Linux Review

This is the intellectual property of Professor Hands at Purdue University

Linux Commands

In this guide, Kali Linux is our primary pentesting OS. The following are helpful Linux commands that are very useful:

1. **File System**:

ls — list items in current directory
ls -l — list items in current directory and show in long format to see permissions, size, and modification date
ls -a — list all items in current directory, including hidden files
ls -F — list all items in current directory and show directories with a slash and executables with a star
ls dir — list all items in directory dir
cd dir — change directory to dir
cd .. — go up one directory
cd / — go to the root directory
cd ~ — go to to your home directory
cd - — go to the last directory you were just in
pwd — show present working directory
mkdir dir — make directory dir
rm file — remove file
rm -r dir — remove directory dir recursively
cp file1 file2 — copy file1 to file2
cp -r dir1 dir2 — copy directory dir1 to dir2 recursively
mv file1 file2 — move (rename) file1 to file2
ln -s file link — create symbolic link to file
touch file — create or update file
cat file — output the contents of file
less file — view file with page navigation
head file — output the first 10 lines of file
tail file — output the last 10 lines of file
tail -f file — output the contents of file as it grows, starting with the last 10 lines
vim file — edit file
alias name 'command' — create an alias for a command
tree dir – print a tree diagram of file structure starting from directory dir

2. **System**:

shutdown — shut down machine
reboot — restart machine
date — show the current date and time
finger user — display information about user
man command — show the manual for command
df — show disk usage
du — show directory space usage
free — show memory and swap usage
whereis app — show possible locations of app
which app — show which app will be run by default

3. **Process Management**:

ps — display your currently active processes
ps aux – display all running processes on the system
top — display all running processes with continuous updates
kill pid — kill process id pid
kill -9 pid — force kill process id pid

4. **Permissions**:

ls -l — list items in current directory and show permissions
ls –alh – list all items in current directory, including hidden files, in long format, with human readable file sizes
chmod ugo file — change permissions of file to ugo - u is the user's permissions, g is the group's permissions, and o is everyone else's permissions. The values of u, g, and o can be any number between 0 and 7.
7 — full permissions
6 — read and write only
5 — read and execute only
4 — read only
3 — write and execute only
2 — write only
1 — execute only
0 — no permissions
chmod 600 file — you can read and write - good for files
chmod 700 file — you can read, write, and execute - good for scripts
chmod 644 file — you can read and write, and everyone else can only read - good for web pages
chmod 755 file — you can read, write, and execute, and everyone else can read and execute - good for programs that you want to share

chown user:group file – change the ownership of file to the user and group listed
addgroup groupname – create a new group by the name of groupname
sudo command – execute command with root privilege
sudo su – obtain a shell as the root user, with user id (uid) of zero and group id (gid) of zero
su username – obtain a shell as username, with that user’s uid and gid
chgrp groupname – operate as current user under groupname membership
whoami — who you are logged in as

5. **Networking**:

wget file — download a file
curl file — download a file
scp user@host:file dir — secure copy a file from remote server to the dir directory on your machine
scp file user@host:dir — secure copy a file from your machine to the dir directory on a remote server
scp -r user@host:dir dir — secure copy the directory dir from remote server to the directory dir on your machine
ssh user@host — connect to host as user
ssh -p port user@host — connect to host on port as user
ssh-copy-id user@host — add your key to host for user to enable a keyed or passwordless login
ping host — ping host and output results
whois domain — get information for domain
dig domain — get DNS information for domain
dig -x host — reverse lookup host
lsof -i tcp:1337 — list all processes running on port 1337

6. **Searching**:

grep pattern files — search for pattern in files
grep -r pattern dir — search recursively for pattern in dir
grep -rn pattern dir — search recursively for pattern in dir and show the line number found
grep -r pattern dir --include='*.ext — search recursively for pattern in dir and only search in files with .ext extension
command | grep pattern — search for pattern in the output of command
find file — find all instances of file in real system
locate file — find all instances of file using indexed database built from the updatedb command. Much faster than find
sed -i 's/day/night/g' file — find all occurrences of day in a file and replace them with night - s means substitute and g means global - sed also supports regular expressions

7. **Compression**:

tar cf file.tar files — create a tar (tape archive) named file.tar containing files
tar xf file.tar — extract the files from file.tar
tar czf file.tar.gz files — create a tar with Gzip compression
tar xzf file.tar.gz — extract a tar using Gzip
gzip file — compresses file and renames it to file.gz
gzip -d file.gz — decompresses file.gz back to file

8. **Shortcuts**:

ctrl+a — move cursor to beginning of line
ctrl+f — move cursor to end of line
alt+f — move cursor forward 1 word
alt+b — move cursor backward 1 word

Common Network Configuration Commands

1. `ifconfig`
2. `iwconfig` (wireless extensions)
3. `ping <ip_address>`
4. `arp -a` (Will show IP addresses and the corresponding MAC address)
5. `netstat -ano` (Will show active connections running on the machine)
6. `route` (Will print the IP Routing Table)

Common Commands for Installing and Updating OS/Tools

1. `apt update && apt upgrade`
2. `apt install python-pip` (for pip)
3. `apt install python3-pip` (for pip3)
4. `git clone <github resource link>` (For github files)
5. Download the Impacket tool using "`git clone https://github.com/SecureAuthCorp/impacket.git`"

This is the intellectual property of Professor Hands at Purdue University

---