



Kali Cheat Sheet

Directory Commands

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

```
(vagrant@kali)-[~]
└─$ pwd
/home/vagrant
```

- 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:

```
(vagrant@kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  forsec_192.168.56.50.cfg  sliver
```

```
(vagrant@kali)-[~]
└─$ ll
total 40
drwxr-xr-x 2 vagrant vagrant 4096 Dec 26 2023 Desktop
drwxr-xr-x 2 vagrant vagrant 4096 Dec 26 2023 Documents
drwxr-xr-x 7 vagrant vagrant 4096 Feb 27 20:47 Downloads
drwxr-xr-x 2 vagrant vagrant 4096 Dec 26 2023 Music
drwxr-xr-x 2 vagrant vagrant 4096 Jan 30 21:26 Pictures
drwxr-xr-x 2 vagrant vagrant 4096 Jan 30 21:12 Public
drwxr-xr-x 2 vagrant vagrant 4096 Dec 26 2023 Templates
drwxr-xr-x 2 vagrant vagrant 4096 Dec 26 2023 Videos
-rw----- 1 vagrant vagrant 1840 Jan 30 21:03 forsec_192.168.56.50.cfg
drwxr-xr-x 2 vagrant vagrant 4096 Jan 30 20:59 sliver
```

- 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:



```
(vagrant@kali)-[~]
└─$ cd Downloads

(vagrant@kali)-[~/Downloads]
└─$ cd

(vagrant@kali)-[~]
└─$
```

- 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

```
(vagrant@kali)-[~]
└─$ mkdir newdirectory

(vagrant@kali)-[~]
└─$ ls
newdirectory

(vagrant@kali)-[~]
└─$ rmdir newdirectory

(vagrant@kali)-[~]
└─$ ls
```

File Commands

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

```
(vagrant@kali)-[~]
└─$ touch newfile.txt

(vagrant@kali)-[~]
└─$ ls
newfile.txt
```

- cat (concatenate)



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

```
(vagrant@kali)-[~]
└─$ cat newfile.txt
Hello SEC-110!
```

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

```
(vagrant@kali)-[~]
└─$ ls
different_directory  newfile.txt

(vagrant@kali)-[~]
└─$ mv newfile.txt different_directory/new_dir/

(vagrant@kali)-[~]
└─$ ls different_directory/new_dir/
newfile.txt
```

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

```
(vagrant@kali)-[~]
└─$ ls
copy_file.txt  different_directory

(vagrant@kali)-[~]
└─$ cp copy_file.txt different_directory/new_dir/

(vagrant@kali)-[~]
└─$ ls
copy_file.txt  different_directory

(vagrant@kali)-[~]
└─$ ls different_directory/new_dir/
copy_file.txt  newfile.txt
```

- 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)

```
(vagrant@kali)-[~]
└─$ ls
copy_file.txt  different_directory

(vagrant@kali)-[~]
└─$ rm copy_file.txt

(vagrant@kali)-[~]
└─$ ls
different_directory
```

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

```
(vagrant@kali)-[~]
└─$ file test.jpeg
test.jpeg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 225x225, components 3
```

- 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

```
(vagrant@kali)-[~]
└─$ nano file.txt
```

```
vagrant@kali: ~
File Actions Edit View Help
GNU nano 8.2 file.txt *
This is my example for nano!
```

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`



```
(vagrant@kali)-[~]
└─$ whoami
vagrant
```

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

```
(vagrant@kali)-[~]
└─$ mv file.txt /home/kali
mv: cannot stat '/home/kali/file.txt': Permission denied

(vagrant@kali)-[~]
└─$ sudo mv file.txt /home/kali
[sudo] password for vagrant:
```

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

```
(vagrant@kali)-[~]
└─$ su kali
Password:
(kali@kali)-[/home/vagrant]
└─$
```

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

```
(vagrant@kali)-[~]
└─$ sudo useradd newuser1

(vagrant@kali)-[~]
└─$
```

- 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



```
(vagrant@kali)-[~]
└─$ sudo adduser newuser2
info: Adding user `newuser2' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `newuser2' (1003) ...
info: Adding new user `newuser2' (1003) with group `newuser2 (1003)' ...
info: Creating home directory `/home/newuser2' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for newuser2
Enter the new value, or press ENTER for the default
  Full Name []: User 2
  Room Number []: 100
  Work Phone []: 111-111-1111
  Home Phone []: 111-111-1111
  Other []:
Is the information correct? [Y/n] Y
info: Adding new user `newuser2' to supplemental / extra groups `users' ..
info: Adding user `newuser2' to group `users' ...
```

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

```
(vagrant@kali)-[~]
└─$ sudo passwd newuser1
New password:
Retype new password:
passwd: password updated successfully
```

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

```
(vagrant@kali)-[~]
└─$ sudo userdel newuser1
```

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
```