312-50V10 Q&As

Certified Ethical Hacker Exam (C|EH v10)

Pass EC-COUNCIL 312-50V10 Exam with 100% Guarantee

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

https://www.pass2lead.com/312-50v10.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What is correct about digital signatures?

A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.

B. Digital signatures may be used in different documents of the same type.

C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.

D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Correct Answer: A

QUESTION 2

> NMAP -sn 192.168.11.200-215

The NMAP command above performs which of the following?

A. A ping scan

B. A trace sweep

C. An operating system detect

D. A port scan

Correct Answer: A

NMAP -sn (No port scan)

This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that

responded to the host discovery probes. This is often known as a "ping scan", but you can also request

that traceroute and NSE host scripts be run.

References: https://nmap.org/book/man-host-discovery.html

QUESTION 3

One of your team members has asked you to analyze the following SOA record.

What is the TTL? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)

A. 200303028

B. 3600

C. 604800

D. 2400

E. 60

F. 4800

Correct Answer: D

QUESTION 4

You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator\\'s bank account password and login information for the administrator\\'s bitcoin account.

What should you do?

A. Report immediately to the administrator

B. Do not report it and continue the penetration test.

C. Transfer money from the administrator\\'s account to another account.

D. Do not transfer the money but steal the bitcoins.

Correct Answer: A

QUESTION 5

A penetration tester is hired to do a risk assessment of a company\\'s DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

A. white box

B. grey box

C. red box

D. black box

Correct Answer: D

QUESTION 6

You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.

What tool will help you with the task?

A. Metagoofil

B. Armitage

C. Dimitry

D. cdpsnarf

Correct Answer: A

Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company.

Metagoofil will perform a search in Google to identify and download the documents to local disk and then will extract the metadata with different libraries like Hachoir, PdfMiner? and others. With the results it will generate a report with usernames, software versions and servers or machine names that will help Penetration testers in the information gathering phase.

References: http://www.edge-security.com/metagoofil.php

QUESTION 7

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

A. har.txt

B. SAM file

C. wwwroot D. Repair file

Correct Answer: B

QUESTION 8

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
```

A. That the Joe account has a SID of 500

B. These commands demonstrate that the guest account has NOT been disabled

C. These commands demonstrate that the guest account has been disabled

D. That the true administrator is Joe

E. Issued alone, these commands prove nothing

Correct Answer: D

QUESTION 9

Which utility will tell you in real time which ports are listening or in another state?

A. Netstat

B. TCPView

C. Nmap

D. Loki

Correct Answer: B

QUESTION 10

A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am.

Which of the following programming languages would most likely be used?

A. PHP

B. C#

C. Python

D. ASP.NET

Correct Answer: C

QUESTION 11

Which service in a PKI will vouch for the identity of an individual or company?

A. KDC

B. CA

C. CR

D. CBC

Correct Answer: B

QUESTION 12

Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

A. RSA 1024 bit strength

B. AES 1024 bit strength

C. RSA 512 bit strength

D. AES 512 bit strength

Correct Answer: A

QUESTION 13

What is the main difference between a "Normal" SQL Injection and a "Blind" SQL Injection vulnerability?

A. The request to the web server is not visible to the administrator of the vulnerable application.

B. The attack is called "Blind" because, although the application properly filters user input, it is still vulnerable to code injection.

C. The successful attack does not show an error message to the administrator of the affected application.

D. The vulnerable application does not display errors with information about the injection results to the attacker.

Correct Answer: D

QUESTION 14

Which of the following techniques will identify if computer files have been changed?

A. Network sniffing

B. Permission sets

C. Integrity checking hashes

D. Firewall alerts

Correct Answer: C

QUESTION 15

What is the process of logging, recording, and resolving events that take place in an organization?

A. Incident Management Process

B. Security Policy

C. Internal Procedure

D. Metrics

Correct Answer: A

The activities within the incident management process include:

References: https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_proced ure