Exam Code: 412-79

Exam Name: EC-Council Certified Security Analyst (ECSA)

Vendor: EC-Council

Version: DEMO

Part: A

1: When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?
A.Passive IDS
B.Active IDS
C.Progressive IDS
D.NIPS
Correct Answers: B

2: 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.Send DOS commands to crash the DNS servers
B.Perform DNS poisoning
C.Perform a zone transfer
D.Enumerate all the users in the domain
Correct Answers: C

3: What will the following command produce on a website login page?
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'
A.Deletes the entire members table
B.Inserts the Error! Reference source not found. email address into the members table
C.Retrieves the password for the first user in the members table
D.This command will not produce anything since the syntax is incorrect
Correct Answers: A

4: You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)
A.162
B.161
C.163
D.160
Correct Answers: A B

5: 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 CSS
B.Your website is not vulnerable
C.Your website is vulnerable to SQL injection
D.Your website is vulnerable to web bugs
Correct Answers: A

6: If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?
A.The zombie will not send a response
B.31402
C.31399
D.31401
Correct Answers: D

7: Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?
A.Closed
B.Open
C.Stealth
D.Filtered
Correct Answers: B

8: 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.Packet filtering firewall
B.Circuit-level proxy firewall
C.Application-level proxy firewall
D.Statefull firewall
Correct Answers: D

9: Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?
A.Tracert
B.Smurf scan
C.Ping trace
D.ICMP ping sweep

Correct Answers: D

10: 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?
A.Ping sweep
B.Nmap
C.Netcraft
D.Dig
Correct Answers: C

11: You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config
After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?
A.HTTP Configuration Arbitrary Administrative Access Vulnerability
B.HTML Configuration Arbitrary Administrative Access Vulnerability
C.Cisco IOS Arbitrary Administrative Access Online Vulnerability
D.URL Obfuscation Arbitrary Administrative Access Vulnerability
Correct Answers: A

12: What is the following command trying to accomplish? C:\> nmap -sU -p445 192.168.0.0/24
A.Verify that UDP port 445 is open 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 NETBIOS is running for the 192.168.0.0 network
D.Verify that UDP port 445 is closed for the 192.168.0.0 network
Correct Answers: A

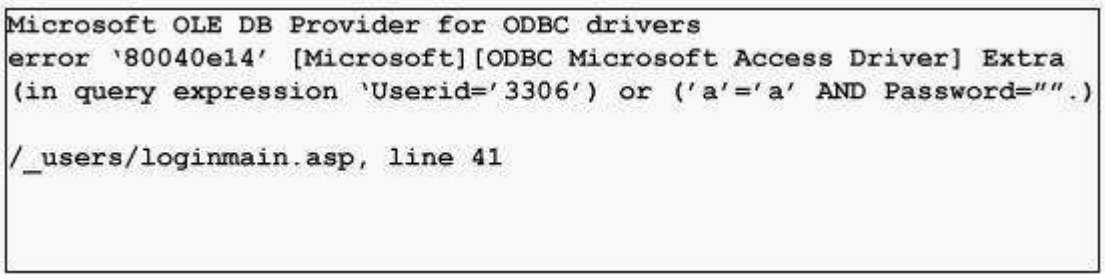
13: You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so quickly?
A.Passwords of 14 characters or less are broken up into two 7-character hashes
B.A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
C.Networks using Active Directory never use SAM databases so the SAM database pulled was empty
D.The passwords that were cracked are local accounts on the Domain Controller

Correct Answers: A

14: An "idle" system is also referred to as what?
A.PC not connected to the Internet
B.Zombie
C.PC not being used
D.Bot
Correct Answers: B

15: Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and ombies? What type of Penetration Testing is Larry planning to carry out?
A.Router Penetration Testing
B.DoS Penetration Testing
C.Firewall Penetration Testing
D.Internal Penetration Testing
Correct Answers: B

16: Click on the Exhibit Button
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?



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

17: John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found.
What information will he be able to gather from this?
A.Hillary network username and password hash
B.The SID of Hillary network account
C.The SAM file from Hillary computer
D.The network shares that Hillary has permissions

Correct Answers: A

18: Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?
A.PDF passwords can easily be cracked by software brute force tools
B.PDF passwords are converted to clear text when sent through E-mail
C.PDF passwords are not considered safe by Sarbanes-Oxley
D.When sent through E-mail, PDF passwords are stripped from the document completely
Correct Answers: A

19: Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?
A.EFS Encryption
B.DFS Encryption
C.IPS Encryption
D.SDW Encryption
Correct Answers: A

20: Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?
A.ATM
B.UDP
C.BPG
D.OSPF
Correct Answers: D