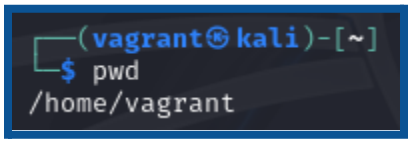
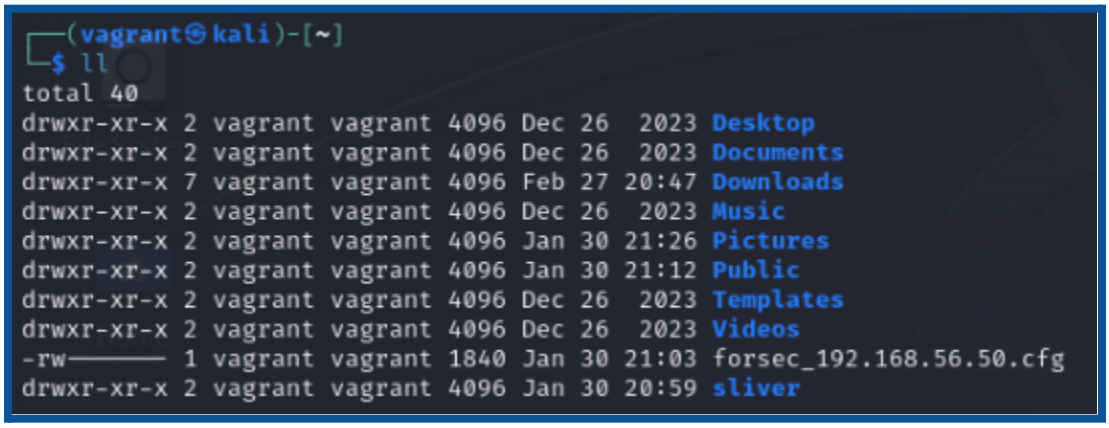
Kali Cheat Sheet

Directory Commands

- pwd (print working directory)
  - Description: Displays the directory the user is currently in
  - Usage: pwd



- ls (list)
  - Description: Displays all files and directories within the current directory
  - Usage: ls
    - ls -l OR ll (displays more information about directories/files)
  - Example:

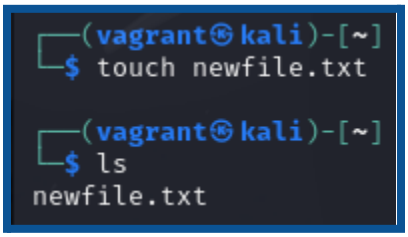


- cd (change directory)
  - Description: Changes the current working directory
  - Usage: cd Desktop
    - cd Desktop/folder1 (traverse multiple directories at once)
    - cd ~ (change to home directory)
  - Example:

- mkdir (make directory)
  - Description: creates a directory within the current directory
  - Usage: mkdir newdirectory
- rmdir (remove directory)
  - Description: removes an **empty** directory
  - Usage: rmdir newdirectory

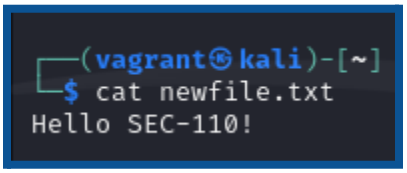
File Commands

- touch
  - Description: Creates a file without entering a text editor
  - Usage: touch newfile.txt

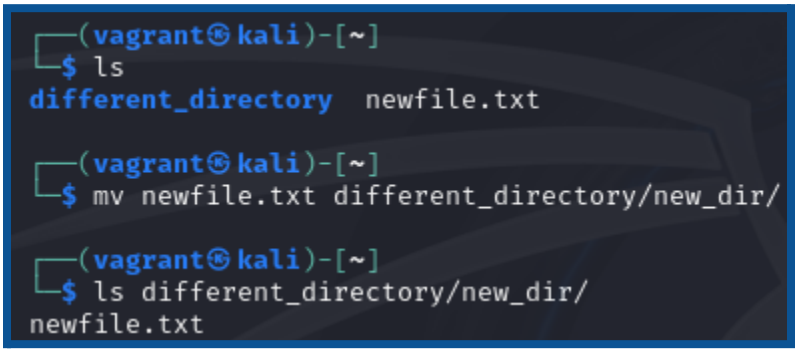


- cat (concatenate)

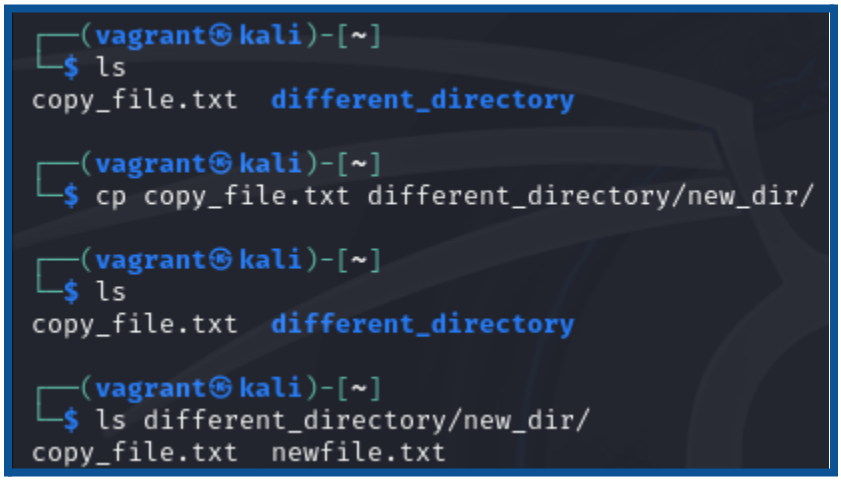
- Description: displays the contents of a given file
- Usage: cat file.txt



- mv (move)
  - Description: Moves a file to a specified location
  - Usage: mv file.txt *destination path*

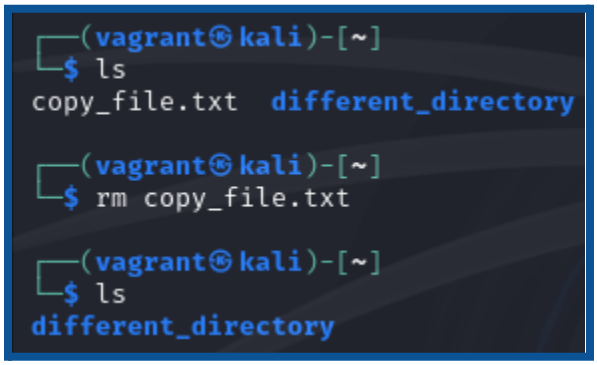


- cp (copy)
  - Description: copies a specified file from your current directory to another directory
  - Usage: cp file.txt home/Desktop

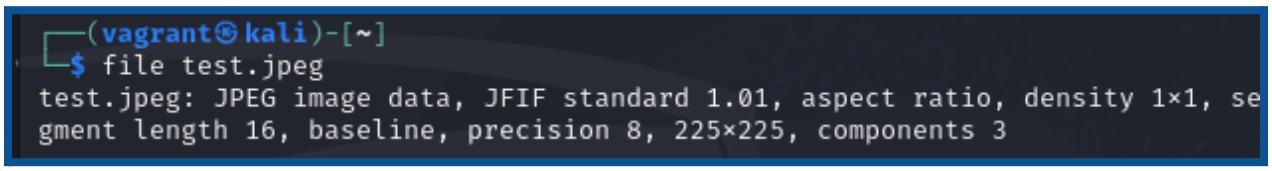


- rm (remove)
  - Description: deletes given file or directory
  - Usage: rm file.txt
    - rm newdirectory

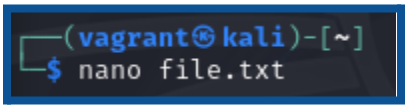
- rm newdirectory -r (recursive, removes directory, all subdirectories, and all files)

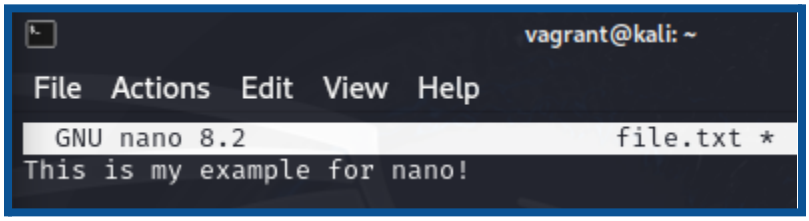


- file
  - Description: checks the file type of a specified file (txt, pdf, etc.)
  - Usage: file file.txt



- nano
  - Description: a text editor for editing files
  - Usage: nano file.txt
    - Quit and save with ctrl X and y to save to modified buffer



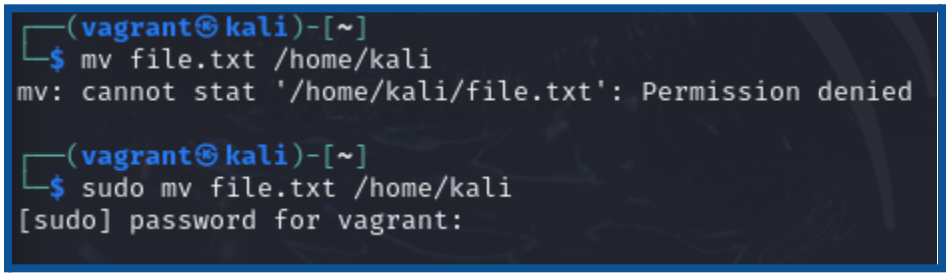


User Commands:

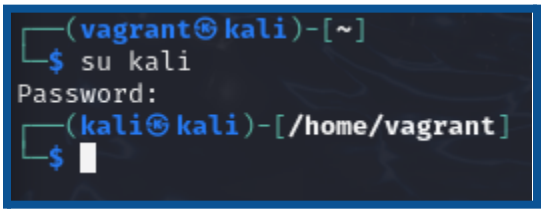
Keep in mind that making changes to the system (such as adding and removing users) will likely require sudo elevation

- whoami
  - Description: Displays the user who is currently logged in
  - Usage: whoami

- sudo
  - Description: Runs a command with administrator privilege after authentication
  - Usage: sudo command that needs administrator privileges

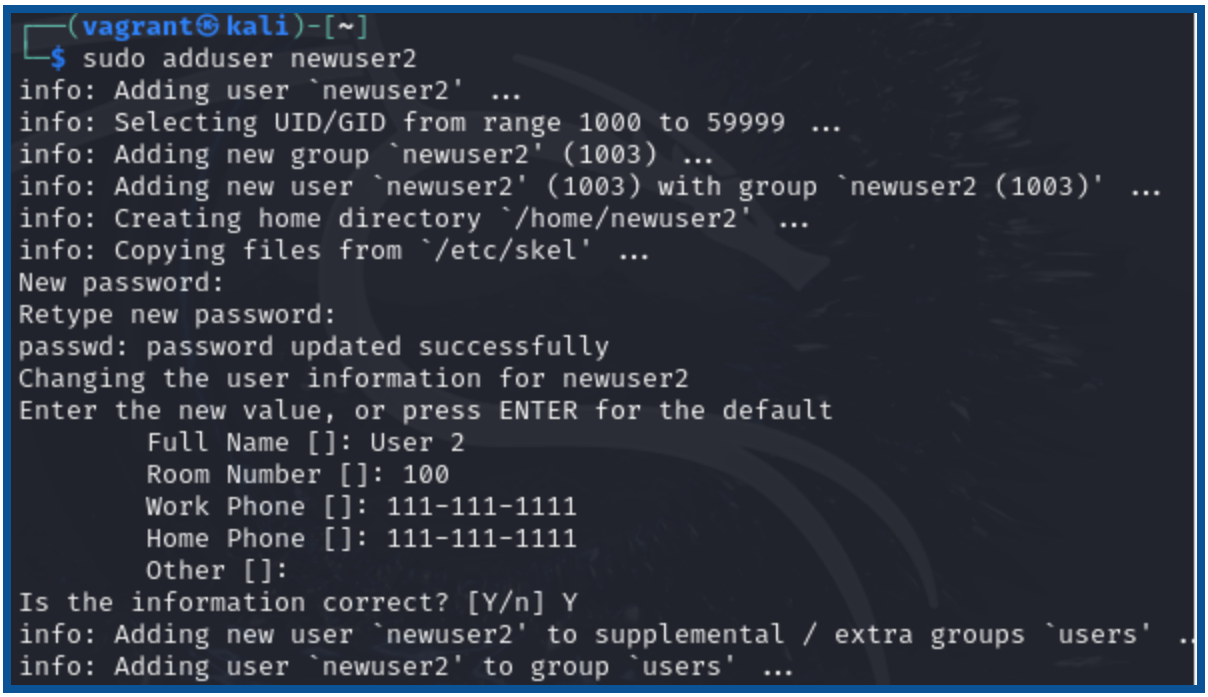


- su (substitute user)
  - Description: switch to another user within the terminal session
  - Usage: sudo su - (puts user into a **root** environment)
    - sudo su (username)

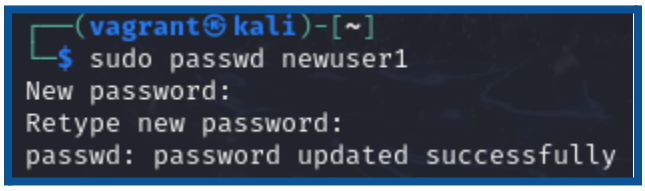


- useradd
  - Description: Low level script that creates a new account within the system
  - Usage: useradd newuser

- adduser
  - Description: Higher level script that creates a new account within the system, prompts for more user information and creates a home directory for the user.
  - Usage: adduser newuser



- passwd (password)
  - Description: sets a password for a specific user
  - Usage: passwd newuser



- userdel (user delete)
  - Description: deletes a specific user account
  - Usage: userdel newuser

Networking Commands:

- ip addr (IP address)
  - Description: view the IP address of your machine
  - Usage: ip addr

```
┌──(vagrant㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state U
roup default qlen 1000
    link/ether 00:0c:29:16:82:96 brd ff:ff:ff:ff:ff:ff
    inet 192.168.126.128/24 brd 192.168.126.255 scope global dynamic nopre
route eth0
       valid_lft 1291sec preferred_lft 1291sec
    inet6 fe80::fe1c:e713:3a19:a305/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- ping
  - Description: test connectivity to a remote host
  - Usage: ping hostname.com (ping by hostname)
    - ping 100.100.100.100 (ping by IP address)
    - ping -c4 *ip.address* (pings a given amount of times, here, 4)

```
┌──(vagrant㉿kali)-[~]
└─$ ping -c4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=12.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=12.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=12.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=12.7 ms

── 8.8.8.8 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 12.166/12.595/12.843/0.256 ms
```

- traceroute
  - Description: tracks a packets path to a remote host
  - Usage: traceroute hostname.com (traceroute by hostname)
    - traceroute 100.100.100.100 (traceroute by IP address)
    - * * * signifies that a router has been set to remain anonymous

```
┌──(vagrant㉿kali)-[~]
└─$ traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets
 1  192.168.126.2 (192.168.126.2)  0.680 ms  0.591 ms  0.556 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
```

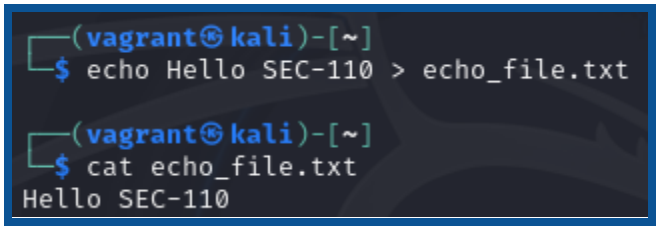
- nslookup (Name Server lookup)
    - Description: sends a DNS request to check the domain name associated with an IP address or vice versa
    - Usage: nslookup hostname.com (nslookup by hostname)
        - nslookup 100.100.100.100 (nslookup by IP address)

```
┌──(vagrant㉿kali)-[~]
└─$ nslookup 8.8.8.8
8.8.8.8.in-addr.arpa    name = dns.google.

Authoritative answers can be found from:
8.8.8.in-addr.arpa      nameserver = ns4.google.com.
8.8.8.in-addr.arpa      nameserver = ns1.google.com.
8.8.8.in-addr.arpa      nameserver = ns3.google.com.
8.8.8.in-addr.arpa      nameserver = ns2.google.com.
ns3.google.com  internet address = 216.239.36.10
ns2.google.com  internet address = 216.239.34.10
ns1.google.com  internet address = 216.239.32.10
ns4.google.com  internet address = 216.239.38.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns4.google.com  has AAAA address 2001:4860:4802:38::a
```

Misc. Commands:

- clear
    - Description: clears the terminal screen
    - Usage: clear
- echo
    - Description: prints text in a command as a terminal output
    - Usage: echo Hello World
        - echo Hello World > file.txt (redirects to print “Hello World” to file.txt instead of the terminal)


(vagrant㉿kali)-[~]
$ echo Hello SEC-110 > echo_file.txt
(vagrant㉿kali)-[~]
$ cat echo_file.txt
Hello SEC-110