



[EC-COUNCIL 312-50](#)

Exam Name: *Ethical Hacking and Countermeasures (CEHv6)*

Q & A : 574 Q&As

Pdf Demo

Quality and Value for the 312-50 Exam

[Just4Exams Practice Exams](#) for EC-COUNCIL Certified Ethical Hacker 312-50 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

100% Guarantee to Pass Your 312-50 Exam

If you do not pass the Certified Ethical Hacker 312-50 exam on your first attempt using our Just4Exams **312-50 testing engine and pdf study guide**, we will give you a FULL REFUND of your purchasing fee.

Downloadable, Interactive 312-50 Testing engines and PDF Version

Our Exam Preparation Material provides you everything you will need to take a [Certified Ethical Hacker certification](#) examination. Details are researched and produced by [EC-COUNCIL Certification](#) Experts who are constantly using industry experience to produce precise, and logical.

Free 312-50 Exams:

This is demo only, this pdf do not include the questions and answers picture

Exam : EC-Council 312-50

Title : Ethical Hacking and Countermeasures (CEHv6)

1. NSLookup is a good tool to use to gain additional information about a target network. What does the following command accomplish?

```
nslookup
```

```
> server <ipaddress>
```

```
> set type =any
```

```
> ls -d <target.com>
```

A. Enables DNS spoofing

B. Loads bogus entries into the DNS table

C. Verifies zone security

- D. Performs a zone transfer
- E. Resets the DNS cache

Answer: D

2. Which of the following tools are used for footprinting?(Choose four.

- A. Sam Spade
- B. NSLookup
- C. Traceroute
- D. Neotrace
- E. Cheops

Answer: ABCD

3. To what does "message repudiation" refer to what concept in the realm of email security?

- A. Message repudiation means a user can validate which mail server or servers a message was passed through.
- B. Message repudiation means a user can claim damages for a mail message that damaged their reputation.
- C. Message repudiation means a recipient can be sure that a message was sent from a particular person.
- D. Message repudiation means a recipient can be sure that a message was sent from a certain host.
- E. Message repudiation means a sender can claim they did not actually send a particular message.

Answer: E

4. How does Traceroute map the route that a packet travels from point A to point B?

- A. It uses a TCP Timestamp packet that will elicit a time exceed in transit message.
- B. It uses a protocol that will be rejected at the gateways on its way to its destination.
- C. It manipulates the value of time to live (TTL) parameter packet to elicit a time exceeded in transit message.
- D. It manipulated flags within packets to force gateways into generating error messages.

Answer: C

5. A very useful resource for passively gathering information about a target company is:

- A. Host scanning
- B. Whois search
- C. Traceroute
- D. Ping sweep

Answer: B

6. What is "Hacktivism"?

- A. Hacking for a cause
- B. Hacking ruthlessly
- C. An association which groups activists
- D. None of the above

Answer: A

7. What is the essential difference between an 'Ethical Hacker' and a 'Cracker'?

- A. The ethical hacker does not use the same techniques or skills as a cracker.
- B. The ethical hacker does it strictly for financial motives unlike a cracker.
- C. The ethical hacker has authorization from the owner of the target.
- D. The ethical hacker is just a cracker who is getting paid.

Answer: C

8. While footprinting a network, what port/service should you look for to attempt a zone transfer?

- A. 53 UDP
- B. 53 TCP
- C. 25 UDP
- D. 25 TCP
- E. 161 UDP
- F. 22 TCP
- G. 60 TCP

Answer: B

9. Doug is conducting a port scan of a target network. He knows that his client target network has a web server and that there is a mail server also which is up and running. Doug has been sweeping the network but has not been able to elicit any response from the remote target. Which of the following could be the most likely cause behind this lack of response? Select 4.

- A. UDP is filtered by a gateway
- B. The packet TTL value is too low and cannot reach the target
- C. The host might be down
- D. The destination network might be down
- E. The TCP windows size does not match
- F. ICMP is filtered by a gateway

Answer: ABCF

10. Who is an Ethical Hacker?

- A. A person who hacks for ethical reasons
- B. A person who hacks for an ethical cause
- C. A person who hacks for defensive purposes
- D. A person who hacks for offensive purposes

Answer: C

11. Your Certkiller trainee Sandra asks you which are the four existing Regional Internet Registry (RIR's)?

- A. APNIC, PICNIC, ARIN, LACNIC
- B. RIPE NCC, LACNIC, ARIN, APNIC
- C. RIPE NCC, NANIC, ARIN, APNIC
- D. RIPE NCC, ARIN, APNIC, LATNIC

Answer: B

12. Exhibit

Joe Hacker runs the hping2 hacking tool to predict the target host's sequence numbers in one of the hacking session.

What does the first and second column mean? Select two.

- A. The first column reports the sequence number
- B. The second column reports the difference between the current and last sequence number
- C. The second column reports the next sequence number
- D. The first column reports the difference between current and last sequence number

Answer: AB

13. Bob has been hired to perform a penetration test on Certkiller .com. He begins by looking at IP address ranges owned by the company and details of domain name registration. He then goes to News Groups and financial web sites to see if they are leaking any sensitive information or have any technical details online. Within the context of penetration testing methodology, what phase is Bob involved with?

- A. Passive information gathering
- B. Active information gathering
- C. Attack phase
- D. Vulnerability Mapping

Answer: A

14. You receive an email with the following message:

Hello Steve, We are having technical difficulty in restoring user database record after the recent blackout. Your account data is corrupted.

Please logon to the SuperEmailServices.com and change your password.

<http://www.supermailservices.com@0xde.0xad.0xbe.0xef/support/login.htm> If you do not reset your password within 7 days, your account will be permanently disabled locking you out from our e-mail services.

Sincerely,

Technical Support

SuperEmailServices

From this e-mail you suspect that this message was sent by some hacker since you have been using their e-mail services for the last 2 years and they have never sent out an e-mail such as this. You also observe the URL in the message and confirm your suspicion about 0xde.0xad.0xbde.0xef which looks like hexadecimal numbers. You immediately enter the following at Windows 2000 command prompt:

Ping0xde.0xad.0xbe.0xef

You get a response with a valid IP address.

What is the obstructed IP address in the e-mail URL?

- A. 222.173.190.239
- B. 233.34.45.64
- C. 54.23.56.55
- D. 199.223.23.45

Answer: A

15. The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts;

however, a few are successful. Study the log given below and answer the following question:

(Note: The objective of this questions is to test whether the student has learnt about passive OS fingerprinting (which should tell them the OS from log captures): can they tell a SQL injection attack signature; can they infer if a user ID has been created by an attacker and whether they can read plain source - destination entries from log entries.)

What can you infer from the above log?

- A. The system is a windows system which is being scanned unsuccessfully.
- B. The system is a web application server compromised through SQL injection.
- C. The system has been compromised and backdoored by the attacker.
- D. The actual IP of the successful attacker is 24.9.255.53.

Answer: A

16. According to the CEH methodology, what is the next step to be performed after footprinting?

- A. Enumeration
- B. Scanning
- C. System Hacking
- D. Social Engineering
- E. Expanding Influence

Answer: B

17. While performing a ping sweep of a subnet you receive an ICMP reply of Code 3/Type 13 for all the pings sent out.

What is the most likely cause behind this response?

- A. The firewall is dropping the packets.
- B. An in-line IDS is dropping the packets.
- C. A router is blocking ICMP.
- D. The host does not respond to ICMP packets.

Answer: C

18. Where should a security tester be looking for information that could be used by an attacker against an organization? (Select all that apply)

- A. CHAT rooms
- B. WHOIS database
- C. News groups
- D. Web sites
- E. Search engines
- F. Organization's own web site

Answer: ABCDEF

19. You are footprinting an organization to gather competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but not it is not there.

How would it be possible for you to retrieve information from the website that is outdated?

- A. Visit google's search engine and view the cached copy.
- B. Visit Archive.org web site to retrieve the Internet archive of the company's website.
- C. Crawl the entire website and store them into your computer.
- D. Visit the company's partners and customers website for this information.

Answer: B

20. A Certkiller security System Administrator is reviewing the network system log files.

He notes the following:

- Network log files are at 5 MB at 12:00 noon.
- At 14:00 hours, the log files at 3 MB.

What should he assume has happened and what should he do about the situation?

- A. He should contact the attacker's ISP as soon as possible and have the connection disconnected.
- B. He should log the event as suspicious activity, continue to investigate, and take further steps according to site security policy.
- C. He should log the file size, and archive the information, because the router crashed.
- D. He should run a file system check, because the Syslog server has a self correcting file system problem.
- E. He should disconnect from the Internet discontinue any further unauthorized use, because an attack has taken place.

Answer: B

21. You are footprinting Acme.com to gather competitive intelligence. You visit the acme.com websire for contact information and telephone number numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12

months ago but now it is not there. How would it be possible for you to retrieve information from the website that is outdated?

- A. Visit google search engine and view the cached copy.
- B. Visit Archive.org site to retrieve the Internet archive of the acme website.
- C. Crawl the entire website and store them into your computer.
- D. Visit the company's partners and customers website for this information.

Answer: B

22. Which of the following would be the best reason for sending a single SMTP message to an address that does not exist within the target company?

- A. To create a denial of service attack.
- B. To verify information about the mail administrator and his address.
- C. To gather information about internal hosts used in email treatment.
- D. To gather information about procedures that are in place to deal with such messages.

Answer: C

23. Your lab partner is trying to find out more information about a competitors web site. The site has a .com extension. She has decided to use some online whois tools and look in one of the regional Internet registrys. Which one would you suggest she looks in first?

- A. LACNIC
- B. ARIN
- C. APNIC
- D. RIPE
- E. AfriNIC

Answer: B

24. Which of the following activities will NOT be considered as passive footprinting?

- A. Go through the rubbish to find out any information that might have been discarded.
- B. Search on financial site such as Yahoo Financial to identify assets.
- C. Scan the range of IP address found in the target DNS database.
- D. Perform multiples queries using a search engine.

Answer: C

25. Network Administrator Patricia is doing an audit of the network. Below are some of her findings concerning DNS. Which of these would be a cause for alarm? Select the best answer.

- A. There are two external DNS Servers for Internet domains. Both are AD integrated.
- B. All external DNS is done by an ISP.
- C. Internal AD Integrated DNS servers are using private DNS names that are
- D. unregistered.
- E. Private IP addresses are used on the internal network and are registered with the internal AD integrated DNS server.

Answer: A

26. Which one of the following is defined as the process of distributing incorrect Internet Protocol (IP) addresses/names with the intent of diverting traffic?

- A. Network aliasing
- B. Domain Name Server (DNS) poisoning
- C. Reverse Address Resolution Protocol (ARP)
- D. Port scanning

Answer: B

27. What does the term "Ethical Hacking" mean?

- A. Someone who is hacking for ethical reasons.
- B. Someone who is using his/her skills for ethical reasons.
- C. Someone who is using his/her skills for defensive purposes.
- D. Someone who is using his/her skills for offensive purposes.

Answer: C

28. User which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

- A. 18 U.S.C 1029 Possession of Access Devices
- B. 18 U.S.C 1030 Fraud and related activity in connection with computers
- C. 18 U.S.C 1343 Fraud by wire, radio or television
- D. 18 U.S.C 1361 Injury to Government Property
- E. 18 U.S.C 1362 Government communication systems

F. 18 U.S.C 1831 Economic Espionage Act

G. 18 U.S.C 1832 Trade Secrets Act

Answer: B

29. Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?

(Note: The student is being tested on concept learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)

```
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1 TCP TTL:44 TOS:0x10 ID:242
```

```
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
```

...

```
05/20-17:06:58.685879 192.160.13.4:31337 ->
```

```
172.16.1.101:1024
```

```
TCP TTL:44 TOS:0x10 ID:242
```

```
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
```

What is odd about this attack? (Choose the most appropriate statement)

- A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
- B. This is back orifice activity as the scan comes from port 31337.
- C. The attacker wants to avoid creating a sub-carrier connection that is not normally valid.
- D. These packets were created by a tool; they were not created by a standard IP stack.

Answer: B

30. What are the two basic types of attacks?(Choose two.

- A. DoS
- B. Passive
- C. Sniffing
- D. Active
- E. Cracking

Answer: BD

More [312-50 Braindumps](#) Information

Related 312-50 Exams

EC0-350 312-49 312-50 EC0-349

Other EC-COUNCIL Exams

EC0-349 EC0-479 EC0-350 312-50 EC0-232
412-79 312-49