

CompTIA.SY0-601.v2023-03-23.q103

Exam Code:	SY0-601
Exam Name:	CompTIA Security+ Exam
Certification Provider:	CompTIA
Free Question Number:	103
Version:	v2023-03-23
# of views:	1447
# of Questions views:	1030
https://www.freepdfdumps.com/CompTIA.SY0-601.v2023-03-23.q103.html	

NEW QUESTION: 1

The Chief Information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the BEST solution to Implement?

- A. DLP
- B. USB data blocker
- C. USB OTG
- D. Disabling USB ports

Answer: A (LEAVE A REPLY)

Explanation

USB data blockers are good, but they're reliant on the employee actually using them. A DLP solution such as MobileIron forces compliance, by locking corporate resources behind a secure application. For example: Users any mobile device policy, such as BYOD, CYOD, and COPE. If they want to access their corporate email on their phone. They will need to sign into the MobileIron application, in order to be granted visibility to their corporate email account. Since the emails are being read/sent through the MobileIron application. Safeguards can be applied even on an outside network-mobile level. If an employee attempts to send a customers social security number, the MobileIron will either block it, alert it, or both, contingent on how the company setup the MobileIron service to work.

NEW QUESTION: 2

As part of a security compliance assessment, an auditor performs automated vulnerability scans. In addition, which of the following should the auditor do to complete the assessment?

- A. User behavior analysis
- B. Packet captures
- C. Configuration reviews
- D. Log analysis

Answer: (SHOW ANSWER)

Explanation

A vulnerability scanner is essentially doing that. It scans every part of your network configuration that it can, and determines if known vulnerabilities are known at any point of that.

NEW QUESTION: 3

A security proposal was set up to track requests for remote access by creating a baseline of the users' common sign-in properties. When a baseline deviation is detected, an lv1FA challenge will be triggered. Which of the following should be configured in order to deploy the proposal?

- A. Context-aware authentication
- B. Simultaneous authentication of equals
- C. Extensive authentication protocol
- D. Agentless network access control

Answer: A (LEAVE A REPLY)

Explanation

An access control scheme that verifies an object's identity based on various environmental factors, like time, location, and behavior.

NEW QUESTION: 4

Which of the following can be used by a monitoring tool to compare values and detect password leaks without providing the actual credentials?

- A. Hashing
- B. Tokenization
- C. Masking
- D. Encryption

Answer: A (LEAVE A REPLY)

Explanation

<https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/>

NEW QUESTION: 5

Which of the following organizations sets frameworks and controls for optimal security configuration on systems?

- A. PCI DSS
- B. NIST
- C. ISO
- D. GDPR

Answer: B (LEAVE A REPLY)

NEW QUESTION: 6

Which of the following describes the continuous delivery software development methodology?

- A. Waterfall

- B. Agile
- C. V-shaped
- D. Spiral

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 7

The Chief Compliance Officer from a bank has approved a background check policy for all new hires Which of the following is the policy MOST likely protecting against?

- A. Filternng applicants who have added false information to resumes so they appear better qualified
- B. Hiring an employee who has been convicted of theft to adhere to industry compliance
- C. Preventing any current employees' siblings from working at the bank to prevent nepotism
- D. Ensuring no new hires have worked at other banks that may be trying to steal customer information

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 8

Which of the following is a reason to publish files' hashes?

- A. To validate the integrity of the files
- B. To use the hash as a software activation key
- C. To verify if the software was digitally signed
- D. To use the hash as a decryption passphrase

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 9

Which of the following is a targeted attack aimed at compromising users within a specific industry or group?

- A. Watering hole
- B. Typosquatting
- C. Hoax
- D. Impersonation

Answer: A ([LEAVE A REPLY](#))

Explanation

A targeted attack refers to a type of threat in which threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over a long-term period. They can adapt, adjust, or improve their attacks to counter their victim's defenses. Background Targeted attacks often employ similar methods found in traditional online threats such as malicious emails, compromised or malicious sites, exploits, and malware.

Targeted attacks differ from traditional online threats in many ways:* Targeted attacks are typically conducted as campaigns. APTs are often conducted in campaigns-a series of failed and

successful attempts over time to get deeper and deeper into a target's network-and are thus not isolated incidents.* They usually target specific industries such as businesses, government agencies, or political groups. Attackers often have long-term goals in mind, with motives that include, but are not limited to, political gain, monetary profit, or business data theft. Attackers often customize, modify and improve their methods depending on the nature of their target sector and to circumvent any security measures implemented.

Phases of a Targeted Attack*

- Intelligence gathering.** Threat actors identify and gather publicly available information about their target to customize their attacks. This initial phase aims to gain strategic information not only on the intended target's IT environment but also on its organizational structure. The information gathered can range from the business applications and software an enterprise utilizes to the roles and relationships that exist within it. This phase also utilizes social engineering techniques that leverage recent events, work-related issues or concerns, and other areas of interest for the intended target.*
- Point of entry.** Threat actors may use varied methods to infiltrate a target's infrastructure. Common methods include customized spearphishing email, zero-day or software exploits, and watering hole techniques. Attackers also utilize instant-messaging and social networking platforms to entice targets to click a link or download malware. Eventually, establishing a connection with the target is acquired.*
- Command-and-control (C&C) communication.** After security has been breached, threat actors constantly communicate to the malware to either execute malicious routines or gather information within the company network. Threat actors use techniques to hide this communication and keep their movements under the radar.*
- Once inside the network,** threat actors move laterally throughout the network to seek key information or infect other valuable systems.*
- Asset/Data Discovery.** Notable assets or data are determined and isolated for future data exfiltration. Threat actors have access to "territories" that contain valuable information and noteworthy assets. These data are then identified and transferred through tools like remote access Trojans (RATs) and customized and legitimate tools. A possible technique used in this stage may be sending back file lists in different directories so attackers can identify what are valuable.*
- Data Exfiltration.** This is the main goal of targeted attacks. An attack's objective is to gather key information and transfer this to a location that the attackers control. Transferring such data can be conducted quickly or gradually. Targeted attacks strive to remain undetected in the network in order to gain access to the company's crown jewels or valuable data. These valuable data include intellectual property, trade secrets, and customer information. In addition, threat actors may also seek other sensitive data such as top-secret documents from government or military institutions.

Once a targeted attack is successful and has reached as far as the data exfiltration stage, it is not difficult for attackers to draw out the data. Although targeted attacks are not known to specifically target consumers, their data are also at risk once target business sectors have been infiltrated. As a result, such attacks (if successful) may damage a company's reputation.

<https://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks#:~:text=A%20targeted%20attack%20r>

NEW QUESTION: 10

Two organizations plan to collaborate on the evaluation of new SIEM solutions for their respective companies.

A combined effort from both organizations' SOC teams would speed up the effort. Which of the following can be written to document this agreement?

- A. MOU
- B. ISA
- C. SLA
- D. NDA

Answer: A ([LEAVE A REPLY](#))

Explanation

A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high-level roles and responsibilities in management of a cross-domain connection.

https://csrc.nist.gov/glossary/term/interconnection_security_agreement

NEW QUESTION: 11

During a recent incident an external attacker was able to exploit an SMB vulnerability over the internet. Which of the following action items should a security analyst perform FIRST to prevent this from occurring again?

- A. Check for any recent SMB CVEs
- B. Deploy a NIDS in the affected subnet
- C. Install AV on the affected server
- D. Block unneeded TCP 445 connections

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 12

A user forwarded a suspicious email to the security team, Upon investigation, a malicious URL was discovered. Which of the following should be done FIRST to prevent other users from accessing the malicious URL?

- A. Configure the web content filter for the web address.
- B. Set the SIEM to alert for any activity to the web address.
- C. Report the website to threat intelligence partners
- D. Send out a corporate communication to warn all users Of the malicious email.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 13

After multiple on premises security solutions were migrated to the cloud, the incident response time increased.

The analyst are spending a long time to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?

- A. SWG
- B. CASB
- C. CMS
- D. VPC

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 14

A junior security analyst is conducting an analysis after passwords were changed on multiple accounts without users' interaction. The SIEM have multiple log entries with the following text:

```
suspicious event - user: scheduledtasks successfully authenticate on AD on abnormal time  
suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\amazing-3rdparty-domain-assessment.py  
suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\secureyourAD-3rdparty-compliance.sh  
suspicious event - user: scheduledtasks successfully executed c:\weekly_checkups\amazing-3rdparty-domain-assessment.py
```

Which of the following is the MOST likely attack conducted on the environment?

- A. Domain hijacking
- B. Malicious script
- C. DNS poisoning
- D. Privilege escalation

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 15

A company recently experienced a significant data loss when proprietary information was leaked to a competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage.

Which of the following is the BEST remediation for this data leak?

- A. User training
- B. MDM
- C. DLP
- D. CASB

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 16

Which of the following is assured when a user signs an email using a private key?

- A. Non-repudiation
- B. Confidentiality
- C. Availability

D. Authentication

Answer: A ([LEAVE A REPLY](#))

Explanation

Non Repudiation is your virtual John Hancock. It's a way of virtually stamping any data or document with "I am who I say I am". Only way to break this would be if the private key owners' private key became compromised. Which at that point you got bigger problems than Non Repudiation.

Valid SY0-601 Dumps shared by Actual4test.com for Helping Passing SY0-601 Exam! Actual4test.com now offer the **newest SY0-601 exam dumps**, the Actual4test.com SY0-601 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-601 dumps with Test Engine here:

https://www.actual4test.com/SY0-601_examcollection.html (**1061** Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 17

A security engineer is building a file transfer solution to send files to a business partner. The users would like to drop off the files in a specific directory and have the server send to the business partner. The connection to the business partner is over the internet and needs to be secure. Which of the following can be used?

- A. S/MIME
- B. SSH
- C. SRTP
- D. LDAPS

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 18

Which of the following risk management strategies would an organization use to maintain a legacy system with known risks for operational purposes?

- A. Mitigation
- B. Transference
- C. Acceptance
- D. Avoidance

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 19

Which of the following would be the BEST way to analyze diskless malware that has infected a VDI?

- A. Shut down the VDI and copy off the event logs.

- B. Use NetFlow to identify command-and-control IPs.
- C. Take a memory snapshot of the running system.
- D. Run a full on-demand scan of the root volume.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 20

An analyst receives multiple alerts for beaconing activity for a host on the network, After analyzing the activity, the analyst observes the following activity:

- * A user enters comptia.org into a web browser.
- * The website that appears is not the comptia.org site.
- * The website is a malicious site from the attacker.
- * Users in a different office are not having this issue.

Which of the following types of attacks was observed?

- A. Locator (URL) redirection
- B. Domain hijacking
- C. On-path attack
- D. DNS poisoning

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 21

A security analyst is evaluating solutions to deploy an additional layer of protection for a web application The goal is to allow only encrypted communications without relying on network devices Which of the following can be implemented?

- A. S/MIME
- B. HTTP security header
- C. DNSSEC implementation
- D. SRTP

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 22

A security analyst needs to be able to search and correlate logs from multiple sources in a single tool Which of the following would BEST allow a security analyst to have this ability?

- A. SOAR
- B. SIEM
- C. Log collectors
- D. Network-attached storage

Answer: B ([LEAVE A REPLY](#))

Explanation

SIEM event correlation is an essential part of any SIEM solution. It aggregates and analyzes log data from across your network applications, systems, and devices, making it possible to discover

security threats and malicious patterns of behaviors that otherwise go unnoticed and can lead to compromise or data loss.

NEW QUESTION: 23

A company is providing security awareness training regarding the importance of not forwarding social media messages from unverified sources. Which of the following risks would this training help to prevent?

- A. Hoaxes
- B. SPIMs
- C. Identity fraud
- D. Credential harvesting

Answer: A ([LEAVE A REPLY](#))

Explanation

Hoax

A hoax is a falsehood deliberately fabricated to masquerade as the truth. It is distinguishable from errors in observation or judgment, rumors, urban legends, pseudo sciences, and April Fools' Day events that are passed along in good faith by believers or as jokes.

Identity theft

Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The term identity theft was coined in 1964. Identity fraud (also known as identity theft or crime) involves someone using another individual's personal information without consent, often to obtain a benefit.

Credential Harvesting

Credential Harvesting (or Account Harvesting) is the use of MITM attacks, DNS poisoning, phishing, and other vectors to amass large numbers of credentials (username / password combinations) for reuse.

NEW QUESTION: 24

During a security incident investigation, an analyst consults the company's SIEM and sees an event concerning high traffic to a known, malicious command-and-control server. The analyst would like to determine the number of company workstations that may be impacted by this issue. Which of the following can provide the information?

- A. Application logs
- B. DNS logs
- C. WAF logs
- D. System logs

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 25

A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage. Which of the following BEST describes these threat actors?

- A. State actors
- B. Semi-authorized hackers
- C. Script kiddies
- D. Advanced persistent threats

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 26

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS

Not all attacks and remediation actions will be used.

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

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	- Botnet - RAT - Logic Bomb - Backdoor - Virus - Spyware - Worm - Adware - Ransomware - Keylogger - Phishing	- Enable DDoS protection - Patch vulnerable systems - Disable vulnerable services - Change the default system password - Update the cryptographic algorithms - Change the default application password - Implement 2FA using push notification - Conduct a code review - Implement application fuzzing - Implement a host-based IPS - Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	- Botnet - RAT - Logic Bomb - Backdoor - Virus - Spyware - Worm - Adware - Ransomware - Keylogger - Phishing	- Enable DDoS protection - Patch vulnerable systems - Disable vulnerable services - Change the default system password - Update the cryptographic algorithms - Change the default application password - Implement 2FA using push notification - Conduct a code review - Implement application fuzzing - Implement a host-based IPS - Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	- Botnet - RAT - Logic Bomb - Backdoor - Virus - Spyware - Worm - Adware - Ransomware - Keylogger - Phishing	- Enable DDoS protection - Patch vulnerable systems - Disable vulnerable services - Change the default system password - Update the cryptographic algorithms - Change the default application password - Implement 2FA using push notification - Conduct a code review - Implement application fuzzing - Implement a host-based IPS - Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	- Botnet - RAT - Logic Bomb - Backdoor - Virus - Spyware - Worm - Adware - Ransomware - Keylogger - Phishing	- Enable DDoS protection - Patch vulnerable systems - Disable vulnerable services - Change the default system password - Update the cryptographic algorithms - Change the default application password - Implement 2FA using push notification - Conduct a code review - Implement application fuzzing - Implement a host-based IPS - Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	- Botnet - RAT - Logic Bomb - Backdoor - Virus - Spyware - Worm - Adware - Ransomware - Keylogger - Phishing	- Enable DDoS protection - Patch vulnerable systems - Disable vulnerable services - Change the default system password - Update the cryptographic algorithms - Change the default application password - Implement 2FA using push notification - Conduct a code review - Implement application fuzzing - Implement a host-based IPS - Disable remote access services

Explanation

Web server Botnet Enable DDoS protection RAT Implement a host-based IPS Database server
Worm Change the default application password Keylogger Disable vulnerable services Application

Backdoor Implement 2FA using push notification Graphical user interface, application Description automatically generated

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

NEW QUESTION: 27

Which of the following processes will eliminate data using a method that will allow the storage device to be reused after the process is complete?

- A. Pulverizing
- B. Overwriting
- C. Shredding
- D. Degaussing

Answer: D ([LEAVE A REPLY](#))

Explanation

<https://dataspan.com/blog/what-are-the-different-types-of-data-destruction-and-which-one-should-you-use/>

NEW QUESTION: 28

After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset This technique is an example of:

- A. footprinting
- B. persistence
- C. pivoting.
- D. privilege escalation

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 29

Which of the following is the MOST effective way to detect security flaws present on third-party libraries embedded on software before it is released into production?

- A. Employ different techniques for server- and client-side validations.
- B. Use a different version control system for third-party libraries.
- C. Implement a vulnerability scan to assess dependencies earlier on SDLC.
- D. Increase the number of penetration tests before software release.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 30

A security engineer is deploying a new wireless for a company. The company shares office space with multiple tenants. Which of the following should the engineer configured on the wireless network to ensure that confidential data is not exposed to unauthorized users?

- A. AES
- B. EAP
- C. TLS
- D. HTTPS

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 31

An application developer accidentally uploaded a company's code-signing certificate private key to a public web server. The company is concerned about malicious use of its certificate. Which of the following should the company do FIRST?

- A. Delete the private key from the repository.
- B. Verify the public key is not exposed as well.
- C. Update the DLP solution to check for private keys.
- D. Revoke the code-signing certificate.

Answer: D ([LEAVE A REPLY](#))

Explanation

We need to revoke the code-signing certificate as this is the most secure way to ensure that the comprised key wont be used by attackers. Usually there are bots crawling all over repos searching this kind of human errors.

Valid SY0-601 Dumps shared by Actual4test.com for Helping Passing SY0-601 Exam!

Actual4test.com now offer the **newest SY0-601 exam dumps**, the Actual4test.com SY0-601 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-601 dumps with Test Engine here:

https://www.actual4test.com/SY0-601_examcollection.html (1061 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 32

Which of the following concepts BEST describes tracking and documenting changes to software and managing access to files and systems?

- A. Version control
- B. Continuous monitoring
- C. Stored procedures
- D. Automation

Answer: A ([LEAVE A REPLY](#))

Explanation

Version control, also known as source control, is the process of tracking and managing changes to files over time. VCS - version control systems - are software tools designed to help teams work in parallel.

<https://www.perforce.com/blog/vcs/what-is-version-control>

NEW QUESTION: 33

Which of the following is a security best practice that ensures the integrity of aggregated log files within a SIEM?

- A. Set up hashing on the source log file servers that complies with local regulatory requirements,
- B. Back up the source log files and archive them for at least six years or in accordance with local regulatory requirements.
- C. Back up the aggregated log files at least two times a day or as stated by local regulatory requirements.
- D. Write protect the aggregated log files and move them to an isolated server with limited access.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 34

An administrator is configuring a firewall rule set for a subnet to only access DHCP, web pages, and SFTP, and to specifically block FTP. Which of the following would BEST accomplish this goal?

- A. [Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Allow: Any Any 67
Allow: Any Any 68
Allow: Any Any 22
Deny: Any Any 21
Deny: Any Any
- B. [Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Allow: Any Any 67
Allow: Any Any 68
Deny: Any Any 22
Allow: Any Any 21
Deny: Any Any
- C. [Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Allow: Any Any 22
Deny: Any Any 67
Deny: Any Any 68
Deny: Any Any 21
Allow: Any Any
- D. [Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Deny: Any Any 67
Allow: Any Any 68
Allow: Any Any 22
Allow: Any Any 21
Allow: Any Any

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 35

A company recently experienced an inside attack using a corporate machine that resulted in data compromise.

Analysis indicated an unauthorized change to the software circumvented technological protection measures. The analyst was tasked with determining the best method to ensure the integrity of the systems remains intact and local and remote boot attestation can take place. Which of the following would provide the BEST solution?

- A. HIPS
B. Fly
C. TPM

D. DLP

Answer: C ([LEAVE A REPLY](#))

Explanation

<https://docs.microsoft.com/en-us/azure/security/fundamentals/measured-boot-host-attestation>

NEW QUESTION: 36

An organization has developed an application that needs a patch to fix a critical vulnerability In which of the following environments should the patch be deployed LAST?

- A. Test
- B. Staging
- C. Production
- D. Development

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 37

Which of the following is an example of transference of risk?

- A. Application owner risk sign-off
- B. Purchasing insurance
- C. Retiring outdated applications
- D. Patching vulnerable servers

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 38

Data exfiltration analysis indicates that an attacker managed to download system configuration notes from a web server. The web-server logs have been deleted, but analysts have determined that the system configuration notes were stored in the database administrator's folder on the web server Which of the following attacks explains what occurred? (Select TWO)

- A. SQL injection
- B. Request forgery
- C. Pass-the- hash
- D. Directory traversal
- E. Privilege escalation
- F. Cross-site scripting

Answer: C,E ([LEAVE A REPLY](#))

NEW QUESTION: 39

A Chief Information Security Officer has defined resiliency requirements for a new data center architecture The requirements are as follows

- * Critical fileshares will remain accessible during and after a natural disaster
- * Five percent of hard disks can fail at any given time without impacting the data.

* Systems will be forced to shut down gracefully when battery levels are below 20% Which of the following are required to BEST meet these objectives? (Select THREE)

- A. Fiber switching
- B. IaC
- C. UPS
- D. Load balancing
- E. Snapshots
- F. Geographic dispersal
- G. NAS
- H. Redundant power supplies
- I. RAID

Answer: C,F,I ([LEAVE A REPLY](#))

NEW QUESTION: 40

A company is considering transitioning to the cloud. The company employs individuals from various locations around the world The company does not want to increase its on-premises infrastructure blueprint and only wants to pay for additional compute power required. Which of the following solutions would BEST meet the needs of the company?

- A. Hot backup site
- B. Private cloud
- C. Hybrid environment
- D. Managed security service provider

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 41

While preparing a software Inventory report, a security analyst discovers an unauthorized program installed on most of the company's servers. The program utilizes the same code signing certificate as an application deployed to only the accounting team. Which of the following mitigations would BEST secure the server environment?

- A. Add the accounting application file hash to the allowed list.
- B. Update the code signing certificate for the approved application.
- C. Revoke the code signing certificate used by both programs.
- D. Block all unapproved file hashes from installation.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 42

A company's security team received notice of a critical vulnerability affecting a high-profile device within the web infrastructure. The vendor patch was just made available online but has not yet been regression tested in development environments. In the interim, firewall rules were implemented to reduce the access to the interface affected by the vulnerability. Which of the following controls does this scenario describe?

- A. Compensating
- B. Preventive
- C. Detective
- D. Deterrent

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 43

A business operations manager is concerned that a PC that is critical to business operations will have a costly hardware failure soon. The manager is looking for options to continue business operations without incurring large costs. Which of the following would mitigate the manager's concerns?

- A. Implement a full system upgrade
- B. Install uninterruptible power supplies
- C. Purchase cybersecurity insurance
- D. Perform a physical-to-virtual migration

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 44

A company labeled some documents with the public sensitivity classification This means the documents can be accessed by:

- A. only the individuate listed in the documents
- B. only the company's employees and those listed in the document
- C. all members of the department that created the documents
- D. employees of other companies and the press

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 45

A tax organization is working on a solution to validate the online submission of documents The solution should be earned on a portable USB device that should be inserted on any computer that is transmitting a transaction securely. Which of the following is the BEST certificate for these requirements?

- A. User certificate
- B. Root certificate
- C. Computer certificate
- D. Self-signed certificate

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 46

A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select TWO).

- A. A CRC32 checksum

- B. The provenance of the artifacts
- C. The vendor's name
- D. The date time
- E. A warning banner
- F. The order of volatility

Answer: ([SHOW ANSWER](#))

Valid SY0-601 Dumps shared by Actual4test.com for Helping Passing SY0-601 Exam!
Actual4test.com now offer the **newest SY0-601 exam dumps**, the Actual4test.com SY0-601 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-601 dumps with Test Engine here:

https://www.actual4test.com/SY0-601_examcollection.html (1061 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 47

A company is auditing the manner in which its European customers' personal information is handled Which of the following should the company consult?

- A. ISO
- B. GDPR
- C. NIST
- D. PCI DSS

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 48

DDoS attacks are causing an overload on the cluster of cloud servers. A security architect is researching alternatives to make the cloud environment respond to load fluctuation in a cost-effective way. Which of the following options BEST fulfils the architect's requirements?

- A. An orchestration solution that can adjust scalability of cloud assets
- B. Use of multipath by adding more connections to cloud storage
- C. Cloud assets replicated on geographically distributed regions
- D. An on-site backup that is deployed and only used when the load increases

Answer: A ([LEAVE A REPLY](#))

Explanation

Scaling cloud infrastructures can experience lag during the periods of high activity, where other assets have to either be added, or become active. This is the compromise for a cost-effective solution that scales. The company could go for a system that is absolutely overkill on assets at all times, in preparation for those brief peak moments. But this is expensive, and unlikely to be taken by most companies. Only case you would want to use one of these is if you have a sensitive or

critical service that MUST remain online. Stock exchange servers, military servers, bank servers, etc. come to mind for this criteria.

NEW QUESTION: 49

A user enters a username and a password at the login screen for a web portal. A few seconds later the following message appears on the screen: Please use a combination of numbers, special characters, and letters in the password field. Which of the following concepts does this message describe?

- A. Password reuse
- B. Password age
- C. Password history
- D. Password complexity

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 50

The Chief information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the Best solution to implement?

- A. USB OTG
- B. DLP
- C. USB data blocker
- D. Disabling USB ports

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 51

A user is attempting to navigate to a website from inside the company network using a desktop. When the user types in the URL. https://www.site.com, the user is presented with a certificate mismatch warning from the browser. The user does not receive a warning when visiting http://www.anothersite.com. Which of the following describes this attack?

- A. Domain hijacking
- B. Evil twin
- C. DNS poisoning
- D. On-path

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 52

A user wanted to catch up on some work over the weekend but had issues logging in to the corporate network using a VPN. On Monday, the user opened a ticket for this issue but was able to log in successfully. Which of the following BEST describes the policy that is being implemented?

- A. Network location

- B. Password history
- C. Geofencing
- D. Time-based logins

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 53

Which of the following would detect intrusions at the perimeter of an airport?

- A. Fencing
- B. Signage
- C. Motion sensors
- D. Lighting
- E. Bollards

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 54

Which biometric error would allow an unauthorized user to access a system?

- A. False entrance
- B. False acceptance
- C. False rejection
- D. False denial

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 55

Which of the following control Types would be BEST to use in an accounting department to reduce losses from fraudulent transactions?

- A. Recovery
- B. Deterrent
- C. Corrective
- D. Detective

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 56

Which of the following would BEST provide a systems administrator with the ability to more efficiently identify systems and manage permissions and policies based on location, role, and service level?

- A. Standard naming conventions
- B. Baseline configurations
- C. Diagrams
- D. Domain services

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 57

During a recent penetration test, the tester discovers large amounts of data were exfiltrated over the course of

12 months via the internet. The penetration tester stops the test to inform the client of the findings

Which of the following should be the client's NEXT step to mitigate the issue"

- A. Conduct a full vulnerability scan to identify possible vulnerabilities
- B. Perform containment on the critical servers and resources
- C. Review the firewall and identify the source of the active connection
- D. Disconnect the entire infrastructure from the internet

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 58

An organization is planning to roll out a new mobile device policy and issue each employee a new laptop, These laptops would access the users' corporate operating system remotely and allow them to use the laptops for purposes outside of their job roles. Which of the following deployment models is being utilized?

- A. CYOD and VMs
- B. MDM and application management
- C. BYOO and containers
- D. COPE and VDI

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 59

A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.

Perform the following steps:

1. Configure the RADIUS server.
2. Configure the WiFi controller.
3. Preconfigure the client for an incoming guest. The guest AD credentials are:

User: guest01

Password: guestpass



WiFi Controller

SSID: CORPGUEST

Shared key:

AAA server IP:

PSK:

Authentication type:

Controller IP: 192.168.1.10

Reset Answer Save Close

WiFi

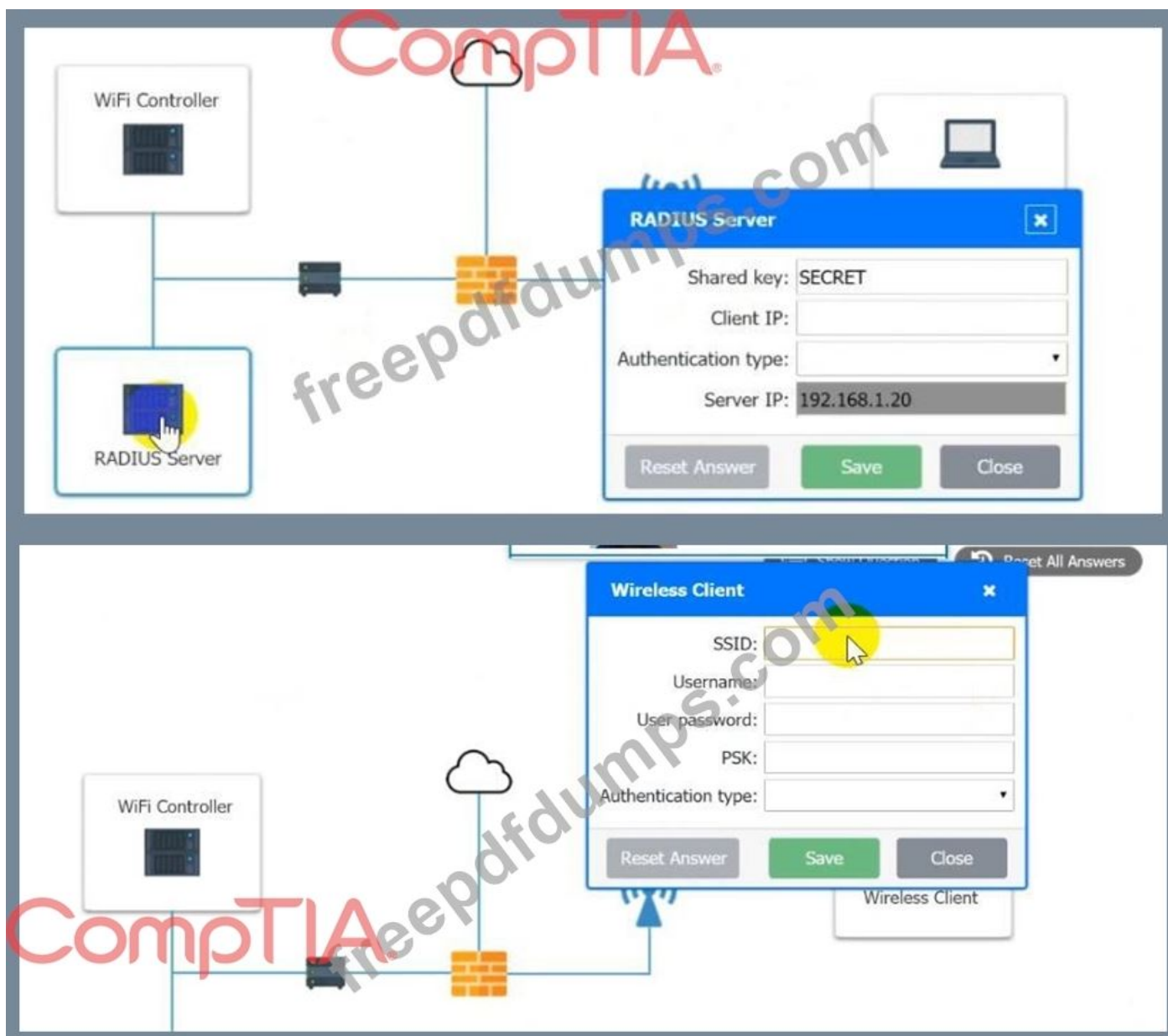
RADIUS Server

Wireless Client

CompTIA

freepdfdumps.com

Show Question Reset All Answers



Answer:

See the answer below.

Explanation

Use the same settings as describe in below images.

Graphical user interface, application Description automatically generated



Graphical user interface, text, application Description automatically generated



NEW QUESTION: 60

Which of the following is a known security risk associated with data archives that contain financial information?

- A. Data can become a liability if archived longer than required by regulatory guidance
- B. Companies are prohibited from providing archived data to e-discovery requests
- C. Unencrypted archives should be preserved as long as possible and encrypted
- D. Data must be archived off-site to avoid breaches and meet business requirements

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 61

A vulnerability has been discovered and a known patch to address the vulnerability does not exist. Which of the following controls works BEST until a proper fix is released?

- A. Compensating
- B. Deterrent
- C. Corrective
- D. Detective

Answer: D ([LEAVE A REPLY](#))

Valid SY0-601 Dumps shared by Actual4test.com for Helping Passing SY0-601 Exam!

Actual4test.com now offer the **newest SY0-601 exam dumps**, the Actual4test.com SY0-601 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-601 dumps with Test Engine here:

https://www.actual4test.com/SY0-601_examcollection.html (1061 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 62

Which of the following is an effective tool to stop or prevent the exfiltration of data from a network?

- A. DLP
- B. TPM
- C. NIDS
- D. FDE

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 63

An organization is migrating several SaaS applications that support SSO. The security manager wants to ensure the migration is completed securely. Which of the following should the organization consider before implementation? (Select TWO).

- A. The hashing method
- B. The encryption method
- C. The certificate authority
- D. The back-end directory source
- E. The identity federation protocol
- F. The registration authority

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 64

An analyst is reviewing logs associated with an attack. The logs indicate an attacker downloaded a malicious file that was quarantined by the AV solution. The attacker utilized a local non-administrative account to restore the malicious file to a new location. The file was then used by another process to execute a payload.

Which of the following attacks did the analyst observe?

- A. Privilege escalation
- B. Request forgeries
- C. Injection
- D. Replay attack

Answer: ([SHOW ANSWER](#)**)**

Explanation

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf[1]) or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts.[2]

There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge.

Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.[3] In a CSRF attack, an innocent end user is

tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

NEW QUESTION: 65

Which of the following explains why RTO is included in a BIA?

- A.** It informs the backup approach so that the organization can recover data to a known time.
- B.** It prioritizes risks so the organization can allocate resources appropriately,
- C.** It monetizes the loss of an asset and determines a break-even point for risk mitigation.
- D.** It identifies the amount of allowable downtime for an application or system,

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 66

A company wants to simplify the certificate management process. The company has a single domain with several dozen subdomains, all of which are publicly accessible on the internet.

Which of the following BEST describes the type of certificate the company should implement?

- A.** Subject alternative name
- B.** Wildcard
- C.** Self-signed
- D.** Domain validation

Answer: **B** ([LEAVE A REPLY](#))

Explanation

Wildcard SSL certificates are for a single domain and all its subdomains. A subdomain is under the umbrella of the main domain. Usually subdomains will have an address that begins with something other than 'www.' For example, www.cloudflare.com has a number of subdomains, including blog.cloudflare.com, support.cloudflare.com, and developers.cloudflare.com. Each is a subdomain under the main cloudflare.com domain.

Wildcard SSL Certificate

A single Wildcard SSL certificate can apply to all of these subdomains. Any subdomain will be listed in the SSL certificate. Users can see a list of subdomains covered by a particular certificate by clicking on the padlock in the URL bar of their browser, then clicking on "Certificate" (in Chrome) to view the certificate's details.

<https://www.cloudflare.com/learning/ssl/types-of-ssl-certificates/>

NEW QUESTION: 67

An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email regarding the credit card statement with unusual purchases. Which of the following attacks took place?

- A.** Protocol poisoning
- B.** Bluejacking

- C. On-path attack
- D. Domain hijacking

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 68

An organization wants to implement a biometric system with the highest likelihood that an unauthorized user will be denied access. Which of the following should the organization use to compare biometric solutions?

- A. Cost
- B. FAR
- C. FRR
- D. CER
- E. Difficulty of use

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 69

A customer service representative reported an unusual text message that was sent to the help desk. The message contained an unrecognized invoice number with a large balance due and a link to click for more details. Which of the following BEST describes this technique?

- A. Vishing
- B. Phishing
- C. Whaling
- D. Smishing

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 70

A SOC operator is analyzing a log file that contains the following entries:

```
[06-Apr-2021-18:00:06] GET /index.php/../../../../../../etc/passwd
[06-Apr-2021-18:01:07] GET /index.php/../../../../../../etc/shadow
[06-Apr-2021-18:01:26] GET /index.php/../../../../../../etc/passwd
[06-Apr-2021-18:02:16] GET /index.php?var1=;cat /etc/passwd;&var2=7865tgydk
[06-Apr-2021-18:02:56] GET /index.php?var1=;cat /etc/shadow;&var2=7865tgydk
```

- A. SQL injection and improper input-handling attempts
- B. Cross-site scripting and resource exhaustion attempts
- C. Command injection and directory traversal attempts
- D. Error handling and privilege escalation attempts

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 71

Which of the following is the MOST effective control against zero-day vulnerabilities?

- A. Patch management
- B. Multiple vulnerability scanners

- C. Intrusion prevention system
- D. Network segmentation

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 72

A SOC operator is receiving continuous alerts from multiple Linux systems indicating that unsuccessful SSH attempts to a functional user ID have been attempted on each one of them in a short period of time. Which of the following BEST explains this behavior?

- A. Rainbow table attack
- B. Password spraying
- C. Logic bomb
- D. Malware bot

Answer: (SHOW ANSWER)

Explanation

Password Spraying is a variant of what is known as a brute force attack. In a traditional brute force attack, the perpetrator attempts to gain unauthorized access to a single account by guessing the password "repeatedly" in a very short period of time.

NEW QUESTION: 73

Which of the following is an example of risk avoidance?

- A. Buying insurance to prepare for financial loss associated with exploits
- B. Not installing new software to prevent compatibility errors
- C. Installing security updates directly in production to expedite vulnerability fixes
- D. Not taking preventive measures to stop the theft of equipment

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 74

A security analyst is evaluating the risks of authorizing multiple security solutions to collect data from the company's cloud environment Which of the following is an immediate consequence of these integrations?

- A. Non-compliance with data sovereignty rules
- B. Loss of the vendor's interoperability support
- C. Mandatory deployment of a SIEM solution
- D. Increase in the attack surface

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 75

An organization has hired a red team to simulate attacks on its security posture Which of the following will the blue team do after detecting an IoC?

- A. Conduct forensics on the compromised system
- B. Conduct passive reconnaissance to gather information

- C. Activate runbooks for incident response
- D. Reimage the impacted workstations

Answer: (SHOW ANSWER)

NEW QUESTION: 76

Which of the following control types fixes a previously identified issue and mitigates a risk?

- A. Preventative
- B. Finalized
- C. Detective
- D. Corrective

Answer: D (LEAVE A REPLY)

Valid SY0-601 Dumps shared by Actual4test.com for Helping Passing SY0-601 Exam! Actual4test.com now offer the **newest SY0-601 exam dumps**, the Actual4test.com SY0-601 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-601 dumps with Test Engine here:

https://www.actual4test.com/SY0-601_examcollection.html (1061 Q&As Dumps, **30%OFF**

Special Discount: **Freepdfdumps**)

NEW QUESTION: 77

A company wants to build a new website to sell products online. The website will host a storefront application that will allow visitors to add products to a shopping cart and pay for the products using a credit card. Which of the following protocols would be the MOST secure to implement?

- A. FTP
- B. TLS
- C. SSL
- D. SNMP

Answer: C (LEAVE A REPLY)

NEW QUESTION: 78

Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a security analyst for further review. The security analyst reviews the following metrics:

Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting-PC	22%	48%	12	66
HR-PC	35%	55%	15	57
IT-PC	78%	98%	25	92
Sales-PC	28%	50%	20	56
Manager-PC	21%	44%	18	49

Which of the following is MOST likely the result of the security analyst's review?

- A. Corporate PCs have been turned into a botnet
- B. The user of the Sales-PC fell for a phishing attack

- C. The ISP is dropping outbound connections
- D. An on-path attack is taking place between PCs and the router

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 79

Which of the following employee roles is responsible for protecting an organization's collected personal information?

- A. CTO
- B. DPO
- C. CEO
- D. DBA

Answer: B ([LEAVE A REPLY](#))

Explanation

Many companies also have a data protection officer or DPO. This is a higher-level manager who is responsible for the organization

<https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/#:~:text=M>

NEW QUESTION: 80

A security analyst receives an alert from the company's SIEM that anomalous activity is coming from a local source IP address of 192.168.34.26. The Chief Information Security Officer asks the analyst to block the originating source. Several days later, another employee opens an internal ticket stating that vulnerability scans are no longer being performed properly. The IP address the employee provides is 192.168.34.26. Which of the following describes this type of alert?

- A. False positive
- B. True negative
- C. False negative
- D. True positive

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 81

A social media company based in North America is looking to expand into new global markets and needs to maintain compliance with international standards. With which of the following is the company's data protection officer MOST likely concerned?

- A. GDPR
- B. NIST Framework
- C. PCI-DSS
- D. ISO 27001

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 82

Which of the following secure coding techniques makes compromised code more difficult for hackers to use?

- A. Obfuscation
- B. Normalization
- C. Execution
- D. Reuse

Answer: ([SHOW ANSWER](#))

Explanation

[https://en.wikipedia.org/wiki/Obfuscation_\(software\)](https://en.wikipedia.org/wiki/Obfuscation_(software))

NEW QUESTION: 83

A recent audit cited a risk involving numerous low-criticality vulnerabilities created by a web application using a third-party library. The development staff state there are still customers using the application even though it is end of life and it would be a substantial burden to update the application for compatibility with more secure libraries. Which of the following would be the MOST prudent course of action?

- A. Use containerization to segment the application from other applications to eliminate the risk
- B. Accept the risk if there is a clear road map for timely decommission
- C. Deny the risk due to the end-of-life status of the application.
- D. Outsource the application to a third-party developer group

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 84

A security policy states that common words should not be used as passwords. A security auditor was able to perform a dictionary attack against corporate credentials Which of the following controls was being violated?

- A. Password complexity
- B. Password length
- C. Password reuse
- D. Password history

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 85

A business operations manager is concerned that a PC that is critical to business operations will have a costly hardware failure soon. The manager is looking for options to continue business operations without incurring large costs. Which of the following would mitigate the manager's concerns?

- A. Implement a full system upgrade
- B. Perform a physical-to-virtual migration
- C. Purchase cybersecurity insurance
- D. Install uninterruptible power supplies

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 86

A company wants to restrict emailing of PHI documents. The company is implementing a DLP solution. In order to restrict PHI documents which of the following should be performed FIRST?

- A. Governance
- B. Change management
- C. Classification
- D. Retention

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 87

An administrator is experiencing issues when trying to upload a support file to a vendor. A pop-up message reveals that a payment card number was found in the file, and the file upload was blocked. Which of the following controls is most likely causing this issue and should be checked FIRST?

- A. MDM
- B. Content filter
- C. Application allow list
- D. Firewall rule
- E. DLP

Answer: E ([LEAVE A REPLY](#))

NEW QUESTION: 88

A penetration tester was able to compromise an internal server and is now trying to pivot the current session in a network lateral movement. Which of the following tools if available on the server, will provide the MOST useful information for the next assessment step?

- A. Autopsy
- B. Cuckoo
- C. Memdump
- D. Nmap

Answer: ([SHOW ANSWER](#))

Explanation

Nmap is basically mapping a network. The purpose of lateral pivoting is to gain a new perspective, or new information that will allow you to either privilege escalate, or to achieve the goal of the attack. If the compromised server the pen tester is exploiting has nmap enabled, the pen tester will be able to get an in-depth inside view of the internal network structure.

NEW QUESTION: 89

Which of the following provides a calculated value for known vulnerabilities so organizations can prioritize mitigation steps?

- A. SOAR
- B. CVSS
- C. CVE
- D. SIEM

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 90

The Chief Information Security Officer (CISO) has requested that a third-party vendor provide supporting documents that show proper controls are in place to protect customer data. Which of the following would be BEST for the third-party vendor to provide to the CISO?

- A. GDPR compliance attestation
- B. Cloud Security Alliance materials
- C. SOC 2 Type 2 report
- D. NIST RMF workbooks

Answer: C ([LEAVE A REPLY](#))

Explanation

<https://www.itgovernance.co.uk/soc-reporting>

NEW QUESTION: 91

A security administrator is analyzing the corporate wireless network. The network only has two access points running on channels 1 and 11. While using airodump-ng, the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access points. Which of the following attacks is happening on the corporate network?

- A. Disassociation
- B. Rogue access point
- C. Man in the middle
- D. Jamming
- E. Evil twin

Answer: ([SHOW ANSWER](#))

Valid SY0-601 Dumps shared by Actual4test.com for Helping Passing SY0-601 Exam! Actual4test.com now offer the **newest SY0-601 exam dumps**, the Actual4test.com SY0-601 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-601 dumps with Test Engine here:

https://www.actual4test.com/SY0-601_examcollection.html (1061 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 92

While reviewing an alert that shows a malicious request on one web application, a cybersecurity analyst is alerted to a subsequent token reuse moments later on a different service using the same single sign-on method.

Which of the following would BEST detect a malicious actor?

- A. Utilizing SIEM correlation engines
- B. Deploying Netflow at the network border
- C. Disabling session tokens for all sites
- D. Deploying a WAF for the web server

Answer: ([SHOW ANSWER](#))

Explanation

The initial compromise was a malicious request on a web server. Moments later the token created with SSO was used on another service, the question does not specify what type of service.

Deploying a WAF on the web server will detect the attacker but only on that server. If the attacker issues the same malicious request to get another SSO token correlating that event with using that SSO token in other services would allow to detect the malicious activity.

NEW QUESTION: 93

Which of the following can work as an authentication method and as an alerting mechanism for unauthorized access attempts?

- A. Attestation service
- B. HMAC-based, one-time password
- C. push notifications
- D. Smart card

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 94

A security analyst is investigating some users who are being redirected to a fake website that resembles www.comptia.org. The following output was found on the naming server of the organization:

Name	Type	Data
www	A	192.168.1.10
server1	A	10.10.10.10
server2	A	10.10.10.11
file	A	10.10.10.12

Which of the following attacks has taken place?

- A. DNS poisoning
- B. Disassociation
- C. Domain reputation
- D. Domain hijacking

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 95

Which of the following is the MOST likely reason for securing an air-gapped laboratory HVAC system?

- A. To avoid data leakage
- B. To protect surveillance logs
- C. To facilitate third-party access
- D. To ensure availability

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 96

A security architect is required to deploy to conference rooms some workstations that will allow sensitive data to be displayed on large screens. Due to the nature of the data, it cannot be stored in the conference rooms. The fileshare is located in a local data center. Which of the following should the security architect recommend to BEST meet the requirement?

- A. Full drive encryption and thick clients
- B. VDI and thin clients
- C. Private cloud and DLP
- D. Fog computing and KVMs

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 97

A security analyst is concerned about critical vulnerabilities that have been detected on some applications running inside containers. Which of the following is the BEST remediation strategy?

- A. Patch each running container individually and test the application
- B. Update the base container image and redeploy the environment
- C. Include the containers in the regular patching schedule for servers
- D. Update the host in which the containers are running

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 98

Security analysts are conducting an investigation of an attack that occurred inside the organization's network.

An attacker was able to connect network traffic between workstation throughout the network. The analysts review the following logs:



VLAN	Address
1	0007.1e5d.3213
1	002a.7d.44.8801
1	0011.aab4.344d

The layer 2 address table has hundred of entries similar to the ones above. Which of the following attacks has MOST likely occurred?

- A. ARP poisoning

- B. SQL injection
- C. DNS spoofing
- D. MAC flooding

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 99

To reduce and limit software and infrastructure costs, the Chief Information Officer has requested to move email services to the cloud. The cloud provider and the organization must have security controls to protect sensitive data. Which of the following cloud services would BEST accommodate the request?

- A. PaaS
- B. IaaS
- C. DaaS
- D. SaaS

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 100

A security analyst is reviewing application logs to determine the source of a breach and locates the following log:

```
https://www.comptia.com/login.php?id='%20or%20'1'1='1
```

Which Of the following has been observed?

- A. API attack
- B. XSS
- C. DLL Injection
- D. SQLI

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 101

A Chief Security Officer is looking for a solution that can provide increased scalability and flexibility for back-end infrastructure, allowing it to be updated and modified without disruption to services. The security architect would like the solution selected to reduce the back-end server resources and has highlighted that session persistence is not important for the applications running on the back-end servers. Which of the following would BEST meet the requirements?

- A. Reverse proxy
- B. Automated patch management
- C. Snapshots
- D. NIC teaming

Answer: A ([LEAVE A REPLY](#))

Explanation

A reverse proxy would be the best solution for increased scalability and flexibility for back-end infrastructure.

NEW QUESTION: 102

Two hospitals merged into a single organization. The privacy officer requested a review of all records to ensure encryption was used during record storage, in compliance with regulations. During the review, the officer discovered that medical diagnosis codes and patient names were left unsecured. Which of the following types of data does this combination BEST represent?

- A. Personal health information
- B. Personally Identifiable Information
- C. Tokenized data
- D. Proprietary data

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 103

A security manager has tasked the security operations center with locating all web servers that respond to an unsecure protocol. Which of the following commands could an analyst run to find requested servers?

- A. nslookup 10.10.10.0
- B. no -1 -p 80
- C. nmap -p 80 10.10.10.0/24
- D. pathping 10.10.10.0 -p 80

Answer: ([SHOW ANSWER](#)**)**

Valid SY0-601 Dumps shared by Actual4test.com for Helping Passing SY0-601 Exam!
Actual4test.com now offer the **newest SY0-601 exam dumps**, the Actual4test.com SY0-601 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-601 dumps with Test Engine here:

https://www.actual4test.com/SY0-601_examcollection.html (**1061** Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)