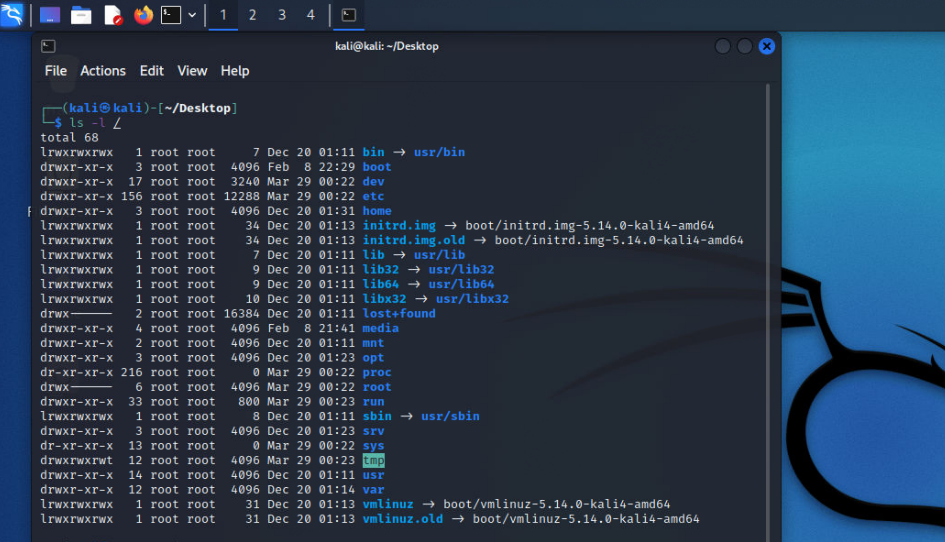
Linux Forensics

Part I: Linux File Structure and Important Files

**Step-1**

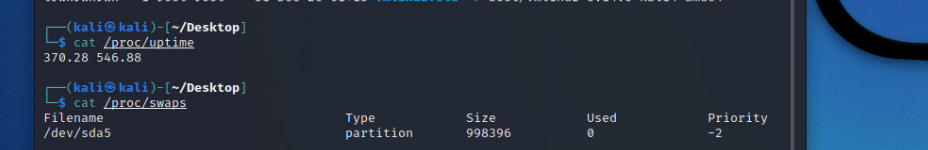
One of the most interesting parts of kali linux is the way their Files are structured. There is a main folder called **“/”** with-in which all of the subfolders exist.”**/home**” is for user personal files,”**/etc.**” has system and configuration files,”**/boot**” contains boot and kernel files, etc.



If you go to the root folder **“/”** and then use the “**ls -l**” command it is going to display all of the subfolders for you.

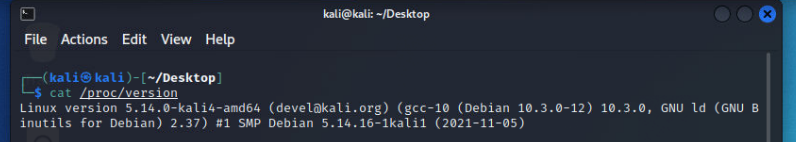
**Step-2**

Kali linux has some important files that contains useful information.” **/etc/apt/sources.list**”contains sources list of Debian packages.”**/etc/passwd**” has local user account information.”**/etc/shadow**” contain local user password (**hash form**),”**/proc/crypto**”List all ciphers etc.



”**/proc/uptime**” Returns two values; first is the total number of seconds the system has been switched on. The second is the sum of the idle time of all the processors

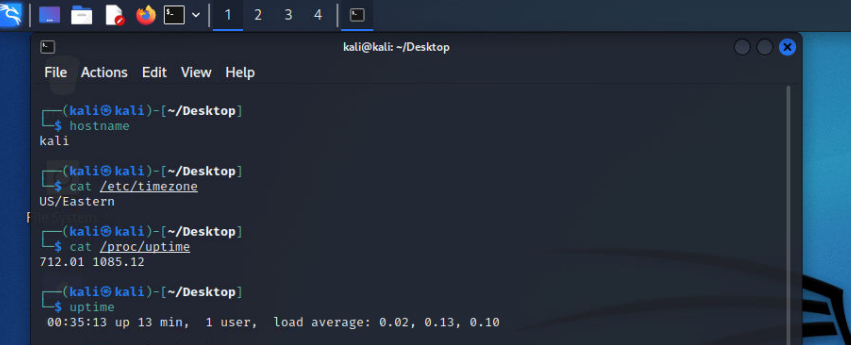
“**/proc/swaps**” Contains information about system swap space.



Part II: Collecting Basic Volatile Information

**Step-3**

Here we are using hostname to check our profile name and read the time zone and the system uptime



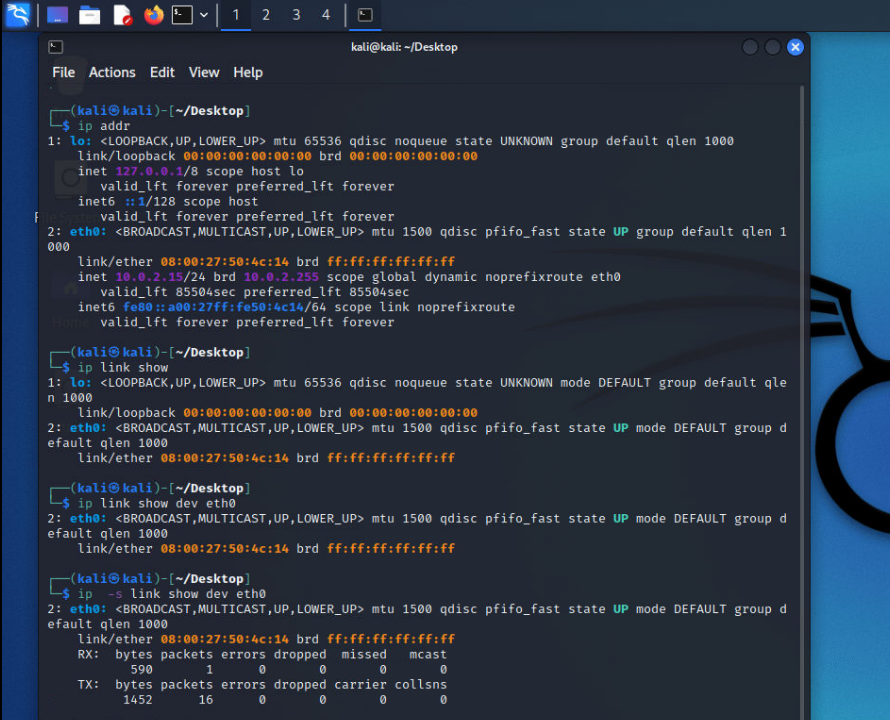
**Step-4**

In this part we are collecting network information.

“**Ip addr**” is used to display id address of all the interfaces

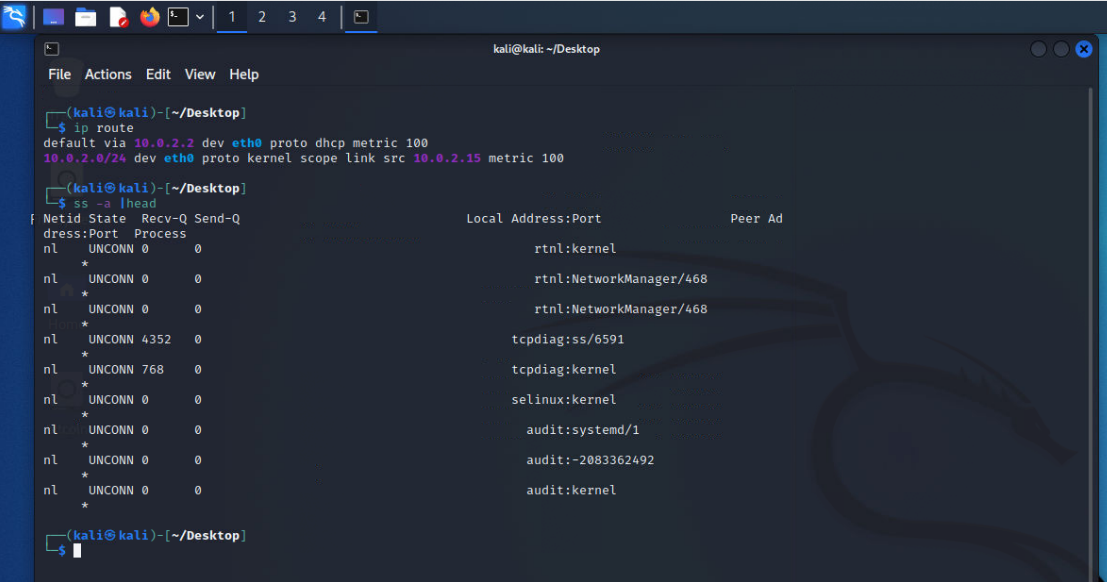
“**Ip link show**” is used to list down all of the interfaces

“**Ip link show dev (interface-name)**” shows information related to the specific interface



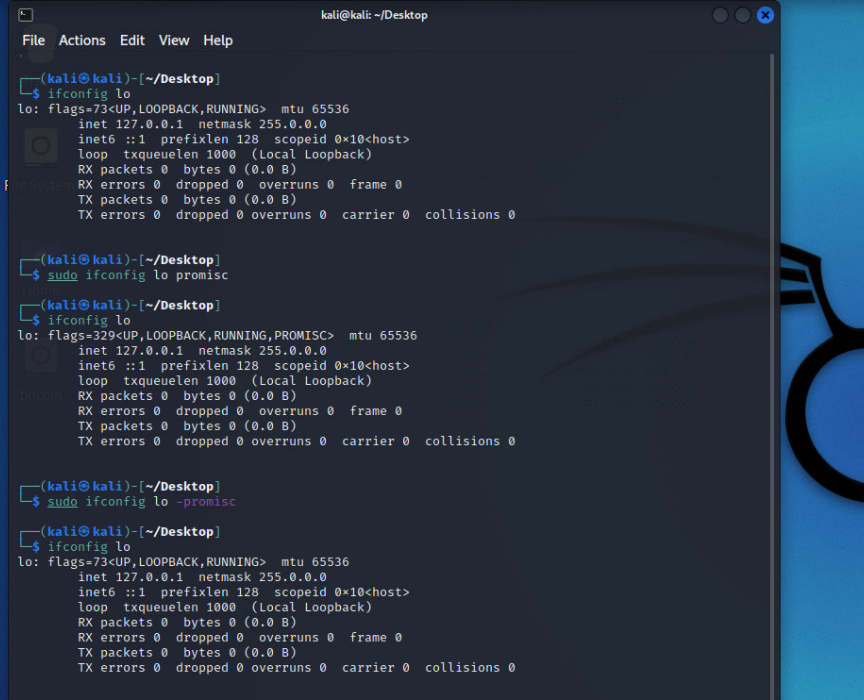
“Ip route default” is used to show the default route or the gateway

“**Ss -a | head**” Display socket statistics



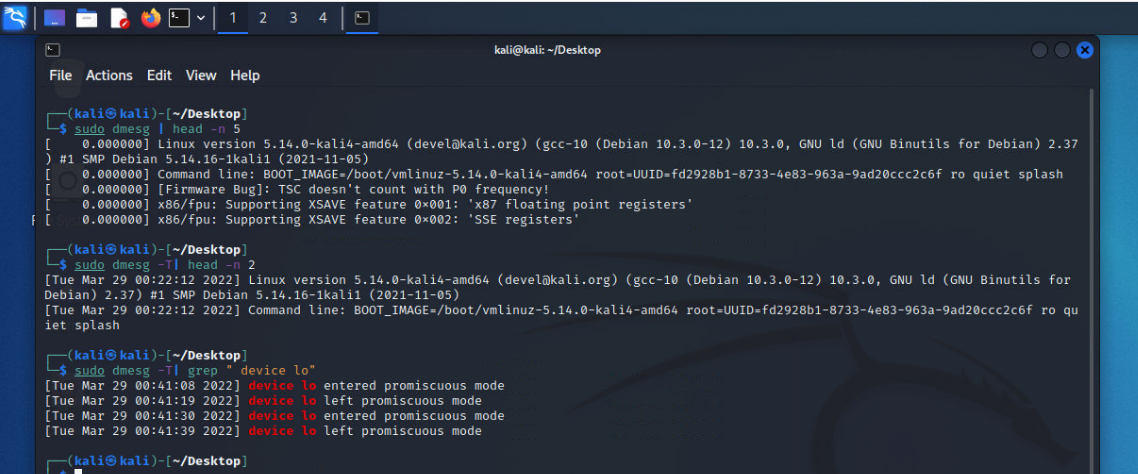
**Step-5**

Here we set our interface in **promiscuous** **mode** and saw that the number of packets increases this means that they might be accepting malicious packets.



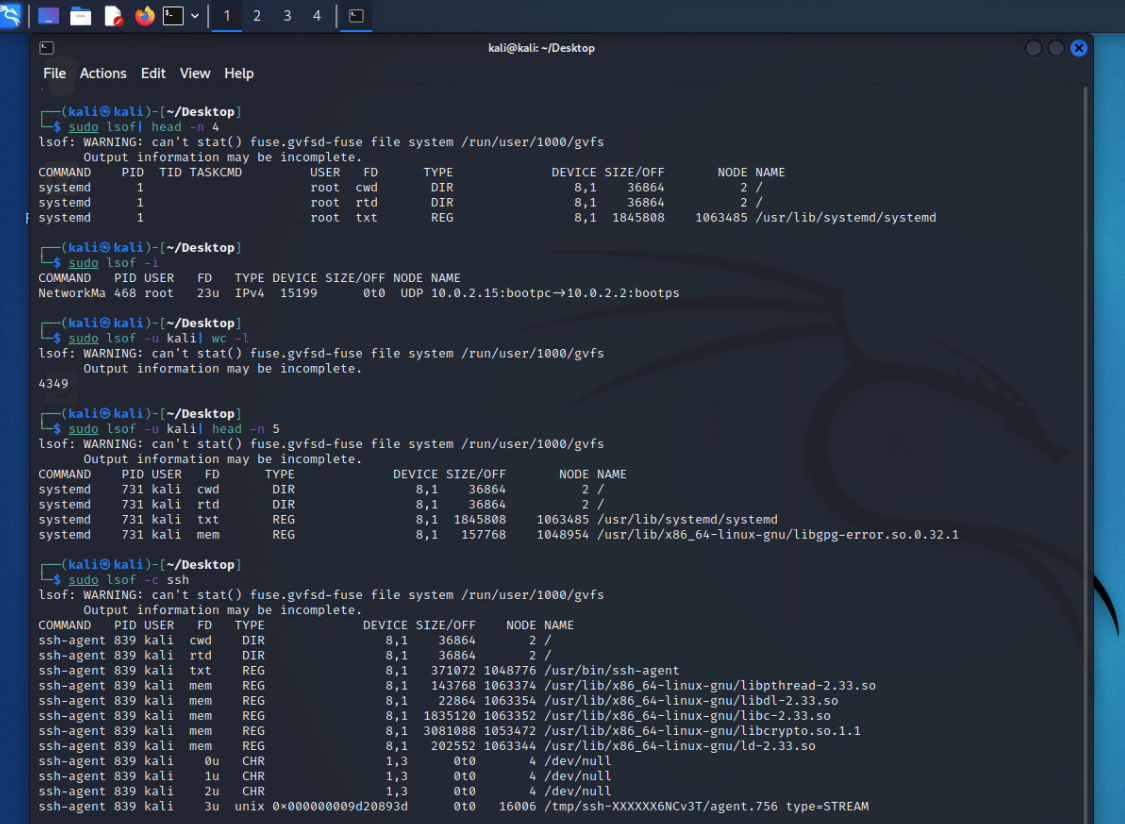
**Step-6**

The **dmesg** command is used to retrieve the Kernel messages to help investigators track actions performed on the investigated machine. This command displays all messages since the kernel is started.



**Step-7**

**Lsof** is used to see all of the open files

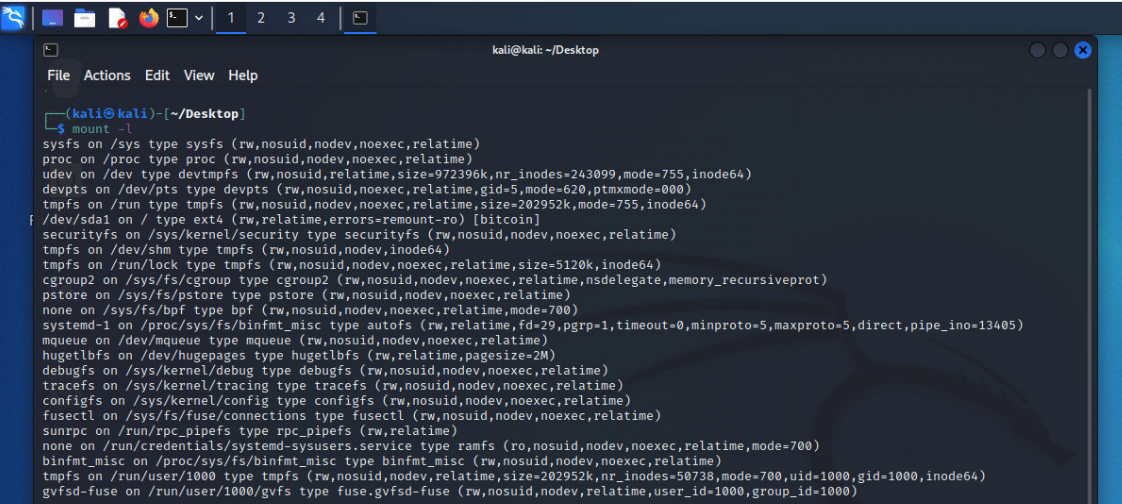


“**lsof -u <user>**” is used to display files opened by a specific user

“**lsof -c <process-name>**” Display all opened files by particular process.

**Step-8**

The command “**mount**” list the mounted file systems.



**Step-9**

“**df**” displays the amounts of free.



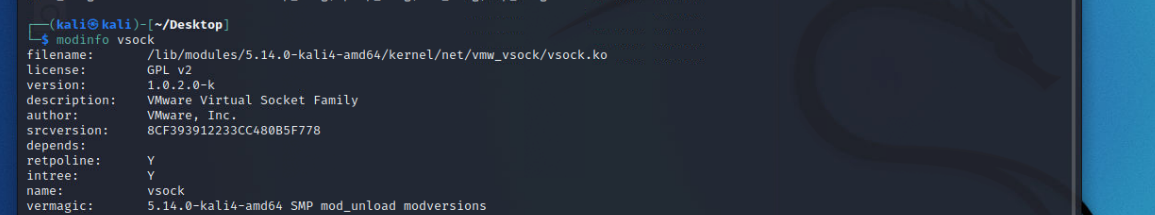
**Step-10**

To display the kernel loaded modules, use the **lsmod** command



**Step-11**

**modinfo** to display the information of a particular module



**Step-12&13**

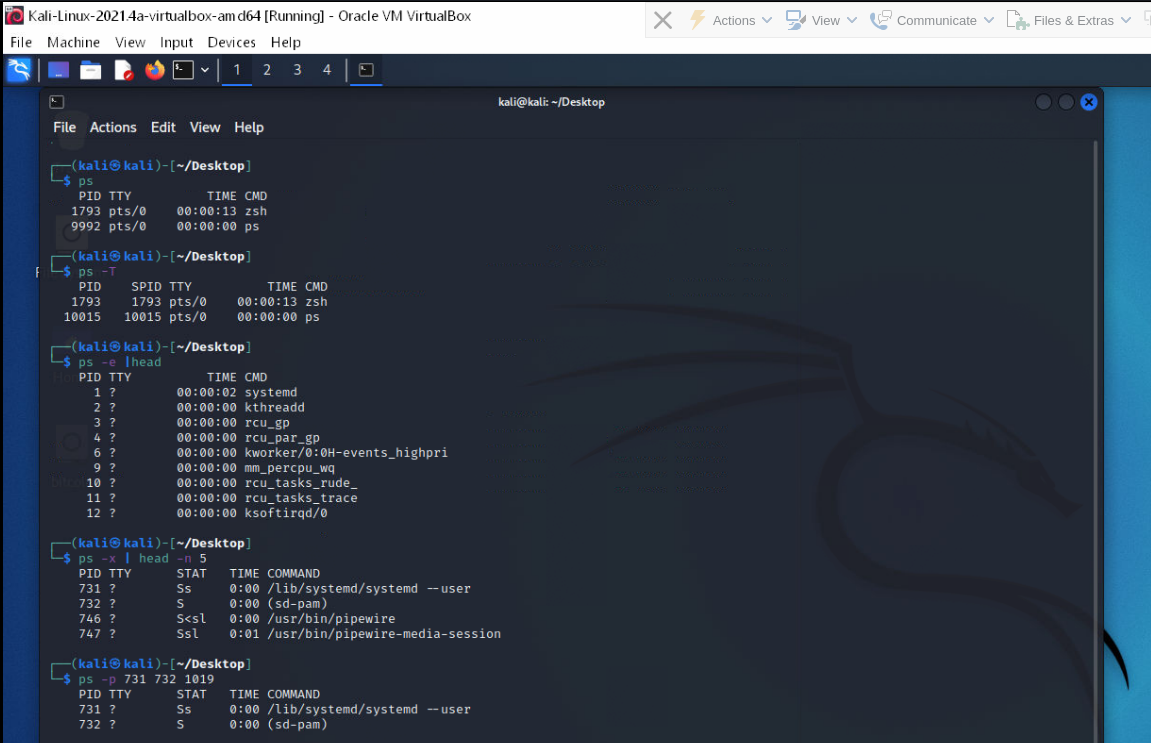
Another great command to use is “**ps**”, it is used to list down all of the process id’s

“**Ps -T**” list processes for current terminal

“**Ps -e| head**” list all processes

“**Ps -x | head -n 5**” list processes associated with current user

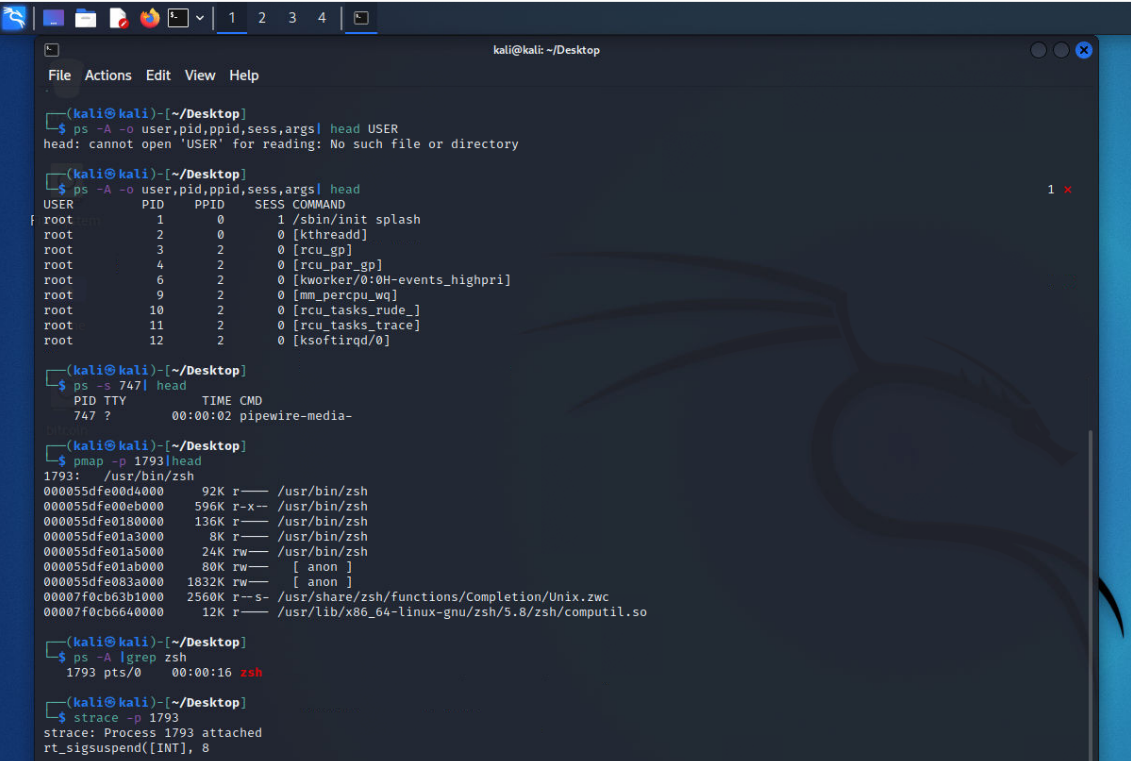
**“Ps -s <PID> | head**” list processes attributed to a particular session



**Step-14&15**

“**pmap**” is used to report on the memory map of a particular process.

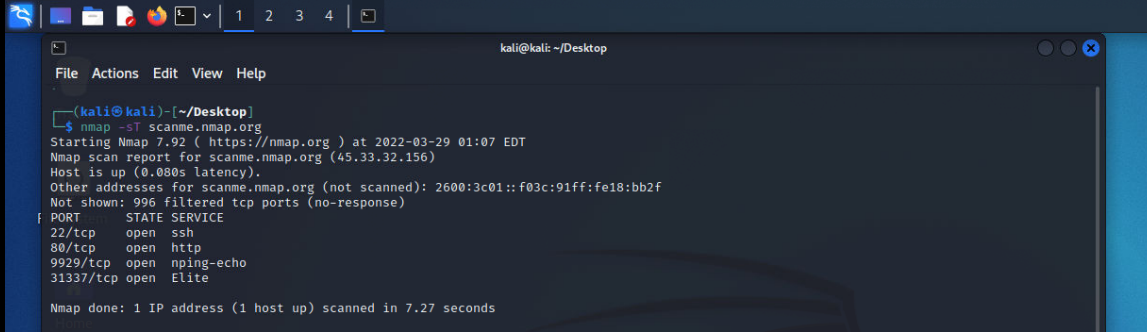
**strace** is used to trace the system calls and signals issued by a particular process.



Part III: Linux Firewall, SSH Service, and Port Scanning using nmap

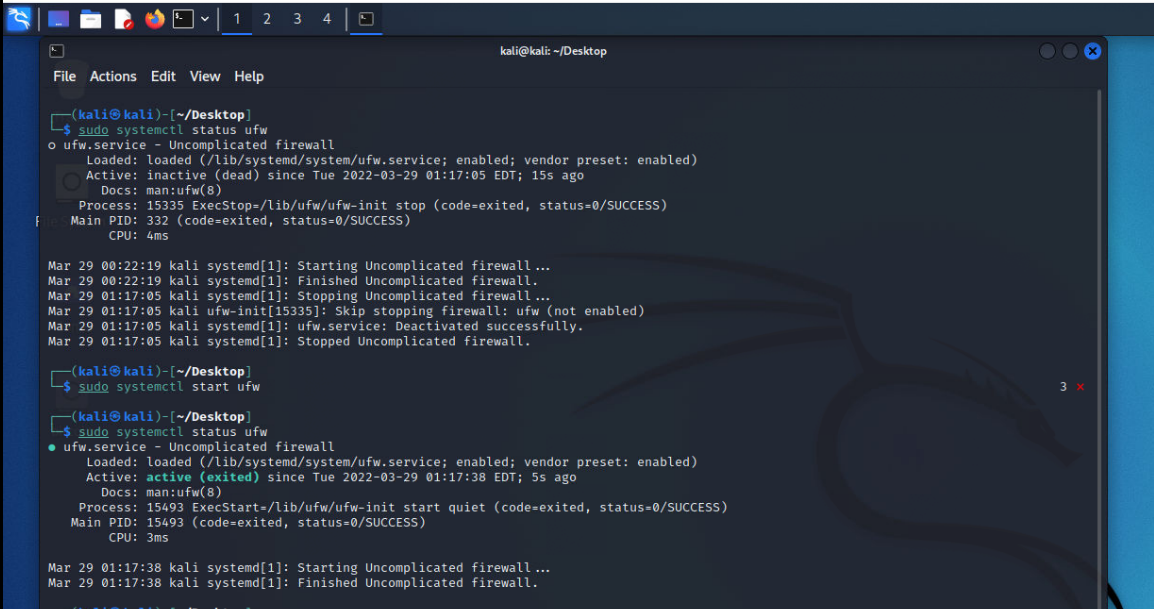
**Step-16&17**

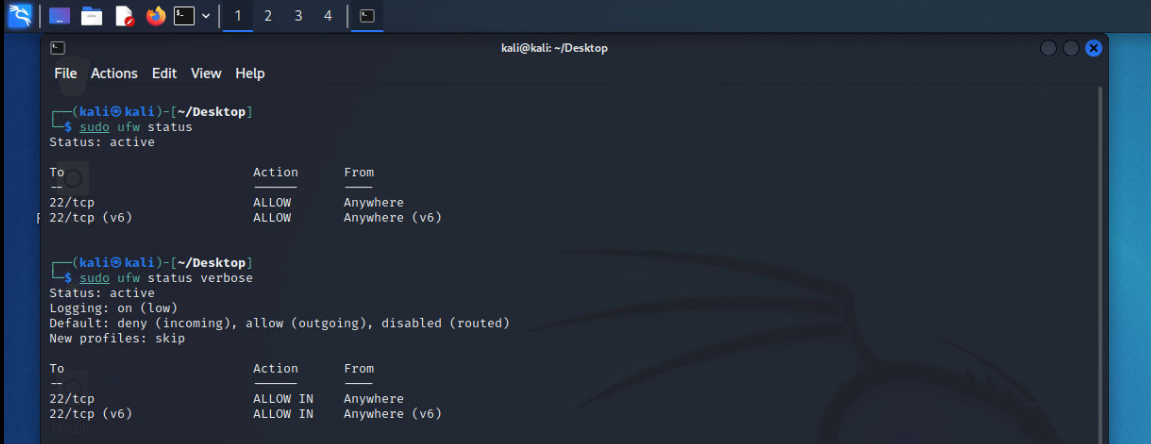
**Nmap** is a powerful tool used for port scanning

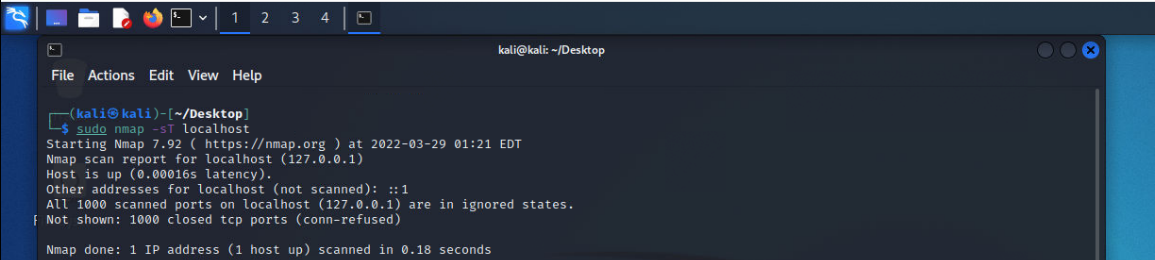


**Step-18&19**

Firewall **ufw** is used to filter the port and drop the **nmap** packets, it is a security tool that is used by many companies

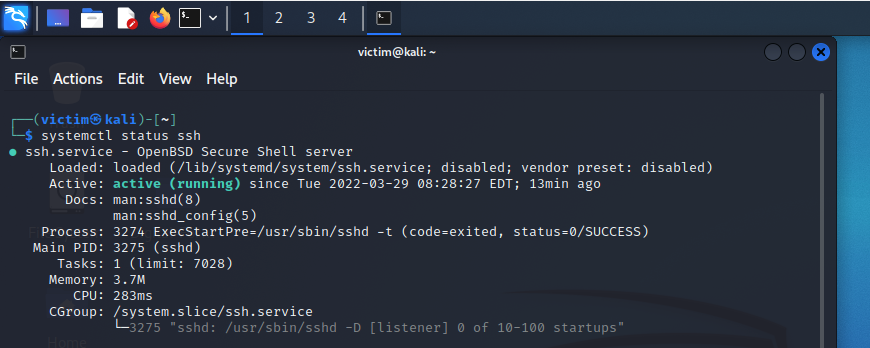




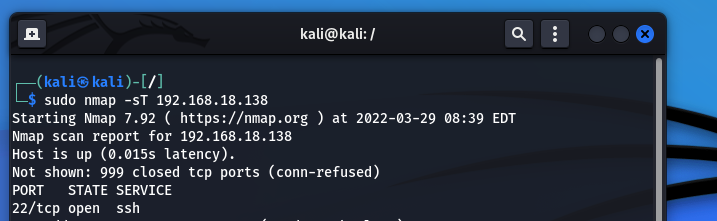


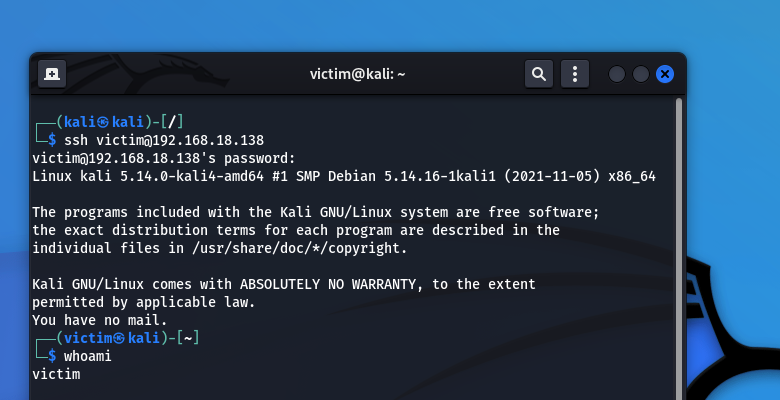
Here we are going to establish ssh connection using openssh, we have installed openssh on victim’s machine and using our machine we will connect to it.

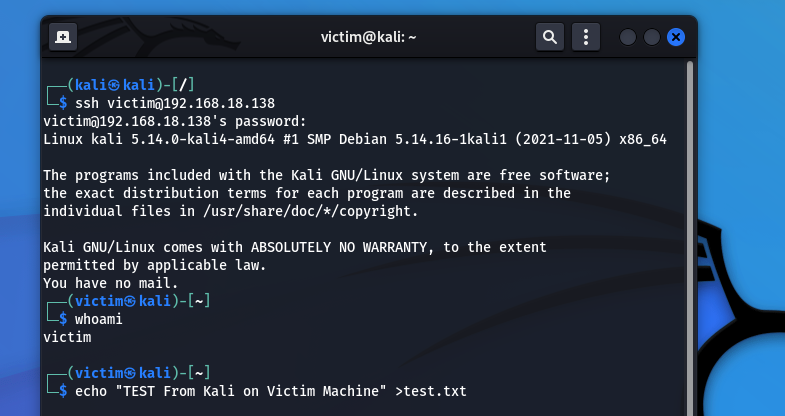
“**ssh victim@<ip>”**

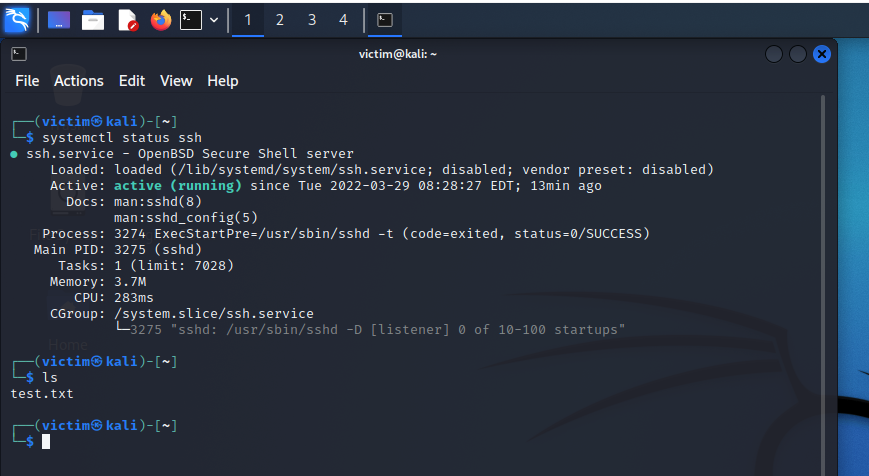


Here we have scanned the device to see if ssh port 22 is open









SUMMARY

We have learned a lot about linux from the file structure to the remote connection. In the first part we looked how the linux files are evenly structured in descending order, then we saw the important files that are used to extract useful information. In the second part we collected basic linux information such as hostname, time zone, uptime, network interface, default route, socket statistics, we also saw how dangerous is promiscuous mode is that allows malicious packets to infect the system. We also looked over the commands like dmesg, lsof, mount, df, lsmod and modinfo. Another very useful command is ps that is used to display the list of processes running. In third part we make use of firewall to block the packets to see our open ports and then we installed openssh which is used to establish secure connection between two devices. At the end we successfully connected to the victim’s machine using ssh and wrote a test.txt file remotely