- **Vendor:** CompTIA
- **Exam Code:** SY0-501
- **Exam Name:** CompTIA Security+ Certification Exam
- **New Updated Questions from Braindump2go (Updated in July/2020)**

QUESTION 1197
Which of the following attacks is used to capture the WPA2 handshake?

A. Replay
B. IV
C. Evil twin
D. Disassociation

Answer: D

QUESTION 1198
A user loses a COPE device. Which of the following should the user do NEXT to protect the data on the device?

A. Call the company help desk to remotely wipe the device.
B. Report the loss to authorities.
C. Check with corporate physical security for the device.
D. Identify files that are potentially missing on the device.

Answer: A

QUESTION 1199
A government agency with sensitive information wants to virtualize its infrastructure. Which of the following cloud deployment models BEST fits the agency's needs?

A. Public
B. Community
C. Private
D. Hybrid

Answer: C

QUESTION 1200
An organization is developing its mobile device management policies and procedures and is concerned about vulnerabilities that are associated with sensitive data being saved to a mobile device, as well as weak authentication when using a PIN. As part of some discussions on the topic, several solutions are proposed. Which of the following controls, when required together, will address the protection of data-at- rest as well as strong authentication? (Choose two.)

A. Containerization

B. FDE
C. Remote wipe capability
D. MDM
E. MFA
F. OTA updates

Answer: BE

QUESTION 1201
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 1202
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 server. 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 1203
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 IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

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

Answer: A

QUESTION 1204
A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing 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=00001111&acct=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 1205
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 1206
A network administrator at a large organization is reviewing methods to improve the security of the wired LAN. Any security improvement must be centrally managed and allow corporate-owned devices to have access to the intranet but limit others to Internet access only. Which of the following should the administrator recommend?

A. 802.1X utilizing the current PKI infrastructure
B. SSO to authenticate corporate users
C. MAC address filtering with ACLs on the router
D. PAM for users account management

Answer: A

QUESTION 1207
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 1208
In which of the following risk management strategies would cybersecurity insurance be used?

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

Answer: A

QUESTION 1209
A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST meet these requirements?

A. RA
B. OCSP
C. CRI

D. CSR

Answer: B

QUESTION 1210
A company needs to fix some audit findings related to its physical security. A key finding was that multiple people could physically enter a location at the same time. Which of the following is the BEST control to address this audit finding?

A. Faraday cage
B. Mantrap
C. Biometrics
D. Proximity cards

Answer: B

QUESTION 1211
A network administrator was concerned during an audit that users were able to use the same passwords the day after a password change policy took effect. The following settings are in place:

```
- Users must change their passwords every 30 days.
- Users cannot reuse the last 10 passwords.
```

Which of the following settings would prevent users from being able to immediately reuse the same passwords?

A. Minimum password age of five days
B. Password history of ten passwords
C. Password length greater than ten characters
D. Complex passwords must be used

Answer: A

QUESTION 1212
After successfully breaking into several networks and infecting multiple machines with malware, hackers contact the network owners, demanding payment to remove the infection and decrypt files. The hackers threaten to publicly release information about the breach if they are not paid. Which of the following BEST describes these attackers?

A. Gray hat hackers
B. Organized crime
C. Insiders
D. Hacktivists

Answer: B

QUESTION 1213
When implementing automation with IoT devices, which of the following should be considered FIRST to keep the network secure?

A. Z-Wave compatibility
B. Network range
C. Zigbee configuration
D. Communication protocols

Answer: D