2 Linux Fundamentals

Lab Scenario

If you are new to Linux it is time to do a little playing to get used to the Linux command line. Your boss is giving you 1 hour to become an expert! This lab has been designed to introduce you to the basic steps in using Linux, more specifically, the Kali Linux distribution.

Lab Objectives

1. Learn network interface management with the ifconfig command.
2. Learn how to connect to FTP site for storage keeping.
3. Learn how to mount a Windows partition.

Lab Resources

1. Kali Linux VM Image

Lab Tasks Overview

1. Learn the network interface management with the ifconfig command.
    a. Configure your own static IP address.
    b. View the configuration of the LAN interface.
    c. Configure your gateway.
    d. Configure a DNS server.
    e. Look at some of the other basic settings for the LAN interface.
        i. ifconfig [interface] [IP address] netmask [subnet-mask] (manually set IP and subnet-mask details)
        ii. ifconfig [interface] hw ether [MAC] (Change the network cards MAC address, specify in format 11:11:11:11:11:11)
2. Learn how to connect to FTP site.
    a. Connect to FTP site for uploading/downloading.
3. Learn how to mount a Windows partition.
    a. Create 2 new user accounts with passwords.

Lab Details - Step-by-Step Instructions

2.1 Command Line Tips & Tricks

Note: Similar to Cisco IOS, you can finish typing file or folder names in Linux by hitting the tab key after you have started typing the first few characters of what you are looking for, this will save you a lot of time and typos. The operating system only requires enough keystrokes to make the command or folder name unique from others.

Note: Linux is case sensitive.

1. To search for a command that was previously entered, press CTRL + r and start typing the first few characters of the command you're looking for. Try it now using "ifc" as the search characters:

```
File  Edit  View  Search  Terminal  Help
(reverse-i-search)`c': clear
```

2. To move to the beginning of the command line, press CTRL + a. To move to the end of the command line, press CTRL + E. To remove the command completely, press CTRL + u. Type a command now and try these shortcuts. They're guaranteed to save you time!

3. Oftentimes, you'll have to search for a file in Linux. The find command is a very powerful tool that can find a file based on almost any criteria. Find can easily locate files based on the filename. From Kali, try locating the nc.exe file using find / -name nc.exe or locate nc.exe

```
root@kali:~# find / -name nc.exe
/usr/share/wfuzz/wordlist/fuzzdb/web-backdoors/exe/nc.exe
/usr/share/sqlninja/apps/nc.exe
/usr/share/ikat/src/Windows/files/nc.exe
/usr/share/windows-binaries/nc.exe
/root/nc.exe
root@kali:~# locate nc.exe
/root/nc.exe
/usr/share/ikat/src/Windows/files/nc.exe
/usr/share/sqlninja/apps/nc.exe
/usr/share/wfuzz/wordlist/fuzzdb/web-backdoors/exe/nc.exe
/usr/share/windows-binaries/nc.exe
```

4. Check the man page for find to learn more about how to search for files in Linux. Run "man find" now. When reading man pages, use the spacebar to view the next page. To close the manpage, just press "q".

```
FIND(1)                                                    FIND(1)

NAME
       find - search for files in a directory hierarchy

SYNOPSIS
       find [-H] [-L] [-P] [-D debugopts] [-Olevel] [path...] [expression]

DESCRIPTION
       This  manual  page documents the GNU version of find.  GNU find searches the directory tree rooted at
       each given file name by evaluating the given expression from left to right, according to the rules of
       precedence  (see  section OPERATORS), until the outcome is known (the left hand side is false for and
       operations, true for or), at which point find moves on to the next file name.
```

5. The Grep utility can be used to find text within a file. Try the following command:

   grep address /etc/network/interfaces

```
root@kali:~# grep address /etc/network/interfaces
address 192.168.21.22
```

   Grep displays any line in /etc/network/interfaces that contains our search string, “address”.

6. Use grep on your own to find the line in /etc/passwd that contains the word “root”.

   grep root /etc/passwd

   FYI: If a permissions problem exists in upcoming labs (on Debian) using a Root Shell, return to this step to remedy.

   sudo gedit /etc/sudoers

   Scroll down to the section labeled #User_priviledges_specification:

   Add this line:

   student ALL=(ALL:ALL) ALL

   (similar to the root account)

   File/Save

2.2 Linux Networking for Hackers

(do not attempt these next steps in the Lab environment)

1. Kali Linux is configured to start networking by default (if you need to initialize the default interface, eth0, you can do so using the ifup command).

```
root@kali:~# ifup eth0
ifup: interface eth0 already configured
```

2. If you want to bring the interface down, use the ifdown command.

```
root@kali:~# ifdown eth0
```

3. Using ifup or ifdown automatically configures your interface from the /etc/network/interfaces file.

```
root@kali:~# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 192.168.21.22
netmask 255.255.0.0
gateway 192.168.1.1
dns-domain localdomain
dns-nameserver 192.168.1.1
```

4. You can use the ifconfig command to manually configure an IP Address.

5. To view your current settings for the eth0 interface, type ifconfig eth0, then hit enter.

```
root@kali:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:56:80:66:34
          inet addr:192.168.21.22  Bcast:192.168.255.255  Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:fe80:6634/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:703 errors:0 dropped:1 overruns:0 frame:0
          TX packets:4659 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:81659 (79.7 KiB)  TX bytes:207486 (202.6 KiB)
          Interrupt:19 Base address:0x2000
```

6. Try changing your IP address by running the following command:

```
root@kali:~# ifconfig eth0 192.168.1.151/24
root@kali:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:56:80:66:34
          inet addr:192.168.1.151  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe80:6634/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:710 errors:0 dropped:1 overruns:0 frame:0
          TX packets:4664 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:82584 (80.6 KiB)  TX bytes:207888 (203.0 KiB)
          Interrupt:19 Base address:0x2000
```

7. Be sure to change your IP address back using the ifconfig command.

   For our example: ifconfig eth0 192.168.21.22 netmask 255.255.0.0

```
root@kali:~# ifconfig eth0 192.168.21.22 netmask 255.255.0.0
```

8. To view your default gateway use the route command. The -n option prevents DNS lookups from the route command. Use it to see the output more quickly. Run the following command: route -n

```
root@kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     0.0.0.0         255.255.0.0     U     0      0        0 eth0
```

   a) You can add or remove your default gateway using the route command. The format to add a default gateway is: route add default gw <*IP address of gateway*>. Run the following command: route add default gw 192.168.1.100

   b) If you end up with two default gateways, you probably want to remove one of them. Change the "add" to "del" and run the route command again.

```
root@kali:~# route add default gw 192.168.1.1
root@kali:~# route del default gw 192.168.1.1
```

9. DNS servers are listed in the /etc/resolv.conf file after the keywork "nameserver". Run the following command to see the contents of resolv.conf: cat /etc/resolv.conf

```
root@kali:~# cat /etc/resolv.conf
nameserver 192.168.1.1
root@kali:~#
```

2.3 Files

In Linux, everything is a file. As a Pen Tester, you'll need to know how to move files from one system to another using whatever tools are installed on the target.

To install Pure FTP on the Debian VM (if not already installed), type in the following:

apt-get install pure-ftpd-common pure-ftpd

```
root@kali:~# apt-get install pure-ftpd-common pure-ftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

1. Move the file ca_setup from your Kali VM to the Debian VM

   a. Change to your home directory by running the cd command without any options.

   b. Using ftp, login to your Debian VM with the student account. (student / P@ssw0rd)

```
root@kali:~# ftp 192.168.21.21
Connected to 192.168.21.21.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 12:01. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (192.168.21.21:root): student
331 User student OK. Password required
Password:
230 OK. Current directory is /home/student
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

2. Now that you're connected, use the "put" command to transfer ca_setup.exe from Kali to Debian. From the FTP prompt (ftp>), run the following command:

put ca_setup.exe

```
ftp> put ca_setup.exe
local: ca_setup.exe remote: ca_setup.exe
200 PORT command successful
150 Connecting to port 50162
226-File successfully transferred
226 0.708 seconds (measured here), 10.85 Mbytes per second
8049726 bytes sent in 0.71 secs (11119.9 kB/s)
ftp>
```

3. To close an FTP session, type “bye” at the FTP prompt.

```
ftp> bye
221-Goodbye. You uploaded 7862 and downloaded 0 kbytes.
221 Logout.
root@kali:~#
```

4. From Kali, connect to Debian using SSH.

```
root@kali:~# ssh student@192.168.21.21
student@192.168.21.21's password:
Linux debian 3.2.0-4-amd64 #1 SMP Debian 3.2.54-2 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Thu Jan  2 20:33:15 2014 from 192.168.1.101
```

5. The ca_setup file should be in your home directory if you completed the previous steps. Verify that it’s there and that it’s the correct size.

```
student@debian:~$ ls -lh
total 7.8M
-rw-r--r-- 1 student student 7.7M Apr 10 12:03 ca setup.exe
drwxr-xr-x 2 student student 4.0K Dec 23  2013 Desktop
drwxr-xr-x 2 student student 4.0K Dec 20  2013 Documents
drwxr-xr-x 3 student student 4.0K Jul 30  2014 Downloads
```

6. Now, let’s mount a Windows share, so we can get this file on to the Windows 2003 Server.

7. First, list the shares that are available.

```
student@debian:~$ smbclient -L W2K3-XXX -U Administrator
Enter Administrator's password:
Domain=[W2K3-XXX] OS=[Windows Server 2003 3790] Server=[Windows Server 2003 5.2]

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       Remote IPC
        Share           Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
```

8. Connect to “Share” on W2K3-XXX by typing sudo mount –t cifs <ip address>:Share /mnt –o username=Administrator,pass=P@ssw0rd

```
student@debian:~$ sudo mount -t cifs 192.168.21.25:Share /mnt -o username=Administrator,pass=P@ssw0rd
```

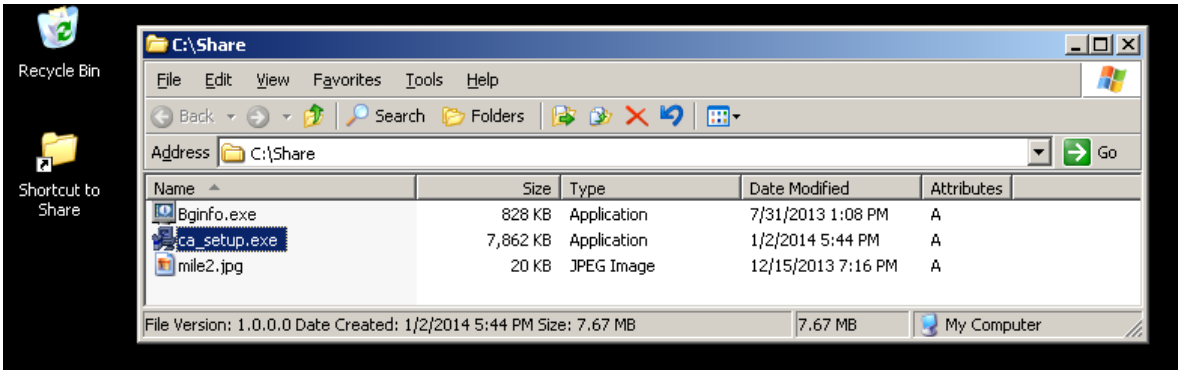
9. Copy the ca_setup file into the newly mounted share by typing sudo cp ca_setup.exe /mnt

```
student@debian:~$ sudo cp ca_setup.exe /mnt
```

10. Verify that ca_setup is on the Share by typing ls –lh /mnt

```
student@debian:~$ ls -lh /mnt
total 7.8M
-rwxr-xr-x 0 root root 7.7M Apr 10 12:12 ca_setup.exe
-rwxr-xr-x 0 root root  58K Mar 15 17:58 nc.exe
-rwxr-xr-x 0 root root  10K Dec 23  2013 Thumbs.db
student@debian:~$
```

11. Finally, open Windows 2003 VM in VMware and look in the Share folder



12. Let's copy another important file into our Windows share. This time, we'll use SCP to transfer the file from Kali to Debian. Before we begin, make sure you close your previous ftp session and are back to the Kali command prompt. You can type exit to get back to the Kali prompt.

```
student@debian:~$ exit
logout
Connection to 192.168.21.21 closed.
root@kali:~#
```

13. Kali Linux comes with a few windows tools. Find it by using locate nc.exe command.

```
root@kali:~# locate nc.exe
/root/nc.exe
/usr/share/ikat/src/Windows/files/nc.exe
/usr/share/sqlninja/apps/nc.exe
/usr/share/wfuzz/wordlist/fuzzdb/web-backdoors/exe/nc.exe
/usr/share/windows-binaries/nc.exe
```

14. Copy nc.exe from the /usr/share/windows-binaries directory into your home folder.
cp /usr/share/windows-binaries/nc.exe ~

```
root@kali:~# cp /usr/share/windows-binaries/nc.exe ~
```

15. Transfer nc.exe from Kali to Debian using SCP.
    scp nc.exe student@<ipaddress>:~

```
root@kali:~# scp nc.exe student@192.168.21.21:~
student@192.168.21.21's password:
nc.exe                                        100%   58KB  58.0KB/s   00:00
```

16. Go ahead and copy nc.exe onto the Windows share on your own.

sudo scp nc.exe root@<DebianIP>:/mnt

17. Verify that the files, nc.exe and ca_setup.exe, are on W2K3-XXX\Share. You'll need them later on this week!