**QUESTION 237**
Which of the following disaster recovery tests is The LEAST time consuming for the disaster recovery team?

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

**Correct Answer:** D

**QUESTION 238**
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.

**Correct Answer:** C

**QUESTION 239**
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.

**Correct Answer:** A

**QUESTION 240**
A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

A. DNSSEC
B. Reverse proxy
C. VPN concentrator
D. PKI
E. Active Directory
F. RADIUS

**Correct Answer:** EF

**QUESTION 241**
During a routine scan of a wireless segment at a retail company, a security administrator discovers several devices are connected to the network that do not match the company's naming

convention and are not in the asset Inventory. WiFi access Is protected with 255-Wt encryption via WPA2. Physical access to the company's facility requires two-factor authentication using a badge and a passcode. Which of the following should the administrator implement to find and remediate the Issue? (Select TWO).

A. Check the SIEM for failed logins to the LDAP directory.
B. Enable MAC filtering on the switches that support the wireless network.
C. Run a vulnerability scan on all the devices in the wireless network
D. Deploy multifactor authentication for access to the wireless network
E. Scan the wireless network for rogue access points.
F. Deploy a honeypot on the network

**Correct Answer:** BE
**Explanation:**
Security is pretty good already up to a point, clearly Rogue AP bypass is in the picture MAC filtering on the switch the AP's hang from will ensure the only AP's allowed to touch the core network are approved known AP's and ze "bad guys" will find themselves trapped on an AP island with nowhere to go!

**QUESTION 242**
A security analyst is reviewing logs on a server and observes the following output:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Which of the following is the security analyst observing?

A. A rainbow table attack
B. A password-spraying attack
C. A dictionary attack
D. A keylogger attack

**Correct Answer:** C

**QUESTION 243**
A cybersecurity administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive All connections are being dropped by the firewall. Which of the following would be the BEST option to remove the rules?

A. # iptables -t mangle -X
B. # iptables -F
C. # iptables -Z
D. # iptables -P INPUT -j DROP

**Correct Answer:** D

**QUESTION 244**
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.

**Correct Answer:** C

**QUESTION 245**
Which of the following will MOST likely cause machine learning and AI-enabled systems to operate with unintended consequences?

A. Stored procedures
B. Buffer overflows
C. Data bias
D. Code reuse

**Correct Answer:** C
**Explanation:**
https://lionbridge.ai/articles/7-types-of-data-bias-in-machine-learning/
https://bernardmarr.com/default.asp?contentID=1827

**QUESTION 246**
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

**Correct Answer:** D
**Explanation:**
https://www.comparitech.com/net-admin/pcap-guide/#:~:text=Packet%20Capture%20or%20PCAP%20(also,packet%20data%20from%20a%20network.

**QUESTION 247**
The process of passively gathering information prior to launching a cyberattack is called:

A. tailgating
B. reconnaissance
C. pharming
D. prepending

**Correct Answer:** B

**QUESTION 248**
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

**Correct Answer:** D
**Explanation:**
Creating a whole new hot sire just because of DDoS seems extremely expensive. Instead, deploying a countermeasure like challenge response would mitigate the DDoS.
https://www.radware.com/security/ddos-knowledge-center/ddospedia/http-challenge
https://www.nexusguard.com/hubfs/Nexusguard_Whitepaper_DDoS_Mitigation_EN_A4.pdf?t=1487581897757

**QUESTION 249**
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

**Correct Answer:** D

**QUESTION 250**
The website http://companywebsite.com requires users to provide personal Information, Including security question responses, for registration. Which of the following would MOST likely cause a data breach?

A. Lack of input validation
B. Open permissions
C. Unsecure protocol
D. Missing patches

**Correct Answer:** C

**QUESTION 251**
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

**Correct Answer:** B

**QUESTION 252**
An attacker is exploiting a vulnerability that does not have a patch available. Which of the following is the attacker exploiting?

A. Zero-day
B. Default permissions
C. Weak encryption
D. Unsecure root accounts
**Correct Answer:** A

**QUESTION 253**
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

**Correct Answer:** AD

**QUESTION 254**
An analyst has determined that a server was not patched and an external actor exfiltrated data on port 139. Which of the following sources should the analyst review to BEST ascertain how the Incident could have been prevented?

A. The vulnerability scan output
B. The security logs
C. The baseline report
D. The correlation of events

**Correct Answer:** A

**QUESTION 255**
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