

Exam : **[EC-COUNCIL 412-79](#)**

Title : **EC-Council Certified
Security Analyst (ECSA)**

Version : **Demo**

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

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

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

Answer: A

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

4. What operating system would respond to the following command?

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

Answer: D

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

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

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

Answer: D

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

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

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

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