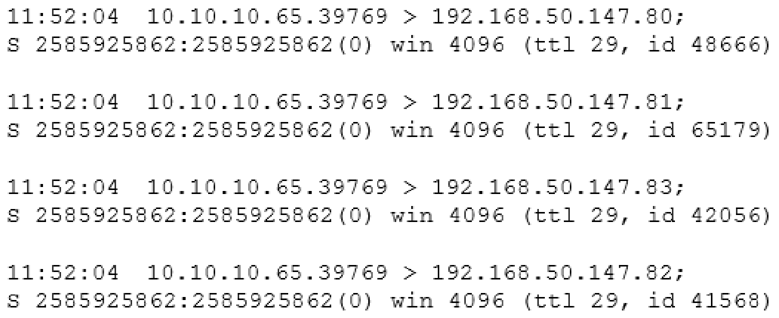
CompTIA CS0-001 Exam

Volume: 75 Questions

Question No: 1

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

Answer: B

Question No: 2

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.

A. 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. Once the simulation is submitted, please select the Next button to continue.

B. 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.

C. 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.

Answer: C

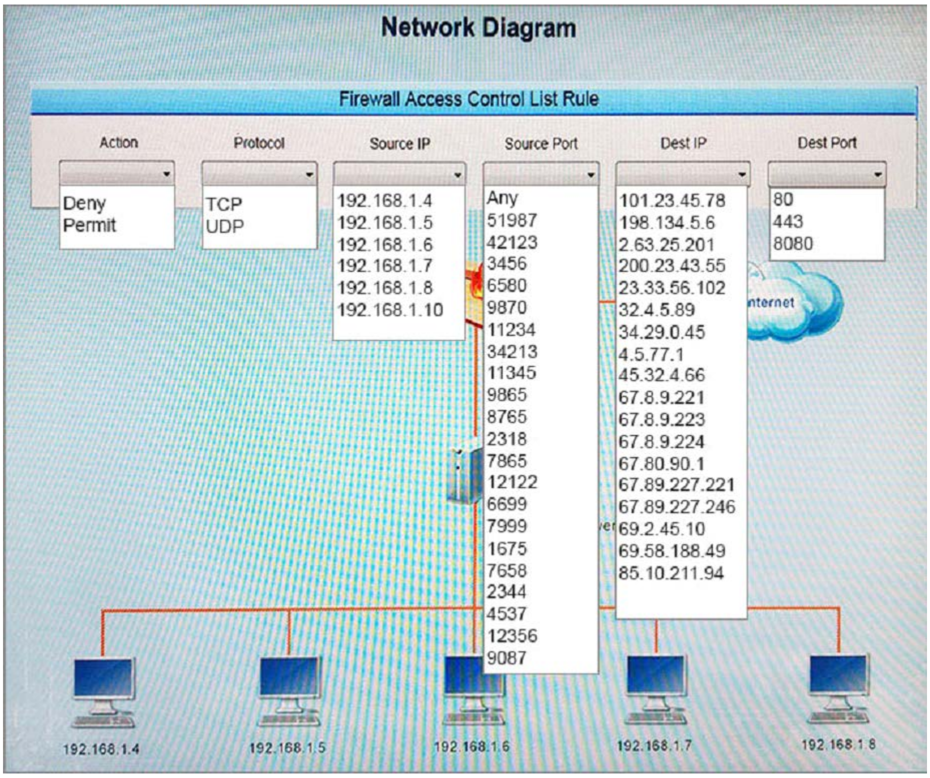
Question No: 3 HOTSPOT

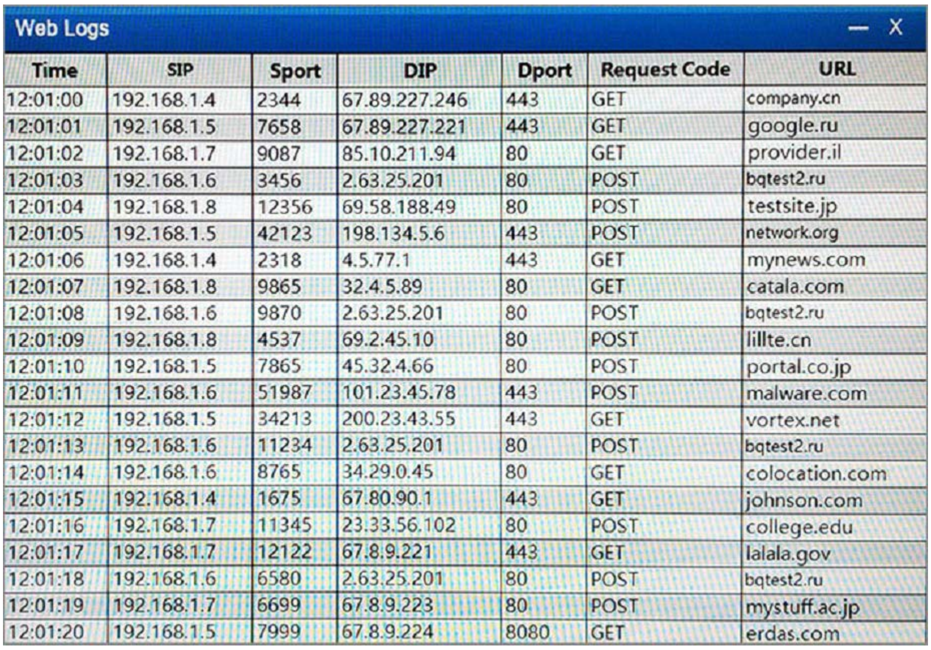
A security analyst suspects that a workstation may be beaconing to a command and control server.

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.

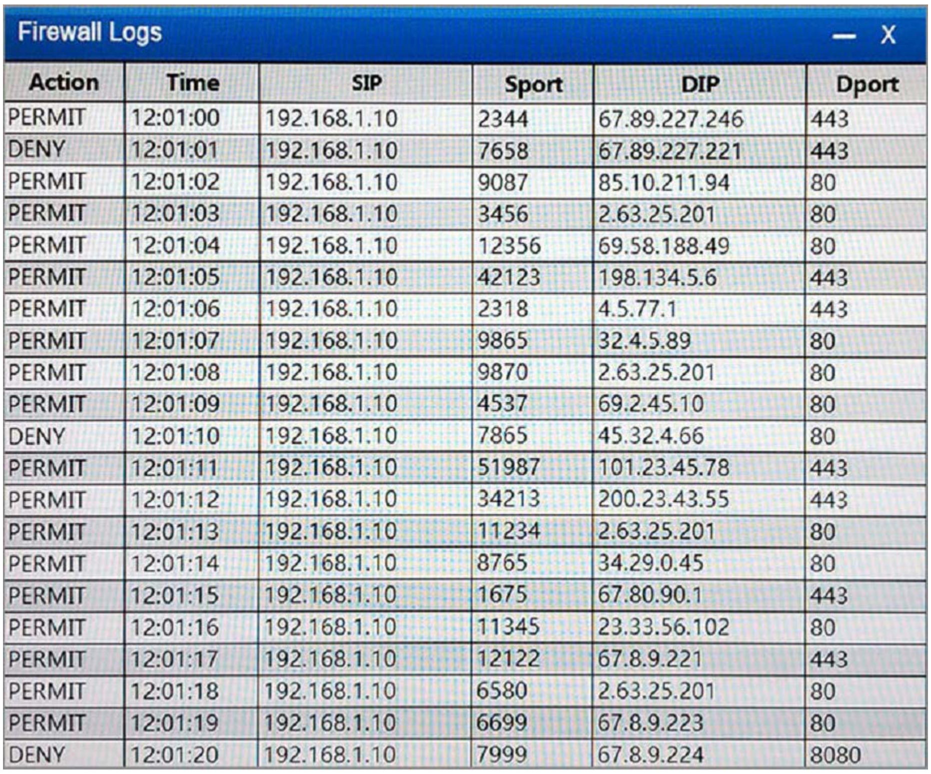
Instructions:

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.





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
12:01:16	192.168.1.7	11345	23.33.56.102	80	POST	college.edu
12:01:17	192.168.1.7	12122	67.8.9.221	443	GET	lalala.gov
12:01:18	192.168.1.6	6580	2.63.25.201	80	POST	bqtest2.ru
12:01:19	192.168.1.7	6699	67.8.9.223	80	POST	mystuff.ac.jp
12:01:20	192.168.1.5	7999	67.8.9.224	8080	GET	erdas.com



Action	Time	SIP	Sport	DIP	Dport
PERMIT	12:01:00	192.168.1.10	2344	67.89.227.246	443
DENY	12:01:01	192.168.1.10	7658	67.89.227.221	443
PERMIT	12:01:02	192.168.1.10	9087	85.10.211.94	80
PERMIT	12:01:03	192.168.1.10	3456	2.63.25.201	80
PERMIT	12:01:04	192.168.1.10	12356	69.58.188.49	80
PERMIT	12:01:05	192.168.1.10	42123	198.134.5.6	443
PERMIT	12:01:06	192.168.1.10	2318	4.5.77.1	443
PERMIT	12:01:07	192.168.1.10	9865	32.4.5.89	80
PERMIT	12:01:08	192.168.1.10	9870	2.63.25.201	80
PERMIT	12:01:09	192.168.1.10	4537	69.2.45.10	80
DENY	12:01:10	192.168.1.10	7865	45.32.4.66	80
PERMIT	12:01:11	192.168.1.10	51987	101.23.45.78	443
PERMIT	12:01:12	192.168.1.10	34213	200.23.43.55	443
PERMIT	12:01:13	192.168.1.10	11234	2.63.25.201	80
PERMIT	12:01:14	192.168.1.10	8765	34.29.0.45	80
PERMIT	12:01:15	192.168.1.10	1675	67.80.90.1	443
PERMIT	12:01:16	192.168.1.10	11345	23.33.56.102	80
PERMIT	12:01:17	192.168.1.10	12122	67.8.9.221	443
PERMIT	12:01:18	192.168.1.10	6580	2.63.25.201	80
PERMIT	12:01:19	192.168.1.10	6699	67.8.9.223	80
DENY	12:01:20	192.168.1.10	7999	67.8.9.224	8080

Answer: DENY TCP 192.168.1.5 7999 67.8.9.224 8080

Question No: 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

Answer: A

Question No: 5
After analyzing and correlating activity from multiple sensors, the security analyst has determined a group from a high-risk country is responsible for a sophisticated breach of the company network and continuous administration of targeted attacks for the past three months. Until now, the attacks went unnoticed. This is an example of:

A. privilege escalation.

B. advanced persistent threat.

C. malicious insider threat.

D. spear phishing.

Answer: B

Question No: 6
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

Answer: B

Question No: 7

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

Answer: A

Question No: 8

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.

Answer: B

Question No: 9

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.

Answer: D

Question No: 10
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.

Answer: B

Question No: 11
File integrity monitoring states the following files have been changed without a written request or approved change. The following change has been made:
ch mod 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.

Answer: C

Question No: 12

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.

Answer: C

Question No: 13

A cybersecurity analyst is currently investigating a server outage. The analyst has discovered the following value was entered for the username: Oxbfff601a. 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

Answer: D

Question No: 14

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

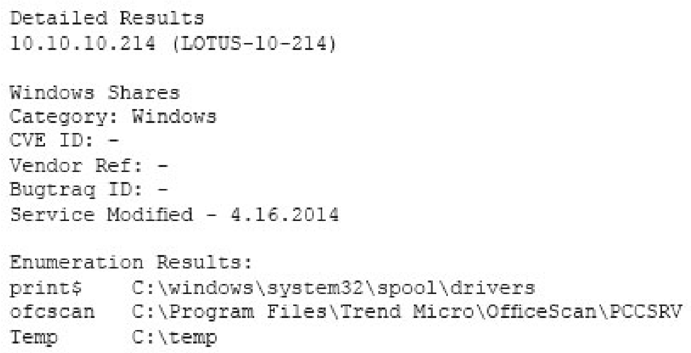
B. Regression testing

C. Input validation

D. Fuzzing

Answer: A

Question No: 15
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.

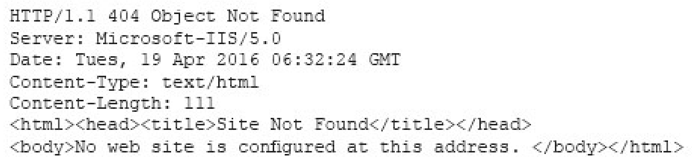
B. Connecting to the host using a null session allows enumeration of share names.

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.

Answer: B

Question No: 16
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 "Allow late scanning" to 1 in the URLScan.ini configuration file.

B. Set "Remove server header" to 1 in the URLScan.ini configuration file.

C. Set "Enable logging" to O in the URLScan.ini configuration file.

D. Set "Perprocess logging" to 1 in the URLScan.ini configuration file.

Answer: A,B,C,D

Question No: 17
An analyst has initiated an assessment of an organization's security posture. As a part of this review, the analyst would like to determine how much information about the organization is exposed externally. Which of the following techniques would BEST help the analyst accomplish this goal? (Select two.)

A. Fingerprinting

B. DNS query log reviews

C. Banner grabbing

D. Internet searches

E. Intranet portal reviews

F. Sourcing social network sites

G. Technical control audits

Answer: A,F

Question No: 18
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.

Answer: D

Question No: 19
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.

Answer: D

Question No: 20
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.lx backed by a RADIUS or LDAP server.

Answer: C

Question No: 21
An analyst was tasked with providing recommendations of technologies that are PKI X.509 compliant for a