Vendor: CompTIA

Exam Code:SY0-701

Exam Name: CompTIA Security+ 2024

Version: Demo

QUESTION 1

A systems administrator is working on a solution with the following requirements:

Provide a secure zone.

Enforce a company-wide access control policy.

Reduce the scope of threats.

Which of the following is the systems administrator setting up?

A. Zero Trust

B. AAA

C. Non-repudiation

D. CIA

Correct Answer: A

Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company- wide access control policy by applying the principle of least privilege and granular segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.

References:

5: This source explains the concept and benefits of Zero Trust security and how it differs from traditional security models.

8: This source provides an overview of Zero Trust identity security and how it can help verify the identity and integrity of users and devices.

QUESTION 2

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 3

An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?

A. Smishing

B. Disinformation

C. Impersonating

D. Whaling

Correct Answer: D

Whaling is a type of phishing attack that targets high-profile individuals, such as executives, celebrities, or politicians. The attacker impersonates someone with authority or influence and tries to trick the victim into performing an action, such as transferring money, revealing sensitive information, or clicking on a malicious link. Whaling is also called CEO fraud or business email compromise2.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 97.

QUESTION 4

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

A. Insurance

B. Patching

C. Segmentation

D. Replacement

Correct Answer: C

Segmentation is a technique that divides a network into smaller subnetworks or segments, each with its own security policies and controls. Segmentation can help mitigate network access vulnerabilities in legacy IoT devices by isolating them from other devices and systems, reducing their attack surface and limiting the potential impact of a breach. Segmentation can also improve network performance and efficiency by reducing congestion and traffic. Patching, insurance, and replacement are other possible strategies to deal with network access vulnerabilities, but they may not be feasible or effective in the short term. Patching may not be available or compatible for legacy IoT devices, insurance may not cover the costs or damages of a cyberattack, and replacement may be expensive and time-consuming.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143

QUESTION 5

Which of the following teams combines both offensive and defensive testing techniques to protect an organization\\'s critical systems?

A. Red

B. Blue

C. Purple

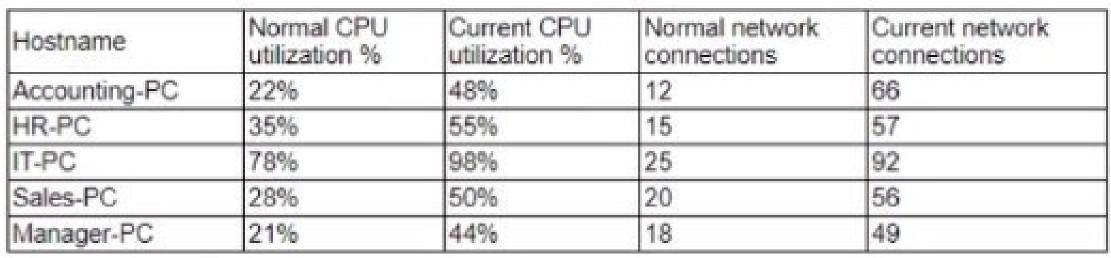
D. Yellow

Correct Answer: C

Purple is the team that combines both offensive and defensive testing techniques to protect an organization\\'s critical systems. Purple is not a separate team, but rather a collaboration between the red team and the blue team. The red team is the offensive team that simulates attacks and exploits vulnerabilities in the organization\\'s systems. The blue team is the defensive team that monitors and protects the organization\\'s systems from real and simulated threats. The purple team exists to ensure and maximize the effectiveness of the red and blue teams by integrating the defensive tactics and controls from the blue team with the threats and vulnerabilities found by the red team into a single narrative that improves the overall security posture of the organization. Red, blue, and yellow are other types of teams involved in security testing, but they do not combine both offensive and defensive techniques. The yellow team is the team that builds software solutions, scripts, and other programs that the blue team uses in the security testing. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1331; Penetration Testing: Understanding Red, Blue, and Purple Teams3

QUESTION 6

Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a secunty 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. The ISP is dropping outbound connections

B. The user of the Sales-PC fell for a phishing attack

C. Corporate PCs have been turned into a botnet

D. An on-path attack is taking place between PCs and the router

Correct Answer: C

The metrics show a significant increase in both CPU utilization and network connections for all the listed PCs compared to their normal values. This could indicate that the machines are being used for unauthorized activities. The current CPU utilization of all the PCs is significantly higher than the normal CPU utilization. This indicates that the PCs are running a lot of processes, which is a common symptom of a botnet infection. The number of current network connections for all the PCs is also significantly higher than the normal number of network connections. This is another common symptom of a botnet infection. A botnet is a network of computers that have been infected with malware and controlled by a remote attacker. The attacker can use the botnet to carry out a variety of malicious activities, such as sending spam, launching DDoS attacks, or stealing data.

QUESTION 7

Which of the following is used to validate a certificate when it is presented to a user?

A. OCSP

B. CSR

C. CA

D. CRC

Correct Answer: A

OCSP stands for Online Certificate Status Protocol. It is a protocol that allows applications to check the revocation status of a certificate in real-time. It works by sending a query to an OCSP responder, which is a server that maintains a database of revoked certificates. The OCSP responder returns a response that indicates whether the certificate is valid, revoked, or unknown. OCSP is faster and more efficient than downloading and parsing Certificate Revocation Lists (CRLs), which are large files that contain the serial numbers of all revoked certificates issued by a Certificate Authority (CA).

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 337 1

QUESTION 8

An organization disabled unneeded services and placed a firewall in front of a business- critical legacy system. Which of the following best describes the actions taken by the organization?

A. Exception

B. Segmentation

C. Risk transfer

D. Compensating controls

Correct Answer: D

Compensating controls are alternative security measures that are implemented when the primary controls are not feasible, cost-effective, or sufficient to mitigate the risk. In this case, the organization used compensating controls to protect the

legacy system from potential attacks by disabling unneeded services and placing a firewall in front of it. This reduced the attack surface and the likelihood of exploitation.

References:

Official CompTIA Security+ Study Guide (SY0-701), page 29 Security Controls - CompTIA Security+ SY0-701 - 1.1 1

QUESTION 9

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device. Which of the following best describes the user\\'s activity?

A. Penetration testing

B. Phishing campaign

C. External audit

D. Insider threat

Correct Answer: D

An insider threat is a security risk that originates from within the organization, such as an employee, contractor, or business partner, who has authorized access to the organization\\'s data and systems. An insider threat can be malicious, such as stealing, leaking, or sabotaging sensitive data, or unintentional, such as falling victim to phishing or social engineering. An insider threat can cause significant damage to the organization\\'s reputation, finances, operations, and legal compliance. The user\\'s activity of logging in remotely after hours and copying large amounts of data to a personal device is an example of a malicious insider threat, as it violates the organization\\'s security policies and compromises the confidentiality and integrity of the data.

References: Insider Threats -CompTIA Security+ SY0-701: 3.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 133.

QUESTION 10

Which of the following provides the details about the terms of a test with a third-party penetration tester?

A. Rules of engagement

B. Supply chain analysis

C. Right to audit clause

D. Due diligence

Correct Answer: A

Rules of engagement are the detailed guidelines and constraints regarding the execution of information security testing, such as penetration testing. They define the scope, objectives, methods, and boundaries of the test, as well as the roles

and responsibilities of the testers and the clients. Rules of engagement help to ensure that the test is conducted in a legal, ethical, and professional manner, and that the results are accurate and reliable. Rules of engagement typically include

the following elements:

The type and scope of the test, such as black box, white box, or gray box, and the target systems, networks, applications, or data.

The client contact details and the communication channels for reporting issues, incidents, or emergencies during the test.

The testing team credentials and the authorized tools and techniques that they can use.

The sensitive data handling and encryption requirements, such as how to store, transmit, or dispose of any data obtained during the test. The status meeting and report schedules, formats, and recipients, as well as the confidentiality and nondisclosure agreements for the test results. The timeline and duration of the test, and the hours of operation and testing windows.

The professional and ethical behavior expectations for the testers, such as avoiding unnecessary damage, disruption, or disclosure of information. Supply chain analysis, right to audit clause, and due diligence are not related to the terms of a

test with a third-party penetration tester. Supply chain analysis is the process of evaluating the security and risk posture of the suppliers and partners in a business network. Right to audit clause is a provision in a contract that gives one party

the right to audit another party to verify their compliance with the contract terms and conditions. Due diligence is the process of identifying and addressing the cyber risks that a potential vendor or partner brings to an organization.

References: https://www.yeahhub.com/every-penetration-tester-you-should-know-about- this-rules-of-engagement/

https://bing.com/search?q=rules+of+engagement+penetration+testing

---

QUESTION 11

A systems administrator set up a perimeter firewall but continues to notice suspicious connections between internal endpoints. Which of the following should be set up in order to mitigate the threat posed by the suspicious activity?

A. Host-based firewall

B. Web application firewall

C. Access control list

D. Application allow list

Correct Answer: A

A host-based firewall is a software application that runs on an individual endpoint and filters the incoming and outgoing network traffic based on a set of rules. A host-based firewall can help to mitigate the threat posed by suspicious connections between internal endpoints by blocking or allowing the traffic based on the source, destination, port, protocol, or application. A host-based firewall is different from a web application firewall, which is a type of firewall that protects web applications from common web-based attacks, such as SQL injection, cross-site scripting, and session hijacking. A host-based firewall is also different from an access control list, which is a list of rules that control the access to network resources, such as files, folders, printers, or routers. A host- based firewall is also different from an application allow list, which is a list of applications that are authorized to run on an endpoint, preventing unauthorized or malicious applications from executing.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 254

QUESTION 12

Which of the following can be used to identify potential attacker activities without affecting production servers?

A. Honey pot

B. Video surveillance

C. Zero Trust

D. Geofencing

Correct Answer: A

A honey pot is a system or a network that is designed to mimic a real production server and attract potential attackers. A honey pot can be used to identify the attacker\\'s methods, techniques, and objectives without affecting the actual production servers. A honey pot can also divert the attacker\\'s attention from the real targets and waste their time and resources12. The other options are not effective ways to identify potential attacker activities without affecting production servers: Video surveillance: This is a physical security technique that uses cameras and monitors to record and observe the activities in a certain area. Video surveillance can help to deter, detect, and investigate physical intrusions, but it does not directly identify the attacker\\'s activities on the network or the servers3. Zero Trust: This is a security strategy that assumes that no user, device, or network is trustworthy by default and requires strict verification and validation for every request and transaction. Zero Trust can help to improve the security posture and reduce the attack surface of an organization, but it does not directly identify the attacker\\'s activities on the network or the servers4. Geofencing: This is a security technique that uses geographic location as a criterion to restrict or allow access to data or resources. Geofencing can help to protect the data sovereignty and compliance of an organization, but it does not directly identify the attacker\\'s activities on the network or the servers5.

References: 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Honeypots and Deception -SY0-601 CompTIA Security+ : 2.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 985: CompTIA Security+ SY0-701 Certification Study Guide, page 99.