EC-Council 412-79

EC-Council Certified Security Analyst (ECSA)

Version: 5.0

QUESTION NO: 1

Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Change the default community string names
B. Block all internal MAC address from using SNMP
C. Block access to UDP port 171
D. Block access to TCP port 171

Answer: A

Explanation:

SNMP Version 1 does not provide encryption, so the community strings are in the clear.
Known community strings, the default of Public and Private, are well known because these are the default community strings that come out of the box. By changing these values to different community string names, guessing the actual names will be difficult.

QUESTION NO: 2

At what layer of the OSI model do routers function on?

A. 3
B. 4
C. 5
D. 1

Answer: A

Explanation:

1 – Physical
2 – Data Link
3 – Network
4 – Transport
5 – Session
6 – Presentation
7 - Application

QUESTION NO: 3

An "idle" system is also referred to as what?

A. Zombie
B. PC not being used
C. Bot
D. PC not connected to the Internet

Answer: A
Explanation:
In this case “idle” refers to a system that can be used as a go between for an idle scan. One workstation, sends spoofed packets to a target machine, but uses the address f the idle machine as the spoofed source address. Examination of the idle system’s behavior is then evaluated. In order for this to work properly, the idle system must be quiet on its network traffic. The ‘Idle” system is called a zombie.
The idle system is not a PC not being used because even a PC that is not in use could be generating network traffic. The issue is not whether a PC is in use, the issue is whether the PC is creating or processing network traffic.

QUESTION NO: 4

What operating system would respond to the following command?

```
C:\> nmap -sW 10.10.145.65
```

A. Mac OS X
B. Windows XP
C. Windows 95
D. FreeBSD

Answer: D
Explanation:
-sW Window scan: This advanced scan is very similar to
the ACK scan, except that it can sometimes detect
open ports as well as filtered/nonfiltered due to
an anomaly in the TCP window size reporting by some
operating systems. Systems vulnerable to this
include at least some versions of AIX, Amiga, BeOS,

BSDI, Cray, Tru64 UNIX, DG/UX, OpenVMS, Digital UNIX, **FreeBSD**, HP-UX, OS/2, IRIX, MacOS, NetBSD, OpenBSD, OpenStep, QNX, Rhapsody, SunOS 4.X, Ultrix, VAX, and VxWorks. See the nmap-hackers mailing list archive for a full list.

QUESTION NO: 5

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Windows computers will not respond to idle scans
B. Linux/Unix computers are constantly talking
C. Linux/Unix computers are easier to compromise
D. Windows computers are constantly talking

Answer: D
Explanation:
In an idle scan, one workstation sends spoofed packets to a target machine, but uses the address f the idle machine as the spoofed source address. Examination of the idle system's behavior is then evaluated. In order for this to work properly, the idle system must be quiet on its network traffic

QUESTION NO: 6

How many bits is Source Port Number in TCP Header packet?

A. 48
B. 32
C. 64
D. 16

Answer: D
Explanation:
48 bits is the size of a MAC address, and is layer 2
32 bits is the size of a IPV4 IP address, and is layer 3
16 bits is the size of an address for the TCP header and UDP header, and supports up to 65K ports

In each of these cases, the address size is the same for both a “source” and “destination” address.

QUESTION NO: 7

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the AXFR and IXFR commands using DIG. What is Simon trying to accomplish here?

A. Enumerate all the users in the domain
B. Perform DNS poisoning
C. Send DOS commands to crash the DNS servers
D. Perform a zone transfer

Answer: D

Explanation:

AXFR is a full DNS zone transfer, IXFR is an incremental DNS zone transfer.

QUESTION NO: 8

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

<script>alert("This is a test.")</script>

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

A. Your website is vulnerable to web bugs
B. Your website is vulnerable to XSS
C. Your website is not vulnerable

D. Your website is vulnerable to SQL injection

Answer: B

Explanation:

This indicates that Cross Site Scripting is possible. The proper acronym that is used is XSS and not CSS because CSS is already used in HTML for Cascading Style Sheets.

Web Bugs are usually a single pixel by single pixel within the HTML code.

SQL injection is usually performed by insertion of a quote character into a data field.

QUESTION NO: 9

After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A. RestrictAnonymous must be set to "2" for complete security
B. RestrictAnonymous must be set to "3" for complete security
C. There is no way to always prevent an anonymous null session from establishing
D. RestrictAnonymous must be set to "10" for complete security

Answer: A

Explanation:

RestrictAnonymous is set by changing the registry key to 0 or 1 for Windows NT 4.0 or to 0, 1, or 2 for Windows 2000. These numbers correspond to the following settings:0 None. Rely on default permissions1 Do not allow enumeration of SAM accounts and names2 No access without explicit anonymous permissions

QUESTION NO: 10

What will the following command accomplish?

```
C:\> nmap -v -sS -Po 172.16.28.251 -data_length 66000-packet_trace
```

A. Test ability of a router to handle over-sized packets
B. Test the ability of a router to handle fragmented packets
C. Test the ability of a WLAN to handle fragmented packets
D. Test the ability of a router to handle under-sized packets

Answer: A

Explanation:

-v (verbose) –sS (SYN scan) –Po (Ping Disable ICMP) target –data_length (option to control packet length) 66000 (size of packet) –packet_trace (Display nmap conversations during trace)

QUESTION NO: 11

What are the security risks of running a "repair" installation for Windows XP?

A. There are no security risks when running the "repair" installation for Windows XP
B. Pressing Shift+F1 gives the user administrative rights
C. Pressing Ctrl+F10 gives the user administrative rights
D. Pressing Shift+F10 gives the user administrative rights

Answer: D

Explanation:

QUESTION NO: 12

You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. RaidSniff
B. Snort
C. Ettercap
D. Airsnort

Answer: C

Explanation: Ettercap is the best answer as that tool makes extracting of username and password easier.