QUESTIONS

1. Examine the following password hashes obtained from a Windows XP machine using LM hashing:

   B757BF5C0D87772FAAD3B435B51404EE

   BA810DBA98995F1817306D272A9441BB

   E52CAC67419A9A224A3B108F3FA6CB6D

   0182BD0BD4444BF836077A718CCDF409

   CEC52EB9C8E3455DC2265B23734E0DAC

   Which of the following is true regarding the hashes listed?

   A. The hashes are protected using Syskey.

   B. The third hash listed is the local administrator's password.

   C. The first hash listed is from a password of seven characters or less.

   D. The hashes can be easily decrypted by reversing the hash algorithm.

2. Amanda works as a security administrator for a large organization. She discovers some remote tools installed on a server and has no record of a change request asking for them. After some investigation, she discovers an unknown IP address connection that was able to access the network through a high-level port that was not closed. The IP address is first traced to a proxy server in Mexico. Further investigation shows the connection bounced between several proxy servers in many locations. Which of the following is the most likely proxy tool used by the attacker to cover his tracks?

   A. ISA proxy

   B. IAS proxy

   C. TOR proxy

   D. Netcat

3. Which of the following correctly describes brute-force password attacks?

   A. Feeding a list of words into a cracking program

   B. Comparing the hash values to lists of prehashed values for a match

   C. Attempting all possible combinations of letters, numbers, and special characters in succession

   D. Threatening the user with physical violence unless they reveal their password

4. Which password theft method is almost always successful, requires little technical knowledge, and is nearly impossible to detect?

   A. Installing a hardware keylogger

   B. Installing a software keylogger

- **C.** Sniffing the network segment with Ettercap
- **D.** Attempting a brute-force attack using Cain and Abel

5. Which of the following will extract an executable file from NTFS streaming?

- **A.** c:\> cat file1.txt:hidden.exe > visible.exe
- **B.** c:\> more file1.txt | hidden.exe > visible.exe
- **C.** c:\> type notepad.exe > file1.txt:hidden.exe
- **D.** c:\> list file1.txt$hidden.exe > visible.exe

6. Which command is used to allow all privileges to the user, read-only to the group, and read-only for all others to a particular file, on a Linux machine?

- **A.** chmod 411 file1
- **B.** chmod 114 file1
- **C.** chmod 117 file1
- **D.** chmod 711 file1
- **E.** chmod 744 file1

7. Examine the following passwd file:

```
root:x:0:0:root:/root:/bin/bash
mwalk:x:500:500:Matt Walker,Room 2238,email:/home/mwalk:/bin/sh
jboll:x:501:501:Jason Bollinger,Room 2239,email:/home/jboll:/bin/sh
rbell:x:502:502:Rick Bell,Room 1017,email:/home/rbell:/bin/sh
afrench:x:503:501:Alecia French,Room 1017,email:/home/afrench:/bin/sh
```

Which of the following statements are true regarding this passwd file? (Choose all that apply.)

- **A.** None of the user accounts has passwords assigned.
- **B.** The system makes use of the shadow file.
- **C.** The root account password is root.
- **D.** The root account has a shadowed password.
- **E.** Files created by Alecia will initially be viewable by Jason.

8. You are attempting to hack a Windows machine and want to gain a copy of the SAM file. Where can you find it? (Choose all that apply.)

- **A.** /etc/passwd
- **B.** /etc/shadow
- **C.** c:\windows\system32\config
- **D.** c:\winnt\config
- **E.** c:\windows\repair

9. Which of the following statements are true concerning Kerberos? (Choose all that apply.)

   A. Kerberos uses symmetric encryption.

   B. Kerberos uses asymmetric encryption.

   C. Clients ask for authentication tickets from the KDC in clear text.

   D. KDC responses to clients never include a password.

   E. Clients decrypt a TGT from the server.

10. What is the difference between a dictionary attack and a hybrid attack?

   A. Dictionary attacks are based solely on word lists, whereas hybrid attacks make use of both word lists and rainbow tables.

   B. Dictionary attacks are based solely on whole word lists, whereas hybrid attacks can use a variety of letters, numbers, and special characters.

   C. Dictionary attacks use predefined word lists, whereas hybrid attacks substitute numbers and symbols within those words.

   D. Hybrid and dictionary attacks are the same.

11. Which of the following contains a listing of port numbers for well-known services defined by IANA?

   A. %windir%\etc\lists

   B. %windir%\system32\drivers\etc\lmhosts

   C. %windir%\system32\drivers\etc\services

   D. %windir%\system32\drivers\etc\hosts

12. Which of the following SIDs indicates the true administrator account?

   A. S-1-5-21-1388762127-2960977290-773940301-1100

   B. S-1-5-21-1388762127-2960977290-773940301-1101

   C. S-1-5-21-1388762127-2960977290-773940301-500

   D. S-1-5-21-1388762127-2960977290-773940301-501

13. In which step of EC-Council's system hacking methodology would you find steganography?

   A. Cracking passwords

   B. Escalating privileges

   C. Executing applications

   D. Hiding files

   E. Covering tracks

14. Examine the following extract from a compromised system:

```
c:\> cmd /c type c:\winnt\repair\sam > c:\syskey.txt
```

Which of the following is the best description of what the attacker is attempting to accomplish?

A. Replacing the SAM file with a file of his choosing

B. Copying the SAM file for offline cracking attempts

C. Cracking any Syskey encryption on the SAM file

D. Uploading a virus

15. Which password would be considered the most secure?

A. CEH123TEST

B. CEHisaHARDTEST

C. 638154849675

D. C3HisH@rd

16. Which of the following are true statements? (Choose all that apply.)

A. John the Ripper does not display the case of cracked LM hash passwords.

B. NTLMV1 represents an effective countermeasure to password cracking.

C. Syskey provides additional protection against password cracking.

D. The hash value of a Windows LM password that is seven characters or less will always be passed as 00112233445566778899.

E. Enforcing complex passwords provides additional protection against password cracking.

17. Which of the following are considered offline password attacks? (Choose all that apply.)

A. Using a hardware keylogger

B. Brute-force cracking with Cain and Abel on a stolen SAM file

C. Using John the Ripper on a stolen passwd file

D. Shoulder surfing

18. If a rootkit is discovered on the system, which of the following is the *best* alternative for recovery?

A. Replacing all data files from a good backup

B. Installing Tripwire

C. Reloading the entire system from known good media

D. Deleting all data files and reboot

19. Examine the following portion of a log file, captured during a hacking attempt:

```
[matt@localhost]#rm -rf /tmp/mykit_headers
[matt@localhost]#rm -rf /var/log/messages
[matt@localhost]#rm -rf /root/.bash_history
```

What was the attacker attempting to do?

A. Copy files for later examination

B. Cover his tracks

C. Change the shell to lock out other users

D. Upload a rootkit

20. You suspect a hack has occurred against your Linux machine. Which command will display all running processes for you to review?

A. ls -d

B. ls -l

C. su

D. ps -ef

E. ifconfig

21. An organization wants to control network traffic and perform stateful inspection of traffic going into and out of their DMZ. Which built-in functionality of Linux can achieve this?

A. iptables

B. ipchains

C. ipsniffer

D. ipfirewall

22. Which of the following best describes Cygwin?

A. Cygwin is a UNIX subsystem running on top of Windows.

B. Cygwin is a Windows subsystem running on top of UNIX.

C. Cygwin is a C++ compiler.

D. Cygwin is a password cracking tool.

23. Which folder in Linux holds administrative commands and daemons?

A. /sbin

B. /bin

C. /dev

D. /mnt

E. /usr

24. Which of the following is the appropriate means to pivot within a Metasploit attack session?

  A. Use the pivot exploit outside meterpreter.

  B. Reconfigure network settings in meterpreter.

  C. Set the payload to propagate.

  D. Create a route statement in the meterpreter.

25. You are examining files on a Windows machine and note one file's attributes include "h." What does this indicate?

  A. The file is flagged for backup.

  B. The file is part of the help function.

  C. The file is fragmented because of size.

  D. The file has been quarantined by an antivirus program.

  E. The file is hidden.

26. You have gained access to a SAM file from an older Windows machine and are preparing to run a Syskey cracker against it. How many bits are used for Syskey encryption?

  A. 128

  B. 256

  C. 512

  D. 1024

27. Which of the following tools can assist in discovering the use of NTFS file streams? (Choose all that apply.)

  A. LADS

  B. ADS Spy

  C. Sfind

  D. Snow

28. Which of the following are true regarding Kerberos?

  A. Kerberos makes use of UDP as a transport protocol.

  B. Kerberos makes use of TCP as a transport protocol.

  C. Kerberos uses port 88 for the transmission of data.

  D. Kerberos makes use of both symmetric and asymmetric encryption techniques.

  E. All of the above.

29. Which authentication method uses DES for encryption and forces 14-character passwords for hash storage?

    A. NTLMv1

    B. NTLMv2

    C. LAN Manager

    D. Kerberos