Vendor: CompTIA

Exam Code:SY0-601

Exam Name: CompTIA Security+

Version: Demo

QUESTION 1

A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?

A. Evil twin

B. Jamming

C. DNS poisoning

D. Bluesnarfing

E. DDoS

Correct Answer: A

In an Evil Twin attack, the attacker sets up a rogue wireless access point (WAP) with the same SSID as a legitimate WAP to mimic it and trick users into connecting to the rogue WAP. The rogue WAP is configured to perform various malicious activities, such as intercepting sensitive data, stealing credentials, and performing man-in-the-middle attacks.

In this scenario, the large amount of sensitive data being downloaded from various mobile devices to an external site is likely being intercepted and exfiltrated by the attacker via the rogue WAP. The "impossible travel times" in successful login attempts indicate that the attacker is likely performing man-in-the-middle attacks, intercepting user login credentials, and using them to access the company\\'s internal resources and download the sensitive data.

The presence of two WAPs using the same SSID with non-standard DHCP configurations and overlapping channels suggests the existence of the rogue WAP, which is characteristic of an Evil Twin attack.

QUESTION 2

Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

A. Hashing

B. Salting

C. Integrity

D. Digital signature

Correct Answer: A

File verification, also known as hashing, is the process of checking that a file you have on your machine is identical to the source file... When you hash a file, you are left with a checksum, a random alpha numeric string with a set length. Hashing a file doesn\\'t encrypt the file and you can\\'t take a checksum and run it back through an algorithm to get the original source file.

QUESTION 3

Which of the following methods is the most effective for reducing vulnerabilities?

A. Joining an information-sharing organization

B. Using a scan-patch-scan process

C. Implementing a bug bounty program

D. Patching low-scoring vulnerabilities first

Correct Answer: B

Vulnerability scanning: Conducting regular vulnerability scans to identify potential security weaknesses in the organization\\'s systems, networks, and applications.

Patching: Addressing the identified vulnerabilities by applying the necessary security patches and updates to the affected systems. Patching helps to close the known security holes that could be exploited by attackers.

Re-scanning: After applying the patches, conducting another round of vulnerability scanning to verify that the identified vulnerabilities have been properly addressed and that the systems are no longer at risk.

QUESTION 4

Accompany has a flat network that is deployed in the cloud. Security policy states that all production and development servers must be segmented. Which of the following should be used to design the network to meet the security requirements?

A. CASB

B. VPC

C. Perimeter network

D. WAF

Correct Answer: B

"Security policy states that all production and development servers must be segmented" which can be achieved by using a VPC

QUESTION 5

A Chief Security Officer (CSO) is concerned about the volume and integrity of sensitive information that is exchanged between the organization and a third party through email. The CSO is particularly concerned about an unauthorized party who is intercepting information that is in transit between the two organizations.

Which of the following would address the CSO\\'s concerns?

A. SPF

B. DMARC

C. SSL

D. DKIM

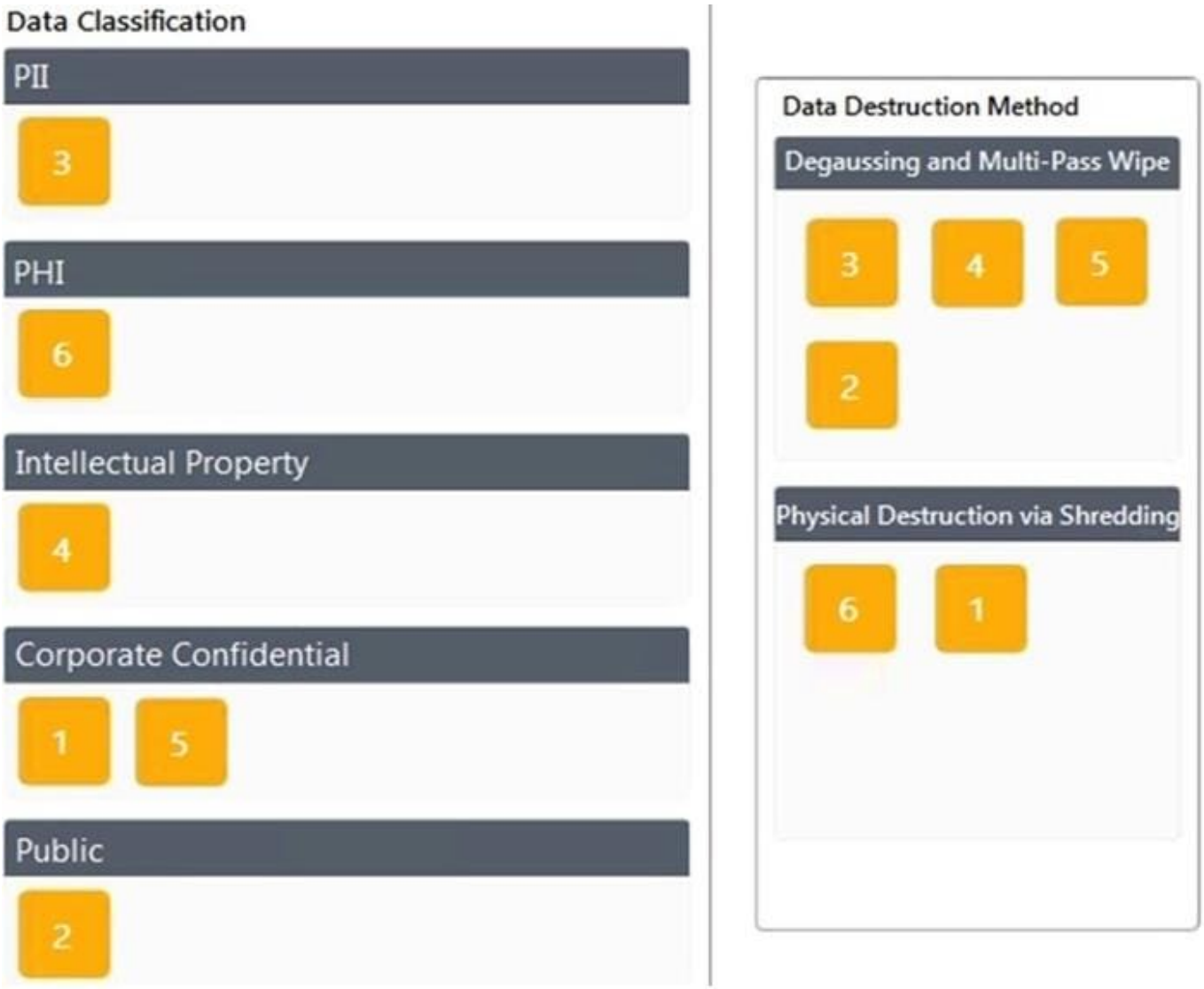
E. TLS

Correct Answer: E

DKIM (DomainKeys Identified Mail) is a protocol that allows an organization to take responsibility for transmitting a message by signing it in a way that mailbox providers can verify. DKIM record verification is made possible through cryptographic authentication. Transport Layer Security (TLS) encrypts data sent over the Internet to ensure that eavesdroppers and hackers are unable to see what you transmit which is particularly useful for private and sensitive information such as passwords, credit card numbers, and personal correspondence

---

QUESTION 6



DRAG DROP

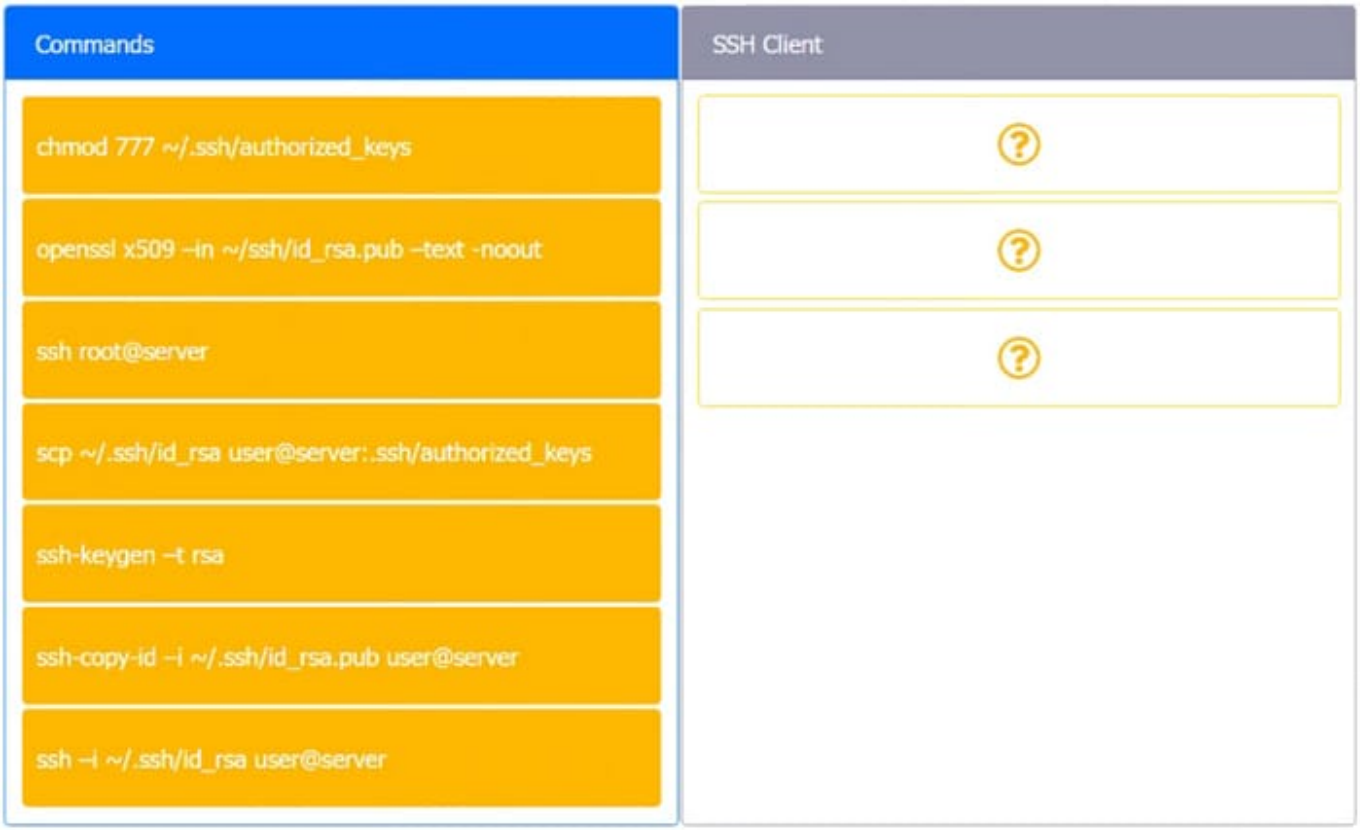
A security engineer is setting up passwordless authentication for the first time.

INSTRUCTIONS

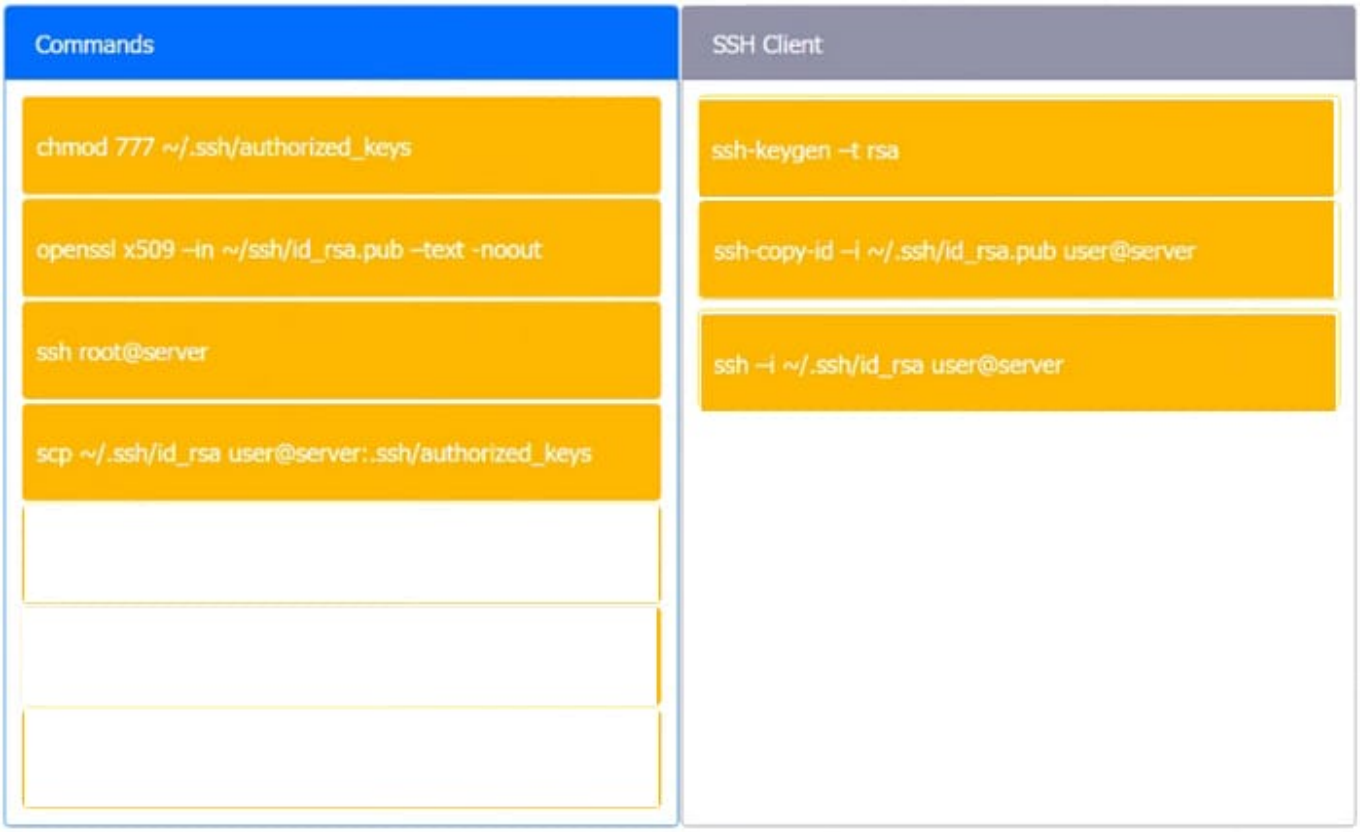
Drag and drop the MINIMUM set of commands to set this up and verify that it works. Commands may only be used once, and not all will be used.

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

Select and Place:



Correct Answer:



QUESTION 7

A company uses specially configured workstations for any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery. Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced. Which of the following MOST likely occurred?

A. Fileless malware

B. A downgrade attack

C. A supply-chain attack

D. A logic bomb

E. Misconfigured BIOS

Correct Answer: C

QUESTION 8

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

1.

A user enters comptia.org into a web browser.

2.

The website that appears is not the comptia.org site.

3.

The website is a malicious site from the attacker.

4.

Users in a different office are not having this issue.

Which of the following types of attacks was observed?

A. On-path attack

B. DNS poisoning

C. Locator (URL) redirection

D. Domain hijacking

Correct Answer: B

Only some client have this problem about web tarns to malicious site. So choose B.

QUESTION 9

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. Time-based logins

B. Geofencing

C. Network location

D. Password history

Correct Answer: A

Time based logins should be the answer because Geofencing is accepting or rejecting access requests based on location.

QUESTION 10

An annual information security assessment has revealed that several OS-level configurations are not in compliance due to outdated hardening standards the company is using. Which of the following would be BEST to use to update and reconfigure the OS-level security configurations?

A. CIS benchmarks

B. GDPR guidance

C. Regional regulations

D. ISO 27001 standards

Correct Answer: A

CIS Benchmarks for mobile devices cover security configurations for operating systems that run on mobile phones, tablets, and other hand-held devices.

ISO/IEC 27001 is an Information security management standard that structures how businesses should manage risk associated with information security threats;

The General Data Protection Regulation sets guidelines for the collection and processing of personal data of individuals within the European Union; its about how organizations should handle the personal data of individuals

https://www.beyondtrust.com/resources/glossary/systems-hardening

---

QUESTION 11

A network administrator has been asked to install an IDS to improve the security posture of an organization.

Which of the following control types is an IDS?

A. Corrective

B. Physical

C. Detective

D. Administrative

Correct Answer: C

Intrusion DECECTION system.. DETECTION, as in sherlock holmes. Imagine sherlock holmes smoking a big fat bowl and you\\'ll always answer this correctly

---

QUESTION 12

Which of the following should a data owner require all personnel to sign to legally protect intellectual property?

A. An NDA

B. An AUP

C. An ISA

D. An MOU

Correct Answer: A