1. A security analyst wants to capture large amounts of network data that will be analyzed at a later time. The packet capture does not need to be in a format that is readable by humans, since it will be put into a binary file called "packetCapture." The capture must be as efficient as possible, and the analyst wants to minimize the likelihood that packets will be missed.

Which of the following commands will best accomplish the analyst's objectives?

A. tcpdump -w packetCapture
B. tcpdump -a packetCapture
C. tcpdump -n packetCapture
D. nmap -v > packetCapture
E. nmap -oA > packetCapture

Answer: A

2. A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with.

Which of the following is the best mitigation technique?

A. Geoblock the offending source country
B. Block the IP range of the scans at the network firewall.
C. Perform a historical trend analysis and look for similar scanning activity.D. Block the specific IP address of the scans at the network firewall

Answer: A

3. A security team identified several rogue Wi-Fi access points during the most recent network scan.

The network scans occur once per quarter.

Which of the following controls would best all ow the organization to identity rogue devices more quickly?

A. Implement a continuous monitoring policy.
B. Implement a BYOD policy.
C. Implement a portable wireless scanning policy.
D. Change the frequency of network scans to once per month.

Answer: A

4. SIMULATION

A healthcare organization must develop an action plan based on the findings from a risk assessment.

The action plan must consist of:

? Risk categorization

? Risk prioritization

? Implementation of controls

Instructions:

1. Click on the audit report, risk matrix, and SLA expectations documents to review their contents.
2. On the Risk categorization tab, prioritize the findings for remediation based on their risk rating score.
3. Assign a categorization to each risk.
4. On the Controls tab, select the appropriate control(s) for each risk finding. Note:
    - Multiple controls may be applied to a single finding.
    - Some controls may be used repeatedly or not at all.
5. If you need to reset the simulation to its initial state at any time, click the "Reset All" button.

5. A security analyst has prepared a vulnerability scan that contains all of the company's functional subnets. During the initial scan, users reported that network printers began to print pages that contained unreadable text and icons.

Which of the following should the analyst do to ensure this behavior does not oocur during subsequent vulnerability scans?

A. Perform non-credentialed scans.

B. Ignore embedded web server ports.

C. Create a tailored scan for the printer subnet.

D. Increase the threshold length of the scan timeout.

Answer: C

6. SIMULATION

An organization's website was maliciously altered.

INSTRUCTIONS

Review information in each tab to select the source IP the analyst should be concerned about, the indicator of compromise, and the two appropriate corrective actions.

Answer:

Step 1: Analyzing the SFTP Log

The SFTP log provides a record of file transfer and login activities:

User “sjames” logged in from several IP addresses:

7. While observing several host machines, a security analyst notices a program is overwritingdata to a buffer.

Which of the following controls will best mitigate this issue?

A. Data execution prevention

B. Output encoding

C. Prepared statements

D. Parameterized queries

Answer: A

8. A company is deploying new vulnerability scanning software to assess its systems. The current network is highly segmented, and the networking team wants to minimize the number of unique firewall rules.

Which of the following scanning techniques would be most efficient to achieve the objective?

A. Deploy agents on all systems to perform the scans.

B. Deploy a central scanner and perform non-credentialed scans.

C. Deploy a cloud-based scanner and perform a network scan.

D. Deploy a scanner sensor on every segment and perform credentialed scans.

Answer: A

9. A security analyst is investigating a compromised Linux server.
The analyst issues the ps command and receives the following output:

Which of the following commands should the administrator run next to further analyze the compromised system?
A. gbd /proc/1301
B. rpm -V openssh-server
C. /bin/Is -1 /proc/1301/exe
D. kill -9 1301

Answer: A

10. A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst.
Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?
A. SLA
B. MOU
C. NDA
D. Limitation of liability

Answer: A

11. How many employees Clicked on the link in the Phishing email?

12. An incident response team is working with law enforcement to investigate an active webserver compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must connect to a database server.

Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Select two).
A. Drop the tables on the database server to prevent data exfiltration.
B. Deploy EDR on the web server and the database server to reduce the adversariescapabilities.

C. Stop the httpd service on the web server so that the adversary can not use web exploits
D. use micro segmentation to restrict connectivity to/from the web and database servers.
E. Comment out the HTTP account in the / etc/passwd file of the web server
F. Move the database from the database server to the web server.

Answer: BD

13. A risk assessment concludes that the perimeter network has the highest potential for compromise by an attacker, and it is labeled as a critical risk environment.
Which of the following is a valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques?
A. A control that demonstrates that all systems authenticate using the approved authenticationmethod
B. A control that demonstrates that access to a system is only allowed by using SSH
C. A control that demonstrates that firewall rules are peer reviewed for accuracy and approvedbefore deployment
D. A control that demonstrates that the network security policy is reviewed and updated yearly

Answer: C

14. A security analyst needs to ensure that systems across the organization are protected based on the sensitivity of the content each system hosts. The analyst is working with the respective system owners to help determine the best methodology that seeks to promote confidentiality, availability, and integrity of the data being hosted.
Which of the following should the security analyst perform first to
categorize and prioritize the respective systems?
A. Interview the users who access these systems,
B. Scan the systems to see which vulnerabilities currently exist.
C. Configure alerts for vendor-specific zero-day exploits.
D. Determine the asset value of each system.

Answer: D

15. An analyst is evaluating a vulnerability management dashboard. The analyst sees that a previously remediated vulnerability has reappeared on a database server.
Which of the following is the most likely cause?
A. The finding is a false positive and should be ignored.
B. A rollback had been executed on the instance.
C. The vulnerability scanner was configured without credentials.
D. The vulnerability management software needs to be updated.

Answer: B

16. A disgruntled open-source developer has decided to sabotage a code repository with a logic bomb that will act as a wiper.
Which of the following parts of the Cyber Kill Chain does this act exhibit?
A. Reconnaissance
B. Weaponization
C. Exploitation
D. Installation

Answer: B

17. A systems administrator receives reports of an internet-accessible Linux server that is running very sluggishly. The administrator examines the server, sees a high amount of memory utilization, and suspects a DoS attack related to half-open TCP sessions consuming memory.
Which of the following tools would best help to prove whether this server was experiencing this behavior? A. Nmap
B. TCPDump
C. SIEM
D. EDR

Answer: B

18. A Chief Information Officer wants to implement a BYOD strategy for all company laptops and mobile phones. The Chief Information Security Officer is concerned with ensuring all devices are patched and running some sort of protection against malicious software.
Which of the following existing technical controls should a security analyst recommend to best meet all the requirements?
A. EDR
B. Port security
C. NAC
D. Segmentation

Answer: A

19. During a cybersecurity incident, one of the web servers at the perimeter network was affected by ransomware.
Which of the following actions should be performed immediately?
A. Shut down the server. B. Reimage the server
C. Quarantine the server
D. Update the OS to latest version.

Answer: C

20. An analyst discovers unusual outbound connections to an IP that was previously blocked at the web proxy and firewall. Upon further investigation, it appears that the proxy and firewall rules that were in place were removed by a service account that is not recognized.
Which of the following parts of the Cyber Kill Chain does this describe?
A. Delivery
B. Command and control
C. Reconnaissance
D. Weaporization

Answer: B

21. A security team is concerned about recent Layer 4 DDoS attacks against the company website.
Which of the following controls would best mitigate the attacks?
A. Block the attacks using firewall rules.
B. Deploy an IPS in the perimeter network.
C. Roll out a CDN.
D. Implement a load balancer.

Answer: C

22. A cybersecurity analyst is recording the following details
* ID
* Name
* Description
* Classification of information
* Responsible party
In which of the following documents is the analyst recording this information?
A. Risk register
B. Change control documentation
C. Incident response playbook
D. Incident response plan

Answer: A

23. A security analyst is working on a server patch management policy that will allow the infrastructure team to be informed more quickly about new patches.
Which of the following would most likely be required by the infrastructure team so that vulnerabilities can be remediated quickly? (Select two).

A. Hostname
B. Missing KPI
C. CVE details
D. POC availability
E. loCs
F. npm identifier

Answer: CE

24. An end-of-life date was announced for a widely used OS. A business-critical function is performed by some machinery that is controlled by a PC, which is utilizing the OS that is approaching the end-of-life date.
Which of the following best describes a security analyst's concern?
A. Any discovered vulnerabilities will not be remediated.
B. An outage of machinery would cost the organization money.
C. Support will not be available for the critical machinery
D. There are no compensating controls in place for the OS.

Answer: A

25. A company has the following security requirements:
. No public IPs
? All data secured at rest
. No insecure ports/protocols
After a cloud scan is completed, a security analyst receives reports that several misconfigurations are putting the company at risk.
Given the following cloud scanner output:
Which of the following should the analyst recommend be updated first to meet the security requirements and reduce risks?
A. VM_PRD_DB
B. VM_DEV_DB
C. VM_DEV_Web02
D. VM_PRD_Web01

Answer: D

26. A security analyst discovers an ongoing ransomware attack while investigating a phishing email. The analyst downloads a copy of the file from the email and isolates the affected workstation from the network.
Which of the following activities should the analyst perform next?
A. Wipe the computer and reinstall software
B. Shut down the email server and quarantine it from the network.
C. Acquire a bit-level image of the affected workstation.
D. Search for other mail users who have received the same file.
Answer: C

27. Which of the following stakeholders are most likely to receive a vulnerability scan report? (Select two).

A. Executive management
B. Law enforcement
C. Marketing
D. Legal
E. Product owner
F. Systems admininstration

Answer: EF

28. The Chief Information Security Officer for an organization recently received approval to install a new EDR solution. Following the installation, the number of alerts that require remediation by an analyst has tripled.
Which of the following should the organization utilize to best centralize the workload for the internal security team? (Select two).

A. SOAR
B. SIEM
C. MSP
D. NGFW
E. XDR
F. DLP

Answer: AB Explanation:

29. A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network.
Which of the following would best aid in decreasing the workload without increasing staff?

A. SIEM
B. XDR
C. SOAR
D. EDR

Answer: C

30. How many employees clicked on the link in the phishing email?

Answer: According to the email server logs, 25 employees clicked on the link in the phishing email.

31. A security analyst needs to mitigate a known, exploited vulnerability related not tack vector that embeds software through the USB interface.
Which of the following should the analyst do first?
A. Conduct security awareness training on the risks of using unknown and unencrypted USBs.
B. Write a removable media policy that explains that USBs cannot be connected to a companyasset.
C. Check configurations to determine whether USB ports are enabled on company assets.
D. Review logs to see whether this exploitable vulnerability has already impacted the company.

Answer: C

32. A security analyst reviews the latest vulnerability scans and observes there are vulnerabilities with similar CVSSv3 scores but different base score metrics.
Which of the following attack vectors should the analyst remediate first?
A. CVSS 3.0/AVP/AC:L/PR:L/UI:N/S U/C:H/I:H/A:H
B. CVSS 3.0/AV:A/AC .L/PR:L/UI:N/S:U/C:H/I:H/A:H
C. CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S;U/C:H/I:H/A:H
D. CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Answer: C

33. During an incident involving phishing, a security analyst needs to find the source of the malicious email.
Which of the following techniques would provide the analyst with this information?
A. Header analysis
B. Packet capture
C. SSL inspection
D. Reverse engineering

Answer: A

34. An organization has established a formal change management process after experiencing several critical system failures over the past year.
Which of the following are key factors that the change management process will include in order to reduce the impact of system failures? (Select two).
A. Ensure users the document system recovery plan prior to deployment.
B. Perform a full system-level backup following the change.
C. Leverage an audit tool to identify changes that are being made.
D. Identify assets with dependence that could be impacted by the change.
E. Require diagrams to be completed for all critical systems.
F. Ensure that all assets are properly listed in the inventory management system.

Answer: DF

35. A company is in the process of implementing a vulnerability management program, and there are concerns about granting the security team access to sensitive data.
Which of the following scanning methods can be implemented to reduce the access to systems while providing the most accurate vulnerability scan results?
A. Credentialed network scanning
B. Passive scanning
C. Agent-based scanning
D. Dynamic scanning

Answer: C

36. Following an attack, an analyst needs to provide a summary of the event to the Chief Information Security Officer. The summary needs to include the who-what-when information and evaluate the effectiveness of the plans in place.
Which of the following incident management life cycle processes
does this describe?
A. Business continuity plan
B. Lessons learned
C. Forensic analysis
D. Incident response plan

Answer: B

37. A systems administrator is reviewing after-hours traffic flows from data-center servers and sees regular outgoing HTTPS connections from one of the servers to a public IP address. The server should not be making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well.
Which of the following is the most likely explanation?
A. C2 beaconing activity
B. Data exfiltration
C. Anomalous activity on unexpected ports
D. Network host IP address scanning
E. A rogue network device

Answer: A

38. A security analyst is reviewing the following alert that was triggered by FIM on a critical system:

Which of the following best describes the suspicious activity that is occurring?
A. A fake antivirus program was installed by the user.
B. A network drive was added to allow exfiltration of data
C. A new program has been set to execute on system start
D. The host firewall on 192.168.1.10 was disabled.

Answer: C

39. A company that has a geographically diverse workforce and dynamic IPs wants to implement a vulnerability scanning method with reduced network traffic.
Which of the following would best meet this requirement?
A. External
B. Agent-based
C. Non-credentialed
D. Credentialed

Answer: B

40. The security analyst received the monthly vulnerability report.
The following findings were included in the report
• Five of the systems only required a reboot to finalize the patch application.
• Two of the servers are running outdated operating systems and cannot be patched
The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them.
Which of the following approaches will best minimize the risk of the outdated servers being compromised?
A. Compensating controls
B. Due diligence
C. Maintenance windows
D. Passive discovery

Answer: A

41. There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat.
Which of the following security controls would best support the company in this scenario?
A. Implement step-up authentication for administrators
B. Improve employee training and awareness
C. Increase password complexity standards
D. Deploy mobile device management

Answer: B

42. A company brings in a consultant to make improvements to its website. After the consultant leaves. a web developer notices unusual activity on the website and submits a suspicious file containing the following code to the security team:

Which of the following did the consultant do?

Implanted a backdoor
Implemented privilege escalation
Implemented clickjacking
Patched the web server

Answer: A

43. An incident response analyst is taking over an investigation from another analyst. The investigation has been going on for the past few days.
Which of the following steps is most important during the transition between the two analysts?
A. Identify and discuss the lessons learned with the prior analyst.
B. Accept all findings and continue to investigate the next item target.
C. Review the steps that the previous analyst followed.
D. Validate the root cause from the prior analyst.

Answer: C

44. Legacy medical equipment, which contains sensitive data, cannot be patched.
Which of the following is the best solution to improve the equipment's security posture?
A. Move the legacy systems behind a WAR
B. Implement an air gap for the legacy systems.
C. Place the legacy systems in the perimeter network.
D. Implement a VPN between the legacy systems and the local network.

Answer: B

45. Which of the following threat actors is most likely to target a company due to its questionable environmental policies?
A. Hacktivist
B. Organized crime
C. Nation-state
D. Lone wolf

Answer: A

46. An organization's email account was compromised by a bad actor. Given the following Information:

Which of the following is the length of time the team took to detect the threat?
A. 25 minutes
B. 40 minutes
C. 45 minutes
D. 2 hours

Answer: A

47. A development team is preparing to roll out a beta version of a web application and wants to quickly test for vulnerabilities, including SQL injection, path traversal, and cross-site scripting. Which of the following tools would the security team most likely recommend to perform this test?
A. Has heat
B. OpenVAS
C. OWASP ZAP
D. Nmap

Answer: C

48. On how many workstations was the malware installed?

Answer: According to the file server logs, the malware was installed on 15 workstations.

49. A security analyst must preserve a system hard drive that was involved in a litigationrequest. Which of the following is the best method to ensure the data on the device is not modified?
A. Generate a hash value and make a backup image.
B. Encrypt the device to ensure confidentiality of the data.
C. Protect the device with a complex password.
D. Perform a memory scan dump to collect residual data.

Answer: A

50. Which of the following would eliminate the need for different passwords for a variety or internal application?

A. CASB

B. SSO

C. PAM

D. MFA

Answer: B

51. A security analyst is analyzing the following output from the Spider tab of OWASP ZAP after a vulnerability scan was completed:

Which of the following options can the analyst conclude based on the provided output?

A. The scanning vendor used robots to make the scanning job faster

B. The scanning job was successfully completed, and no vulnerabilities were detected

C. The scanning job did not successfully complete due to an out of scope error

D. The scanner executed a crawl process to discover pages to be assessed

Answer: D

52. A security analyst has identified a new malware file that has impacted the organization. The malware is polymorphic and has built-in conditional triggers that require a connection to the internet. The CPU has an idle process of at least 70%.

Which of the following best describes how the security analyst can effectively review the malware without compromising the organization's network?

A. Utilize an RDP session on an unused workstation to evaluate the malware.

B. Disconnect and utilize an existing infected asset off the network.

C. Create a virtual host for testing on the security analyst workstation.

D. Subscribe to an online service to create a sandbox environment.

Answer: D

53. The SOC received a threat intelligence notification indicating that an employee's credentials were found on the dark web. The user's web and log-in activities were reviewed for malicious or anomalous connections, data uploads/downloads, and exploits. A review of the controls confirmed multifactor authentication was enabled.
Which of the following should be done first to mitigate impact to the business networks and assets?
A. Perform a forced password reset.
B. Communicate the compromised credentials to the user.
C. Perform an ad hoc AV scan on the user's laptop.
D. Review and ensure privileges assigned to the user's account reflect least privilege.
E. Lower the thresholds for SOC alerting of suspected malicious activity.

Answer: A

54. A security analyst responds to a series of events surrounding sporadic bandwidth consumption from an endpoint device.
The security analyst then identifies the following additional details:
• Bursts of network utilization occur approximately every seven days.
• The content being transferred appears to be encrypted or obfuscated.
• A separate but persistent outbound TCP connection from the host to infrastructure in a third-party cloud is in place.
• The HDD utilization on the device grows by 10GB to 12GB over the course of every sevendays.
• Single file sizes are 10GB.
Which of the following describes the most likely cause of the issue?
A. Memory consumption
B. Non-standard port usage
C. Data exfiltration
D. System update
E. Botnet participant

Answer: C

55. A security analyst is validating a particular finding that was reported in a web application vulnerability scan to make sure it is not a false positive.
The security analyst uses the snippet below:

Which of the following vulnerability types is the security analyst validating?
A. Directory traversal
B. XSS
C. XXE
D. SSRF

Answer: B

56. While reviewing system logs, a network administrator discovers the following entry:
Which of the following occurred?
A. An attempt was made to access a remote workstation.
B. The PsExec services failed to execute.
C. A remote shell failed to open.
D. A user was trying to download a password file from a remote system.

Answer: D

57. An analyst is designing a message system for a bank. The analyst wants to include a feature that allows the recipient of a message to prove to a third party that the message came from the sender.
Which of the following information security goals is the analyst most likely trying to achieve?
A. Non-repudiation
B. Authentication
C. Authorization
D. Integrity

Answer: A

58. A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URIs that should be denied access prior to more in-depth scanning.
Which of following best fits the type of scanning activity requested?
A. Uncredentialed scan
B. Discqyery scan
C. Vulnerability scan
D. Credentialed scan

Answer: B

59. Which of the following will most likely cause severe issues with authentication and logging?
A. Virtualization
B. Multifactor authentication
C. Federation
D. Time synchronization

Answer: D

60. The security team reviews a web server for XSS and runs the following Nmap scan:

Which of the following most accurately describes the result of the scan?
A. An output of characters > and " as the parameters used m the attempt
B. The vulnerable parameter ID hccp://l72.31.15.2/1.php?id-2 and unfiltered characters returned
C. The vulnerable parameter and unfiltered or encoded characters passed > and " as unsafe
D. The vulnerable parameter and characters > and " with a reflected XSS attempt

Answer: D

61. During the forensic analysis of a compromised machine, a security analyst discovers some binaries
that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content.
Which of the following is the next step the analyst should take?
A. Validate the binaries' hashes from a trusted source.
B. Use file integrity monitoring to validate the digital signature
C. Run an antivirus against the binaries to check for malware.
D. Only allow binaries on the approve list to execute.

Answer: A

62. An organization is conducting a pilot deployment of an e-commerce application. The application's source code is not available.
Which of the following strategies should an analyst recommend to evaluate the security of the software?
A. Static testing
B. Vulnerability testing
C. Dynamic testing
D. Penetration testing

Answer: C

63. An organization was compromised, and the usernames and passwords of all employees were leaked online.
Which of the following best describes the remediation that could reduce the impact of this situation?
A. Multifactor authentication
B. Password changes
C. System hardening
D. Password encryption

Answer: B

64. Which of the following describes the difference between intentional and unintentional insider threats?

A. Their access levels will be different

B. The risk factor will be the same

C. Their behavior will be different

D. The rate of occurrence will be the same

Answer: C

Question 1 (Exam A)

A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

- **Answer: A.** CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:K/A:L

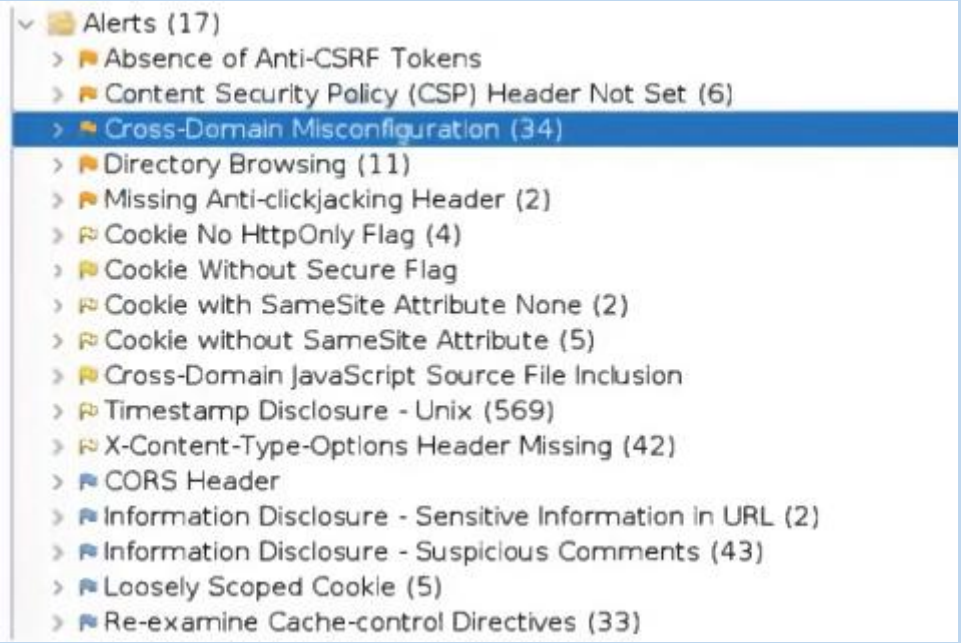
Question 2 (Exam A)

Which of the following tools would work best to prevent the exposure of PII outside of an organization?

- **Answer: D.** DLP

Question 3 (Exam A)

An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



Which of the following tuning recommendations should the security analyst share?

- **Answer: C.** Configure an Access-Control-Allow-Origin header to authorized domains

Question 4 (Exam A)

Which of the following items should be included in a vulnerability scan report? (Choose two.)

- **Answer: D.** Affected hosts
- **Answer: E.** Risk score

Question 5 (Exam A)

The Chief Executive Officer of an organization recently heard that exploitation of new attacks in the industry was happening approximately 45 days after a patch was released. Which of the following would best protect this organization?

- **Answer: A.** A mean time to remediate of 30 days

Question 6 (Exam A)

A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:

```
foreach ($user in Get-Content .\this.txt)
{
    Get-ADUser $user -Properties primaryGroupID |select-object primaryGroupID
    Add-ADGroupMember "Domain Users" -Members $user
    Set-ADUser $user -Replace @{primaryGroupID=513}
}
```

Which of the following scripting languages was used in the script?

- **Answer: A.** PowerShell

Question 7 (Exam A)

A company's user accounts have been compromised. Users are also reporting that the company's internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?

- **Answer: B.** An on-path attack is being performed by someone with internal access that forces users into port 80

Question 8 (Exam A)

A security analyst is tasked with prioritizing vulnerabilities for remediation. The relevant company security policies are shown below:
Security Policy 1006: Vulnerability Management
1. The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.
2. In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.
3. The Company shall prioritize patching of publicly available systems and services over patching of internally available system.
According to the security policy, which of the following vulnerabilities should be the highest priority to patch?

- **Answer: B.** Name: CAP.SHIELD
CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
External System

Question 9 (Exam A)

Which of the following will most likely ensure that mission-critical services are available in the event of an incident?

- **Answer: A.** Business continuity plan

Question 10 (Exam A)

The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

- **Answer: A.** Deploy a CASB and enable policy enforcement

Question 11 (Exam A)

An incident response team receives an alert to start an investigation of an internet outage. The outage is preventing all users in multiple locations from accessing external SaaS resources. The team determines the organization was impacted by a DDoS attack. Which of the following logs should the team review first?

- **Answer: C.** DNS

Question 12 (Exam A)

A malicious actor has gained access to an internal network by means of social engineering. The actor does not want to lose access in order to continue the attack. Which of the following best describes the current stage of the Cyber Kill Chain that the threat actor is currently operating in?

- **Answer: D.** Exploitation

Question 13 (Exam A)

An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?

- **Answer: B.** Reconnaissance

Question 14 (Exam A)

An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. Which of the following best describes what is happening? (Choose two.)

- **Answer: C.** Social engineering attack
- **Answer: E.** Obfuscated links

Question 15 (Exam A)

During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

- **Answer: C.** Use application security scanning as part of the pipeline for the CI/CD flow

Question 16 (Exam A)

An analyst is reviewing a vulnerability report and must make recommendations to the executive team. The analyst finds that most systems can be upgraded with a reboot resulting in a single downtime window. However, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. Which of the following inhibitors to remediation do these systems and associated vulnerabilities best represent?

- **Answer: A.** Proprietary systems

Question 17 (Exam A)

The security team reviews a web server for XSS and runs the following Nmap scan:

```
#nmap -p80 --script http-unsafe-output-escaping 172.31.15.2

PORT     STATE    SERVICE REASON
80/tcp   open     http    syn-ack
| http-unsafe-output-escaping:
|_ Characters [> " '] reflected in parameter id at
http://172.31.15.2/1.php?id=2
```

Which of the following most accurately describes the result of the scan?

- **Answer: D.** The vulnerable parameter and characters > and " with a reflected XSS attempt

Question 18 (Exam A)

Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

- **Answer: B.** Schedule a review with all teams to discuss what occurred

Question 19 (Exam A)

A security analyst received a malicious binary file to analyze. Which of the following is the best technique to perform the analysis?

- **Answer: C.** Reverse engineering

Question 20 (Exam A)

An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

- **Answer: D.** Routing table

Question 21 (Exam A)

Which of the following security operations tasks are ideal for automation?

- **Answer: D.** Email header analysis:
  Check the email header for a phishing confidence metric greater than or equal to five
  Add the domain of sender to the block list
  Move the email to quarantine

Question 22 (Exam A)

An organization has experienced a breach of customer transactions. Under the terms of PCI DSS, which of the following groups should the organization report the breach to?

- **Answer: D.** Card issuer

Question 23 (Exam A)

Which of the following is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system?

- **Answer: A.** Mean time to detect

Question 24 (Exam A)

A company is implementing a vulnerability management program and moving from an on-premises environment to a hybrid IaaS cloud environment. Which of the following implications should be considered on the new hybrid environment?

- **Answer: B.** Cloud-specific misconfigurations may not be detected by the current scanners

Question 25 (Exam A)

A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user's workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?

- **Answer: B.** Ensure that the case details do not reflect any user-identifiable information
Password protect the evidence and restrict access to personnel related to the investigation

Question 26 (Exam A)

Which of the following is the first step that should be performed when establishing a disaster recovery plan?

- **Answer: A.** Agree on the goals and objectives of the plan

Question 27 (Exam A)

A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

- **Answer: C.** Validation

Question 28 (Exam A)

The analyst reviews the following endpoint log entry:

```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {HOSTName}
clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {net user /add invoke_u1}
The command completed successfully.
```

Which of the following has occurred?

- **Answer: C.** New account introduced

Question 29 (Exam A)

A security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM. The analyst no longer had to jump between tools. Which of the following best describes what the security program did?

- **Answer: D.** Single pane of glass

Question 30 (Exam A)

Due to reports of unauthorized activity that was occurring on the internal network, an analyst is performing a network discovery. The analyst runs an Nmap scan against a corporate network to evaluate which devices were operating in the environment. Given the following output:

Which of the following choices should the analyst look at first?

- **Answer: E.** p4wnp1_aloa.lan (192.168.86.56)

```
Nmap scan report for officerokuplayer.lan (192.168.86.22)
Host is up (0.11s latency).
All 100 scanned ports on officerokuplayer.lan (192.168.86.22) are filtered
MAC Address: B8:3E:59:86:1A:13 (Roku)

Nmap scan report for p4wnp1_aloa.lan (192.168.86.56)
Host is up (0.022s latency).
Not shown: 96 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
8000/tcp  open  http-alt
MAC Address: B8:27:EB:D0:8E:D1 (Raspberry Pi Foundation)

Nmap scan report for wh4dc-748gy.lan (192.168.86.152)
Host is up (0.033s latency).
Not shown: 95 filtered ports
PORT     STATE SERVICE
80/tcp    open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 38:BA:F8:E3:41:CB (Intel Corporate)

Nmap scan report for xlaptop.lan (192.168.86.249)
Host is up (0.024s latency).
Not shown: 93 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 64:00:6A:8E:D8:F5 (Dell)

Nmap scan report for imaging.lan (192.168.86.150)
Host is up (0.0013s latency).
Not shown: 95 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 38:BA:F8:F4:32:CA (Intel Corporate)
```