312-50$^{Q\&As}$

Ethical Hacker Certified

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

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

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

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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 2

Clive has been monitoring his IDS and sees that there are a huge number of ICMP Echo Reply packets that are being received on the external gateway interface. Further inspection reveals that they are not responses from the internal hosts\\' requests but simply responses coming from the Internet.

What could be the most likely cause?

A. Someone has spoofed Clive\\'s IP address while doing a smurf attack.

B. Someone has spoofed Clive\\'s IP address while doing a land attack.

C. Someone has spoofed Clive\\'s IP address while doing a fraggle attack.

D. Someone has spoofed Clive\\'s IP address while doing a DoS attack.

Correct Answer: A

The smurf attack, named after its exploit program, is a denial-of-service attack that uses spoofed broadcast ping messages to flood a target system. In such an attack, a perpetrator sends a large amount of ICMP echo (ping) traffic to IP broadcast addresses, all of it having a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, hundreds of machines might reply to each packet.

QUESTION 3

Neil is closely monitoring his firewall rules and logs on a regular basis. Some of the users have complained to Neil that there are a few employees who are visiting offensive web site during work hours, without any consideration for others. Neil knows that he has an up-to-date content filtering system and such access should not be authorized. What type of technique might be used by these offenders to access the Internet without restriction?

A. They are using UDP that is always authorized at the firewall

B. They are using an older version of Internet Explorer that allow them to bypass the proxy server

C. They have been able to compromise the firewall, modify the rules, and give themselves proper access

D. They are using tunneling software that allows them to communicate with protocols in a way it was not intended

Correct Answer: D

This can be accomplished by, for example, tunneling the http traffic over SSH if you have a SSH server answering to your connection, you enable dynamic forwarding in the ssh client and configure Internet Explorer to use a SOCKS Proxy for network traffic.

QUESTION 4

Which of the following ICMP message types are used for destinations unreachables?

A. 0

B. 3

C. 11

D. 13

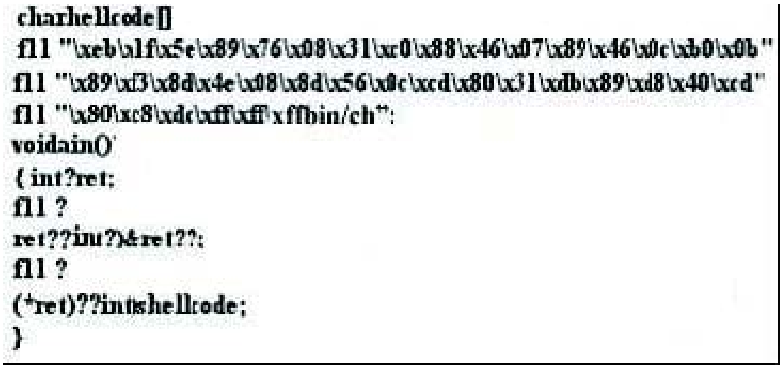
E. 17

Correct Answer: B

Type 3 messages are used for unreachable messages. 0 is Echo Reply, 8 is Echo request, 11 is time exceeded, 13 is timestamp and 17 is subnet mask request. Learning these would be advisable for the test.

QUESTION 5

When writing shellcodes, you must avoid __________________ because these will end the string.



```
charhellcode[]
f11 "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
f11 "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
f11 "\x80\xe8\xdc\xff\xff\xffbin/ch";
voidain()
{ int?ret;
f11 ?
ret??int?)&ret??;
f11 ?
(*ret)??intshellcode;
}
```

A. Null Bytes

B. Root Bytes

C. Char Bytes

D. Unicode Bytes

Correct Answer: A

The null character (also null terminator) is a character with the value zero, present in the ASCII and Unicode character sets, and available in nearly all mainstream programming languages. The original meaning of this character was like NOP -- when sent to a printer or a terminal, it does nothing (some terminals, however, incorrectly display it as space). Strings ending in a null character are said to be null-terminated.