Introduction to Linux

Overview

Windows is the predominant fixed (not mobile) operating system worldwide. While Microsoft rule the desktop, Linux/Unix is by far the most commonly deployed operating system globally, mobile phones (IOS & Android) make use of a UNIX or Linux kernel, and embedded devices such as routers, toasters, fitness tracking devices, vehicles, traffic light systems, etc.

In the security world Linux is the operating system for penetration testing / ethical hacking. From a forensic perspective, many of the emerging challenges centre on mobile devices, the Internet of Things and the Cloud, all of which rely heavily of UNIX/Linux. For these reasons, a good understanding of Linux is a fundamental skill that you will develop in this unit.

Resources

- Please bring a large USB storage device to next week's lab session, ideally 32GB+ USB 3.0 (100MB/s) See Moodle link for details.
- The Red Team Field Manual is a useful resource, it is available online and in paper format. See Moodle link for details.

Important Notes

- Labs will be run using Linux
- **Your coursework will require the use of Linux**
- Linux is free, you can download various distributions for use at home
- You can install Linux alongside your Windows operating system (dual booting), backup your computer prior to attempting this as you can easily destroy your Windows install
- Virtualisation provides a good environment in which to utilise Linux (Particularly hacking tools) as it separates your activities from real world systems. More on this next week.

Tips

- If you enter a command with no exit condition e.g. ping, press `ctrl+c` to kill the process.
- Type any command followed by `-help` to get instructions on how to use the command.
- To redirect the standard output of a command to a new file use "*command* > *file*"
- To append the standard output to an existing file use the "*command* >> *file"*
- To pipe the output of a command through another command use the pipe command "|"
- Type `q` to exit the man page.

Task 1 – Command Line Help

The command line interface exists on most UNIX/Linux devices, it is often reached via Telnet or SSH on embedded systems.

1. Boot into Linux if you haven't already
2. Open a terminal
3. Type the command "`man`" at the command line, followed by the command "`ls`", this will show the manual for the ls command
4. Read the man page, and look at the syntax used by the command and its associated arguments, there may also be examples. Note down what the command does.
5. Press "`q`" to exit the man page

Task 2 - Navigation & File Handling

Navigation without a GUI can be daunting; however, most security tools use the command line interface, and once you become familiar it is much faster than clicking, dragging, etc.

1. Use the "`ls`" command to list the files and directories in your home directory.
2. Create a file in your home directory that contains your name, Refer to the nano documentation below;
    a. http://tinyurl.com/7djaprl
3. Create a directory in your home directory using the "`mkdir`" command, refer to the man page for "`mkdir`" for more information.
4. Research the Linux command to move a file, then move the file you created in your home directory to the directory you just created
5. Research the Linux command to change directory, then change into the directory containing the file you created
6. List the files in the directory in the long format, showing all entries, refer to man page for "`ls`" if required.

Task 3

Auditing a computer system is all about finding information out about the system. Check out the man pages for the following commands;

```
ls, mkdir, cd, cp, rm, cat,  /sbin/ifconfig, netstat, date, ping,
who, ps, last, ,whoami, free, pwd
```

By typing "`man command`" into the terminal window. Consider how each command may be useful while auditing a system. Use each command then document each its's functionality and its purpose in the context of auditing the system.

Task 4

Before completing task 5, take 10 minutes out to enjoy some of these fun Linux Easter eggs (Emacs games are particularly retro and entertaining ☺);

http://tinyurl.com/kc2ng6b

Research and identify another Easter egg on the Linux system.

Task 5 – Code Academy Training

Follow the training guide at the link below:

http://tinyurl.com/pjkuxc7

Summary

The command line interface is a powerful way of interacting with the operating system. Many standard command line tools can be used to find out information about a computer system. Through your course you will use both standard and specialist Linux based tools that require experience of using the command line interface.