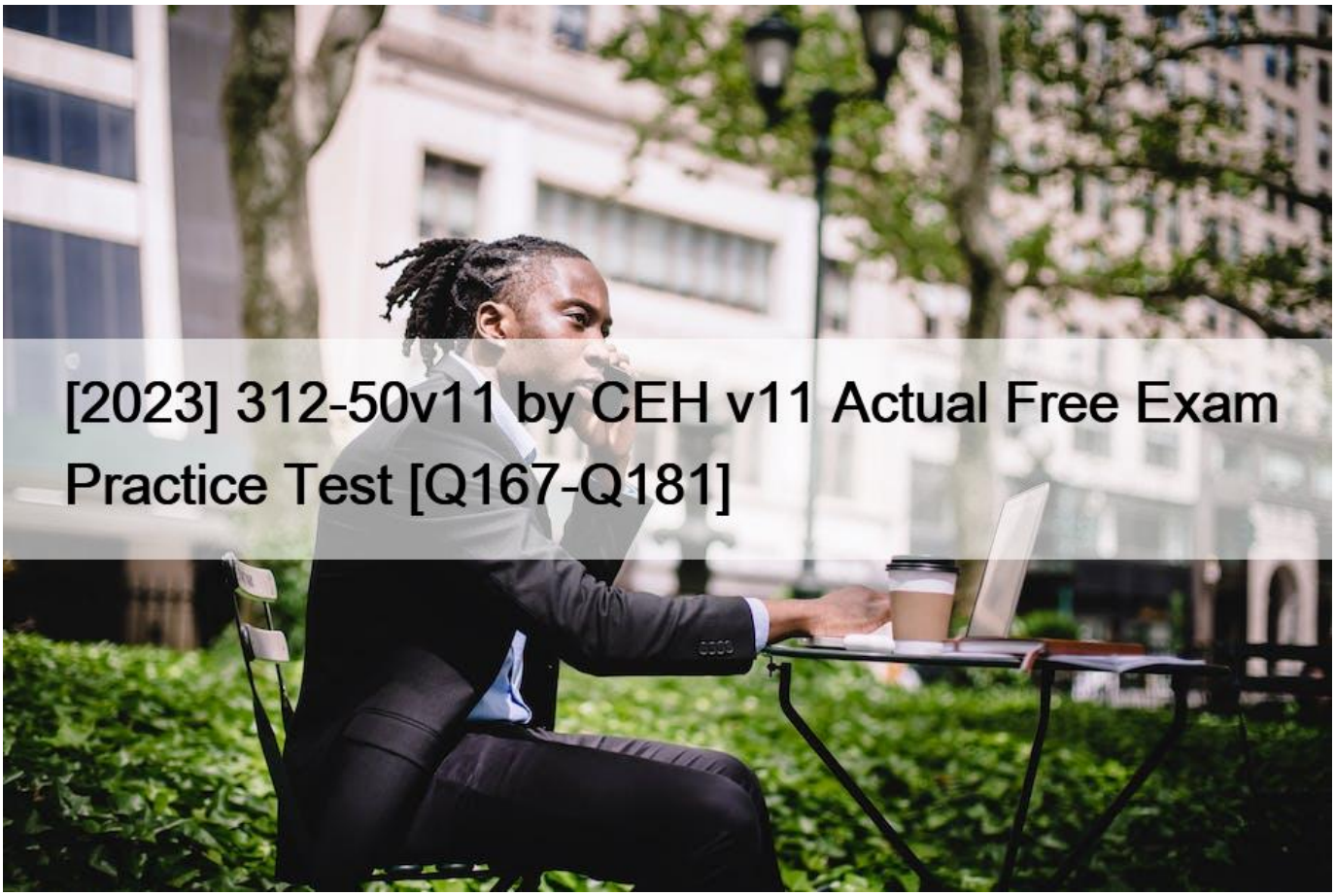
[2023 312-50v11 by CEH v11 Actual Free Exam Practice Test [Q167-Q181



[2023] 312-50v11 by CEH v11 Actual Free Exam Practice Test
Free CEH v11 312-50v11 Exam Question

EC-COUNCIL, the organization that administers the CEH v11 certification exam, is a leading provider of cybersecurity training and certification programs. The organization has a global network of over 2,000 authorized training centers, and its certification programs are recognized by governments, military organizations, and private companies worldwide. EC-COUNCIL's mission is to raise awareness about the importance of cybersecurity and to provide individuals and organizations with the necessary skills and knowledge to protect themselves from cyber threats.

EC-COUNCIL 312-50v11 (Certified Ethical Hacker Exam (CEH v11)) is a certification exam that validates the skills and knowledge of individuals in the field of ethical hacking. 312-50v11 exam is designed to test the abilities of cybersecurity professionals to identify vulnerabilities in computer systems, networks, and applications, and to use their knowledge to prevent and mitigate cyber attacks.

QUESTION 167

Your organization has signed an agreement with a web hosting provider that requires you to take full responsibility of the maintenance of the cloud-based resources. Which of the following models covers this?
* Platform as a service
* Software as a service
* Functions as a
* service Infrastructure as a service

QUESTION 168

Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?
* 137 and 139
* 137 and 443
* 139 and 443
* 139 and 445

QUESTION 169

DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switchers leverages the DHCP snooping database to help prevent man-in-the-middle attacks?
* Spanning tree
* Dynamic ARP Inspection (DAI)
* Port security
* Layer 2 Attack Prevention Protocol (LAPP)

QUESTION 170

Sam, a professional hacker. targeted an organization with intention of compromising AWS IAM credentials.

He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS 1AM credentials and further compromise the employee’s account. What is the technique used by Sam to compromise the AWS IAM credentials?
* Social engineering
* insider threat
* Password reuse
* Reverse engineering

QUESTION 171

Richard, an attacker, aimed to hack loT devices connected to a target network.

In this process. Richard recorded the frequency required to share information between connected devices.

After obtaining the frequency, he captured the original data when commands were initiated by the connected devices.

Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the loT network, which repeats the captured signals of the devices.

What Is the type of attack performed by Richard In the above scenario?
* Side-channel attack
* Replay attack
* CrypTanalysis attack
* Reconnaissance attack

Replay Attack could be a variety of security attack to the info sent over a network. In this attack, the hacker or a person with unauthorized access, captures the traffic and sends communication to its original destination, acting because the original sender. The receiver feels that it’s Associate in Nursing genuine message however it’s really the message sent by the aggressor. the most feature of the Replay Attack is that the consumer would receive the message double, thence the name, Replay Attack.

Prevention from Replay Attack : 1. Timestamp technique –

Prevention from such attackers is feasible, if timestamp is employed at the side of the info. Supposedly, the timestamp on an information is over a precise limit, it may be discarded, and sender may be asked to send the info once more.

2. Session key technique –

Another way of hindrance, is by victimisation session key. This key may be used one time (by sender and receiver) per dealing, and can’t be reused.

QUESTION 172

You are a penetration tester tasked with testing the wireless network of your client Brakeme SA.

You are attempting to break into the wireless network with the SSID “Brakeme-lnternal.” You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?
* Dragonblood
* Cross-site request forgery
* Key reinstallation attack
* AP Myconfiguration

Dragonblood allows an attacker in range of a password-protected Wi-Fi network to get the password and gain access to sensitive information like user credentials, emails and mastercard numbers. consistent with the published report: “The WPA3 certification aims to secure Wi-Fi networks, and provides several advantages over its predecessor WPA2, like protection against offline dictionary attacks and forward secrecy. Unfortunately, we show that WPA3 is suffering from several design flaws, and analyze these flaws both theoretically and practically. Most prominently, we show that WPA3’s Simultaneous Authentication of Equals (SAE) handshake, commonly referred to as Dragonfly, is suffering from password partitioning attacks.” Our Wi-Fi researchers at WatchGuard are educating businesses globally that WPA3 alone won’t stop the Wi-Fi hacks that allow attackers to steal information over the air (learn more in our recent blog post on the topic). These Dragonblood vulnerabilities impact alittle amount of devices that were released with WPA3 support, and makers are currently making patches available. one among the most important takeaways for businesses of all sizes is to know that a long-term fix might not be technically feasible for devices with lightweight processing capabilities like IoT and embedded systems. Businesses got to consider adding products that enable a Trusted Wireless Environment for all kinds of devices and users alike. Recognizing that vulnerabilities like KRACK and Dragonblood require attackers to initiate these attacks by bringing an “Evil Twin” Access Point or a Rogue Access Point into a Wi-Fi environment, we’ve been that specialize in developing Wi-Fi security solutions that neutralize these threats in order that these attacks can never occur. The Trusted Wireless Environment framework protects against the “Evil Twin” Access Point and Rogue Access Point. one among these hacks is required to initiate the 2 downgrade or side-channel attacks referenced in Dragonblood. What’s next? WPA3 is an improvement over WPA2 Wi-Fi encryption protocol, however, as we predicted, it still doesn’t provide protection from the six known Wi-Fi threat categories. It’s highly likely that we’ll see more WPA3 vulnerabilities announced within the near future. To help reduce Wi-Fi vulnerabilities, we’re asking all of you to hitch the Trusted Wireless Environment movement and advocate for

a worldwide security standard for Wi-Fi.

QUESTION 173

You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: “The attacker must scan every port on the server several times using a set of spoofed sources IP addresses. ” Suppose that you are using Nmap to perform this scan. What flag will you use to satisfy this requirement?
* The -A flag
* The -g flag
* The -f flag
* The -D flag

Explanation

flags -source-port and -g are equivalent and instruct nmap to send packets through a selected port. this option is used to try to cheat firewalls whitelisting traffic from specific ports. the following example can scan the target from the port twenty to ports eighty, 22, 21,23 and 25 sending fragmented packets to LinuxHint.

QUESTION 174

env x='(){ :;};echo exploit’ bash -c ‘cat/etc/passwd’

What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?
* Removes the passwd file
* Changes all passwords in passwd
* Add new user to the passwd file
* Display passwd content to prompt

QUESTION 175

George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m.

What is the short-range wireless communication technology George employed in the above scenario?
* LPWAN
* MQTT
* NB-IoT
* Zigbee

QUESTION 176

During the enumeration phase. Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.

Which of the following services is enumerated by Lawrence in this scenario?
* Server Message Block (SMB)
* Network File System (NFS)
* Remote procedure call (RPC)
* Telnet

Explanation

Worker Message Block (SMB) is an organization document sharing and information texture convention. SMB is utilized by billions of gadgets in a different arrangement of working frameworks, including Windows, MacOS, iOS , Linux, and Android. Customers use SMB to get to information on workers. This permits sharing of records, unified information the board, and brought down capacity limit needs for cell phones. Workers additionally use SMB as a feature of the Software-characterized Data Center for outstanding burdens like grouping and replication.

Since SMB is a far off record framework, it requires security from assaults where a Windows PC may be fooled into reaching a pernicious worker running inside a confided in organization or to a far off worker outside the organization edge. Firewall best practices and arrangements can upgrade security keeping malevolent traffic from leaving the PC or its organization.

For Windows customers and workers that don’t have SMB shares, you can obstruct all inbound SMB traffic utilizing the Windows Defender Firewall to keep far off associations from malignant or bargained gadgets. In the Windows Defender Firewall, this incorporates the accompanying inbound principles.

You should also create a new blocking rule to override any other inbound firewall rules. Use the following suggested settings for any Windows clients or servers that do not host SMB Shares:

* Name: Block all inbound SMB 445

* Description: Blocks all inbound SMB TCP 445 traffic. Not to be applied to domain controllers or computers that host SMB shares.

* Action: Block the connection

* Programs: All

* Remote Computers: Any

* Protocol Type: TCP

* Local Port: 445

* Remote Port: Any

* Profiles: All

* Scope (Local IP Address): Any

* Scope (Remote IP Address): Any

* Edge Traversal: Block edge traversal

You must not globally block inbound SMB traffic to domain controllers or file servers. However, you can restrict access to them from trusted IP ranges and devices to lower their attack surface. They should also be restricted to Domain or Private firewall profiles and not allow Guest/Public traffic.

QUESTION 177

Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France. Which regional Internet registry should Becky go to for detailed information?
* ARIN
* APNIC
* RIPE
* LACNIC

QUESTION 178

which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?
* intrusion detection system
* Honeypot
* Botnet
D Firewall

Explanation:

A honeypot may be a trap that an IT pro lays for a malicious hacker, hoping that they will interact with it during a way that gives useful intelligence. It’s one among the oldest security measures in IT, but beware: luring hackers onto your network, even on an isolated system, are often a dangerous game. honeypot may be a good starting place: “A honeypot may be a computer or computing system intended to mimic likely targets of cyberattacks.” Often a honeypot are going to be deliberately configured with known vulnerabilities in situation to form a more tempting or obvious target for attackers. A honeypot won’t contain production data or participate in legitimate traffic on your network – that’s how you’ll tell anything happening within it’s a results of an attack. If someone’s stopping by, they’re up to no good. That definition covers a various array of systems, from bare-bones virtual machines that only offer a couple of vulnerable systems to ornately constructed fake networks spanning multiple servers. and therefore the goals of these who build honeypots can vary widely also , starting from defense thorough to academic research. additionally , there’s now an entire marketing category of deception technology that, while not meeting the strict definition of a honeypot, is certainly within the same family. But we’ll get thereto during a moment. honeypots aim to permit close analysis of how hackers do their dirty work. The team controlling the honeypot can watch the techniques hackers use to infiltrate systems, escalate privileges, and otherwise run amok through target networks. These sorts of honeypots are found out by security companies, academics, and government agencies looking to look at the threat landscape. Their creators could also be curious about learning what kind of attacks are out there, getting details on how specific sorts of attacks work, or maybe trying to lure a specific hackers within the hopes of tracing the attack back to its source. These systems are often inbuilt fully isolated lab environments, which ensures that any breaches don’t end in non-honeypot machines falling prey to attacks. Production honeypots, on the opposite hand, are usually deployed in proximity to some organization’s production infrastructure, though measures are taken to isolate it the maximum amount as possible. These honeypots often serve both as bait to distract hackers who could also be trying to interrupt into that organization’s network, keeping them faraway from valuable data or services; they will also function a canary within the coalpit , indicating that attacks are underway and are a minimum of partially succeeding.

QUESTION 179

Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.

What is the technique used by Jacob in the above scenario to improve the security of the mobile application?
* Reverse engineering
* App sandboxing
* Jailbreaking
* Social engineering

QUESTION 180

Which of the following allows attackers to draw a map or outline the target organization’s network infrastructure to know about the actual environment that they are going to hack.
* Enumeration
* Vulnerability analysis
* Malware analysis
* Scanning networks

QUESTION 181

Robin, a professional hacker, targeted an organization’s network to sniff all the traffic. During this process, Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.

What is the attack performed by Robin in the above scenario?
* ARP spoofing attack
* STP attack
* DNS poisoning attack
* VLAN hopping attack