security analyst reviews the email and decides to download the attachment to a Linux sandbox for review. Which of the following commands would MOST likely indicate if the email is malicious?

A. sha256sum ~/Desktop/file.pdf
B. file ~/Desktop/file.pdf
C. strings ~/Desktop/file.pdf | grep "<script"
D. cat < ~/Desktop/file.pdf | grep -i .exe

Correct Answer: A

QUESTION 64
An organization has several systems that require specific logons Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?

A. Use SSO across all applications
B. Perform a manual privilege review
C. Adjust the current monitoring and logging rules
D. Implement multifactor authentication

Correct Answer: A

QUESTION 65
A team of security analysts has been alerted to potential malware activity. The initial examination indicates one of the affected workstations is beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

A. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.
B. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.
C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.
D. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.

Correct Answer: D

QUESTION 66
While reviewing log files, a security analyst uncovers a brute-force attack that is being performed against an external webmail portal. Which of the following would be BEST to prevent this type of attack from beinq successful?

A. Implement MFA on the email portal using out-of-band code delivery.
B. Create a new rule in the IDS that triggers an alert on repeated login attempts
C. Leverage password filters to prevent weak passwords on employee accounts from being exploited.
D. Alter the lockout policy to ensure users are permanently locked out after five attempts.
E. Configure a WAF with brute force protection rules in block mode

Correct Answer: A

QUESTION 67
A company's change management team has asked a security analyst to review a potential change to the email server before it is released into production. The analyst reviews the following change request:

Change request date:	2020-01-30
Change requester:	Cindy Richardson
Change asset:	WIN2K-EMAIL001
Change requested:	Modify the following SPF record to change +all to –all

Which of the following is the MOST likely reason for the change?

A. To reject email from servers that are not listed in the SPF record
B. To reject email from email addresses that are not digitally signed.
C. To accept email to the company's domain.
D. To reject email from users who are not authenticated to the network.

Correct Answer: A

QUESTION 68
A company recently experienced a breach of sensitive information that affects customers across multiple geographical regions. Which of the following roles would be BEST suited to determine the breach notification requirements?

A. Legal counsel
B. Chief Security Officer
C. Human resources
D. Law enforcement

Correct Answer: A

QUESTION 69
While investigating reports or issues with a web server, a security analyst attempts to log in remotely and recedes the following message:

```
[root@localhost /root]# ssh user1@10.254.2.25
Connection timed out.
```

The analyst accesses the server console, and the following console messages are displayed:

```
Out of memory: Kill process 3448(httpd) score 41 or sacrifice child
Killed process 3448(httpd) totle-vm:74716kB, anon-rss: 23456kB, file-rss:1683kB
Out of memory: Kill process 3449(httpd) score 41 or sacrifice child
Killed process 3449(httpd) totle-vm:74634kB, anon-rss: 28542kB, file-rss:1357kB
Out of memory: Kill process 3452(httpd) score 41 or sacrifice child
Killed process 3452(httpd) totle-vm:73466kB, anon-rss: 29753kB, file-rss:1925kB
```

The analyst is also unable to log in on the console. While reviewing network captures for the server, the analyst sees many packets with the following signature:

```
10.254.2.25.6781 > 128.50.100.23.80
10.254.2.25.6782 > 128.50.100.23.80
10.254.2.25.6783 > 128.50.100.23.80
10.254.2.25.6784 > 128.50.100.23.80
```

Which of the following is the BEST step for the analyst to lake next in this situation?

A. Load the network captures into a protocol analyzer to further investigate the communication with 128.30.100.23, as this may be a botnet command server.
B. After ensuring network captures from the server are saved isolate the server from the network take a memory snapshot, reboot and log in to do further analysis.
C. Corporate data is being exfilltrated from the server Reboot the server and log in to see if it contains any sensitive data.
D. Cryptomining malware is running on the server and utilizing an CPU and memory. Reboot the server and disable any cron Jobs or startup scripts that start the mining software.

Correct Answer: A

QUESTION 70
A security analyst is supporting an embedded software team. Which of the following is the BEST recommendation to ensure proper error handling at runtime?

A. Perform static code analysis.
B. Require application fuzzing.
C. Enforce input validation
D. Perform a code review

Correct Answer: B

QUESTION 71
An organization that uses SPF has been notified emails sent via its authorized third-party partner are getting rejected A security analyst reviews the DNS entry and sees the following:

v=spf1 ip4:180.10.6.5 ip4:180.10.6.10 include:robustmail.com -all

The organization's primary mail server IP is 180.10 6.6, and the secondary mail server IP is 180.10.6.5. The organization's third-party mail provider is "Robust Mail" with the domain name robustmail.com.

Which of the following is the MOST likely reason for the rejected emails?

A. The wrong domain name is in the SPF record.
B. The primary and secondary email server IP addresses are out of sequence.
C. SPF version 1 does not support third-party providers
D. An incorrect IP version is being used.

Correct Answer: A

QUESTION 72
The IT department is concerned about the possibility of a guest device infecting machines on the corporate network or taking down the company's singe internet connection. Which of the following should a security analyst recommend to BEST meet the requirements outlined by the IT Department?

A. Require the guest machines to install the corporate-owned EDR solution.
B. Configure NAC to only alow machines on the network that are patched and have active antivirus.
C. Place a firewall In between the corporate network and the guest network
D. Configure the IPS with rules that will detect common malware signatures traveling from the guest network.

Correct Answer: A

QUESTION 73
White reviewing incident reports from the previous night, a security analyst notices the corporate websites were defaced with po mcai propaganda. Which of the following BEST Describes this type of actor?

A. Hacktivist
B. Nation-state
C. insider threat
D. Organized crime

Correct Answer: A

QUESTION 74
While analyzing network traffic, a security analyst discovers several computers on the network are connecting to a malicious domain that was blocked by a DNS sinkhole. A new private IP range is now visible, but no change requests were made to add it. Which of the following is the BEST solution for the security analyst to implement?

A. Block the domain IP at the firewall.
B. Blacklist the new subnet
C. Create an IPS rule.
D. Apply network access control.

Correct Answer: A

QUESTION 75

Which of the following is a best practice when sending a file/data to another individual in an organization?

A. Encrypt the file but do not compress it.
B. When encrypting, split the file: and then compress each file.
C. Compress and then encrypt the file.
D. Encrypt and then compress the file.

Correct Answer: C

QUESTION 76
A threat feed notes malicious actors have been infiltrating companies and exfiltration data to a specific set of domains. Management at an organization wants to know if it is a victim. Which of the following should the security analyst recommend to identity this behavior without alerting any potential malicious actors?

A. Create an IPS rule to block these domains and trigger an alert within the SIEM tool when these domains are requested
B. Add the domains to a DNS sinkhole and create an alert m the SIEM toot when the domains are queried
C. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443
D. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this information

Correct Answer: D

QUESTION 77
An incident responder successfully acquired application binaries off a mobile device for later forensic analysis. Which of the following should the analyst do NEXT?

A. Decompile each binary to derive the source code.
B. Perform a factory reset on the affected mobile device.
C. Compute SHA-256 hashes for each binary.
D. Encrypt the binaries using an authenticated AES-256 mode of operation.
E. Inspect the permissions manifests within each application.

Correct Answer: C

QUESTION 78
An organization has been seeing increased levels of malicious traffic. A security analyst wants to take a more proactive approach to identify the threats that are acting against the organization's network. Which of the following approaches should the security analyst recommend?

A. Use the MITRE ATT&CK framework to develop threat models.
B. Conduct internal threat research and establish indicators of compromise.
C. Review the perimeter firewall rules to ensure rule-set accuracy.
D. Use SCAP scans to monitor for configuration changes on the network.

Correct Answer: D