# 312-50V7 Q&As

Ethical Hacking and Countermeasures (CEHv7)

## Pass EC-COUNCIL 312-50V7 Exam with 100% Guarantee

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

**https://www.leads4pass.com/312-50v7.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

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 2**

Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

A. Ping of death

B. SYN flooding

C. TCP hijacking

D. Smurf attack

Correct Answer: A

**QUESTION 3**

Which of the following programs is usually targeted at Microsoft Office products?

A. Polymorphic virus

B. Multipart virus

C. Macro virus

D. Stealth virus

Correct Answer: C

**QUESTION 4**

Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

A. Metasploit scripting engine

B. Nessus scripting engine

C. NMAP scripting engine

D. SAINT scripting engine

Correct Answer: C

**QUESTION 5**

Buffer X in an Accounting application module for Brownies Inc. can contain 200 characters. The programmer makes an assumption that 200 characters are more than enough. Because there were no proper boundary checks being conducted, Bob decided to insert 400 characters into the 200-character buffer. (Overflows the buffer). Below is the code snippet: How can you protect/fix the problem of your application as shown above?

```
Void func (void)
{
int I; char buffer [200];
for (I=0; I<400; I++)
buffer [I]= 'A';
return;
}
```

A. Because the counter starts with 0, we would stop when the counter is less than 200

B. Because the counter starts with 0, we would stop when the counter is more than 200

C. Add a separate statement to signify that if we have written less than 200 characters to the buffer, the stack should stop because it cannot hold any more data

D. Add a separate statement to signify that if we have written 200 characters to the buffer, the stack should stop because it cannot hold any more data

Correct Answer: AD

**QUESTION 6**

Dan is conducting penetration testing and has found a vulnerability in a Web Application which gave him the sessionID token via a cross site scripting vulnerability. Dan wants to replay this token. However, the session ID manager (on the server) checks the originating IP address as well. Dan decides to spoof his IP address in order to replay the sessionID. Why do you think Dan might not be able to get an interactive session?

A. Dan cannot spoof his IP address over TCP network

B. The scenario is incorrect as Dan can spoof his IP and get responses

C. The server will send replies back to the spoofed IP address

D. Dan can establish an interactive session only if he uses a NAT

Correct Answer: C

**QUESTION 7**

Which of the following examples best represents a logical or technical control?

A. Security tokens

B. Heating and air conditioning

C. Smoke and fire alarms

D. Corporate security policy

Correct Answer: A

**QUESTION 8**

Which of the following are variants of mandatory access control mechanisms? (Choose two.)

A. Two factor authentication

B. Acceptable use policy

C. Username / password

D. User education program

E. Sign in register

Correct Answer: AC

**QUESTION 9**

During a penetration test, the tester conducts an ACK scan using NMAP against the external interface of the DMZ firewall. NMAP reports that port 80 is unfiltered. Based on this response, which type of packet inspection is the firewall conducting?

A. Host

B. Stateful

C. Stateless

D. Application

Correct Answer: C

**QUESTION 10**

Which of the following is a protocol that is prone to a man-in-the-middle (MITM) attack and maps a 32-bit address to a 48-bit address?

A. ICPM

B. ARP

C. RARP

D. ICMP

Correct Answer: B

**QUESTION 11**

Information gathered from social networking websites such as Facebook, Twitter and LinkedIn can be used to launch which of the following types of attacks? (Choose two.)

A. Smurf attack

B. Social engineering attack

C. SQL injection attack

D. Phishing attack

E. Fraggle attack

F. Distributed denial of service attack

Correct Answer: BD

**QUESTION 12**

Hampton is the senior security analyst for the city of Columbus in Ohio. His primary responsibility is to ensure that all physical and logical aspects of the city\\'s computer network are secure from all angles. Bill is an IT technician that works with Hampton in the same IT department. Bill\\'s primary responsibility is to keep PC\\'s and servers up to date and to keep track of all the agency laptops that the company owns and lends out to its employees. After Bill setup a wireless network for the agency, Hampton made sure that everything was secure. He instituted encryption, rotating keys, turned off SSID broadcasting, and enabled MAC filtering. According to agency policy, only company laptops are allowed to use the wireless network, so Hampton entered all the MAC addresses for those laptops into the wireless security utility so that only those laptops should be able to access the wireless network.

Hampton does not keep track of all the laptops, but he is pretty certain that the agency only purchases Dell laptops. Hampton is curious about this because he notices Bill working on a Toshiba laptop one day and saw that he was on the Internet. Instead of jumping to conclusions, Hampton decides to talk to Bill\\'s boss and see if they had purchased a Toshiba laptop instead of the usual Dell. Bill\\'s boss said no, so now Hampton is very curious to see how Bill is accessing the Internet. Hampton does site surveys every couple of days, and has yet to see any outside wireless network signals inside the company\\'s building.

How was Bill able to get Internet access without using an agency laptop?

A. Bill spoofed the MAC address of Dell laptop

B. Bill connected to a Rogue access point

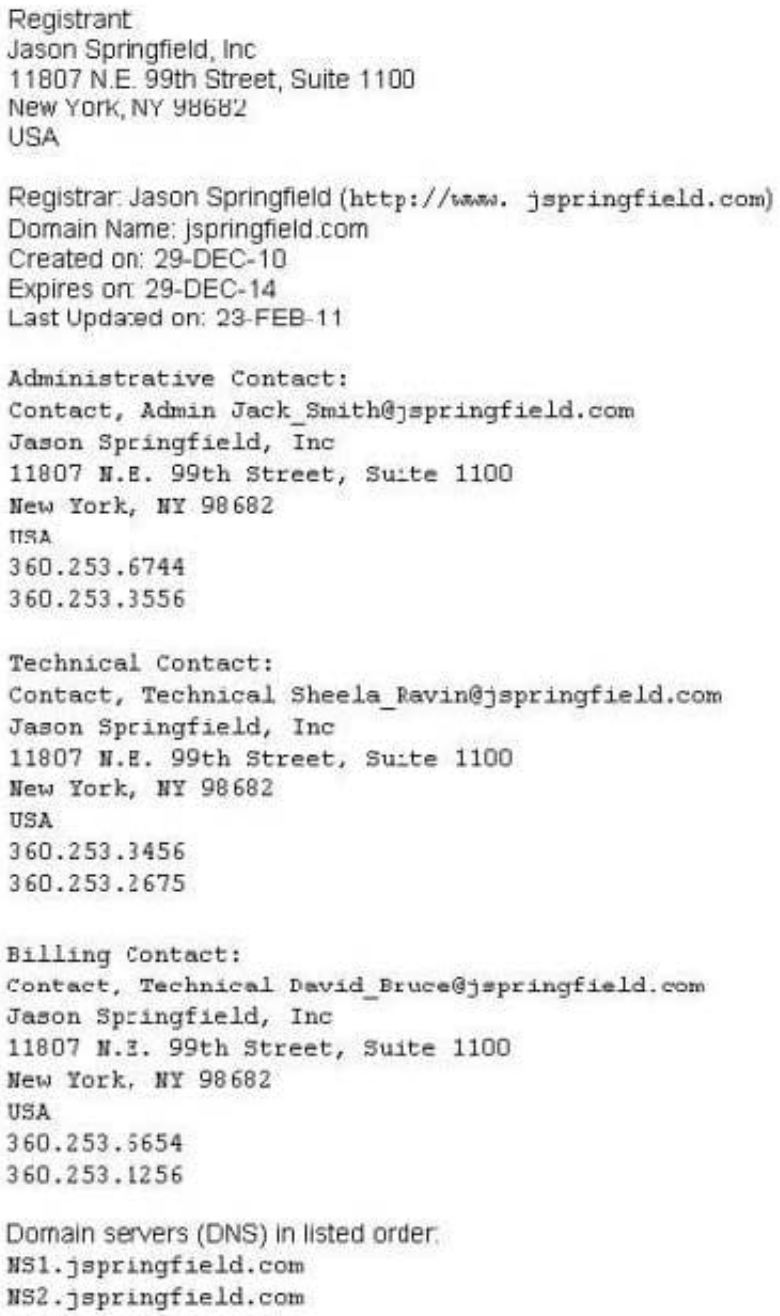
C. Toshiba and Dell laptops share the same hardware address

D. Bill brute forced the Mac address ACLs

Correct Answer: A

**QUESTION 13**

This is an example of whois record.



Sometimes a company shares a little too much information on their organization through public domain records. Based on the above whois record, what can an attacker do? (Select 2 answers)

A. Search engines like Google, Bing will expose information listed on the WHOIS record

B. An attacker can attempt phishing and social engineering on targeted individuals using the information from WHOIS record

C. Spammers can send unsolicited e-mails to addresses listed in the WHOIS record

D. IRS Agents will use this information to track individuals using the WHOIS record information

Correct Answer: BC

**QUESTION 14**

Data hiding analysis can be useful in

A. determining the level of encryption used to encrypt the data.

B. detecting and recovering data that may indicate knowledge, ownership or intent.

C. identifying the amount of central processing unit (cpu) usage over time to process the data.

D. preventing a denial of service attack on a set of enterprise servers to prevent users from accessing the data.

Correct Answer: B

**QUESTION 15**

Passive reconnaissance involves collecting information through which of the following?

A. Social engineering

B. Network traffic sniffing

C. Man in the middle attacks

D. Publicly accessible sources

Correct Answer: D