QUESTION 234

You are performing a port scan with nmap. You are in hurry and conducting the scans at the fastest possible speed. However, you don't want to sacrifice reliability for speed. If stealth is not an issue, what type of scan should you run to get very reliable results?

A. Stealth scan
B. Connect scan
C. Fragmented packet scan
D. XMAS scan

Correct Answer: B

QUESTION 235

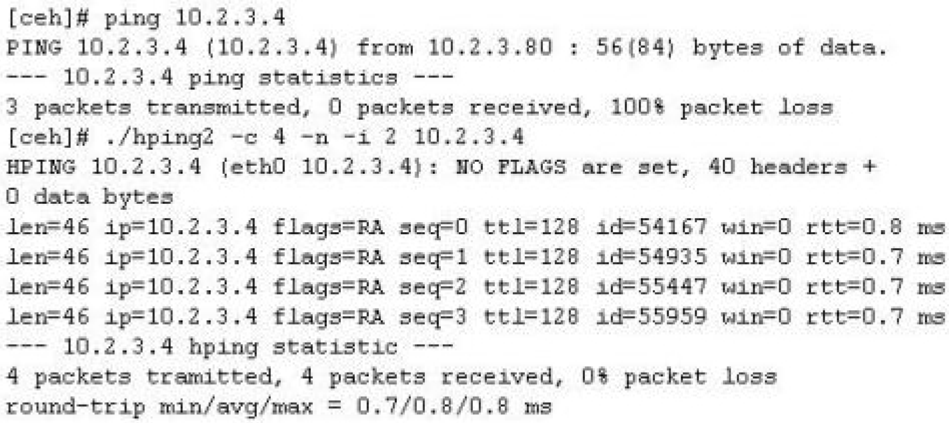
Blane is a security analyst for a law firm. One of the lawyers needs to send out an email to a client but he wants to know if the email is forwarded on to any other recipients. The client is explicitly asked not to re-send the email since that would be a violation of the lawyer's and client's agreement for this particular case. What can Blane use to accomplish this?

A. He can use a split-DNS service to ensure the email is not forwarded on.
B. A service such as HTTrack would accomplish this.
C. Blane could use MetaGoofil tracking tool.
D. Blane can use a service such as ReadNotify tracking tool.

Correct Answer: D

QUESTION 236

You ping a target IP to check if the host is up. You do not get a response. You suspect ICMP is blocked at the firewall. Next you use hping2 tool to ping the target host and you get a response. Why does the host respond to hping2 and not ping packet?



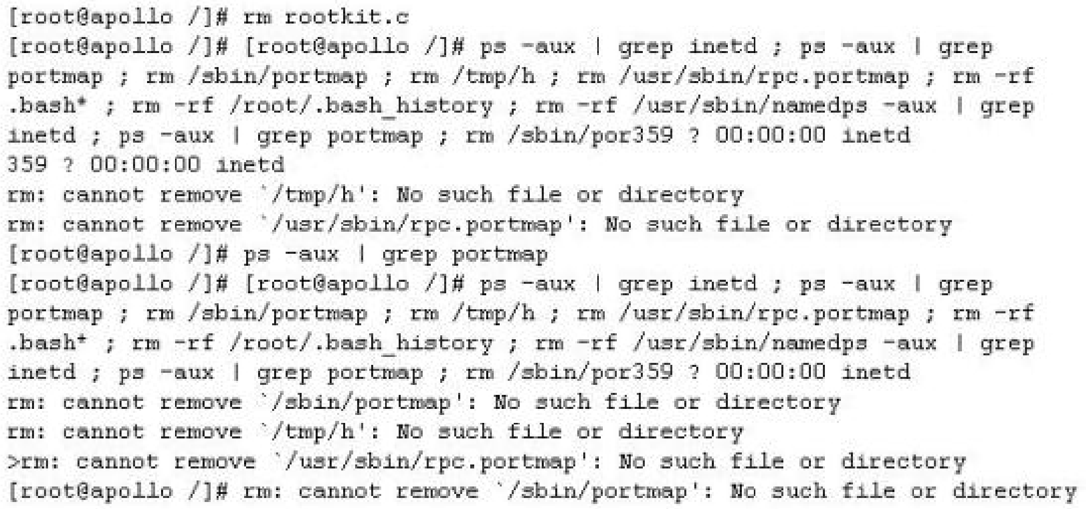
```
[ceh]# ping 10.2.3.4
PING 10.2.3.4 (10.2.3.4) from 10.2.3.80 : 56(84) bytes of data.
--- 10.2.3.4 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
[ceh]# ./hping2 -c 4 -n -i 2 10.2.3.4
HPING 10.2.3.4 (eth0 10.2.3.4): NO FLAGS are set, 40 headers +
0 data bytes
len=46 ip=10.2.3.4 flags=RA seq=0 ttl=128 id=54167 win=0 rtt=0.8 ms
len=46 ip=10.2.3.4 flags=RA seq=1 ttl=128 id=54935 win=0 rtt=0.7 ms
len=46 ip=10.2.3.4 flags=RA seq=2 ttl=128 id=55447 win=0 rtt=0.7 ms
len=46 ip=10.2.3.4 flags=RA seq=3 ttl=128 id=55959 win=0 rtt=0.7 ms
--- 10.2.3.4 hping statistic ---
4 packets tramitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.8/0.8 ms
```

A. Ping packets cannot bypass firewalls.
B. You must use ping 10.2.3.4 switch.
C. Hping2 uses stealth TCP packets to connect.
D. Hping2 uses TCP instead of ICMP by default.

Correct Answer: D

QUESTION 237

John is the network administrator of XSECURITY systems. His network was recently compromised. He analyzes the log files to investigate the attack. Take a look at the following Linux log file snippet. The hacker compromised and "owned" a Linux machine. What is the hacker trying to accomplish here?



```
[root@apollo /]# rm rootkit.c
[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ; ps -aux | grep
portmap ; rm /sbin/portmap ; rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf
.bash* ; rm -rf /root/.bash_history ; rm -rf /usr/sbin/namedps -aux | grep
inetd ; ps -aux | grep portmap ; rm /sbin/por359 ? 00:00:00 inetd
359 ? 00:00:00 inetd
rm: cannot remove `/tmp/h': No such file or directory
rm: cannot remove `/usr/sbin/rpc.portmap': No such file or directory
[root@apollo /]# ps -aux | grep portmap
[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ; ps -aux | grep
portmap ; rm /sbin/portmap ; rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf
.bash* ; rm -rf /root/.bash_history ; rm -rf /usr/sbin/namedps -aux | grep
inetd ; ps -aux | grep portmap ; rm /sbin/por359 ? 00:00:00 inetd
rm: cannot remove `/sbin/portmap': No such file or directory
rm: cannot remove `/tmp/h': No such file or directory
>rm: cannot remove `/usr/sbin/rpc.portmap': No such file or directory
[root@apollo /]# rm: cannot remove `/sbin/portmap': No such file or directory
```

A. The hacker is attempting to compromise more machines on the network.
B. The hacker is planting a rootkit.
C. The hacker is running a buffer overflow exploit to lock down the system.
D. The hacker is trying to cover his tracks.

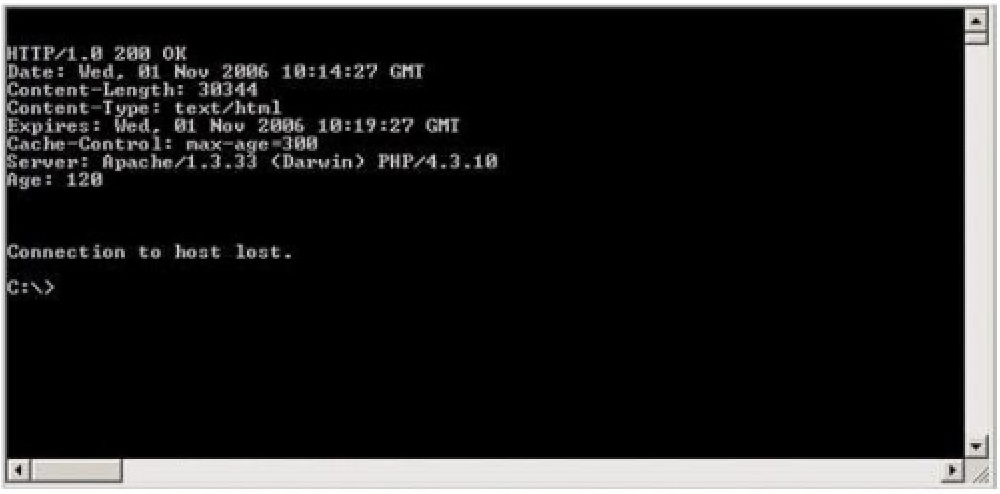
Correct Answer: D

QUESTION 238

Blake is in charge of securing all 20 of his company's servers. He has enabled hardware and software firewalls, hardened the operating systems, and disabled all unnecessary services on all the servers. Unfortunately, there is proprietary AS400 emulation software that must run on one of the servers that requires the telnet service to function properly. Blake is especially concerned about this since telnet can be a very large security risk in an organization. Blake is concerned about how this particular server might look to an outside attacker so he decides to perform some footprinting, scanning, and penetration tests on the server. Blake telnets into the server using Port 80 and types in the following command:

HEAD / HTTP/1.0

After pressing enter twice, Blake gets the following results: What has Blake just accomplished?



```
HTTP/1.0 200 OK
Date: Wed, 01 Nov 2006 10:14:27 GMT
Content-Length: 30344
Content-Type: text/html
Expires: Wed, 01 Nov 2006 10:19:27 GMT
Cache-Control: max-age=300
Server: Apache/1.3.33 (Darwin) PHP/4.3.10
Age: 120


Connection to host lost.

C:\>
```

A. Downloaded a file to his local computer.
B. Submitted a remote command to crash the server.
C. Poisoned the local DNS cache of the server.
D. Grabbed the Operating System banner.

Correct Answer: D

QUESTION 239

You want to perform advanced SQL Injection attack against a vulnerable website. You are unable to perform command shell hacks on this server. What must be enabled in SQL Server to launch these attacks?

A. System services
B. EXEC master access
C. xp_cmdshell
D. RDC

Correct Answer: C

QUESTION 240

Kevin is an IT security analyst working for Emerson Time Makers, a watch manufacturing company in Miami. Kevin and his girlfriend Katy recently broke up after a big fight. Kevin believes that she was seeing another person. Kevin, who has an online email account that he uses for most of his mail, knows that Katy has an account with that same company. Kevin logs into his email account online and gets the following URL after successfully logged in:

http://www.youremailhere.com/mail.asp?mailbox=Kevin&Smith=121%22

Kevin changes the URL to:
http://www.youremailhere.com/mail.asp?mailbox=Katy&Sanchez=121%22

Kevin is trying to access her email account to see if he can find out any information. What is Kevin attempting here to gain access to Katy's mailbox?

A. This type of attempt is called URL obfuscation when someone manually changes a URL to try and gain unauthorized access.
B. By changing the mailbox's name in the URL, Kevin is attempting directory transversal.
C. Kevin is trying to utilize query string manipulation to gain access to her email account.
D. He is attempting a path-string attack to gain access to her mailbox.

Correct Answer: C

QUESTION 241

A majority of attacks come from insiders, people who have direct access to a company's computer system as part of their job function or a business relationship. Who is considered an insider?

A. A competitor to the company because they can directly benefit from the publicity generated by making such an attack.
B. Disgruntled employee, customers, suppliers, vendors, business partners, contractors, temps, and consultants.
C. The CEO of the company because he has access to all of the computer systems.
D. A government agency since they know the company's computer system strengths and weaknesses.

Correct Answer: B

QUESTION 242

Jeremy is web security consultant for Information Securitas. Jeremy has just been hired to perform contract work for a large state agency in Michigan. Jeremy's first task is to scan all the company's external websites. Jeremy comes upon a login page which appears to allow employees access to sensitive areas on the website. James types in the following statement in the username field:

SELECT * from Users where username='admin' ?AND password='' AND email like
'%@testers.com%'

What will the SQL statement accomplish?

A. If the page is susceptible to SQL injection, it will look in the Users table for usernames of admin.
B. This statement will look for users with the name of admin, blank passwords, and email addresses that end in @testers.com.
C. This Select SQL statement will log James in if there are any users with NULL passwords.
D. James will be able to see if there are any default user accounts in the SQL database.

Correct Answer: B

QUESTION 243

An attacker is attempting to telnet into a corporation's system in the DMZ. The attacker doesn't want to get caught and is spoofing his IP address. After numerous tries he remains unsuccessful in connecting to the system. The attacker rechecks that the target system is actually listening on Port 23 and he verifies it with both nmap and hping2. He is still unable to connect to the target system. What could be the reason?

A. The firewall is blocking port 23 to that system.
B. He needs to use an automated tool to telnet in.
C. He cannot spoof his IP and successfully use TCP.
D. He is attacking an operating system that does not reply to telnet even when open.

Correct Answer: C

QUESTION 244

If an attacker's computer sends an IPID of 31400 to a zombie (Idle Scanning) computer on an open port, what will be the response?

A. 31400
B. 31402
C. The zombie will not send a response