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

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

In what stage of Virus life does a stealth virus gets activated with the user performing certain actions such as running an infected program?

A. Design

B. Elimination

C. Incorporation

D. Replication

E. Launch

F. Detection

Correct Answer: E

QUESTION 2

The FIN flag is set and sent from host A to host B when host A has no more data to transmit (Closing a TCP connection). This flag releases the connection resources. However, host A can continue to receive data as long as the SYN sequence number of transmitted packets from host B are lower than the packet segment containing the set FIN flag.

A. True

B. False

Correct Answer: A

For sequence number purposes, the SYN is considered to occur before the first actual data octet of the segment in which it occurs, while the FIN is considered to occur after the last actual data octet in a segment in which it occurs. So packets receiving out of order will still be accepted.

QUESTION 3

Cyber Criminals have long employed the tactic of masking their true identity. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine,

by "spoofing" the IP address of that machine.

How would you detect IP spoofing?

A. Check the IPID of the spoofed packet and compare it with TLC checksum. If the numbers match then it is spoofed packet

B. Probe a SYN Scan on the claimed host and look for a response SYN/FIN packet, if the connection completes then it is a spoofed packet

C. Turn on \\'Enable Spoofed IP Detection\\' in Wireshark, you will see a flag tick if the packet is spoofed

D. Sending a packet to the claimed host will result in a reply. If the TTL in the reply is not the same as the packet being checked then it is a spoofed packet

Correct Answer: D

QUESTION 4

What is the proper response for a X-MAS scan if the port is closed?

A. SYN

B. ACK

C. FIN

D. PSH

E. RST

F. No response

Correct Answer: E

Closed ports respond to a X-MAS scan with a RST.

QUESTION 5

Clive has been hired to perform a Black-Box test by one of his clients.

How much information will Clive obtain from the client before commencing his test?

A. IP Range, OS, and patches installed.

B. Only the IP address range.

C. Nothing but corporate name.

D. All that is available from the client site.

Correct Answer: C

Penetration tests can be conducted in one of two ways: black-box (with no prior knowledge the infrastructure to be tested) or white-box (with complete knowledge of the infrastructure to be tested). As you might expect, there are conflicting opinions about this choice and the value that either approach will bring to a project.