312-38 Q&As

Certified Network Defender (CND)

Pass EC-COUNCIL 312-38 Exam with 100% Guarantee

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

https://www.passapply.com/312-38.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Fill in the blank with the appropriate term. is an enumeration technique used to glean information about computer systems on a network and the services running its open ports.

Correct Answer: Banner grabbing

Banner grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports. Administrators can use this to take inventory of the systems and services on their network. An intruder however can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits. Some examples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 respectively. Tools commonly used to perform banner grabbing are Telnet, which is included with most operating systems, and Netcat. For example, one could establish a connection to a target host running a Web service with netcat, then send a bad html request in order to get information about the service on the host: [root@prober] nc www.targethost.com 80 HEAD / HTTP/1.1 HTTP/1.1 200 OK Date: Mon, 11 May 2009 22:10:40 EST Server: Apache/2.0.46 (Unix) (Red Hat/Linux) Last-Modified: Thu, 16 Apr 2009 11:20:14 PST ETag: "1986-69b-123a4bc6" Accept-Ranges: bytes Content-Length: 1110 Connection: close Content-Type: text/html The administrator can now catalog this system or an intruder now knows what version of Apache to look for exploits.

QUESTION 2

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

,,It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys."

Which of the following tools is John using to crack the wireless encryption keys?

A. PsPasswd

B. Kismet

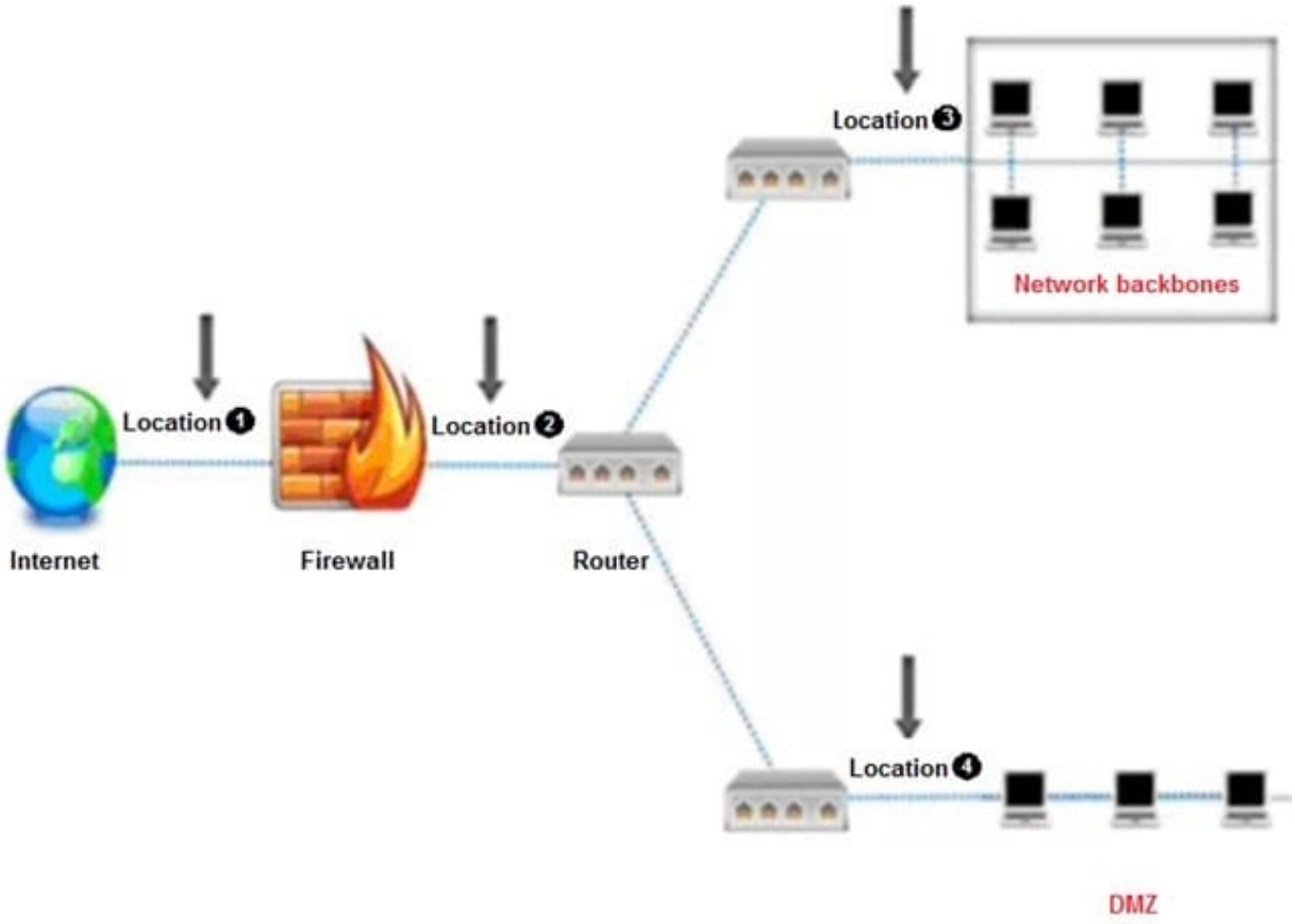
C. AirSnort

D. Cain

Correct Answer: C

AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys. Answer option B is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks: To identify networks by passively collecting packets To detect standard named networks To detect masked networks To collect the presence of non-beaconing networks via data traffic Answer option D is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks: Dictionary attack Brute force attack Rainbow attack Hybrid attack Answer option A is incorrect. PsPasswd is a tool that helps Network Administrators

change an account password on the local or remote system. The command syntax of PsPasswd is as follows: pspasswd [\\computer[,computer[,..] | @file [-u user [-p psswd]] Username [NewPassword]



QUESTION 3

Which of the following refers to a potential occurrence of an undesired event that can eventually damage and interrupt the operational and functional activities of an organization?

A. Attack

B. Risk

C. Threat

D. Vulnerability

Correct Answer: C

QUESTION 4

You want to increase your network security implementing a technology that only allows certain MAC addresses in

specific ports in the switches; which one of the above is the best choice?

A. Port Security

B. Port Authorization

C. Port Detection

D. Port Knocking

Correct Answer: A

QUESTION 5

Which of the following types of coaxial cable used for cable television and cable modems?

A. RG-8

B. RG-59

C. RG-58

D. None

E. RG-62

Correct Answer: B