the phishing team, and the forwarded email revealed the link to be:

<a href-"https://www.company.com/payto.do?routing=00001111&accc=22223334&amount-250">Click here to unsubscribe

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

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

Correct Answer: D

QUESTION 185
A security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices the following requirements must be met:

▪ Mobile device OSs must be patched up to the latest release
▪ A screen lock must be enabled (passcode or biometric)
▪ Corporate data must be removed if the device is reported lost or stolen

Which of the following controls should the security engineer configure? (Select TWO)

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

Correct Answer: CD

QUESTION 186
A security analyst Is hardening a Linux workstation and must ensure It has public keys forwarded to remote systems for secure login. Which of the following steps should the analyst perform to meet these requirements? (Select TWO).

A. Forward the keys using ssh-copy-id.
B. Forward the keys using scp.
C. Forward the keys using ash -i.
D. Forward the keys using openssl -s.
E. Forward the keys using ssh-keyger.

Correct Answer: AD

QUESTION 187
A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst Include in this documentation? (Select TWO).

A. The order of volatility
B. A checksum
C. The location of the artifacts

D. The vendor's name
E. The date and time
F. A warning banner

Correct Answer: AE

QUESTION 188
A company is launching a new internet platform for its clients. The company does not want to implement its own authorization solution but instead wants to rely on the authorization provided by another platform. Which of the following is the BEST approach to implement the desired solution?

A. OAuth
B. TACACS+
C. SAML
D. RADIUS

Correct Answer: D

QUESTION 189
Which of the following relets 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

Correct Answer: A

QUESTION 190
An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

A. hping3 -S corsptia.org -p 80
B. nc -l -v comptia.org -p 80
C. nmap comptia.org -p 80 -sV
D. nslookup -port=80 comptia.org

Correct Answer: C

QUESTION 191
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

Correct Answer: D

Explanation:
CVE entries are brief. They don't include technical data, or information about risks, impacts, and fixes. Those details appear in other databases, including the U.S. National Vulnerability Database (NVD), the CERT/CC Vulnerability Notes Database, and various lists maintained by vendors and other organizations. Across these different systems, CVE IDs give users a reliable way to tell one unique security flaw from another.

QUESTION 192
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

Correct Answer: C

QUESTION 193
Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?

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

Correct Answer: A

QUESTION 194
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

Correct Answer: D

QUESTION 195
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

Correct Answer: C

QUESTION 196
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.

Correct Answer: B

QUESTION 197
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.

Correct Answer: AB

QUESTION 198
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

Correct Answer: A

QUESTION 199
An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker MOST likely attempting?

A. A spear-phishing attack

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

Correct Answer: B

QUESTION 200
A client sent several inquiries to a project manager about the delinquent delivery status of some
critical reports. The project manager darned the reports were previously sent via email but then
quickly generated and backdated the reports before submitting them via a new email message.
Which of the following actions MOST likely supports an investigation for fraudulent submission?

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

Correct Answer: D

QUESTION 201
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

Correct Answer: BE

QUESTION 202
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?