312-50V12 Q&As

Certified Ethical Hacker Exam (CEHv12)

Pass EC-COUNCIL 312-50V12 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/312-50v12.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What is the following command used for?

sqlmap.py-u ,,http://10.10.1.20/?p=1andforumaction=search" -dbs

A. Creating backdoors using SQL injection

B. A Enumerating the databases in the DBMS for the URL

C. Retrieving SQL statements being executed on the database

D. Searching database statements at the IP address given

Correct Answer: A

QUESTION 2

Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it. Which of the following tools did Bob employ to gather the above Information?

A. search.com

B. EarthExplorer

C. Google image search

D. FCC ID search

Correct Answer: D

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques ncludes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc. pg. 5052 ECHv11 manual

https://en.wikipedia.org/wiki/FCC_mark An FCC ID is a unique identifier assigned to a device registered with the United States Federal Communications Commission. For legal sale of wireless deices in the US, manufacturers must: ?Have the device evaluated by an independent lab to ensure it conforms to FCC standards ?Provide documentation to the FCC of the lab results ?Provide User Manuals, Documentation, and Photos relating to the device ?Digitally or physically label the device with the unique identifier provided by the FCC (upon approved application) The FCC gets its authourity from Title 47 of the Code of Federal Regulations (47 CFR). FCC IDs are required for all wireless emitting devices sold in the USA. By searching an FCC ID, you can find details on the wireless operating frequency (including strength), photos of the device, user manuals for the device, and SAR reports on the wireless emissions

QUESTION 3

How can rainbow tables be defeated?

A. Use of non-dictionary words

B. All uppercase character passwords

C. Password salting

D. Lockout accounts under brute force password cracking attempts

Correct Answer: C

https://en.wikipedia.org/wiki/Salt_(cryptography)

A salt is random data that is used as an additional input to a one-way function that hashes data, a password, or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time additional safeguards were developed to protect a user\\'s password against being read from the system. A salt is one of those methods.

A new salt is randomly generated for each password. In a typical setting, the salt and the password (or its version after key stretching) are concatenated and processed with a cryptographic hash function, and the output hash value (but not the original password) is stored with the salt in a database. Hashing allows for later authentication without keeping and therefore risking exposure of the plaintext password in the event that the authentication data store is compromised. Salts defend against a pre-computed hash attack, e.g. rainbow tables. Since salts do not have to be memorized by humans they can make the size of the hash table required for a successful attack prohibitively large without placing a burden on the users. Since salts are different in each case, they also protect commonly used passwords, or those users who use the same password on several sites, by making all salted hash instances for the same password different from each other.

QUESTION 4

Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 64

B. 128

C. 255

D. 138

Correct Answer: B

Windows TTL 128, Linux TTL 64, OpenBSD 255 ...

https://subinsb.com/default-device-ttl-values/

Time to Live (TTL) represents to number of \\'hops\\' a packet can take before it is considered invalid. For Windows/Windows Phone, this value is 128. This value is 64 for Linux/Android.

QUESTION 5

You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to

be accessible. But they are not accessible when you try using the URL.

What may be the problem?

A. Traffic is Blocked on UDP Port 53

B. Traffic is Blocked on TCP Port 80

C. Traffic is Blocked on TCP Port 54

D. Traffic is Blocked on UDP Port 80

Correct Answer: A

Most likely have an issue with DNS.

DNS stands for "Domain Name System." It\\'s a system that lets you connect to websites by matching human-readable domain names (like example.com) with the server\\'s unique ID where a website is stored.

Think of the DNS system as the internet\\'s phonebook. It lists domain names with their corresponding identifiers called IP addresses, instead of listing people\\'s names with their phone numbers. When a user enters a domain name like

wpbeginner.com on their device, it looks up the IP address and connects them to the physical location where that website is stored.

NOTE: Often DNS lookup information will be cached locally inside the querying computer or remotely in the DNS infrastructure. There are typically 8 steps in a DNS lookup. When DNS information is cached, steps are skipped from the DNS

lookup process, making it quicker. The example below outlines all 8 steps when nothing is cached.

The 8 steps in a DNS lookup:

1.

A user types `example.com\\' into a web browser, and the query travels into the Internet and is received by a DNS recursive resolver;

2.

The resolver then queries a DNS root nameserver;

3.

The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward

the .com TLD;

4.

The resolver then requests the .com TLD;

5.

The TLD server then responds with the IP address of the domain\\'s nameserver, example.com;

6.

Lastly, the recursive resolver sends a query to the domain\\'s nameserver;

7.

The IP address for example.com is then returned to the resolver from the nameserver;

8.

The DNS resolver then responds to the web browser with the IP address of the domain requested initially;

Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser can request the web page:

9.

The browser makes an HTTP request to the IP address;

10.

The server at that IP returns the webpage to be rendered in the browser. NOTE 2: DNS primarily uses the User Datagram Protocol (UDP) on port number 53 to serve requests. And if this port is blocked, then a problem arises already in

the first step.

But the ninth step is performed without problems.