312-50V8 Q&As

Certified Ethical Hacker v8

Pass EC-COUNCIL 312-50V8 Exam with 100% Guarantee

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

https://www.passapply.com/312-50v8.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Attackers target HINFO record types stored on a DNS server to enumerate information.

These are information records and potential source for reconnaissance. A network administrator has the option of entering host information specifically the CPU type and operating system when creating a new DNS record. An attacker can extract this type of information easily from a DNS server.

Which of the following commands extracts the HINFO record?

A.
```
c:> nslookup
> Set type=hinfo
> certhack-srv
Server: dns.certifiedhacker.com
Address: 10.0.0.4
sales.certifiedhacker.com      CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com        Internet address = 10.0.0.56
```

B.
```
c:> nslookup
> Set dns=hinfo
> certhack-srv
Server: dns.certifiedhacker.com
IP: 10.0.0.4
sales.certifiedhacker.com      CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com        Internet address = 10.0.0.56
```

C.
```
c:> nslookup
> Set record=hinfo
> certhack-srv
host: dns.certifiedhacker.com
Address: 10.0.0.4
sales.certifiedhacker.com      CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com        Internet address = 10.0.0.56
```

D.
```
c:> nslookup
> Configure type=hinfo
> certhack-srv
Host: dns.certifiedhacker.com
IP: 10.0.0.4
sales.certifiedhacker.com      CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com Internet address = 10.0.0.56
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 2

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. Jack the ripper

B. nessus

C. tcpdump

D. ethereal

Correct Answer: C

QUESTION 3

Jake is a network administrator who needs to get reports from all the computer and network devices on his network. Jake wants to use SNMP but is afraid that won\\'t be secure since passwords and messages are in clear text.

How can Jake gather network information in a secure manner?

A. He can use SNMPv3

B. Jake can use SNMPrev5

C. He can use SecWMI

D. Jake can use SecSNMP

Correct Answer: A

QUESTION 4

Which tool would be used to collect wireless packet data?

A. NetStumbler

B. John the Ripper

C. Nessus

D. Netcat

Correct Answer: A

QUESTION 5

Fred is scanning his network to ensure it is as secure as possible. Fred sends a TCP probe packet to a host with a FIN flag and he receives a RST/ACK response.

What does this mean?

A. This response means the port he is scanning is open.

B. The RST/ACK response means the port Fred is scanning is disabled.

C. This means the port he is scanning is half open.

D. This means that the port he is scanning on the host is closed.

Correct Answer: D

QUESTION 6

In Buffer Overflow exploit, which of the following registers gets overwritten with return address of the exploit code?

A. EEP

B. ESP

C. EAP

D. EIP

Correct Answer: D

QUESTION 7

You have been called to investigate a sudden increase in network traffic at XYZ. It seems that the traffic generated was too heavy that normal business functions could no longer be rendered to external employees and clients. After a quick investigation, you find that the computer has services running attached to TFN2k and Trinoo software.

What do you think was the most likely cause behind this sudden increase in traffic?

A. A distributed denial of service attack.

B. A network card that was jabbering.

C. A bad route on the firewall.

D. Invalid rules entry at the gateway.

Correct Answer: A

QUESTION 8

How does the Address Resolution Protocol (ARP) work?

A. It sends a reply packet for a specific IP, asking for the MAC address.

B. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.

C. It sends a request packet to all the network elements, asking for the domainname from a specific IP.

D. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.

Correct Answer: D

QUESTION 9

Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

A. ESP confidential

B. AH Tunnel mode

C. ESP transport mode

D. AH permiscuous

Correct Answer: C

QUESTION 10

Attackers send an ACK probe packet with random sequence number, no response means port is filtered (Stateful firewall is present) and RST response means the port is not filtered.

What type of Port Scanning is this?

A. RST flag scanning

B. FIN flag scanning

C. SYN flag scanning

D. ACK flag scanning

Correct Answer: D

QUESTION 11

You have successfully run a buffer overflow attack against a default IIS installation running on a Windows 2000 Server. The server allows you to spawn a shell. In order to perform the actions you intend to do, you

need elevated permission. You need to know what your current privileges are within the shell. Which of the following options would be your current privileges?

A. Administrator

B. IUSR_COMPUTERNAME

C. LOCAL_SYSTEM

D. Whatever account IIS was installed with

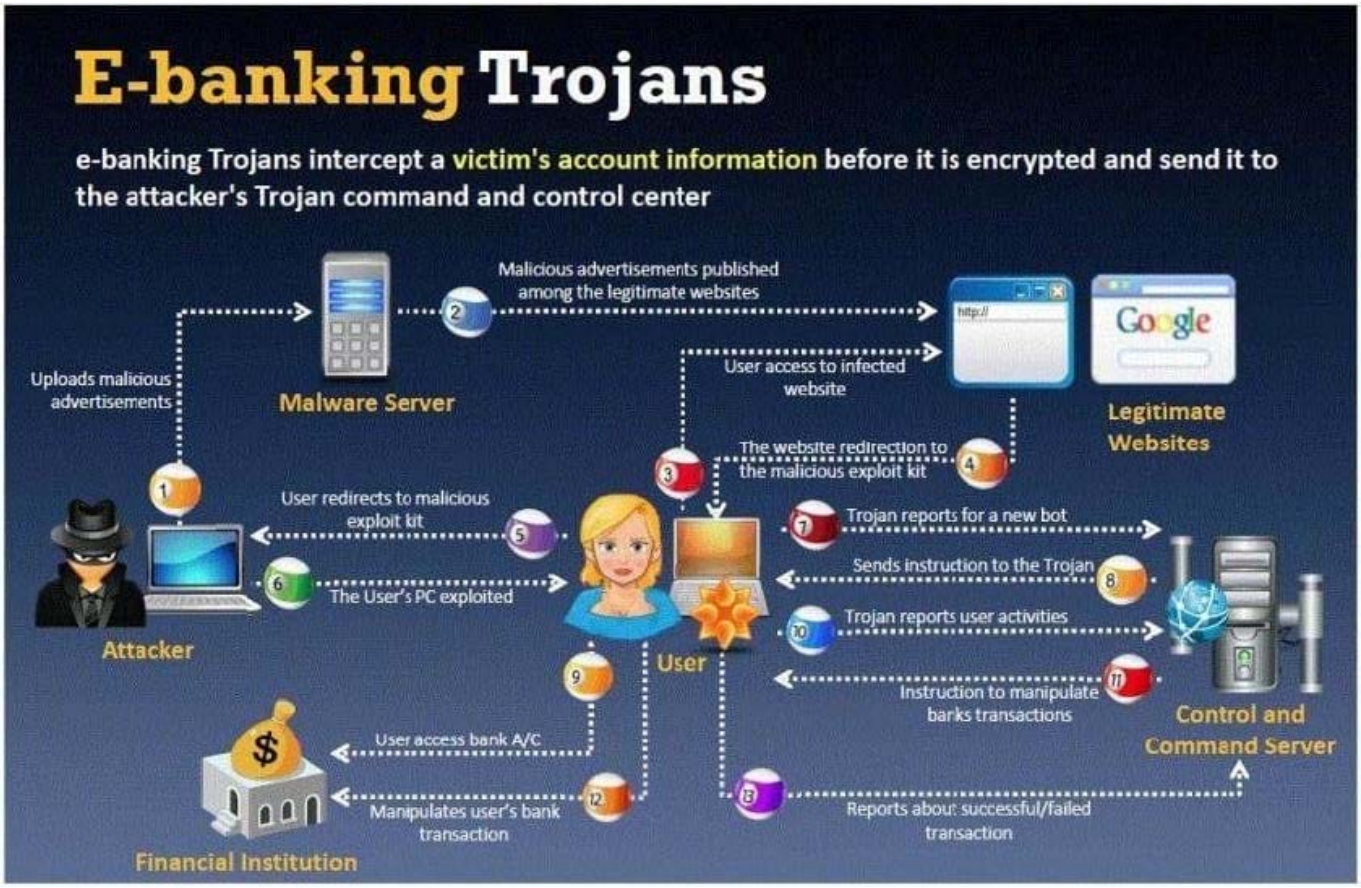
Correct Answer: C

QUESTION 12

BankerFox is a Trojan that is designed to steal users\\' banking data related to certain banking entities.

When they access any website of the affected banks through the vulnerable Firefox 3.5 browser, the Trojan is activated and logs the information entered by the user. All the information entered in that website will be logged by the Trojan and transmitted to the attacker\\'s machine using covert channel.

BankerFox does not spread automatically using its own means. It needs an attacking user\\'s intervention in order to reach the affected computer.



What is the most efficient way an attacker located in remote location to infect this banking Trojan on a victim\\'s machine?

A. Physical access - the attacker can simply copy a Trojan horse to a victim\\'s hard disk infecting the machine via Firefox add-on extensions

B. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer

C. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer

D. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is

unique to that particular computer

E. Downloading software from a website? An attacker can offer free software,such as shareware programs and pirated mp3 files

Correct Answer: E

QUESTION 13

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position. Harold is currently trying to run a Sniffer on the agency\\'s network to get an idea of what kind of traffic is being passed around, but the program he is using does not seem to be capturing anything. He pours through the Sniffer\\'s manual, but cannot find anything that directly relates to his problem. Harold decides to ask the network administrator if he has any thoughts on the problem. Harold is told that the Sniffer was not working because the agency\\'s network is a switched network, which cannot be sniffed by some programs without some tweaking.

What technique could Harold use to sniff his agency\\'s switched network?

A. ARP spoof the default gateway

B. Conduct MiTM against the switch

C. Launch smurf attack against the switch

D. Flood the switch with ICMP packets

Correct Answer: A

QUESTION 14

Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites. Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.

In this context, what would be the most affective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer)

A. Educate everyone with books,articles and training on risk analysis,vulnerabilities and safeguards.

B. Hire more computer security monitoring personnel to monitor computer systems and networks.

C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.

D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

Correct Answer: A

QUESTION 15

What results will the following command yielD. \\'NMAP -sS -O -p 123-153 192.168.100.3\\'?

A. A stealth scan,opening port 123 and 153

B. A stealth scan,checking open ports 123 to 153

C. A stealth scan,checking all open ports excluding ports 123 to 153

D. A stealth scan,determine operating system,and scanning ports 123 to 153

Correct Answer: D