**Getting Started with Kali**

**Getting started with Kali**

Welcome to Hakin9’s first Advanced Offensive Security Training! Over the next ten months, you will learn the how to attack various types of information technology infrastructure, including Web Applications, and even develop our own exploits. Along the way, we will learn each of the steps we need to take to prepare for such an attack, including reconnaissance and scripting.

Before we begin on this long journey, we first need to put into place some stepping stones to get us there. In this first module, we will introduce you to Offensive Security’s hacking distribution, Kali Linux. Kali Linux is Offensive Security’s latest hacking/penetration testing platform, having replaced Offensive Security’s widely known and used BackTrack. Unlike Backtrack, Kali is built on Debian Linux rather than Ubuntu.

**Navigating Kali**

As we will be using Kali as our primary means of attacking IT assets over the next 10 months, it is important that we have an introduction and tour of Kali. For those of you who are new to Kali, please make certain that you spend adequate time familiarizing yourself with it and Linux, as it will pay dividends in the long run in this course and your career as a penetration tester. For those of you who already have significant experience with Kali and Linux, consider this a review and bear with us for just  a bit.

Kali is a Debian distribution of Linux with a GNOME interface by default (if you are more comfortable with KDE or other interface, you can replace it, but I will be using the default interface in this course), built by  Offensive Security and for offensive security. It has hundreds of tools built-in and is designed for hacking.  Most of the tools we want to access and use can be found under the Kali Linux tab under the Applications tab at the top of the screen. Let’s take a look at those.

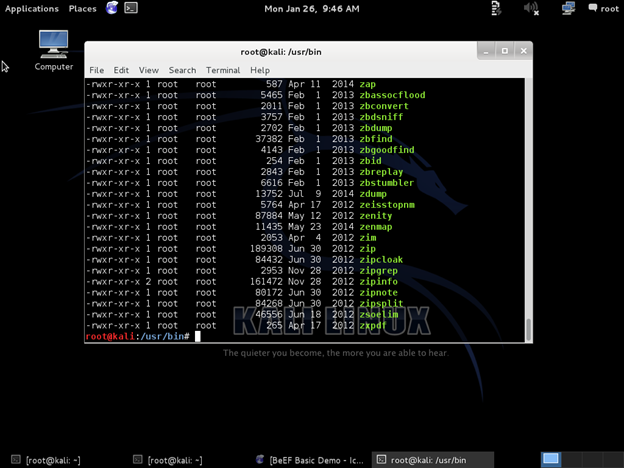
As you can see in the screenshot above, when I click on the Applications tab at the top of the screen, it pulls down a list of choices and about mid-way down, we can see the Kali Linux tab. When we click on it, it expands to numerous categories of hacking tools. Hovering the mouse over any of those categories will reveal the tools available to us in each of those areas.

We can also select Top 10 Security Tools and it will reveal some very common and effective security/hacking tools. These are:

* + aircrack-ng
  + burpsuite
  + hydra
  + john
  + maltego
  + metasploit framework
  + nmap
  + owasp-zap
  + sqlmap
  + wireshark

One can quibble over whether these are the Top 10 security tools, but they are ALL great tools and we will be using each of them in this course.

The tools will generally be run from the CLI or command line interface. Unlike earlier versions of Backtrack and other hacking distributions, Offensive Security has placed all the applications in the /usr/bin directory and since this directory is in our PATH variable, these applications can be run from any directory,  making using Kali a bit simpler than BackTrack or other security distributions. If we navigate to /usr/bin and type ls -l, we can see displayed all of the applications available to us.



For those new to Linux and Kali, there are numerous commands that are useful. Probably the most important initially are the locate and find commands. Locate enables us to search through a database maintained by the operating system for the name of a particular file. So, if we were looking for the apache2.conf file, we could type

kali > locate apache2.conf

The locate command is fast and easy, but it can only find files that have been there at least 24 hours as the database is updated overnight on most systems. A file that you created a couple of hours ago will not appear in the database until tomorrow.

While the locate command is fast, the find command is far more powerful. It enables us to find files by attributes and define where to look for them. For instance, if I wanted to find the same apache2.conf file, I could tell it to start looking in the **/etc** directory and look for a file (-type f) with the name (-name) **apache2.conf**

kali > find /etc -type f -name apache2.conf

Where:

**/etc** is the directory to search in

**-type f** tells it to search for  a file

**-name** tells find to search by name

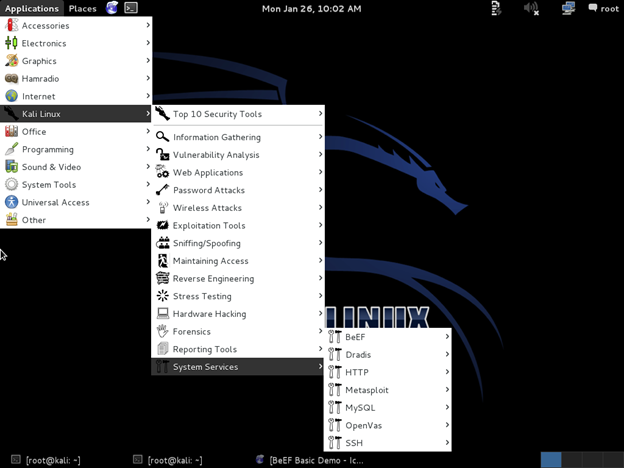
**apache2.conf** is the name of the file to search for

https://hakin9.org/wp-content/uploads/2015/02/5e194783081a7e5e5f1a652956774e9d.png

After running this command, it comes back and tells us that **apache2.conf** is in the **/etc/apache2** directory.  The find command is a very powerful Linux command with almost innumerable switches and options to help us find files based upon various attributes, such as ownership, time, size,  permissions, etc. It would be worth your time to further explore this command, but it is beyond the scope of our course.

**Kali Linux Services**

Kali has a number of built-in services that will be useful to our attacks. Probably most importantly will be the apache web server, but also SSH, TFTP, FTP and others. Many of these services can be started, stopped and restarted from the GUI interface.



As you can see from the screenshot above, I can find the GUI interface for these services by going to Applications then Kali Linux and then System Services. When I hover over System Services it opens a menu of services. This is NOT a complete list of services, but only those that can be started and stopped via the GUI.

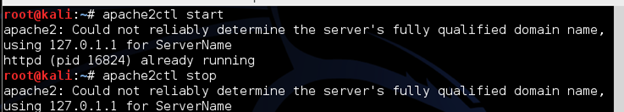
Other services are available, but must be started via the command line interface (CLI). We can start and stop any service by typing:

kali > service <name of service><action:start,stop,restart>

So, if I wanted to start the apache web server via the command line, it would be:

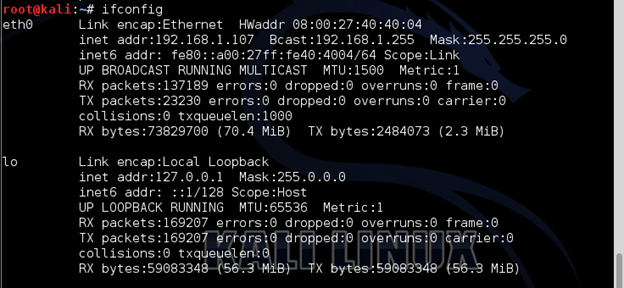
kali > service apache2 start

In addition, apache2 has a control script named apache2ctl. We can use it to start and stop the apache web server.



**Networking in Kali**

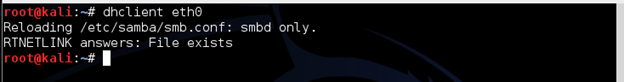
Throughout this course, we will need to configure and reconfigure our network for optimal hacking. To do so, we will need to be familiar with a few  commands in Linux. The first and probably most important is ifconfig.  It is very similar to windows ipconfig as it will reveal the requisite networking and interface information.



**DHCP**

To acquire DHCP assigned IP address, simply use the dhclient command with the name of the interface, in this case eth0

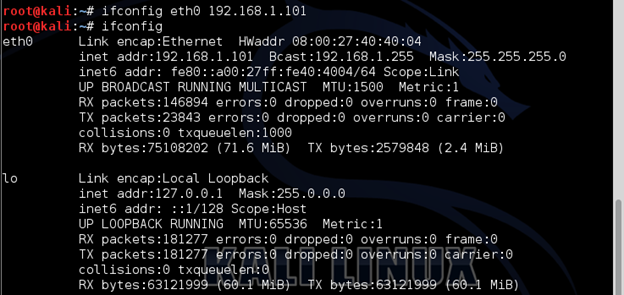
kali > dhclient eth0



**Setting a Static IP**

To set a static IP, you can use ifconfig as follows:

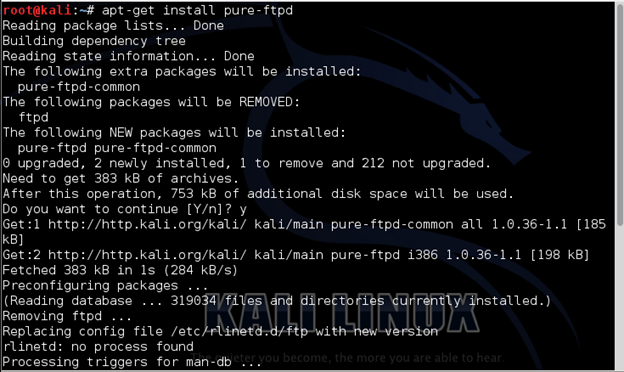
kali > ifconfig eth0 <IP address>



**FTP**

Next, we want to install the pure-ftpd server. I prefer the pure-ftp server and it is in our Kali repository, so we can install it by typing:

kali > apt-get install pure-ftpd



**TFTP**

We will need a trivial FTP server for some of our labs, so let’s start one now. Built into this Kali Linux is the advanced TFTP server or atftpd. We can start it by typing:

kali> atftpd --daemon --port 69 /tmp

Where:

**–daemon** tells the service to run in the background

**–port** tells atftpd to listen on port 69

**/tmp** tells the service to use the /tmp directory as a source of files

https://hakin9.org/wp-content/uploads/2015/02/667e74e0a598ef7af68a9438f9a5922c.png

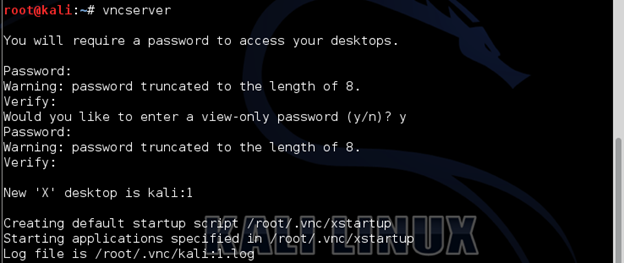
To test to make certain the atftpd daemon is running, we can use the netstat command and pipe it to grep filtering it for atftpd. As you can see in the screenshot above, we found it running on port 69.

**VNC Server**

Last, let’s test the vncserver built into Kali. We can activate it by typing:

kali> vncserver

Note that the first time you activate VNC Server, it will prompt you for a password. Provide it a password up to 8 characters and remember it, as you will need it again later.



**Exercises for Module 1, Lesson 1:**

1. Log on to Kali and check what interfaces you have. This will vary dependent upon your setup.
2. Select the wired interface (eth0) and set a static IP address such as 192.168.1.101.
3. Re-set your IP to a DHCP assigned IP and check Internet connectivity.
4. Start and stop your SSH, Apache, FTP, TFTP and VNC servers using the CLI and/or the GUI, if available.