Jan-2024 New Version 312-38 Certificate & Helpful Exam Dumps is Online [Q45-Q59

Jan-2024 New Version 312-38 Certificate & Helpful Exam Dumps is Online 312-38 Free Certification Exam Material with 232 Q&As

The EC-Council Certified Network Defender CND certification exam is designed for IT professionals, network administrators, security analysts, and anyone interested in a career in network security. The EC-Council Certified Network Defender (CND) certification is globally recognized and provides a competitive edge in the job market. It demonstrates the candidate's proficiency in network security and validates their commitment to maintaining the highest security standards. Overall, the EC-Council Certified Network Defender (CND) certification is an excellent choice for individuals seeking a career in network security and is an essential requirement for many job roles in the field.

NO.45 Which of the following RAID storage techniques divides the data into multiple blocks, which are further written across the RAID system?

* Striping
* None of these
* Parity

* Mirroring

NO.46 A newly joined network administrator wants to assess the organization against possible risk. He notices the organization doesn’t have a_____identified which helps measure how risky an activity is.
* Risk Severity
* Risk Matrix
* Key Risk Indicator
* Risk levels

NO.47 Which of the following is a congestion control mechanism that is designed for unicast flows operating in an Internet environment and competing with TCP traffic?
* Sliding Window
* TCP Friendly Rate Control
* Selective Acknowledgment
* Additive increase/multiplicative-decrease

NO.48 Which type of modulation technique is used in local area wireless networks (LAWNs)?
* FHSS
* OFDM
* DSSS
* MIMO-OFDM

NO.49 Which among the following options represents professional hackers with an aim of attacking systems for profit?
* Script kiddies
* Organized hackers
* Hacktivists
* Cyber terrorists

NO.50 Which of the following tools is a free portable tracker that helps the user to trace the laptop if it is stolen?
* Nessus
* bridle
* SAINT
* Adeona
* None

NO.51 Which of the following IEEE standards is an example of a DQDB access method?
* 802.3
* 802.5
* 802.6
* 802.4

NO.52 A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It provides an attacker unauthorized access to a computer. Which of the following tools can an attacker use to perform war dialing? Each correct answer represents a complete solution. Choose all that apply.
* ToneLoc
* Wingate
* THC-Scan
* NetStumbler

THC-Scan and ToneLoc are tools used for war dialing. A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It provides the attacker unauthorized access to a computer. Answer option D is incorrect. NetStumbler is

a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. It detects wireless

networks and marks their relative position with a GPS. It uses an 802.11 Probe Request

that has been sent to the broadcast destination address.

Answer option B is incorrect. Wingate is a proxy server.

NO.53 Implementing access control mechanisms, such as a firewall, to protect the network is an example of which of the following network defense approach?
* Proactive approach
* Retrospective approach
* Preventive approach
* Reactive approach

NO.54 Which of the following steps of the OPSEC process examines each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then compare those indicators with the adversary’s intelligence collection capabilities identified in the previous action?
* Analysis of Threats
* Analysis of Vulnerabilities
* Assessment of Risk
* Identification of Critical Information
* Application of Appropriate OPSEC Measures

OPSEC is a 5-step process that helps in developing protection mechanisms in order to safeguard sensitive information and preserve essential secrecy. The OPSEC process has five steps, which are as follows:

1.Identification of Critical Information: This step includes identifying information vitally needed by an adversary, which focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to protect all classified or sensitive unclassified information.

2.Analysis of Threats: This step includes the research and analysis of intelligence, counter-intelligence, and open source information to identify likely adversaries to a planned operation.

3.Analysis of Vulnerabilities: It includes examining each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary’s intelligence collection capabilities identified in the previous action. 4.Assessment of Risk: Firstly, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Secondly, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff.

5.Application of Appropriate OPSEC Measures: The command implements the OPSEC measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

NO.55 This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE

802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:

It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc.

It is commonly used for the following purposes:

a.War driving

b.Detecting unauthorized access points

c.Detecting causes of interference on a WLAN

d.WEP ICV error tracking

e.Making Graphs and Alarms on 802.11 Data, including Signal Strength

This tool is known as _____.
* Kismet
* Absinthe
* THC-Scan
* NetStumbler

NO.56 Which of the following statements is not true about the FAT16 file system? Each correct answer represents a complete solution. Choose all that apply.
* It supports task compression files.
* It works well with large disk, because the cluster size increases as the disk partition size increases.
* It does not support file protection.
* It supports the Linux operating system.

NO.57 Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice’s password read from the last session, which Bob accepts.

Which of the following attacks is being used by Eve?
* Replay
* Fire walking
* Cross site scripting
* Session fixation

Explanation

Explanation:

Eve is using Replay attack. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet. Session tokens can be used to avoid replay attacks. Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Mallory has captured this value and tries to use it on another session; Bob sends a different session token, and when Mallory replies with the captured value it will be different from Bob’s computation.

Answer option C is incorrect. In the cross site scripting attack, an attacker tricks the user’s computer into running code, which is treated as trustworthy because it appears to belong to the server, allowing the attacker to obtain a copy of the cookie or perform other operations.

Answer option B is incorrect. Firewalking is a technique for gathering information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.

Answer option D is incorrect. In session fixation, an attacker sets a user’s session id to one known to him, for example by sending the user an email with a link that contains a particular session id. The attacker now only has to wait until the user logs in.

NO.58 Larry is responsible for the company’s network consisting of 300 workstations and 25 servers.

After using a hosted email service for a year, the company wants to control the email internally.

Larry likes this idea because it will give him more control over the email. Larry wants to purchase a server for email but does not want the server to be on the internal network due to the potential to cause security risks. He decides to place the server outside of the company’s internal firewall.

There is another firewall connected directly to the Internet that will protect traffic from accessing the email server. The server will be placed between the two firewalls. What logical area is Larry putting the new email server into?
* He is going to place the server in a Demilitarized Zone (DMZ)
* He will put the email server in an IPsec zone.
* Larry is going to put the email server in a hot-server zone.
* For security reasons, Larry is going to place the email server in the company’s Logical Buffer Zone (LBZ).

NO.59 Which of the following UTP cables supports transmission up to 20MHz?
* Category 2
* Category 5e
* Category 4
* Category 1