



CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam

NEW QUESTION 1

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 2

Which of the following describes the BEST approach for deploying application patches?

- A. Apply the patches to systems in a testing environment then to systems in a staging environment, and finally to production systems.
- B. Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems
- C. Test the patches in a test environment apply them to the production systems and then apply them to a staging environment
- D. Apply the patches to the production systems apply them in a staging environment, and then test all of them in a testing environment

Answer: A

NEW QUESTION 3

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 4

A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely the cause of the cause of the access issues?

- A. False rejection
- B. Cross-over error rate
- C. Efficacy rate
- D. Attestation

Answer: B

NEW QUESTION 5

A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?

- A. MSSP
- B. SOAR
- C. IaaS
- D. PaaS

Answer: B

NEW QUESTION 6

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 the identifies the following:

- The legitimate websites 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
- AH 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 7

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 8

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 9

A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?

- A. An external access point is engaging in an evil-twin attack.
- B. The signal on the WAP needs to be increased in that section of the building.
- C. The certificates have expired on the devices and need to be reinstalled.
- D. The users in that section of the building are on a VLAN that is being blocked by the firewall.

Answer: A

NEW QUESTION 10

A security administrator currently spends a large amount of time on common security tasks, such as report generation, phishing investigations, and user provisioning and deprovisioning. This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

- A. DAC
- B. ABAC
- C. SCAP
- D. SOAR

Answer: D

NEW QUESTION 10

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 15

A security analyst has received an alert about being sent via email. The analyst's Chief Information Security Officer (CISO) has made it clear that PII must be handled with extreme care. From which of the following did the alert MOST likely originate?

- A. S/MIME
- B. DLP
- C. IMAP
- D. HIDS

Answer: B

NEW QUESTION 17

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 21

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 25

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 26

A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

- A. Configure the perimeter firewall to deny inbound external connections to SMB ports.
- B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
- C. Deny unauthenticated users access to shared network folders.
- D. Verify computers are set to install monthly operating system, updates automatically.

Answer: A

NEW QUESTION 28

A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:

```

3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:11 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:12 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:13 AM Audit Failure: CompanyNetwork\User1 Account locked out.
3/16/20 3:31:14 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:15 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:16 AM Audit Failure: CompanyNetwork\User2 Account locked out.
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:19 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:20 AM Audit Failure: CompanyNetwork\User3 Successful logon.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:32:40 AM Audit Failure: CompanyNetwork\User4 Successful logon.
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful logon.

```

Which of the following attacks MOST likely occurred?

- A. Dictionary
- B. Credential-stuffing
- C. Password-spraying
- D. Brute-force

Answer: D

NEW QUESTION 31

A security analyst needs to be proactive in understand the types of attacks that could potentially target the company's execute. Which of the following intelligence sources should to security analyst review?

- A. Vulnerability feeds
- B. Trusted automated exchange of indicator information
- C. Structured threat information expression
- D. Industry information-sharing and collaboration groups

Answer: D

NEW QUESTION 34

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 37

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 39

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 44

A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

- A. Perform a site survey
- B. Deploy an FTK Imager
- C. Create a heat map
- D. Scan for rogue access points
- E. Upgrade the security protocols
- F. Install a captive portal

Answer: AC

NEW QUESTION 48

Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

- A. SSAE SOC 2
- B. PCI DSS
- C. GDPR
- D. ISO 31000

Answer: C

NEW QUESTION 52

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 availability
- D. Replace the business's wired network with a wireless network.

Answer: C

NEW QUESTION 57

A security analyst is looking for a solution to help communicate to the leadership team the severity 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 58

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 59

Which of the following refers to applications and systems that are used within an organization without consent or approval?

- A. Shadow IT
- B. OSINT
- C. Dark web
- D. Insider threats

Answer: A

NEW QUESTION 61

A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

- A. Dual power supply
- B. Off-site backups
- C. Automatic OS upgrades
- D. NIC teaming
- E. Scheduled penetration testing
- F. Network-attached storage

Answer: AB

NEW QUESTION 63

A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this task?

- A. Netcat
- B. Netstat
- C. Nmap
- D. Nessus

Answer: B

NEW QUESTION 68

A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

- A. Credential harvesting
- B. Keylogger
- C. Brute-force

D. Spraying

Answer: D

NEW QUESTION 70

A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a projected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

- A. DNS sinkholding
- B. DLP rules on the terminal
- C. An IP blacklist
- D. Application whitelisting

Answer: D

NEW QUESTION 73

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 78

Which of the following describes the ability of code to target a hypervisor from inside

- A. Fog computing
- B. VM escape
- C. Software-defined networking
- D. Image forgery
- E. Container breakout

Answer: B

NEW QUESTION 82

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent data? (Select TWO)

- A. VPN
- B. Drive encryption
- C. Network firewall
- D. File-level encryption
- E. USB blocker
- F. MFA

Answer: BE

NEW QUESTION 84

The following is an administrative control that would be MOST effective to reduce the occurrence of malware execution?

- A. Security awareness training
- B. Frequency of NIDS updates
- C. Change control procedures
- D. EDR reporting cycle

Answer: A

NEW QUESTION 85

An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

- A. The system was configured with weak default security settings.
- B. The device uses weak encryption ciphers.
- C. The vendor has not supplied a patch for the appliance.
- D. The appliance requires administrative credentials for the assessment.

Answer: C

NEW QUESTION 90

A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device

approach?

- A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
- B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
- C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
- D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

Answer: C

NEW QUESTION 91

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 94

An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?

- A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
- B. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
- C. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
- D. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.

Answer: A

NEW QUESTION 95

A security analyst sees the following log output while reviewing web logs:

```
[02/Feb/2019:03:39:21 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=%2f..%2f..%2f..%2fetc%2fpasswd HTTP/1.0" 80:200:200
[02/Feb/2019:03:39:25 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=../../../../etc/passwd HTTP/1.0" 80:200:200
```

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

- A. Secure cookies
- B. Input validation
- C. Code signing
- D. Stored procedures

Answer: B

NEW QUESTION 100

A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

- A. Create a new acceptable use policy.
- B. Segment the network into trusted and untrusted zones.
- C. Enforce application whitelisting.
- D. Implement DLP at the network boundary.

Answer: C

NEW QUESTION 102

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 104

Which of the following algorithms has the SMALLEST key size?

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

Answer: B

NEW QUESTION 108

A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected.

Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Choose two.)

- A. DoS
- B. SSL stripping
- C. Memory leak
- D. Race condition
- E. Shimming
- F. Refactoring

Answer: AD

NEW QUESTION 112

A security analyst is reviewing logs on a server and observes the following output:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Which of the following is the security analyst observing?

- A. A rainbow table attack
- B. A password-spraying attack
- C. A dictionary attack
- D. A keylogger attack

Answer: C

NEW QUESTION 113

A well-known organization has been experiencing attacks from APIs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?

- A. Configuring signature-based antivirus to update every 30 minutes
- B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.
- C. Implementing application execution in a sandbox for unknown software.
- D. Fuzzing new files for vulnerabilities if they are not digitally signed

Answer: C

NEW QUESTION 114

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 118

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 119

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 124

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 128

A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

- A. dd
- B. chmod
- C. dnsenum
- D. logger

Answer: A

NEW QUESTION 131

A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

- A. OAuth
- B. SSO
- C. SAML
- D. PAP

Answer: C

NEW QUESTION 132

Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

- A. Least privilege
- B. Awareness training
- C. Separation of duties
- D. Mandatory vacation

Answer: C

NEW QUESTION 136

A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack. Which of the following sources would reveal if the CEO's personal information is for sale?

- A. Automated information sharing
- B. Open-source intelligence
- C. The dark web
- D. Vulnerability databases

Answer: C

NEW QUESTION 140

Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hot-spots?

- A. Footprinting
- B. White-box testing
- C. A drone/UAV
- D. Pivoting

Answer: A

NEW QUESTION 144

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 146

Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

- A. Investigation
- B. Containment
- C. Recovery
- D. Lessons learned

Answer: B

NEW QUESTION 150

A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:

`http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us`

The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:

`http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us` Which of the following application attacks is being tested?

- A. Pass-the-hash
- B. Session replay
- C. Object deference
- D. Cross-site request forgery

Answer: B

NEW QUESTION 152

Local guidelines require that all information systems meet a minimum-security baseline to be compliant. Which of the following can security administrators use to assess their system configurations against the baseline?

- A. SOAR playbook
- B. Security control matrix
- C. Risk management framework
- D. Benchmarks

Answer: D

NEW QUESTION 156

A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

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

Answer: D

NEW QUESTION 158

A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

- A. Recovery
- B. Identification
- C. Lessons learned
- D. Preparation

Answer: C

NEW QUESTION 159

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 163

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern? (Select TWO).

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens
- E. Geotagging
- F. Role-based access controls

Answer: AE

NEW QUESTION 168

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 170

After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

- A. The vulnerability scan output
- B. The IDS logs
- C. The full packet capture data
- D. The SIEM alerts

Answer: A

NEW QUESTION 175

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 176

A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

```

Commands
-----
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys
ssh root@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh -i ~/.ssh/id_rsa user@server
    
```

```

SSH Client
-----
?
    
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```

Commands
-----
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys
ssh root@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh -i ~/.ssh/id_rsa user@server
    
```

```

SSH Client
-----
ssh root@server
scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys
ssh -i ~/.ssh/id_rsa user@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
chmod 777 ~/.ssh/authorized_keys
chmod 644 ~/.ssh/id_rsa
    
```

NEW QUESTION 178

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 183

The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of \$10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

- A. Phishing
- B. Whaling
- C. Typo squatting
- D. Pharming

Answer: B

NEW QUESTION 185

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 wireless virus is spreading in the local network environment.

Answer: A

NEW QUESTION 190

Which of the following types of controls is a turnstile?

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

Answer: A

NEW QUESTION 192

An organization hired a consultant to assist with an active attack, and the consultant was able to identify the compromised accounts and computers. Which of the following is the consultant MOST likely to recommend to prepare for eradication?

- A. Quarantining the compromised accounts and computers, only providing them with network access
- B. Segmenting the compromised accounts and computers into a honeynet so as to not alert the attackers.
- C. Isolating the compromised accounts and computers, cutting off all network and internet access.
- D. Logging off and deleting the compromised accounts and computers to eliminate attacker access.

Answer: B

NEW QUESTION 196

Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?

- A. OWASP
- B. Vulnerability scan results
- C. NIST CSF
- D. Third-party libraries

Answer: A

NEW QUESTION 199

Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

- A. The data protection officer
- B. The data processor
- C. The data owner
- D. The data controller

Answer: C

NEW QUESTION 204

A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to account to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

- A. Create consultant accounts for each region, each configured with push MFA notifications.
- B. Create one global administrator account and enforce Kerberos authentication
- C. Create different accounts for each regio
- D. limit their logon times, and alert on risky logins
- E. Create a guest account for each regio
- F. remember the last ten passwords, and block password reuse

Answer: C

NEW QUESTION 206

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 all 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 207

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 209

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 213

.....

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

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 2

Which of the following describes the BEST approach for deploying application patches?

- A. Apply the patches to systems in a testing environment then to systems in a staging environment, and finally to production systems.
- B. Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems
- C. Test the patches in a test environment apply them to the production systems and then apply them to a staging environment
- D. Apply the patches to the production systems apply them in a staging environment, and then test all of them in a testing environment

Answer: A

NEW QUESTION 3

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 4

A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely the cause of the cause of the access issues?

- A. False rejection
- B. Cross-over error rate
- C. Efficacy rate
- D. Attestation

Answer: B

NEW QUESTION 5

A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?

- A. MSSP
- B. SOAR
- C. IaaS
- D. PaaS

Answer: B

NEW QUESTION 6

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
- AH 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 7

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 8

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 9

A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?

- A. An external access point is engaging in an evil-twin attack.
- B. The signal on the WAP needs to be increased in that section of the building.
- C. The certificates have expired on the devices and need to be reinstalled.
- D. The users in that section of the building are on a VLAN that is being blocked by the firewall.

Answer: A

NEW QUESTION 10

A security administrator currently spends a large amount of time on common security tasks, such as report generation, phishing investigations, and user provisioning and deprovisioning. This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

- A. DAC
- B. ABAC
- C. SCAP
- D. SOAR

Answer: D

NEW QUESTION 10

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 15

A security analyst has received an alert about being sent via email. The analyst's Chief Information Security Officer (CISO) has made it clear that PII must be handled with extreme care. From which of the following did the alert MOST likely originate?

- A. S/MIME
- B. DLP
- C. IMAP
- D. HIDS

Answer: B

NEW QUESTION 17

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 21

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 25

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 26

A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

- A. Configure the perimeter firewall to deny inbound external connections to SMB ports.
- B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
- C. Deny unauthenticated users access to shared network folders.
- D. Verify computers are set to install monthly operating system, updates automatically.

Answer: A

NEW QUESTION 28

A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:

```

3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:11 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:12 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:13 AM Audit Failure: CompanyNetwork\User1 Account locked out.
3/16/20 3:31:14 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:15 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:16 AM Audit Failure: CompanyNetwork\User2 Account locked out.
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:19 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:20 AM Audit Failure: CompanyNetwork\User3 Successful logon.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:32:40 AM Audit Failure: CompanyNetwork\User4 Successful logon.
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful logon.
    
```

Which of the following attacks MOST likely occurred?

- A. Dictionary
- B. Credential-stuffing
- C. Password-spraying
- D. Brute-force

Answer: D

NEW QUESTION 31

A security analyst needs to be proactive in understand the types of attacks that could potentially target the company's execute. Which of the following intelligence sources should to security analyst review?

- A. Vulnerability feeds
- B. Trusted automated exchange of indicator information
- C. Structured threat information expression
- D. Industry information-sharing and collaboration groups

Answer: D

NEW QUESTION 34

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 37

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 39

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 44

A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

- A. Perform a site survey
- B. Deploy an FTK Imager
- C. Create a heat map
- D. Scan for rogue access points
- E. Upgrade the security protocols
- F. Install a captive portal

Answer: AC

NEW QUESTION 48

Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

- A. SSAE SOC 2
- B. PCI DSS
- C. GDPR
- D. ISO 31000

Answer: C

NEW QUESTION 52

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 availability.
- D. Replace the business's wired network with a wireless network.

Answer: C

NEW QUESTION 57

A security analyst is looking for a solution to help communicate to the leadership team the severity 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 58

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 59

Which of the following refers to applications and systems that are used within an organization without consent or approval?

- A. Shadow IT
- B. OSINT
- C. Dark web
- D. Insider threats

Answer: A

NEW QUESTION 61

A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

- A. Dual power supply
- B. Off-site backups
- C. Automatic OS upgrades
- D. NIC teaming
- E. Scheduled penetration testing
- F. Network-attached storage

Answer: AB

NEW QUESTION 63

A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this task?

- A. Netcat
- B. Netstat
- C. Nmap
- D. Nessus

Answer: B

NEW QUESTION 68

A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

- A. Credential harvesting
- B. Keylogger
- C. Brute-force

D. Spraying

Answer: D

NEW QUESTION 70

A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a projected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

- A. DNS sinkholding
- B. DLP rules on the terminal
- C. An IP blacklist
- D. Application whitelisting

Answer: D

NEW QUESTION 73

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 78

Which of the following describes the ability of code to target a hypervisor from inside

- A. Fog computing
- B. VM escape
- C. Software-defined networking
- D. Image forgery
- E. Container breakout

Answer: B

NEW QUESTION 82

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent data? (Select TWO)

- A. VPN
- B. Drive encryption
- C. Network firewall
- D. File-level encryption
- E. USB blocker
- F. MFA

Answer: BE

NEW QUESTION 84

The following is an administrative control that would be MOST effective to reduce the occurrence of malware execution?

- A. Security awareness training
- B. Frequency of NIDS updates
- C. Change control procedures
- D. EDR reporting cycle

Answer: A

NEW QUESTION 85

An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

- A. The system was configured with weak default security settings.
- B. The device uses weak encryption ciphers.
- C. The vendor has not supplied a patch for the appliance.
- D. The appliance requires administrative credentials for the assessment.

Answer: C

NEW QUESTION 90

A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device

approach?

- A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
- B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
- C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
- D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

Answer: C

NEW QUESTION 91

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 94

An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?

- A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
- B. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
- C. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
- D. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.

Answer: A

NEW QUESTION 95

A security analyst sees the following log output while reviewing web logs:

```
[02/Feb/2019:03:39:21 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=%2f..%2f..%2f..%2fetc%2fpasswd HTTP/1.0" 80:200:200  
[02/Feb/2019:03:39:25 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=../../../../etc/passwd HTTP/1.0" 80:200:200
```

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

- A. Secure cookies
- B. Input validation
- C. Code signing
- D. Stored procedures

Answer: B

NEW QUESTION 100

A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

- A. Create a new acceptable use policy.
- B. Segment the network into trusted and untrusted zones.
- C. Enforce application whitelisting.
- D. Implement DLP at the network boundary.

Answer: C

NEW QUESTION 102

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 104

Which of the following algorithms has the SMALLEST key size?

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

Answer: B

NEW QUESTION 108

A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected.

Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Choose two.)

- A. DoS
- B. SSL stripping
- C. Memory leak
- D. Race condition
- E. Shimming
- F. Refactoring

Answer: AD

NEW QUESTION 112

A security analyst is reviewing logs on a server and observes the following output:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Which of the following is the security analyst observing?

- A. A rainbow table attack
- B. A password-spraying attack
- C. A dictionary attack
- D. A keylogger attack

Answer: C

NEW QUESTION 113

A well-known organization has been experiencing attacks from APIs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?

- A. Configuring signature-based antivirus to update every 30 minutes
- B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.
- C. Implementing application execution in a sandbox for unknown software.
- D. Fuzzing new files for vulnerabilities if they are not digitally signed

Answer: C

NEW QUESTION 114

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 118

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 119

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 124

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 128

A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

- A. dd
- B. chmod
- C. dnsenum
- D. logger

Answer: A

NEW QUESTION 131

A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

- A. OAuth
- B. SSO
- C. SAML
- D. PAP

Answer: C

NEW QUESTION 132

Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

- A. Least privilege
- B. Awareness training
- C. Separation of duties
- D. Mandatory vacation

Answer: C

NEW QUESTION 136

A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack. Which of the following sources would reveal if the CEO's personal information is for sale?

- A. Automated information sharing
- B. Open-source intelligence
- C. The dark web
- D. Vulnerability databases

Answer: C

NEW QUESTION 140

Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hot-spots?

- A. Footprinting
- B. White-box testing
- C. A drone/UAV
- D. Pivoting

Answer: A

NEW QUESTION 144

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 146

Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

- A. Investigation
- B. Containment
- C. Recovery
- D. Lessons learned

Answer: B

NEW QUESTION 150

A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:

`http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us`

The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:

`http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us` Which of the following application attacks is being tested?

- A. Pass-the-hash
- B. Session replay
- C. Object deference
- D. Cross-site request forgery

Answer: B

NEW QUESTION 152

Local guidelines require that all information systems meet a minimum-security baseline to be compliant. Which of the following can security administrators use to assess their system configurations against the baseline?

- A. SOAR playbook
- B. Security control matrix
- C. Risk management framework
- D. Benchmarks

Answer: D

NEW QUESTION 156

A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

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

Answer: D

NEW QUESTION 158

A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

- A. Recovery
- B. Identification
- C. Lessons learned
- D. Preparation

Answer: C

NEW QUESTION 159

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 163

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern? (Select TWO).

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens
- E. Geotagging
- F. Role-based access controls

Answer: AE

NEW QUESTION 168

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 170

After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

- A. The vulnerability scan output
- B. The IDS logs
- C. The full packet capture data
- D. The SIEM alerts

Answer: A

NEW QUESTION 175

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 176

A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

```

Commands
-----
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys
ssh root@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh -i ~/.ssh/id_rsa user@server
    
```

```

SSH Client
-----
?
    
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```

Commands
-----
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys
ssh root@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh -i ~/.ssh/id_rsa user@server
    
```

```

SSH Client
-----
ssh root@server
scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys
ssh -i ~/.ssh/id_rsa user@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
chmod 777 ~/.ssh/authorized_keys
chmod 644 ~/.ssh/id_rsa
    
```

NEW QUESTION 178

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 183

The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of \$10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

- A. Phishing
- B. Whaling
- C. Typo squatting
- D. Pharming

Answer: B

NEW QUESTION 185

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 wireless virus is spreading in the local network environment.

Answer: A

NEW QUESTION 190

Which of the following types of controls is a turnstile?

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

Answer: A

NEW QUESTION 192

An organization hired a consultant to assist with an active attack, and the consultant was able to identify the compromised accounts and computers. Which of the following is the consultant MOST likely to recommend to prepare for eradication?

- A. Quarantining the compromised accounts and computers, only providing them with network access
- B. Segmenting the compromised accounts and computers into a honeynet so as to not alert the attackers.
- C. Isolating the compromised accounts and computers, cutting off all network and internet access.
- D. Logging off and deleting the compromised accounts and computers to eliminate attacker access.

Answer: B

NEW QUESTION 196

Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?

- A. OWASP
- B. Vulnerability scan results
- C. NIST CSF
- D. Third-party libraries

Answer: A

NEW QUESTION 199

Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

- A. The data protection officer
- B. The data processor
- C. The data owner
- D. The data controller

Answer: C

NEW QUESTION 204

A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to account to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

- A. Create consultant accounts for each region, each configured with push MFA notifications.
- B. Create one global administrator account and enforce Kerberos authentication
- C. Create different accounts for each region
- D. limit their logon times, and alert on risky logins
- E. Create a guest account for each region
- F. remember the last ten passwords, and block password reuse

Answer: C

NEW QUESTION 206

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 all 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 207

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 209

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 213

.....

Relate Links

100% Pass Your SY0-601 Exam with Examible 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/>