



312-50

Certified Ethical Hacker



Last Updated:
May 22, 2006

www.examguru.net

ExamGuru, Inc. © 2004 – 2006, All Rights Reserved.

WWW.EXAMGURU.NET

DO NOT COPY OR DUPLICATE

**Paper Copies of These Materials
or Software Files Downloaded From Website
For Use By Anyone Other Than Original Purchaser**

Violators Will Be Held Liable For Copyright Infringement

Copyrights © 2004-2006 ExamGuru, Inc. All Rights Reserved.

Exam Name:	Certified Ethical Hacker		
Exam Type:	EC-Council		
Exam Code:	312-50	Total Questions:	314

Question: 1

What is the name of the software tool used to crack a single account on Netware Servers using a dictionary attack?

- A. NPWCrack
- B. NWPCrack
- C. NovCrack
- D. CrackNov
- E. GetCrack

Answer: B

Explanation:

NWPCrack is the software tool used to crack single accounts on Netware servers.

Question: 2

How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

- A. There is no way to tell because a hash cannot be reversed
- B. The right most portion of the hash is always the same
- C. The hash always starts with AB923D
- D. The left most portion of the hash is always the same
- E. A portion of the hash will be all 0's

Answer: B

Explanation:

When looking at an extracted LM hash, you will sometimes observe that the right most portion is always the same. This is padding that has been added to a password that is less than 8 characters long.

Question: 3

Several of your co-workers are having a discussion over the etc/passwd file. They are at odds over what types of encryption are used to secure Linux passwords.(Choose all that apply).

- A. Linux passwords can be encrypted with MD5
- B. Linux passwords can be encrypted with SHA
- C. Linux passwords can be encrypted with DES
- D. Linux passwords can be encrypted with Blowfish
- E. Linux passwords are encrypted with asymmetric algorithms

Answer: A, C, D

Explanation:

Linux passwords are encrypted using MD5, DES, and the NEW addition Blowfish. The default on most linux systems is dependant on the distribution, RedHat uses MD5, while slackware uses DES. The blowfish option is there for those who wish to use it. The encryption algorithm in use can be determined by authconfig on RedHat-based systems, or by reviewing one of two locations, on PAM-based systems (Pluggable Authentication Module) it can be found in /etc/pam.d/, the system-auth file or authconfig files. In other systems it can be found in /etc/security/ directory.

Question: 4

What are the two basic types of attacks?(Choose two).

Exam Name:	Certified Ethical Hacker		
Exam Type:	EC-Council		
Exam Code:	312-50	Total Questions:	314

- A. DoS
- B. Passive
- C. Sniffing
- D. Active
- E. Cracking

Answer: B, D

Explanation:

Passive and active attacks are the two basic types of attacks.

Question: 5

Sniffing is considered an active attack.

- A. True
- B. False

Answer: B

Explanation:

Sniffing is considered a passive attack.

Question: 6

When discussing passwords, what is considered a brute force attack?

- A. You attempt every single possibility until you exhaust all possible combinations or discover the password
- B. You threaten to use the rubber hose on someone unless they reveal their password
- C. You load a dictionary of words into your cracking program
- D. You create hashes of a large number of words and compare it with the encrypted passwords
- E. You wait until the password expires

Answer: A

Explanation:

Brute force cracking is a time consuming process where you try every possible combination of letters, numbers, and characters until you discover a match.

Question: 7

Which of the following are well know password-cracking programs?(Choose all that apply).

- A. L0phtcrack
- B. NetCat
- C. Jack the Ripper
- D. Netbus
- E. John the Ripper

Answer: A, E

Explanation:

L0phtcrack and John the Ripper are two well know password-cracking programs. Netcat is considered the Swiss-army knife of Hacking tools, but is not used for password cracking

Question: 8

Exam Name:	Certified Ethical Hacker		
Exam Type:	EC-Council		
Exam Code:	312-50	Total Questions:	314

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

- A. True
- B. False

Answer: B

Explanation:

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

What does the following command achieve?

```
Telnet <IP Address> <Port 80>  
HEAD /HTTP/1.0  
<Return>  
<Return>
```

- 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

Answer: C

Explanation:

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

Question: 10

Your lab partner is trying to find out more information about a competitors web site. The site has a .com extension. She has decided to use some online whois tools and look in one of the regional Internet registries.

Which one would you suggest she looks in first?

- A. LACNIC
- B. ARIN
- C. APNIC
- D. RIPE
- E. AfriNIC

Answer: B

Explanation:

Regional registries maintain records from the areas from which they govern. ARIN is responsible for domains served within North and South America and therefore, would be a good starting point for a .com domain.

Question: 11

Which of the following tools are used for foot printing?(Choose four).

Exam Name:	Certified Ethical Hacker		
Exam Type:	EC-Council		
Exam Code:	312-50	Total Questions:	314

- A. Sam Spade
- B. NSLookup
- C. Traceroute
- D. Neotrace
- E. Cheops

Answer: A, B, C, D

Explanation:

All of the tools listed are used for footprinting except Cheops.

Question: 12

According to the CEH methodology, what is the next step to be performed after footprinting?

- A. Enumeration
- B. Scanning
- C. System Hacking
- D. Social Engineering
- E. Expanding Influence

Answer: B

Explanation:

Once footprinting has been completed, scanning should be attempted next. Scanning should take place on two distinct levels: network and host.

Question: 13

NSLookup is a good tool to use to gain additional information about a target network. What does the following command accomplish?

```
nslookup
> server <ipaddress>
> set type =any
> ls -d <target.com>
```

- A. Enables DNS spoofing
- B. Loads bogus entries into the DNS table
- C. Verifies zone security
- D. Performs a zone transfer
- E. Resets the DNS cache

Answer: D

Explanation:

If DNS has not been properly secured, the command sequence displayed above will perform a zone transfer.

Question: 14

While footprinting a network, what port/service should you look for to attempt a zone transfer?

- A. 53 UDP
- B. 53 TCP
- C. 25 UDP
- D. 25 TCP
- E. 161 UDP