Prüfungsnummer: 412-79

Prüfungsname: EC-Council Certified Security Analyst (ECSA)

Version : Demo

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.