

Muhammad Abdullah

221546

LAB MANUAL NUMBER 01

COMMAND NUMBER 01:

```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)~$ echo Abdullah
Abdullah
(kali@kali)~$
```

Echo outputs anything on the terminal or a file.

COMMAND NUMBER 02:

```
(kali@kali)~$ who
kali          tty7          2024-02-11 22:30 (:0)
(kali@kali)~$
```

Who tells about login name, date and time.

COMMAND NUMBER 03:

```
(kali@kali)~$ whoami
kali
(kali@kali)~$
```

Whoami Tells the username.

COMMAND NUMBER 04:

```
(kali@kali)~$ uptime
22:38:16 up 8 min,  1 user,  load average: 0.36, 0.44, 0.31
(kali@kali)~$
```

Uptime Tell how long the system has been up.

COMMAND NUMBER 05:

```
(kali㉿kali)-[~]  
$ uname  
Linux  
  
(kali㉿kali)-[~]  
$
```

Uname Tells the system name

COMMAND NUMBER 06:

```
(kali㉿kali)-[~]  
$ hostname  
kali  
  
(kali㉿kali)-[~]  
$
```

Hostname Display the hostname of the system.

COMMAND NUMBER 07:

```
(kali㉿kali)-[~]  
$ pwd  
/home/kali
```

Pwd Tells current working directory

COMMAND NUMBER 08:

```
(kali㉿kali)-[~]  
$ ls  
192.168.216.132  find      l.py      Pictures  practice-01.log.csv  smb      Videos  
Ahmad          hell.txt  main.exe  practice-01.cap  Public              snort3    'system, letting Wget finish the'  
Desktop       kali-anonsurf  Music     practice-01.csv  samreen.crt        Storm-Breaker  Zeeshan  
Documents     list1.py  output.txt practice-01.kismet.csv  samreen.csr      Templates     zphisher  
Downloads     list.py   pentbox   practice-01.kismet.netxml  samreen.key      usman
```

```
(kali㉿kali)-[~]  
$
```

Ls tells all the elements within a particular directory.

COMMAND NUMBER 09:

```
(kali㉿kali)-[~]  
$ clear
```

Clear clears the whole terminal.

COMMAND NUMBER 10:

```
(kali㉿kali)-[~/Documents]
$ touch 221546

(kali㉿kali)-[~/Documents]
$ ls
221546

(kali㉿kali)-[~/Documents]
$
```

Touch creates an empty file

COMMAND NUMBER 11:

```
(kali㉿kali)-[~/Documents]
$ mkdir Abdullah.221546

(kali㉿kali)-[~/Documents]
$ ls
221546  Abdullah.221546

(kali㉿kali)-[~/Documents]
$
```

mkdir creates a new directory.

COMMAND NUMBER 12:

```
(kali㉿kali)-[~/Documents]
$ cd Abdullah.221546

(kali㉿kali)-[~/Documents/Abdullah.221546]
$
```

Cd means change directory.

COMMAND NUMBER 13:

```
(kali㉿kali)-[~/Documents]
$ mv Abdullah.221546 Radeel.221544

(kali㉿kali)-[~/Documents]
$ ls
221546  Radeel.221544

(kali㉿kali)-[~/Documents]
$
```

mv moves the elements within a file to another file of different name.

COMMAND NUMBER 14:

```
(kali㉿kali)-[~/Documents]
└─$ cat hello.txt
Hello World ;)
```

Cat contaminates file data and shows it on the terminal.

COMMAND NUMBER 15:

```
(kali㉿kali)-[~/Documents]
└─$ cp hello.txt new.txt

(kali㉿kali)-[~/Documents]
└─$ cat hello.txt
Hello World ;)

(kali㉿kali)-[~/Documents]
└─$ cat new.txt
Hello World ;)
```

Cp copies the elements of one file into another file.

COMMAND NUMBER 16:

```
(kali㉿kali)-[~/Documents]
└─$ touch new2.txt

(kali㉿kali)-[~/Documents]
└─$ ls
221546  hello.txt  new2.txt  new.txt  Radeel.221544

(kali㉿kali)-[~/Documents]
└─$ cat new2.txt

(kali㉿kali)-[~/Documents]
└─$
```

Touch creates a new but empty file.

COMMAND NUMBER 17:

```
(kali㉿kali)-[~/Documents]
└─$ date
Sun Feb 11 11:01:11 PM EST 2024
```

Date command tell the current data.

COMMAND NUMBER 18:

```
(kali㉿kali)-[~/Documents]
$ wc -l new.txt
1 new.txt
```

Wc command tells the number of lines in a file.

COMMAND NUMBER 19:

```
(kali㉿kali)-[~/Documents]
$ chmod u+rw,g+rw new.txt
```

Chmod gives permissions to users to read or write or do both or do non.

COMMAND NUMBER 20:

```
(kali㉿kali)-[~/Documents]
$ man nmap
```

```
NMAP(1)                                Nmap Reference Guide                                NMAP(1)

NAME
  nmap - Network exploration tool and security / port scanner

SYNOPSIS
  nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
  Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

  The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (-s0), Nmap provides information on supported IP protocols rather than listening ports.

  In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

  A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are -A, to enable OS and version detection, script scanning, and traceroute; -T4 for faster execution; and then the hostname.

Example 1. A representative Nmap scan

# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
log file: 
```

Man gives manual related to a command suppose here I used the following command that gave me the manual of namp

\$ man nmap

COMMAND NUMBER 21:

```
(kali㉿kali)-[~/Documents]
$ less hello.txt
```

```
Hello World ;)
hello.txt (END)
```

Less shows the less contents the very large file.

COMMAND NUMBER 22:

```
(kali㉿kali)-[~/Documents]
$ rm -rf Radeel.221544

(kali㉿kali)-[~/Documents]
$ LS
LS: command not found

(kali㉿kali)-[~/Documents]
$ ls
221546  hello.txt  new2.txt  new.txt

(kali㉿kali)-[~/Documents]
$
```

rm -rf command removes/deletes a directory

COMMAND NUMBER 23:

```
(kali㉿kali)-[~/Documents]
$ cat hello.txt
Hello World ;)
Football
Abdullah

(kali㉿kali)-[~/Documents]
$ sort hello.txt
Abdullah
Football
Hello World ;)
```

Sort command sorts the elements of a particular file.

COMMAND NUMBER 24:

```
(kali㉿kali)-[~/Documents]
$ sudo su
(root㉿kali)-[/home/kali/Documents]
# exit

(kali㉿kali)-[~/Documents]
$
```

Exit command is used to exit the shell

COMMAND NUMBER 25:

```
(kali㉿kali)-[~/Documents]
$ head /usr/share/wordlists/rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123

(kali㉿kali)-[~/Documents]
$ tail /usr/share/wordlists/rockyou.txt
1234567
1
xCvBnM,
ie168
abygurl69
a6_123
*7;Vamos!
```

Head and **tail** commands tell first 10 and last 10 elements of a file

COMMAND NUMBER 26:

```
(kali㉿kali)-[~/Documents]
└─$ grep 123456 /usr/share/wordlists/rockyou.txt
123456
123456789
1234567
12345678
```

Grep finds matching text with the text that you have entered.

COMMAND NUMBER 27:

```
(kali㉿kali)-[~/Documents]
└─$ ls
221546  hello.txt  new2.txt  new.txt

(kali㉿kali)-[~/Documents]
└─$ rm 221546

(kali㉿kali)-[~/Documents]
└─$ ls
hello.txt  new2.txt  new.txt
```

Rm command is used to remove a file in a directory.

COMMAND NUMBER 28:

```
(kali㉿kali)-[~/Documents]
└─$ sort hello.txt
Abdullah
Football
Hello World ;)

(kali㉿kali)-[~/Documents]
└─$ sort -r hello.txt
Hello World ;)
Football
Abdullah
```

Sort -r command removes the sort that you have applied.

MY 'CAL' AND 'BC' COMMMANDS WEREN'T WORKING ON KALI LINUX