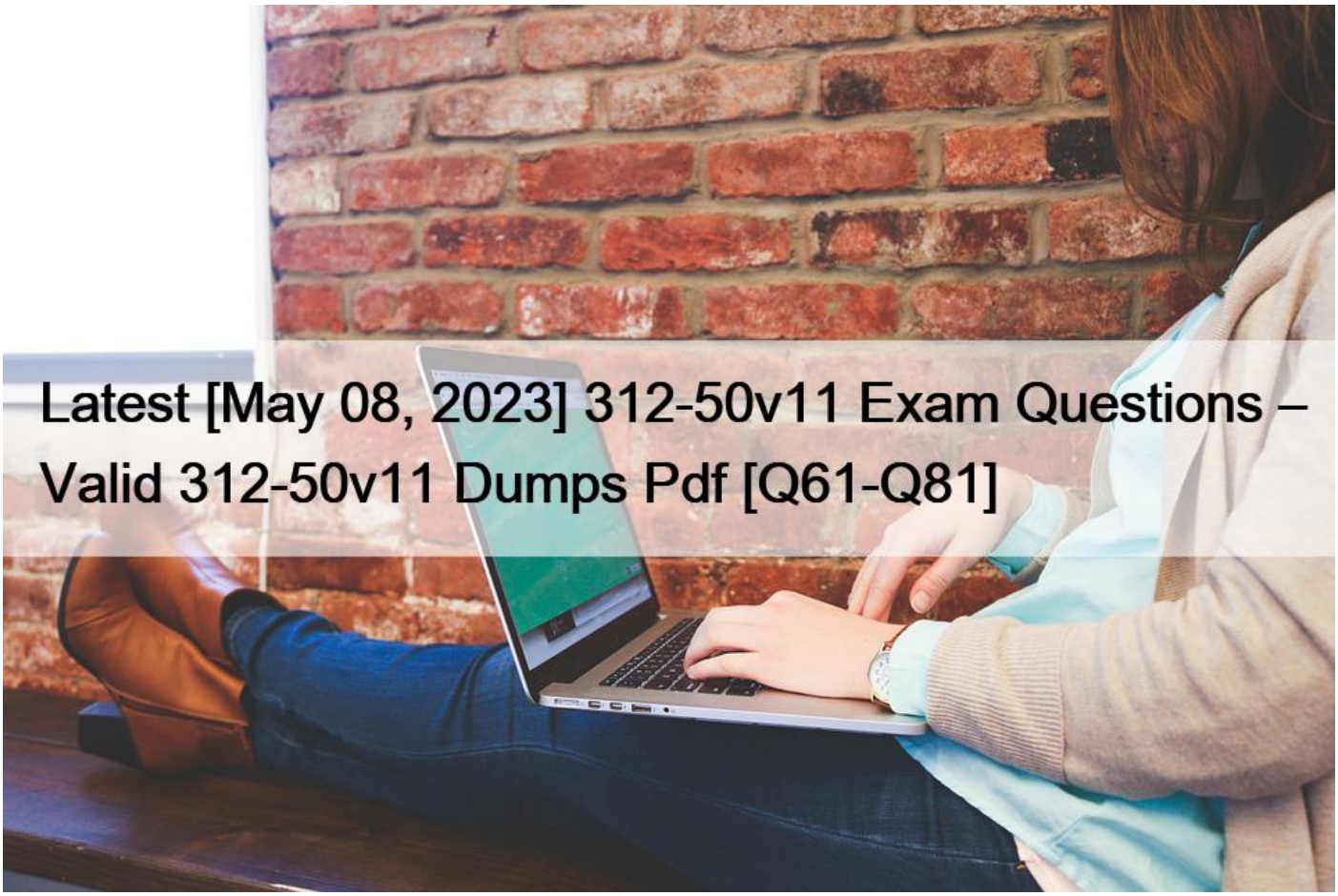
Latest [May 08, 2023 312-50v11 Exam Questions ? Valid 312-50v11 Dumps Pdf [Q61-Q81



Latest [May 08, 2023] 312-50v11 Exam Questions – Valid 312-50v11 Dumps Pdf
312-50v11 Practice Test Questions Answers Updated 525 Questions

Training Courses **For better 312-50v11 exam readiness, it is wise to join a training course endorsed by the vendor. Overall, there are many official live online classes so here are the best picks:** - CEH Exam Prep ? Live Online - This training course covers the CEH exam content and details via a skilled instructor through online live sessions.- CEH MasterClass Program - To master the exam domains and acquire noteworthy practical as well as conjectural subject matter cognizance, join the CEH MasterClass Program. This package includes CEH e-courseware, exam insurance information, and live labs so it is worth a try.

To better understand the exam content, you need to have a look at the topics that this test covers. Thus, the domains you should study for are the following: **Cloud Computing: 6%**Here you will gain an understanding of Cloud computing concepts, serverless computing, Cloud security, container technology, Cloud hacking, and Cloud computing threats. **Phases of System Hacking & Attack Methods: 17%**This domain covers the students' understanding of vulnerability assessment concepts & reports, system hacking concepts, gaining & maintaining access, hiding files, executing applications, malware concepts, and clearing logs. You will also learn about anti-malware software, file-less malware concepts, and malware countermeasures. **Web Application Hacking: 16%**This module evaluates your understanding of web server concepts, webserver attacks, patch

management, web server attack tools, security tools, and countermeasures, as well as web app concepts and footprint web infrastructure. You should also know about attack access controls, web app security, attack web app client, and attack authorization schemes. It also covers one's knowledge of attack shared environments, web API, web shell, and Webhooks. The learners will need to have the skills in analyzing web applications and performing injection attacks as well as know about attack database connectivity and attack app logic flaws. The potential candidates should also understand SQL injection concepts, tools, countermeasures, and methodology as well as evasion techniques. **Reconnaissance Methods: 21%**This section focuses on the concepts, such as footprinting concepts & methodology, footprinting via search engines, web services, and social networking sites, email & website footprinting, as well as DNS footprinting. It also covers one's understanding of Whois footprinting, network footprinting, footprinting countermeasures & tools, and footprinting via social engineering. It also includes the concepts in scanning networks and enumerations. **Cryptography: 6%**The last area focuses on the applicants' understanding of cryptography concepts, cryptography tools, encryption algorithms, email encryption, countermeasures, cryptanalysis, disk encryption, and public key infrastructure. **Overview of Information Security & Ethical Hacking: 6%**This topic covers the areas, such as information security standards & laws, information security controls, ethical hacking, hacking, concepts, concepts of the cyber kill chain, as well as information security overview. **Mobile Platform, OT Hacking, and IoT: 8%**For this part, it is important to know about mobile security tools & guidelines, hacking iOS, mobile device management, and hacking Android iOS. It also includes the details of IoT hacking & OT hacking, which includes the concepts, hacking methodology, attacks & countermeasures, and hacking tools. You should also have knowledge of the OT concepts, hacking methodology, attacks, countermeasures, as well as hacking tools. **Wireless Network Hacking: 6%**This objective requires that the students understand wireless concepts, wireless threats, wireless encryption, wireless hacking tools, wireless hacking methodology, wireless security tools, and wireless countermeasures.

QUESTION 61

Attacker Rony installed a rogue access point within an organization’s perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack.

What is the type of vulnerability assessment performed by Johnson in the above scenario?
* Wireless network assessment
* Application assessment
* Host-based assessment
* Distributed assessment

QUESTION 62

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?
* tcpsplice
* Burp
* Hydra
* Whisker

QUESTION 63

Which type of virus can change its own code and then cipher itself multiple times as it replicates?
* Stealth virus
* Tunneling virus
* Cavity virus

* Encryption virus

QUESTION 64

An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization deckled to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware. Which of the following tools must the organization employ to protect its critical infrastructure?
* Robotium
* BalenaCloud
* Flowmon
* IntentFuzzer
Source: https://www.flowmon.com

Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks confidently to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible.

QUESTION 65

Your company was hired by a small healthcare provider to perform a technical assessment on the network.

What is the best approach for discovering vulnerabilities on a Windows-based computer?
* Use the built-in Windows Update tool
* Use a scan tool like Nessus
* Check MITRE.org for the latest list of CVE findings
* Create a disk image of a clean Windows installation

QUESTION 66

infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?
* Reconnaissance
* Maintaining access
* Scanning
* Gaining access
This phase having the hacker uses different techniques and tools to realize maximum data from the system. they’re – * Password cracking – Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered. * Password attacks – Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

QUESTION 67

Joseph was the Web site administrator for the Mason Insurance in New York, who’s main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent

phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker’s message ”Hacker Message: You are dead! Freaks!” From his office, which was directly connected to Mason Insurance’s internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.

No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

```
H@cker Mess@ge:
Y0u @re De@d! Fre@ks!
```

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?

* ARP spoofing
* SQL injection
* DNS poisoning
* Routing table injection

QUESTION 68

What is the port to block first in case you are suspicious that an IoT device has been compromised?

* 22
* 48101
* 80
* 443

QUESTION 69

You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

```
char shellcode[] =
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb\x16\x5b\x31\xc0"
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d"
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73"
"\x68";
```

What is the hexadecimal value of NOP instruction?

* 0x60
* 0x80
* 0x70
* 0x90

QUESTION 70

Ralph, a professional hacker, targeted Jane, who had recently bought new systems for her company. After a few days, Ralph contacted Jane while masquerading as a legitimate customer support executive, informing that her systems need to be serviced for

proper functioning and that customer support will send a computer technician. Jane promptly replied positively. Ralph entered Jane’s company using this opportunity and gathered sensitive information by scanning terminals for passwords, searching for important documents in desks, and rummaging bins.

What is the type of attack technique Ralph used on Jane?
* Impersonation
* Dumpster diving
* Shoulder surfing
* Eavesdropping

QUESTION 71

How does a denial-of-service attack work?
* A hacker prevents a legitimate user (or group of users) from accessing a service
* A hacker uses every character, word, or letter he or she can think of to defeat authentication
* A hacker tries to decipher a password by using a system, which subsequently crashes the network
* A hacker attempts to imitate a legitimate user by confusing a computer or even another person

QUESTION 72

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 73

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

QUESTION 74

jane invites her friends Alice and John over for a LAN party. Alice and John access Jane’s wireless network without a password. However. Jane has a long, complex password on her router. What attack has likely occurred?
* Wireless sniffing
* Piggybacking
* Evil twin
* Wardriving

Explanation

A wireless sniffer may be a sort of packet analyzer. A packet analyzer (also referred to as a packet sniffer) may be a piece of software or hardware designed to intercept data because it is transmitted over a network and decode the info into a format that’s readable for humans. Wireless sniffers are packet analyzers specifically created for capturing data on wireless networks. Wireless sniffers also are commonly mentioned as wireless packet sniffers or wireless network sniffers.Wireless sniffer tools have many uses in commercial IT environments. Their ability to watch , intercept, and decode data because it is in transit makes them useful for:* Diagnosing and investigating network problems* Monitoring network usage, activity, and security* Discovering network misuse, vulnerabilities, malware, and attack attempts* Filtering network traffic* Identifying configuration issues and network bottlenecks* Wireless Packet Sniffer AttacksWhile wireless packet sniffers are valuable tools for maintaining wireless networks, their capabilities make them popular tools for malicious actors also . Hackers can use wireless sniffer software to steal data, spy on network activity, and gather information to use in attacking the network. Logins (usernames and passwords) are quite common targets for attackers using wireless sniffer tools. Wireless network sniffing attacks usually target unsecure networks, like free WiFi publicly places (coffee shops, hotels, airports, etc).Wireless sniffer tools also are commonly utilized in “spoofing” attacks. Spoofing may be a sort of attack where a malicious party uses information obtained by a wireless sniffer to impersonate another machine on the network. Spoofing attacks often target business’ networks and may be wont to steal sensitive information or run man-in-the-middle attacks against network hosts.There are two modes of wireless sniffing: monitor mode and promiscuous mode.

In monitor mode, a wireless sniffer is in a position to gather and skim incoming data without sending any data of its own. A wireless sniffing attack in monitor mode are often very difficult to detect due to this. In promiscuous mode, a sniffer is in a position to read all data flowing into and out of a wireless access point.

Since a wireless sniffer in promiscuous mode also sniffs outgoing data, the sniffer itself actually transmits data across the network. This makes wireless sniffing attacks in promiscuous mode easier to detect. it’s more common for attackers to use promiscuous mode in sniffing attacks because promiscuous mode allows attackers to intercept the complete range of knowledge flowing through an access point.

Preventing Wireless Sniffer AttacksThere are several measures that organizations should fancy mitigate wireless packet sniffer attacks. First off, organizations (and individual users) should refrain from using insecure protocols. Commonly used insecure protocols include basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Secure protocols like HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be utilized in place of their insecure alternatives when possible. Secure protocols make sure that any information transmitted will automatically be encrypted. If an insecure protocol must be used, organizations themselves got to encrypt any data which will be sent using that protocol. Virtual Private Networks (VPNs) are often wont to encrypt internet traffic and are a well-liked tool for organizations today.Additionally to encrypting information and using secure protocols, companies can prevent attacks by using wireless sniffer software to smell their own networks. this enables security teams to look at their networks from an attacker’s perspective and find out sniffing vulnerabilities and attacks ongoing . While this method won’t be effective in discovering wireless network sniffers in monitor mode, it’s possible to detect sniffers in promiscuous mode (the preferred mode for attackers) by sniffing your own network.

Tools for Detecting Packet SniffersWireless sniffer software programs frequently include features like intrusion and hidden network detection for helping organizations discover malicious sniffers on their networks. additionally to using features that are built into wireless sniffer tools, there are many aftermarket tools available that are designed specifically for detecting sniffing attacks. These tools typically perform functions like monitoring network traffic or scanning network cards in promiscuous mode to detect wireless network sniffers. There are dozens of options (both paid and open source) for sniffer detection tools, so organizational security teams will got to do some research before selecting the proper tool for his or her needs.

QUESTION 75

At what stage of the cyber kill chain theory model does data exfiltration occur?
* Actions on objectives

* Weaponization
* installation
* Command and control

The longer an adversary has this level of access, the greater the impact. Defenders must detect this stage as quickly as possible and deploy tools which can enable them to gather forensic evidence. One example would come with network packet captures, for damage assessment. Only now, after progressing through the primary six phases, can intruders take actions to realize their original objectives. Typically, the target of knowledge exfiltration involves collecting, encrypting and extracting information from the victim(s) environment; violations of knowledge integrity or availability are potential objectives also . Alternatively, and most ordinarily , the intruder may only desire access to the initial victim box to be used as a hop point to compromise additional systems and move laterally inside the network. Once this stage is identified within an environment, the implementation of prepared reaction plans must be initiated. At a minimum, the plan should include a comprehensive communication plan, detailed evidence must be elevated to the very best ranking official or board , the deployment of end-point security tools to dam data loss and preparation for briefing a CIRT Team. Having these resources well established beforehand may be a “MUST” in today’s quickly evolving landscape of cybersecurity threats

QUESTION 76

Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently. Abel is verifying and validating image contents, signing images, and sending them to the registries. Which of the following tiers of the container technology architecture Is Abel currently working in?

* Tier-1: Developer machines
* Tier-4: Orchestrators
* Tier-3: Registries
* Tier-2: Testing and accreditation systems

Explanation

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization to operate (ATO).

Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization.

Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter.

For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary. Rationale: The Risk Management Framework uses a new term to refer to the concept of accreditation, and it is called authorization.

Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

QUESTION 77

What did the following commands determine?

```
C: user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

* That the Joe account has a SID of 500
* These commands demonstrate that the guest account has NOT been disabled
* These commands demonstrate that the guest account has been disabled
* That the true administrator is Joe
* Issued alone, these commands prove nothing

QUESTION 78

Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfilltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs, what type of malware did the attacker use to bypass the company’s application whitelisting?
* Phishing malware
* Zero-day malware
* File-less malware
* Logic bomb malware
https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html

QUESTION 79

Which of the following is a component of a risk assessment?
* Administrative safeguards
* Physical security
* DMZ
* Logical interface

QUESTION 80

Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes WI-FI sync on the computer so that the device could continue communication with that computer even after being physically disconnected.

Now, Clark gains access to Steven’s iPhone through the infected computer and is able to monitor and read all of Steven’s activity on the iPhone, even after the device is out of the communication zone.

Which of the following attacks is performed by Clark in above scenario?
* IOS trustjacking
* lOS Jailbreaking
* Exploiting SS7 vulnerability
* Man-in-the-disk attack
Explanation

An iPhone client’s most noticeably terrible bad dream is to have somebody oversee his/her gadget, including the capacity to record and control all action without waiting be in a similar room. In this blog entry, we present another weakness called “Trustjacking”, which permits an aggressor to do precisely that.

This weakness misuses an iOS highlight called iTunes Wi-Fi sync, which permits a client to deal with their iOS gadget without genuinely interfacing it to their PC. A solitary tap by the iOS gadget proprietor when the two are associated with a similar organization permits an assailant to oversee the gadget. Furthermore, we will stroll through past related weaknesses and show the progressions that iPhone has made to alleviate them, and why these are adequately not to forestall comparative assaults.

After interfacing an iOS gadget to another PC, the clients are being found out if they trust the associated PC or not. Deciding to believe the PC permits it to speak with the iOS gadget by means of the standard iTunes APIs.

This permits the PC to get to the photographs on the gadget, perform reinforcement, introduce applications and considerably more, without requiring another affirmation from the client and with no recognizable sign.

Besides, this permits enacting the “iTunes Wi-Fi sync” highlight, which makes it conceivable to proceed with this sort of correspondence with the gadget even after it has been detached from the PC, as long as the PC and the iOS gadget are associated with a similar organization. It is intriguing to take note of that empowering

“iTunes Wi-Fi sync” doesn’t need the casualty’s endorsement and can be directed simply from the PC side.

Getting a live stream of the gadget’s screen should be possible effectively by consistently requesting screen captures and showing or recording them distantly.

It is imperative to take note of that other than the underlying single purpose of disappointment, approving the vindictive PC, there is no other component that forestalls this proceeded with access. Likewise, there isn’t anything that informs the clients that by approving the PC they permit admittance to their gadget even in the wake of detaching the USB link.

QUESTION 81

Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes, images, and networks.

What is the component of the Docker architecture used by Annie in the above scenario?
* Docker objects
* Docker daemon
* Docker client
* Docker registries