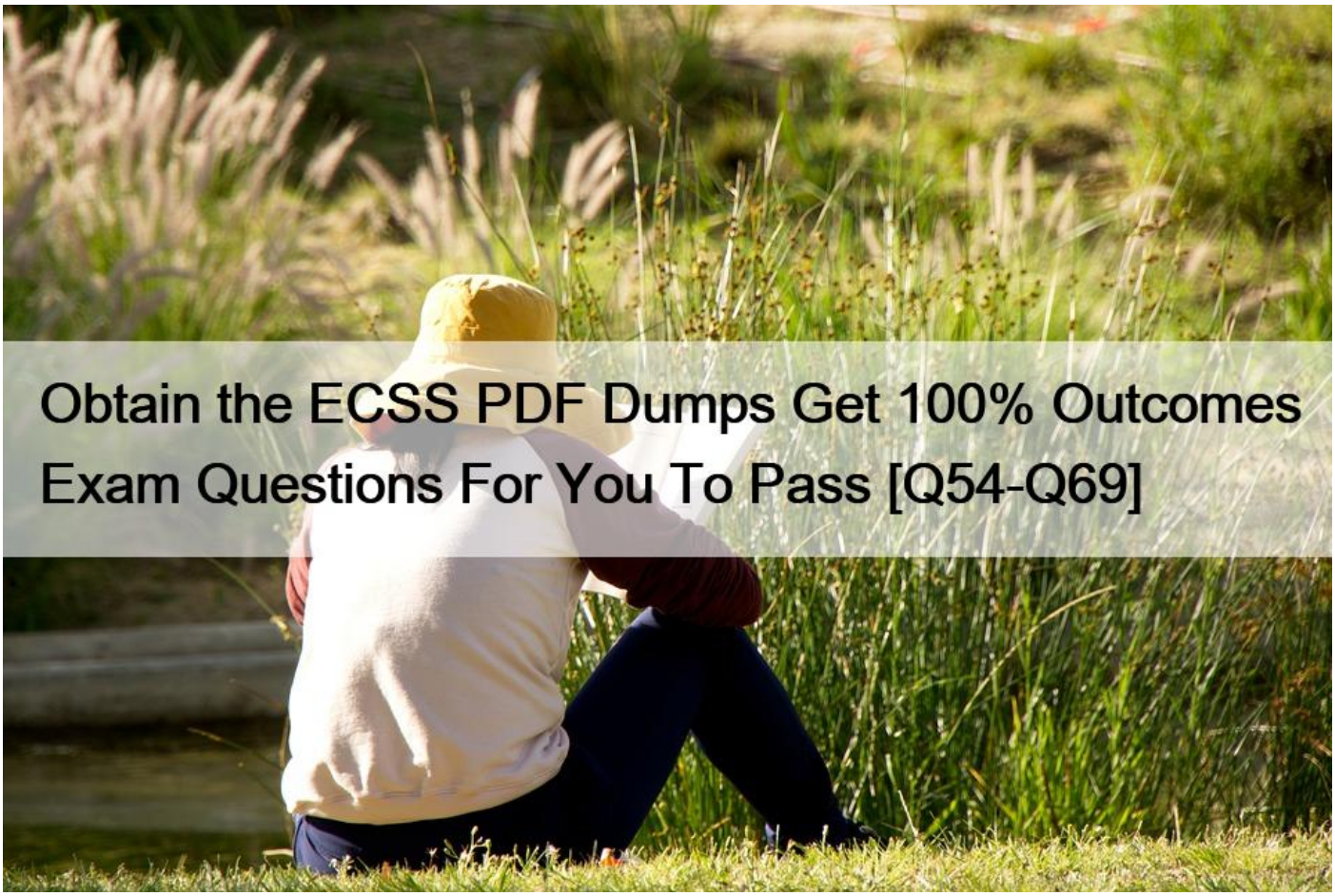
# Obtain the ECSS PDF Dumps Get 100% Outcomes Exam Questions For You To Pass [Q54-Q69




Obtain the ECSS PDF Dumps Get 100% Outcomes Exam Questions For You To Pass
ECSS Exam Dumps Contains FREE Real Quesions from the Actual Exam

EC-COUNCIL ECSS certification exam is designed to test the knowledge and skills of candidates in various areas of cybersecurity such as network security, cryptography, access controls, and security operations. The ECSS certification exam consists of 50 multiple-choice questions, and candidates have 2 hours to complete the exam. ECSS exam is designed to test the candidate's knowledge and understanding of cybersecurity concepts and principles.

**NO.54** Which of the following steps in the Computer Forensic Investigation process limits the extent and significance of an incident to ensure that it does not spread to other systems?
* Containment
* Detection
* Preparation
* Eradication

**NO.55** Alana, an employee in an organization, took a short break after spending exhausting hours on a project. For relaxation, she went to a cafeteria with her laptop, where she connected to the public Internet. While browsing the web, she received a project modifications file on her mail and reverted with another file that contained the required changes.

Which of the following BYOD risks has emerged from the above scenario?
* Mixing personal and private data
* Endpoint security issue
* Improper disposing of devices
* Sharing confidential data on unsecured networks
In the given scenario, Alana’s actions pose a risk related to sharing confidential data on unsecured networks. Here’s why:

* BYOD (Bring Your Own Device): Alana used her personal laptop in a public cafeteria. This falls under the BYOD concept, where employees use their personal devices for work-related tasks.

* Unsecured Network: Connecting to the public Internet in a cafeteria means she is using an unsecured network. Public Wi-Fi networks are often vulnerable to eavesdropping and unauthorized access.

* Email Communication: Alana received a project modifications file via email and sent back another file with changes. Email communication over an unsecured network can expose sensitive information to potential attackers.

* Risk: By sharing project-related files over an unsecured network, Alana risks exposing confidential data to unauthorized individuals.

References:

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

* EC-Council Certified Security Specialist (E|CSS) documents and course content12.

**NO.56** Fill in the blank with the appropriate name of the attack.

_____ takes best advantage of an existing authenticated connection
* session hijacking

**NO.57** 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.
* Stateful protocol analysis
* Anomaly-based
* Signature-based
* Application proxy
Messy has deployed an anomaly-based Intrusion 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. References: EC-Council Certified Security Specialist (E|CSS) course materials12.

**NO.58** Wesley, a professional hacker, deleted a confidential file in a compromised system using the “/bin/rm/ command to deny access to forensic specialists.

Identify the operating system on which Don has performed the file carving activity.
* Windows
* Mac OS
* Linux
* Android
In the scenario described, Wesley used the “/bin/rm/” command to delete a confidential file. The “/bin/rm/” command is commonly associated with Linux operating systems. It is used to remove files and directories. By deleting the file, Wesley aimed to hinder forensic specialists’ access to it. Therefore, the operating system on which Wesley performed the file carving activity is Linux. References: EC-Council Certified Security Specialist (E|CSS) documents and study guide12.

**NO.59** Which of the following malicious software implements itself on the kernel level of any operating system and is hard to detect and delete?
* Worm
* Adware
* Spyware
* Rootkit

**NO.60** What is the major difference between a worm and a Trojan horse?
* A worm is self replicating, while a Trojan horse is not.
* A Trojan horse is a malicious program, while a worm is an anti-virus software.
* A worm spreads via e-mail, while a Trojan horse does not.
* A worm is a form of malicious program, while a Trojan horse is a utility.

**NO.61** Which of the following representatives of incident response team takes forensic backups of the systems that are the focus of the incident?
* Lead investigator
* Information security representative
* Technical representative
* Legal representative

**NO.62** Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?
* Snooping
* Copyright
* Utility model
* Patent

**NO.63** John works as a Network Security Administrator for NetPerfect Inc. The manager of the company has told John that the company’s phone bill has increased drastically. John suspects that the company’s phone system has been cracked by a malicious hacker. Which attack is used by malicious hackers to crack the phone system?
* Sequence++ attack
* Phreaking
* Man-in-the-middle attack
* War dialing

**NO.64** Burp Suite is a Java application for attacking web applications. This tool includes a proxy server, a spider, an intruder, and a repeater. Which of the following can be used to perform stress testing?
* Repeater

* Spider
* Intruder
* Proxy Server

**NO.65** Clark, a digital forensic expert, was assigned to investigate a malicious activity performed on an organization’s network. The organization provided Clark with all the information related to the incident. In this process, he assessed the impact of the incident on the organization, reasons for and source of the incident, steps required to tackle the incident, investigating team required to handle the case, investigative procedures, and possible outcome of the forensic process.

Identify the type of analysis performed by Clark in the above scenario.
* Data analysis
* Log analysis
* Traffic analysis
* Case analysis

In the given scenario, Clark performed a case analysis. This involves assessing the impact of the incident, understanding its reasons and source, determining the necessary steps to address it, assembling an investigative team, defining investigative procedures, and considering potential outcomes of the forensic process. Case analysis is crucial in digital forensics to effectively handle incidents and gather relevant evidence.

References: 12

https://www.eccouncil.org/train-certify/certified-soc-analyst-csa/

**NO.66** Victor works as a network administrator for DataSecu Inc. He uses a dual firewall Demilitarized Zone (DMZ) to insulate the rest of the network from the portions that is available to the Internet.

Which of the following security threats may occur if DMZ protocol attacks are performed?

Each correct answer represents a complete solution. Choose all that apply.
* The attacker can exploit any protocol used to go into the internal network or intranet of thecompany.
* The attacker can gain access to the Web server in a DMZ and exploit the database.
* The attacker can perform a Zero Day attack by delivering a malicious payload that is not a part of the intrusion detection/prevention systems guarding the network.
* The attacker managing to break the first firewall defense can access the internal network without breaking the second firewall if it is different.

**NO.67** Which of the following parameters are required to be followed on receiving a suspicious mail according to the Department of Justice?

Each correct answer represents a part of the solution. Choose all that apply.
* Call
* Look
* Stop
* Identify

**NO.68** Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?
* Incident response policy
* Chain of custody
* Chain of evidence
* Evidence access policy

**NO.69** Fill in the blank with the command to complete the statement below. Do not enter the full path of the command.

The _____ command is used to remove the print jobs that have been queued for printing by using a secure connection.
* lprm -E