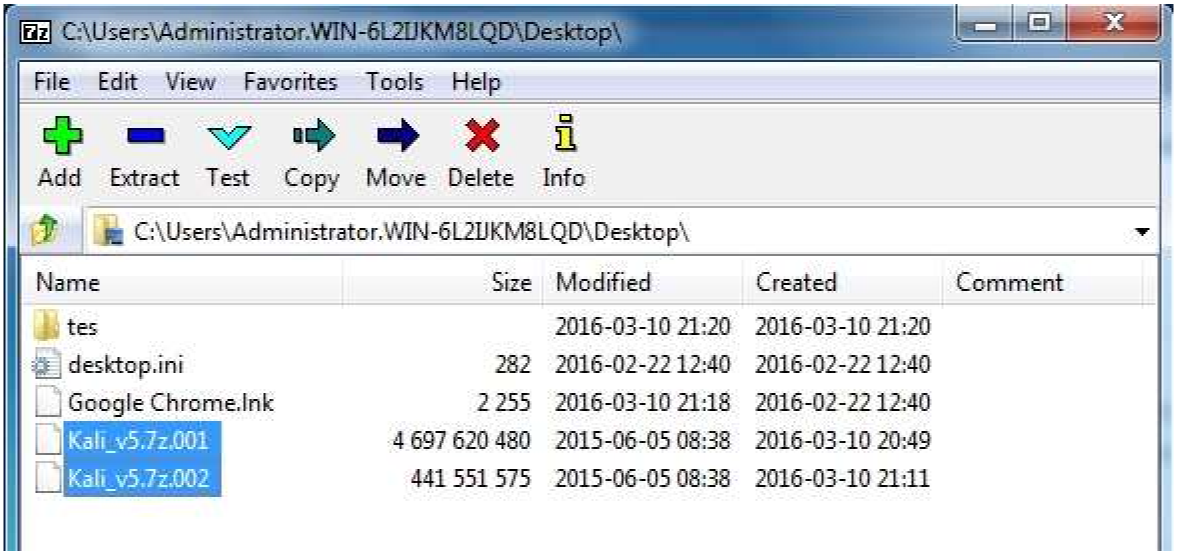
Additional Hacking Thoughts

Extracting the KALI Attack Server

The KALI Attack server on the CD is a VM directory that was compressed with 7zip and broken into 2 parts. To decompress:

1. Copy the files off of the DVD (Kali_v5.7z.001) and off of the CD (Kali_v5.7z.001) onto your computer.
2. Download and install 7zip
3. Open 7zip and browse to the directory where the two files are.
4. Select both files and click Extract. This will take about 10 minutes.


C:\Users\Administrator.WIN-6L2IJKM8LQD\Desktop\
File
Edit
View
Favorites
Tools
Help
Add
Extract
Test
Copy
Move
Delete
Info
C:\Users\Administrator.WIN-6L2IJKM8LQD\Desktop\

Name	Size	Modified	Created	Comment
tes		2016-03-10 21:20	2016-03-10 21:20	
desktop.ini	282	2016-02-22 12:40	2016-02-22 12:40	
Google Chrome.lnk	2 255	2016-03-10 21:18	2016-02-22 12:40	
Kali_v5.7z.001	4 697 620 480	2015-06-05 08:38	2016-03-10 20:49	
Kali_v5.7z.002	441 551 575	2015-06-05 08:38	2016-03-10 21:11	

The resulting Kali directory is about 15 GB.

You can now open the .vmx file with VMWare Player or workstation.

Setting Up for the CPT Practical

1. Create a folder on your desktop called CPT, in that folder create new folders called Docs, Archive, and VMs

2. Copy the four (4) RAR files: Debian 7 (Kali) part 1 and part 2, CPT VM1, & CPT VM2, to the CPT folder and then extract the files to the VMs folder-- **use winrar or 7Zip for the extraction**.

3. Start VM Workstation; on the HOME tab, click -- **Open a Virtual Machine**, and open your three VMs (Debian, CPTVM1 and CPTVM2). ***NOTE: Open but do not power on the three VM's***

4. On the two target VM's(CPTVM1 and CPTVM2) increase memory with the setting option. By default both are set to 256M, increase both to minimum of 512M. Make sure all three VM's (Kali, CPTVM1 and CPTVM2) are set to the same network mode (NAT or Bridged is fine, but NAT might be easier to manage, **especially if** the IP address for the network is 192.168.1.x).

5. Start the KALI server. Create a project directory in your home folder (/root) -- **mkdir CPT**. Use this directory to hold all your findings from the pentest and as the file transfer area.

Additional Hacking Thoughts

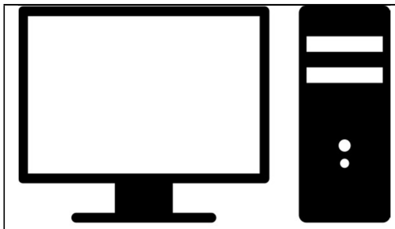
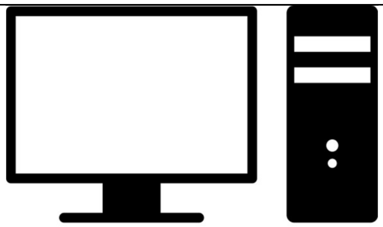
READ THE INSTRUCTIONS!!!

If you don't read the instructions on the CD, you won't know what your goal is. You can't just copy the walkthrough.

As you gather information, you may need to transfer between machines. You can use the enabled protocols, netcat (as we learned in class, or Secure Copy (see notes)

Using Netcat for File Transfer

Netcat is like a swiss army knife for geeks. It can be used for just about anything involving TCP or UDP. One of its most practical uses is to transfer files. netcat is just a single executable, and works across all platforms (Windows,Mac OS X, Linux).

	
Sender 192.168.10.1 **user@linux#** nc -w 3 192.168.30.10 1234 < out.file where out.file is the file you want to send	Receiver-Listening 192.168.30.10 **user@linux#** nc -l -p 1234 > out.file

Using SCP for file transfer

Secure copy is a tool that allows for secure copying using SSH. It is easy to use from the command line, if you have the credentials to access another system.

Copy the file "foobar.txt" from a remote host to the local host

```
$ scp your_username@remotehost.edu:foobar.txt /some/local/directory
```

Copy the file "foobar.txt" from the local host to a remote host

```
$ scp foobar.txt your_username@remotehost.edu:/some/remote/directory
```

Copy the directory "foo" from the local host to a remote host's directory "bar"

```
$ scp -r foo your_username@remotehost.edu:/some/remote/directory/bar
```

Copy the file "foobar.txt" from remote host "rh1.edu" to remote host "rh2.edu"

```
$ scp your_username@rh1.edu:/some/remote/directory/foobar.txt \
your_username@rh2.edu:/some/remote/directory/
```

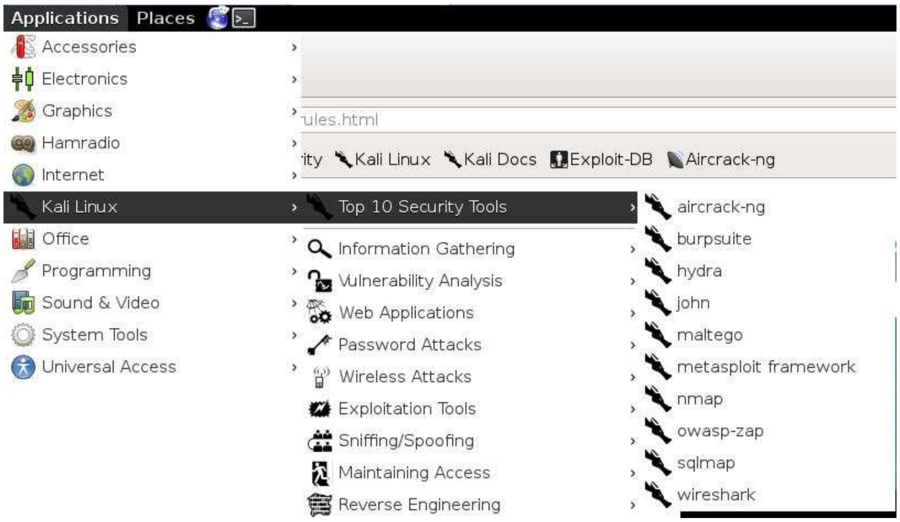
http://www.hypexr.org/linux_scp_help.php

Additional Hacking Thoughts

Linux Password Cracking

Linux passwords are stored in the /etc/passwd file in cleartext in older systems and in /etc/shadow file in hash form on newer systems. We should expect that the passwords on anything other than old legacy systems to be stored in /etc/shadow.

John the Ripper is a simple, but powerful password cracker without a GUI (this helps to make it faster as GUIs consume resources). It can be accessed from the command line, or from the KALI menu system Applications->Kali->10 Most Used Tools-> John. This will open John in a command prompt.



Linux stores its passwords in /etc/shadow, so what we want to do is copy this file to our current directory along with the /etc/passwd file, then "unshadow" them and store them in file we'll call passwords. So, let's type both:

ATTACKServer# cp /etc/shadow ./

ATTACKServer# cp /etc/passwd ./

Next we need to combine the information in the /etc/shadow and the /etc/passwd files, so that John can do its magic.

ATTACKServer# unshadow passwd shadow > passwords

Now that we have unshadowed the critical files, we can simply let John run on our password file.

ATTACKServer# john passwords

This will use the defaults…You will probably want to grab a better wordlist, and possible update the “mangling” rules used to find variations on the files in the wordlist.

Making John the Ripper better

John the Ripper comes with a default wordlist, but you can modify the list that is used. I recommend looking on http://download.openwall.net/pub/wordlists/ for the all.gz wordlist.

Additional Hacking Thoughts

Luckily, there is an advanced wordlist included with the KALI attack server. Look for the rockyou.txt.gz file. You can search for it with:

```
ATTACKServer# find / -name rockyou*
```

Copy the wordlist to your CPT directory, and you can use it to crack the passwords you gather. You do have to unizip it first:

```
ATTACKServer#  gzip –d Rockyou.txt.gz
```

This will result in a file named Rockyou.txt. If the wordlist and the password/hashes file are in the same directory, you can use this wordlist with the –w option

```
ATTACKServer#  John –w=all [hashedpasswordfile]
```

Below are some additional sites with details if you are interested in learning more about John the Ripper.

http://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-user-passwords-linux-system-0147164/

This document is a good review of John the Rippers modes- http://www.openwall.com/john/doc/MODES.shtml

Privilege Escalation

Once you have compromised the first server, and gained access to the second, you will need to escalate your privilege to root. This can be done by taking advantage of the older Linux 2.4 kernel. Youc an search google for various exploits related to kernel escalation with the Linux 2.4 kernel.

I would recommend the exploit located at https://www.exploit-db.com/exploits/17462/. You will need to get the source code onto the machine you want to attack, and then compile it. The compiler can be called from the command line:

```
CPTVM2> gcc269 778.c –o 778_exploit
```

Where 778.c is the source code and the 778_exploit is the code you will execute. You can then make it executable and execute it:

```
CPTVM2> chmod u+x 778_exploit

CPTVM2> ./778_exploit
```

Many exploits will require you to run them repeatedly to have them “win the race” to get to the exploit. Be patient, and contact me if you are concerned. Obviously, you may want to try other exploits as well.

Here is a good article about looking for places or things to exploit:

http://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

Additional Hacking Thoughts

Down and Dirty Penetration Walkthrough:

DOCUMENT, DOCUMENT, DOCUMENT. Screen shots, copy and paste, etc. You want to include details in your report.

1. Set up attack server and victims on the same network
2. Use wireshark to sniff traffic
3. Look for clear text passwords (refer to your lab book for ideas).
4. Do scans of both machines to look for additional services/potentials services to exploit
5. Use the credentials found in step 3 to log in to one machine.
6. Get the /etc/passwd and /etc/shadow files
7. Copy these files to the attack server
8. Use john the ripper to “crack” the passwords (don’t forget to unshadow)
9. Try these passwords with one of the login methods available on the other machine, it might use the same credentials
10. Look for potential weaknesses, services, etc that you can exploit.
11. Copy exploit code to the 2nd victim
12. Compile exploit
13. Execute exploit, maybe many times (many, many failures before success)
14. Once you have root, give yourself continued root access by adding your credentials to the sudoers file by running visudo (you may have to search for the visudo executable, check the lab book for how to search for programs and files).
15. Gather the /etc/passwd and /etc/shadow from the 3nd machine
16. Transfer the /etc/passwd and /etc/shadow to the Attack Server
17. Run John the Ripper against these hashes (unshadow first!!!)
18. Verify the root password access by logging in.
19. Document the heck out of your exploits!!!

Good Luck and contact me with any questions!!