**Linux for hackers 1**

What is ethical hacking ?

1. Penetration testing
2. Military and Espionage(cyber warfare, military files etc..)

Why hackers use Linux ?

It is open source(modify source code), Transparent(OS parts), offers granular control.

* Most hacking tools are written in Linux
* Future belongs to Linux (2/3 of the web servers in the market are running on Linux).

>90% of hacking tools are written for linux

Linux = stability, reliability and robustness

* Virtualization is dominated by Linux, VMWare and Citrix are built on Linux Kernel.
* 80% mobile devices run(ios Unix, Android Linux)

\*\***Linus Trovalds** developed linux in 1991 as open source alternative to UNIX.

* **Kali linux** was developed by **offensive security** as a hacking OS built on a distribution called Debian. There are many distributions of Linux available.
* Ubuntu is a desktop distribution of Linux(Ubuntu is also Debian). RedHat, CentOS, Mint, Arch and SUSE are other distros.
* **Kernel** is the heart of the operating system that controls CPU, RAM and so on..
* Kali linux was designed for penetration testers and hackers, comes with significant hacking tools.

**Virtual Machines**

* Installing VMWare or Virtualbox and creating VM(Kali Linux), don’t allocate >25% of your RAM(20-25GM minimum HD space)
* Graphical install 🡪 Enter host name(Kali) 🡪 choose password
* Guided : use entire disk, kali will detect your hard drives and detect your hard drives and setup a partitioner automatically🡪 YES and continue 🡪 GRUB(YES) 🡪 Enter device manually 🡪 Kali login screen.

**OR**

Download the Kali VM from [Get Kali | Kali Linux](https://www.kali.org/get-kali/#kali-virtual-machines) select the VMWare or Virtualbox and appropriate bit version 🡪 create a VM in your hypervisor(VMWare or Virtualbox) and call the downloaded VM.

If you need assistance please refer to this video : [How To Install Kali Linux in VirtualBox (2021) | Kali Linux 2021.2 - YouTube](https://www.youtube.com/watch?v=irGTD6jmYhc)

**Welcome to Hacking**

**\*\*Basics**

1. **Binaries:** similar to .exe files on windows, binaries are the files that can be executed. These reside in /usr/bin or /usr/sbin and include utilities ps,cat,ls and cd ….
2. **Case sensitivity:** Unlike windows linux is case sensitive.
3. **Directory:** Way of organizing files, usually hierarchical manner.
4. **Home:** /home for each user.
5. **Kali** is preinstalled with 100’s of tools: to know more follow this link [Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution](https://www.kali.org/)
6. **Root:** Super user (#)
7. **Script:** series of commands run in an interpretive environment that converts each line to source code.

* **Python** is popular interpreter/compiler among hackers(python, perl & ruby etc..)

1. **Shell:** This is a environment and interpreter for running commands in linux that converts each line to source code.

* **BASH** bourne-again shell, (C-shell, Z-shell are other examples)

1. **Terminal:** Command line interface (CLI). BASH/SHELL is a command line interpreter (**echo $SHELL)**
2. **Console:** Physical machine keyboard/monitor

* To change password – **passwd**

\*\* **The Linux filesystem (logical filesystem)** **– ‘/’ root**

**A picture containing text, whiteboard

Description automatically generated**

More about file system here : [the Linux File System explained in 1,233 seconds // Linux for Hackers // EP 2 - YouTube](https://www.youtube.com/watch?v=A3G-3hp88mo)

**\*\*Basic Commands**

1. pwd –
2. whoami
3. cd /etc & pwd
4. cd .. (one level up) cd .. .. (two level up) cd .. .. ..(you guessed it!)
5. ls – list contents. In windows it is **dir**
6. ls -l ( permissions, last modified etc..)
7. ls -la (-a hidden files) the . ones
8. aircrack-ng –help(best wireless cracking tool). Try -h as well. check the manual page(man)
9. nmap –help
10. **locate aircrack-ng** : finding stuff

* locate used db and it updates once a day, so if a file has been created few hours ago it won’t find it.

1. Finding binaries – **whereis aircrack-ng**
2. Finding binaries in the PATH variable with **which** (**which aircrack-ng**)
3. Find syntax – find directory options expression

Ex: find / -type f -name apache2 [ / - directory, -type f (options), -name (expression)]

find /etc -type f -name apache2

find /etc -type f -name apache2.\*

-----------------------------

Processes:

**ps** – to view the processes

**ps aux | grep apache2** – will list the processes running for all users and pipe(|) output to input for the grep command and here we are trying to grab the apache2 process from all the processes.

**\*\*Modifying files and directories**

1. **cat > hacking skills**

hacking is the most valuable skill of 21st century

1. **cat >> hacking skills**

Everyone should learn to hack

1. **touch** newfile – touch is used to create a new file
2. **mkdir** newdir – mkdir is used to create a new directory (cd to navigate into the newly created folder)
3. **touch** oldfile ; **cp** oldfile /root/newdir/newfile – check if the file is copied
4. **mv** newfile newfile2 – to rename file : try ls to check if it is renamed
5. **rm** newfile – to remove the file
6. **rm -r** newdir – to remove the newdir (empty dir only)

**Exercise:**

1. Use ls command & explore the directory structure of linux. Try cd and pwd
2. Try whoami
3. Locate and find wordlists that can be used for password cracking
4. cat to create new file & append to that file ‘>’ & ‘>>’
5. create a new directory called hackerdirectory and create a newfile(named ‘hackerfile’) in that directory. Now copy the hackerfile to your /root directory & rename it to ‘secretfile’.