Exam Code: ec0-350

Exam Name: ethical hacking and countermeasures

Vendor: EC-Council

Version: DEMO

Part: A

1: Samuel is the network administrator of DataX Communications, Inc. He is trying to configure his firewall to block password brute force attempts on his network. He enables blocking the intruder's IP address for a period of 24 hours time after more than three unsuccessful attempts. He is confident that this rule will secure his network from hackers on the Internet.

But he still receives hundreds of thousands brute-force attempts generated from various IP addresses around the world. After some investigation he realizes that the intruders are using a proxy somewhere else on the Internet which has been scripted to enable the random usage of various proxies on each request so as not to get caught by the firewall rule.

Later he adds another rule to his firewall and enables small sleep on the password attempt so that if the password is incorrect, it would take 45 seconds to return to the user to begin another attempt. Since an intruder may use multiple machines to brute force the password, he also throttles the number of connections that will be prepared to accept from a particular IP address. This action will slow the intruder's attempts.

Samuel wants to completely block hackers brute force attempts on his network.

What are the alternatives to defending against possible brute-force password attacks on his site?

A.Enforce a password policy and use account lockouts after three wrong logon attempts even though this might lock out legit users

B.Enable the IDS to monitor the intrusion attempts and alert you by e-mail about the IP address of the intruder so that you can block them at the Firewall manually

C.Enforce complex password policy on your network so that passwords are more difficult to brute force

D.You cannot completely block the intruders attempt if they constantly switch proxies

Correct Answers: D

2: Which programming language is NOT vulnerable to buffer overflow attacks?

A.Java

B.ActiveX

C.C++

D.Assembly Language

Correct Answers: A

3: A client has approached you with a penetration test requirement. They are concerned with the possibility of external threat, and have invested considerable resources in protecting their Internet exposure. However, their main concern is the possibility of an employee elevating his/her privileges and gaining access to information outside of their department. What kind of penetration test would you recommend that would best address the client's concern?

A.A Grey Hat test

B.A Grey Box test

C.A Black Hat test

D.A White Hat test

E.A Black Box test

F.A White Box test

Correct Answers: B

4: What type of port scan is shown below?
Scan directed at open port:
ClientServer
192.5.2.92:4079 ---------FIN--------->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--------->192.5.2.110:23
192.5.2.92:4079<-----RST/ACK----------192.5.2.110:23
A.Idle Scan
B.FIN Scan
C.XMAS Scan
D.Windows Scan
Correct Answers: B

5: Which of the following built-in C/C++ functions you should avoid to prevent your program from buffer overflow attacks?
A.strcpy()
B.strcat()
C.streadd()
D.strsock()
Correct Answers: A B C

6: Bob is acknowledged as a hacker of repute and is popular among visitors of 'underground' sites. Bob is willing to share his knowledge to those who are willing to learn, and many have expressed their interest in learning from him.
However, this knowledge has risks associated with it, as the same knowledge can be used for malevolent attacks as well. In this context, what would be the most effective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals?
A.Hire more computer security monitoring personnel to monitor computer systems and networks
B.Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards
C.Train more national guard and reservist in the art of computer security to help out in times of emergency or crises
D.Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life
Correct Answers: B

7: After a client sends a connection request (SYN) packet to the server, the server will respond (SYN-ACK) with a sequence number of its choosing, which then must be acknowledged (ACK) by the client. This sequence number is predictable; the attack connects to a service first with its

own IP address, records the sequence number chosen, and then opens a second connection from a forged IP address. The attack doesn't see the SYN-ACK (or any other packet) from the server, but can guess the correct responses. If the source IP address is used for authentication, then the attacker can use the one-sided communication to break into the server.
What attacks can you successfully launch against a server using the above technique?
A.Session Hijacking attacks
B.Denial of Service attacks
C.Web page defacement attacks
D.IP spoofing attacks
Correct Answers: A

8: Eric notices repeated probes to port 1080. He learns that the protocol being used is designed to allow a host outside of a firewall to connect transparently and securely through the firewall. He wonders if his firewall has been breached. What would be your inference?
A.Eric's network has been penetrated by a firewall breach
B.The attacker is using the ICMP protocol to have a covert channel
C.Eric has a Wingate package providing FTP redirection on his network
D.Somebody is using SOCKS on the network to communicate through the firewall
Correct Answers: D

9: Mark works as a contractor for the Department of Defense and is in charge of network security. He has spent the last month securing access to his network from all possible entry points. He has segmented his network into several subnets and has installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except ports that must be used. He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Mark is fairly confident of his perimeter defenses, but is still worried about programs like Hping2 that can get into a network through covert channels.
How should mark protect his network from an attacker using Hping2 to scan his internal network?
A.Block ICMP type 13 messages
B.Block all incoming traffic on port 53
C.Block all outgoing traffic on port 53
D.Use stateful inspection on the firewalls
Correct Answers: A

10: Bill has started to notice some slowness on his network when trying to update his company's website and while trying to access the website from the Internet. Bill asks the help desk manager if he has received any calls about slowness from the end users, but the help desk manager says that he has not. Bill receives a number of calls from customers that cannot access the company website and cannot purchase anything online. Bill logs on to a couple of his routers and notices that the logs show network traffic is at an all time high.?He also notices that almost all the traffic is originating from a specific address.
Bill decides to use Geotrace to find out where the suspect IP is originates from. The Geotrace utility runs a traceroute and finds that the IP is coming from Panama.?Bill knows that none of his customers are in Panama so he immediately thinks that his company is under a Denial of Service

attack. Now Bill needs to find out more about the originating IP address.
What Internet registry should Bill look in to find the IP address?
A.LACNIC
B.ARIN
C.RIPE LACNIC
D.APNIC
Correct Answers: A

11: Bill has successfully executed a buffer overflow against a Windows IIS web server. He has been able to spawn an interactive shell and plans to deface the main web page. He first attempts to use the "Echo" command to simply overwrite index.html and remains unsuccessful. He then attempts to delete the page and achieves no progress. Finally, he tries to overwrite it with another page in which also he remains unsuccessful. What is the probable cause of Bill's problem?
A.The system is a honeypot
B.The HTML file has permissions of read only
C.You cannot use a buffer overflow to deface a web page
D.There is a problem with the shell and he needs to run the attack again
Correct Answers: B

12: Clive is conducting a pen-test and has just port scanned a system on the network. He has identified the operating system as Linux and been able to elicit responses from ports 23, 25 and 53. He infers port 23 as running Telnet service, port 25 as running SMTP service and port 53 as running DNS service. The client confirms these findings and attests to the current availability of the services. When he tries to telnet to port 23 or 25, he gets a blank screen in response. On typing other commands, he sees only blank spaces or underscores symbols on the screen. What are you most likely to infer from this?
A.The services are protected by TCP wrappers
B.There is a honeypot running on the scanned machine
C.An attacker has replaced the services with trojaned ones
D.This indicates that the telnet and SMTP server have crashed
Correct Answers: A

13: Maurine is working as a security consultant for Hinklemeir Associates.She has asked the Systems Administrator to create a group policy that would not allow null sessions on the network. The Systems Administrator is fresh out of college and has never heard of null sessions and does not know what they are used for. Maurine is trying to explain to the Systems Administrator that hackers will try to create a null session when footprinting the network.
Why would an attacker try to create a null session with a computer on a network?
A.Enumerate users and shares
B.Install a backdoor for later attacks
C.Escalate his/her privileges on the target server
D.To create a user with administrative privileges for later use
Correct Answers: A

14: What file system vulnerability does the following command take advantage of?

type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe

A.HFS

B.ADS

C.NTFS

D.Backdoor access

Correct Answers: B

15: What is the purpose of firewalking?

A.It's a technique used to map routers on a network link

B.It's a technique used to discover Wireless network on foot

C.It's a technique used to discover interface in promiscuous mode

D.It's a technique used to discover what rules are configured on a gateway

Correct Answers: D