GSNA$^{Q\&As}$

GIAC Systems and Network Auditor

QUESTION 1

Which of the following tools is a Windows-based commercial wireless LAN analyzer for IEEE 802.11b and supports all high level protocols such as TCP/IP, NetBEUI, and IPX?

A. SamSpade

B. John the Ripper

C. Cheops-ng

D. AiroPeek

Correct Answer: D

AiroPeek is a Windows-based commercial wireless LAN analyzer for IEEE 802.11b. It supports all high level protocols such as TCP/IP, NetBEUI, IPX, etc. It can be used to perform the following tasks:

1.

Site surveys

2.

Security assessments

3.

Channel scanning

4.

Real time and past capture

5.

WEP decryption

6.

Client troubleshooting

7.

WLAN monitoring

8.

Remote WLAN analysis

9.

Application layer protocol analysis ting tool Answer: A is incorrect. Sam Spade is a penetration-testing tool that is used in the discovery phase. It provides GUI graphics and a lot of functionalities. It can perform mainly who is queries, ping requests, DNS requests, tracerouting, OS finger-printing, zone transferring, SMTP mail relay checking, and Web site crawling and mirroring. Sam Spade runs on Windows operating systems. Answer: B is incorrect. John the Ripper is a fast password cracking tool that is available for most versions of UNIX, Windows, DOS, BeOS, and Open VMS. It also supports Kerberos, AFS, and Windows NT/2000/ XP/2003 LM hashes. John the Ripper requires a user to have a copy of the password file. Answer: C is incorrect. Cheops-ng is a network management tool that is used for mapping and monitoring networks. It can detect a network of a host and provides OS detection for hosts. On some services, Cheops-ng is able to see what program is running for a service and what is the version number of that program. The main difference between Cheops and Cheops-ng is that Cheops-ng does not have monitoring capabilities.

QUESTION 2

Which of the following user authentications are supported by the SSH-1 protocol but not by the SSH-2 protocol?

A. TIS authentication

B. Kerberos authentication

C. Rhosts (rsh-style) authentication

D. Password-based authentication

Correct Answer: ABC

The Rhosts (rsh-style), TIS, and Kerberos user authentication methods are supported by the SSH-1 protocol but not by SSH-2 protocol. Answer: D is incorrect. Password-based authentication is supported by both the SSH-1 and SSH-2 protocols.

QUESTION 3

In which of the following techniques does an attacker take network traffic coming towards a host at one port and forward it from that host to another host?

A. Snooping

B. UDP port scanning

C. Firewalking

D. Portredirection

Correct Answer: D

Port redirection is a technique by which an attacker takes network traffic coming towards a host at one port and redirects it from that host to another host. For example, tools such as Fpipe and Datapipe are port redirection tools that accept connections at any specified port and resend them to other specified ports on specified hosts. For example, the following command establishes a listener on port 25 on the test system and then redirects the connection to port 80 on the target system using the source port of 25. C.\>fpipe -l 25 -s 25 -r 80 IP_address Answer: C is incorrect. Firewalking is a technique for gathering information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. If the firewall allows this crafted packet through, it forwards the packet to the next hop. On the next hop, the packet expires and elicits an ICMP "TTL expired in transit" message to the attacker. If the firewall does not allow the traffic, there should be no response, or an ICMP "administratively prohibited" message should be returned to the attacker. Amalicious attacker can use firewalking to determine the types of ports/ protocols that can bypass the firewall. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall. The main drawback of this technique is that if an administrator blocks ICMP packets from leaving the network, it is ineffective. Answer: A is incorrect. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e- mail and other private communications. Sometimes, organizations also snoop their employees legitimately to monitor their use of organizations\\' computers and track Internet usage. Answer: B is incorrect. In UDP port scanning, a UDP packet is sent to each port of the target system. If the remote port is closed, the server replies that the remote port is unreachable. If the remote Port is open, no such error is generated. Many firewalls block the TCP port scanning, at that time the UDP port scanning may be useful. Certain IDS and firewalls can detect UDP port scanning easily.

QUESTION 4

Which of the following techniques can be used to determine the network ranges of any network?

A. Whois query

B. SQL injection

C. Snooping

D. Web ripping

Correct Answer: A

Whois queries are used to determine the IP address ranges associated with clients. A whois query can be run on most UNIX environments. In a Windows environment, the tools such as WsPingPro and Sam Spade can be used to perform

whois queries. Whois queries can also be executed over the Web from www.arin.net and www.networksolutions.com.

Answer: B is incorrect. A SQL injection attack is a process in which an attacker tries to execute unauthorized SQL statements. These statements can be used to delete data from a database, delete database objects such as tables, views,

stored procedures, etc. An attacker can either directly enter the code into input variables or insert malicious code in strings that can be stored in a database. For example, the following line of code illustrates one form of SQL injection attack:

query = "SELECT * FROM users WHERE name = \\'" + userName + "\\';" This SQL code is designed to fetch the records of any specified username from its table of users. However, if the "userName" variable is crafted in a specific way by a

malicious hacker, the SQL statement maydo more than the code author intended. For example, if the attacker puts the "userName" value as \\' or \\'\\'=\\', the SQL statement will now be as follows:

SELECT * FROM users WHERE name = \\'\\' OR \\'\\'=\\'\\';

Answer: D is incorrect. Web ripping is a technique in which the attacker copies the whole structure of a Web site to the local disk and obtains all files of the Web site. Web ripping helps an attacker to trace the loopholes of the Web site.

Answer: C is incorrect. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or

network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e- mail and other private communications. Sometimes,

organizations also snoop their employees legitimately to monitor their use of organizations\\' computers and track Internet usage.

QUESTION 5

In a network, a data packet is received by a router for transmitting it to another network. For forwarding the packet to the other available networks, the router is configured with a static or a dynamic route.

What are the benefits of using a static route?

A. It is a fault tolerant path.

B. It reduces load on routers, as no complex routing calculations are required.

C. It reduces bandwidth usage, as there is no excessive router traffic.

D. It provides precise control over the routes that packets will take across the network.

Correct Answer: BCD

Static routing is a data communication concept that describes a way to configure path selection of routers in computer networks. This is achieved by manually adding routes to the routing table. However, when there is a change in the network

or a failure occurs between two statically defined nodes, traffic will not be rerouted.

Static routing is beneficial in many ways:

Precise control over the routes that a packet will take across the network Reduced load on the routers, as no complex routing calculations are required Reduced bandwidth use, as there is no excessive router traffic.

Easy to configure in small networks

Answer: A is incorrect. This is a property of a dynamic route. A static route cannot choose the best path. It can only choose the paths that are manually entered. When there is a change in the network or a failure occurs between two statically

defined nodes, traffic will not be rerouted.