

## 312-50

### Ethical Hacking and Countermeasures (CEHv6)

Version: Demo



## About Exambible

### *Your Partner of IT Exam*

## Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

1. 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**

2. 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**

3. 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**

4. What is "Hacktivism"?

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

**Answer: A**

5. 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:** A, B, C, D, E, F

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

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

**Answer:** B, D

7. You are footprinting Acme.com to gather competitive intelligence. You visit the acme.com 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 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**

8. 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**

9. 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**

10. 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**

11. 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 now 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 website 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**

12. 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 are 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 to discontinue any further unauthorized use, because an attack has taken place.

**Answer: B**

13. 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**

14. 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 exceeded 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**

15. 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 dumo.)

```
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**

16. 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**

17. 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**

18. 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/logon.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**

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

A. Sam Spade

B. NSLookup

C. Traceroute

D. Neotrace

E. Cheops

**Answer: A, B, C, D**

20. 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**

## Relate Links

**100% Pass Your 312-50 Exam with Exambible Prep Materials**

<http://www.exambible.com/312-50-exam/>

## Contact us

**We are proud of our high-quality customer service, which serves you around the clock 24/7.**

**Viste - <http://www.exambible.com/>**