CuramSoftware.CS0-002.v2022-03-25.q285

Exam Code:	CS0-002
Exam Name:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
Certification Provider:	CompTIA
Free Question Number:	285
Version:	v2022-03-25
# of views:	6563
# of Questions views:	2850
https://www.freepdfdumps.com/CuramSoftware.CS0-002.v2022-03-25.q285.html	

NEW QUESTION: 1
A cybersecurity analyst is contributing to a team hunt on an organization's endpoints.
Which of the following should the analyst do FIRST?
A. Write detection logic.
B. Establish a hypothesis.
C. Profile the threat actors and activities.
D. Perform a process analysis.
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://www.cybereason.com/blog/blog-the-eight-steps-to-threat-hunting

NEW QUESTION: 2
A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures.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:
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 true negative and the new computers have the correct version of the software
B. This is a false positive and the scanning plugin needs to be updated by the vendor
C. This is a false negative and the new computers need to be updated by the desktop team
D. This is a true positive and the new computers were imaged with an old version of the software
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
Hotspot Question
A security analyst performs various types of vulnerability scans. You must review the vulnerability scan results to determine the type of scan that was executed and determine if a false positive occurred for each device.
Instructions:
Select the drop option for whether the results were generated from a credentialed scan, non- credentialed scan, or a compliance scan.
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives.

NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time. Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.
The Linux Web Server, File-Print Server and Directory Server are draggable. If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.
Answer:

NEW QUESTION: 4
A security analyst has noticed an alert from the SIEM. A workstation is repeatedly trying to connect to port 445 of a file server on the production network. All of the attempts are made with invalid credentials. Which of the following describes what is occurring?
A. An attacker has gained control of the workstation and is attempting to pivot to the file server by creating an SMB session.
B. An attacker has gained control of the workstation and is port scanning the network.
C. Malware has infected the workstation and is beaconing out to the specific IP address of the file server.
D. The file server is attempting to transfer malware to the workstation via SMB.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 5
Clients are unable to access a company's API to obtain pricing dat
a. An analyst discovers sources other than
clients are scraping the API for data, which is causing the servers to exceed available resources. Which of the following would be BEST to protect the availability of the APIs?
A. Virtual private network
B. Certificate-based authentication
C. IP whitelisting
D. Web application firewall
Answer: C (LEAVE A REPLY)

NEW QUESTION: 6
When reviewing network traffic, a security analyst detects suspicious activity:
Based on the log above, which of the following vulnerability attacks is occurring?
A. ShellShock
B. DROWN
C. Zeus
D. Heartbleed
E. POODLE
Answer: (SHOW ANSWER)
The DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) attack is a cross- protocol security bug that attacks servers supporting modern TLS protocol suites by using their support for the obsolete, insecure, SSL v2 protocol to leverage an attack on connections using up-to-date protocols that would otherwise be secure.DROWN can affect all types of servers that offer services encrypted with TLS yet still support SSLv2, provided they share the same public key credentials between the two protocols. Additionally, if the same public key certificate is used on a different server that supports SSLv2, the TLS server is also vulnerable due to the SSLv2 server leaking key information that can be used against the TLS server.

NEW QUESTION: 7
In order to leverage the power of data correlation within Nessus, a cybersecurity analyst needs to write an SQL statement that will provide how long a vulnerability has been present on the network.
Given the following output table:
Which of the following SQL statements would provide the resulted output needed for this correlation?
A. SELECT Port, ScanDate, IP, PlugIn FROM MyResults WHERE PluginID=`1000'
B. SELECT ScanDate, IP, Port, PlugIn SET MyResults WHERE PluginID=`1000'
C. SELECT ScanDate, IP, Port, PlugIn FROM MyResults WHERE PluginID=`1000'
D. SELECT IP, PORT, PlugIn, ScanDate FROM MyResults SET PluginID=`1000'
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
After reading about data breaches at a competing company, senior leaders in an organization have grown increasingly concerned about social engineering attacks. They want to increase awareness among staff regarding this threat, but do not want to use traditional training methods because they regard these methods as ineffective.
Which of the following approaches would BEST meet the requirements?
A. Simulated phishing emails asking employees to reply to the email with their updated phone number and office location
B. USB drives randomly placed inside and outside the organization that contain a pop-up warning to any users who plug the drive into their computer
C. Classroom training on the dangers of social media followed by a test and gift certificates for any employee getting a perfect score.
D. A poster contest to raise awareness of PII and asking employees to provide examples of data breaches and consequences
Answer: C (LEAVE A REPLY)

NEW QUESTION: 9
Bootloader malware was recently discovered on several company workstations. All the workstations run Windows and are current models with UEFI capability.
Which of the following UEFI settings is the MOST likely cause of the infections?
A. Compatibility mode
B. Secure boot mode
C. Native mode
D. Fast boot mode
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 10
A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?
A. Option C
B. Option B
C. Option D
D. Option A
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11

A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:
The analyst runs the following command next:
Which of the following would explain the difference in results?
A. ICMP is being blocked by a firewall.
B. The routing tables for ping and hping3 were different.
C. hping3 is returning a false positive.
D. The original ping command needed root permission to execute.
Answer: (SHOW ANSWER)

NEW QUESTION: 12
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. Ensure EDR signatures are updated every day to avert infection.
B. Implement an EDR mail module that will rewrite and analyze email links.
C. Turn on full behavioral analysis to avert an infection
D. Reconfigure the EDR solution to perform real-time scanning of all files
E. Modify the EDR solution to use heuristic analysis techniques for malware.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 13
The Chief Information Officer (CIO) for a large manufacturing organization has noticed a significant number of unknown devices with possible malware infections are on the organization's corporate network.
Which of the following would work BEST to prevent the issue?
A. Segment the network to isolate all systems that contain highly sensitive information, such as intellectual property.
B. Reconfigure the NAC solution to prevent access based on a full device profile and ensure antivirus is installed.
C. Implement certificate validation on the VPN to ensure only employees with the certificate can access the company network.
D. Update the antivirus configuration to enable behavioral and real-time analysis on all systems within the network.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:
Which of the following is MOST likely a false positive?
A. ICMP timestamp request remote date disclosure
B. Anonymous FTP enabled
C. Unsupported web server detection
D. Windows SMB service enumeration via \srvsvc
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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 and can only be programmed once. Code deployment safeguards are needed.
C. FPGAs have an inflexible architecture. Additional training for developers is needed
D. FPGAs are expensive to produce. Anti-counterierting safeguards are needed.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
A company provides wireless connectivity to the internal network from all physical locations for company- owned devices. Users were able to connect the day before, but now all users have reported that when they connect to an access point in the conference room, they cannot access company resources. Which of the following BEST describes the cause of the problem?
A. The access point is a rogue device. Follow incident response procedures.
B. The network is not available. Escalate the issue to network support.
C. Expired DNS entries on users' devices. Request the affected users perform a DNS flush.
D. The access point is blocking access by MAC address. Disable MAC address filtering.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 17
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. false positives
B. verification of mitigation
C. hardening validation.
D. the criticality index
E. false negatives
Answer: (SHOW ANSWER)

NEW QUESTION: 18
An analyst is detecting Linux machines on a Windows network. Which of the following tools should be used to detect a computer operating system?
A. nmap
B. nslookup
C. whois
D. netstat
Answer: A (LEAVE A REPLY)

NEW QUESTION: 19
Which of the following policies BEST explains the purpose of a data ownership policy?
A. The policy should describe the roles and responsibilities between users and managers, and the management of specific data types.
B. The policy should establish the protocol for retaining information types based on regulatory or business needs.
C. The policy should document practices that users must adhere to in order to access data on the corporate network or Internet.
D. The policy should outline the organization's administration of accounts for authorized users to access the appropriate data.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 20
A cybersecurity analyst was hired to resolve a security issue within a company after it was reported that many employee account passwords had been compromised. Upon investigating the incident, the cybersecurity analyst found that a brute force attack was launched against the company. Which of the following remediation actions should the cybersecurity analyst recommend to senior management to address these security issues?
A. Implement DLP solution.
B. Require security awareness training.
C. Deploy multifactor authentication.
D. Prohibit password reuse using a GPO.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21
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:
Which of the following should be the focus of the investigation?
A. webserver.org-dmz.org
B. 83hht23.org-int.org
C. sftp.org-dmz.org
D. ftps.bluemed.net
Answer: D (LEAVE A REPLY)

NEW QUESTION: 22
A technician recently fixed a computer with several viruses and spyware programs on it and notices the Internet settings were set to redirect all traffic through an unknown proxy.
This type of attack is known as which of the following?
A. Shoulder surfing
B. Phishing
C. Social engineering
D. Man-in-the-middle
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
A software development company in the manufacturing sector has just completed the alpha version of its flagship application. The application has been under development for the past three years. The SOC has seen intrusion attempts made by indicators associated with a particular APT.

The company has a hot site location for COOP. Which of the following threats would most likely incur the BIGGEST economic impact for the company?
A. ICS destruction
B. DDoS
C. IPS evasion
D. IP theft
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
A security analyst has been asked to scan a subnet. During the scan, the following output was generated:
Based on the output above, which of the following is MOST likely?
A. 192.168.100.145 is a DNS server
B. 192.168.100.214 is a secure FTP server
C. Both hosts are mail servers
D. 192.168.100.214 is a web server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 25
A security analyst received several service tickets reporting that a company storefront website is not accessible by internal domain users. However, external users are accessing the website without issue. Which of the following is the MOST likely reason for this behavior?
A. The time synchronization server is corrupted.
B. The FQDN is incorrect.
C. The DNS server is corrupted.
D. The certificate is expired.
Answer: (SHOW ANSWER)

NEW QUESTION: 26
A staff member reported that a laptop has degraded performance. The security analyst has investigated the issue and discovered that CPU utilization, memory utilization, and outbound network traffic are consuming the laptop resources. Which of the following is the BEST course of actions to resolve the problem?
A. Ensure the laptop OS is properly patched.
B. Identify and remove malicious processes.
C. Disable scheduled tasks.
D. Increase laptop memory.
E. Suspend virus scan.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 27
A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage The security analyst is trying to determine which user caused the malware to get onto the system Which of the following registry keys would MOST likely have this information?
A)
B)

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

NEW QUESTION: 28
A custom script currently monitors real-time logs of a SAMIL authentication server to mitigate brute-force attacks. Which of the following is a concern when moving authentication to a cloud service?
A. SAML logging is not supported for cloud-based authentication.
B. Log data may be visible to other customers.
C. Logs may contain incorrect information.
D. Access to logs may be delayed for some time.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
A security analyst received a SIEM alert regarding high levels of memory consumption for a critical system.
After several attempts to remediate the issue, the system went down. A root cause analysis revealed a bad actor forced the application to not reclaim memory. This caused the system to be depleted of resources.
Which of the following BEST describes this attack?
A. Array attack
B. Memory corruption
C. Injection attack
D. Denial of service
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
Which one of the following is an example of a computer security incident?
A. User accesses a secure file
B. Intruder breaks into a building
C. Administrator changes a file's permission settings
D. Former employee crashes a server
Answer: (SHOW ANSWER)

NEW QUESTION: 31
A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.
To BEST mitigate this risk, the analyst should use _____.
A. an 802.11ac wireless bridge to create an air gap.

B. a managed switch to segment the lab into a separate VLAN.
C. an unmanaged switch to segment the environments from one another.
D. a firewall to isolate the lab network from all other networks.
Answer: (SHOW ANSWER)

NEW QUESTION: 32
A security analyst is conducting traffic analysis and observes an HTTP POST to a web server.
The POST header is approximately 1000 bytes in length. During transmission, one byte is delivered every ten seconds. Which of the following attacks is the traffic indicative of?
A. SQL injection
B. Exfiltration
C. Buffer overflow
D. DoS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
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. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.
B. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.
C. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.
D. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 34
A company's security officer needs to implement geographical IP blocks for nation-state actors from a foreign country On which of the following should the blocks be implemented'?
A. Data loss prevention
B. Access control list
C. Network access control
D. Web content filter
Answer: B (LEAVE A REPLY)

NEW QUESTION: 35

An employee was conducting research on the Internet when a message from cyber criminals appeared on the screen, stating the hard drive was just encrypted by a ransomware variant. An analyst observes the following:
* Antivirus signatures were updated recently
* The desktop background was changed
* Web proxy logs show browsing to various information security sites and ad network traffic
* There is a high volume of hard disk activity on the file server
* SMTP server shown the employee recently received several emails from blocked senders
* The company recently switched web hosting providers
* There are several IPS alerts for external port scans
Which of the following describes how the employee got this type of ransomware?
A. The employee opened an email attachment
B. The employee fell victim to a CSRF attack
C. The employee was using another user's credentials
D. The employee updated antivirus signatures
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
A security analyst is investigating a system compromise. The analyst verifies the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely exploited?
A. Buffer overflow
B. Advanced persistent threat
C. Insider threat
D. Zero day
Answer: D (LEAVE A REPLY)

NEW QUESTION: 37
A security analyst is reviewing a suspected phishing campaign that has targeted an organisation. The organization has enabled a few email security technologies in the last year: however, the analyst believes the security features are not working. The analyst runs the following command:
> dig domain._domainkey.comptia.orq TXT
Which of the following email protection technologies is the analyst MOST likely validating?
A. DKIM
B. SPF
C. DMARC
D. DNSSEC
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38
D18912E1457D5D1DDCBD40AB3BF70D5D
A security analyst scanned an internal company subnet and discovered a host with the following Nmap output.
Based on the output of this Nmap scan, which of the following should the analyst investigate FIRST?
A. Port 22

B. Port 3389
C. Port 445
D. Port 135
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39
A company decides to move three of its business applications to different outsourced cloud providers. After moving the applications, the users report the applications time out too quickly and too much time is spent logging back into the different web-based applications throughout the day.
Which of the following should a security architect recommend to improve the end-user experience without lowering the security posture?
A. Configure user accounts for self-service account management.
B. Configure a web browser to cache the user credentials.
C. Create a group policy to extend the default system lockout period.
D. Configure directory services with a federation provider to manage accounts.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 40
Given the following access log:
Which of the following accurately describes what this log displays?
A. A vulnerability in jQuery
B. A vulnerability scan performed from the Internet
C. A vulnerability in Javascript
D. Application integration with an externally hosted database
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
During routine monitoring, a security analyst discovers several suspicious websites that are communicating with a local host. The analyst queries for IP 192.168.50.2 for a 24-hour period:
To further investigate, the analyst should request PCAP for SRC 192.168.50.2 and _____.
A. DST 138.10.2.5.
B. DST 138.10.25.5.
C. DST 172.10.3.5.
D. DST 172.10.45.5.
E. DST 175.35.20.5.
Answer: C (LEAVE A REPLY)
Explanation

NEW QUESTION: 42
A cybersecurity analyst is responding to an incident. The company's leadership team wants to attribute the incident to an attack group. Which of the following models would BEST apply to the situation?
A. Intelligence cycle
B. MITRE ATT&CK

C. Diamond Model of Intrusion Analysis
D. Kill chain
Answer: (SHOW ANSWER)

NEW QUESTION: 43
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 public relations policy
B. senior management's guidance
C. the responder's discretion
D. the communication plan
Answer: C (LEAVE A REPLY)

NEW QUESTION: 44
Which of the following sets of attributes BEST illustrates the characteristics of an insider threat from a security perspective?
A. Unauthorized, unintentional, benign
B. Unauthorized, intentional, malicious
C. Authorized, intentional, malicious
D. Authorized, unintentional, benign
Answer: C (LEAVE A REPLY)
Reference:
https://www.sciencedirect.com/topics/computer-science/insider-attack

NEW QUESTION: 45
A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT.
Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?
A. Attack vectors
B. Adversary capability
C. Diamond Model of Intrusion Analysis
D. Kill chain
E. Total attack surface
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.secureworks.com/blog/advanced-persistent-threats-apt-b

NEW QUESTION: 46
A malicious hacker wants to gather guest credentials on a hotel 802.11 network. Which of the following tools is the malicious hacker going to use to gain access to information found on the hotel network?
A. Aircrak-ng
B. Nikto
C. tcpdump
D. Nessus
Answer: A (LEAVE A REPLY)

NEW QUESTION: 47
A security analyst discovered a specific series of IP addresses that are targeting an organization. None of the attacks have been successful. Which of the following should the security analyst perform NEXT?
A. Begin blocking all IP addresses within that subnet.
B. Conduct threat research on the IP addresses
C. Begin a kill chain analysis to determine the impact.
D. Determine the attack vector and total attack surface.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 48
A threat feed notes malicious actors have been infiltrating companies and exfiltrating data to a specific set of domains. Management at an organization wants to know if it is a victim. Which of the following should the security analyst recommend to identify this behavior without alerting any potential malicious actors?
A. Create an IPS rule to block these domains and trigger an alert within the SIEM tool when these domains are requested.
B. Add the domains to a DNS sinkhole and create an alert in the SIEM tool when the domains are queried
C. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this information
D. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443
Answer: B (LEAVE A REPLY)

NEW QUESTION: 49
Understanding attack vectors and integrating intelligence sources are important components of:
A. a vulnerability management plan.
B. proactive threat hunting
C. an incident response plan.
D. risk management compliance.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50
A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:
Which of the following should the analyst review to find out how the data was exfilltrated?
A. Wednesday's logs
B. Monday's logs
C. Tuesday's logs
D. Thursday's logs

Answer: D (LEAVE A REPLY)

NEW QUESTION: 51
An organization uses Common Vulnerability Scoring System (CVSS) scores to prioritize remediation of vulnerabilities.
Management wants to modify the priorities based on a difficulty factor so that vulnerabilities with lower CVSS scores may get a higher priority if they are easier to implement with less risk to system functionality. Management also wants to quantify the priority. Which of the following would achieve management's objective?
A. ((CVSS Score) * 2) / Difficulty = PriorityWhere CVSS Score is weighted and Difficulty is a range from 1 to 5 with 5 being easiest and lowest risk to implement
B. (CVSS Score) / Difficulty = PriorityWhere Difficulty is a range from 1 to 10 with 10 being easiest and lowest risk to implement
C. (CVSS Score) * Difficulty = PriorityWhere Difficulty is a range from 1 to 5 with 1 being easiest and lowest risk to implement
D. (CVSS Score) * Difficulty = PriorityWhere Difficulty is a range from 0.1 to 1.0 with 1.0 being easiest and lowest risk to implement
Answer: B (LEAVE A REPLY)

NEW QUESTION: 52
An employee at an insurance company is processing claims that include patient addresses, clinic visits, diagnosis information, and prescription. While forwarding documentation to the supervisor, the employee accidentally sends the data to a personal email address outside of the company due to a typo. Which of the following types of data has been compromised?
A. Proprietary information
B. Intellectual property
C. PHI
D. PCI
Answer: (SHOW ANSWER)

NEW QUESTION: 53
A security analyst is reviewing the logs from an internal chat server. The chat.logfile is too large to review manually, so the analyst wants to create a shorter log file that only includes lines associated with a user demonstrating anomalous activity. Below is a snippet of the log:
Which of the following commands would work BEST to achieve the desired result?
A. grep -i chatter14 chat.log
B. grep -i pythonfun chat.log
C. grep -v pythonfun chat.log
D. grep -v chatter14 chat.log
E. grep -v javashark chat.log
F. grep -i javashark chat.log
Answer: E (LEAVE A REPLY)

NEW QUESTION: 54
A security analyst is evaluating two vulnerability management tools for possible use in an organization. The analyst set up each of the tools according to the respective vendor's instructions and generated a report of vulnerabilities that ran against the same target server.
Tool A reported the following:
Tool B reported the following:
Which of the following BEST describes the method used by each tool? (Choose two.)
A. Tool B is agent based.

B. Tool A is agent based.
C. Tool A used fuzzing logic to test vulnerabilities.
D. Tool A is unauthenticated.
E. Tool B is unauthenticated.
F. Tool B utilized machine learning technology.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 55
A cybersecurity consultant is reviewing the following output from a vulnerability scan against a newly installed MS SQL Server 2012 that is slated to go into production in one week:
Based on the above information, which of the following should the system administrator do?
(Select TWO).
A. Verify the vulnerability using penetration testing tools or proof-of-concept exploits.
B. Mark the result as a false positive so it will show in subsequent scans.
C. Configure a network-based ACL at the perimeter firewall to protect the MS SQL port.
D. Review the references to determine if the vulnerability can be remotely exploited.
E. Implement the proposed solution by installing Microsoft patch Q316333.
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Law enforcement has contacted a corporation's legal counsel because correlated data from a breach shows the organization as the common denominator from all indicators of compromise.
An employee overhears the conversation between legal counsel and law enforcement, and then posts a comment about it on social media. The media then starts contacting other employees about the breach.
Which of the following steps should be taken to prevent further disclosure of information about the breach?
A. Law enforcement meeting with employees
B. Security awareness about incident communication channels
C. Request all employees verbally commit to an NDA about the breach
D. Temporarily disable employee access to social media
Answer: (SHOW ANSWER)

NEW QUESTION: 57
A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.
To BEST mitigate this risk, the analyst should use .
A. an unmanaged switch to segment the environments from one another.
B. an 802.11ac wireless bridge to create an air gap.
C. a firewall to isolate the lab network from all other networks.
D. a managed switch to segment the lab into a separate VLAN.
Answer: (SHOW ANSWER)

NEW QUESTION: 58
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. proxy to block all connections to <malwaresource>.
C. IDS to match the malware sample.
D. firewall to block connection attempts to dynamic DNS hosts.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 59
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 communication plan
B. the responder's discretion
C. the public relations policy
D. senior management's guidance
Answer: (SHOW ANSWER)

NEW QUESTION: 60
A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Big 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. $75,000
B. $300,000
C. $1.425 million
D. $1.5 million
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?
A. Data custodian
B. Data owner
C. Data processor
D. Senior management
Answer: (SHOW ANSWER)
Reference:
https://www.pearsonitcertification.com/articles/article.aspx?p=2731933&seqNum=3

NEW QUESTION: 62
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.
Which of the following commands should the analyst investigate FIRST?
A. Line 5
B. Line 6
C. Line 2
D. Line 4
E. Line 1
F. Line 3
Answer: C (LEAVE A REPLY)

NEW QUESTION: 63
Which of me following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?
A. It establishes a continuous integration environment for software development operations
B. It automatically performs remedial configuration changes lo enterprise security services
C. It provides validation of suspected system vulnerabilities through workflow orchestration
D. It enables standard checklist and vulnerability analysis expressions for automaton
Answer: (SHOW ANSWER)

NEW QUESTION: 64
A systems administrator is trying to secure a critical system. The administrator has placed the system behind a firewall, enabled strong authentication, and required all administrators of this system to attend mandatory training.
Which of the following BEST describes the control being implemented?
A. Defense in depth
B. Access control
C. Multifactor authentication
D. Audit remediation
Answer: (SHOW ANSWER)

NEW QUESTION: 65
A new zero-day vulnerability was discovered within a basic screen capture app, which is used throughout the environment. Two days after discovering the vulnerability, the manufacturer of the software has not announced a remediation or if there will be a fix for this newly discovered vulnerability. The vulnerable application is not uniquely critical, but it is used occasionally by the management and executive management teams. The vulnerability allows remote code execution to gain privileged access to the system. Which of the following is the BEST course of actions to mitigate this threat?
A. Block the vulnerable application traffic at the firewall and disable the application services on each computer.
B. Communicate with the end users that the application should not be used until the manufacturer has resolved the vulnerability.

C. Work with the manufacturer to determine the time frame for the fix.
D. Remove the application and replace it with a similar non-vulnerable application.
Answer: (SHOW ANSWER)

NEW QUESTION: 66
The help desk informed a security analyst of a trend that is beginning to develop regarding a suspicious email that has been reported by multiple users.
The analyst has determined the email includes an attachment named invoice.zip that contains the following files:
* Locky.js
* xerty.ini
* xerty.lib
Further analysis indicates that when the .zip file is opened, it is installing a new version of ransomware on the devices.
Which of the following should be done FIRST to prevent data on the company NAS from being encrypted by infected devices?
A. Disable access to the company VPN.
B. Add the URL included in the .js file to the company's web proxy filter.
C. Email employees instructing them not to open the invoice attachment.
D. Set permissions on file shares to read-only.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 67
A security analyst gathered forensics from a recent intrusion in preparation for legal proceedings. The analyst used EnCase to gather the digital forensics, cloned the hard drive, and took the hard drive home for further analysis. Which of the following did the security analyst violate?
A. Hashing procedures
B. Virtualization
C. Chain of custody
D. Cloning procedures
Answer: C (LEAVE A REPLY)

NEW QUESTION: 68
A security analyst is reviewing the following log from an email security service.
Which of the following BEST describes the reason why the email was blocked?
A. The email originated from the www.spamfilter.org URL.
B. The From address is invalid.
C. The To address is invalid.
D. The IP address and the remote server name are the same.
E. The IP address was blacklisted.
Answer: (SHOW ANSWER)

NEW QUESTION: 69
During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation . Which of the following would cause the analyst to further review the incident?
A)

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

NEW QUESTION: 70
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. Remove the rule from the email client and change the password
B. Check the server logs to evaluate which emails were sent to <someaddress@domain.com>
C. Use the SIEM to correlate logging events from the email server and the domain server
D. Recommend that management implement SPF and DKIM
Answer: (SHOW ANSWER)

NEW QUESTION: 71
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. Remove it from the network and require air gapping.
B. Only allow access to the system via a jumpbox
C. Virtualize the system and decommission the physical machine.
D. Implement MFA on the specific system.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 72
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.
Which of the following commands should the analyst investigate FIRST?
A. Line 2
B. Line 5
C. Line 3
D. Line 1
E. Line 6
F. Line 4
Answer: A (LEAVE A REPLY)

NEW QUESTION: 73
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 deep
B. relevant and accurate
C. proprietary and timely
D. proprietary and accurate
Answer: (SHOW ANSWER)

NEW QUESTION: 74
A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output.
Which of the following commands should the administrator run NEXT to further analyze the compromised system?
A. rpm -V openash-server
B. strace /proc/1301
C. /bin/la -1 /proc/1301/exe
D. kill -9 1301
Answer: B (LEAVE A REPLY)

NEW QUESTION: 75
A security analyst has received reports of very slow, intermittent access to a public-facing corporate server.
Suspecting the system may be compromised, the analyst runs the following commands:
Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?
A. Run kill -9 1325 to bring the load average down so the server is usable again.
B. Examine the server logs for further indicators of compromise of a web application.
C. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.
D. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.
Answer: (SHOW ANSWER)

NEW QUESTION: 76
A security analyst is attempting to utilize the blowing threat intelligence for developing detection capabilities:
In which of the following phases is this APT MOST likely to leave discoverable artifacts?
A. Reconnaissance
B. Lateral movement
C. Data collection/exfiltration
D. Defensive evasion
Answer: C (LEAVE A REPLY)

NEW QUESTION: 77
A security analyst for a large pharmaceutical company was given credentials from a threat intelligence resources organisation for Internal users, which contain usernames and valid passwords for company accounts.
Which of the following is the FIRST action the analyst should take as part of security operations monitoring?
A. Change all the user passwords to ensure the malicious actors cannot use them.
B. Search the event logs for event identifiers that indicate Mimikatz was used.
C. Reimage the machines of all users within the group in case of a malware infection.
D. Run scheduled antivirus scans on all employees' machines to look for malicious processes.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 78
A security analyst needs to reduce the overall attack surface.
Which of the following infrastructure changes should the analyst recommend?
A. Implement a honeypot.
B. Air gap sensitive systems.
C. Increase the network segmentation.
D. Implement a cloud-based architecture.
Answer: C (LEAVE A REPLY)
Reference:
https://www.securitymagazine.com/articles/89283-ways-to-reduce-your-attack-surface

NEW QUESTION: 79
A new security manager was hired to establish a vulnerability management program. The manager asked for a corporate strategic plan and risk register that the project management office developed. The manager conducted a tools and skill sets inventory to document the plan. Which of the following is a critical task for the establishment of a successful program?
A. Perform information classification
B. Establish corporate policy
C. Update vulnerability feed
D. Establish continuous monitoring
Answer: B (LEAVE A REPLY)

NEW QUESTION: 80
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:
Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?
A. Accept this risk for now because this is a "high" severity, but testing will require more than the four days available, and the system ATO needs to be competed.

B. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
C. Ignore it. This is false positive, and the organization needs to focus its efforts on other findings.
D. Ensure HTTP validation is enabled by rebooting the server.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 81
A security analyst is reviewing the following log after enabling key-based authentication.
Given the above information, which of the following steps should be performed NEXT to secure the system?
A. Disable password authentication for SSH.
B. Disable remote root SSH logins.
C. Disable anonymous SSH logins.
D. Disable SSHv1.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 82
A technician receives the following security alert from the firewall's automated system:
After reviewing the alert, which of the following is the BEST analysis?
A. This alert is a false positive because DNS is a normal network function.
B. This alert indicates an endpoint may be infected and is potentially contacting a suspect host.
C. This alert was generated by the SIEM because the user attempted too many invalid login attempts.
D. This alert indicates a user was attempting to bypass security measures using dynamic DNS.
Answer: (SHOW ANSWER)

NEW QUESTION: 83
A cybersecurity analyst has received the laptop of a user who recently left the company.
The analyst types `history' into the prompt, and sees this line of code in the latest bash history:
This concerns the analyst because this subnet should not be known to users within the company.
Which of the following describes what this code has done on the network?
A. Sent 255 ping packets to each host on the network.
B. Sequentially sent an ICMP echo reply to the Class C network.
C. Performed a half open SYB scan on the network.
D. Performed a ping sweep of the Class C network.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 84
An organization wants to move non-essential services into a cloud computing environment. Management has a cost focus and would like to achieve a recovery time objective of 12 hours. Which of the following cloud recovery strategies would work BEST to attain the desired outcome?
A. Configure the systems with a cold site at another cloud provider that can be used for failover.
B. Establish a hot site with active replication to another region within the same cloud provider.
C. Set up a warm disaster recovery site with the same cloud provider in a different region
D. Duplicate all services in another instance and load balance between the instances.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 85
An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds.
Which of the following can be inferred from this activity?
A. 10.200.2.5 is exfiltrating data.
B. 10.200.2.5 is a rogue endpoint.
C. 10.200.2.0/24 is infected with ransomware.
D. 10.200.2.0/24 is not routable address space.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 86
During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation. Which of the following would cause the analyst to further review the incident?
A. BadReputationIp - - [2019-04-12 10:43Z] "GET /etc/passwd" 403 1023
B. BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=/etc/passwd" 403 11056
C. BadReputationIp - - [2019-04-12 10:43Z] "GET /favicon.ico?src=../usr/share/ icons" 200 19064
D. BadReputationIp - - [2019-04-12 10:43Z] "GET /index.html?src=../.ssh/id_rsa" 401 17044
E. BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=../../.ssh/id_rsa" 200 15036
Answer: C (LEAVE A REPLY)

NEW QUESTION: 87
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 TACACS+ technology.
B. Switch to the WPA2 protocol.
C. Switch to RADIUS technology
D. Switch to 802 IX technology
Answer: C (LEAVE A REPLY)

NEW QUESTION: 88
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website.
During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.
Which of the following describes the type of attack the proxy has been legitimately programmed to perform?
A. Spoofing
B. Replay
C. Man-in-the-middle
D. Transitive access

Answer: C (LEAVE A REPLY)

NEW QUESTION: 89
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. $300.000
B. $75.000
C. $1.5 million
D. $1.425 million
Answer: B (LEAVE A REPLY)

NEW QUESTION: 90
A company is developing its first mobile application, which will be distributed via the official application stores of the two major mobile platforms.
Which of the following is a prerequisite to making the applications available in the application stores?
A. Deploy machine/computer certificates.
B. Implement a CRL.
C. Distribute user certificates.
D. Obtain a code-signing certificate.
Answer: (SHOW ANSWER)

NEW QUESTION: 91
A company's incident response team is handling a threat that was identified on the network. Security analysts have determined a web server is making multiple connections from TCP port 445 outbound to servers inside its subnet as well as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?
A. Quarantine the web server
B. Deploy virtual firewalls
C. Capture a forensic image of the memory and disk
D. Enable web server containerization
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 92
While reviewing web server logs, a security analyst notices the following code:
Which of the following would prevent this code from performing malicious actions?

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

NEW QUESTION: 93
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. Only allow access to the system via a jumpbox
C. Remove it from the network and require air gapping.
D. Implement MFA on the specific system.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 94
A system administrator has reviewed the following output:
Which of the following can a system administrator infer from the above output?
A. The company web server has been compromised.
B. The company email server is running a non-standard port.
C. The company email server has been compromised.
D. The company is running a vulnerable SSH server.
Answer: (SHOW ANSWER)

NEW QUESTION: 95
A system administrator is doing network reconnaissance of a company's external network to determine the vulnerability of various services that are running. Sending some sample traffic to the external host, the administrator obtains the following packet capture:
Based on the output, which of the following services should be further tested for vulnerabilities?
A. SSH
B. SMB
C. HTTPS
D. HTTP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 96
An analyst has been asked to provide feedback regarding the control required by a revised regulatory framework At this time, the analyst only needs to focus on the technical controls. Which of the following should the analyst provide an assessment of?
A. Establishment o' data classifications
B. Tokenization of sensitive data
C. Reporting on data retention and purging activities
D. Execution of NDAs

E. Formal identification of data ownership
Answer: (SHOW ANSWER)

NEW QUESTION: 97
A company has received the results of an external vulnerability scan from its approved scanning vendor. The company is required to remediate these vulnerabilities for clients within 72 hours of acknowledgement of the scan results.
Which of the following contract breaches would result if this remediation is not provided for clients within the time frame?
A. Organizational governance
B. Memorandum of understanding
C. Regulatory compliance
D. Service level agreement
Answer: (SHOW ANSWER)

NEW QUESTION: 98
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:
Which of the following can the analyst conclude?
A. Malware is attempting to beacon to 128.50.100.3.
B. The system is scanning ajgidwle.com for PII.
C. The system is running a DoS attack against ajgidwle.com.
D. Data is being exfiltrated over DNS.
Answer: (SHOW ANSWER)

NEW QUESTION: 99
A general contractor has a list of contract documents containing critical business data that are stored at a public cloud provider. The organization's security analyst recently reviewed some of the storage containers and discovered most of the containers are not encrypted. Which of the following configurations will provide the MOST security to resolve the vulnerability?
A. Enabling SHA-256 hashing on the containers
B. Implementing AES-256 encryption on the containers
C. Implementing the Triple Data Encryption Algorithm at the file level
D. Upgrading TLS 1.2 connections to TLS 1.3
Answer: A (LEAVE A REPLY)

NEW QUESTION: 100
An organization has recently found some of its sensitive information posted to a social media site.
An investigation has identified large volumes of data leaving the network with the source traced back to host 192.168.1.13. An analyst performed a targeted Nmap scan of this host with the results shown below:
Subsequent investigation has allowed the organization to conclude that all of the well-known, standard ports are secure. Which of the following services is the problem?
A. mysql
B. winHelper
C. rpcbind

D. ssh
E. timbuktu-serv1
Answer: E (LEAVE A REPLY)

NEW QUESTION: 101
The Chief Information Officer (CIO) of a large healthcare institution is concerned about all machines having direct access to sensitive patient information. Which of the following should the security analyst implement to BEST mitigate the risk of sensitive data exposure?
A. Network segmentation
B. MFA on all workstations
C. A cloud access service broker system
D. NAC to ensure minimum standards are met
Answer: (SHOW ANSWER)

NEW QUESTION: 102
A company invested ten percent of its entire annual budget in security technologies. The Chief Information Officer (CIO) is convinced that, without this investment, the company will risk being the next victim of the same cyber attack its competitor experienced three months ago. However, despite this investment, users are sharing their usernames and passwords with their coworkers to get their jobs done. Which of the following will eliminate the risk introduced by this practice?
A. Invest in and implement a solution to ensure non-repudiation
B. Send an email asking users not to share their credentials
C. Run a report on all users sharing their credentials and alert their managers of further actions
D. Force a daily password change
Answer: B (LEAVE A REPLY)

NEW QUESTION: 103
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: 104
After completing a vulnerability scan, the following output was noted:
Which of the following vulnerabilities has been identified?
A. Web application cryptography vulnerability.
B. Active Directory encryption vulnerability.
C. VPN tunnel vulnerability.
D. PKI transfer vulnerability.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 105

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

NEW QUESTION: 106
An analyst is participating in the solution analysis process for a cloud-hosted SIEM platform to centralize log monitoring and alerting capabilities in the SOC.
Which of the following is the BEST approach for supply chain assessment when selecting a vendor?
A. Perform a proof of concept to identify possible solutions.
B. Gather information from providers, including datacenter specifications and copies of audit reports.
C. Consult with senior management for recommendations.
D. Identify SLA requirements for monitoring and logging.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 107
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. VDI
B. WAF
C. DLP
D. SSO
Answer: (SHOW ANSWER)

NEW QUESTION: 108
A security analyst is reviewing IDS logs and notices the following entry:
Which of the following attacks is occurring?
A. SQL injection
B. Cross-site scripting
C. Header manipulation
D. XML injection
Answer: (SHOW ANSWER)

NEW QUESTION: 109
You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.
The company's hardening guidelines indicate the following:
* TLS 1.2 is the only version of TLS running.
* Apache 2.4.18 or greater should be used.
* Only default ports should be used.
INSTRUCTIONS
Using the supplied data, record the status of compliance with the company's guidelines for each server.
The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for issues based ONLY on the hardening guidelines provided.

Answer:
See explanation below.
Explanation
Part 1 answer:
Check on the following:
AppServ1 is only using TLS.1.2
AppServ4 is only using TLS.1.2
AppServ1 is using Apache 2.4.18 or greater
AppServ3 is using Apache 2.4.18 or greater
AppServ4 is using Apache 2.4.18 or greater
Part 2 answer:
Recommendation:
Recommendation is to disable TLS v1.1 on AppServ2 and AppServ3. Also upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48

NEW QUESTION: 110
Organizational policies require vulnerability remediation on severity 7 or greater within one week.
Anything with a severity less than 7 must be remediated within 30 days. The organization also requires security teams to investigate the details of a vulnerability before performing any remediation. If the investigation determines the finding is a false positive, no remediation is performed and the vulnerability scanner configuration is updates to omit the false positive from future scans:
The organization has three Apache web servers:
The results of a recent vulnerability scan are shown below:
The team performs some investigation and finds a statement from Apache:
Which of the following actions should the security team perform?
A. Remediate 192.168.1.20 within 30 days
B. Ignore the false positive on 192.168.1.22
C. Investigate the false negative on 192.168.1.20
D. Remediate 192.168.1.22 within 30 days
Answer: D (LEAVE A REPLY)

NEW QUESTION: 111
A company has been a victim of multiple volumetric DoS attacks. Packet analysis of the offending traffic shows the following:
Which of the following mitigation techniques is MOST effective against the above attack?
A. The company should implement a network-based sinkhole to drop all traffic coming from 192.168.1.1 at their gateway router.
B. The company should contact the upstream ISP and ask that RFC1918 traffic be dropped.
C. The company should enable the DoS resource starvation protection feature of the gateway NIPS.
D. The company should implement the following ACL at their gateway firewall:DENY IP HOST 192.168.1.1 170.43.30.0/24.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 112
A security analyst's company uses RADIUS to support a remote sales staff of more than 700 people. The Chief Information Security Officer (CISO) asked to have IPSec using ESP and 3DES enabled to ensure the confidentiality of the communication as per RFC 3162. After the implementation was complete, many sales users reported latency issues and other performance issues when attempting to connect remotely. Which of the following is occurring?
A. The implementation should have used AES instead of 3DES.
B. The IPSec implementation has significantly increased the amount of bandwidth needed.
C. RFC 3162 is known to cause significant performance problems.
D. The device running RADIUS lacks sufficient RAM and processing power to handle ESP implementation.
Answer: (SHOW ANSWER)

NEW QUESTION: 113
Which of the following organizations would have to remediate embedded controller vulnerabilities?
A. Public universities
B. Regulatory agencies
C. Hydroelectric facilities
D. Banking institutions
Answer: C (LEAVE A REPLY)

NEW QUESTION: 114
A system administrator is doing network reconnaissance of a company's external network to determine the vulnerability of various services that are running. Sending some sample traffic to the external host, the administrator obtains the following packet capture:
Based on the output, which of the following services should be further tested for vulnerabilities?
A. HTTPS
B. HTTP
C. SSH
D. SMB
Answer: C (LEAVE A REPLY)

NEW QUESTION: 115
A cybersecurity analyst is reviewing log data and sees the output below:

Which of the following technologies MOST likely generated this log?
A. Host-based intrusion detection system
B. Network-based intrusion detection system
C. Stateful inspection firewall
D. Web application firewall
Answer: D (LEAVE A REPLY)

NEW QUESTION: 116
Which of the following is a feature of virtualization that can potentially create a single point of failure?
A. Faster server provisioning
B. Load balancing hypervisors
C. Running multiple OS instances
D. Server consolidation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117
After receiving reports latency, a security analyst performs an Nmap scan and observes the following output:
Which of the following suggests the system that produced output was compromised?
A. MySQL services is identified on a standard PostgreSQL port.
B. Standard HTP is open on the system and should be closed.
C. There are no indicators of compromise on this system.
D. Secure shell is operating of compromise on this system.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 118
A security analyst is auditing firewall rules with the goal of scanning some known ports to check the firewall's behavior and responses. The analyst executes the following commands.
Which of the following BEST describes the firewall rule?
A. REJECT with --tcp-reset
B. LOG -log-tcp-sequence
C. DNAt -to-destination 1.1.1.1:3000
D. DROP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 119
A security analyst is performing ongoing scanning and continuous monitoring of the corporate datacenter. Over time, these scans are repeatedly showing susceptibility to the same vulnerabilities and an increase in new vulnerabilities on a specific group of servers that are clustered to run the same application. Which of the following vulnerability management processes should be implemented?
A. Frequent server scanning
B. Group policy modification
C. Automated report generation

D. Regular patch application
Answer: D (LEAVE A REPLY)

NEW QUESTION: 120
An organization is performing vendor selection activities for penetration testing, and a security analyst is reviewing the MOA and rules of engagement, which were supplied with proposals.
Which of the following should the analyst expect will be included in the documents and why?
A. The scope of the penetration test should be included in the MOA to ensure penetration testing is conducted against only specifically authorized network resources.
B. The rules of engagement should include detailed results of the penetration scan, including all findings, as well as designation of whether vulnerabilities identified during the scanning phases are found to be exploitable during the penetration test.
C. The MOA should address the client SLA in relation to reporting results to regulatory authorities, including issuing banks for organizations that process cardholder data.
D. The exploitation standards should be addressed in the rules of engagement to ensure both parties are aware of the depth of exploitation that will be attempted by penetration testers.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 121
Review the following results:
Which of the following has occurred?
A. 172.29.0.109 is infected with a Trojan.
B. 123.120.110.212 is infected with a Trojan.
C. 172.29.0.109 is infected with a worm.
D. This is normal network traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 122
An organization has several systems that require specific logons Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?
A. Perform a manual privilege review
B. Adjust the current monitoring and logging rules
C. Use SSO across all applications
D. Implement multifactor authentication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 123

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. Work backward, restoring each backup until the server is clean
B. Stand up a new server and restore critical data from backups
C. Restore the previous backup and scan with a live boot anti-malware scanner
D. Offload the critical data to a new server and continue operations
Answer: B (LEAVE A REPLY)

NEW QUESTION: 124
A company requests a security assessment of its network. Permission is given, but no details are provided. It is discovered that the company has a web presence, and the company's IP address is 70.182.11.4. Which of the following Nmap commands would reveal common open ports and their versions?
A. nmap -vO
B. nmap - oV
C. nmap -sv
Answer: (SHOW ANSWER)

NEW QUESTION: 125
During an investigation, an incident responder intends to recover multiple pieces of digital media.
Before removing the media, the responder should initiate:
A. chain of custody forms.
B. decryption tools.
C. secure communications.
D. malware scans.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 126
A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost- paymonts.conf file.
The output of the diff command against the known-good backup reads as follows
Which of the following MOST likely occurred?
A. The file was altered to harvest credit card numbers
B. The file was altered to accept payments without charging the cards
C. The file was altered to verify the card numbers are valid.
D. The file was altered to avoid logging credit card information
Answer: D (LEAVE A REPLY)

NEW QUESTION: 127
Drag and Drop Question
You suspect that multiple unrelated security events have occurred on several nodes on a corporate network. You must review all logs and correlate events when necessary to discover each security event by clicking on each node. Only select corrective actions if the logs shown a security event that needs remediation. Drag and drop the appropriate corrective actions to mitigate the specific security event occurring on each affected device.
Instructions:

The Web Server, Database Server, IDS, Development PC, Accounting PC and Marketing PC are clickable. Some actions may not be required and each actions can only be used once per node.
The corrective action order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Answer:

NEW QUESTION: 128
A security team identified some specific known tactics and techniques to help mitigate repeated credential access threats, such as account manipulation and brute forcing. Which of the following frameworks or models did the security team MOST likely use to identify the tactics and techniques'?
A. MITRE ATT&CK
B. Diamond Model of Intrusion Analysis
C. ITIL
D. Kill chain
Answer: A (LEAVE A REPLY)

NEW QUESTION: 129
In order to leverage the power of data correlation within Nessus, a cybersecurity analyst needs to write an SQL statement that will provide how long a vulnerability has been present on the network.
Given the following output table:
Which of the following SQL statements would provide the resulted output needed for this correlation?
A. SELECT ScanDate, IP, Port, PlugIn FROM MyResults WHERE PluginID=`1000'
B. SELECT Port, ScanDate, IP, PlugIn FROM MyResults WHERE PluginID=`1000'
C. SELECT ScanDate, IP, Port, PlugIn SET MyResults WHERE PluginID=`1000'
D. SELECT IP, PORT, PlugIn, ScanDate FROM MyResults SET PluginID=`1000'
Answer: A (LEAVE A REPLY)

NEW QUESTION: 130
An analyst performs a routine scan of a host using Nmap and receives the following output:
Which of the following should the analyst investigate FIRST?
A. Port 80
B. Port 23
C. Port 22
D. Port 21
Answer: D (LEAVE A REPLY)

NEW QUESTION: 131
The Chief Information Security Officer (CISO) has asked the security analyst to examine abnormally high processor utilization on a key server. The output below is from the company's research and development (R&D) server.
Which of the following actions should the security analyst take FIRST?
A. Isolate the R&D server

B. Initiate an investigation
C. Reimage the server
D. Determine availability
Answer: (SHOW ANSWER)

NEW QUESTION: 132
As part of the SDLC, software developers are testing the security of a new web application by inputting large amounts of random data.
Which of the following types of testing is being performed?
A. Fuzzing
B. Input validation
C. Regression testing
D. Stress testing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133
A cybersecurity analyst is hired to review the security measures implemented within the domain controllers of a company. Upon review, the cybersecurity analyst notices a brute force attack can be launched against domain controllers that run on a Windows platform. The first remediation step implemented by the cybersecurity analyst is to make the account passwords more complex.
Which of the following is the NEXT remediation step the cybersecurity analyst needs to implement?
A. Disable the ability to store a LAN manager hash.
B. Move administrator accounts to a new security group.
C. Perform more frequent port scanning.
D. Install a different antivirus software.
E. Deploy a vulnerability scanner tool.
Answer: (SHOW ANSWER)

NEW QUESTION: 134
A cybersecurity analyst is conducting a security test to ensure that information regarding the web server is protected from disclosure.
The cybersecurity analyst requested an HTML file from the web server, and the response came back as follows:
Which of the following actions should be taken to remediate this security issue?
A. Set "Perprocesslogging" to 1 in the URLScan.ini configuration file.
B. Set "Removeserverheader" to 1 in the URLScan.ini configuration file.
C. Set "Enablelogging" to 0 in the URLScan.ini configuration file.
D. Set "Allowlatescanning" to 1 in the URLScan.ini configuration file.
Answer: (SHOW ANSWER)

NEW QUESTION: 135
A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost-paymonts
.conf file The output of the diff command against the known-good backup reads as follows
Which of the following MOST likely occurred?
A. The file was altered to harvest credit card numbers

B. The file was altered to avoid logging credit card information
C. The file was altered to accept payments without charging the cards
D. The file was altered to verify the card numbers are valid.
Answer: (SHOW ANSWER)

NEW QUESTION: 136
An analyst performs a routine scan of a host using Nmap and receives the following output:
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: 137
As part of a merger with another organization, a Chief Information Security Officer (CISO) is working with an assessor to perform a risk assessment focused on data privacy compliance. The CISO is primarily concerned with the potential legal liability and fines associated with data privacy. Based on the CISO's concerns, the assessor will MOST likely focus on:
A. qualitative magnitude.
B. quantitative magnitude.
C. quantitative probabilities.
D. qualitative probabilities.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 138
A security audit revealed that port 389 has been used instead of 636 when connecting to LDAP for the authentication of users.
The remediation recommended by the audit was to switch the port to 636 wherever technically possible.
Which of the following is the BEST response?
A. Change all devices and servers that support it to 636, as encrypted services run by default on
636.
B. Correct the audit. This finding is a well-known false positive; the services that typically run on 389 and 636 are identical.
C. Change all devices and servers that support it to 636, as 389 is a reserved port that requires root access and can expose the server to privilege escalation attacks.
D. Correct the audit. This finding is accurate, but the correct remediation is to update encryption keys on each of the servers to match port 636.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 139
A security analyst is reviewing the following requirements (or new time clocks that will be installed in a shipping warehouse:
* The clocks must be configured so they do not respond to ARP broadcasts.
* The server must be configured with static ARP entries for each clock.
Which of the following types of attacks will this configuration mitigate?
A. Rootkits
B. Overflows
C. Sniffing
D. Spoofing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140
A vulnerability scan has returned the following information:
Which of the following describes the meaning of these results?
A. Connecting to the host using a null session allows enumeration of share names.
B. Trend Micro has a known exploit that must be resolved or patched.
C. No CVE is present, so it is a false positive caused by Lotus running on a Windows server.
D. There is an unknown bug in a Lotus server with no Bugtraq ID.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 141
A new policy requires the security team to perform web application and OS vulnerability scans. All of the company's web applications use federated authentication and are accessible via a central portal. Which of the following should be implemented to ensure a more thorough scan of the company's web application, while at the same time reducing false positives?
A. The vulnerability scanner should be configured to perform authenticated scans.
B. The vulnerability scanner should scan for known and unknown vulnerabilities.
C. The vulnerability scanner should implement OS and network service detection.
D. The vulnerability scanner should be installed on the web server.
Answer: (SHOW ANSWER)

NEW QUESTION: 142
Three similar production servers underwent a vulnerability scan. The scan results revealed that the three servers had two different vulnerabilities rated "Critical". The administrator observed the following about the three servers:
- The servers are not accessible by the Internet
- AV programs indicate the servers have had malware as recently as two
weeks ago
- The SIEM shows unusual traffic in the last 20 days
- Integrity validation of system files indicates unauthorized
modifications
Which of the following assessments is valid and what is the most appropriate NEXT step? (Select TWO).
A. Activate the incident response plan

B. Servers may be generating false positives via the SIEM
C. Schedule recurring vulnerability scans on the servers
D. Immediately rebuild servers from known good configurations
E. Servers may have been built inconsistently
F. Servers may have been tampered with
Answer: A,F (LEAVE A REPLY)

NEW QUESTION: 143
The help desk provided a security analyst with a screenshot of a user's desktop:
For which of the following is aircrack-ng being used?
A. Brute-force attack
B. Wireless access point discovery
C. PCAP data collection
D. Rainbow attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 144
A cybersecurity analyst is reviewing the following outputs:
Which of the following can the analyst infer from the above output?
A. The remote host is redirecting port 80 to port 8080.
B. The remote host is running a service on port 8080.
C. The remote host's firewall is dropping packets for port 80.
D. The remote host is running a web server on port 80.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 145
The Chief Information Security Officer (CISO) asked for a topology discovery to be conducted and verified against the asset inventory. The discovery is failing and not providing reliable or complete data. The syslog shows the following information:
Which of the following describes the reason why the discovery is failing?
A. The server running LDAP has antivirus deployed.
B. The scanning tool lacks valid LDAP credentials.
C. The LDAP server is configured on the wrong port.
D. The scan is returning LDAP error code 52255a.
E. The connection to the LDAP server is timing out.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 146
After running a packet analyzer on the network, a security analyst has noticed the following output:
Which of the following is occurring?
A. A ping sweep
B. A service discovery

C. A port scan
D. A network map
Answer: C (LEAVE A REPLY)

NEW QUESTION: 147
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. proxy to block all connections to <malwaresource>.
B. IDS to match the malware sample.
C. email server that automatically deletes attached executables.
D. firewall to block connection attempts to dynamic DNS hosts.
Answer: (SHOW ANSWER)

NEW QUESTION: 148
An analyst needs to provide recommendations for the AUP Which of the following is the BEST recommendation to protect the company's intellectual property?
A. Company assets should never leave the company's property.
B. Company assets must be stored in a locked cabinet when not in use.
C. AII Internet access must be via a proxy server.
D. Company assets must not be utilized for personal use or gain.
Answer: (SHOW ANSWER)

NEW QUESTION: 149
A security operations team was alerted to abnormal DNS activity coming from a user's machine.
The team performed a forensic investigation and discovered a host had been compromised.
Malicious code was using DNS as a tunnel to extract data from the client machine, which had been leaked and transferred to an unsecure public Internet site. Which of the following BEST describes the attack?
A. Pharming
B. Phishing
C. Data exfiltration
D. Cache poisoning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 150
A security analyst is reviewing the following log from an email security service.
Which of the following BEST describes the reason why the email was blocked?
A. The IP address was blacklisted.
B. The email originated from the www.spamfilter.org URL.
C. The IP address and the remote server name are the same.
D. The To address is invalid.
E. The From address is invalid.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 151
Which of the following countermeasures should the security administrator apply to MOST effectively mitigate Bootkit-level infections of the organization's workstation devices?
A. Configure a BIOS-level password on the device.
B. Install a secondary virus protection application.
C. Enforce a system state recovery after each device reboot.
D. Remove local administrator privileges.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 152
A security analyst is reviewing the logs from an internal chat server. The chat.log file is too large to review manually, so the analyst wants to create a shorter log file that only includes lines associated with a user demonstrating anomalous activity. Below is a snippet of the log:
Which of the following commands would work BEST to achieve the desired result?
A. grep -i javashark chat.log
B. grep -i chatter14 chat.log
C. grep -v chatter14 chat.log
D. grep -v javashark chat.log
E. grep -i pythonfun chat.log
F. grep -v pythonfun chat.log
Answer: D (LEAVE A REPLY)

NEW QUESTION: 153
An organisation is assessing risks so it can prioritize its mitigation actions. Following are the risks and their probability and impact:
Which of the following is the order of priority for risk mitigation from highest to lowest?
A. A, D, B, C
B. A, B, C, D
C. D, A, C, B
D. C, B, D, A
E. B, C, A, D
Answer: (SHOW ANSWER)

NEW QUESTION: 154
An incident response report indicates a virus was introduced through a remote host that was connected to corporate resources.
A cybersecurity analyst has been asked for a recommendation to solve this issue.

Which of the following should be applied?
A. TAP
B. ACL
C. MAC
D. NAC
Answer: D (LEAVE A REPLY)

NEW QUESTION: 155
A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication.
Which of the following will remediate this software vulnerability?
A. Implement email filtering with anti-phishing protection.
B. Use a parameterized query to check the credentials.
C. Check for and enforce the proper domain for the redirect.
D. Deploy a WAF in front of the web application.
E. Enforce unique session IDs for the application.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 156
Which of the following attacks can be prevented by using output encoding?
A. Command injection
B. Cross-site scripting
C. Directory traversal
D. Cross-site request forgery
E. Server-side request forgery
F. SQL injection
Answer: (SHOW ANSWER)

NEW QUESTION: 157
While analyzing logs from a WAF, a cybersecurity analyst finds the following:
Which of the following BEST describes what the analyst has found?
A. This is an encrypted GET HTTP request
B. This is an encrypted packet
C. This is an encoded WAF bypass
D. A packet is being used to bypass the WAF
Answer: C (LEAVE A REPLY)

NEW QUESTION: 158
A company has a popular shopping cart website hosted geographically diverse locations. The company has started hosting static content on a content delivery network (CDN) to improve performance. The CDN provider has reported the company is occasionally sending attack traffic to other CDN-hosted targets.

Which of the following has MOST likely occurred?
A. The company has been breached, and customer PII is being exfiltrated to the CDN.
B. The CDN provider has mistakenly performed a GeoIP mapping to the company.
C. The CDN provider has misclassified the network traffic as hostile.
D. A vulnerability scan has tuned to exclude web assets hosted by the CDN.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 159
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. 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.
B. 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.
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. 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.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 160
A web-based front end for a business intelligence application uses pass-through authentication to authenticate users The application then uses a service account, to perform queries and look up data m a database A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?
A. Configure database security logging using syslog or a SIEM
B. Enforce unique session IDs so users do not get a reused session ID
C. Change the security model to force the users to access the database as themselves
D. Parameterize queries to prevent unauthorized SQL queries against the database
Answer: D (LEAVE A REPLY)

NEW QUESTION: 161
A Chief Information Security Officer (CISO) wants to standardize the company's security program so it can be objectively assessed as part of an upcoming audit requested by management. Which of the following would holistically assist in this effort?
A. AUP
B. Nessus
C. Scrum
D. NIST
E. ITIL
Answer: D (LEAVE A REPLY)

NEW QUESTION: 162
Which of the following is the use of tools to simulate the ability for an attacker to gain access to a specified network?

A. Reverse engineering
B. Fuzzing
C. Penetration testing
D. Network mapping
Answer: C (LEAVE A REPLY)

NEW QUESTION: 163
The development team currently consists of three developers who each specialize in a specific programming language:
Developer 1 - C++/C#
Developer 2 - Python
Developer 3 - Assembly
Which of the following SDLC best practices would be challenging to implement with the current available staff?
A. Stress testing
B. Peer review
C. Regression testing
D. Fuzzing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 164
A security analyst needs to reduce the overall attack surface.
Which of the following infrastructure changes should the analyst recommend?
A. Implement a honeypot.
B. Air gap sensitive systems.
C. Increase the network segmentation.
D. Implement a cloud-based architecture.
Answer: C (LEAVE A REPLY)
Explanation
Explanation/Reference: https://www.securitymagazine.com/articles/89283-ways-to-reduce-your-attack-surface

NEW QUESTION: 165
Which of the following types of policies is used to regulate data storage on the network?
A. Password
B. Acceptable use
C. Account management
D. Retention
Answer: D (LEAVE A REPLY)
Explanation/Reference: http://www.css.edu/administration/information-technologies/computing-policies/computer-and- network-policies.html

NEW QUESTION: 166

A contained section of a building is unable to connect to the Internet A security analyst. A security analyst investigates me issue but does not see any connections to the corporate web proxy However the analyst does notice a small spike in traffic to the Internet. The help desk technician verifies all users are connected to the connect SSID. but there are two of the same SSIDs listed in the network connections. Which of the following BEST describes what is occurring?

A. Denial of service

B. Beaconing

C. Rogue device on the network

D. Bandwidth consumption

Answer: D (LEAVE A REPLY)

NEW QUESTION: 167

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

Which of the following commands should the administrator run NEXT to further analyze the compromised system?

A. /bin/la -1 /proc/1301/exe

B. kill -9 1301

C. rpm -V openash-server

D. strace /proc/1301

Answer: (SHOW ANSWER)

NEW QUESTION: 168

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

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

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

C. Initiate chain-of-custody documentation.

D. Perform a physical hard disk image.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 169

Which of the following principles describes how a security analyst should communicate during an incident?

A. The communication should come from law enforcement.

B. The communication should be limited to trusted parties only.

C. The communication should be limited to management only.

D. The communication should be limited to security staff only.

Answer: (SHOW ANSWER)

NEW QUESTION: 170

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

NEW QUESTION: 171
A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party in1marketingpartners.com Below is the exiting SPP word:
Which of the following updates to the SPF record will work BEST to prevent the emails from being marked as spam or blocked?
A)
B)
C)
D)
A. Option A
B. Option C
C. Option D
D. Option B
Answer: D (LEAVE A REPLY)

NEW QUESTION: 172
A developer wrote a script to make names and other PII data unidentifiable before loading a database export into the testing system Which of the following describes the type of control that is being used?
A. Data loss prevention
B. Data masking
C. Data encoding
D. Data classification
Answer: A (LEAVE A REPLY)

NEW QUESTION: 173
A company has monthly scheduled windows for patching servers and applying configuration changes. Out- of-window changes can be done, but they are discouraged unless absolutely necessary. The systems administrator is reviewing the weekly vulnerability scan report that was just released. Which of the following vulnerabilities should the administrator fix without waiting for the next scheduled change window?
A. The administrator should fix http (80/tcp). The `greeting.cgi' script is installed. This CGI has a well- known security flaw that lets anyone execute arbitrary commands with the privileges of the
http daemon.
B. The administrator should fix http (80/tcp). An information leak occurs on Apache web servers with the UserDir module enabled, allowing an attacker to enumerate accounts by requesting access to home directories and monitoring the response.

C. The administrator should fix general/tcp. The remote host does not discard TCP SYN packets that have the FIN flag set. Depending on the kind of firewall a company is using, an attacker may use this flaw to bypass its rules.
D. The administrator should fix smtp (25/tcp). The remote SMTP server is insufficiently protected against relaying. This means spammers might be able to use the company's mail server to send their emails to the world.
E. The administrator should fix dns (53/tcp). BIND `NAMED' is an open-source DNS server from ISC.org. The BIND-based NAMED server (or DNS servers) allow remote users to query for version and type information.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 174
A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage The security analyst is trying to determine which user caused the malware to get onto the system Which of the following registry keys would MOST likely have this information?
A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
B. HKEY_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2
C. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub
D. HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run
E. HKEY_USERS\<user SID>\Software\Microsoft\Internet Explorer\Typed URLs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 175
Review the following results:
Which of the following has occurred?
A. 123.120.110.212 is infected with a Trojan.
B. 172.29.0.109 is infected with a worm.
C. 172.29.0.109 is infected with a Trojan.
D. This is normal network traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 176
An organization has a practice of running some administrative services on non-standard ports as a way of frustrating any attempts at reconnaissance. The output of the latest scan on host
192.168.1.13 is shown below:
Which of the following statements is true?
A. The use of OpenSSH on its default secure port will supersede any other remote connection attempts.
B. Despite the results of the scan, the service running on port 23 is actually Telnet and not SSH, and creates an additional vulnerability
C. Running SSH on port 23 provides little additional security from running it on the standard port.
D. Remote SSH connections will automatically default to the standard SSH port.
E. Running SSH on the Telnet port will now be sent across an unencrypted port.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 177

A security analyst is reviewing the following log entries to identify anomalous activity:
Which of the following attack types is occurring?
A. Cross-site scripting
B. SQL injection
C. Directory traversal
D. Buffer overflow
Answer: (SHOW ANSWER)

NEW QUESTION: 178
A network attack that is exploiting a vulnerability in the SNMP is detected.
Which of the following should the cybersecurity analyst do FIRST?
A. Apply the required patches to remediate the vulnerability.
B. Escalate the incident to senior management for guidance.
C. Disable all privileged user accounts on the network.
D. Temporarily block the attacking IP address.
Answer: (SHOW ANSWER)
Reference:
https://beyondsecurity.com/scan-pentest-network-vulnerabilities-snmp-protocol-version- detection.html

NEW QUESTION: 179
An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security analyst is reviewing vulnerability scan results from a recent web server scan.
Portions of the scan results are shown below:
Which of the following lines indicates information disclosure about the host that needs to be remediated?
A. Finding#5144322
B. Response: :\Documents\MarySmith\mailingList.pdf
C. Request: GET http://myOrg.com/mailingList.aspx?content=volunteer
D. First Time Detected 10 Nov 2015 09:00 GMT-0600
E. Access Path: http://myOrg.com/mailingList.htm
Answer: B (LEAVE A REPLY)

NEW QUESTION: 180
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. false negatives
B. verification of mitigation
C. the criticality index
D. false positives
E. hardening validation.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 181
A pharmaceutical company's marketing team wants to send out notifications about new products to alert users of recalls and newly discovered adverse drug reactions.
The team plans to use the names and mailing addresses that users have provided.
Which of the following data privacy standards does this violate?
A. Purpose limitation
B. Data minimization
C. Retention
D. Sovereignty
Answer: A (LEAVE A REPLY)

NEW QUESTION: 182
Because some clients have reported unauthorized activity on their accounts, a security analyst is reviewing network packet captures from the company's API server. A portion of a capture file is shown below:
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.s/soap/envelope/
"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/XMLSchema-instance
"></s:Body></s:Envelope> 192.168.1.22 - - api.somesite.com 200 0 1006 1001 0 192.168.1.22 POST /services/v1_0/Public/Members.svc/soap
<<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/><a:Username>somebody@companyname.com
192.168.5.66 - - api.somesite.com 200 0 11558 1712 2024 192.168.4.89
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.xmlsoap.org/soap
/envelope/"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation></s:Body><
192.168.1.22 - - api.somesite.com 200 0 1003 1011 307 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/ http://tempuri.org/">
<request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="
http://www.w3.org/2001/XMLSch
<a:ApiToken>kmL4krg2CwwWBan5BReGv5Djb7syxXTNKcWFuSjd</a:ApiToken><a:ImpersonateUserId>0<
<a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId>13026046</a:UserId></a:Authe
192.168.5.66 - - api.somesite.com 200 0 1378 1209 48 192.168.4.89
Which of the following MOST likely explains how the clients' accounts were compromised?
A. The clients' usernames and passwords were transmitted in cleartext.
B. The clients' authentication tokens were impersonated and replayed.

C. A SQL injection attack was carried out on the server.
D. An XSS scripting attack was carried out on the server.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 183
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. federated authentication
B. manual account reviews
C. role-based access control.
D. multifactor authentication.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 184
A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party in1marketingpartners.com Below is the exiting SPP word:
Which of the following updates to the SPF record will work BEST to prevent the emails from being marked as spam or blocked?
A)
B)
C)
D)
A. Option D
B. Option A
C. Option C
D. Option B
Answer: D (LEAVE A REPLY)

NEW QUESTION: 185
Which of the following is a control that allows a mobile application to access and manipulate information which should only be available by another application on the same mobile device (e.g. a music application posting the name of the current song playing on the device on a social media site)?
A. Co-hosted application
B. Dual authentication
C. Mutually exclusive access
D. Transitive trust
Answer: (SHOW ANSWER)

NEW QUESTION: 186
A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:
Which of the following is MOST likely a false positive?
A. Anonymous FTP enabled

B. Unsupported web server detection
C. Windows SMB service enumeration via \srvsvc
D. ICMP timestamp request remote date disclosure
Answer: (SHOW ANSWER)

NEW QUESTION: 187
A security analyst has been asked to scan a subnet. During the scan, the following output was generated:
Based on the output above, which of the following is MOST likely?
A. 192.168.100.214 is a web server
B. Both hosts are mail servers
C. 192.168.100.145 is a DNS server
D. 192.168.100.214 is a secure FTP server
Answer: A (LEAVE A REPLY)

NEW QUESTION: 188
An organization is experiencing issues with emails that are being sent to external recipients Incoming emails to the organization are working fine. A security analyst receives the following screenshot ot email error from the help desk.
The analyst the checks the email server and sees many of the following messages in the logs.
Error 550 - Message rejected
Which of the following is MOST likely the issue?
A. The DKIM private key has expired
B. SPF is failing.
C. The DMARC queue is full
D. Port 25 is not open.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 189
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. role-based access control.
B. multifactor authentication.
C. federated authentication
D. manual account reviews
Answer: (SHOW ANSWER)

NEW QUESTION: 190
During a recent audit, there were a lot of findings similar to and including the following:
Which of the following would be the BEST way to remediate these findings and minimize similar findings in the future?
A. Run Microsoft Baseline Security Analyzer on all of the servers.
B. Schedule regular vulnerability scans for all servers on the network.
C. Remove the affected software programs from the servers.

D. Use an automated patch management solution.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 191
An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation platform.
Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?
A. FaaS
B. RTOS
C. SoC
D. GPS
E. CAN bus
Answer: B (LEAVE A REPLY)
Explanation
IoT devices also often run real-time operating systems (RTOS). These are either special purpose operating systems or variants of standard operating systems designed to process data rapidly as it arrives from sensors or other IoT components.

NEW QUESTION: 192
The Chief Executive Officer (CEO) instructed the new Chief Information Security Officer (CISO) to provide a list of enhancement to the company's cybersecurity operation. As a result, the CISO has identified the need to align security operations with industry best practices. Which of the following industry references is appropriate to accomplish this?
A. OSSIM
B. NIST
C. PCI
D. OWASP
Answer: (SHOW ANSWER)
https://www.nist.gov/sites/default/files/documents/itl/Cybersecurity_Green- Paper_FinalVersion.pdf

NEW QUESTION: 193
During an investigation, an incident responder intends to recover multiple pieces of digital media. Before removing the media, the responder should initiate:
A. secure communications.
B. malware scans.
C. chain of custody forms.
D. decryption tools.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 194
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. Create classification criteria for data residing on different servers and provide remediation only for servers housing sensitive data.
B. Create an SLA stating that remediation actions must occur within 30 days of discovery for all levels of vulnerabilities.

C. Incorporate prioritization levels into the remediation process and address critical findings first.
D. 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.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 195
A security analyst is reviewing packet captures for a specific server that is suspected of containing malware and discovers the following packets:
Which of the following traffic patterns or data would be MOST concerning to the security analyst?
A. Anonymous access granted by 103.34.243.12
B. Unencrypted password sent from 103.34.243.12
C. Ports used for HTTP traffic from 202.53.245.78
D. Port used for SMTP traffic from 73.252.34.101
Answer: A (LEAVE A REPLY)

NEW QUESTION: 196
An analyst is reviewing the following code output of a vulnerability scan:
Which of the following types of vulnerabilities does this MOST likely represent?
A. An HTTP response split vulnerability
B. A XSS vulnerability
C. A credential bypass vulnerability
D. A insecure direct object reference vulnerability
Answer: (SHOW ANSWER)

NEW QUESTION: 197
A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:
A. which systems were exploited more frequently.
B. detection and prevention capabilities to improve.
C. which analysts require more training.
D. the time spent by analysts on each of the incidents.
E. possible evidence that is missing during forensic analysis.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 198
An analyst is observing unusual network traffic from a workstation. The workstation is communicating with a known malicious site over an encrypted tunnel.
A full antivirus scan with an updated antivirus signature file does not show any sign of infection.
Which of the following has occurred on the workstation?

A. Zero-day attack
B. Session hijack
C. Known malware attack
D. Cookie stealing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 199
While reviewing log files, a security analyst uncovers a brute-force attack that is being performed against an external webmail portal. Which of the following would be BEST to prevent this type of attack from beinq successful1?
A. Leverage password filters to prevent weak passwords on employee accounts from being exploited.
B. Implement MFA on the email portal using out-of-band code delivery.
C. Alter the lockout policy to ensure users are permanently locked out after five attempts.
D. Configure a WAF with brute force protection rules in block mode
E. Create a new rule in the IDS that triggers an alert on repeated login attempts
Answer: (SHOW ANSWER)

NEW QUESTION: 200
A security analyst is reviewing the following web server log:
Which of the following BEST describes the issue?
A. SQL injection
B. Cross-site request forgery
C. Directory traversal exploit
D. Cross-site scripting
Answer: C (LEAVE A REPLY)

NEW QUESTION: 201
After scanning the main company's website with the OWASP ZAP tool, a cybersecurity analyst is reviewing the following warning:
The analyst reviews a snippet of the offending code:
Which of the following is the BEST course of action based on the above warning and code snippet?
A. The developer should review the code and implement a code fix.
B. The system administrator should disable SSL and implement TLS.
C. The analyst should implement a scanner exception for the false positive.
D. The organization should update the browser GPO to resolve the issue.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 202
Hotspot Question
Malware is suspected on a server in the environment. The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware. Servers 1, 2 and 4 are clickable. Select the Server which hosts the malware, and select the process which hosts this malware.
Instructions:

If any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Answer:

NEW QUESTION: 203
A security analyst has been asked to remediate a server vulnerability.
Once the analyst has located a patch for the vulnerability, which of the following should happen NEXT?
A. Rescan to ensure the vulnerability still exists.
B. Begin the incident response process.
C. Start the change control process.
D. Implement continuous monitoring.
Answer: (SHOW ANSWER)

NEW QUESTION: 204
A security analyst working in the SOC recently discovered Balances m which hosts visited a specific set of domains and IPs and became infected with malware. Which of the following is the MOST appropriate action to take in the situation?
A. implement an IPS signature for the malware and update the blacklisting for the associated domains and IPs
B. Implement a change request to the firewall setting to not allow traffic to and from the IPs and domains
C. Implement an IPS signature for the malware and a change request to the firewall setting to not allow traffic to and from the IPs and domains
D. Implement an IPS signature for the malware and another signature request to Nock all the associated domains and IPs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 205
A red team actor observes it is common practice to allow cell phones to charge on company computers, but access to the memory storage is blocked. Which of the following are common attack techniques that take advantage of this practice? (Choose two.)
A. A USB attack that tricks the system into thinking it is a network adapter, then runs a user password hash gathering utility for offline password cracking
B. A Bluetooth attack that modifies the device registry (Windows PCs only) to allow the flash drive to mount, and then launches a Java applet attack
C. A USB attack that turns the connected device into a rogue access point that spoofs the configured wireless SSIDs
D. A USB attack that tricks the computer into thinking the connected device is a keyboard, and then sends characters one at a time as a keyboard to launch the attack (a prerecorded series of keystrokes)
E. A Bluetooth peering attack called "Snarfing" that allows Bluetooth connections on blocked device types if physically connected to a USB port
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 206
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 werbserverlist,text. Which of the fallowing Nmap commands would BEST accomplish this goal?
A)
B)
C)

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

NEW QUESTION: 207
After receiving reports latency, a security analyst performs an Nmap scan and observes the following output:
Which of the following suggests the system that produced output was compromised?
A. MySQL services is identified on a standard PostgreSQL port.
B. Secure shell is operating of compromise on this system.
C. There are no indicators of compromise on this system.
D. Standard HTP is open on the system and should be closed.
Answer: (SHOW ANSWER)

NEW QUESTION: 208
The human resources division is moving all of its applications to an IaaS cloud. The Chief Information Officer (CIO) has asked the security architect to design the environment securely to prevent the IaaS provider from accessing its data-at-rest and data-in-transit within the infrastructure. Which of the following security controls should the security architect recommend?
A. Implement a non-data breach agreement
B. Ensure all backups are remote outside the control of the IaaS provider
C. Ensure all of the IaaS provider's workforce passes stringent background checks
D. Render data unreadable through the use of appropriate tools and techniques
Answer: D (LEAVE A REPLY)

NEW QUESTION: 209
Datacenter access is controlled with proximity badges that record all entries and exits from the datacenter.
The access records are used to identify which staff members accessed the data center in the event of equipment theft.
Which of the following MUST be prevented in order for this policy to be effective?
A. Social engineering
B. Phishing
C. Tailgating
D. Password reuse
Answer: C (LEAVE A REPLY)

NEW QUESTION: 210
A security analyst scanned an internal company subnet and discovered a host with the following Nmap output.
Based on the output of this Nmap scan, which of the following should the analyst investigate FIRST?
A. Port 22
B. Port 445

C. Port 3389
D. Port 135
Answer: D (LEAVE A REPLY)

NEW QUESTION: 211
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:
Which of the following should be the focus of the investigation?
A. webserver.org-dmz.org
B. sftp.org-dmz.org
C. 83hht23.org-int.org
D. ftps.bluemed.net
Answer: (SHOW ANSWER)

NEW QUESTION: 212
While analyzing logs from a WAF, a cybersecurity analyst finds the following:
"GET /form.php?id=463225%2b%2575%256e%2569%256f%256e%2b%2573%2574%
2box3133333731,1223,1224&name=&state=IL"
Which of the following BEST describes what the analyst has found?
A. This is an encoded WAF bypass
B. A packet is being used to bypass the WAF
C. This is an encrypted GET HTTP request
D. This is an encrypted packet
Answer: (SHOW ANSWER)

NEW QUESTION: 213
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. Information sharing and analysis
B. Static and dynamic analysis
C. Automation and orchestration
D. Continuous integration and deployment
Answer: (SHOW ANSWER)

NEW QUESTION: 214

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

NEW QUESTION: 215
An organization has recently found some of its sensitive information posted to a social media site.
An investigation has identified large volumes of data leaving the network with the source traced back to host 192.168.1.13. An analyst performed a targeted Nmap scan of this host with the results shown below:
Subsequent investigation has allowed the organization to conclude that all of the well-known, standard ports are secure. Which of the following services is the problem?
A. winHelper
B. ssh
C. mysql
D. rpcbind
E. timbuktu-serv1
Answer: (SHOW ANSWER)

NEW QUESTION: 216
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. Minutes from meetings in which risk assessment activities addressing the servers were discussed
C. Copies of change orders relating to the vulnerable servers
D. Copies of prior audits that did not identify the servers as an issue
E. ACLs from perimeter firewalls showing blocked access to the servers
Answer: (SHOW ANSWER)

NEW QUESTION: 217
A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication.
Which of the following will remediate this software vulnerability?
A. Enforce unique session IDs for the application.
B. Use a parameterized query to check the credentials.
C. Deploy a WAF in front of the web application.
D. Check for and enforce the proper domain for the redirect.

E. Implement email filtering with anti-phishing protection.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 218
A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs.
Which of the following is the main concern a security analyst should have with this arrangement?
A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.
B. Moving the FPGAs between development sites will lessen the time that is available for security testing.
C. Development phases occurring at multiple sites may produce change management issues.
D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 219
A system administrator who was using an account with elevated privileges deleted a large amount of log files generated by a virtual hypervisor in order to free up disk space.
These log files are needed by the security team to analyze the health of the virtual machines.
Which of the following compensating controls would help prevent this from reoccurring? (Select two.)
A. Succession planning
B. Mandatory vacation
C. Job rotation
D. Personnel training
E. Separation of duties
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 220
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. Blacklist the new subnet
C. Apply network access control.
D. Block the domain IP at the firewall.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 221
An organization suspects it has had a breach, and it is trying to determine the potential impact.
The organization knows the following:
- The source of the breach is linked to an IP located in a foreign
country.
- The breach is isolated to the research and development servers.

- The hash values of the data before and after the breach are
unchanged.
- The affected servers were regularly patched, and a recent scan showed no vulnerabilities.
Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)
A. The threat is an APT.
B. The integrity of the data is unaffected.
C. The source IP of the threat has been spoofed.
D. The confidentiality of the data is unaffected.
E. The threat is an insider.
Answer: (SHOW ANSWER)

NEW QUESTION: 222
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. Network and host scanning
D. Social media profiling and phishing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 223
Which of the following software security best practices would prevent an attacker from being able to run arbitrary SQL commands within a web application? (Choose two.)
A. Parameterized queries
B. Session management
C. Input validation
D. Output encoding
E. Data protection
F. Authentication
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/

NEW QUESTION: 224
When reviewing the system logs, the cybersecurity analyst noticed a suspicious log entry:
wmic /node: HRDepartment1 computersystem get username
Which of the following combinations describes what occurred, and what action should be taken in this situation?
A. A rogue user has queried for the administrator logged into the system. Attempt to determine who executed the command.
B. A rogue user has queried for users logged in remotely. Disable local access to network shares.
C. A rogue user has queried for users logged into in remotely. Attempt to determine who executed the command.
D. A rogue user has queried for the administrator logged into the system. Disable local access to use cmd prompt.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 225
A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:
Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?
A. Server2
B. Server1
C. Firewall
D. PC1
E. PC2
Answer: C (LEAVE A REPLY)

NEW QUESTION: 226
A small marketing firm uses many SaaS applications that hold sensitive information The firm has discovered terminated employees are retaining access to systems for many weeks after their end date. Which of the following would BEST resolve the issue of lingering access?
A. Perform weekly manual reviews on system access to uncover any issues.
B. Configure federated authentication with SSO on cloud provider systems.
C. Set up a privileged access management tool that can fully manage privileged account access.
D. Implement MFA on cloud-based systems.
Answer: (SHOW ANSWER)

NEW QUESTION: 227
A company's Chief Information Security Officer (CISO) published an Internet usage policy that prohibits employees from accessing unauthorized websites. The IT department whitelisted websites used for business needs. The CISO wants the security analyst to recommend a solution that would improve security and support employee morale. Which of the following security recommendations would allow employees to browse non-business-related websites?
A. Develop a new secured browser.
B. Install kiosks throughout the building.
C. Configure a personal business VLAN.
D. Implement a virtual machine alternative.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 228
Given the following output from a Linux machine:
file2cable *i eth0 -f file.pcap
Which of the following BEST describes what a security analyst is trying to accomplish?

A. The analyst is attempting to replay captured data from a PCAP file.
B. The analyst is attempting to capture traffic on interface eth0.
C. The analyst is attempting to use a protocol analyzer to monitor network traffic.
D. The analyst is attempting to capture traffic for a PCAP file.
E. The analyst is attempting to measure bandwidth utilization on interface eth0.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 229
A recent audit has uncovered several coding errors and a lack of input validation being used on a public portal. Due to the nature of the portal and the severity of the errors, the portal is unable to be patched. Which of the following tools could be used to reduce the risk of being compromised?
A. Network firewall
B. Web application firewall
C. Web proxy
D. Intrusion prevention system
Answer: B (LEAVE A REPLY)

NEW QUESTION: 230
There have been several exploits to critical devices within the network. However, there is currently no process to perform vulnerability analysis.
Which of the following should the security analyst implement during production hours to identify critical threats and vulnerabilities?
A. Vulnerability scanning frequency that does not interrupt workflow
B. Asset inventory of all critical devices
C. Scanning of all types of data regardless of sensitivity levels
D. Daily automated reports of exploited devices
Answer: A (LEAVE A REPLY)

NEW QUESTION: 231
Hotspot Question
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue.
INSTRUCTIONS
Click on me ticket to see the ticket details Additional content is available on tabs within the ticket First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Answer:

NEW QUESTION: 232
What organization manages the global IP address space?
A. WorldNIC
B. ARIN
C. NASA
D. IANA
Answer: D (LEAVE A REPLY)

NEW QUESTION: 233
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. A SQL injection attack was carried out on the server.
B. The clients' authentication tokens were impersonated and replayed.
C. An XSS scripting attack was carried out on the server.
D. The clients' usernames and passwords were transmitted in cleartext.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 234
A from the production environment to the test environment to test accuracy and functionality.
Which of the following would BEST protect the sensitivity of this data while still allowing the team to perform the testing?
A. Encryption
B. Watermarking
C. Encoding
D. Deidentification
Answer: (SHOW ANSWER)

NEW QUESTION: 235
A company wants to establish a threat-hunting team. Which of the following BEST describes the rationale for integration intelligence into hunt operations?
A. It supports rapid response and recovery during and followed an incident.
B. It provide critically analyses for key enterprise servers and services.
C. It enables the team to prioritize the focus area and tactics within the company's environment.
D. It allow analysis to receive updates on newly discovered software vulnerabilities.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 236

A malware infection spread to numerous workstations within the marketing department. The workstations were quarantined and replaced with machines. Which of the following represents a FINAL step in the eradication of the malware?
A. The workstations should be donated for reuse.
B. The workstations should be patched and scanned.
C. The workstations should be isolated from the network.
D. The workstations should be reimaged.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 237
A penetration tester is preparing for an audit of critical systems that may impact the security of the environment. This includes the external perimeter and the internal perimeter of the environment.
During which of the following processes is this type of information normally gathered?
A. Scoping
B. Enumeration
C. Authorization
D. Timing
Answer: (SHOW ANSWER)

NEW QUESTION: 238
An analyst needs to provide a recommendation that will allow a custom-developed application to have full access to the system's processors and peripherals but still be contained securely from other applications that will be developed. Which of the following is the BEST technology for the analyst to recommend?
A. Hardware security module
B. Software-based drive encryption
C. Unified Extensible Firmware Interface
D. Trusted execution environment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 239
A security professional is analyzing the results of a network utilization report. The report includes the following information:
Which of the following servers needs further investigation?
A. mrktg.file.srvr.02
B. hr.dbprod.01
C. R&D.file.srvr.01
D. web.srvr.03
Answer: (SHOW ANSWER)

NEW QUESTION: 240
A cybersecurity analyst is contributing to a team hunt on an organization's endpoints.
Which of the following should the analyst do FIRST?
A. Write detection logic.
B. Profile the threat actors and activities.

C. Establish a hypothesis.
D. Perform a process analysis.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 241
During a physical penetration test at a client site, a local law enforcement officer stumbled upon the test questioned the legitimacy of the team.
Which of the following information should be shown to the officer?
A. Timing information
B. Letter of engagement
C. Scope of work
D. Team reporting
Answer: B (LEAVE A REPLY)

NEW QUESTION: 242
A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost-paymonts
.conf file The output of the diff command against the known-good backup reads as follows
Which of the following MOST likely occurred?
A. The file was altered to verify the card numbers are valid.
B. The file was altered to avoid logging credit card information
C. The file was altered to accept payments without charging the cards
D. The file was altered to harvest credit card numbers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 243
A security analyst at a technology solutions firm has uncovered the same vulnerabilities on a vulnerability scan for a long period of time. The vulnerabilities are on systems that are dedicated to the firm's largest client. Which of the following is MOST likely inhibiting the remediation efforts?
A. There is a potential disruption of the vendor-client relationship
B. There is an SLA with the client that allows very little downtime
C. Patches for the vulnerabilities have not been fully tested by the software vendor
D. The parties have an MOU between them that could prevent shutting down the systems
Answer: (SHOW ANSWER)

NEW QUESTION: 244
A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:
The analyst runs the following command next:

Which of the following would explain the difference in results?
A. ICMP is being blocked by a firewall.
B. The original ping command needed root permission to execute.
C. The routing tables for ping and hping3 were different.
D. hping3 is returning a false positive.
Answer: (SHOW ANSWER)

NEW QUESTION: 245
The Chief Information Security Officer (CISO) has asked the security analyst to examine abnormally high processor utilization on a key server. The output below is from the company's research and development (R&D) server.
Which of the following actions should the security analyst take FIRST?
A. Determine availability
B. Initiate an investigation
C. Reimage the server
D. Isolate the R&D server
Answer: (SHOW ANSWER)

NEW QUESTION: 246
Which of the following secure coding techniques can be used to prevent cross-site request forgery attacks?
A. Parameterized queries
B. Input validation
C. Tokenization
D. Output encoding
Answer: (SHOW ANSWER)

NEW QUESTION: 247
An analyst received a forensically sound copy of an employee's hard drive. The employee's manager suspects inappropriate images may have been deleted from the hard drive. Which of the following could help the analyst recover the deleted evidence?
A. File timestamps
B. File carving tool
C. File hashing utility
D. File analysis tool
Answer: B (LEAVE A REPLY)

NEW QUESTION: 248
A security administrator determines several months after the first instance that a local privileged user has been routinely logging into a server interactively as "root" and browsing the Internet. The administrator determines this by performing an annual review of the security logs on that server.
For which of the following security architecture areas should the administrator recommend review and modification? (Select TWO).
A. Network isolation and separation
B. Log aggregation and analysis
C. Software assurance

D. Encryption
E. Acceptable use policies
F. Password complexity
Answer: (SHOW ANSWER)

NEW QUESTION: 249
A security analyst is reviewing logs and discovers that a company-owned computer issued to an employee is generating many alerts and warnings. The analyst continues to review the log events and discovers that a non-company-owned device from a different, unknown IP address is generating the same events. The analyst informs the manager of these findings, and the manager explains that these activities are already known and part of an ongoing events. Given this scenario, which of the following roles are the analyst, the employee, and the manager filling?
A. The analyst is red team.
The employee is blue team.
The manager is white team.
B. The analyst is white team.
The employee is red team.
The manager is blue team.
C. The analyst is red team.
The employee is white team.
The manager is blue team.
D. The analyst is blue team.
The employee is red team.
The manager is white team.
Answer: D (LEAVE A REPLY)
https://danielmiessler.com/study/red-blue-purple-teams/

NEW QUESTION: 250
A security analyst is attempting to utilize the blowing threat intelligence for developing detection capabilities:
In which of the following phases is this APT MOST likely to leave discoverable artifacts?
A. Reconnaissance
B. Data collection/exfiltration
C. Defensive evasion
D. Lateral movement
Answer: B (LEAVE A REPLY)

NEW QUESTION: 251
During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect.
Which of the following is the BEST place to acquire evidence to perform data carving?
A. The system memory
B. The hard drive
C. Network packets
D. The Windows Registry

Answer: A (LEAVE A REPLY)
Explanation/Reference: https://resources.infosecinstitute.com/memory-forensics/#gref
https://www.computerhope.com/jargon/d/data-carving.htm

NEW QUESTION: 252
A security manager has asked an analyst to provide feedback on the results of a penetration test.
After reviewing the results, the manager requests information regarding the possible exploitation of vulnerabilities. Which of the following information data points would be MOST useful for the analyst to provide to the security manager, who would then communicate the risk factors to senior management? (Choose two.)
A. Indicators of compromise
B. Classification
C. Adversary capability
D. Probability
E. Impact
F. Attack vector
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 253
Which of the following types of policies is used to regulate data storage on the network?
A. Password
B. Acceptable use
C. Account management
D. Retention
Answer: (SHOW ANSWER)
Reference:
http://www.css.edu/administration/information-technologies/computing-policies/computer-and- network-policies.html

NEW QUESTION: 254
A company's computer was recently infected with ransomware. After encrypting all documents, the malware logs a random AES-128 encryption key and associated unique identifier onto a compromised remote website. A ransomware code snippet is shown below:
Based on the information from the code snippet, which of the following is the BEST way for a cybersecurity professional to monitor for the same malware in the future?
A. Write an ACL to block the IP address of www.malwaresite.com at the gateway firewall.
B. Reconfigure the enterprise antivirus to push more frequent to the clients.
C. Configure the company proxy server to deny connections to www.malwaresite.com.
D. Use an IDS custom signature to create an alert for connections to www.malwaresite.com.
Answer: (SHOW ANSWER)

NEW QUESTION: 255
During a recent breach, an attacker was able to use tcpdump on a compromised Linux server to capture the password of a network administrator that logged into a switch using telnet. Which of the following compensating controls could be implemented to address this going forward?
A. Implement separation of duties.
B. Require SSH on network devices.

C. Change the network administrator password to a more complex one.
D. Whitelist tcpdump of Linux servers.
Answer: (SHOW ANSWER)

NEW QUESTION: 256
An analyst is reviewing a list of vulnerabilities, which were reported from a recent vulnerability scan of a Linux server.
Which of the following is MOST likely to be a false positive?
A. OpenSSH/OpenSSL Package Random Number Generator Weakness
B. HTTP TRACE / TRACK Methods Allowed (002-1208)
C. Apache HTTP Server Byte Range DoS
D. SSL Certificate Expiry
E. GDI+ Remote Code Execution Vulnerability (MS08-052)
Answer: (SHOW ANSWER)

NEW QUESTION: 257
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. Sanitization policy
B. Encryption policy
C. Retention standards
D. Data sovereignty
Answer: C (LEAVE A REPLY)

NEW QUESTION: 258
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: 259
After reviewing the following packet, a cybersecurity analyst has discovered an unauthorized service is running on a company's computer.
Which of the following ACLs, if implemented, will prevent further access ONLY to the unauthorized service and will not impact other services?

A. DENY IP HOST 10.38.219.20 ANY EQ 25
B. DENY IP HOST192.168.1.10 HOST 10.38.219.20 EQ 3389
C. DENY TCP ANY HOST 10.38.219.20 EQ 3389
D. DENY TCP ANY HOST 192.168.1.10 EQ 25
Answer: C (LEAVE A REPLY)

NEW QUESTION: 260
A company's data is still being exfiltered to business competitors after the implementation of a DLP solution. Which of the following is the most likely reason why the data is still being compromised?
A. DRM must be implemented with the DLP solution
B. Printed reports from the database contain sensitive information
C. Users are not labeling the appropriate data sets
D. DLP solutions are only effective when they are implemented with disk encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 261
A technician is troubleshooting a desktop computer with low disk space. The technician reviews the following information snippets:
Which of the following should the technician do to BEST resolve the issue based on the above information? (Choose two.)
A. Disable the movieDB service
B. Install a file integrity tool
C. Delete the movies/movies directory
D. Defragment the disk
E. Enable OS auto updates
Answer: (SHOW ANSWER)

NEW QUESTION: 262
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: 263
A large amount of confidential data was leaked during a recent security breach. As part of a forensic investigation, the security team needs to identify the various types of traffic that were captured between two compromised devices.
Which of the following should be used to identify the traffic?
A. Hashing
B. Memory dump

C. Carving
D. Packet analysis
E. Disk imaging
Answer: D (LEAVE A REPLY)

NEW QUESTION: 264
A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer data. Developers use personal workstations, giving the company little to no visibility into the development activities.
Which of the following would be BEST to implement to alleviate the CISO's concern?
A. Encryption
B. DLP
C. NDA
D. Test data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 265
A malicious hacker wants to gather guest credentials on a hotel 802.11 network. Which of the following tools is the malicious hacker going to use to gain access to information found on the hotel network?
A. Nessus
B. Nikto
C. tcpdump
D. Aircrak-ng
Answer: B (LEAVE A REPLY)

NEW QUESTION: 266
A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost- paymonts.conf file.
The output of the diff command against the known-good backup reads as follows
Which of the following MOST likely occurred?
A. The file was altered to accept payments without charging the cards
B. The file was altered to harvest credit card numbers
C. The file was altered to avoid logging credit card information
D. The file was altered to verify the card numbers are valid.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 267
Which of the following is the BEST way to share incident-related artifacts to provide non-repudiation?
A. Encrypted USB drives
B. Network folders
C. Cloud containers
D. Secure email
Answer: A (LEAVE A REPLY)

NEW QUESTION: 268
A security analyst on the threat-hunting team has developed a list of unneeded, benign services that are currently running as part of the standard OS deployment for workstations. The analyst will provide this list to the operations team to create a policy that will automatically disable the services for all workstations in the organization. Which of the following BEST describes the security analyst's goal?
A. To create a system baseline
B. To optimize system performance
C. To reduce the attack surface
D. To improve malware detection
Answer: (SHOW ANSWER)

NEW QUESTION: 269
A company has implemented WPA2, a 20-character minimum for the WiFi passphrase, and a new WiFi passphrase every 30 days, and has disabled SSID broadcast on all wireless access points. Which of the following is the company trying to mitigate?
A. Downgrade attacks
B. Forced deauthentication
C. SSL pinning
D. Rainbow tables
Answer: A (LEAVE A REPLY)

NEW QUESTION: 270
A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost-paymonts .conf file The output of the diff command against the known-good backup reads as follows
Which of the following MOST likely occurred?
A. The file was altered to harvest credit card numbers
B. The file was altered to accept payments without charging the cards
C. The file was altered to verify the card numbers are valid.
D. The file was altered to avoid logging credit card information
Answer: B (LEAVE A REPLY)

NEW QUESTION: 271
The help desk provided a security analyst with a screenshot of a user's desktop:
For which of the following is aircrack-ng being used?
A. Wireless access point discovery
B. Brute-force attack
C. Rainbow attack
D. PCAP data collection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 272
An analyst is reviewing the following output:
Which of the following was MOST likely used to discover this?
A. A passive vulnerability scan
B. A web application vulnerability scan
C. A static analysis vulnerability scan
D. Reverse engineering using a debugger
Answer: A (LEAVE A REPLY)

NEW QUESTION: 273
An analyst is participating in the solution analysis process for a cloud-hosted SIEM platform to centralize log monitoring and alerting capabilities in the SOC.
Which of the following is the BEST approach for supply chain assessment when selecting a vendor?
A. Identify SLA requirements for monitoring and logging.
B. Gather information from providers, including datacenter specifications and copies of audit reports.
C. Consult with senior management for recommendations.
D. Perform a proof of concept to identify possible solutions.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 274
A security analyst received a series of antivirus alerts from a workstation segment, and users reported ransomware messages. During lessons- learned activities, the analyst determines the antivirus was able to alert to abnormal behavior but did not stop this newest variant of ransomware. Which of the following actions should be taken to BEST mitigate the effects of this type of threat in the future?
A. Enabling sandboxing technology
B. Enabling application blacklisting
C. Purchasing cyber insurance
D. Installing a firewall between the workstations and Internet
Answer: A (LEAVE A REPLY)

NEW QUESTION: 275
A security analyst performed a review of an organization's software development life cycle. The analyst reports that the life cycle does not contain in a phase in which team members evaluate and provide critical feedback on another developer's code. Which of the following assessment techniques is BEST for describing the analyst's report?
A. Waterfall
B. Whitebox testing
C. Architectural evaluation
D. Peer review

Answer: D (LEAVE A REPLY)

NEW QUESTION: 276
A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:
Which of the following is MOST likely a false positive?
A. ICMP timestamp request remote date disclosure
B. Unsupported web server detection
C. Anonymous FTP enabled
D. Windows SMB service enumeration via \srvsvc
Answer: D (LEAVE A REPLY)

NEW QUESTION: 277
A security analyst is performing a review of Active Directory and discovers two new user accounts in the accounting department. Neither of the users has elevated permissions, but accounts in the group are given access to the company's sensitive financial management application by default.
Which of the following is the BEST course of action?
A. Remove the accounts' access privileges to the sensitive application
B. Follow the incident response plan for the introduction of new accounts
C. Monitor the outbound traffic from the application for signs of data exfiltration
D. Confirm the accounts are valid and ensure role-based permissions are appropriate
E. Disable the user accounts
Answer: (SHOW ANSWER)

NEW QUESTION: 278
After analyzing and correlating activity from multiple sensors, the security analyst has determined a group from a high-risk country is responsible for a sophisticated breach of the company network and continuous administration of targeted attacks for the past three months. Until now, the attacks went unnoticed. This is an example of:
A. advanced persistent threat.
B. spear phishing.
C. privilege escalation.
D. malicious insider threat.
Answer: (SHOW ANSWER)

NEW QUESTION: 279
An organization has had problems with security teams remediating vulnerabilities that are either false positives or are not applicable to the organization's servers. Management has put emphasis on security teams conducting detailed analysis and investigation before conducting any remediation.
The output from a recent Apache web server scan is shown below:
The team performs some investigation and finds this statement from Apache on 07/02/2008:
"Fixed in Apache HTTP server 2.2.6, 2.0.61, and 1.3.39"
Which of the following conditions would require the team to perform remediation on this finding?
A. The organization is running version 2.0.5 and has ExtendedStatus enabled
B. The organization is running version 2.0.59 is not using a public-server-status page
C. The organization is running version 1.3.39 and is using a public-server-status page

D. The organization is running version 2.2.6 and has ExtendedStatus enabled
Answer: A (LEAVE A REPLY)

NEW QUESTION: 280
It is important to parameterize queries to prevent _____.
A. a memory overflow that executes code with elevated privileges.
B. the establishment of a web shell that would allow unauthorized access.
C. the execution of unauthorized actions against a database.
D. the queries from using an outdated library with security vulnerabilities.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 281
The security team for a large, international organization is developing a vulnerability management program. The development staff has expressed concern that the new program will cause service interruptions and downtime as vulnerabilities are remedied.
Which of the following should the security team implement FIRST as a core component of the remediation process to address this concern?
A. Change control procedures
B. Security regression testing
C. Isolation of vulnerable servers
D. Automated patch management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 282
A user received an invalid password response when trying to change the password. Which of the following policies could explain why the password is invalid?
A. Access control policy
B. Account management policy
C. Data ownership policy
D. Password policy
Answer: (SHOW ANSWER)

NEW QUESTION: 283
A cybersecurity analyst is currently checking a newly deployed server that has an access control list applied.
When conducting the scan, the analyst received the following code snippet of results:
Which of the following describes the output of this scan?
A. The analyst has discovered a False Positive, and the status code is incorrect providing a server error message.
B. The analyst has discovered a True Positive, and the status code is correct providing a file not found error message.
C. The analyst has discovered a True Positive, and the status code is incorrect providing a forbidden message.
D. The analyst has discovered a False Positive, and the status code is incorrect providing an OK message.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 284
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: (SHOW ANSWER)
Reference:
https://greenlightcorp.com/blog/cyber-security-solutions-data-spillage-and-how-to-create-an-after- incident-to-do-list/

NEW QUESTION: 285
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. Reaver
B. Prowler
C. ZAP
D. Nmap
Answer: (SHOW ANSWER)