# Download Eccouncil ECSS Exam Dumps Free

**Shared by Dodson on 17-06-2026**

**For More Free Questions and Preparation Resources**

Check the Links on Last Page

# Question 1

Question Type: MultipleChoice

Below are the various steps involved in establishing a network connection using the shared key authentication process.

l .The AP sends a challenge text to the station.

2 .The station connects to the network.

3 .The station encrypts the challenge text using its configured 128-bit key and sends the encrypted text to the AP.

4 .The station sends an authentication frame to the AP.

5 .The AP uses its configured WEP key to decrypt the encrypted text and compares it with the original challenge text.

What is the correct sequence of steps involved in establishing a network connection using the shared key authentication process?

## Options:

A- 2 >4 >3
B- 4--->2--->1--->3--->5
C- 4--->1--->3--->5--->2
D- 4-->5->3->2-->1

## Answer:

C

## Explanation:

The AP sends a challenge text to the station.

The Access Point (AP) initiates the authentication process by sending a challenge text to the station (client device).

The station connects to the network.

The station (client device) associates with the wireless network by connecting to the AP.

The station encrypts the challenge text using its configured 128-bit key and sends the encrypted text to the AP.

The station encrypts the challenge text using the shared secret key (configured on both the station and the AP).

It then sends the encrypted challenge text back to the AP.

The station sends an authentication frame to the AP.

The station constructs an authentication frame containing the encrypted challenge text.

This frame is sent to the AP for verification.

The AP uses its configured WEP key to decrypt the encrypted text and compares it with the original challenge text.

The AP decrypts the received encrypted challenge text using its configured WEP (Wired Equivalent Privacy) key.

If the decrypted text matches the original challenge text, the station is authenticated successfully.

Therefore, the correct sequence isC. 4--->1--->3--->5--->21. This order ensures that the challenge text is exchanged securely and verified by both the station and the AP during the shared key authentication process.

EC-Council Certified Security Specialist (E|CSS) documents and study guide.

EC-Council Certified Security Specialist (E|CSS) course materials1234

# Question 2

Question Type: MultipleChoice

A type of malware allows an attacker to trick the target entity into performing a predefined action, and upon its activation, it grants the attacker unrestricted access to all the data stored on the compromised system.

Which of the following is this type of malware?

## Options:

A- Key log ger
B- Botnet
C- Worm
D- Trojan

## Answer:

D

## Explanation:

ATrojan(short for ''Trojan horse'') is one of the most insidious types of malware. Trojans disguise themselves as legitimate software programs, such as a game or utility, while secretly damaging the host device. Unlike viruses and worms, Trojans mainly use social engineering techniques to replicate themselves, fooling victims into downloading and installing them.

EC-Council Certified Security Specialist (E|CSS) course materials and study guide12.



# Question 3

Question Type: MultipleChoice

Clark is an unskilled hacker attempting to perform an attack on a target organization to gain popularity. He downloaded and used freely available hacking tools and software developed by other professional hackers for this purpose.

Identify the type of threat actor described in the above scenario.

## Options:

A- Script kiddie
B- industrial spy
C- Hacktivist
D- Cyber terrorist



## Answer:

A

## Explanation:

Ascript kiddieis an unskilled individual who uses pre-written hacking tools and software to perform attacks without fully understanding the underlying techniques.They often seek attention or popularity by exploiting vulnerabilities using readily available tools.Reference: EC-Council Certified Security Specialist (E|CSS) documents and study guide12.

# Question 4

Question Type: MultipleChoice

While investigating a web attack on a Windows-based server, Jessy executed the following command on her system:

C:\> net view <10.10.10.11>

What was Jessy's objective in running the above command?

## Options:

A- Verify the users using open sessions
B- Check file space usage to look for a sudden decrease in free space
C- Check whether sessions have been opened with other systems
D- Review file shares to ensure their purpose

## Answer:

D

## Explanation:

Thenet viewcommand in Windows is used to display a list of resources being shared on a computer.When used with a specific computer name or IP address, as innet view <10.10.10.11>, it displays the shared resources available on that particular computer1. Jessy's objective in running this command was likely to review the file shares on the server with the IP address 10.10.10.11 to ensure that they are correctly purposed and not maliciously altered or added as part of the web attack.

This command does not verify users using open sessions, check file space usage, or check whether sessions have been opened with other systems. Instead, it specifically lists the shared resources, which can include file shares and printer shares, providing insight into what is being shared from the server in question. This information is crucial during a forensic investigation of a web attack to understand if and how the server's shared resources were compromised or utilized by the attacker.

# Question 5

Question Type: MultipleChoice

Below are the various steps involved in an email crime investigation.

1.Acquiring the email data

2.Analyzing email headers

3.Examining email messages

4.Recovering deleted email messages

5.Seizing the computer and email accounts

6.Retrieving email headers

What is the correct sequence of steps involved in the investigation of an email crime?

## Options:

A- 5->l->3->6-->2 >4
B- 2->4->3-->6->5-->l
C- 1--->3->4--->2-->5'>6
D- 5 -> 1 -> 6 -> 2 -> 3 -> 4

## Answer:

D

## Explanation:

Seizing the computer and email accounts (Step 5): This is the initial step to secure potential evidence. It involves physically or remotely seizing the suspect's computer and email accounts to prevent tampering.

Acquiring the email data (Step 1): After seizing the devices, investigators acquire the email data. This includes collecting email files, attachments, and metadata.

Retrieving email headers (Step 6): Email headers contain valuable information such as sender IP addresses, timestamps, and routing details. Retrieving headers helps trace the email's origin.

Analyzing email headers (Step 2): Investigators analyze the headers to identify any anomalies, spoofing, or suspicious patterns.

Examining email messages (Step 3): Investigators review the actual email content, attachments, and any embedded links. This step helps understand the context and intent.

Recovering deleted email messages (Step 4): Deleted emails may contain critical evidence. Investigators use specialized tools to recover deleted messages.

EC-Council Certified Security Specialist (E|CSS) documents and study guide.

EC-Council Certified Security Specialist (E|CSS) course materials123

# Question 6

Question Type: MultipleChoice

Messy, a network defender, was hired to secure an organization's internal network. He deployed an IDS in which the detection process depends on observing and comparing the observed events with the normal behavior and then detecting any deviation from it.

Identify the type of IDS employed by Messy in the above scenario.

## Options:

A- Stateful protocol analysis
B- Anomaly-based
C- Signature-based
D- Application proxy

## Answer:

B

## Explanation:

Messy has deployed ananomaly-basedIntrusion Detection System (IDS). This type of IDS observes and compares observed events with normal behavior, detecting deviations from the established patterns.It identifies anomalies that may indicate potential security threats.Reference: EC-Council Certified Security Specialist (E|CSS) course materials12.

# Question 7

Question Type: MultipleChoice

Bob, a forensic investigator, is investigating a live Windows system found at a crime scene. In this process, Bob extracted subkeys containing information such as SAM. Security, and software using an automated tool called FTK Imager.

Which option best Windows Registry hives' subkeys provide the above information to Bob?

## Options:

A- H KEY-CLASSES. ROOT
B- HKEY .CURRENT CONFIG
C- HKEY CURRENT USER
D- HKEY LOCAL MACHINE

## Answer:

D

## Explanation:

Certainly! Let's break down the question and identify which Windows Registry hives' subkeys contain the requested information.

Windows Registry Hives:

The Windows Registry is a hierarchical database that holds configuration settings and options for both low-level operating system components and running programs.

It includes settings for the kernel, device drivers, services, user interface, and third-party applications.

The registry allows access to counters for system performance profiling.

Registry Hives:

The registry is organized into different hives, each containing keys and values.

Some important hives include:

HKEY_LOCAL_MACHINE (HKLM): Contains system-wide settings.

HKEY_CURRENT_USER (HKCU): Contains settings specific to the currently logged-in user.

HKEY_USERS (HKU): Contains profiles for all users on the system.

HKEY_CLASSES_ROOT (HKCR): Contains file association information.

HKEY_CURRENT_CONFIG (HKCC): Contains information about the current hardware configuration (only in certain Windows versions).

Subkeys Relevant to Bob's Investigation:

Bob is interested in information related toSAM,Security, andsoftware.

Let's see which hives contain these subkeys:

SAM(Security Account Manager):

The SAM hive stores user account information, including usernames, passwords, account types, enabled status, group memberships, and last logon time.

It is crucial for authentication and security.

Located in:HKEY_LOCAL_MACHINE\SAM

Security:

The Security hive contains security-related information, including access control lists (ACLs), user privileges, and security tokens.

It plays a vital role in enforcing security policies.

Located in:HKEY_LOCAL_MACHINE\Security

Software:

The Software subkey within the HKLM hive contains information related to installed software, configurations, and settings.

It is essential for forensic investigations.

Located in:HKEY_LOCAL_MACHINE\Software

Answer :

The subkeys that provide the requested information to Bob are:

SAM(located inHKEY_LOCAL_MACHINE\SAM)

Security(located inHKEY_LOCAL_MACHINE\Security)

# Question 8

Question Type: MultipleChoice

Stephen, a security specialist, was instructed to identify emerging threats on the organization's network. In this process, he employed a computer system on the Internet intended to attract and trap those who attempt unauthorized host system utilization to penetrate the organization's network.

Identify the type of security solution employed by Stephen in the above scenario.

## Options:

A- Firewall
B- IDS
C- Honeypot
D- Proxy server

## Answer:

C

## Explanation:

Stephen employed ahoneypotin the given scenario. A honeypot is a simulation of an IT system or software application that acts as bait to attract the attention of attackers. While it appears to be a legitimate target, it is actually fake and carefully monitored by an IT security team.The purpose of a honeypot includes distraction for attackers, threat intelligence gathering, and research/training for IT security professionals1.

EC-Council Certified Security Specialist (E|CSS) documents and study guide1.

# Question 9

Question Type: MultipleChoice

Kalley, a shopping freak, often visits different e commerce websites from her office system. One day, she received a free software on her mail with the claim that it is loaded with new clothing offers. Tempted by this, Kalley downloaded the malicious software onto her system. The software infected Kalley's system and began spreading the infection to other systems connected to the network.

Identify the threat source through which Kalley unintentionally invited the malware into the network?

## Options:

A- File sharing services
B- Portable hardware media
C- insecure patch management
D- Decoy application

## Answer:

D

## Explanation:

Kalley's actions inadvertently introduced malware into the network. Here's how:

Decoy Application:

Adecoy applicationis a seemingly legitimate software or tool that disguises itself as something useful or appealing.

In Kalley's case, she received an email claiming that the software was loaded with new clothing offers. Tempted by this, she downloaded it.

Unfortunately, the software turned out to bemalicious, infecting her system.

Decoy applications often exploit users' curiosity or desire for freebies, enticing them to install harmful software.

EC-Council Certified Security Specialist (E|CSS) documents and course materials.

# Question 10

Question Type: MultipleChoice

Ben, a computer user, applied for a digital certificate. A component of PKI verifies Ben's identity using the credentials provided and passes that request on behalf of Ben to grant the digital certificate.

Which option best PKI components verified Ben as being legitimate to receive the certificate?

## Options:

A- Certificate directory
B- Validation authority (VA)
C- Certificate authority (CA)
D- Registration authority (RA)

## Answer:

D

## Explanation:

In the context of Public Key Infrastructure (PKI), theRegistration Authority (RA)plays a crucial role in verifying the identity of individuals or entities requesting digital certificates. Here's how it works:

Ben, the computer user, applies for a digital certificate.

TheRAverifies Ben's identity using the credentials provided.

Once verified, theRAforwards the request on behalf of Ben to theCertificate Authority (CA).

TheCAthen issues the digital certificate to Ben.

Therefore, theRAis responsible for ensuring that legitimate individuals receive valid digital certificates by verifying their identity.

EC-Council Certified Security Specialist (E|CSS) documents and study guide1.

EC-Council Certified Security Specialist (E|CSS) course materials2.