Leads4Pass
https://www.leads4pass.com/sy0-701.html

SY0-701^{Q&As}

CompTIA Security+ 2024

Pass CompTIA SY0-701 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/sy0-701.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

An organization discovered files with proprietary financial data have been deleted. The files have been recovered from backup but every time the Chief Financial Officer logs in to the file server, the same files are deleted again No other users are experiencing this issue. Which of the following types of malware is MOST likely causing this behavior?

A. Logic bomb

B. Crypto malware

C. Spyware

D. Remote access Trojan

Correct Answer: A

Logic bomb: a set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out, usually with harmful effects.

QUESTION 2

The SOC for a large MSSP is meeting to discuss the lessons learned from a recent incident that took much too long to resolve This type of incident has become more common in recent weeks and is consuming large amounts of the analysts\\' time due to manual tasks being performed Which of the following solutions should the SOC consider to BEST improve its response time?

A. Configure a NIDS appliance using a Switched Port Analyzer

B. Collect OSINT and catalog the artifacts in a central repository

C. Implement a SOAR with customizable playbooks

D. Install a SIEM with community-driven threat intelligence

Correct Answer: C

SOAR (Security Orchestration, Automation, and Response) Can use either playbook or runbook. It assists in collecting threat related data from a range of sources and automate responses to low level threats. (frees up some of the CSIRT time)

QUESTION 3

Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

A. VM escape

B. SQL injection

C. Buffer overflow

D. Race condition

Correct Answer: C

A buffer overflow is a vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. A register is a small storage area in the CPU that holds temporary data or instructions. An attacker can exploit a buffer overflow to overwrite a register with a malicious address that points to a shellcode, which is a piece of code that gives the attacker control over the system. By doing so, the attacker can bypass the normal execution flow of the application and execute arbitrary commands.

References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Threats, Attacks, and Vulnerabilities, Section 2.3: Application Attacks, Page 76 1; Buffer Overflows - CompTIA Security+ SY0-701 - 2.3 2

QUESTION 4

A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?

A. Implementing a bastion host

B. Deploying a perimeter network

C. Installing a WAF

D. Utilizing single sign-on

Correct Answer: A

A bastion host is a special-purpose server that is designed to withstand attacks and provide secure access to internal resources. A bastion host is usually placed on the edge of a network, acting as a gateway or proxy to the internal network. A bastion host can be configured to allow only certain types of traffic, such as SSH or HTTP, and block all other traffic. A bastion host can also run security software such as firewalls, intrusion detection systems, and antivirus programs to monitor and filter incoming and outgoing traffic. A bastion host can provide administrative access to internal resources by requiring strong authentication and encryption, and by logging all activities for auditing purposes12. A bastion host is the most secure method among the given options because it minimizes the traffic allowed through the security boundary and provides a single point of control and defense. A bastion host can also isolate the internal network from direct exposure to the internet or other untrusted networks, reducing the attack surface and the risk of compromise3. Deploying a perimeter network is not the correct answer, because a perimeter network is a network segment that separates the internal network from the external network. A perimeter network usually hosts public-facing services such as web servers, email servers, or DNS servers that need to be accessible from the internet. A perimeter network does not provide administrative access to internal resources, but rather protects them from unauthorized access. A perimeter network can also increase the complexity and cost of network management and security4. Installing a WAF is not the correct answer, because a WAF is a security tool that protects web applications from common web-based attacks by monitoring, filtering, and blocking HTTP traffic. A WAF can prevent attacks such as cross-site scripting, SQL injection, or file inclusion, among others. A WAF does not provide administrative access to internal resources, but rather protects them from web application vulnerabilities. A WAF is also not a comprehensive solution for network security, as it only operates at the application layer and does not protect against other types of attacks or threats5. Utilizing single sign-on is not the correct answer, because single sign-on is a method of authentication that allows users to access multiple sites, services, or applications with one username and password. Single sign-on can simplify the sign-in process for users and reduce the number of passwords they have to remember and manage. Single sign-on does not provide administrative access to internal resources, but rather enables access to various resources that the user is authorized to use. Single sign-on can also introduce security risks if the user\'s credentials are compromised or if the single sign-on provider is breached6.

References: 1: Bastion host - Wikipedia, 2: 14 Best Practices to Secure SSH Bastion Host - goteleport.com, 3: The Importance Of Bastion Hosts In Network Security, 4: What is the network perimeter? | Cloudflare, 5: What is a WAF? | Web Application Firewall explained, 6: [What is single sign-on (SSO)? - Definition from WhatIs.com]

QUESTION 5

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following best describes this step?

A. Capacity planning

B. Redundancy

C. Geographic dispersion

D. Tablet exercise

Correct Answer: A

Capacity planning is the process of determining the resources needed to meet the current and future demands of an organization. Capacity planning can help a company develop a business continuity strategy by estimating how many staff members would be required to sustain the business in the case of a disruption, such as a natural disaster, a cyberattack, or a pandemic. Capacity planning can also help a company optimize the use of its resources, reduce costs, and improve performance.

References: CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 184. CompTIA Security+ (SY0- 701) Certification Exam Objectives, Domain 4.1, page 14. Business Continuity -SY0-601 CompTIA Security+ : 4.1

QUESTION 6

A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

A. Password spraying

B. Account forgery

C. Pass-t he-hash

D. Brute-force

Correct Answer: A

Password spraying is a type of brute force attack that tries common passwords across several accounts to find a match. It is a mass trial-and-error approach that can bypass account lockout protocols. It can give hackers access to personal or business accounts and information. It is not a targeted attack, but a high-volume attack tactic that uses a dictionary or

a list of popular or weak passwords12. The logs show that the attacker is using the same password ("password123") to attempt to log in to different accounts ("admin", "user1", "user2", etc.) on the same web server. This is a typical pattern of password spraying, as the attacker is hoping that at least one of the accounts has a weak password that matches the one they are trying. The attacker is also using a tool called Hydra, which is one of the most popular brute force tools, often used in cracking passwords for network authentication3. Account forgery is not the correct answer, because it involves creating fake accounts or credentials to impersonate legitimate users or entities. There is no evidence of account forgery in the logs, as the attacker is not creating any new accounts or using forged credentials. Pass-the-hash is not the correct answer, because it involves stealing a hashed user credential and using it to create a new authenticated session on the same network. Pass- the-hash does not require the attacker to know or crack the password, as they use the stored version of the password to initiate a new session4. The logs show that the attacker is using plain text passwords, not hashes, to try to log in to the web server. Brute-force is not the correct answer, because it is a broader term that encompasses different types of attacks that involve trying different variations of symbols or words until the correct password is found. Password spraying is a specific type of brute force attack that uses a single common password against multiple accounts5. The logs show that the attacker is using password spraying, not brute force in general, to try to gain access to the web server.

References: 1: Password spraying: An overview of password spraying attacks ... - Norton, 2: Security: Credential Stuffing vs. Password Spraying - Baeldung, 3: Brute Force Attack: A definition + 6 types to know | Norton, 4: What is a Pass-the-Hash Attack? - CrowdStrike, 5: What is a Brute Force Attack? | Definition, Types and How It Works - Fortinet

QUESTION 7

An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

A. ACL

B. DLP

C. IDS

D. IPS

Correct Answer: D

An intrusion prevention system (IPS) is a security device that monitors network traffic and blocks or modifies malicious packets based on predefined rules or signatures. An IPS can prevent attacks that exploit known vulnerabilities in older browser versions by detecting and dropping the malicious packets before they reach the target system. An IPS can also perform other functions, such as rate limiting, encryption, or redirection.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

QUESTION 8

A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

A. Active

B. Passive

C. Defensive

D. Offensive

Correct Answer: A

Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they involve probing the target for specific information.

References: CompTIA Security+ Certification Exam Objectives, Domain 1.1: Given a scenario, conduct reconnaissance using appropriate techniques and tools. CompTIA Security+ Study Guide (SY0-701), Chapter 2: Reconnaissance and Intelligence Gathering, page 47. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 1.

QUESTION 9

During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?

A. Analysis

B. Lessons learned

C. Detection

D. Containment

Correct Answer: A

Analysis is the incident response activity that describes the process of understanding the source of an incident. Analysis involves collecting and examining evidence, identifying the root cause, determining the scope and impact, and assessing the threat actor\'s motives and capabilities. Analysis helps the incident response team to formulate an appropriate response strategy, as well as to prevent or mitigate future incidents. Analysis is usually performed after detection and before containment, eradication, recovery, and lessons learned.

References: CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 223. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.2, page 13.

QUESTION 10

A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?

A. MSA

B. SLA

C. BPA

D. SOW

Correct Answer: D

An ISOW is a document that outlines the project, the cost, and the completion time frame for a security company to provide a service to a client. ISOW stands for Information Security Operations Work, and it is a type of contract that specifies the scope, deliverables, milestones, and payment terms of a security project. An ISOW is usually used for one-time or short-term projects that have a clear and defined objective and outcome. For example, an ISOW can be used for a security assessment, a penetration test, a security audit, or a security training. The other options are not correct because they are not documents that outline the project, the cost, and the completion time frame for a security company to provide a service to a client. A MSA is a master service agreement, which is a type of contract that establishes the general terms and conditions for a long-term or ongoing relationship between a security company and a client. A MSA does not specify the details of each individual project, but rather sets the framework for future projects that will be governed by separate statements of work (SOWs). A SLA is a service level agreement, which is a type of contract that defines the quality and performance standards for a security service provided by a security company to a client. A SLA usually includes the metrics, targets, responsibilities, and penalties for measuring and ensuring the service level. A BPA is a business partnership agreement, which is a type of contract that establishes the roles and expectations for a strategic alliance between two or more security companies that collaborate to provide a joint service to a client. A BPA usually covers the objectives, benefits, risks, and obligations of the partnership.

References: CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 387. Professor Messer\'s CompTIA SY0-701 Security+ Training Course, Section 8.2: Compliance and Controls, video: Contracts and Agreements (5:12).

QUESTION 11

A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of end users. Which of the following would be a good use case for this task?

A. Off-the-shelf software

B. Orchestration

C. Baseline

D. Policy enforcement

Correct Answer: B

Orchestration is the process of automating multiple tasks across different systems and applications. It can help save time and reduce human error by executing predefined workflows and scripts. In this case, the systems administrator can use orchestration to create accounts for a large number of end users without having to manually enter their information and assign permissions.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 457 1

QUESTION 12

A security practitioner completes a vulnerability assessment on a company\'s network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done next?

A. Conduct an audit.

B. Initiate a penetration test.

C. Rescan the network.

D. Submit a report.

Correct Answer: C

After completing a vulnerability assessment and remediating the identified vulnerabilities, the next step is to rescan the network to verify that the vulnerabilities have been successfully fixed and no new vulnerabilities have been introduced. A vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network, system, or application that could be exploited by attackers. A vulnerability assessment typically involves using automated tools, such as scanners, to scan the network and generate a report of the findings. The report may include information such as the severity, impact, and remediation of the vulnerabilities. The operations team is responsible for applying the appropriate patches, updates, or configurations to address the vulnerabilities and reduce the risk to the network. A rescan is necessary to confirm that the remediation actions have been effective and that the network is secure. Conducting an audit, initiating a penetration test, or submitting a report are not the next steps after completing a vulnerability assessment and remediating the vulnerabilities. An audit is a process of reviewing and verifying the compliance of the network with the established policies, standards, and regulations. An audit may be performed by internal or external auditors, and it may use the results of the vulnerability assessment as part of the evidence. However, an audit is not a mandatory step after a vulnerability assessment, and it does not validate the effectiveness of the remediation actions. A penetration test is a process of simulating a real-world attack on the network to test the security defenses and identify any gaps or weaknesses. A penetration test may use the results of the vulnerability assessment as a starting point, but it goes beyond scanning and involves exploiting the vulnerabilities to gain access or cause damage. A penetration test may be performed after a vulnerability assessment, but only with the proper authorization, scope, and rules of engagement. A penetration test is not a substitute for a rescan, as it does not verify that the vulnerabilities have been fixed. Submitting a report is a step that is done after the vulnerability assessment, but before the remediation. The report is a document that summarizes the findings and recommendations of the vulnerability assessment, and it is used to communicate the results to the stakeholders and the operations team. The report may also include a follow-up plan and a timeline for the remediation actions. However, submitting a report is not the final step after the remediation, as it does not confirm that the network is secure.

References: CompTIA Security+ SY0-701 Certification Study Guide, page 372- 375; Professor Messer\\'s CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 0:00 - 8:00.

QUESTION 13

A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider first?

A. Local data protection regulations

B. Risks from hackers residing in other countries

C. Impacts to existing contractual obligations

D. Time zone differences in log correlation

Correct Answer: A

Local data protection regulations are the first thing that a cloud-hosting provider should consider before expanding its data centers to new international locations. Data protection regulations are laws or standards that govern how personal or sensitive data is collected, stored, processed, and transferred across borders. Different countries or regions may have different data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, or the California Consumer Privacy Act (CCPA) in the United States. A cloud-hosting provider must comply with the local data protection regulations of the countries or regions where it operates or serves customers, or else it may face legal penalties, fines, or reputational damage. Therefore, a cloud-hosting provider should research and understand the local data protection regulations of the new international locations before expanding its data centers there.

References: CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 7, page 269. CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1, page 14.

QUESTION 14

Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?

A. Insider

B. Unskilled attacker

C. Nation-state

D. Hacktivist

Correct Answer: C

A nation-state is a threat actor that is sponsored by a government or a political entity to conduct cyberattacks against other countries or organizations. Nation- states have large financial resources, advanced technical skills, and strategic objectives that may target critical systems such as military, energy, or infrastructure. Nation-states are often motivated by espionage, sabotage, or warfare12.

References: 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Threat Actors -CompTIA Security+ SY0-701 ?2.1, video by Professor Messer.

QUESTION 15

A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

A. Packet captures

B. Vulnerability scans

C. Metadata

D. Dashboard

Correct Answer: D

A dashboard is a graphical user interface that provides a visual representation of key performance indicators, metrics, and trends related to security events and incidents. A dashboard can help the board of directors to understand the number and impact of incidents that affected the organization in a given period, as well as the status and effectiveness of the security controls and processes. A dashboard can also allow the board of directors to drill down into specific details or filter the data by various criteria12. A packet capture is a method of capturing and analyzing the network traffic that passes through a device or a network segment. A packet capture can provide detailed information about the source, destination, protocol, and content of each packet, but it is not a suitable way to present a summary of incidents to the board of directors13. A vulnerability scan is a process of identifying and assessing the weaknesses and exposures in a system or a network that could be exploited by attackers. A vulnerability scan can help the organization to prioritize and remediate the risks and improve the security posture, but it is not a relevant way to report the number of incidents that occurred in a quarter14. Metadata is data that describes other data, such as its format, origin, structure, or

context. Metadata can provide useful information about the characteristics and properties of data, but it is not a meaningful way to communicate the impact and frequency of incidents to the board of directors.

References: 1: CompTIA Security+ SY0-701 Certification Study Guide, page 3722: SIEM Dashboards -SY0-601 CompTIA Security+ : 4.3, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 3464: CompTIA Security+ SY0-701 Certification Study Guide, page 362. : CompTIA Security+ SY0-701 Certification Study Guide, page 97.

Latest SY0-701 Dumps   SY0-701 Practice Test   SY0-701 Exam Questions