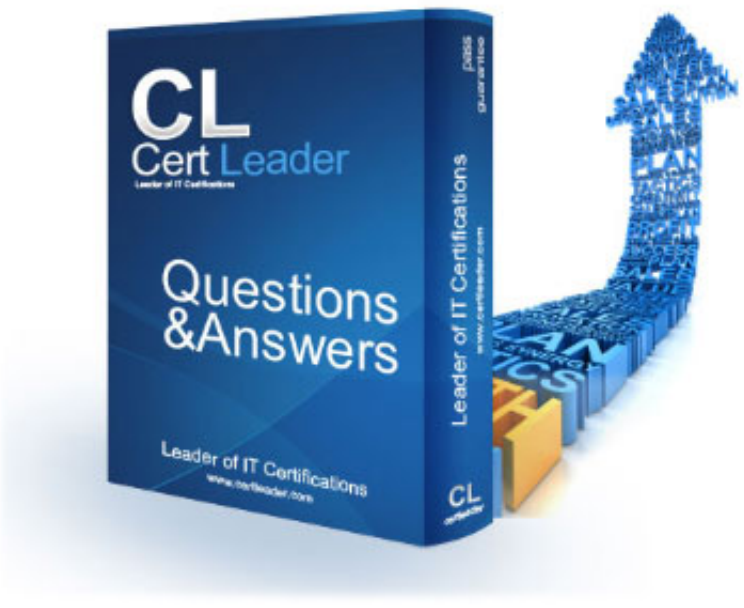
CS0-001 Dumps

CompTIA CSA+ Certification Exam

https://www.certleader.com/CS0-001-dumps.html

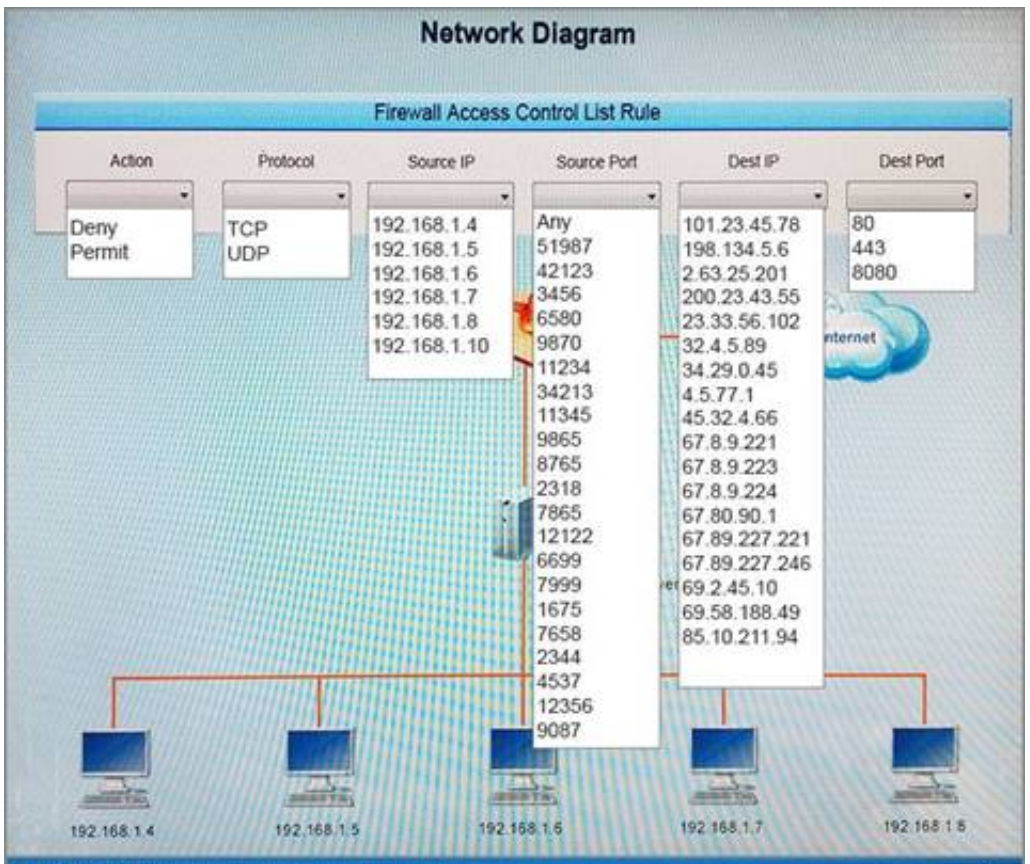


NEW QUESTION 1
Company A permits visiting business partners from Company B to utilize Ethernet ports available in Company A's conference rooms. This access is provided to allow partners the ability to establish VPNs back to Company B's network. The security architect for Company A wants to ensure partners 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 2
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.



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

Answer:

Explanation: DENYTCP 192.168.1.5 7999 67.8.9.2248080

NEW QUESTION 3
Several users have reported that when attempting to save documents in team folders, the following message is received:
The File Cannot Be Copied or Moved – Service Unavailable.
Upon further investigation, it is found that the syslog server is not obtaining log events from the file server to which the users are attempting to copy files. Which of the following is the MOST likely scenario causing these issues?

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

Answer: A

NEW QUESTION 4
A cybersecurity analyst is completing an organization's vulnerability report and wants it to reflect assets accurately. Which of the following items should be in the report?

A. Processor utilization
B. Virtual hosts
C. Organizational governance
D. Log disposition
E. Asset isolation

Answer: B

NEW QUESTION 5
Management is concerned with administrator access from outside the network to a key server in the company. Specifically, firewall rules allow access to the server from anywhere in the company. Which of the following would be an effective solution?

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

Answer: B

NEW QUESTION 6
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 7
Which of the following best practices is used to identify areas in the network that may be vulnerable to penetration testing from known external sources?

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

Answer: A

NEW QUESTION 8
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 9
As part of an upcoming engagement for a client, an analyst is configuring a penetration testing application to ensure the scan complies with information defined in the SOW. Which of the following types of information should be considered based on information traditionally found in the SOW? (Select two.)

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

Answer: AC

NEW QUESTION 10

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

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

Answer: C

NEW QUESTION 10
A security professional is analyzing the results of a network utilization report. The report includes the following information:

IP Address	Server Name	Server Uptime	Historical	Current
172.20.2.58	web.srvr.03	30D 12H 52M 09S	41.3GB	37.2GB
172.20.1.215	dev.web.srvr.01	30D 12H 52M 09S	1.81GB	2.2GB
172.20.1.22	hr.dbprod.01	30D 12H 17M 22S	2.24GB	29.97GB
172.20.1.26	mrktg.file.srvr.02	30D 12H 41M 09S	1.23GB	0.34GB
172.20.1.28	accnt.file.srvr.01	30D 12H 52M 09S	3.62GB	3.57GB
172.20.1.30	R&D.file.srvr.01	1D 4H 22M 01S	1.24GB	0.764GB

Which of the following servers needs further investigation?

A. hr.dbprod.01
B. R&D.file.srvr.01
C. mrktg.file.srvr.02
D. web.srvr.03

Answer: A

NEW QUESTION 15
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 20
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 23
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 26
A security administrator determines several months after the first instance that a local privileged user has been routinely logging into a server interactively as "root" and browsing the Internet. The administrator determines this by performing an annual review of the security logs on that server. For which of the following security architecture areas should the administrator recommend review and modification? (Select TWO).

A. Log aggregation and analysis
B. Software assurance
C. Encryption
D. Acceptable use policies

E. Password complexity
F. Network isolation and separation

Answer: AD

NEW QUESTION 30
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 33
An organization has recently recovered from an incident where a managed switch had been accessed and reconfigured without authorization by an insider. The incident response team is working on developing a lessons learned report with recommendations. Which of the following recommendations will BEST prevent the same attack from occurring in the future?

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

Answer: B

NEW QUESTION 37
An organization is requesting the development of a disaster recovery plan. The organization has grown and so has its infrastructure. Documentation, policies, and procedures do not exist. Which of the following steps should be taken to assist in the development of the disaster recovery plan?

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

Answer: D

NEW QUESTION 38
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 42
A threat intelligence feed has posted an alert stating there is a critical vulnerability in the kernel. Unfortunately, the company's asset inventory is not current. Which of the following techniques would a cybersecurity analyst perform to find all affected servers within an organization?

A. A manual log review from data sent to syslog
B. An OS fingerprinting scan across all hosts
C. A packet capture of data traversing the server network
D. A service discovery scan on the network

Answer: B

NEW QUESTION 43
Which of the following policies BEST explains the purpose of a data ownership policy?

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

Answer: D

NEW QUESTION 45
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 46
Which of the following is MOST effective for correlation analysis by log for threat management?

A. PCAP
B. SCAP
C. IPS
D. SIEM

Answer: D

NEW QUESTION 51
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 53
Which of the following commands would a security analyst use to make a copy of an image for forensics use?

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

Answer: A

NEW QUESTION 55
After running a packet analyzer on the network, a security analyst has noticed the following output:

```
11:52:04  10.10.10.65.39769 > 192.168.50.147.80;
S 2585925862:2585925862(0) win 4096 (ttl 29, id 48666)

11:52:04  10.10.10.65.39769 > 192.168.50.147.81;
S 2585925862:2585925862(0) win 4096 (ttl 29, id 65179)

11:52:04  10.10.10.65.39769 > 192.168.50.147.83;
S 2585925862:2585925862(0) win 4096 (ttl 29, id 42056)

11:52:04  10.10.10.65.39769 > 192.168.50.147.82;
S 2585925862:2585925862(0) win 4096 (ttl 29, id 41568)
```

Which of the following is occurring?

A. A ping sweep
B. A port scan
C. A network map
D. A service discovery

Answer: B

NEW QUESTION 56
A security analyst is performing a review of Active Directory and discovers two new user accounts in the accounting department. Neither of the users has elevated permissions, but accounts in the group are given access to the company's sensitive financial management application by default. Which of the following is the BEST course of action?

A. Follow the incident response plan for the introduction of new accounts
B. Disable the user accounts
C. Remove the accounts' access privileges to the sensitive application

D. Monitor the outbound traffic from the application for signs of data exfiltration
E. Confirm the accounts are valid and ensure role-based permissions are appropriate

Answer: E

NEW QUESTION 57
A cybersecurity analyst has received an alert that well-known “call home” messages are continuously observed by network sensors at the network boundary. The proxy firewall successfully drops the messages. After determining the alert was a true positive, which of the following represents the MOST likely cause?

A. Attackers are running reconnaissance on company resources.
B. An outside command and control system is attempting to reach an infected system.
C. An insider is trying to exfiltrate information to a remote network.
D. Malware is running on a company system.

Answer: B

NEW QUESTION 61
A security audit revealed that port 389 has been used instead of 636 when connecting to LDAP for the authentication of users. The remediation recommended by the audit was to switch the port to 636 wherever technically possible. Which of the following is the BEST response?

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

Answer: B

NEW QUESTION 64
A vulnerability scan has returned the following information:

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

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

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

Which of the following describes the meaning of these results?

A. There is an unknown bug in a Lotus server with no Bugtraq ID.
B. Connecting to the host using a null session allows enumeration of share names.
C. Trend Micro has a known exploit that must be resolved or patched.
D. No CVE is present, so it is a false positive caused by Lotus running on a Windows server.

Answer: B

NEW QUESTION 65
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 69
A security analyst is reviewing IDS logs and notices the following entry:

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

Which of the following attacks is occurring?

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

Answer: C

NEW QUESTION 73
During a routine review of firewall logs, an analyst identified that an IP address from the organization's server subnet had been connecting during nighttime hours to a foreign IP address, and had been sending between 150 and 500 megabytes of data each time. This had been going on for approximately one week, and the affected server was taken offline for forensic review. Which of the following is MOST likely to drive up the incident's impact assessment?

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

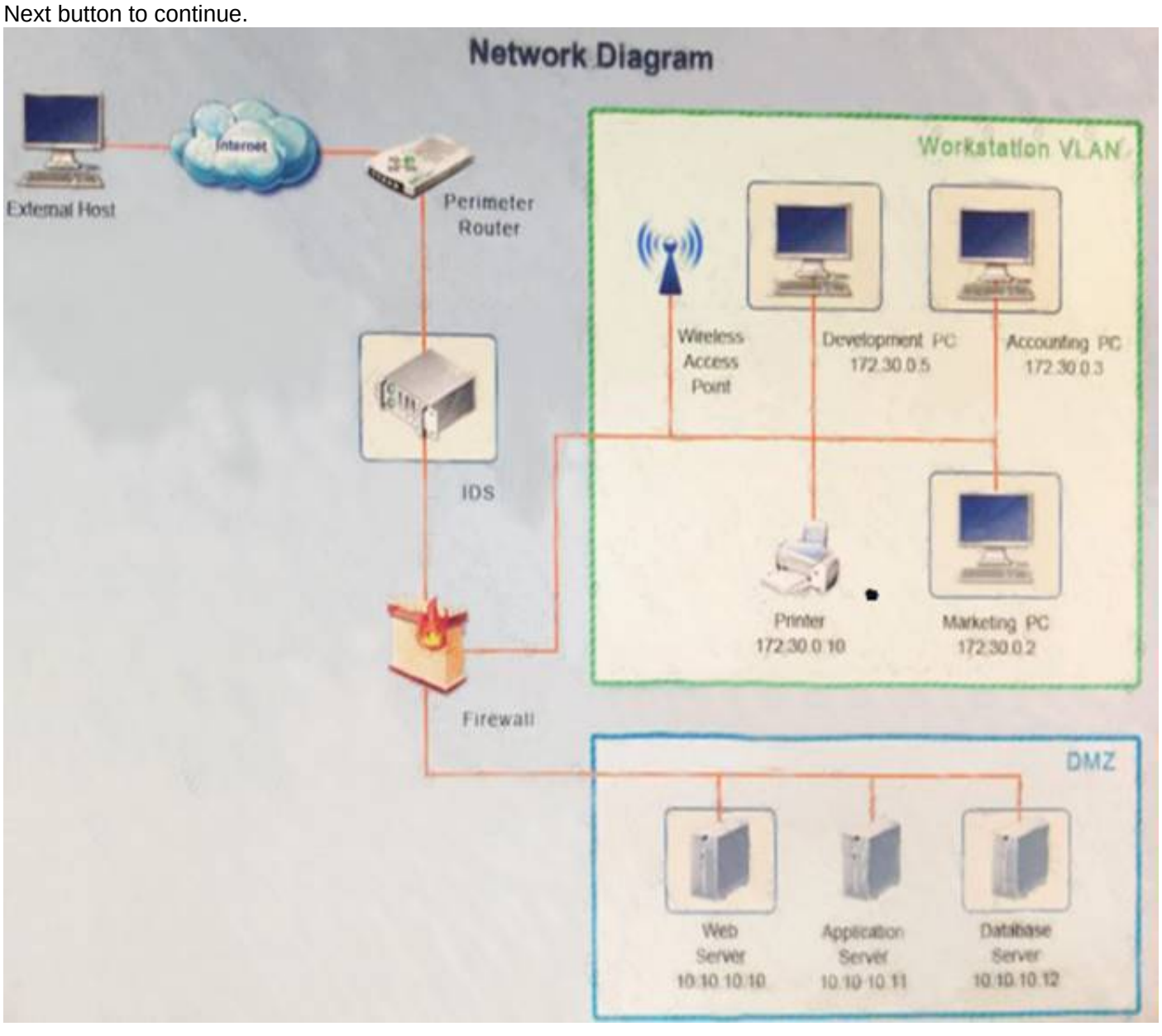
Answer: A

NEW QUESTION 75
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

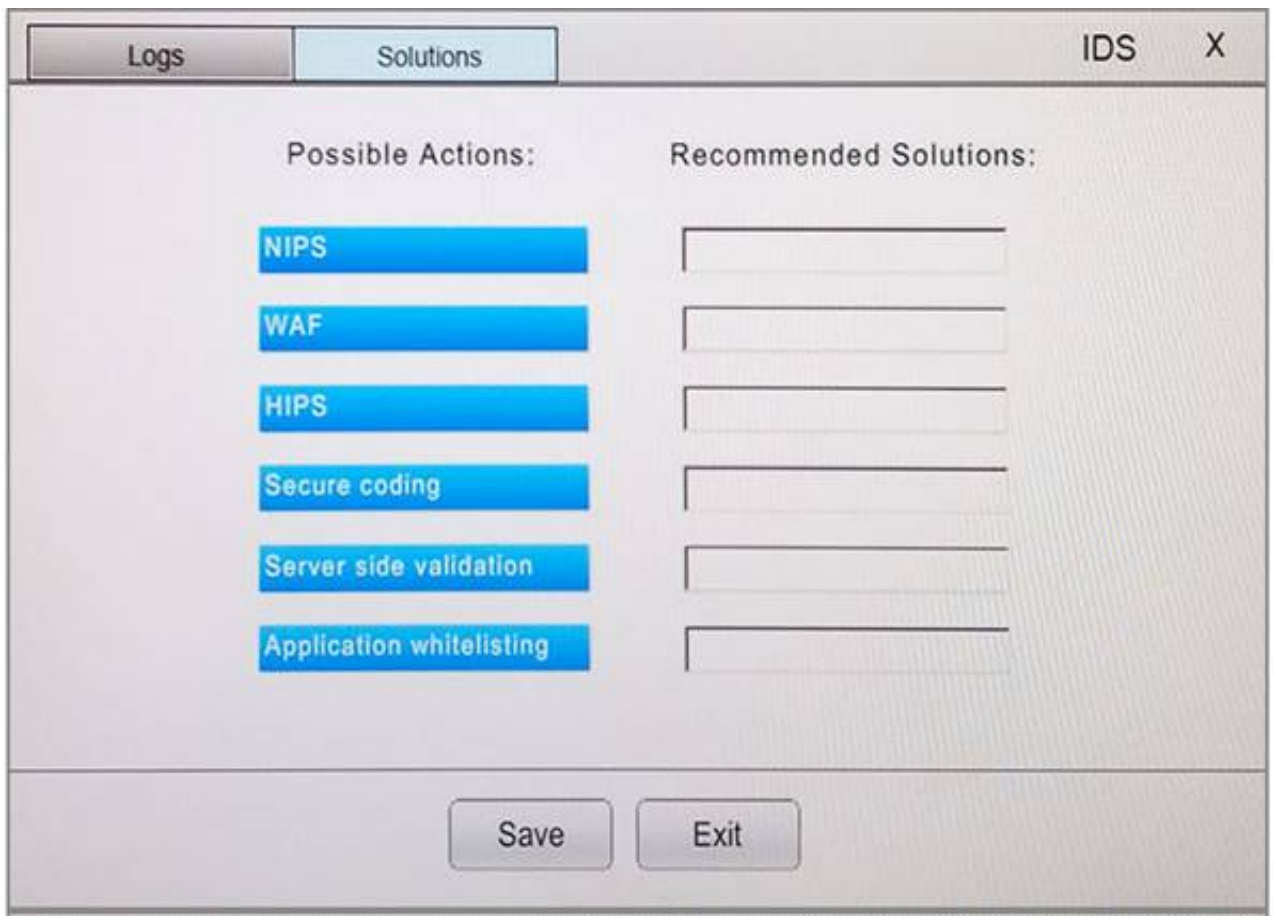
Answer: C

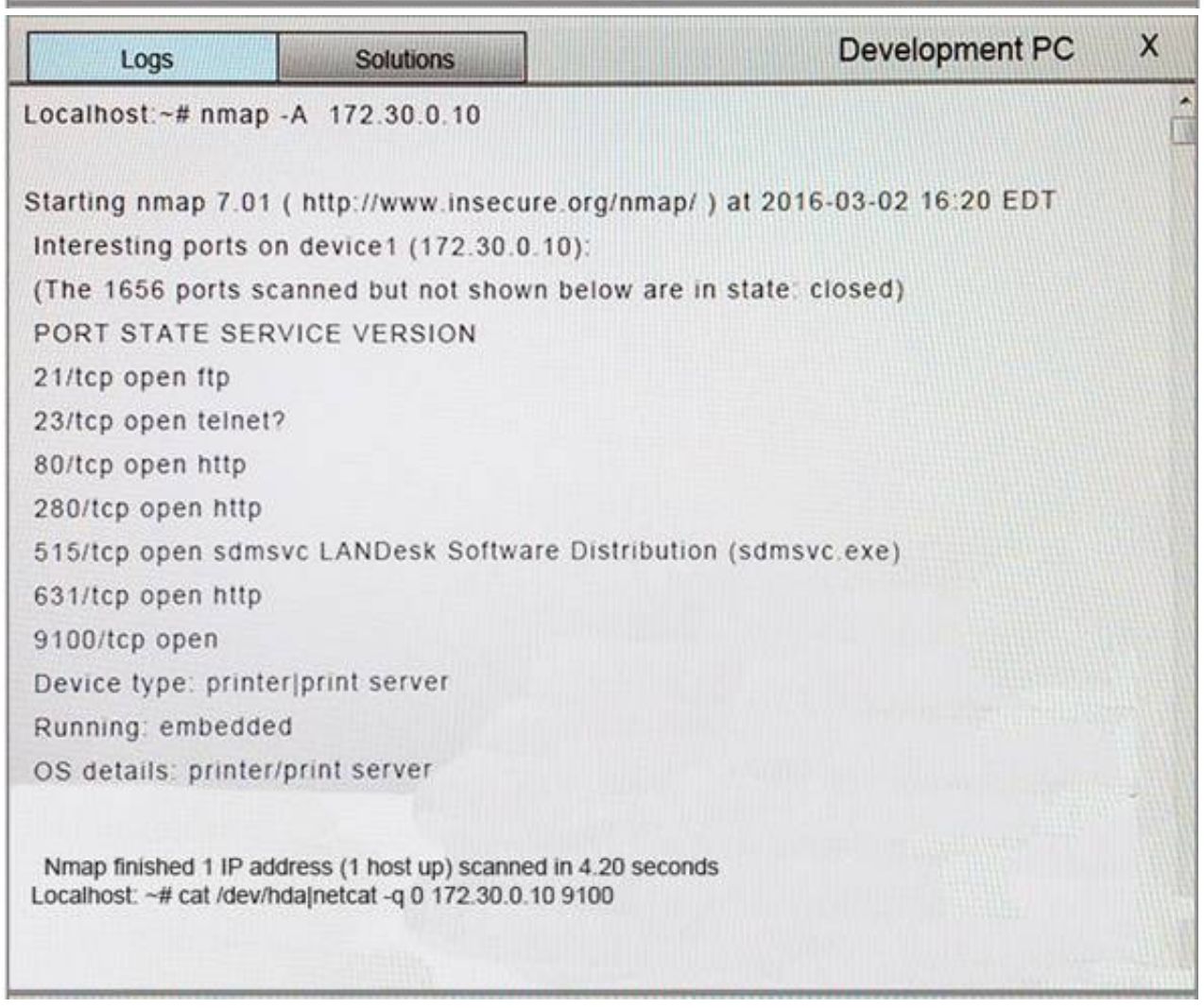
NEW QUESTION 78
You suspect that multiple unrelated security events have occurred on several nodes on a corporate network. You must review all logs and correlate events when necessary to discover each security event by clicking on each node. Only select corrective actions if the logs shown a security event that needs remediation. Drag and drop the appropriate corrective actions to mitigate the specific security event occurring on each affected device.
Instructions:
The Web Server, Database Server, IDS, Development PC, Accounting PC and Marketing PC are clickable. Some actions may not be required and each actions can only be used once per node. The corrective action order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

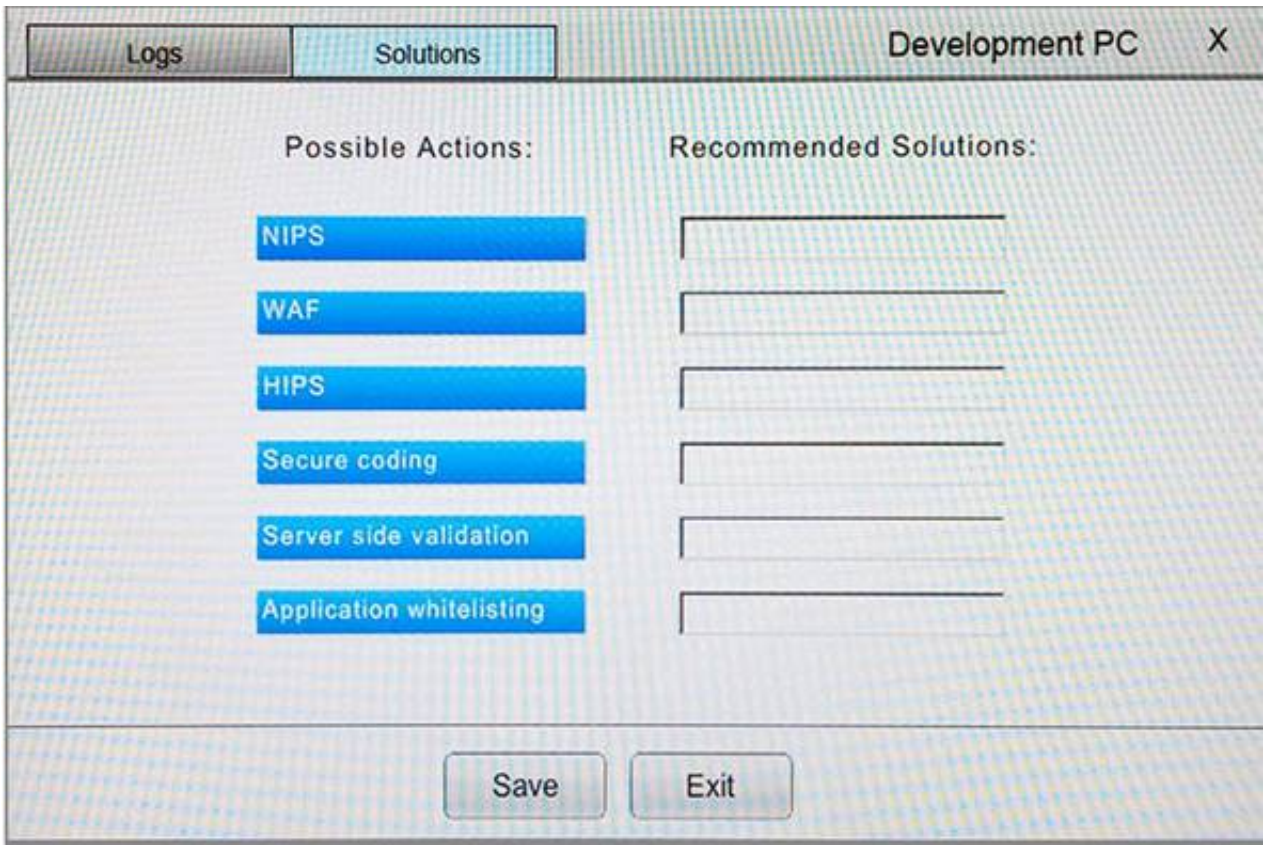


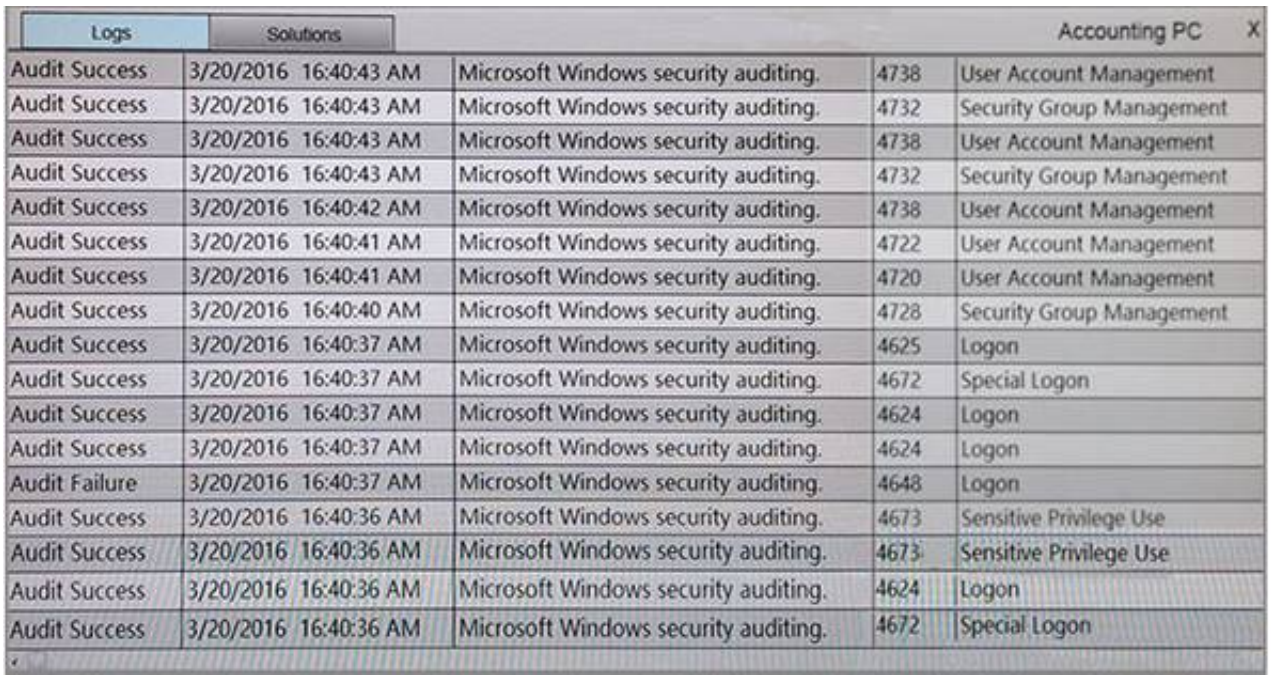
Logs | Solutions — IDS X

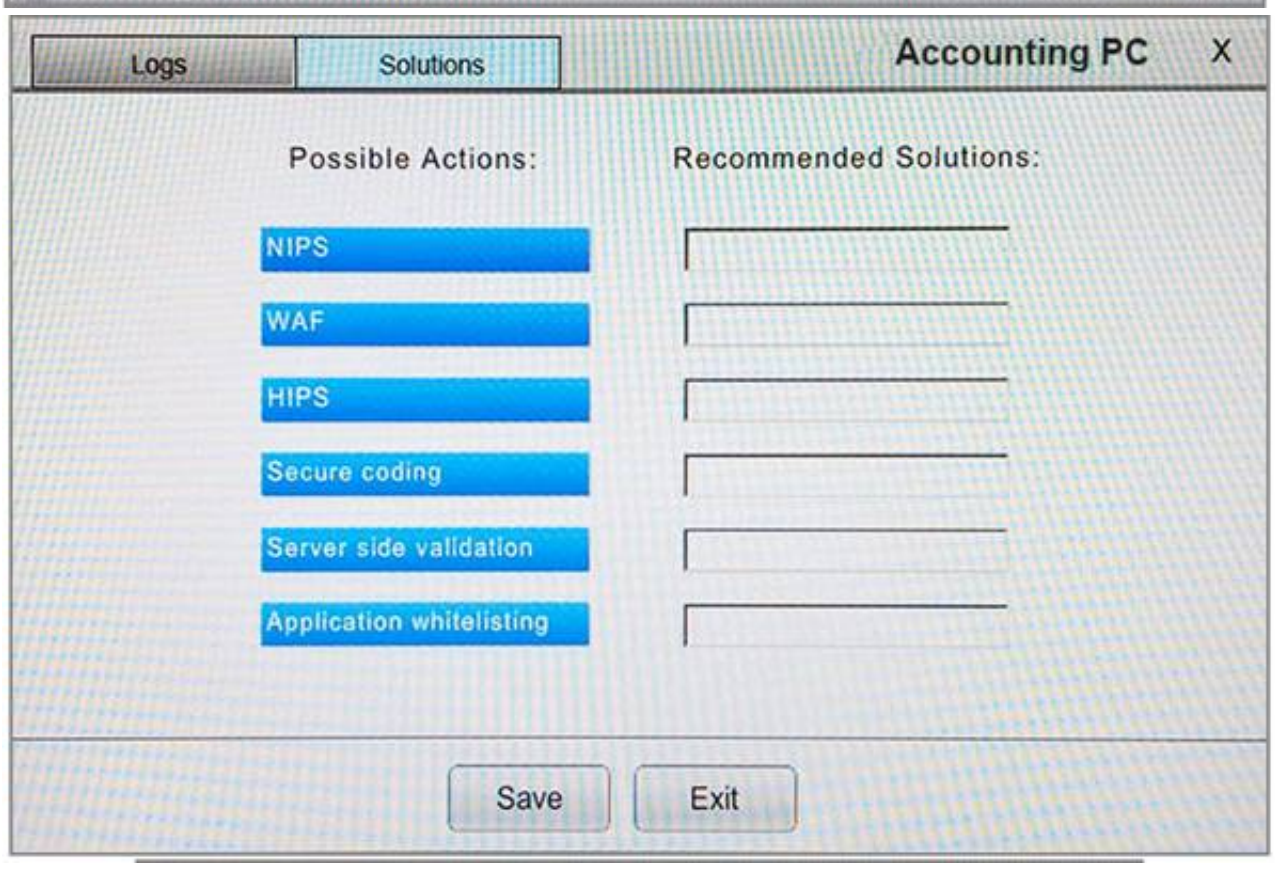
Time	Source	Destination	Protocol	Length	Rule
2016/03/02 16:20.2934	172.30.0.2:6881	73.34.229.20:49876	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:20.8142	123.123.123.123:5922	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GET"; content:"/cgi-bin/newcount"; classtype:policypass;)
2016/03/02 16:20.9013	77.250.9.31:12402	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgdl resource request; flow to server; established; content:"GET"; content:"/download/windows/asctab31.zip"; classtype:policypass;)
2016/03/02 16:21.0032	123.123.123.123:5922	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgsi resource request; flow to server; established; content:"GET"; content:"/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;)

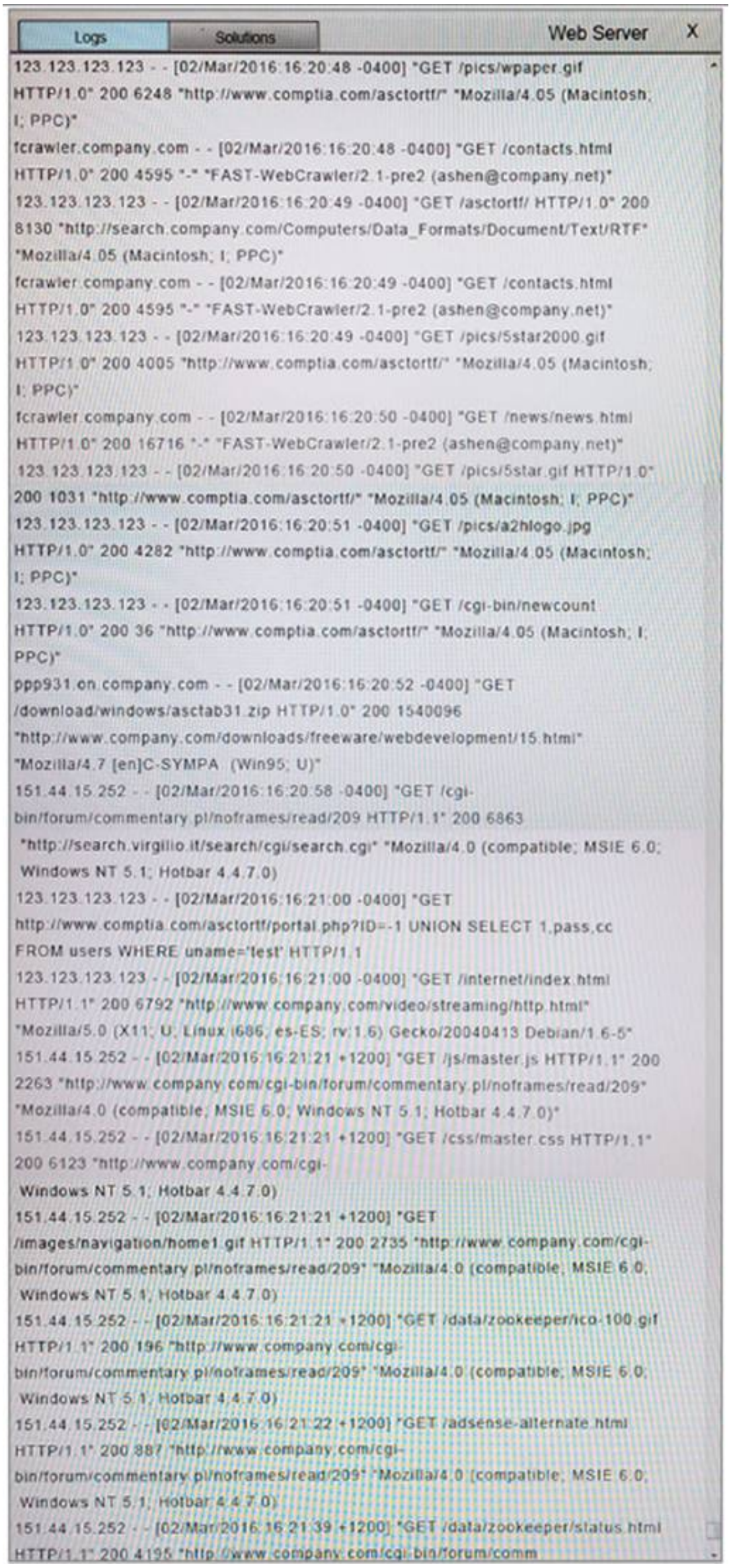


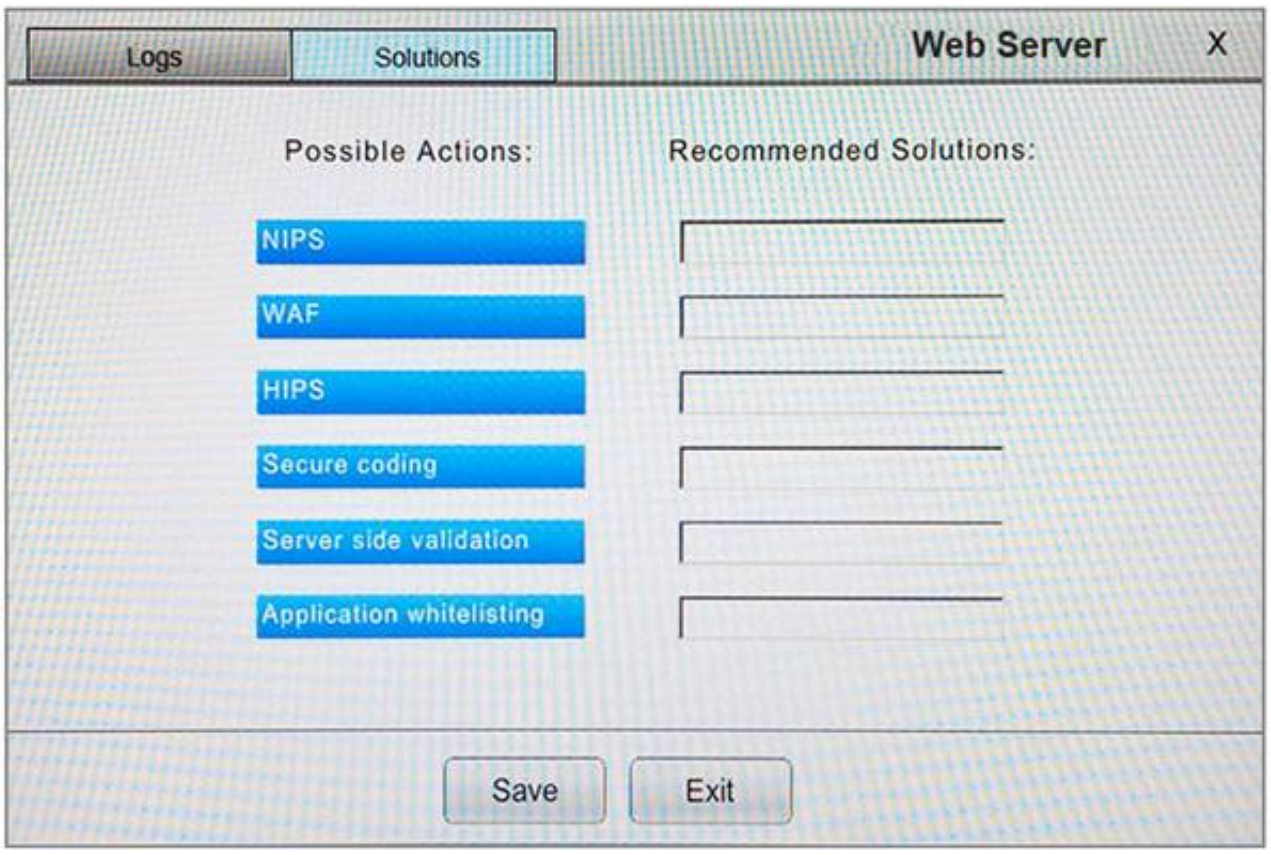


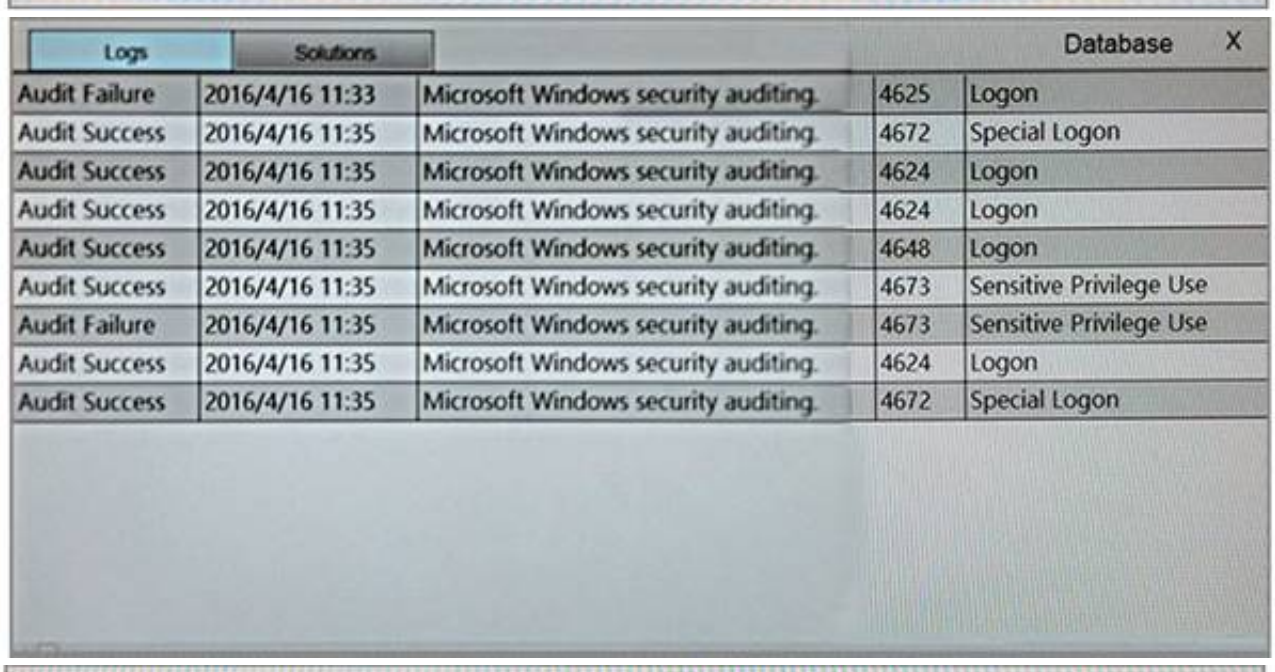

Logs
Solutions
Development PC
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Save
Exit

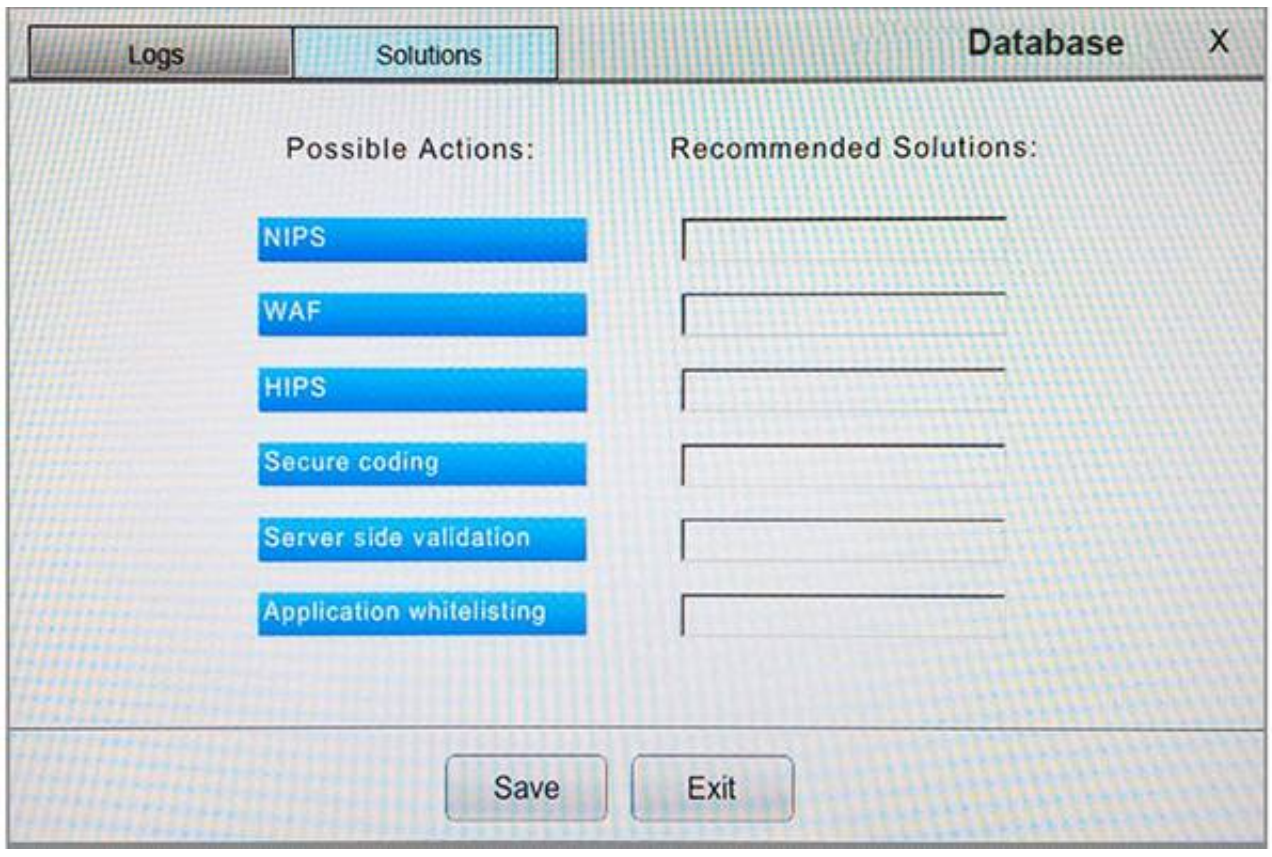

Logs
Solutions
Accounting PC
X
Audit Success 3/20/2016 16:40:43 AM Microsoft Windows security auditing. 4738 User Account Management
Audit Success 3/20/2016 16:40:43 AM Microsoft Windows security auditing. 4732 Security Group Management
Audit Success 3/20/2016 16:40:43 AM Microsoft Windows security auditing.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

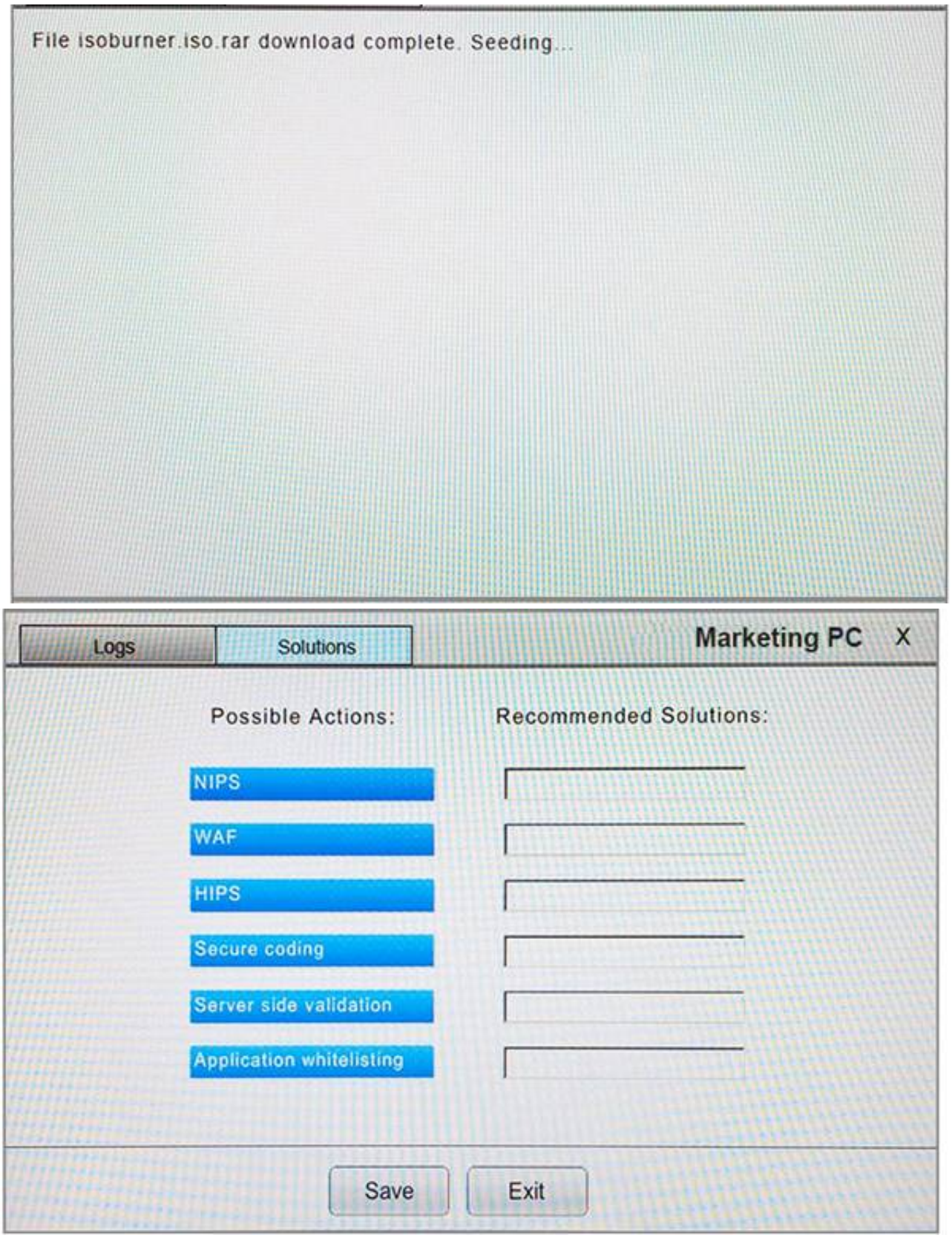

Logs
Solutions
Accounting PC
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Save
Exit


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


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

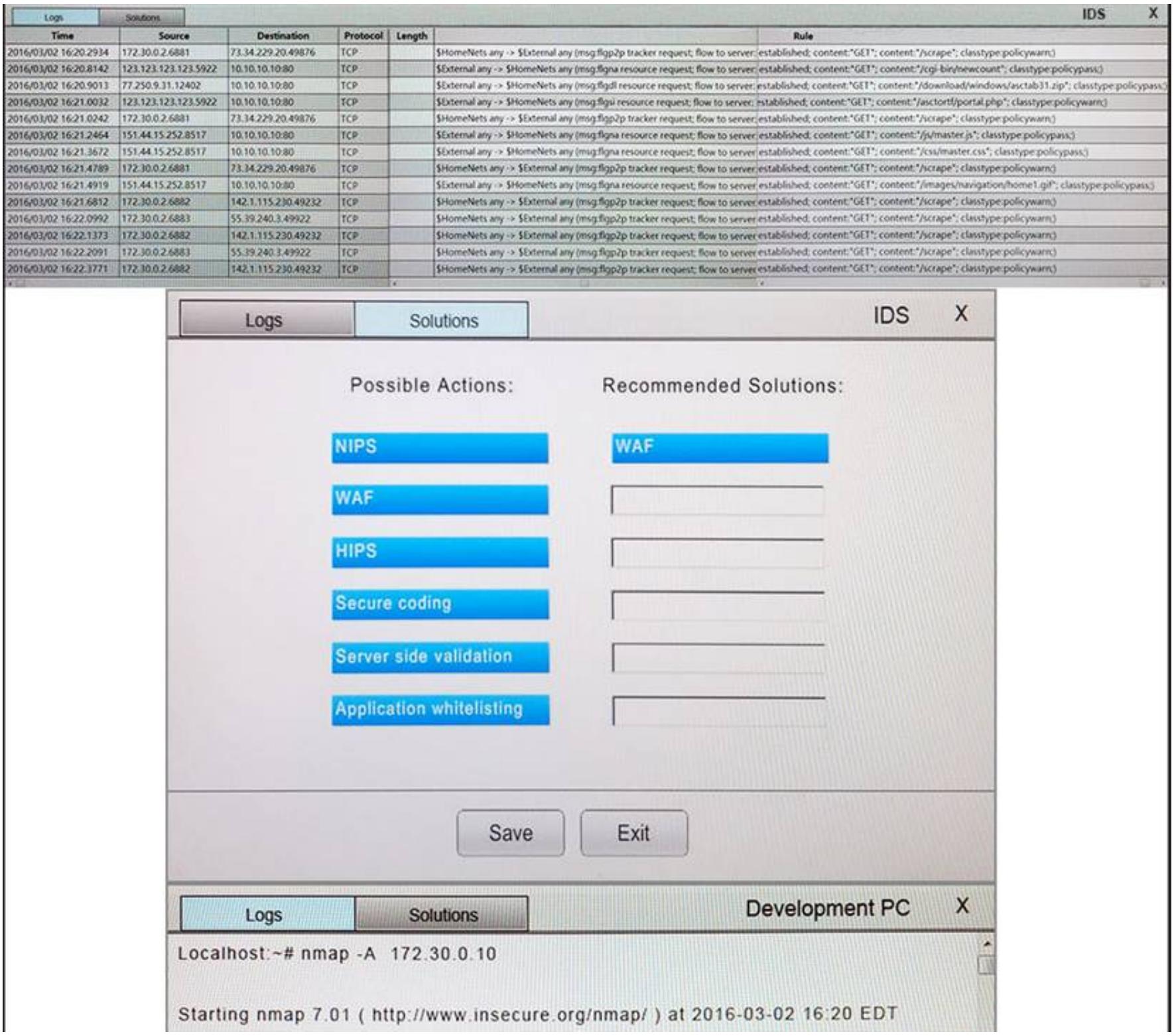

Logs
Solutions
Database
X
Audit Failure 2016/4/16 11:33 Microsoft Windows security auditing. 4625 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4672 Special Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4624 Logon
Audit Success 2016/4/16 11:35 Microsoft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

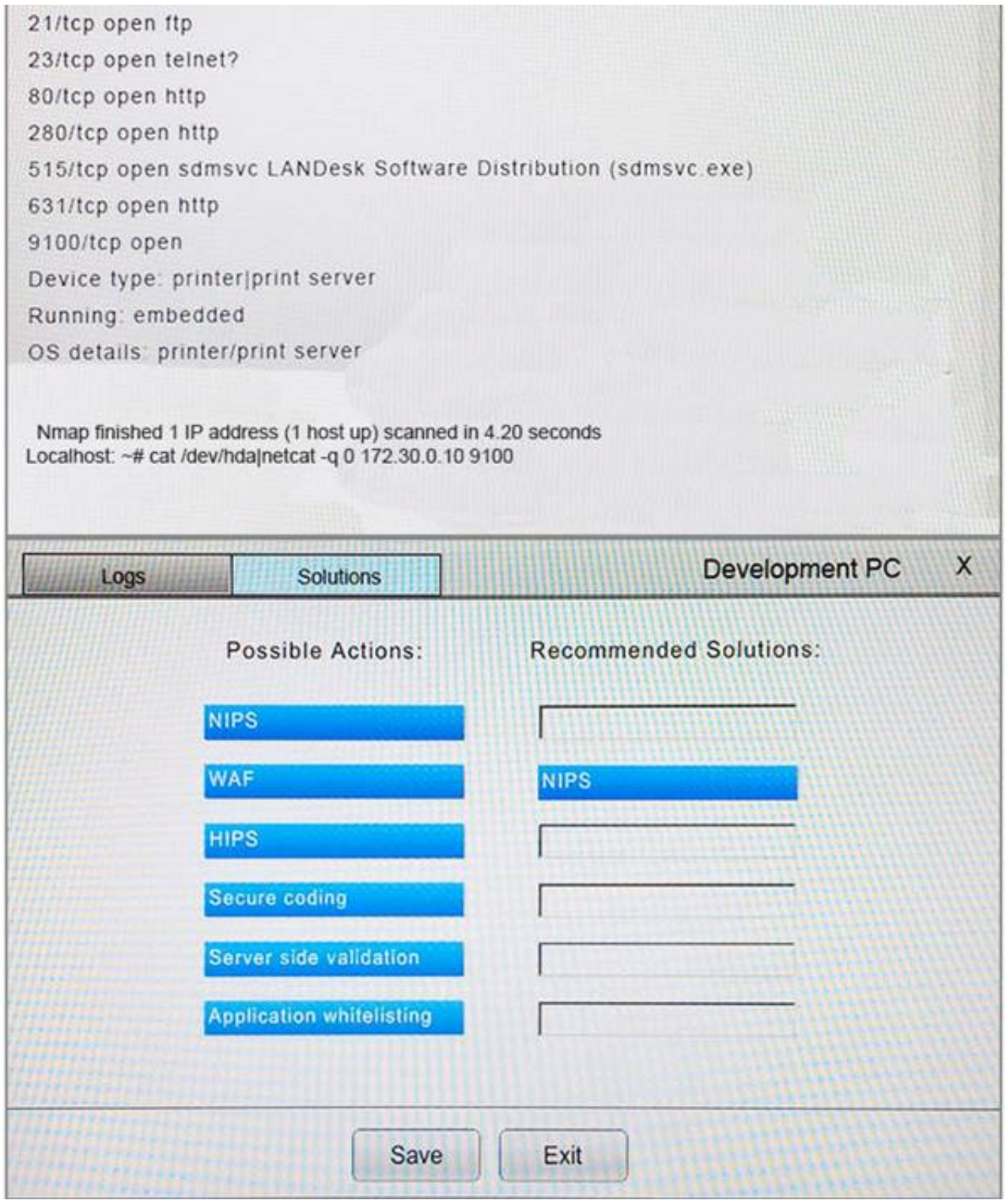

Logs
Solutions
Database
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Save
Exit

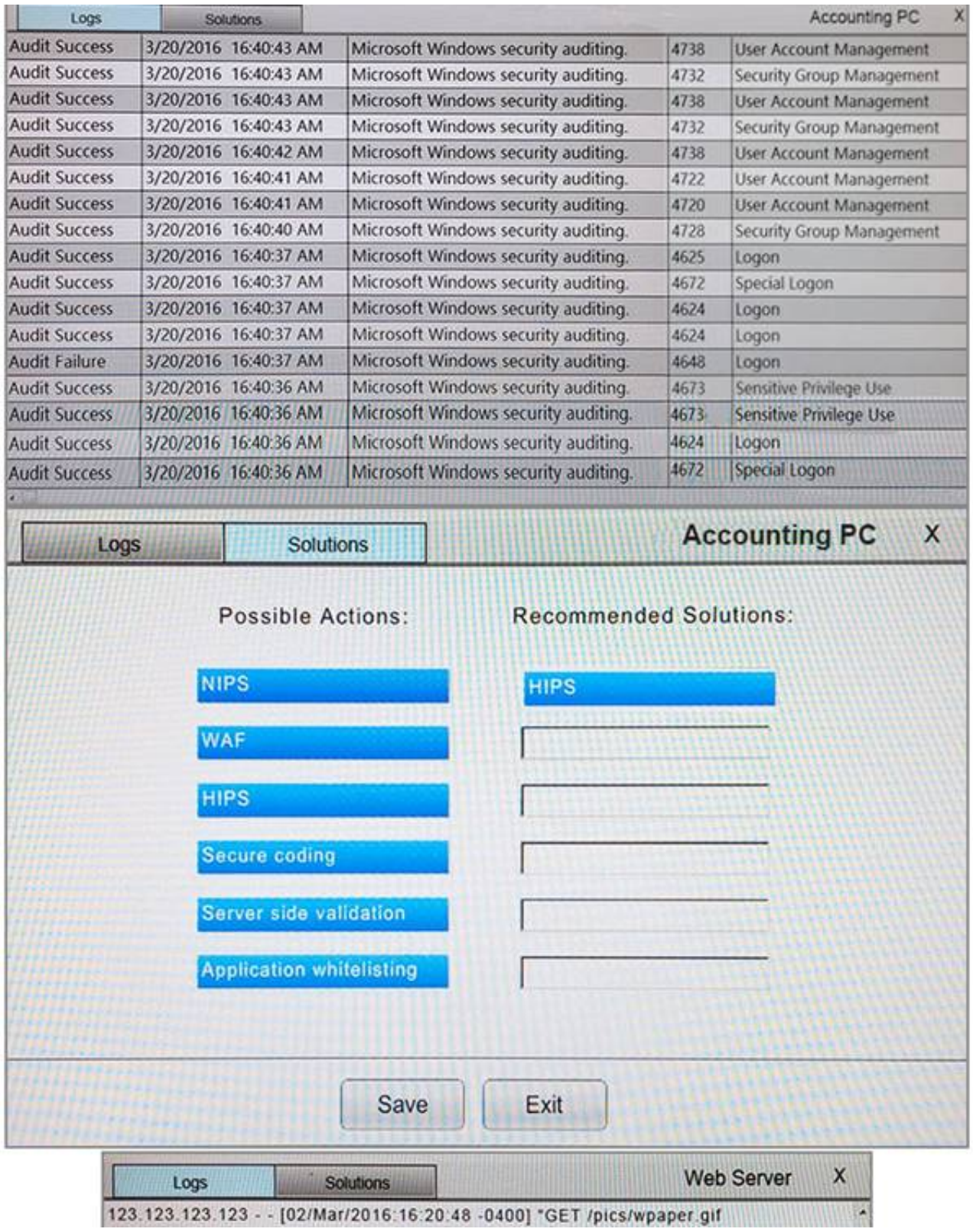


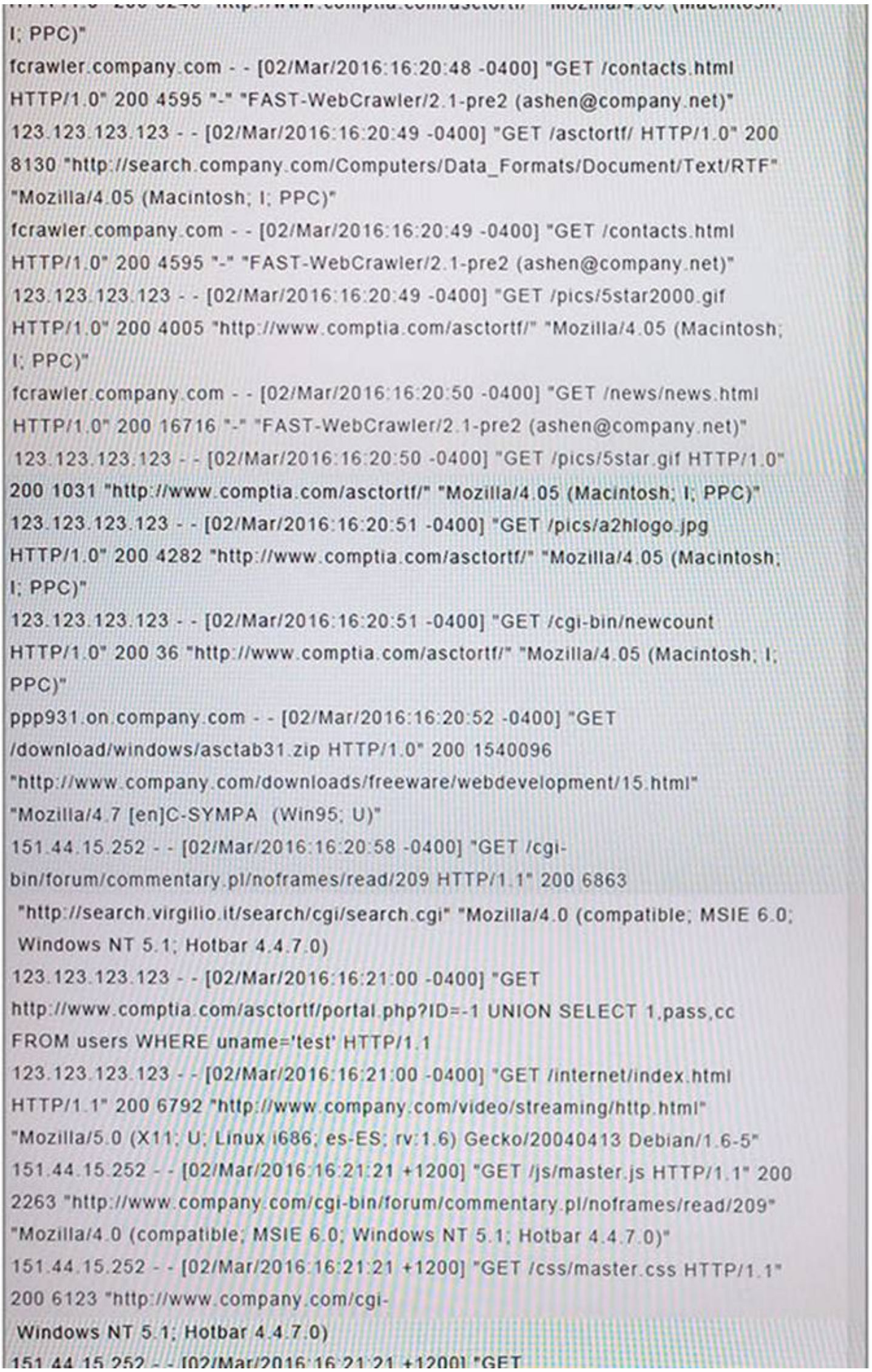
Answer:

Explanation:

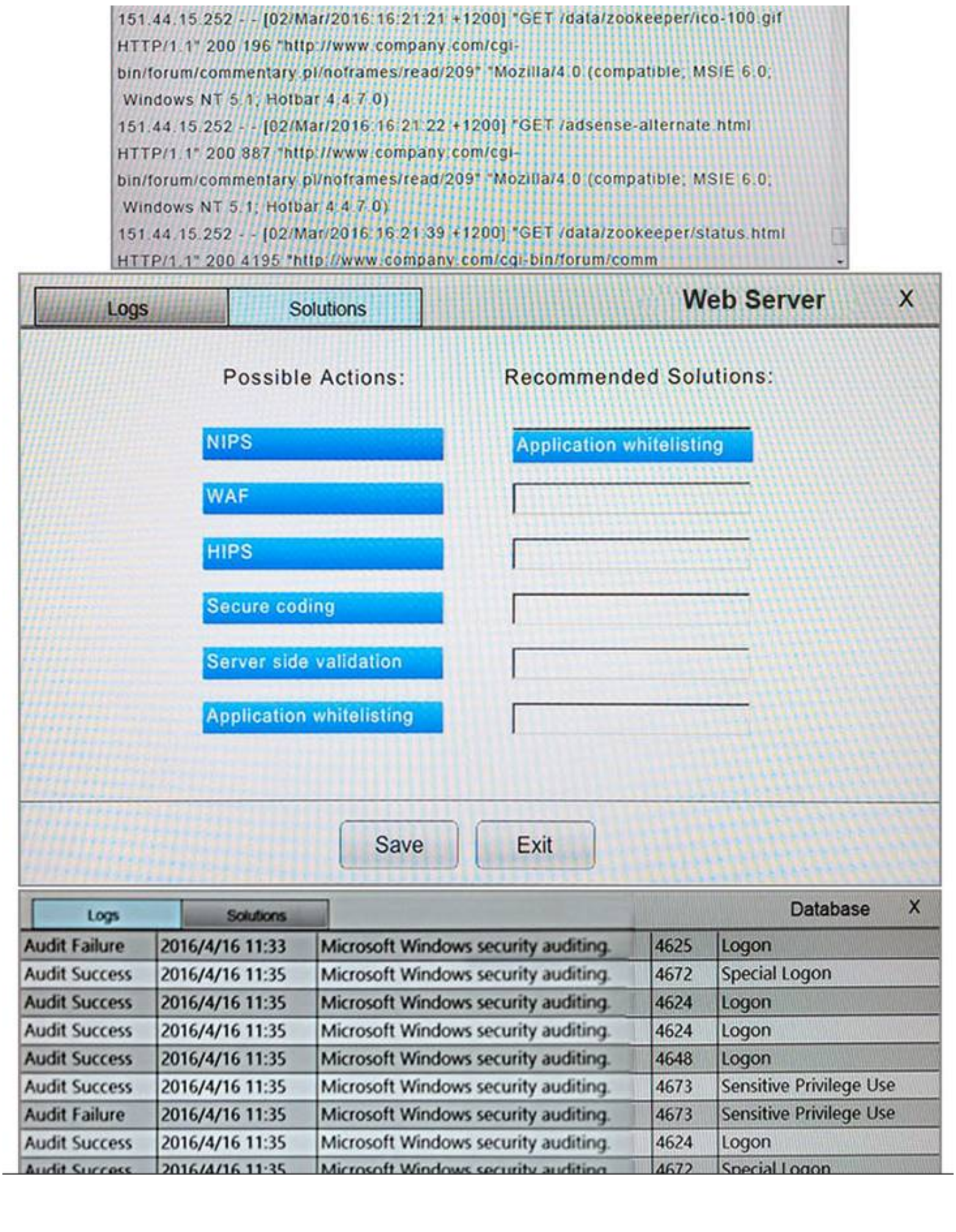

Logs
Solutions
IDS
X
Time
Source
Destination
Protocol
Length
Rule
2016/03/02 16:20.2934 172.30.0.2.6881 73.34.229.20.49876 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:20.8142 123.123.123.123.5922 10.10.10.10:80 TCP $External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GET"; content:"/cgi-bin/newcount"; classtype:policypass;)
2016/03/02 16:20.9013 77.250.9.31.12402 10.10.10.10:80 TCP $External any -> $HomeNets any (msg:flgdl resource request; flow to server; established; content:"GET"; content:"/download/windows/asctab31.zip"; classtype:policypass;)
2016/03/02 16:21.0032 123.123.123.123.5922 10.10.10.10:80 TCP $External any -> $HomeNets any (msg:flgsi resource request; flow to server; established; content:"GET"; content:"/asctortf/portal.php"; classtype:policywarn;)
2016/03/02 16:21.0242 172.30.0.2.6881 73.34.229.20.49876 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:21.2464 151.44.15.252.8517 10.10.10.10:80 TCP $External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GET"; content:"/js/master.js"; classtype:policypass;)
2016/03/02 16:21.3672 151.44.15.252.8517 10.10.10.10:80 TCP $External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GET"; content:"/css/master.css"; classtype:policypass;)
2016/03/02 16:21.4789 172.30.0.2.6881 73.34.229.20.49876 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:21.4919 151.44.15.252.8517 10.10.10.10:80 TCP $External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GET"; content:"/images/navigation/home1.gif"; classtype:policypass;)
2016/03/02 16:21.6812 172.30.0.2.6882 142.1.115.230.49232 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:22.0992 172.30.0.2.6883 55.39.240.3.49922 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:22.1373 172.30.0.2.6882 142.1.115.230.49232 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:22.2091 172.30.0.2.6883 55.39.240.3.49922 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:22.3771 172.30.0.2.6882 142.1.115.230.49232 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
Logs
Solutions
IDS
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Save
Exit
Logs
Solutions
Development PC
X
Localhost:~# nmap -A 172.30.0.10
Starting nmap 7.01 (http://www.insecure.org/nmap/) at 2016-03-02 16:20 EDT

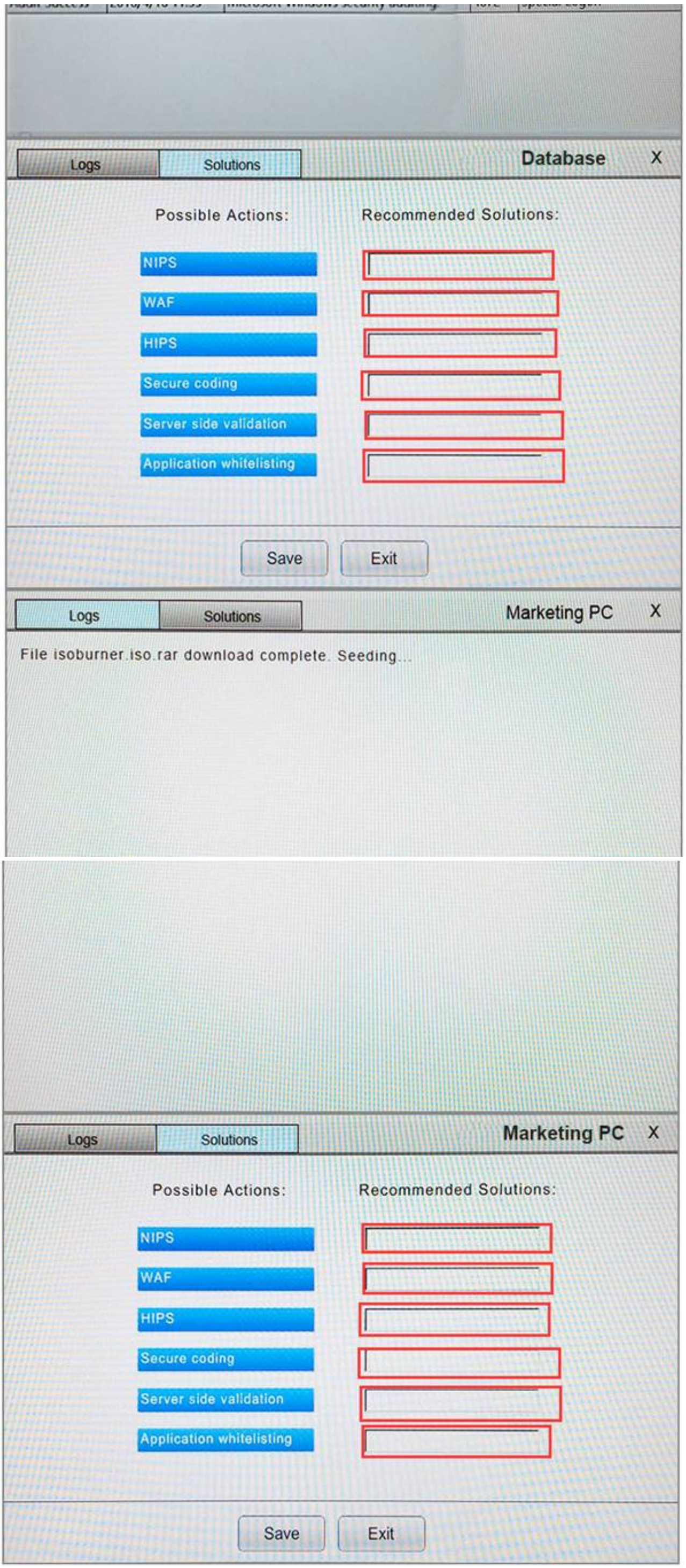

21/tcp open ftp
23/tcp open telnet?
80/tcp open http
280/tcp open http
515/tcp open sdmsvc LANDesk Software Distribution (sdmsvc.exe)
631/tcp open http
9100/tcp open
Device type: printer|print server
Running: embedded
OS details: printer/print server
Nmap finished 1 IP address (1 host up) scanned in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


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



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


151.44.15.252 - - [02/Mar/2016:16:21:21 +1200] "GET /data/zookeeper/ico-100.gif
HTTP/1.1" 200 196 "http://www.company.com/cgi-
bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1; Hotbar 4.4.7.0)
151.44.15.252 - - [02/Mar/2016:16:21:22 +1200] "GET /adsense-alternate.html
HTTP/1.1" 200 887 "http://www.company.com/cgi-
bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1; Hotbar 4.4.7.0)
151.44.15.252 - - [02/Mar/2016:16:21:39 +1200] "GET /data/zookeeper/status.html
HTTP/1.1" 200 4195 "http://www.company.com/cgi-bin/forum/comm
Logs
Solutions
Web Server
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Application whitelisting
Save
Exit
Logs
Solutions
Database
X
Audit Failure 2016/4/16 11:33 Microsoft Windows security auditing. 4625 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4672 Special Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4624 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4624 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4648 Logon
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4673 Sensitive Privilege Use
Audit Failure 2016/4/16 11:35 Microsoft Windows security auditing. 4673 Sensitive Privilege Use
Audit Success 2016/4/16 11:35 Microsoft Windows security auditing. 4624 Logon


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

NEW QUESTION 79
Which of the following items represents a document that includes detailed information on when an incident was detected, how impactful the incident was, and how it was remediated, in addition to incident response effectiveness and any identified gaps needing improvement?

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

Answer: D

NEW QUESTION 83
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 88
Datacenter access is controlled with proximity badges that record all entries and exits from the datacenter.
The access records are used to identify which staff members accessed the data center in the event of equipment theft.
Which of the following MUST be prevented in order for this policy to be effective?

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

Answer: D

NEW QUESTION 92
The help desk informed a security analyst of a trend that is beginning to develop regarding a suspicious email that has been reported by multiple users. The analyst has determined the email includes an attachment named invoice.zip that contains the following files:
Locky.js xerty.ini xerty.lib
Further analysis indicates that when the .zip file is opened, it is installing a new version of ransomware on the devices. Which of the following should be done FIRST to prevent data on the company NAS from being encrypted by infected devices?

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

Answer: B

NEW QUESTION 95
A technician is running an intensive vulnerability scan to detect which ports are open to exploit. During the scan, several network services are disabled and production is affected. Which of the following sources would be used to evaluate which network service was interrupted?

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

Answer: A

NEW QUESTION 100
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 105
Law enforcement has contacted a corporation's legal counsel because correlated data from a breach shows the organization as the common denominator from all

indicators of compromise. An employee overhears the conversation between legal counsel and law enforcement, and then posts a comment about it on social media. The media then starts contacting other employees about the breach. Which of the following steps should be taken to prevent further disclosure of information about the breach?

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

Answer: A

NEW QUESTION 107
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 109
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 111
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 115
Which of the following represent the reasoning behind careful selection of the timelines and time-of-day boundaries for an authorized penetration test? (Select TWO).

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

Answer: AC

NEW QUESTION 120
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 125
A web application has a newly discovered vulnerability in the authentication method used to validate known company users. The user ID of Admin with a password of "password" grants elevated access to the application over the Internet. Which of the following is the BEST method to discover the vulnerability before a production deployment?

A. Manual peer review

B. User acceptance testing
C. Input validation
D. Stress test the application

Answer: C

NEW QUESTION 128
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 133
An alert has been distributed throughout the information security community regarding a critical Apache vulnerability. Which of the following courses of action would ONLY identify the known vulnerability?

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

Answer: B

NEW QUESTION 134
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 135
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 137
The security operations team is conducting a mock forensics investigation. Which of the following should be the FIRST action taken after seizing a compromised workstation?

A. Activate the escalation checklist
B. Implement the incident response plan
C. Analyze the forensic image
D. Perform evidence acquisition

Answer: D

Explanation: Reference https://staff.washington.edu/dittrich/misc/forensics/

NEW QUESTION 138
An analyst was testing the latest version of an internally developed CRM system. The analyst created a basic user account. Using a few tools in Kali's latest distribution, the analyst was able to access configuration files, change permissions on folders and groups, and delete and create new system objects. Which of the following techniques did the analyst use to perform these unauthorized activities?

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

Answer: C

NEW QUESTION 142
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 146
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 150
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 154
An organization uses Common Vulnerability Scoring System (CVSS) scores to prioritize remediation of vulnerabilities.
Management wants to modify the priorities based on a difficulty factor so that vulnerabilities with lower CVSS scores may get a higher priority if they are easier to implement with less risk to system functionality. Management also wants to quantify the priority. Which of the following would achieve management's objective?

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

Answer: C

NEW QUESTION 156
There have been several exploits to critical devices within the network. However, there is currently no process to perform vulnerability analysis.
Which of the following should the security analyst implement during production hours to identify critical threats and vulnerabilities?

A. Asset inventory of all critical devices
B. Vulnerability scanning frequency that does not interrupt workflow
C. Daily automated reports of exploited devices
D. Scanning of all types of data regardless of sensitivity levels

Answer: B

NEW QUESTION 158
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 160
After a recent security breach, it was discovered that a developer had promoted code that had been written to the production environment as a hotfix to reserve a user navigation issue that was causing issues for several customers. The code had inadvertently granted administrative privileges to all users, allowing inappropriate access to sensitive data and reports. Which of the following could have prevented the code from being released into the production environment?

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

Answer: D

NEW QUESTION 163
A security analyst at a small regional bank has received an alert that nation states are attempting to infiltrate financial institutions via phishing campaigns. Which of the following techniques should the analyst recommend as a proactive measure to defend against this type of threat?

A. Honeypot
B. Location-based NAC
C. System isolation
D. Mandatory access control
E. Bastion host

Answer: B

NEW QUESTION 165
A business-critical application is unable to support the requirements in the current password policy because it does not allow the use of special characters. Management does not want to accept the risk of a possible security incident due to weak password standards. Which of the following is an appropriate means to limit the risks related to the application?

A. A compensating control
B. Altering the password policy
C. Creating new account management procedures
D. Encrypting authentication traffic

Answer: D

NEW QUESTION 170
The security configuration management policy states that all patches must undergo testing procedures before being moved into production. The security analyst notices a single web application server has been downloading and applying patches during non-business hours without testing. There are no apparent adverse reactions, server functionality does not seem to be affected, and no malware was found after a scan.
Which of the following actions should the analyst take?

A. Reschedule the automated patching to occur during business hours.
B. Monitor the web application service for abnormal bandwidth consumption.
C. Create an incident ticket for anomalous activity.
D. Monitor the web application for service interruptions caused from the patching.

Answer: C

NEW QUESTION 175
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 180
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 184
During a web application vulnerability scan, it was discovered that the application would display inappropriate data after certain key phrases were entered into a webform connected to a SQL database server. Which of the following should be used to reduce the likelihood of this type of attack returning sensitive data?

A. Static code analysis
B. Peer review code
C. Input validation
D. Application fuzzing

Answer: C

NEW QUESTION 189
A SIEM analyst noticed a spike in activities from the guest wireless network to several electronic health record (EHR) systems. After further analysis, the analyst discovered that a large volume of data has been uploaded to a cloud provider in the last six months. Which of the following actions should the analyst do FIRST?

A. Contact the Office of Civil Rights (OCR) to report the breach
B. Notify the Chief Privacy Officer (CPO)
C. Activate the incident response plan
D. Put an ACL on the gateway router

Answer: D

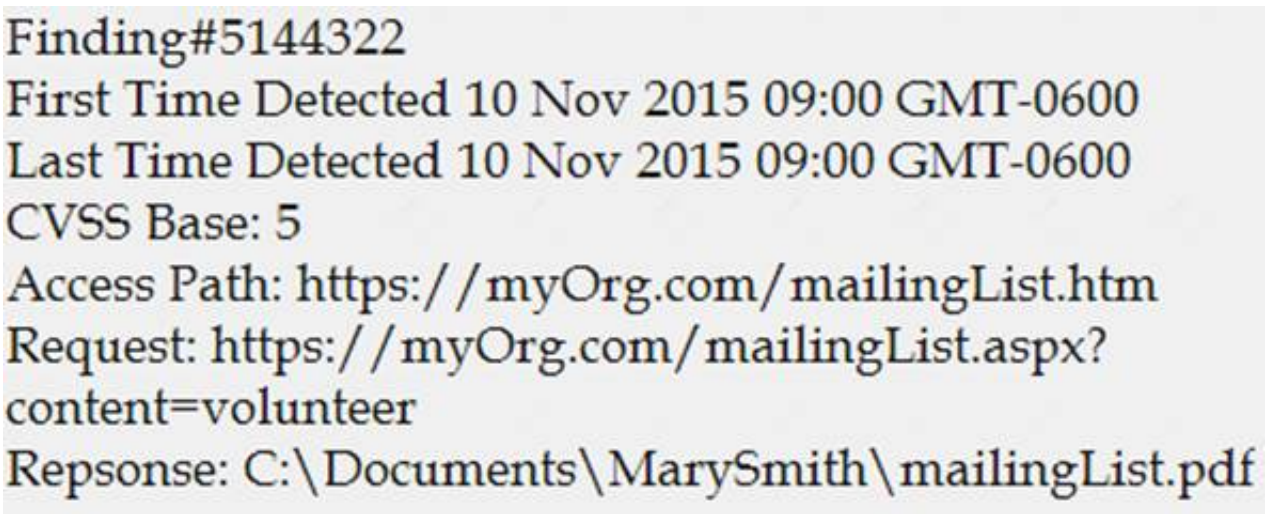
NEW QUESTION 192
The director of software development is concerned with recent web application security incidents, including the successful breach of a back-end database server. The director would like to work with the security team to implement a standardized way to design, build, and test web applications and the services that support them. Which of the following meets the criteria?

A. OWASP
B. SANS
C. PHP
D. Ajax

Answer: A

Explanation: Reference https://www.synopsys.com/software-integrity/resources/knowledge-database/owasp-top-10.html

NEW QUESTION 197
An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security analyst is reviewing vulnerability scan results from a recent web server scan.
Portions of the scan results are shown below:



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

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

Answer: A

NEW QUESTION 202
A threat intelligence analyst who works for a financial services firm received this report:
“There has been an effective waterhole campaign residing at www.bankfinancecompsoftware.com. This domain is delivering ransomware. This ransomware variant has been called “LockMaster” by researchers due to its ability to overwrite the MBR, but this term is not a malware signature. Please execute a defensive operation regarding this attack vector.”
The analyst ran a query and has assessed that this traffic has been seen on the network. Which of the following actions should the analyst do NEXT? (Select TWO).

A. Advise the firewall engineer to implement a block on the domain
B. Visit the domain and begin a threat assessment
C. Produce a threat intelligence message to be disseminated to the company
D. Advise the security architects to enable full-disk encryption to protect the MBR
E. Advise the security analysts to add an alert in the SIEM on the string “LockMaster”
F. Format the MBR as a precaution

Answer: BD

NEW QUESTION 204
The primary difference in concern between remediating identified vulnerabilities found in general-purpose IT network servers and that of SCADA systems is that:

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

D. patch installation on SCADA systems cannot be verified.

Answer: B

NEW QUESTION 207
A cybersecurity consultant is reviewing the following output from a vulnerability scan against a newly installed MS SQL Server 2012 that is slated to go into production in one week:

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

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

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

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

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

Answer: DE

NEW QUESTION 212
A cybersecurity analyst is reviewing log data and sees the output below:

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

Which of the following technologies MOST likely generated this log?

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

Answer: C

NEW QUESTION 217
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 221
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 225
Which of the following stakeholders would need to be aware of an e-discovery notice received by the security office about an ongoing case within the manufacturing department?

A. Board of trustees
B. Human resources
C. Legal
D. Marketing

Answer: C

NEW QUESTION 228
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 232
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 234
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 236
Given the following access log:

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

access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /js/query-ui/js/?a.aspectRatio:this.originalSize.height | |
1;a=e( HTTP/1.1" 303 333

access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /scripts/query-ui/js/J);F.optgroup=F .option;F .tbody=F
.tfoot=F .colorgroup=F .caption=F .thread;F .th=F .td;if (!c.support.htmlSerialize)F._default=(1, HTTP/1.1"
403 338
```

Which of the following accurately describes what this log displays?

A. A vulnerability in jQuery
B. Application integration with an externally hosted database
C. A vulnerability scan performed from the Internet
D. A vulnerability in Javascript

Answer: C

NEW QUESTION 239
A recently issued audit report highlight exception related to end-user handling of sensitive data access and credentials. A security manager is addressing the findings. Which of the following activities should be implemented?

A. Update the password policy
B. Increase training requirements
C. Deploy a single sign-on platform
D. Deploy Group Policy Objects

Answer: B

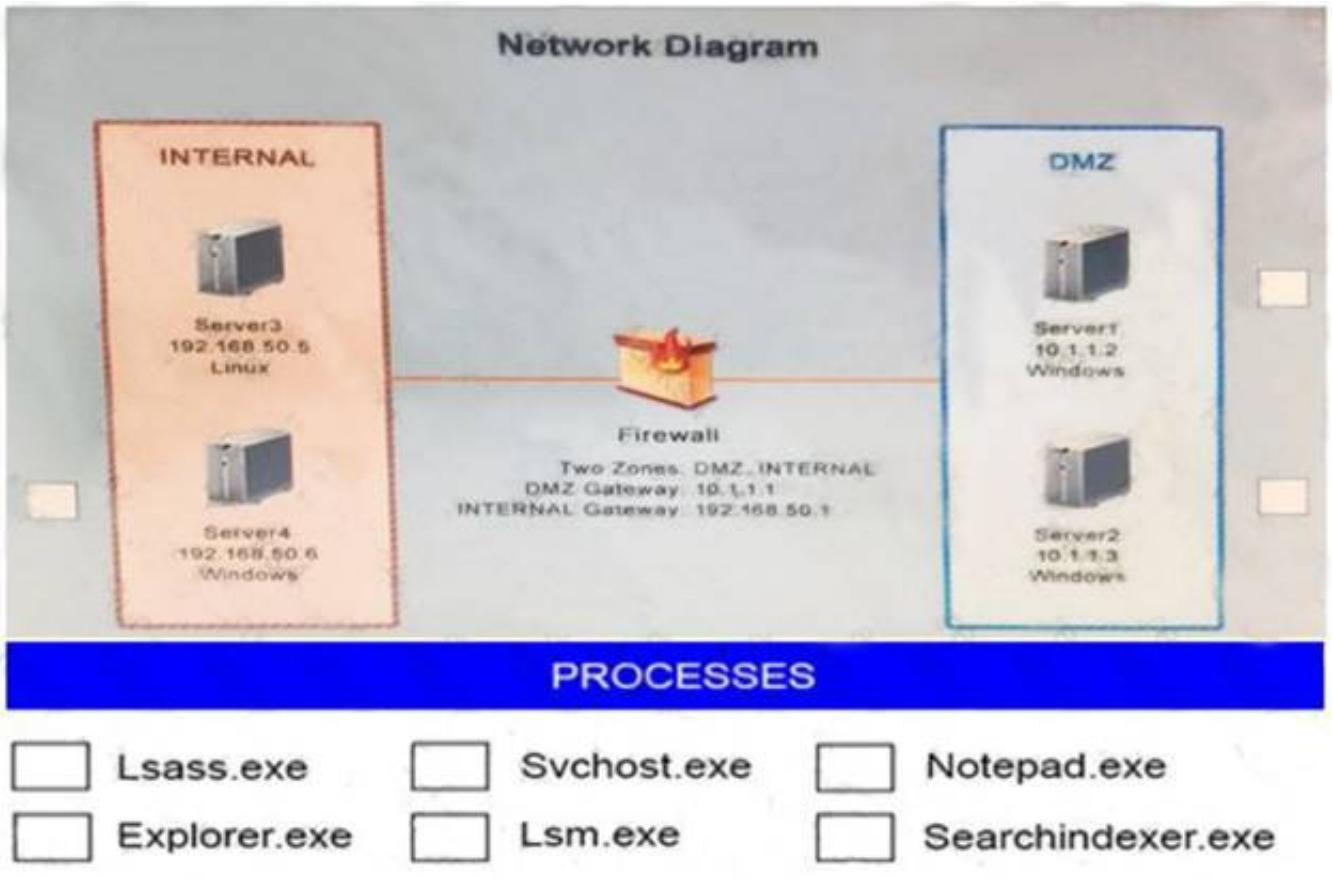
NEW QUESTION 241
A cybersecurity analyst was asked to discover the hardware address of 30 networked assets. From a command line, which of the following tools would be used to provide ARP scanning and reflects the MOST efficient method for accomplishing the task?

A. nmap
B. tracert
C. ping –a
D. nslookup

Answer: A

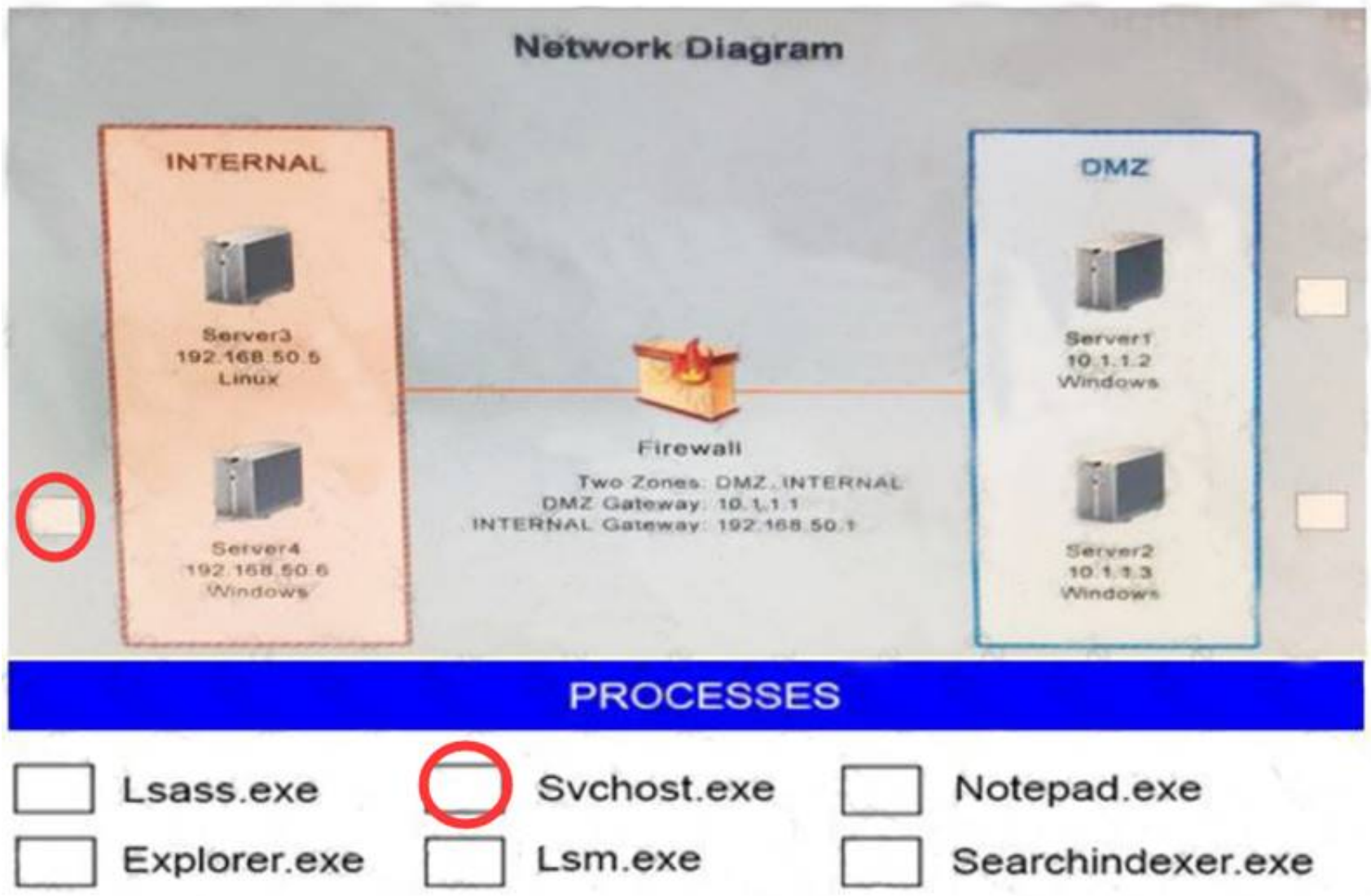
Explanation: Reference
https://serverfault.com/questions/10590/how-to-get-a-list-of-all-ip-addresses-and-ideally-device-names-on-a-lan

NEW QUESTION 245
Malware is suspected on a server in the environment. The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware. Servers 1, 2 and 4 are clickable. Select the Server which hosts the malware, and select the process which hosts this malware.
Instructions:
If any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Answer:

Explanation:



NEW QUESTION 250
The business has been informed of a suspected breach of customer data. The internal audit team, in conjunction with the legal department, has begun working with the cybersecurity team to validate the report. To which of the following response processes should the business adhere during the investigation?

A. The security analysts should not respond to internal audit requests during an active investigation
B. The security analysts should report the suspected breach to regulators when an incident occurs
C. The security analysts should interview system operators and report their findings to the internal auditors
D. The security analysts should limit communication to trusted parties conducting the investigation

Answer: D

NEW QUESTION 255
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 259
A start member reported that a laptop has (traded performance. The security analyst has investigated the issue and discovered that CPU utilization, memory utilization. and outbound network traffic are consuming the laptop resources. Which of the following is the BEST course of action to resolve the problem?

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

Answer: A

NEW QUESTION 260
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 263
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 265
A cybersecurity analyst is conducting packet analysis on the following:

Time	Source	Destination	Info
0.000673	00:48:c2:5f:39:57	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:57
0.001173	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.6 is at 00:48:c2:5f:39:9a
0.002346	00:48:c2:5f:39:2b	00:43:b3:3f:23:e3	172.16.1.12 is at 00:48:c2:5f:39:2b
0.005123	00:48:c2:5f:39:42	00:43:b3:3f:23:e3	172.16.1.13 is at 00:48:c2:5f:39:42
0.010281	00:48:c2:5f:39:6b	00:43:b3:3f:23:e3	172.16.1.2 is at 00:48:c2:5f:39:6b
0.021597	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:9a
0.044812	00:48:c2:5f:39:3c	00:43:b3:3f:23:e3	172.16.1.21 is at 00:43:b3:3f:23:e3
0.06512	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:43:b3:3f:23:e3

Which of the following is occurring in the given packet capture?

A. ARP spoofing
B. Broadcast storm
C. Smurf attack
D. Network enumeration
E. Zero-day exploit

Answer: D

NEW QUESTION 266
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 270
A security analyst is concerned that employees may attempt to exfiltrate data prior to tendering their resignations. Unfortunately, the company cannot afford to purchase a data loss prevention (DLP) system. Which of the following recommendations should the security analyst make to provide defense-in-depth against data loss? (Select THREE).

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

Answer: ABE

NEW QUESTION 272
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 277
During a routine network scan, a security administrator discovered an unidentified service running on a new embedded and unmanaged HVAC controller, which is used to monitor the company's datacenter:

Port	State
161/UDP	open
162/UDP	open
163/UDP	open

The enterprise monitoring service requires SNMP and SNMPTRAP connectivity to operate. Which of the following should the security administrator implement to harden the system?

A. Patch and restart the unknown service.
B. Segment and firewall the controller's network.
C. Disable the unidentified service on the controller.
D. Implement SNMPv3 to secure communication.
E. Disable TCP/UDP ports 161 through 163.

Answer: A

NEW QUESTION 280
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 285
Scan results identify critical Apache vulnerabilities on a company's web servers. A security analyst believes many of these results are false positives because the web environment mostly consists of Windows servers.
Which of the following is the BEST method of verifying the scan results?

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

Answer: A

NEW QUESTION 286
Given the following output from a Linux machine: file2cable –i eth0 -f file.pcap
Which of the following BEST describes what a security analyst is trying to accomplish?

A. The analyst is attempting to measure bandwidth utilization on interface eth0.
B. The analyst is attempting to capture traffic on interface eth0.

C. The analyst is attempting to replay captured data from a PCAP file.
D. The analyst is attempting to capture traffic for a PCAP file.
E. The analyst is attempting to use a protocol analyzer to monitor network traffic.

Answer: E

NEW QUESTION 290
A cybersecurity analyst was hired to resolve a security issue within a company after it was reported that many employee account passwords had been compromised. Upon investigating the incident, the cybersecurity
analyst found that a brute force attack was launched against the company.
Which of the following remediation actions should the cybersecurity analyst recommend to senior management to address these security issues?

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

Answer: B

NEW QUESTION 292
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 293
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 296
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 300
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 301
An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starling any remediation the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive?

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

Answer: A

NEW QUESTION 306
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 310
A company has decided to process credit card transactions directly. Which of the following would meet the requirements for scanning this type of data?

A. Quarterly
B. Yearly
C. Bi-annually
D. Monthly

Answer: A

NEW QUESTION 312
A company has been a victim of multiple volumetric DoS attacks. Packet analysis of the offending traffic shows the following:

```
09:23:45.058939 IP 192.168.1.1:2562 > 170.43.30.4:0 Flags[], seq 1887775210:1887776670, win 512, length 1460
09:23:45.058940 IP 192.168.1.1:2563 > 170.43.30.4:0 Flags[], seq 1887775211:1887776671, win 512, length 1460
09:23:45.058941 IP 192.168.1.1:2564 > 170.43.30.4:0 Flags[], seq 1887775212:1887776672, win 512, length 1460
09:23:45.058942 IP 192.168.1.1:2565 > 170.43.30.4:0 Flags[], seq 1887775213:1887776673, win 512, length 1460
```

Which of the following mitigation techniques is MOST effective against the above attack?

A. The company should contact the upstream ISP and ask that RFC1918 traffic be dropped.
B. The company should implement a network-based sinkhole to drop all traffic coming from 192.168.1.1 at their gateway router.
C. The company should implement the following ACL at their gateway firewall:DENY IP HOST 192.168.1.1 170.43.30.0/24.
D. The company should enable the DoS resource starvation protection feature of the gateway NIPS.

Answer: A

Explanation: Topic 3, Exam Set C

NEW QUESTION 316
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 317
Poky allows scanning of vulnerabilities during production hours. But production servers have been crashing later due lo unauthorized scans performed by junior technicians. Which of the following is the BEST solution to avoid production server downtime due to these types of scans?

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

Answer: B

NEW QUESTION 322
A company installed a wireless network more than a year ago, standardizing on the same model APs in a single subnet. Recently, several users have reported timeouts and connection issues with Internet browsing. The security administrator has gathered some information about the network to try to recreate the issues with the assistance of a user. The administrator is able to ping every device on the network and confirms that the network is very slow.

Administrator's PC:	192.168.1.20
User's PC:	192.168.1.22
AP-Finance:	192.168.1.10
AP-Workshop:	192.168.1.11
AP-Lounge:	192.168.1.12
AP-Reception:	192.168.1.13
AP-Warehouse:	192.168.1.14
AP-IT:	192.168.1.15

Output:

```
Interface: 192.168.1.20 --- 0xf
Internet Address Physical Address Type
192.168.1.4 1a-25-0d-df-c6-27 dynamic
192.168.1.5 1a-25-0d-df-c8-00 dynamic
192.168.1.10 00-dc-3b-67-81-1a dynamic
192.168.1.11 c4-02-03-a1-4a-01 dynamic
192.168.1.12 00-dc-3b-67-82-02 dynamic
192.168.1.13 00-dc-3b-a5-ba-0b dynamic
192.168.1.14 00-dc-3b-67-88-07 dynamic
192.168.1.15 00-dc-3b-67-80-0a dynamic
192.168.1.20 1a-25-0d-df-8d-82 dynamic
192.168.1.22 1a-25-0d-df-89-cb dynamic
```

Given the above results, which of the following should the administrator investigate FIRST?

A. The AP-Workshop device
B. The AP-Reception device
C. The device at 192.168.1.4
D. The AP-IT device
E. The user's PC

Answer: A

NEW QUESTION 324
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 327
A logistics company's vulnerability scan identifies the following vulnerabilities on Internet-facing devices in the DMZ:

- SQL injection on an infrequently used web server that provides files to vendors
- SSL/TLS not used for a website that contains promotional information

The scan also shows the following vulnerabilities on internal resources:

- Microsoft Office Remote Code Execution on test server for a human resources system
- TLS downgrade vulnerability on a server in a development network

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

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

Answer: A

NEW QUESTION 332
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 334
The board of directors made the decision to adopt a cloud-first strategy. The current security infrastructure was designed for on-premise implementation. A critical application that is subject to the Federal Information Security Management Act (FISMA) of 2002 compliance has been identified as a candidate for a hybrid cloud deployment model. Which of the following should be conducted FIRST?

A. Develop a request for proposal.
B. Perform a risk assessment.
C. Review current security controls.
D. Review the SLA for FISMA compliance.

Answer: C

NEW QUESTION 335
Several accounting department users are reporting unusual Internet traffic in the browsing history of their workstations alter returning to work awl logging in. The building security team informs the IT security team that the cleaning stall was caught using the systems after the accounting department users left for the day Which of the following steps should the IT security team take to help prevent this from happening again? (Select TWO)

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

Answer: BC

NEW QUESTION 338
In order to the leverage the power of data correlation with Nessus, a cybersecurity analyst must first be able to create a table for the scan results.
Given the following snippet of code:

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

Which of the following output items would be correct?

A.

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

B.

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

C.

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

D.

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

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

Answer: A

NEW QUESTION 341
During an investigation, a computer is being seized. Which of the following is the FIRST step the analyst should take?

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

Answer: A

NEW QUESTION 342
Which of the following utilities could be used to resolve an IP address to a daman name, assuming the address has a PTR record?

A. ifconfig
B. ping
C. arp
D. nbtotot

Answer: B

NEW QUESTION 343
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 347
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 352
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 355
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 358
A cybersecurity analyst is reviewing Apache logs on a web server and finds that some logs are missing. The analyst has identified that the systems administrator accidentally deleted some log files. Which of the following actions or rules should be implemented to prevent this incident from reoccurring?

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

Answer: D

NEW QUESTION 361
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 363
A security analyst is conducting a vulnerability assessment of older SCADA devices on the corporate network. Which of the following compensating controls is likely to prevent the scans from providing value?

A. Access control list network segmentation that prevents access to the SCADA devices inside the network.
B. Detailed and tested firewall rules that effectively prevent outside access of the SCADA devices.
C. Implementation of a VLAN that allows all devices on the network to see all SCADA devices on the network.
D. SCADA systems configured with 'SCADA SUPPORT'=ENABLE

Answer: B

NEW QUESTION 368
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=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  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 369
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 371
Company A's security policy states that only PKI authentication should be used for all SSH accounts. A security analyst from Company A is reviewing the following auth.log and configuration settings:

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

Nov 1 09:53:12 comptia sshd[16269]: Failed publickey for dev from 192.168.2.6 port 53349 ssh2: RSA
SHA256:66c5a96384aa8ba16a71da278317edf4e62eda2c6453a736759186da3a2f7697
Nov 1 09:53:15 comptia sshd[16269]: Accepted password for dev from 192.168.2.6 port 53349 ssh2
Nov 1 09:53:15 comptia sshd[16269]: pam_unix(sshd:session): session opened for user dev by (uid=0)
Nov 1 09:53:15 comptia systemd-logind[590]: New session 499 of user dev.
Nov 1 09:53:15 comptia sshd[16269]: User child is on pid 16271
Nov 1 09:53:15 comptia sshd[16271]: Starting session: shell on pts/5 for dev from 1

Strict Modes no

RSAAuthentication yes

PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

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

IgnoreRhosts yes

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

RhostsRSSAuthentication no

# similar for protocol version 2

HostbasedAuthentication no

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

# Ignore User KnownHost yes

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

PermitEmptyPasswords no

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

# some PAM modules and threads);

ChallengeResponseAuthentication no

# Change to no to disable tunneled clear text passwords

PasswordAuthentication yes
```

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

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

Answer: E

NEW QUESTION 375
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 377
An analyst is preparing for a technical security compliance check on all Apache servers. Which of the following will be the BEST to use?

A. CIS benchmark
B. Nagios
C. OWASP
D. Untidy
E. Cain & Abel

Answer: A

NEW QUESTION 382
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 384
A security administrator uses FTK to take an image of a hard drive that is under investigation. Which of the following processes are used to ensure the image is the same as the original disk? (Choose two.)

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

Answer: BC

NEW QUESTION 385
A security incident has been created after noticing unusual behavior from a Windows domain controller. The server administrator has discovered that a user logged in to the server with elevated permissions, but the user's account does not follow the standard corporate naming scheme. There are also several other accounts in the administrators group that do not follow this naming scheme. Which of the following is the possible cause for this behavior and the BEST remediation step?

A. The Windows Active Directory domain controller has not completed synchronization, and should forceThe domain controller to sync.
B. The server has been compromised and should be removed from the network and cleaned before reintroducing it to the network.
C. The server administrator created user accounts cloning the wrong user ID, and the accounts should be removed from administrators and placed in an employee group.
D. The naming scheme allows for too many variations, and the account naming convention should be updates to enforce organizational policies.

Answer: D

NEW QUESTION 390
The development team recently moved a new application into production for the accounting department. After this occurred, the Chief Information Officer (CIO) was contacted by the head of accounting because the application is missing a key piece of functionality that is needed to complete the corporation's quarterly tax returns. Which of the following types of testing would help prevent this from reoccurring?

A. Security regression testing
B. User acceptance testing
C. Input validation testing
D. Static code testing

Answer: B

NEW QUESTION 392
An employee at an insurance company is processing claims that include patient addresses, clinic visits, diagnosis information, and prescription. While forwarding documentation to the supervisor, the employee accidentally sends the data to a personal email address outside of the company due to a typo. Which of the following types of data has been compromised?

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

Answer: D

NEW QUESTION 396
Which of the following is a best practice with regard to interacting with the media during an incident?

A. Allow any senior management level personnel with knowledge of the incident to discuss it.
B. Designate a single point of contact and at least one backup for contact with the media.
C. Stipulate that incidents are not to be discussed with the media at any time during the incident.
D. Release financial information on the impact of damages caused by the incident.

Answer: B

NEW QUESTION 399
A security analyst received an alert from the antivirus software identifying a complex instance of malware on a company's network. The company does not have the resources to fully analyze the malware and determine its effect on the system. Which of the following is the BEST action to take in the incident recovery and post-incident response process?

A. Wipe hard drives, reimage the systems, and return the affected systems to ready state.

B. Detect and analyze the precursors and indicators; schedule a lessons learned meeting.
C. Remove the malware and inappropriate materials; eradicate the incident.
D. Perform event correlation; create a log retention policy.

Answer: C

NEW QUESTION 404
A company provides wireless connectivity to the internal network from all physical locations for companyowned devices. Users were able to connect the day before, but now all users have reported that when they connect to an access point in the conference room, they cannot access company resources. Which of the following BEST describes the cause of the problem?

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

Answer: D

NEW QUESTION 408
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 410
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 411
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 413
A medical organization recently started accepting payments over the phone. The manager is concerned about the impact of the storage of different types of data.

Which of the following types of data incurs the highest regulatory constraints?

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

Answer: B

NEW QUESTION 414
An analyst reviews a recent report of vulnerabilities on a company's application server. Which of the following should the analyst rate as being of the HIGHEST importance to the company's environment?

A. Banner grabbing
B. Remote code execution
C. SQL injection
D. Use of old encryption algorithms
E. Susceptibility to XSS

Answer: B

NEW QUESTION 416
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. ^[0-9] (16) $
B. (0-9) × 16
C. " 1234-5678"
D. "04*"

Answer: A

NEW QUESTION 418
An organization is conducting penetration testing to identify possible network vulnerabilities. The penetration tester has already identified active hosts in the network and is now scanning individual hosts to determine if any are running a web server. The output from the latest scan is shown below:

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

PORT     STATE     SERVICE
80/tcp   open      http

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

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

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

Answer: A

NEW QUESTION 421
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 425
Which of the following organizations would have to remediate embedded controller vulnerabilities?

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

Answer: D

NEW QUESTION 430
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 433
The development team cur.en.ly consists of lh.ee developers who each specialize in a specific programming language:
Developer 1 – C++/C#
Developer 2 – Python Developer 3 – Assembly
Which of the following SDLC best practices would be challenging lo implement with the current available staff?

A. Fuzzing
B. Peer review
C. Regression testing
D. Stress testing

Answer: B

NEW QUESTION 437
Management wants to scan servers for vulnerabilities on a periodic basis. Management has decided that the scan frequency should be determined only by vendor patch schedules and the organization's application deployment schedule. Which of the following would force the organization to conduct an out-of-cycle vulnerability scan?

A. Newly discovered PII on a server
B. A vendor releases a critical patch update
C. A critical bug fix in the organization's application
D. False positives identified in production

Answer: B

NEW QUESTION 440
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 445
A cybersecurity analyst wants to use ICMP ECHO_REQUEST on a machine while using Nmap. Which of the following is the correct command to accomplish this?

A. $ nmap –PE 192.168.1.7
B. $ ping --PE 192.168.1.7
C. $ nmap --traceroute 192.168.1.7
D. $ nmap –PO 192.168.1.7

Answer: A

NEW QUESTION 448
A company's asset management software has been discovering a weekly increase in non-standard software installed on end users' machines with duplicate license keys. The security analyst wants to know if any of this software is listening on any non-standard ports, such as 6667. Which of the following tools should the analyst recommend to block any command and control traffic?

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

Answer: A

NEW QUESTION 451
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 454
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 455
On winch of the following organizational resources is the lack of an enabled password or PIN a common vulnerability?

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

Answer: B

NEW QUESTION 460
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CS0-001 Exam with Our Prep Materials Via below:

https://www.certleader.com/CS0-001-dumps.html