a two-step verification process to protect user access to data that is stored in the cloud. Each employee now uses an email address of mobile number a code to access the data. Which of the following authentication methods did the organization implement?

- A. Token key
- B. Static code
- C. Push notification
- D. HOTP

Answer: A

NEW QUESTION 118

A security analyst must determine if either SSH or Telnet is being used to log in to servers. Which of the following should the analyst use?

- A. logger
- B. Metasploit
- C. tcpdump
- D. netstat

Answer: D

NEW QUESTION 123

The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going to the polls. This is an example of:

- A. prebending.
- B. an influence campaign
- C. a watering-hole attack
- D. intimidation
- E. information elicitation

Answer: D

NEW QUESTION 125

Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

- A. SaaS
- B. PaaS
- C. IaaS
- D. DaaS

Answer: C

NEW QUESTION 130

A hospital's administration is concerned about a potential loss of patient data that is stored on tablets. A security administrator needs to implement controls to alert the SOC any time the devices are near exits. Which of the following would BEST achieve this objective?

- A. Geotargeting
- B. Geolocation
- C. Geotagging
- D. Geofencing

Answer: D

NEW QUESTION 133

Which of the following is the correct order of volatility from MOST to LEAST volatile?

- A. Memory, temporary filesystems, routing tables, disk, network storage
- B. Cache, memory, temporary filesystems, disk, archival media
- C. Memory, disk, temporary filesystems, cache, archival media
- D. Cache, disk, temporary filesystems, network storage, archival media

Answer: B

NEW QUESTION 137

A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?

- A. FDE
- B. NIDS
- C. EDR
- D. DLP

Answer: C

NEW QUESTION 141

A security engineer is reviewing log files after a third discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

- A. Man-in- the middle
- B. Spear-phishing
- C. Evil twin
- D. DNS poisoning

Answer: D

NEW QUESTION 142

A security administrator needs to create a RAIS configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drivers will fail simultaneously. Which of the following RAID configurations should the administration use?

- A. RAID 0
- B. RAID 1
- C. RAID 5
- D. RAID 10

Answer: C

NEW QUESTION 146

A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?

- A. A packet capture
- B. A user behavior analysis
- C. Threat hunting
- D. Credentialed vulnerability scanning

Answer: C

NEW QUESTION 151

An organization relies on third-party video conferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources. Which of the following would BEST maintain high-quality video conferencing while minimizing latency when connected to the VPN?

- A. Using geographic diversity to have VPN terminators closer to end users
- B. Utilizing split tunneling so only traffic for corporate resources is encrypted
- C. Purchasing higher-bandwidth connections to meet the increased demand
- D. Configuring QoS properly on the VPN accelerators

Answer: D

NEW QUESTION 155

Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

- A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
- B. The document is a backup file if the system needs to be recovered.
- C. The document is a standard file that the OS needs to verify the login credentials.
- D. The document is a keylogger that stores all keystrokes should the account be compromised.

Answer: A

NEW QUESTION 157

Which of the following is a reason why an organization would define an AUP?

- A. To define the lowest level of privileges needed for access and use of the organization's resources
- B. To define the set of rules and behaviors for users of the organization's IT systems
- C. To define the intended partnership between two organizations
- D. To define the availability and reliability characteristics between an IT provider and consumer

Answer: B

NEW QUESTION 159

A security analyst is performing a forensic investigation compromised account credentials. Using the Event Viewer, the analyst able to detect the following message, "Special privileges assigned to new login." Several of these messages did not have a valid logon associated with the user before these privileges were assigned. Which of the following attacks is MOST likely being detected?

- A. Pass-the-hash
- B. Buffer overflow
- C. Cross-site scripting
- D. Session replay

Answer: A

NEW QUESTION 160

A security assessment determines DES and 3DES at still being used on recently deployed production servers. Which of the following did the assessment identify?

- A. Unsecme protocols
- B. Default settings
- C. Open permissions
- D. Weak encryption

Answer: D

NEW QUESTION 162

Accompany deployed a WiFi access point in a public area and wants to harden the configuration to make it more secure. After performing an assessment, an analyst identifies that the access point is configured to use WPA3, AES, WPS, and RADIUS. Which of the following should the analyst disable to enhance the access point security?

- A. WPA3
- B. AES
- C. RADIUS
- D. WPS

Answer: D

NEW QUESTION 164

A retail company that is launching a new website to showcase the company's product line and other information for online shoppers registered the following URLs:

- www.companysite.com
- shop.companysite.com
- about-us.companysite.com
- contact-us.companysite.com
- secure-logon.companysite.com

Which of the following should the company use to secure its website if the company is concerned with convenience and cost?

- A. A self-signed certificate
- B. A root certificate
- C. A code-signing certificate
- D. A wildcard certificate
- E. An extended validation certificate

Answer: B

NEW QUESTION 167

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

- Check-in/checkout of credentials
- The ability to use but not know the password
- Automated password changes
- Logging of access to credentials

Which of the following solutions would meet the requirements?

- A. OAuth 2.0
- B. Secure Enclave
- C. A privileged access management system
- D. An OpenID Connect authentication system

Answer: D

NEW QUESTION 171

A security modern may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO) A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

- A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
- B. Connect a write blocker to the hard drive Then leveraging a forensic workstation, utilize the dd command m a live Linux environment to create a duplicate copy
- C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
- D. Refrain from completing a forensic analysts of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence

Answer: D

NEW QUESTION 172

A network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on-site customer support. Which of the following should the administrator employ to meet these criteria?

- A. Implement NAC.
- B. Implement an SWG.
- C. Implement a URL filter.
- D. Implement an MDM.

Answer: B

NEW QUESTION 174

A company has been experiencing very brief power outages from its utility company over the last few months. These outages only last for one second each time. The utility company is aware of the issue and is working to replace a faulty transformer. Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?

- A. Dual power supplies
- B. A UPS
- C. A generator
- D. APDU

Answer: B

NEW QUESTION 176

A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

- A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis
- B. Restrict administrative privileges and patch ail systems and applications.
- C. Rebuild all workstations and install new antivirus software
- D. Implement application whitelisting and perform user application hardening

Answer: A

NEW QUESTION 178

An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?

- A. HSM
- B. CASB
- C. TPM
- D. DLP

Answer: A

NEW QUESTION 183

A manufacturer creates designs for very high security products that are required to be protected and controlled by the government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?

- A. An air gap
- B. A Faraday cage
- C. A shielded cable
- D. A demilitarized zone

Answer: A

NEW QUESTION 184

A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

- A. SIEM
- B. DLP
- C. CASB
- D. SWG

Answer: C

NEW QUESTION 188

Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employee's workstations. The security manager investigates but finds no signs of an attack on the perimeter firewall or the NIDS. Which of the following is MOST likely causing the malware alerts?

- A. A worm that has propagated itself across the intranet, which was initiated by presentation media
- B. A fileless virus that is contained on a vCard that is attempting to execute an attack
- C. A Trojan that has passed through and executed malicious code on the hosts
- D. A USB flash drive that is trying to run malicious code but is being blocked by the host firewall

Answer: A

NEW QUESTION 192

Following a prolonged datacenter outage that affected web-based sales, a company has decided to move its operations to a private cloud solution. The security team has received the following requirements:

- There must be visibility into how teams are using cloud-based services.
- The company must be able to identify when data related to payment cards is being sent to the cloud.
- Data must be available regardless of the end user's geographic location
- Administrators need a single pane-of-glass view into traffic and trends. Which of the following should the security analyst recommend?

- A. Create firewall rules to restrict traffic to other cloud service providers.
- B. Install a DLP solution to monitor data in transit.
- C. Implement a CASB solution.
- D. Configure a web-based content filter.

Answer: B

NEW QUESTION 196

A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file download from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control of the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker MOST likely use to gain access?

- A. A bot
- B. A fileless virus
- C. A logic bomb
- D. A RAT

Answer: D

NEW QUESTION 198

A financial institution would like to store its customer data and could but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

- A. Asymmetric
- B. Symmetric
- C. Homeomorphic
- D. Ephemeral

Answer: B

NEW QUESTION 203

An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain chain of custody?

- A. Document the collection and require a sign-off when possession changes.
- B. Lock the device in a safe or other secure location to prevent theft or alteration.
- C. Place the device in a Faraday cage to prevent corruption of the data.
- D. Record the collection in a blockchain-protected public ledger.

Answer: A

NEW QUESTION 204

An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has only been given the documentation available to the customers of the applications. Which of the following BEST represents the type of testing that will occur?

- A. Bug bounty
- B. Black-box
- C. Gray-box

D. White-box

Answer: A

NEW QUESTION 207

A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an item, the password for the wireless network is printed on the receipt so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?

- A. WPA-EAP
- B. WEP-TKIP
- C. WPA-PSK
- D. WPS-PIN

Answer: A

NEW QUESTION 210

After a ransomware attack a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. Which of the following will the company MOST likely review to trace this transaction?

- A. The public ledger
- B. The NetFlow data
- C. A checksum
- D. The event log

Answer: A

NEW QUESTION 211

A Chief Security Officer (CSO) is concerned about the amount of PII that is stored locally on each salesperson's laptop. The sales department has a higher-than-average rate of lost equipment. Which of the following recommendations would BEST address the CSO's concern?

- A. Deploy an MDM solution.
- B. Implement managed FDE.
- C. Replace all hard drives with SEDs.
- D. Install DLP agents on each laptop.

Answer: B

NEW QUESTION 215

Which of the following algorithms has the SMALLEST key size?

- A. DES
- B. Twofish
- C. RSA
- D. AES

Answer: B

NEW QUESTION 220

A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company. Which of the following solutions will BEST meet these requirements?

- A. An NGFW
- B. A CASB
- C. Application whitelisting
- D. An NG-SWG

Answer: B

NEW QUESTION 225

A external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will BEST assist with this investigation?

- A. Perform a vulnerability scan to identify the weak spots.
- B. Use a packet analyzer to investigate the NetFlow traffic.
- C. Check the SIEM to review the correlated logs.
- D. Require access to the routers to view current sessions.

Answer: C

NEW QUESTION 227

Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

- A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.
- B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.
- C. Malware trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox
- D. Routing tables have been compromised, and an attacker is rerouting traffic to malicious websites

Answer: D

NEW QUESTION 229

A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

- A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
- B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
- C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
- D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

Answer: D

NEW QUESTION 233

An attacker has successfully exfiltrated several non-salted password hashes from an online system. Given the logs below:

```
Session           : hashcat
Status            : cracked
Hash.Type         : MD5
Hash.Target       : b3b81d1b7a412bf5aab3a507d0a586a0
Time.Started      : Fri Mar 10 10:18:45 2020
Recovered         : 1/1 (100%) Digests
Progress          : 28756845 / 450365879 (6.38%) hashes
Time.Stopped      : Fri Mar 10 10:20:12 2020
Password found    : Th3B3stP@55w0rd!
```

Which of the following BEST describes the type of password attack the attacker is performing?

- A. Dictionary
- B. Pass-the-hash
- C. Brute-force
- D. Password spraying

Answer: A

NEW QUESTION 234

An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:

```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows\INetCache\IE\pdfdocx.msi
Connection Details: 35.242.219.204:80
```

Which of the following is the MOST likely cause of the issue?

- A. The end user purchased and installed a PUP from a web browser
- B. A bot on the computer is brute forcing passwords against a website
- C. A hacker is attempting to exfiltrate sensitive data
- D. Ransomware is communicating with a command-and-control server.

Answer: A

NEW QUESTION 238

A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?

- A. Monitoring large data transfer transactions in the firewall logs
- B. Developing mandatory training to educate employees about the removable media policy
- C. Implementing a group policy to block user access to system files
- D. Blocking removable-media devices and write capabilities using a host-based security tool

Answer: D

NEW QUESTION 243

A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

- A. Corrective
- B. Physical
- C. Detective
- D. Administrative

Answer: C

NEW QUESTION 248

In which of the following common use cases would steganography be employed?

- A. Obfuscation
- B. Integrity
- C. Non-repudiation
- D. Blockchain

Answer: A

NEW QUESTION 253

A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

- A. Code signing
- B. Fuzzing
- C. Manual code review
- D. Dynamic code analysis

Answer: D

NEW QUESTION 258

An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business. The Chief Information Officer (CIO) is wondering if the organization may need to scale down just as quickly as it scaled up. The CIO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the CIO's concerns?

- A. Disallow new hires from using mobile devices for six months
- B. Select four devices for the sales department to use in a CYOD model
- C. Implement BYOD for the sales department while leveraging the MDM
- D. Deploy mobile devices using the COPE methodology

Answer: C

NEW QUESTION 260

A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money: Which of the following types of attack is MOST likely being conducted?

- A. SQLi
- B. CSRF
- C. Session replay
- D. API

Answer: C

NEW QUESTION 263

The process of passively gathering information prior to launching a cyberattack is called:

- A. tailgating
- B. reconnaissance
- C. pharming
- D. prepending

Answer: B

NEW QUESTION 264

A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

- A. Mobile device management
- B. Full-device encryption
- C. Remote wipe
- D. Biometrics

Answer: A

NEW QUESTION 265

A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

- A. DDoS attack
- B. Memory leak
- C. Buffer overflow
- D. Resource exhaustion

Answer: D

NEW QUESTION 269

An attacker is attempting, to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a random username and password. the logon screen displays the following message:
 Which of the following should the analyst recommend be enabled?

- A. Input validation
- B. Obfuscation
- C. Error handling
- D. Username lockout

Answer: B

NEW QUESTION 274

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS

Not all attacks and remediation actions will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources	Web server	<div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing </div>	<div> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services </div>
The attack establishes a connection, which allows remote commands to be executed.	User	<div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing </div>	<div> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services </div>
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network	Database server	<div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing </div>	<div> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services </div>
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	<div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing </div>	<div> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services </div>
The attacker embeds hidden access in an internally developed application that bypasses account login	Application	<div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing </div>	<div> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services </div>

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

NEW QUESTION 276

A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

- A. Configure the DLP policies to allow all PII
- B. Configure the firewall to allow all ports that are used by this application
- C. Configure the antivirus software to allow the application
- D. Configure the DLP policies to whitelist this application with the specific PII
- E. Configure the application to encrypt the PII

Answer: D

NEW QUESTION 279

A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

- A. Key escrow
- B. A self-signed certificate
- C. Certificate chaining
- D. An extended validation certificate

Answer: B

NEW QUESTION 280

A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

- A. The GPS location
- B. When the file was deleted
- C. The total number of print jobs
- D. The number of copies made

Answer: A

NEW QUESTION 283

A company wants to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy to implement?

- A. Incremental backups followed by differential backups
- B. Full backups followed by incremental backups
- C. Delta backups followed by differential backups
- D. Incremental backups followed by delta backups
- E. Full backups followed by differential backups

Answer: B

NEW QUESTION 285

Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?

- A. MSSP
- B. Public cloud
- C. Hybrid cloud
- D. Fog computing

Answer: C

NEW QUESTION 287

A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen. Which of the following would BEST meet these requirements? (Select TWO).

- A. Full-device encryption
- B. Network usage rules
- C. Geofencing
- D. Containerization
- E. Application whitelisting
- F. Remote control

Answer: AB

NEW QUESTION 290

After a phishing scam for a user's credentials, the red team was able to craft a payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session. Which of the following types of attacks has occurred?

- A. Privilege escalation
- B. Session replay
- C. Application programming interface
- D. Directory traversal

Answer: A

NEW QUESTION 293

A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

- A. CASB
- B. SWG
- C. Containerization
- D. Automated failover

Answer: C

NEW QUESTION 295

An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?

- A. Screen locks
- B. Application management
- C. Geofencing
- D. Containerization

Answer: D

NEW QUESTION 296

An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker MOST likely attempting?

- A. A spear-phishing attack
- B. A watering-hole attack
- C. Typo squatting
- D. A phishing attack

Answer: B

NEW QUESTION 301

A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following scan Types would produce the BEST vulnerability scan report?

- A. Port
- B. Intrusive
- C. Host discovery
- D. Credentialed

Answer: D

NEW QUESTION 306

An organization just experienced a major cyberattack modern. The attack was well coordinated sophisticated and highly skilled. Which of the following targeted the organization?

- A. Shadow IT
- B. An insider threat
- C. A hacktivist
- D. An advanced persistent threat

Answer: D

NEW QUESTION 307

A company wants to deploy PKI on its Internet-facing website. The applications that are currently deployed are:

- www.company.com (main website)
- contactus.company.com (for locating a nearby location)
- quotes.company.com (for requesting a price quote)

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com. Which of the following certificate types would BEST meet the requirements?

- A. SAN
- B. Wildcard
- C. Extended validation
- D. Self-signed

Answer: B

NEW QUESTION 311

Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

- A. Block cipher
- B. Hashing
- C. Private key
- D. Perfect forward secrecy
- E. Salting
- F. Symmetric keys

Answer: BC

NEW QUESTION 312

A security engineer has enabled two-factor authentication on all workstations. Which of the following approaches are the MOST secure? (Select TWO).

- A. Password and security question
- B. Password and CAPTCHA
- C. Password and smart card
- D. Password and fingerprint
- E. Password and one-time token
- F. Password and voice

Answer: CD

NEW QUESTION 316

Which of the following types of controls is a turnstile?

- A. Physical
- B. Detective

- C. Corrective
- D. Technical

Answer: A

NEW QUESTION 319

A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

- A. SDP
- B. AAA
- C. IaaS
- D. MSSP
- E. Microservices

Answer: D

NEW QUESTION 324

A cybersecurity department purchased a new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?

- A. Randomize the shared credentials
- B. Use only guest accounts to connect.
- C. Use SSH keys and remove generic passwords
- D. Remove all user accounts.

Answer: C

NEW QUESTION 325

A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site. Upon investigation, a security analyst identifies the following:

- The legitimate website's IP address is 10.1.1.20 and eRecruit local resolves to the IP
 - The forged website's IP address appears to be 10.2.12.99, based on NetFlow records
 - All three at the organization's DNS servers show the website correctly resolves to the legitimate IP
 - DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.
- Which of the following MOST likely occurred?

- A. A reverse proxy was used to redirect network traffic
- B. An SSL strip MITM attack was performed
- C. An attacker temporarily pawned a name server
- D. An ARP poisoning attack was successfully executed

Answer: B

NEW QUESTION 330

Which of the following is the purpose of a risk register?

- A. To define the level of risk using probability and likelihood
- B. To register the risk with the required regulatory agencies
- C. To identify the risk, the risk owner, and the risk measures
- D. To formally log the type of risk mitigation strategy the organization is using

Answer: C

NEW QUESTION 333

A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

- A. A non-disclosure agreement
- B. Least privilege
- C. An acceptable use policy
- D. Offboarding

Answer: D

NEW QUESTION 335

A network manager is concerned that business may be negatively impacted if the firewall in its datacenter goes offline. The manager would like to implement a high availability pair to:

- A. decrease the mean time between failures
- B. remove the single point of failure
- C. cut down the mean time to repair
- D. reduce the recovery time objective

Answer: B

NEW QUESTION 340

A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that consumes database resources. Which of the following will the CISO MOST likely recommend to mitigate this risk?

- A. Upgrade the bandwidth available into the datacenter
- B. Implement a hot-site failover location
- C. Switch to a complete SaaS offering to customers
- D. Implement a challenge response test on all end-user queries

Answer: B

NEW QUESTION 343

The website <http://companywebsite.com> requires users to provide personal information including security responses, for registration. which of the following would MOST likely cause a data breach?

- A. LACK OF INPUT VALIDATION
- B. OPEN PERMISSIONS
- C. UNSECURE PROTOCOL
- D. MISSING PATCHES

Answer: A

NEW QUESTION 344

A security researcher is attempting to gather data on the widespread use of a Zero-day exploit. Which of the following will the researcher MOST likely use to capture this data?

- A. A DNS sinkhole
- B. A honeypot
- C. A vulnerability scan
- D. cvss

Answer: B

NEW QUESTION 347

An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

- A. `Hping3 -s comptia.org -p 80`
- B. `Nc -l -v comptia.org -p 80`
- C. `npm comptia.org -p 80 -aV`
- D. `nslookup -port=80 comptia.org`

Answer: C

NEW QUESTION 348

A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?

A)

```
http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>
```

B)

```
http://sample.url.com/someotherpageonsite/../../../../etc/shadow
```

C)

```
http://sample.url.com/select-from-database-where-password-null
```

D)

```
http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 350

A Chief Security Officer (CSO) was notified that a customer was able to access confidential internal company files on a commonly used file-sharing service. The

file-sharing service is the same one used by company staff as one of its approved third-party applications.

After further investigation, the security team determines the sharing of confidential files was accidental and not malicious. However, the CSO wants to implement changes to minimize this type of incident from reoccurring but does not want to impact existing business processes. Which of the following would BEST meet the CSO's objectives?

- A. DLP
- B. SWG
- C. CASB
- D. Virtual network segmentation
- E. Container security

Answer: A

NEW QUESTION 355

An organization is developing a plan in the event of a complete loss of critical systems and data. Which of the following plans is the organization MOST likely developing?

- A. Incident response
- B. Communications
- C. Disaster recovery
- D. Data retention

Answer: C

NEW QUESTION 360

While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

- A. A RAT was installed and is transferring additional exploit tools.
- B. The workstations are beaconing to a command-and-control server.
- C. A logic bomb was executed and is responsible for the data transfers.
- D. A fileless virus is spreading in the local network environment.

Answer: A

NEW QUESTION 362

A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).

- A. Something you know
- B. Something you have
- C. Somewhere you are
- D. Someone you are
- E. Something you are
- F. Something you can do

Answer: BE

NEW QUESTION 364

A symmetric encryption algorithm is BEST suited for:

- A. key-exchange scalability.
- B. protecting large amounts of data.
- C. providing hashing capabilities.
- D. implementing non-repudiation.

Answer: D

NEW QUESTION 369

An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls? (Select TWO).

- A. ISO
- B. PCI DSS
- C. SOC
- D. GDPR
- E. CSA
- F. NIST

Answer: BD

NEW QUESTION 371

When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

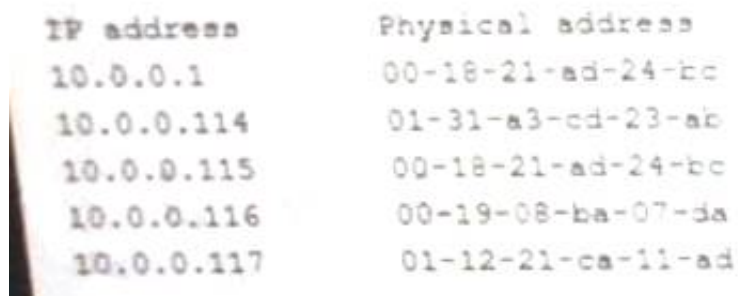
- A. Acceptance

- B. Mitigation
- C. Avoidance
- D. Transference

Answer: D

NEW QUESTION 372

A security analyst is investigating an incident that was first reported as an issue connecting to network shares and the internet. While reviewing logs and tool output, the analyst sees the following:



IP address	Physical address
10.0.0.1	00-18-21-ad-24-bc
10.0.0.114	01-31-a3-cd-23-ab
10.0.0.115	00-18-21-ad-24-bc
10.0.0.116	00-19-08-ba-07-da
10.0.0.117	01-12-21-ca-11-ad

Which of the following attacks has occurred?

- A. IP conflict
- B. Pass-the-hash
- C. MAC flooding
- D. Directory traversal
- E. ARP poisoning

Answer: E

NEW QUESTION 375

Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

- A. Risk matrix
- B. Risk tolerance
- C. Risk register
- D. Risk appetite

Answer: B

NEW QUESTION 377

A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. When of the following should the engineer implement?

- A. An air gap
- B. A hot site
- C. VLAN
- D. A screened subnet

Answer: D

NEW QUESTION 381

Users at organization have been installing programs from the internet on their workstations without first proper authorization. The organization maintains a portal from which users can install standardized programs. However, some users have administrative access on their workstations to enable legacy programs to function properly. Which of the following should the security administrator consider implementing to address this issue?

- A. Application code signing
- B. Application whitelisting
- C. Data loss prevention
- D. Web application firewalls

Answer: B

NEW QUESTION 384

A network administrator would like to configure a site-to-site VPN utilizing IPSec. The administrator wants the tunnel to be established with data integrity encryption, authentication and anti-replay functions. Which of the following should the administrator use when configuring the VPN?

- A. AH
- B. EDR
- C. ESP
- D. DNSSEC

Answer: C

NEW QUESTION 386

An organization recently recovered from a data breach. During the root cause analysis, the organization determined the source of the breach to be a personal cell phone that had been reported lost. Which of the following solutions should the organization implement to reduce the likelihood of future data breaches?

- A. MDM
- B. MAM
- C. VDI
- D. DLP

Answer: A

NEW QUESTION 387

A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?

- A. A captive portal
- B. PSK
- C. 802.1X
- D. WPS

Answer: C

NEW QUESTION 392

A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:

```
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
```

Which of the following BEST describes this kind of attack?

- A. Directory traversal
- B. SQL injection
- C. API
- D. Request forgery

Answer: D

NEW QUESTION 397

A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems. Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage. Which of the following is MOST likely the cause?

- A. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage.
- B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.
- C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
- D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.

Answer: D

NEW QUESTION 398

Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?

- A. The employee's physical access card was cloned.
- B. The employee is colluding with human resources
- C. The employee's biometrics were harvested
- D. A criminal used lock picking tools to open the door.

Answer: A

NEW QUESTION 401

When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

- A. Tokenization
- B. Data masking
- C. Normalization
- D. Obfuscation

Answer: C

NEW QUESTION 406

A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money that it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

- A. MTBF
- B. RPO
- C. RTO
- D. MTTR

Answer: C

NEW QUESTION 409

The cost of '©movable media and the security risks of transporting data have become too great for a laboratory. The laboratory has decided to interconnect with partner laboratones to make data transfers easier and more secure. The Chief Security Officer <CSO) has several concerns about proprietary data being exposed once the interconnections are established. Which of the following security features should the network administrator implement lo prevent unwanted data exposure to users in partner laboratories?

- A. VLAN zoning with a file-transfer server in an external-facing zone
- B. DLP running on hosts to prevent file transfers between networks
- C. NAC that permits only data-transfer agents to move data between networks
- D. VPN with full tunneling and NAS authenticating through the Active Directory

Answer: B

NEW QUESTION 414

The lessons-learned analysis from a recent incident reveals that an administrative office worker received a call from someone claiming to be from technical support. The caller convinced the office worker to visit a website, and then download and install a program masquerading as an antivirus package. The program was actually a backdoor that an attacker could later use to remote control the worker's PC. Which of the following would be BEST to help prevent this type of attack in the future?

- A. Data loss prevention
- B. Segmentation
- C. Application whitelisting
- D. Quarantine

Answer: C

NEW QUESTION 417

A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial option article in a national newspaper, which may result in new cyberattacks Which of the following would be BEST for the security manager to use in a threat mode?

- A. Hacktivists
- B. White-hat hackers
- C. Script kiddies
- D. Insider threats

Answer: A

NEW QUESTION 421

A worldwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

- A. Network location
- B. Impossible travel time
- C. Geolocation
- D. Geofencing

Answer: D

NEW QUESTION 423

A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

- A. Loss of proprietary information
- B. Damage to the company's reputation
- C. Social engineering
- D. Credential exposure

Answer: C

NEW QUESTION 428

A security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices the following requirements must be met:

- Mobile device OSs must be patched up to the latest release
 - A screen lock must be enabled (passcode or biometric)
 - Corporate data must be removed if the device is reported lost or stolen
- Which of the following controls should the security engineer configure? (Select TWO)

- A. Containerization
- B. Storage segmentation
- C. Posturing
- D. Remote wipe
- E. Full-device encryption
- F. Geofencing

Answer: DE

NEW QUESTION 432

A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN? (Select TWO).

- A. Due to foreign travel, the user's laptop was isolated from the network.
- B. The user's laptop was quarantined because it missed the latest patch update.
- C. The VPN client was blacklisted.
- D. The user's account was put on a legal hold.
- E. The laptop is still configured to connect to an international mobile network operator.
- F. The user is unable to authenticate because they are outside of the organization's mobile geofencing configuration.

Answer: AB

NEW QUESTION 437

A security administrator is analyzing the corporate wireless network. The network only has two access points running on channels 1 and 11. While using airodump-ng, the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access points. Which of the following attacks is happening on the corporate network?

- A. Man in the middle
- B. Evil twin
- C. Jamming
- D. Rogue access point
- E. Disassociation

Answer: B

NEW QUESTION 439

Which of the following types of controls is a CCTV camera that is not being monitored?

- A. Detective
- B. Deterrent
- C. Physical
- D. Preventive

Answer: B

NEW QUESTION 441

A security engineer needs to implement the following requirements:

- All Layer 2 switches should leverage Active Directory for authentication.
- All Layer 2 switches should use local fallback authentication if Active Directory is offline.
- All Layer 2 switches are not the same and are manufactured by several vendors.

Which of the following actions should the engineer take to meet these requirements? (Select TWO).

- A. Implement RADIUS.
- B. Configure AAA on the switch with local login as secondary.
- C. Configure port security on the switch with the secondary login method.
- D. Implement TACACS+.
- E. Enable the local firewall on the Active Directory server.
- F. Implement a DHCP server.

Answer: AB

NEW QUESTION 442

A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

- A. IP restrictions
- B. Multifactor authentication
- C. A banned password list
- D. A complex password policy

Answer: B

NEW QUESTION 444

A company has limited storage available and online presence that cannot for more than four hours. Which of the following backup methodologies should the company implement to allow for the FASTEST database restore time in the event of a failure, while being mindful of the limited available storage space?

- A. Implement full tape backup every Sunday at 8:00 p.m. and perform nightly tape rotations.
- B. Implement differential backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m.
- C. Implement nightly full backups every Sunday at 8:00 p.m.
- D. Implement full backups every Sunday at 8:00 p.m. and nightly differential backups at 8:00.

Answer: B

NEW QUESTION 446

A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager darned the reports were previously sent via email but then quickly generated and backdated the reports before submitting them via a new email message Which of the following actions MOST likely supports an investigation for fraudulent submission?

- A. Establish chain of custody
- B. Inspect the file metadata
- C. Reference the data retention policy
- D. Review the email event logs

Answer: D

NEW QUESTION 448

An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

- A. hping3 -S corstia.org -p 80
- B. nc —1 —v comptia.org -p 80
- C. nmap comptia.org -p 80 —sV
- D. nslookup -port=80 comptia.org

Answer: C

NEW QUESTION 449

A local coffee shop runs a small WiFi hot-spot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure. Which of the following technologies will the coffee shop MOST likely use in place of PSK?

- A. WEP
- B. MSCHAP
- C. WPS
- D. SAE

Answer: D

NEW QUESTION 454

A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?

- A. Due to foreign travel, the user's laptop was isolated from the network.
- B. The user's laptop was quarantined because it missed the latest path update.
- C. The VPN client was blacklisted.
- D. The user's account was put on a legal hold.

Answer: A

NEW QUESTION 458

Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

- A. Whaling
- B. Spam
- C. Invoice scam
- D. Pharming

Answer: A

NEW QUESTION 463

A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two- drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

- A. 1
- B. 5
- C. 6

Answer: B

NEW QUESTION 468

Which of the following is MOST likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

- A. An RTO report
- B. A risk register
- C. A business impact analysis
- D. An asset value register
- E. A disaster recovery plan

Answer:

B

NEW QUESTION 473

The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

- A. Install a NIDS device at the boundary.
- B. Segment the network with firewalls.
- C. Update all antivirus signatures daily.
- D. Implement application blacklisting.

Answer: B

NEW QUESTION 475

Which of the following will provide the BEST physical security countermeasures to stop intruders? (Select TWO.)

- A. Alarms
- B. Signage
- C. Lighting
- D. Mantraps
- E. Fencing
- F. Sensors

Answer: DE

NEW QUESTION 478

A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

- A. SPIM
- B. Vishing
- C. Spear phishing
- D. Smishing

Answer: D

NEW QUESTION 480

A company just developed a new web application for a government agency. The application must be assessed and authorized prior to being deployed. Which of the following is required to assess the vulnerabilities resident in the application?

- A. Repository transaction logs
- B. Common Vulnerabilities and Exposures
- C. Static code analysis
- D. Non-credentialed scans

Answer: C

NEW QUESTION 481

An attacker was easily able to log in to a company's security camera by performing a basic online search for a setup guide for that particular camera brand and model Which of the following BEST describes the configurations the attacker exploited?

- A. Weak encryption
- B. Unsecure protocols
- C. Default settings
- D. Open permissions

Answer: C

NEW QUESTION 482

An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes Which of the following is the 60-minute expectation an example of:

- A. MTBF
- B. RPO
- C. MTTR
- D. RTO

Answer: D

NEW QUESTION 486

A bank detects fraudulent activity on user's account. The user confirms transactions completed yesterday on the bank's website at <https://www.company.com>. A security analyst then examines the user's

Internet usage logs and observes the following output: date; username; url;destinationport; responsecode

2020-03-01; userann; http: //www.company.org/;80;302; userann: http://www.company.org/secure_login/;80;200 2020-03-01; userann:

<http://www.company.org/dashboard/;80;200>

Which of the following has MOST likely occurred?

- A. Replay attack
- B. SQL injection
- C. SSL stripping
- D. Race conditions

Answer: A

NEW QUESTION 490

A critical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following RAID levels meets this requirements?

- A. RAID 0+1
- B. RAID 2
- C. RAID 5
- D. RAID 6

Answer: C

NEW QUESTION 491

Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?

- A. Watering-hole attack
- B. Credential harvesting
- C. Hybrid warfare
- D. Pharming

Answer: A

NEW QUESTION 492

An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization MOST likely consult?

- A. The business continuity plan
- B. The disaster recovery plan
- C. The communications plan
- D. The incident response plan

Answer: A

NEW QUESTION 495

A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?

- A. AH
- B. ESP
- C. SRTP
- D. LDAP

Answer: B

NEW QUESTION 496

.....

Relate Links

100% Pass Your SY0-601 Exam with ExamBible Prep Materials

<https://www.exambible.com/SY0-601-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>