



412-79

EC-Council Certified Security Analyst (ECSA)

Q&A

DEMO Version

Copyright (c) 2010 Chinatag LLC. All rights reserved.

Important Note Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website.

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

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

QUESTION NO: 2

At what layer of the OSI model do routers function on?

- A. 3
- B. 4
- C. 5
- D. 1

Answer: A

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

QUESTION NO: 4

What operating system would respond to the following command?

`C:\> nmap -sW 10.10.145.0/24`

- A. Mac OS X
- B. Windows XP
- C. Windows 95
- D. FreeBSD

Answer: D

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

QUESTION NO: 6

How many bits is Source Port Number in TCP Header packet?

- A. 48
- B. 32
- C. 64
- D. 16

Answer: D

QUESTION NO: 7

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

- A. Windows computers are constantly talking
- B. Linux/Unix computers are constantly talking
- C. Linux/Unix computers are easier to compromise
- D. Windows computers will not respond to idle scans

Answer: A

QUESTION NO: 8

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

- A. Enumerate all the users in the domain
- B. Perform DNS poisoning
- C. Send DOS commands to crash the DNS servers
- D. Perform a zone transfer

Answer: D

QUESTION NO: 9

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

```
<script>alert("This is a test.")</script>
```

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

- A. Your website is vulnerable to web bugs
- B. Your website is vulnerable to CSS
- C. Your website is not vulnerable
- D. Your website is vulnerable to SQL injection

Answer: B

QUESTION NO: 10

After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at

the seminar, you succeed in establishing a null session with one of the servers. Why is that?

- A. RestrictAnonymous must be set to "2" for complete security
- B. RestrictAnonymous must be set to "3" for complete security
- C. There is no way to always prevent an anonymous null session from establishing
- D. RestrictAnonymous must be set to "10" for complete security

Answer: A