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=14

87581897757

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

Correct Answer: C

QUESTION 256
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 these requirement?

A. RA
B. OCSP
C. CRL
D. CSR
Correct Answer: C
Explanation:
A CRL can still be preferred over the use of OCSP if a server has issued many certificates to be validated within a single revocation period. It may be more efficient for the organization to download a CRL at the beginning of the revocation period than to utilize the OCSP standard, necessitating an OCSP response every time a certificate requires validation.

QUESTION 257
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. An NDA
C. A BPA
D. An MOU

Correct Answer: D

QUESTION 258
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

Correct Answer: D

QUESTION 259
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.

Correct Answer: A

QUESTION 260
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 the exfiltration of data? (Select TWO).

A. VPN
B. Drive encryption
C. Network firewall
D. File level encryption
E. USB blocker
F. MFA

Correct Answer: BE

QUESTION 261
A security engineer has enabled two-factor authentication on all workstations. Which of the