



**312-50**

**Certified Ethical Hacker**

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](mailto: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 1**

Which of the following steganography utilities exploits the nature of white space and allows the user to conceal information in these white spaces?

- A. Gif-It-Up
- B. Image Hide
- C. NiceText
- D. Snow

**Answer: D**

**Explanation/Reference:**

Explanation:

The program snow is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-in encryption is used, the message cannot be read even if it is detected.

**QUESTION 2**

In the context of Trojans, what is the definition of a Wrapper?

- A. A tool used to encapsulate packets within a new header and footer
- B. An encryption tool to protect the Trojan
- C. A tool used to calculate bandwidth and CPU cycles wasted by the Trojan
- D. A tool used to bind the Trojan with a legitimate file

**Answer: D**

**Explanation/Reference:**

Explanation:

These wrappers allow an attacker to take any executable back-door program and combine it with any legitimate executable, creating a Trojan horse without writing a single line of new code.

**QUESTION 3**

When Jason moves a file via NFS over the company's network, you want to grab a copy of it by sniffing. Which of the following tool accomplishes this?

- A. nfscopy
- B. macof
- C. filesnarf
- D. webspay

**Answer: C**

**Explanation/Reference:**

Explanation:

Filesnarf - sniff files from NFS traffic

OPTIONS

-i interface

Specify the interface to listen on.

-v "Versus" mode. Invert the sense of matching, to select non-matching files.

pattern

Specify regular expression for filename matching.

expression

Specify a tcpdump(8) filter expression to select

traffic to sniff.  
SEE ALSO  
Dsniff, nfsd

#### QUESTION 4

What type of port scan is shown below?

Scan directed at open port:

```
ClientServer
192.5.2.92:4079 -----FIN/URG/PSH----->192.5.2.110:23
192.5.2.92:4079 <-----NO RESPONSE-----192.5.2.110:23
```

Scan directed at closed port:

```
ClientServer
192.5.2.92:4079 -----FIN/URG/PSH----->192.5.2.110:23
192.5.2.92:4079<-----RST/ACK-----192.5.2.110:23
```

- A. Windows Scan
- B. Idle Scan
- C. SYN Stealth Scan
- D. XMAS Scan

**Answer: D**

#### **Explanation/Reference:**

Explanation:

An Xmas port scan is variant of TCP port scan. This type of scan tries to obtain information about the state of a target port by sending a packet which has multiple TCP flags set to 1 - "lit as an Xmas tree". The flags set for Xmas scan are FIN, URG and PSF. The purpose is to confuse and bypass simple firewalls. Some stateless firewalls only check against security policy those packets which have the SYN flag set (that is, packets that initiate connection according to the standards). Since Xmas scan packets are different, they can pass through these simple systems and reach the target host.

#### QUESTION 5

Derek has stumbled upon a wireless network and wants to assess its security. However, he does not find enough traffic for a good capture. He intends to use AirSnort on the captured traffic to crack the WEP key and does not know the IP address range or the AP. How can he generate traffic on the network so that he can capture enough packets to crack the WEP key?

- A. Derek can use a session replay on the packets captured
- B. Derek can use KisMAC as it needs two USB devices to generate traffic
- C. Use any ARP requests found in the capture
- D. Use Ettercap to discover the gateway and ICMP ping flood tool to generate traffic

**Answer: D**

#### **Explanation/Reference:**

Explanation:

By forcing the network to answer to a lot of ICMP messages you can gather enough packets to crack the WEP key.

#### QUESTION 6

The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack. You also notice "/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?



D. LACNIC

**Answer: D**

**Explanation/Reference:**

Explanation:

LACNIC is the Latin American and Caribbean Internet Addresses Registry that administers IP addresses, autonomous system numbers, reverse DNS, and other network resources for that region.

### QUESTION 8

Bob has been hired to do a web application security test. Bob notices that the site is dynamic and must make use of a back end database. Bob wants to see if SQL Injection would be possible. What is the first character that Bob should use to attempt breaking valid SQL request?

- A. Semi Column
- B. Single Quote
- C. Exclamation Mark
- D. Double Quote

**Answer: B**

**Explanation/Reference:**

Explanation:

In SQL single quotes are used around values in queries, by entering another single quote Bob tests if the application will submit a null value and probably returning an error.

### QUESTION 9

Angela is trying to access an education website that requires a username and password to login. When Angela clicks on the link to access the login page, she gets an error message stating that the page cannot be reached. She contacts the website's support team and they report that no one else is having any issues with the site. After handing the issue over to her company's IT department, it is found that the education website requires any computer accessing the site must be able to respond to a ping from the education's server. Since Angela's computer is behind a corporate firewall, her computer cannot ping the education website back.

What can Angela's IT department do to get access to the education website?

- A. Use an Internet browser other than the one that Angela is currently using
- B. Change the settings on the firewall to allow all incoming traffic on port 80
- C. Change the IP on Angela's computer to an address outside the firewall
- D. Change the settings on the firewall to allow all outgoing traffic on port 80

**Answer: C**

**Explanation/Reference:**

Explanation:

Allowing traffic to and from port 80 will not help as this will be UDP or TCP traffic and ping uses ICMP. The browser used by the user will not make any difference. The only alternative here that would solve the problem is to move the computer to outside the firewall.

### QUESTION 10

Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

- A. 137 and 139
- B. 137 and 443
- C. 139 and 445
- D. 139 and 443

**Answer: C**

**Explanation/Reference:**

Explanation:

NULL sessions take advantage of "features" in the SMB (Server Message Block) protocol that exist primarily for trust relationships. You can establish a NULL session with a Windows host by logging on with a NULL user name and password. Primarily the following ports are vulnerable if they are accessible: