QUESTION 1315
An attacker has gained control of several systems on the Internet and is using them to attack a website, causing it to stop responding to legitimate traffic. Which of the following BEST describes the attack?

A. MITM
B. DNS poisoning
C. Buffer overflow
D. DDoS

Answer: D

QUESTION 1316
A company has users and printers in multiple geographic locations, and the printers are located in common areas of the offices. To preserve the confidentiality of PII, a security administrator needs to implement the appropriate controls. Which of the following would BEST meet the confidentiality requirements of the data?

A. Enforcing location-based policy restrictions
B. Adding location to the standard naming convention
C. Implementing time-of-day restrictions based on location
D. Conducting regular account maintenance at each location

Answer: A

QUESTION 1317
The website of a bank that an organization does business with is being reported as untrusted by the organization's web browser. A security analyst has been assigned to investigate. The analyst discovers the bank recently merged with another local bank and combined names. Additionally, the user's bookmark automatically redirects to the website of the newly named bank. Which of the following is the MOST likely cause of the issue?

A. The company's web browser is not up to date
B. The website's certificate still has the old bank's name
C. The website was created too recently to be trusted
D. The website's certificate has expired

Answer: B

QUESTION 1318
A Chief Information Officer (CIO) wants to eliminate the number of calls the help desk is receiving for password resets when users log on to internal portals. Which of the following is the BEST solution?

A. Increase password length
B. Implement a self-service portal
C. Decrease lockout threshold
D. Deploy mandatory access control

Answer: B

QUESTION 1319
A company recently experienced a security breach. The security staff determined that the intrusion was due to an out-of-date proprietary software program running on a non-compliant server. The server was imaged and copied onto a hardened VM, with the previous connections re-established. Which of the following is the NEXT step in the incident response process?

A. Recovery
B. Eradication
C. Lessons learned
D. Containment
E. Identification

Answer: C

QUESTION 1320
Which of the following types of vulnerability scans typically returns more detailed and thorough insights into actual system vulnerabilities?

A. Non-credentialed
B. Intrusive
C. Credentialed
D. Non-intrusive

Answer: C

QUESTION 1321
A security team received reports of increased latency on a highly utilized e-commerce server. This led to eventual service unavailability as a result of internal scanning activity. The following web-server log was shared with the team to support this claim:

```
root@server:~ # tail 5 /var/log/httpd-access.log
192.168.1.101 -- [15/May/2019:10:08:03 +0200] "GET /adjakjaj HTTP/1.1" 404
192.168.1.101 -- [15/May/2019:10:08:03 +0200] "GET /njknfkjn HTTP/1.1" 404
192.168.1.101 -- [15/May/2019:10:08:04 +0200] "GET /manbsbhd HTTP/1.1" 404
192.168.1.101 -- [15/May/2019:10:08:04 +0200] "GET /uwriuiyr HTTP/1.1" 404
192.168.1.101 -- [15/May/2019:10:08:04 +0200] "GET /iuqiuuqi HTTP/1.1" 404
```

Which of the following actions would BEST address the service impact caused by scanning?

A. Enable proper error handling on the web server
B. Run scans during off peak hours
C. Stop scanning the affected servers
D. Disable directory enumeration in the scanning policy

Answer: A

QUESTION 1322
A developer has just finished coding a custom web application and would like to test it for bugs by automatically injecting mailformed data into it. Which of the following is the developer looking to perform?

A. Fuzzing
B. Stress testing
C. Sandboxing
D. Normalization

Answer: A

QUESTION 1323
Which of the following is the BEST example of a reputation impact identified during a risk assessment?

A. A bad software patch taking down the production systems
B. A misconfigured firewall exposing intellectual property to the Internet
C. An attacker defacing the e-commerce portal
D. Malware collecting credentials for company bank accounts

Answer: C

QUESTION 1324
An auditor requiring an organization to perform real-time validation of SSL certificates. Which of the following should the organization implement?

A. OCSP
B. CRL
C. CSR
D. KDC

Answer: A

QUESTION 1325
Which of the following is a resiliency strategy that allows a system to automatically adapt to workload changes?

A. Fault tolerance
B. Redundancy
C. Elasticity
D. High availability

Answer: C

QUESTION 1326
A penetration tester was able to connect to a company's internal network and perform scans and staged attacks for the duration of the testing period without being noticed. The SIEM did not alert the security team to the presence of the penetration tester's devices on the network. Which of the following would provide the security team with notification in a timely manner?

A. Implement rogue system detection and sensors
B. Create a trigger on the IPS and alert the security team when unsuccessful logins occur
C. Decrease the correlation threshold for alerts on the SIEM
D. Run a credentialed vulnerability scan

Answer: A

QUESTION 1327
Which of the following involves the use of targeted and highly crafted custom attacks against a population of users who may have access to a particular service or program?

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

Answer: B

QUESTION 1328
When building a hosted datacenter, which of the following is the MOST important consideration for physical security within the datacenter?

A. Security guards
B. Cameras
C. Secure enclosures
D. Biometrics

Answer: C

QUESTION 1329
An organization would like to set up a more robust network access system. The network administrator suggests the organization move to a certificate-based authentication setup in which a client-side certificate is used while connecting. Which of the following EAP types should be used to meet these criteria?

A. EAP-TLS
B. EAP-FAST
C. EAP-MD5
D. EAP-TTLS

Answer: A

QUESTION 1330
Which of the following is MOST likely the security impact of continuing to operate end-of-life systems?

A. Higher total cost of ownership due to support costs
B. Denial of service due to patch availability
C. Lack of vendor support for decommissioning
D. Support for legacy protocols

Answer: B

QUESTION 1331
After downloading third-party software, a user begins receiving continuous pop-up messages stating the Windows antivirus is outdated. The user is unable to access any files or programs until the subscription is renewed with Bitcoin. Which of the following types of attacks is being executed?

A. Spyware
B. Crypto-malware
C. Adware
D. Ransomware

Answer: D

QUESTION 1332
As a security measure, an organization has disabled all external media from accessing the network. Since some users

may have data that needs to be transferred to the network, which of the following would BEST assist a security administrator with transferring the data while keeping the internal network secure?

A. Upload the media in the DMZ
B. Upload the data in a separate VLAN
C. Contact the data custodian
D. Use a standalone scanning system

Answer: D

QUESTION 1333
A technician is implementing 802.1X with dynamic VLAN assignment based on a user Active Directory group membership. Which of the following configurations supports the VLAN definitions?

A. RADIUS attribute
B. SAML tag
C. LDAP path
D. Shibboleth IdP

Answer: A

QUESTION 1334
Which of the following agreement types is a non-contractual agreement between two or more parties and outlines each party's requirements and responsibilities?

A. BPA
B. SLA
C. MOU
D. ISA

Answer: C

QUESTION 1335
A technician wants to implement PKI-based authentication on an enterprise wireless network. Which of the following should the technician configure to enforce the use of client-side certificates?

A. 802.1X with PEAP
B. WPA2-PSK
C. EAP-TLS
D. RADIUS Federation

Answer: C