

**Exam** : **[EC-Council 312-50](#)**

**Title** : **Ethical Hacking and  
Countermeasures (CEHv6)**

**Version** : **Demo**

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**

Explanation: The ethical hacker uses the same techniques and skills as a cracker and the motive is to find the security breaches before a cracker does. There is nothing that says that a cracker does not get paid for the work he does, a ethical hacker has the owners authorization and will get paid even if he does not succeed to penetrate the target.

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**

Explanation: Ethical hacking is only about defending your self or your employer against malicious persons by using the same techniques and skills.

3. Who is an Ethical Hacker?

- A. A person whohacksfor ethical reasons
- B. A person whohacksfor an ethical cause
- C. A person whohacksfor defensive purposes
- D. A person whohacksfor offensive purposes

**Answer: C**

Explanation: The Ethical hacker is a security professional who applies his hacking skills for defensive purposes.

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**

Explanation: The term was coined by author/critic Jason Logan Bill Sack in an article about media artist Shu Lea Cheang. Acts of hacktivism are carried out in the belief that proper use of code will have leveraged effects similar to regular activism or civil disobedience.

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: ABCDEF**

Explanation: A Security tester should search for information everywhere that he/she can access. You never know where you find that small piece of information that could penetrate a strong defense.

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

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

**Answer: BD**

Explanation: Passive and active attacks are the two basic types of attacks.

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**

Explanation: The Internet Archive (IA) is a non-profit organization dedicated to maintaining an archive of Web and multimedia resources. Located at the Presidio in San Francisco, California, this archive includes "snapshots of the World Wide Web" (archived copies of pages, taken at various points in time), software, movies, books, and audio recordings (including recordings of live concerts from bands that allow it). This site is found at [www.archive.org](http://www.archive.org).

8. Under 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**

Explanation: [http://www.law.cornell.edu/uscode/html/uscode18/usc\\_sec\\_18\\_00001030----000-.html](http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html)

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**

Explanation: Passive footprinting is a method in which the attacker never makes contact with the target systems. Scanning the range of IP addresses found in the target DNS is considered making contact to the systems behind the IP addresses that is targeted by the scan.

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**

Explanation: This reference is close to the one listed DNS poisoning is the correct answer. This is how DNS DOS attack can occur. If the actual DNS records are unattainable to the attacker for him to alter in this fashion, which they should be, the attacker can insert this data into the cache of there server instead of replacing the actual records, which is referred to as cache poisoning.

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 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**

Explanation: Archive.org mirrors websites and categorizes them by date and month depending on the crawl

time. Archive.org dates back to 1996, Google is incorrect because the cache is only as recent as the latest crawl, the cache is over-written on each subsequent crawl. Download the website is incorrect because that's the same as what you see online. Visiting customer partners websites is just bogus. The answer is then Firmly, C, archive.org

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 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**

Explanation: You should never assume a host has been compromised without verification. Typically, disconnecting a server is an extreme measure and should only be done when it is confirmed there is a compromise or the server contains such sensitive data that the loss of service outweighs the risk. Never assume that any administrator or automatic process is making changes to a system. Always investigate the root cause of the change on the system and follow your organizations security policy.

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**

Explanation: A quality that prevents a third party from being able to prove that a communication between two other parties ever took place. This is a desirable quality if you do not want your communications to be traceable. Non-repudiation is the opposite quality-a third party can prove that a communication between two other parties took place. Non-repudiation is desirable if you want to be able to trace your communications and prove that they occurred. Repudiation - Denial of message submission or delivery.

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 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**

Explanation:Traceroute works by increasing the "time-to-live" value of each successive batch of packets sent. The first three packets have a time-to-live (TTL) value of one (implying that they make a single hop). The next three packets have a TTL value of 2, and so on. When a packet passes through a host, normally the host decrements the TTL value by one, and forwards the packet to the next host. When a packet with a TTL of one reaches a host, the host discards the packet and sends an ICMP time exceeded (type 11) packet to the sender. The traceroute utility uses these returning packets to produce a list of hosts that the packets have traversed en route to the destination.

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\*\* Seg: 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**

Explanation: Port 31337 is normally used by Back Orifice. Note that 31337 is hackers spelling of 'elite', meaning 'elite hackers'.

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**

Explanation: All other answers include non existing organizations (PICNIC, NANIC, LATNIC). See [http://www.arin.net/library/internet\\_info/ripe.html](http://www.arin.net/library/internet_info/ripe.html)

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**

Explanation: A, C & D are "Active" scans, the question says: "Passively"

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

Explanation: 0x stands for hexadecimal and DE=222, AD=173, BE=190 and EF=239

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

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

**Answer:** ABCD

Explanation: All of the tools listed are used for footprinting except Cheops.

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**

Explanation: Once footprinting has been completed, scanning should be attempted next. Scanning should take place on two distinct levels: network and host.

21. 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**

Explanation: If DNS has not been properly secured, the command sequence displayed above will perform a zone transfer.

22. 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**

Explanation: IF TCP port 53 is detected, the opportunity to attempt a zone transfer is there.

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 registries.

Which one would you suggest she looks in first?

A. LACNIC

B. ARIN

C. APNIC

D. RIPE

E. AfriNIC

**Answer: B**

Explanation: Regional registries maintain records from the areas from which they govern. ARIN is responsible for domains served within North and South America and therefore, would be a good starting point for a .com domain.

24. 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**

Explanations:A. There are two external DNS Servers for Internet domains. Both are AD integrated. This is the correct answer. Having an AD integrated DNS external server is a serious cause for alarm. There is no

need for this and it causes vulnerability on the network.

B. All external DNS is done by an ISP.

This is not the correct answer. This would not be a cause for alarm. This would actually reduce the company's network risk as it is offloaded onto the ISP. C. Internal AD Integrated DNS servers are using private DNS names that are unregistered. This is not the correct answer. This would not be a cause for alarm. This would actually reduce the company's network risk. D. Private IP addresses are used on the internal network and are registered with the internal AD integrated DNS server.

This is not the correct answer. This would not be a cause for alarm. This would actually reduce the company's network risk.

25. 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

Explanation: If the destination host or the destination network is down there is no way to get an answer and if TTL (Time To Live) is set too low the UDP packets will "die" before reaching the host because of too many hops between the scanning computer and the target. The TCP receive window size is the amount of received data (in bytes) that can be buffered during a connection. The sending host can send only that amount of data before it must wait for an acknowledgment and window update from the receiving host and ICMP is mainly used for echo requests and not in port scans.

26. Exhibit

```
#hping2 192.168.8.46 --seqnum -p 139 -s -i u1 -I eth0
```

```
HPING uaz (eth0 192.168.8.46): S set, 40 headers + 0 data bytes
```

```
2361294848          +2361294848
2411626496          +50331648
2545844224          +134217728
2384705024          +167772160
2552477184          +167772160
3720249344          +167772160
3216932864          +167772160
3384705024          +167772160
3552477184          +167772160
3720249344          +167772160
3888021504          +167772160
4055793664          +167772160
4223565824          +167772160
```

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

27. 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

Explanation: Type 3 message = Destination Unreachable [RFC792], Code 13 (cause) = Communication Administratively Prohibited [RFC1812]

28. 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.)

```
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 ->
172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 ->
172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 ->
172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 63.226.81.13:1351 -> 172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 ->
172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 ->
172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by
(uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by
simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 ->
213.28.22.189:4558
```

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**

29. 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 of 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**

Explanation: He is gathering information and as long as he doesn't make contact with any of the targets systems he is considered gathering this information in a passive mode.

30. 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**

Explanation: The replay from the email server that states that there is no such recipient will also give you some information about the name of the email server, versions used and so on.