ECCouncil

Exam EC0-479

EC-Council Certified Security Analyst (ECSA)

Version: 8.2

[Total Questions: 232]

Topic 1, Volume A

Question No : 1 - (Topic 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 - (Topic 1)

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

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

Answer: A

Question No : 3 - (Topic 1)

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 - (Topic 1)

What operating system would respond to the following command?

```
C:\> nmap -sW 10.10.145.65
```

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

Answer: D

Question No : 5 - (Topic 1)

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 - (Topic 1)

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

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

Answer: D

Question No : 7 - (Topic 1)

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 - (Topic 1)

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 - (Topic 1)

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 - (Topic 1)

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

Question No : 11 - (Topic 1)

What will the following command accomplish?

```
C:\> nmap -v -sS -Po 172.16.28.251 -data_length 66000-packet_trace
```

A. Test ability of a router to handle over-sized packets
B. Test the ability of a router to handle fragmented packets
C. Test the ability of a WLAN to handle fragmented packets
D. Test the ability of a router to handle under-sized packets

Answer: A

Question No : 12 - (Topic 1)

What are the security risks of running a "repair" installation for Windows XP?

A. There are no security risks when running the "repair" installation for Windows XP
B. Pressing Shift+F1 gives the user administrative rights
C. Pressing Ctrl+F10 gives the user administrative rights
D. Pressing Shift+F10 gives the user administrative rights

Answer: D

Question No : 13 - (Topic 1)

You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. RaidSniff
B. Snort
C. Ettercap
D. Airsnort

Answer: C

Question No : 14 - (Topic 1)

George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity.

George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

A. net port 22
B. udp port 22 and host 172.16.28.1/24
C. src port 22 and dst port 22
D. src port 23 and dst port 23

Answer: C

Question No : 15 - (Topic 1)

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Circuit-level proxy firewall
B. Packet filtering firewall
C. Application-level proxy firewall
D. Statefull firewall

Answer: D

Question No : 16 - (Topic 1)

You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Metamorphic
B. Oligomorhic
C. Polymorphic
D. Transmorphic

Answer: A

Question No : 17 - (Topic 1)

In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A. More RESET packets to the affected router to get it to power back up
B. RESTART packets to the affected router to get it to power back up
C. The change in the routing fabric to bypass the affected router
D. STOP packets to all other routers warning of where the attack originated

Answer: C

Question No : 18 - (Topic 1)

What is the following command trying to accomplish?

```
C:\> nmap -sU -p445 192.168.0.0/24
```

A. Verify that NETBIOS is running for the 192.168.0.0 network
B. Verify that TCP port 445 is open for the 192.168.0.0 network
C. Verify that UDP port 445 is open for the 192.168.0.0 network
D. Verify that UDP port 445 is closed for the 192.168.0.0 network

Answer: C

Question No : 19 - (Topic 1)

Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security. Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

A. Simple Network Management Protocol
B. Broadcast System Protocol
C. Cisco Discovery Protocol

D. Border Gateway Protocol

Answer: C

Question No : 20 - (Topic 1)

George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

A. Nessus is too loud
B. There are no ways of performing a "stealthy" wireless scan
C. Nessus cannot perform wireless testing
D. Nessus is not a network scanner

Answer: A

Question No : 21 - (Topic 1)

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. True negatives
B. False negatives
C. False positives
D. True positives

Answer: B

Question No : 22 - (Topic 1)

You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Use attack as a launching point to penetrate deeper into the network
B. Demonstrate that no system can be protected against DoS attacks
C. List weak points on their network
D. Show outdated equipment so it can be replaced

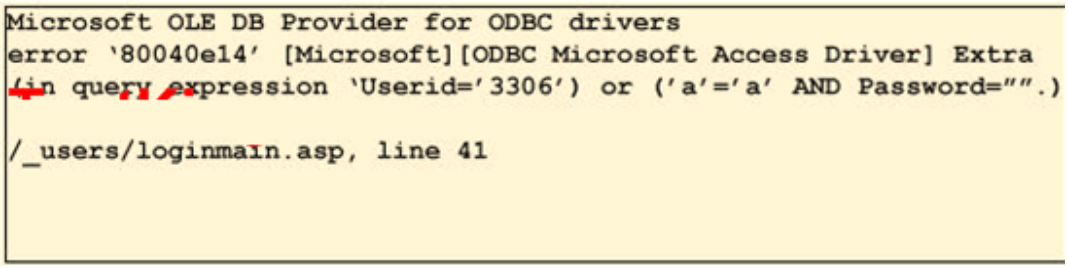
Answer: C

Question No : 23 - (Topic 1)

To test your website for vulnerabilities, you type in a quotation mark (? for the username field. After you click Ok, you receive the following error message window:

What can you infer from this error window?

Exhibit:



A. SQL injection is not possible
B. SQL injection is possible
C. The user for line 3306 in the SQL database has a weak password
D. The quotation mark (? is a valid username

Answer: B

Question No : 24 - (Topic 1)

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?