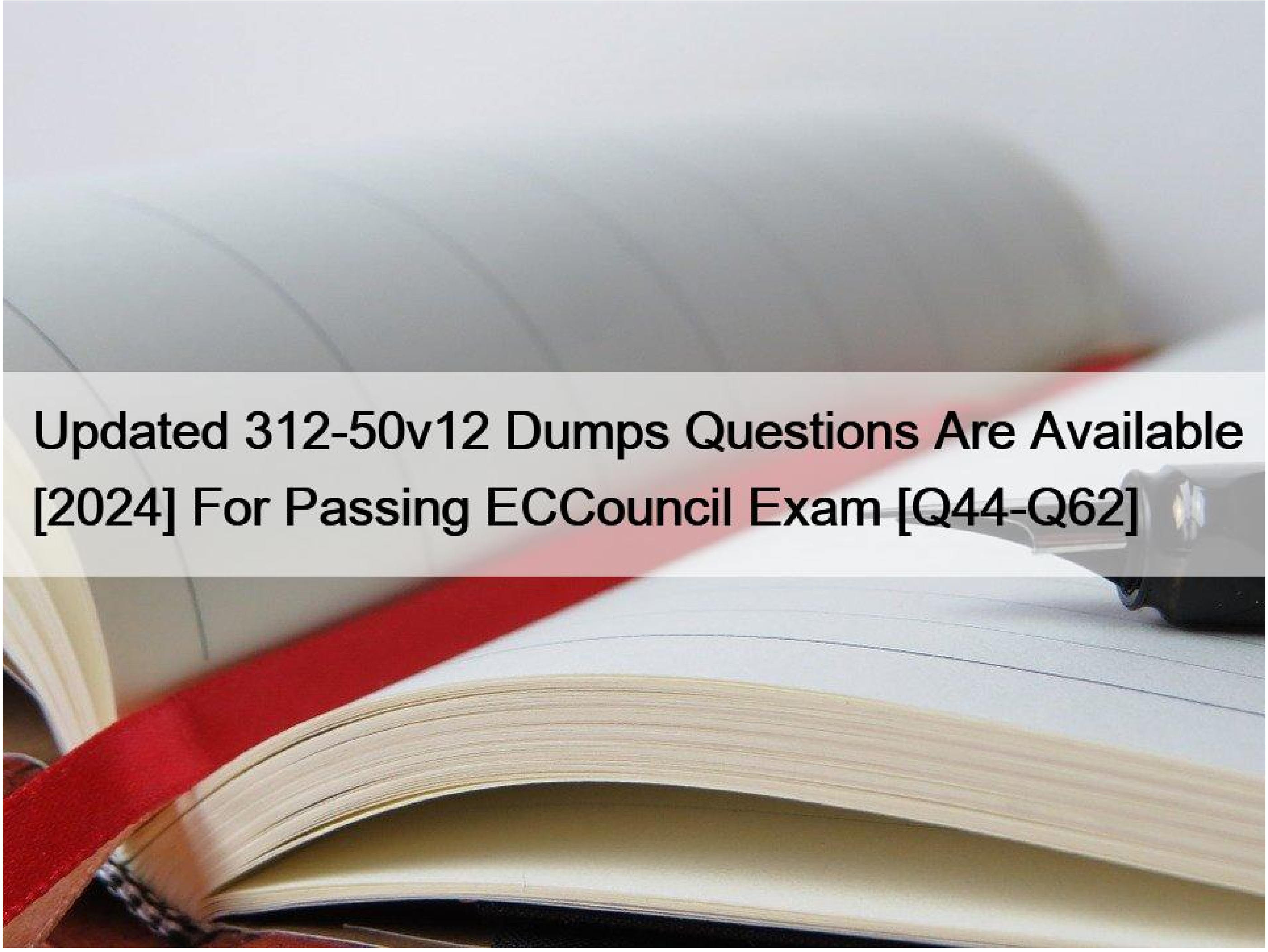
Updated 312-50v12 Dumps Questions Are Available [2024 For Passing ECCouncil Exam [Q44-Q62



Updated 312-50v12 Dumps Questions Are Available [2024] For Passing ECCouncil Exam
Free UPDATED ECCouncil 312-50v12 Certification Exam Dumps is Online

ECCouncil 312-50v12, also known as the Certified Ethical Hacker (CEH) Certification Exam, is an assessment that evaluates an individual's knowledge and skills in ethical hacking. Certified Ethical Hacker Exam certification is designed for professionals who want to become experts in the field of network security and vulnerability assessment. With the CEH credential, individuals can showcase their expertise in identifying security threats, understanding the latest hacking techniques and tools, and implementing countermeasures to protect their organization's infrastructure.

NEW QUESTION 44

Which file is a rich target to discover the structure of a website during web-server footprinting?

- Document root
- Robots.txt
- domain.txt
- index.html

Information Gathering from Robots.txt File A website owner creates a robots.txt file to list the files or directories a web crawler should index for providing search results. Poorly written robots.txt files can cause the complete indexing of website files and directories. If confidential files and directories are indexed, an attacker may easily obtain information such as passwords, email addresses, hidden links, and membership areas. If the owner of the target website writes the robots.txt file without allowing the indexing of restricted pages for providing search results, an attacker can still view the robots.txt file of the site to discover restricted files and then view them to gather information. An attacker types URL/robots.txt in the address bar of a browser to view the target website&#8217;s robots.txt file. An attacker can also download the robots.txt file of a target website using the Wget tool. Certified Ethical Hacker(CEH) Version 11 pg 1650

NEW QUESTION 45

When considering how an attacker may exploit a web server, what is web server footprinting?

- When an attacker implements a vulnerability scanner to identify weaknesses
- When an attacker creates a complete profile of the site&#8217;s external links and file structures
- When an attacker gathers system-level data, including account details and server names
- When an attacker uses a brute-force attack to crack a web-server password

NEW QUESTION 46

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

NEW QUESTION 47

Clark, a professional hacker, was hired by an organization lo gather sensitive Information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whole footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network. What is the online tool employed by Clark in the above scenario?

- AOL
- ARIN
- DuckDuckGo
- Baidu

https://search.arin.net/rdap/?query=199.43.0.43

NEW QUESTION 48

Why should the security analyst disable/remove unnecessary ISAPI filters?

- To defend against social engineering attacks
- To defend against webserver attacks

* To defend against jailbreaking
* To defend against wireless attacks

NEW QUESTION 49

You are using a public Wi-Fi network inside a coffee shop. Before surfing the web, you use your VPN to prevent intruders from sniffing your traffic. If you did not have a VPN, how would you identify whether someone is performing an ARP spoofing attack on your laptop?
* You should check your ARP table and see if there is one IP address with two different MAC addresses.
* You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.
* You should use netstat to check for any suspicious connections with another IP address within the LAN.
* You cannot identify such an attack and must use a VPN to protect your traffic, r
ARP Spoofing Attack ARP packets can be forged to send data to the attacker&#8217;s machine.Attackers flood a target computer&#8217;s ARP cache with forged entries, which is also known as poisoning. (P.1143/1127)

NEW QUESTION 50

You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.

invictus@victim_server.~$ nmap -T4 -O 10.10.0.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!

What seems to be wrong?
* The nmap syntax is wrong.
* This is a common behavior for a corrupted nmap application.
* The outgoing TCP/IP fingerprinting is blocked by the host firewall.
* OS Scan requires root privileges.

NEW QUESTION 51

Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company&#8217;s network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161. what protocol is this port using and how can he secure that traffic?
* it is not necessary to perform any actions, as SNMP is not carrying important information.
* SNMP and he should change it to SNMP V3
* RPC and the best practice is to disable RPC completely
* SNMP and he should change it to SNMP v2, which is encrypted
We have various articles already in our documentation for setting up SNMPv2 trap handling in Opsview, but SNMPv3 traps are a whole new ballgame. They can be quite confusing and complicated to set up the first time you go through the process, but when you understand what is going on, everything should make more sense.

SNMP has gone through several revisions to improve performance and security (version 1, 2c and 3). By default, it is a UDP port based protocol where communication is based on a &#8216;fire and forget&#8217; methodology in which network packets are sent to another device, but there is no check for receipt of that packet (versus TCP port when a network packet must be acknowledged by the other end of the communication link).

There are two modes of operation with SNMP &#8211; get requests (or polling) where one device requests information from an SNMP enabled device on a regular basis (normally using UDP port 161), and traps where the SNMP enabled device sends a message to another device when an event occurs (normally using UDP port 162). The latter includes instances such as someone logging on, the device powering up or down, or a wide variety of other problems that would need this type of investigation.

This blog covers SNMPv3 traps, as polling and version 2c traps are covered elsewhere in our documentation.

SNMP traps

Since SNMP is primarily a UDP port based system, traps may be &#8216;lost&#8217; when sending between devices; the sending device does not wait to see if the receiver got the trap. This means if the configuration on the sending device is wrong (using the wrong receiver IP address or port) or the receiver isn&#8217;t listening for traps or rejecting them out of hand due to misconfiguration, the sender will never know.

The SNMP v2c specification introduced the idea of splitting traps into two types; the original &#8216;hope it gets there&#8217; trap and the newer &#8216;INFORM&#8217; traps. Upon receipt of an INFORM, the receiver must send an acknowledgement back. If the sender doesn&#8217;t get the acknowledgement back, then it knows there is an existing problem and can log it for sysadmins to find when they interrogate the device.

NEW QUESTION 52

What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?
* Man-in-the-middle attack
* Meet-in-the-middle attack
* Replay attack
* Traffic analysis attack
https://en.wikipedia.org/wiki/Meet-in-the-middle_attack

The meet-in-the-middle attack (MITM), a known plaintext attack, is a generic space-time tradeoff cryptographic attack against encryption schemes that rely on performing multiple encryption operations in sequence. The MITM attack is the primary reason why Double DES is not used and why a Triple DES key (168-bit) can be bruteforced by an attacker with 256 space and 2112 operations.

The intruder has to know some parts of plaintext and their ciphertexts. Using meet-in-the-middle attacks it is possible to break ciphers, which have two or more secret keys for multiple encryption using the same algorithm. For example, the 3DES cipher works in this way. Meet-in-the-middle attack was first presented by Diffie and Hellman for cryptanalysis of DES algorithm.

NEW QUESTION 53

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

NEW QUESTION 54

What is the main security service a cryptographic hash provides?
* Integrity and ease of computation
* Message authentication and collision resistance
* Integrity and collision resistance
* Integrity and computational in-feasibility

NEW QUESTION 55

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&#8217;s private key
* Alice&#8217;s public key
* His own private key
* His own public key

NEW QUESTION 56

This kind of password cracking method uses word lists in combination with numbers and special characters:

* Hybrid
* Linear
* Symmetric
* Brute Force

NEW QUESTION 57

Jack, a disgruntled ex-employee of Incalsol Ltd., decided to inject fileless malware into Incalsol&#8217;s systems. To deliver the malware, he used the current employees&#8217; email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate. When a victim employee clicks on the link, they are directed to a fraudulent website that automatically loads Flash and triggers the exploit. What is the technique used byjack to launch the fileless malware on the target systems?

* In-memory exploits
* Phishing
* Legitimate applications
* Script-based injection

Launching Fileless Malware through Phishing Attackers commonly use social engineering techniques such as phishing to spread fileless malware to the target systems. Fileless malware exploits vulnerabilities in system tools to load and run malicious payloads on the victim&#8217;s machine to compromise the sensitive information stored in the process memory. (P.978/962)

NEW QUESTION 58

Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob&#8217;s boss is very worried because of regulations that protect those dat a. Which of the following regulations is mostly violated?

* HIPPA/PHl
* Pll
* PCIDSS
* ISO 2002

PHI stands for Protected Health info. The HIPAA Privacy Rule provides federal protections for private health info held by lined entities and provides patients an array of rights with regard to that info. under HIPAA phi is considered to be any identifiable health info that&#8217;s used, maintained, stored, or transmitted by a HIPAA-covered entity &#8211; a healthcare provider, health plan or health insurer, or a aid clearinghouse &#8211; or a business associate of a HIPAA-covered entity, in relation to the availability of aid or payment for aid services.

It is not only past and current medical info that&#8217;s considered letter under HIPAA Rules, however also future info concerning medical conditions or physical and mental health related to the provision of care or payment for care. phi is health info in any kind, together with physical records, electronic records, or spoken info.

Therefore, letter includes health records, medical histories, lab check results, and medical bills. basically, all health info is considered letter once it includes individual identifiers. Demographic info is additionally thought of phi underneath HIPAA Rules, as square measure several common identifiers like patient names, Social Security numbers, Driver&#8217;s license numbers, insurance details, and birth dates, once they square measure connected with health info.

The eighteen identifiers that create health info letter are:

Names

Dates, except year

phonephone numbers

Geographic information

FAX numbers

Social Security numbers

Email addresses

case history numbers

Account numbers

Health arrange beneficiary numbers

Certificate/license numbers

Vehicle identifiers and serial numbers together with license plates

Web URLs

Device identifiers and serial numbers

net protocol addresses

Full face photos and comparable pictures

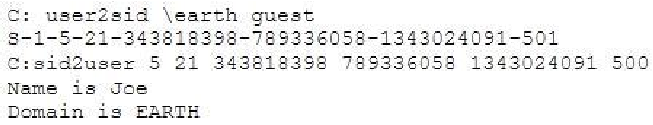
Biometric identifiers (i.e. retinal scan, fingerprints)

Any distinctive identifying variety or code

One or a lot of of those identifiers turns health info into letter, and phi HIPAA Privacy Rule restrictions can then apply that limit uses and disclosures of the data. HIPAA lined entities and their business associates will ought to guarantee applicable technical, physical, and body safeguards are enforced to make sure the confidentiality, integrity, and availability of phi as stipulated within the HIPAA Security Rule.

NEW QUESTION 59

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

NEW QUESTION 60

__________ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.
* Trojan
* RootKit
* DoS tool
* Scanner
* Backdoor

NEW QUESTION 61

While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?
* -sA
* -sX
* -sT
* -sF

NEW QUESTION 62

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?
* Reverse Social Engineering
* Tailgating
* Piggybacking
* Announced
* Identifying operating systems, services, protocols and devices,

* Collecting unencrypted information about usernames and passwords,

* Capturing network traffic for further analysis

are passive network sniffing methods since with the help of them we only receive information and do not make any changes to the target network. When modifying and replaying the captured network traffic, we are already starting to make changes and actively interact with it.

ECCouncil Exam 2024 312-50v12 Dumps Updated Questions: https://www.dumpsmaterials.com/312-50v12-real-torrent.html]