#What is Cyber security

- cyber security is the practice of Protecting Network connected system's,computers and servers, mobile Devices. Including hardware and software. and data from cyber attacks.
- protecting hardware it refers to securing physical devices like computers, servers, and mobile devices from cyber attack.
- Protecting software in cybersecurity means securing applications, programs, and operating systems from cyber attack.

#what is cyber attack

- A cyber attack is an attempt by hackers to damage, steal, or gain unauthorized access to computer systems, networks, or data. These attacks can target individuals, organizations, or even governments.

#How to protect

1.Network security :

- Firewalls: Monitor and filter network traffic to prevent unauthorized access.
- Intrusion Detection/Prevention Systems (IDS/IPS): Detect and block malicious activities.
- VPN (Virtual Private Network): Encrypts internet traffic for secure communication.

2. Endpoint Security

- Antivirus & Anti-malware: Detect and remove malicious software.
- Endpoint Detection & Response (EDR): Monitors devices for suspicious behavior.

3. Application Security

- Secure coding practices: Writing code that is resistant to vulnerabilities.
- Web Application Firewalls (WAF): Protects against web-based attacks like SQL injection and XSS.

4. Data Security

- Encryption: Protects data by converting it into unreadable code.
- Backup & Disaster Recovery: Ensures data can be restored after cyber incidents.

5. Identity & Access Management (IAM)

- Multi-Factor Authentication (MFA): Requires multiple verification methods for access.
- Role-Based Access Control (RBAC): Limits access based on user roles.
- Securing cloud storage and services with access control, encryption, and monitoring.

7. Security Awareness & Training

- Educating employees about phishing, social engineering, and safe browsing habits.

#What is ethical hacking

- Ethical hacking is the process of legally breaking into computers and networks to test and improve security.
- Their goal is to:
- ✅ Identify vulnerabilities.
- ✅ Test if vulnerabilities can be exploited.
- ✅ Suggest or implement fixes to prevent attacks before malicious hackers can exploit them.

#Types of hackers

1.Black hat hacker {crackers}

- Individual with extraordinary computing skills, utilised for malicious (or) destructive activities.
- Who illegally tests for vulnerabilities , exploit them without permission ,and then profits from stolen data.

2.white hat hacker { ethical hacker }

- individual's utilising hacking skills for defensive purpose.

3.gray hat hacker

- Individual's who work both offensively and defensively at various time.
- Who illegally tests for vulnerabilities , exploit them without permission ,they often report them to the organization.

4.sucide hackers

- Suicide Hackers are individuals who carry out cyberattacks without concern for the consequences, even if it means getting caught or facing legal action or fine .

5.script kiddies

- An unskilled hacker who used premade tools that were developed by real hackers, and they don't know how they work in the background.

6.Hacktivist

- who promote a message by defacing a site.

7.state sponsored hackers

- They are government employees to penetrate and gain confidential information from another country government,companies or individual.

#Risk=vulnerability+threat

Vulnerability

- Existence of a weakness in a design, or Implemenatation that can lead to an unexpected event compromising the security of the system.

Threat

- a threat in cybersecurity is anything that can cause harm to your data, devices, or network.
- It should may be Natural, unintentional, Intentional threat's.
- Natural threats = earthquakes , floods , fires etc …
- Unintentional (human erros) = these are caused by mistake or negligence
- Ex : misconfiguring firewalls or security settings
- Clicking on a phishing link by mistake
- Intentional threats = hacking ,phishing,virus spreading.
- Real life example : Leaving a car unlocked at Hyderabad, a very theft-prone place, can create an opportunity for theft; it may happen or may not.

Risk

- #The Potential for loss (or) damage when a threat exploits a vulnerability.
- Example: Financial loss, Privacy loss, reputation loss.

1. Software Vulnerabilities

- Flaws in code, applications, or operating systems that attackers exploit.
- Examples: Buffer overflow, SQL injection, zero-day exploits.
- Cause: Coding errors, outdated software, or misconfigurations.
- Fix: Patching, updating software, secure coding practices.

2. Hardware Vulnerabilities

- Flaws in physical components (CPUs, memory, chips, etc.) that can be exploited.
- Examples: Spectre, Meltdown (CPU vulnerabilities), hardware backdoors.
- Cause: Design flaws, manufacturing defects, or weak security in firmware.
- Fix: Firmware updates, secure hardware design, using trusted components.

3. Network Vulnerabilities

- Weaknesses in network infrastructure that allow unauthorized access or attacks.
- Examples: Open ports, weak encryption, misconfigured firewalls, outdated network protocols.
- Mitigation: Use firewalls, VPNs, strong encryption, and regularly update network devices.

4. Human (Social Engineering) Vulnerabilities

- Exploiting human psychology to bypass security.
- Examples: Phishing emails, weak passwords, insider threats, poor security awareness.
- Mitigation: Security training, multi-factor authentication (MFA), and phishing simulations.

5.Cloud Vulnerabilities

- Security risks in cloud-based systems.
- Examples: Misconfigured cloud storage, insecure APIs, lack of data encryption.
- Mitigation: Strong access controls, data encryption, and regular security audits.

#CIA triad

1.Confidentiality

- confidentiality refers to protecting Information From unauthorized access.

2.Integrity

- integrity refers data have not been modified, deleted by unauthorized user.

3.Availability

- Availability refers data are accessible when you need them.

4.Authentication

- Authentication is the process of verifying the identity of a user, device, or system.

5.Authorization

- Authorization is the process of granting or denying access to resources, systems, or applications, based on the authenticated user's identity, role, or permissions.

5.Non-Repudiation

- Important to ensure that a Party cannot deny having sent (or) a received message.

- common techniques used to establish non repudiation include digital signatures, message authentication codes, time stamps.

Real life example:

- Leaving a car unlocked at Hyderabad, a very theft-prone place, can create an opportunity for theft; it may happen or may not.
- Flipkart order delivered through OTP verification to the customer, when the customer reports to Flipkart that the order was not received, the OTP is proof.

#Phashes of hacking

Attack=goal + method + vulnerability

- Goal is hacking friend's Instagram account, method is asking as a very trusting person, trusting is vulnerability.
- Goal: Steal user credentials (e.g., email login),Method: Sending a fake email with a malicious link to a login page,Vulnerability: User trust and lack of awareness about phishing emails

#Phashes of hacking

1.Reconnaissance

- This Phase involves gathering information about the target system or organization. It includes both Passive and active reconnaissance techniques, such as open source inteligence (OSINT)

2.scanning

- ethical hackers uses various tools and techniques to Identify open Ports, services, vulnerabilities on the target Network, It includes Port scanning Vulnerability scanning and Network mapping .
- Scanning helps to create a Detailed map of the target Network and Identify potential entry Points.

3.Gaining access

* This Phase involves exploiting the Identified vulnerabilities to gain unauthorized access be the target system.

4.Maintaining access

- once access is gained, the ethical hacker focuses on maintaining control over the compromised system or Network, This Phase involves various activities, such as creating back doors, Installing root kits, trojan, key logger, RAT, The objective is to ensure continued access to the targets and gather additional Information without being detected.

5.Covering Tracks

- An intelligent hacker always clears all evidence so that in the later Point of time, no one will find any traces leading to him in this final phase, the ethical hacker removes any evidence of their activities to avoid Detection. This include Deleting log files, clearing system logs, command's history etc...

- The Purpose is to make Difficult for forensic investigators to Determine the extents of the breach and Identify of attacker.

#Foot printing

1. Active Footprinting ⚡

Involves direct interaction with the target system or network.

Examples:Using network scanning tools (Nmap, Wireshark).

Sending ping requests to check if a system is online.

Enumerating services and open ports.

2. Passive Footprinting 🕵️

Collecting data from publicly available sources without directly interacting with the target system.

Examples:Searching on Google, social media, and company websites.

Gathering information from WHOIS databases, DNS records, and job postings.

Using Open Source Intelligence (OSINT) tools like Shodan and Maltego.

- The strength of these components can define the level of security.

Security (Restrictions) ensures that systems are protected against cyber threats, but too many restrictions can make them difficult to use.

🔷 Functionality (Features) enhances user experience by adding more capabilities, but too many features can create vulnerabilities.

🔷 Usability (Ease of Use - GUI) makes systems user-friendly, but prioritizing usability over security can lead to risks like weak authentication or data breaches.

The Trade-Off:

✅ More Security → Less Functionality & Usability

✅ More Features → More Security Risks

✅ Better Usability → Potential Security Weaknesses

#Operating System

An operating system (OS) is a software program that enables computer hardware to communicate and operate with computer software.

Examples: Android, iOS, macOS, Windows, Ubuntu, Linux

#Functions of an Operating System

1. Process Management ⚙️

Starts and stops processes.

The OS decides the order in which processes access the CPU and how much processing time each process gets.

2. Memory Management 💾

Manages the allocation and deallocation of memory to various processes.

Ensures that one process does not consume the memory allocated to another.

3. File System Management 📂

Keeps track of information related to file creation, deletion, transfer, copying, and storage.

Organizes files into directories for efficient navigation and usage.

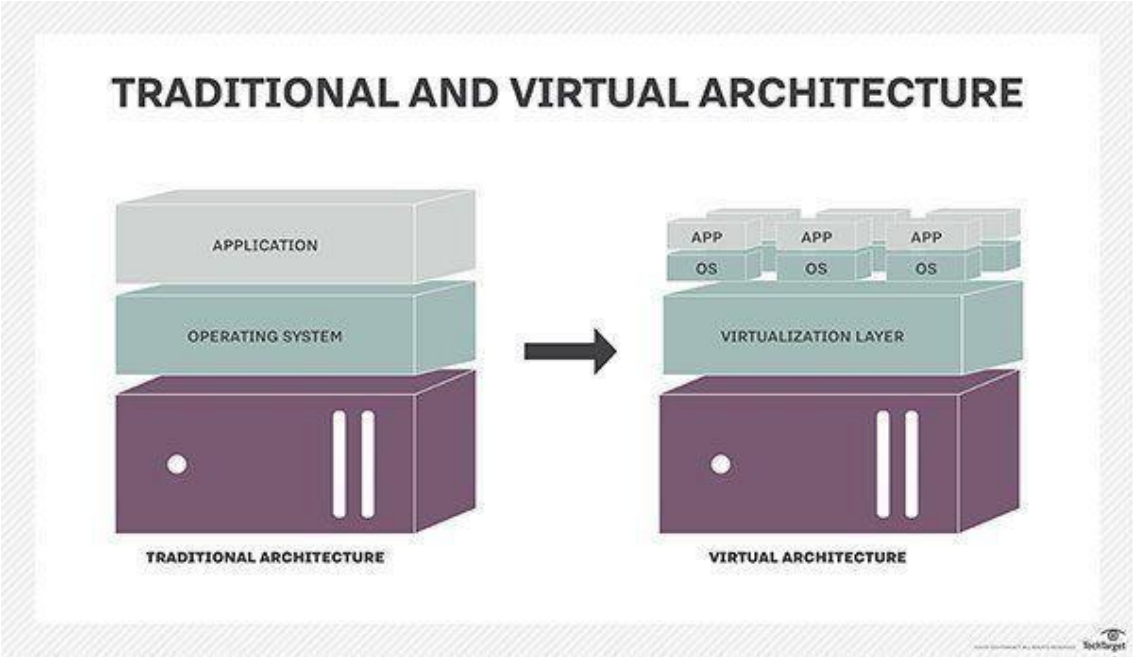
Controls user access settings and tracks where data is stored.

4. Input/Output (I/O) Management 🎛️

Manages input and output operations between the computer and external devices.

Examples of I/O devices: Keyboard, mouse, microphone, printer, hard drive, monitor.

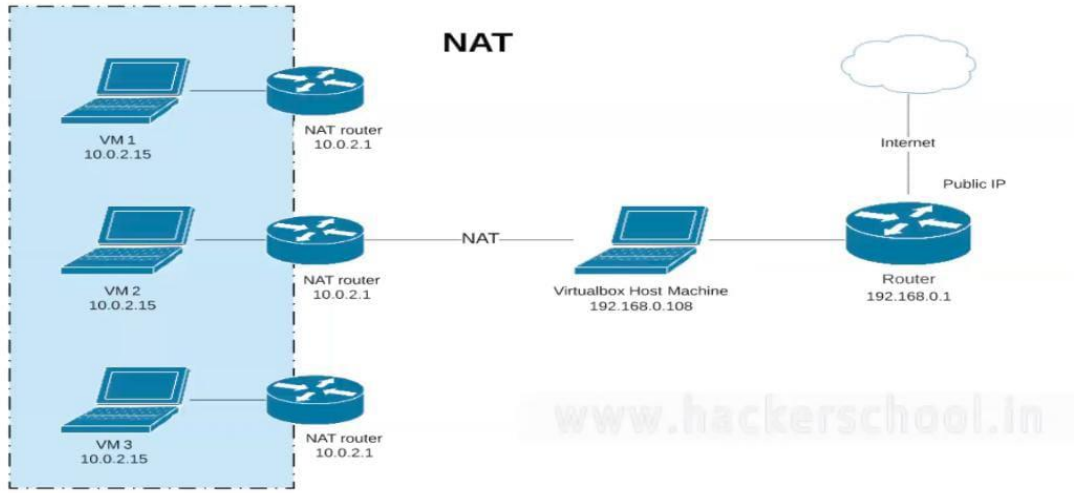
#Vmware/virtualbox

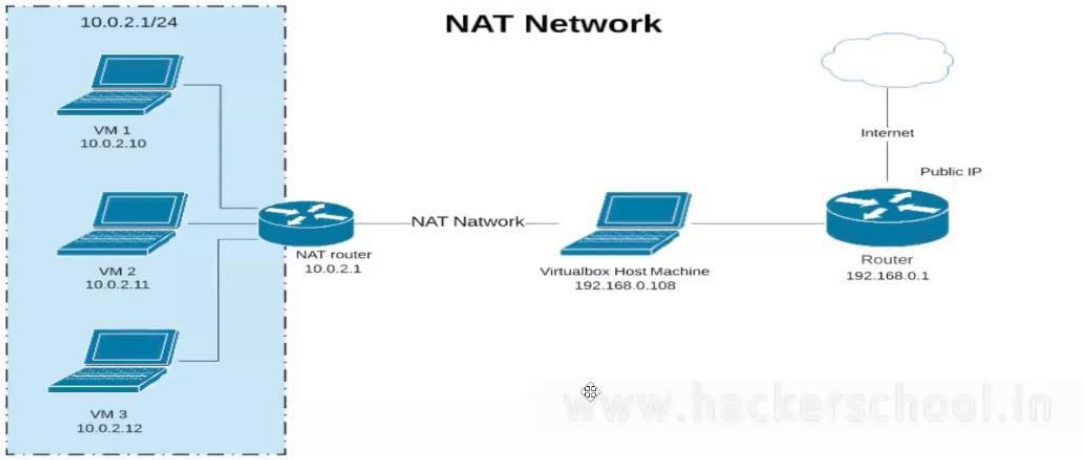


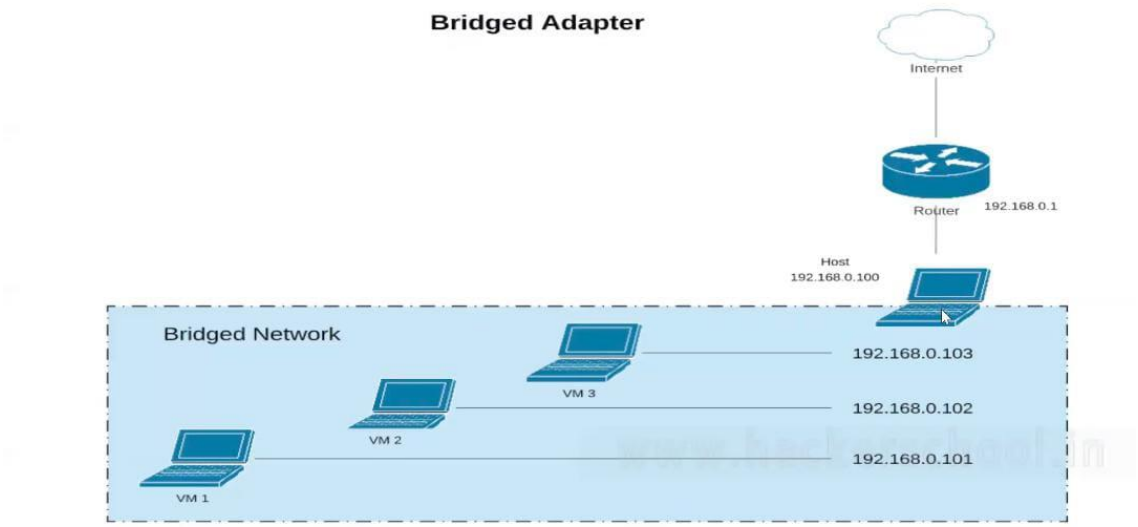
- VirtualBox/vmware is a free and open-source virtualization software's that allows you to run multiple operating systems (OS) on a single physical host machine.
- virtual box takes hardware resources from host machine.
- It create virtual cpu,virtual ram,virtual storage for each virtual machine.

#Network modes

Mode	VM→Host	VM→Host	VM1↔VM2	VM→Net/LAN	VM→Net/LAN
NAT	✓	Port forward	✗	✓	Port forward
NAT Network	✓	Port forward	✓	✓	Port forward
Bridged	✓	✓	✓	✓	✓
Internal	✗	✗	✓	✗	✗
Host-only	✓	✓	✓	✗	✗


NAT
VM 1
10.0.2.15
NAT router
10.0.2.1
VM 2
10.0.2.15
NAT router
10.0.2.1
VM 3
10.0.2.15
NAT router
10.0.2.1
NAT
Virtualbox Host Machine
192.168.0.108
Internet
Public IP
Router
192.168.0.1
www.hackerschool.in


10.0.2.1/24
NAT Network
VM 1
10.0.2.10
VM 2
10.0.2.11
VM 3
10.0.2.12
NAT router
10.0.2.1
NAT Natwork
Virtualbox Host Machine
192.168.0.108
Internet
Public IP
Router
192.168.0.1
www.hackerschool.in



Want to change network modes in VirtualBox? Follow these steps:

1. Open VirtualBox → Select your VM
2. Go to Settings → Click Network
3. Choose a Network Mode: NAT, Bridged, Internal, Host-Only, NAT Network etc..
4. Save & Restart your VM

#Best Virtualization Software's

- 1.VMware Workstation

  #https://www.vmware.com/

- 2.virtualbox

  #https://www.oracle.com/virtualization/technologies/vm/downloads/virtualbox-downloads.html?source=:ow:o:p:nav:mmddyyVirtualBoxHero&intcmp=:ow:o:p:nav:mmddyyVirtualBoxHero

Steps to Install VirtualBox on Windows:

✅ Step 1: Download VirtualBox

1. Go to https://lnkd.in/dCZ529qa

2. Click "Downloads" and select Windows hosts to download the .exe file.

✅ Step 2: Install VirtualBox

3. Double-click the downloaded .exe file to start the setup.

4. Click Next and keep the default settings.

5. Click Yes if you get a network warning (it may temporarily disconnect your internet).

6. Click Install and wait for the process to complete.

7. If prompted, allow VirtualBox to install drivers.

8. Once done, click Finish and launch VirtualBox!

#linux

- Linux is an open-source operating system (OS) created in 1991 by Linus Torvalds. It is

based on the UNIX operating system.

- First released version linux 0.01 in sep 17th 1991.
- Linux Is not os,it is a kernal.
- Linux distributions (distros) are different versions of the Linux operating system. They all use the Linux kernel but come with different software, user interfaces, and purposes.

When interacting with a computer, there are two main types of interfaces When interacting with a computer, there are two main types of interfaces:

Command-Line Interface [CLI]

⇒ Text-based Interface interacts with computer using commands and arguments

graphical user interface [GUI]

⇒ visual interface interacts with computer using graphics, icons, and menus

Shell :

- A shell is a special user program that provides an interface for the user to use operating system services. Shell accepts human-readable commands from users and converts them into something which the kernel can understand.

Here's are the steps :

1. User types a command: The user interacts with the shell by typing a command.

2. Shell checks for validity: The shell checks the command for syntax errors and ensures it's a valid command.

3. Shell converts to kernel-understandable language: If the command is valid, the shell translates it into a language that the kernel can understand. This is often done using system calls.

4. Shell sends the request to the kernel: The shell sends the translated command to the kernel for execution.

5. Kernel executes the command: The kernel receives the request, executes the command, and returns the result to the terminal.

6. terminal displays the result: The shell receives the result from the kernel and displays it to the user.

Types of shells in kali linux.

1) Bourne shell (sh) :-

=> The original Bourne shell is simple and lightweight It's often used as a default shell for system accounts and in scripts due to It's simplicity and fast startup time.

2) Bourne again shell (bash)

=> Bourne again shell is a enhanced version of the Bourne shell. It's the default shell for most linux distributions and offers advance features like job control, command history scripting capabilities.

3) Korn shell (ksh)

=> ksh is a shell developed by David Korn at Bell labs. It's know for It's advanced features such as built-in command editing, job control and a powerful scripting language. It's often used in proffessional environements due to It's robustness and reliability

3) Z shell (zsh)

⇒ zsh is a shell designed for interactive use, although it's also a good scripting shell. It incorporates many features from bash, ksh, and other shells, and offers advanced features like themed prompts, like themed prompts, spell correction and a powerful scripting language.

4.C shell

- The C shell (csh) was **created by Bill Joy while he was a graduate student at the University of California, Berkeley in the late 1970s**.14 It was first distributed in 1978 as part of the 2BSD release of the Berkeley Software Distribution (BSD).
- Csh

5.tcsh shell

- Tcsh is an enhanced but completely compatible version of the Berkeley Unix C shell (csh) and is used both as an interactive login shell and a shell script command processor.
- Tcsh

#Linux Hierarchical Filesystem

1./bin

- Contains essential binary programs, that are used by the system
- EX: cp,mv, rm,nano,nice,netstat etc…
- commands used by all normal users.

2./sbin

- contains system binary executables, such as init, shut down, reboot.
- Ex:add user, add group, arp,arp-scan,
- Commands used by super user.

3./root

- the home directory of the root User,which is the system administrator account.

4./etc

- stores system configuration files, including Network settings, user Information and system wide settings.

5./tmp

- Used for storing temporary files, which are usally deleted when the system is restarted.

6./home

- The /home directory in Linux is where user home directories are stored. Each regular user has a personal directory inside /home, named after their username (e.g., /home/sai for a user named "sai, where users store their personal files.

7./boot

- contains the files needed to boot the operating system.

8./dev

- contains special device files used to interact with system hardware components.

9./media

- used for mounting removable media like usb,dvd,cds or external hard disks.
- When you plug in a usb drive,its get mounted in /media with a subdirectory named after the device.

10./mnt

- A temporary mount point for file system.

11./opt

- The /opt (optional software) directory in Linux is used for installing third-party or optional software that is not part of the default package management system (like apt or yum).

12./lib

- It contains shared librarie's files ned by the system and programs in /bin and /sbin.

13./lost+found

- Stores recovered files after an unexpected system crash (specific to ext file systems).

14./proc

- A virtual filesystem that contains information about running processes and system resources.

15./run

- Holds runtime data like process IDs (PID) and sockets, cleared on reboot.

16./snap

- Used by Snap package manager to store installed Snap applications.

17./srv

- Stores data related to services provided by the system, like web or FTP servers.

18./sys

- A virtual filesystem that provides information about hardware and kernel settings.

19./usr

- Contains user utilities, applications, and libraries (e.g., /usr/bin, /usr/lib).

20./var

- Holds variable data like logs (/var/log), spool files, and temporary data.

Linux commands

#apt update

- This command used fetch latest version of already installed packag’s and not installed packages,It doesn’t download or install any new package.

#apt upgrade

- Update to the latest version installed packages.

#apt install <Package Name>

- used to Install Package from the repositories.

#apt remove <Package Name>

- used to remove Package from your debian-based linux system.

#apt remove --purge Package Name>

- used to remove a Package and It's associated configuration files from your debian-based Linux system.

#apt autoremove <package Name>

- used to remove a Package, and. Its dependencies from your debian-based linux System.

#Difference between configurations & Dependencies

#Configuration's

- In Package management, configuration refers to the settings and options that are

specific to a Package.

#Dependencies

- Dependencies, on the other hand, refer to the Packages that a Package requires to Function Properly.

- when you install Package,It's dependencies are also automatically installed to ensure that the Package can function Properly.

#apt-cache search <keyword>

- used to search for packages in the package cache.

#dpkg -i .deb

- used to install a Debian package file on Debian based system.

#dpkg -r pkname

- used to remove an Debian installed package from a system.

NOTE: - indicates an option or argument ex: ls-l

#cd < directory name>

- change to particular directory.

#cd /

- change current working directory to the root directory.

#cd ..

- one step back going from current working directory.

Relative path: Navigating from your current location.

- Example: cd dir (if dir is in the current directory).

Absolute path: The complete path from the root location (/).

- Example: cd /home/ubuntu/Folder_one.

#=Reprisents root user.

$=Reprisents normal user.

#ctrl+shift+c

- Copy the selected text from the terminal to the clipboard.

#ctrl+shift+v

- Paste the copied text into the terminal.

#ctrl+L

- Clear commands alternative.

#ctrl+A

- Moves the cursor to the beginning of the current line.

#ctrl+E

- Moves the cursor to the end of the current line.

#ctrl+c

- Terminate the currently running foreground process (kill).

#ctrl+z

- Suspends the currently running foreground process (pause).

#ctrl+k

- Delete one by one line at configuration file modification time help.

#ctrl+shift+D

- Split terminal horizontally.

#ctrl+shift+R

- Split terminal vertically.

#ctrl+shift+T

- Going to new tab.

#ctrl+shift++

- Terminal screen zooming.

#ctrl-

- Terminal screen zoom out.

#ctrl+0

- Zoom reset

up arrow key

- brings up the last command you entered.

- Use this quicky rerun or modify previous command without retyping them.

#man <command/tool name>

- Display manual page for the command/tool

- Press q for exit

#<command/tool name> -h/--help

- Display help page for command/tool.

#whatis <command/toolname>

- Nmap = network scanning
- Ettercap = sniffing
- ls =list directory content

#whoami , echo $USER , id -un , logname , grep "^$(whoami)" /etc/passwd

- display the currently, logged User Name into the system.

#id , echo $UID , grep "^$USER:" /etc/passwd

- Display currently logged in user id and user belongs to any groups their names and id's.

#id -u < user name > , grep "^root:" /etc/passwd

- Retrieve the user id of a given username.

#Retrieve all users name and threir id's

- awk -F':' '{print $1, $3}' /etc/passwd

#hostname ,uname -n , nmcli general hostname , hostnamectl

*display the host name (system) of the system,which is Name assigned to the system for Identification purposes.

#hostnamectl set-hostname newname

- Changing host name of the system.

#pwd , echo $pwd , ls -ld $(readlink -f .) , realpath . , printf "%s\n" "$PWD"

*print present working directory, it display the current working directory of the terminal session.

#ip a , ip addr , ifconfig , hostname -I

- displays a list of all available Network Interfaces, Including their IP addresses, Netmask and mac other relevant Information.

#ls

- Display list of files and directories available in the current working directory.

#ls -l

- Display list of files and directories available in the current working directory including with owner of the file/directory ,their permissions ,size of the file ,created date etc..

#ls -a , ls -la

- Display files/dir available in the current working directory including with hidden files also.

#ls -r , la -lr

- List files/dir in reverse order.{z-a}

#ls -t ,la -lt

- Sort by modification time,newest files/dir first.

#ls -i <file name/dir>

- Display inode number of the file/dir.It is a unique identifier for a file/dir.

#ps $$, echo $0

- Identify which shell you are currently using

#chsh -s /bin/bash , sudo chsh -s /bin/bash user1 , sudo usermod --shell /bin/bash $(whoami) , sudo usermod --shell /usr/sbin/nologin user1

- To change the default shell for the currently logged-in user.
- For example, I've chosen /bin/bash, but you can change it to any shell of your preference.
- Manually editing /etc/passwd

#bash , /bin/bash , exec bash

- Swich to the bash shell.
- exit command= again comes to zhell.

#wheris <command/executable>,which <command/executable> , command -v id , type cat , realpath $(which id) , readlink -f $(which id)

- Find path location of a command,binary and souce and executable files.

#clear,ctrl + L

- Erase the current screen content,removeing all typed commands and leaving a blank screen.

#exit

- close the current terminal window.

#touch filename1 filename2 filename3 …

- Used to create an empty file's.
- #touch file{1..10}

#What is directory

- it's a container that holds files, subdirectories, and other directories.

#mkdir directory1 directory2 directory3 ..

- Used to create an new directory's.
- mkdir dir{1..5}=It creates 5 files.

#mkdir -p dir/dir2/dir3

- first dir1 will be created and in that directory , dir2 will be created and within that di2, dir3 will be created.

#rm filename1 filename2 ..

- used to remove empty file's.
- rm file{1..10}

#rmdir dir1 dir2 dir3 ..

- used to remove directory's
- rmdir dir{1..10}

#rm *

- delete all empty files in the current working directory.

#rmdir *

- used to remove all directory's in the current working directory.

#rm a* , rm *n

- Delete a files starting with a letter and ending with n letter .

#rmdir a* , rmdir *n

- Delete a directorie's starting with a letter and ending with n letter.

#rm -r <file/dir>,rm -rf <file/dir>

- used to remove file/dir forcefully.

#rm -r *,rm -rf *

- Delete all files/dir in the current working directory.(forcefully)

#rm -i filename , rmdir -i dir , rm -rf file/dir -i , rm -r file/dir -i

- while removing file/dir,it will ask confirmation.
- y = yes
- n = no

#Cat > filename

- Out put(content) sending into the file.
- Ctrl+D=save

#Cat >> filename

- Used to append text/content to file.

#Cat filename , sed '' file, nl filename

- Used to read the content of the file.

#uname -a

- Display information about kernal.

#cat /etc/os-release , lsb_release -a

- Display information about operating system.

#nano filename

- Creating a file and writing content to a file ,editing a file.
- Ctrl+x=save

- Ctrl+shift+f = searching specific keyword

#sudo apt install Pluma , pluma filename

#vi filename

- Press Esc button on laptop after type :wq ,enter= save and exit

#tree /

- Display files/dir starting from root location,in tree like representation.

#tree

- Display files/dir in current working directory,in tree like representation.

#tree dirname

#date

- Display date,month,year,time,day .

#date +%D

- Display month,date,year

#date +%T

- Display time,{hours,minutes,seconds}

#date +%d

- Display only date

#date +%m

- Display only month {1,2,5,7,)

#date +%y

- Display only year value in yy form.{24=2024,25=2025}

#date +%Y

- Display only year value in yyyy form{2025}

#date +%H

- Display only hours value.

#date +%M

- Display only minutes value.

#date +%s

- Display only seconds value.

#timedatectl

- timedatectl is a command line tool in linux for controlling and display and configuring system time,date and time zone settings.

- timedatectl = Display date,month,year,time.

- timedatectl list-timezones = Display time zones

- sudo timedatectl set-timezone zonename = setup the selected zone time.

#file <file name>

- Identify the type of file format.

#test -f filename && echo "file" || echo "Not a file"

#test -d dirname && echo "Directory" || echo "Not a directory"

#test -x exfile && echo "Executable file" || echo "Not executable"

File Type	Command to create the File	Located in	The file type using “ls -l” is denoted using	FILE command output
Regular FIle	touch	Any directory/Folder	–	PNG Image data, ASCII Text, RAR archive data, etc
Directory File	mkdir	It is a directory	d	Directory
Block Files	fdisk	/dev	b	Block special
Character Files	mknod	/dev	c	Character special
Pipe Files	mkfifo	/dev	p	FIFO
Symbol Link Files	ln	/dev	l	Symbol link to <linkname>
Socket Files	socket() system call	/dev	s	Socket

Identify type of ~~Kolour~~ Files by Colouring:

Blue - Directory

green - Executable or recognized Data File

Cyan (skyblue) - symbolic link file.

Yellow with black background - Device files

magenta (Pink) - graphic Image file

Red - Archive file, zip file

Red with black background - Broken link

#cp filename <existed/non existed filename>

- One file data copying to anther file.

#cp filename <existed/non existed dirname>

- Copy the file into the specified directory.

#cp -r dir dir1

- Copy the directory along with files into another directory.

#mv filename filename1

- Change the file name.

#mv filename dirname

- Move the file into specified directory.

#mv dir dir1

- Move a directory along with a files into a new directory.

#commands > filename

- Redirect the commands output into to a file.
-

| =Redirect’s out from one command as input to another command.

#wc

- Display number of lines,words,bytes
- Ex:cat filename | wc , cat /etc/passwd | wc
-

#wc -l , awk 'END {print NR}' filename.txt , perl -lne 'END { print $. }' filename.txt

- Display only number of lines

#wc -w , awk '{ total += NF } END { print total }' filename.txt , perl -lane '$c += @F; END { print $c }' filename.txt

- Display only number of words. { sai jain} = 2 words

#wc -c , wc -m , awk '{ total += length($0) } END { print total }' filename.txt

- Display only bytes.
- 1 charactes = 1 bytes and even space also 1 byte.
- Sai jain = 8 bytes

#Standard Input(stdin)=0

- Purpose: Reads input from the user or another source (like a file or another program).
- Default source: Keyboard (User input in CLI)

#Standard output=stdout=1

- Purpose: Prints regular output (results, messages).
- Default destination: Screen (Terminal/CLI output)

#Standard error=stderr=2

- Purpose: Prints error messages separately from normal output.

< =Input redirectional operator

- Redirects a file's content as input to a command.
- cat < file.txt

>= out put redirectional operator.

- Redirects output to a file, overwriting it if the file already exists content.
- Overwriting means replacing the existing content of a file with new content.

>> = Double redirectional operator

- Appends output to a file instead of overwriting

#sudo updatedb

- Used to update the date base used by the locate command.

#locate filename/dirname

- locating path of the specific file/dir .
- locate -i keyword
- locate a* =the files name starting with a
- locate *n = the files names ending with n

Wile cards

- S*
- *n
- File = f??e = I know first and last character's but idont know remaing two character's
- [a-z] , [A-Z}
- [abc]
- [0-5]
- [123]

#find :

- /
- .
- -name

- -user
- -not -user
- -type f
- -type d
- -size +512M {M,G}
- -mtime +2 { more then 2 days }
- -mtime -2 { less then 2 days }
- -m time 2 { exactly 2 days }
- 2>/dev/null
- 2>trash.txt

#head , awk 'NR<=10' filename

- Display the first 10 lines (top to bottom) (By default)
- Ex:cat filename | head , cat /etc/passwd | head

#head -n 5 , awk 'NR<=5' file.txt

- Display the first 5 lines (top to bottom) (our choice)
- Ex:cat filename | head -n 5 , cat /etc/passwd | head -n 5

#tail , awk '{lines[NR] = $0} END {for (i=NR-9; i<=NR; i++) print lines[i]}' file.txt

- Display last 10 lines (bottom to top)

#tail -n 2 , awk '{lines[NR] = $0} END {for (i=NR-1; i<=NR; i++) print lines[i]}' file.txt

- Display last 2 lines.

#more filename

- To read the file content,only forward and no back forward option.
- q=exit
- using through arrow keys

#less filename

- To read the file content ,both forward and back forward available.
- q=exit
- using through slider to up and down .

#truncate -s +10K filename

truncate -s +10M filename

truncate -s +1G filename

- Extend a file size.

#truncate -s -10K filename

truncate -s -100M filename

truncate -s -1G filename

- Degrees/shrink a specified size to a file.

- https://www.gbmb.org/bytes-to-kb [convert bytes to kb]
- https://www.gbmb.org/bytes-to-mb [convert bytes to mb]
- https://www.dataunitconverter.com/byte-to-gigabyte/ [convert bytes to gb]

#cat /etc/shells

- List all available valid shells on the system.

#history

- Display a list of previous executed commands.

#HISTSIZE=0

- Delete command's history.
- This command works both zshell & bash shell.

#history -c

- Delete commands's history.
- This command works only bash shell

#Archive

- Group of files into a single unit.

#tar -cf saijain file1 file2 file3 di1 di2 …

- Create a tar archived named saijain , containing file1&file2&file3&dir&dir2.

#tar -tf saijain

- Display list of available files/dir's in saijain archive.

#tar -xf saijain

- Extract the files/dir from the saijain archive.

Zipping

- Zipping refers the process of compressing files into zip archive format,It Degrese file size when you extract them increase the file size again.

#gzip file1 file2 ..

- Compress a files into .tz extension

#gzip -d file1.gz file2.gz .. , gunzip filename.gz

- Decompressing a file.

#zip files.zip filename1 filesname2

- Compresses file's into a zip archive.
- Zip fies.zip *txt
- Zip -r files.zip dirname =Add a dir to zip archive.
- Zip -sf files.zip =list the files and dir along with their files in zip archive
- Zip -d files.zip sai.txt = delete file from zip archive.
- Zip new.zip –password file1 file2 = when unzip time the password will ask.

#unzip filename.zip

- Extract files from zip archives.

#cut -c 1

- Extract first character from each line.
- Cut -c 1-4 = Extract first four character's from each line's
- Cut -c 1,3,5 =Extract first and third and fifth character's from each line's
- Ex: SAI = s=1,A=2,I=3
- cat filename | cut -c 1 , cat /etc/passwed | cut -c 1-4 .

#cut -f 1

- Extract the first field from each line's
- Cut -f 1-4 =Extract first four fields from each lines's.
- Cut -f 1,3,5=Extract first and third and fifth fields from each line's.
- Ex:BOTTA SAI PRASAD = f1,f2,f3

- cat filename | cut -f 1, cat /etc/passwed | cut -f 1-4
- #cut -d “:” , cut -d “;” , cut -d “ “ = delimete’s
- --output-delimeter=”.”
- ex:sai:jain=sai.jain

#grep -i <keyword1> <keyword2> <file1> <file2>

- Global regular expression print = grep
- Grep command search for a particular string/keyword from a filr and print lines matching a patten.
- grep -iw keyword key1 key2=Search exact word
- grep -in keyword=display line numbers that keyword matched line nymber.
- grep iE “keyword1|keyword2” , egrep -i “keyword1|keyword” = Seach both keywords.
- grep ^a keyword=content start with a letter
- grep n$=content end with n letter
- grep -ic keyword =print how many times given keyword matched.
- grep -ih keyword file1 file2 = To suppress file names while searching given keyword in multiple files and directories display matched words lines.
- grep -iR keyword dir = Seach in keyword within files in the given directory and subdirectories.

- pgrep < process name > = Display pid's

- Zgrep -i keyword filename = search keyword in compressed files,with out decompressing.

- zgrep -iw ,zgrep -in , zgrep -ic , zgrep -iE "keyword1|keyword2"

#Sudo apt install pdfgrep

- Pdfgrep -i keyword filename.pdf = search the keywords in a pdf file.

#sed -n '1p'

- It prints first line

- sed -n '1,5p' =It prints 1 to 5 ines.

- Sed -n '1p;3p;5P'=It prints 1 and 3 and 5 line only.

- sed 1d = It deletes 1st line .

- sed 1,10d = It delete's line 1 to 10.

- Sed -e '1d' -e '10d' = delete a specific lines'

- sed '/word/d' = Delete a specified word but it also automatically that word contains line.

- sed 's/oldword/newword/' = Specified old word change to new word.

- sed ‘6 s/oldword/newword/ = Specified old word change to new word,at specified line number only

- (changes does not affect on original file)

#awk ‘{print $1}’

- Prints first field from each line.

- #awk ‘{print $NF}’= prints last fields.

- awk ‘{print $1,$5}’ =prints 1st and 5th field.

- awk -v f1=1 -v f2=3 '{for(i=f1;i<=f2;i++)printf $i" ";print""}' = print from 1st field to 3rd field.

#sort

- sort the lines in alphabetically order.

#sort -r

- sort the lines in reverse alphabetically order.

#sort -u

- sort the lines in alphabetically order and remove duplicate lines.

#Soft link

- The link will be removed if the original file is removed/renamed.
- Original file and soft link file are different inode number and files sizes and time stamps
- Ususlly soft link files has smaller size then original file size.

- command:ln -s filename <non existed filename>

#Hard link

- When we remove the original file or rename file name,link file contains remain same,The link will be not be effected even if the original file is removed/renamed.
- Both original file and hard link files have same inode number ,same size,same time stamps.
- Command:ln filename <non existed file name>

#Terminal

- Terminals receive commands typed by the user and pass them to the shell (such as Bash, Zsh, or PowerShell) for processing.

#echo $TERM , tput -T$TERM longname , printenv TERM ,

- Display the terminal type that your current shell is using.
- x term or x term 256 Coloor = y terminal emulator.
- vt 100 (or) vt 102 = virtual terminal.
- screen (or) tmux = terminal multiplexer.
- dumb = simple minimal terminal.

#export TERM=xterm

- You are telling to the system,use the xterminal, this temporary when you close the terminal it will comes back to the xterm-256colour terminal.
- export TERM=xterm-256colour = get back to again normal terminal

env

- Displays all environment variables and their values.

#alias

- shortcut keyword for command.,when you execute shortcut keyword the original command will be executed.
- alias sai=”ls-l” = create a shortcut keyword for command.
- Unalias sai =Removes a shortcut keyword for command.
- alias=Display list of all setted shortcut keyword along with command.
- Unalias-a = unalias all shorcuted keyword’s in single command
- By default they are temporary when you close the terminal they are not work after open the terminal when you trying to use the shortcut keyword , for permenent setup of alias follow the below process …
- For zshell edit this file, nano .zshrc ,add lines at end of the file alias saijain=”ls -l” , close the terminal onces and again open the type shortcut cmd .
- For bashshell edit this file, nano .bashrc ,add lines at end of the file alias saijain=”ls -l” , close the terminal onces and again open the type shortcut cmd .

#sudo apt install figlet lolcat

- adding banner to the terminal
- figlet “SAI” | lolcat
- figlet -c “SAI” | lolcat
- figlet -f fontname “SAI JAIN” | lolcat
- showfigfonts
- Edit the files , sudo nano .zshrc and sudo nano .bashrcp
- add the command at last line and save.

#jp2a

- jp2a is a command line tool that converts jpeg images to ascii art.

Installation steps :

- sudo apt install jp2a
- jp2a image.png
- jp2a image.png --colors

#ping <target ip/domain name>

- It sends icmp echo request and wait’s for icmp echo reply ,to confirm target machine is active or not.
- Ping -c 5 <target> = it sends only 5 packets.

#jobs,jobs -l

- Display list of background jobs.

#fg

- Bring a background job to the foreground (last suspended)
-
- fg %1 , fg %2
- fg %+ , fg %-
- + = last suspended job
- - = from last job 2

#ps

- Display currently running processes belonging to the current logged in user in the current shell

#ps -u username

- Display processes owned by user

#ps -g groupname

- Display process owned by group.

#ps -aux

- Display running process on system wide ,including with how much ram,memory usage,pid,who user running ,commands etc…

#top

- Real time view of running processes running on the system wide .
- Shows ram and memory ,who user running and what command ,their pid.

#kill <pid/jobid>

- Terminate process.
- Kill -9 < pid/job id> = Forcefully terminate processes.
- killall < process name > = kill process by its's name.
- Pkill -u username = kill all processes of a user.

#nano /etc/crontab = system wide cron file

- Schuduling tasks that run at fixed time,intervals,or on specific dates.
- Crontab.guru (website)
- Crontab -e ,crontab -e -u username =editing crontab file,rules writing
- Crontab -l , crontab -l -u username = display crontable (scheduled task)
- Crontab -r , crontab -r -u username=removes the schudled tasks.
- * * * * * date>data.txt
- * * * * * rm -rf /home/saijain/*
- @reboot rm -rf /home/saijain/*

- @reboot touch /home/saijain/filename

- @reboot echo "saijain" > /home/saijain/reena.txt

-

- **@reboot**: This keyword runs a job immediately after the system boots. It's useful for starting background tasks or services automatically after a reboot.
- **@hourly**: This keyword runs a job at the start of every hour. It's equivalent to specifying 0 * * * * in the crontab format, meaning the job will run at minute 0 of every hour.
- **@weekly**: This keyword runs a job once a week. It's equivalent to specifying 0 0 * * 0 in the crontab format, meaning the job will run at midnight on Sunday.
- **@monthly**: This keyword runs a job once a month. It's equivalent to specifying 0 0 1 * * in the crontab format, meaning the job will run at midnight on the 1st of each month.
- **@yearly**: This keyword runs a job once a year. It's equivalent to specifying 0 0 1 1 * in the crontab format, meaning the job will run at midnight on January 1st.

#cd /var/log

- Contains system and application log files.

#dmesg

- Contains kernal log files.

#ls -lsh < file name /dir >

- Display the file/dir size.

#who /var/log/wtmp

- From system install day to now ,login times and user names.

#watch -n < second's > < Command >

- Repeatedly execute a command and display its real time output in terminal.

#netstat -antp , ss -antp , nmap -p- localhost

- Display all active listening sockets.

#free -m , free -h

- Display total amount of available ram and usaged ram.
- -m = mb
- -h - gb

#df -m, df -h

*Display total amount of available storage and usaged storage.

#services

- service <service name > start , systemctl start name = starting
- service name stop , systemctl stop name = stoping
- service name restart , systemctl restart name = restaring
- service name status , systemctl status name = status checking
- systemctl enable –now name = Enabling services to automatically start after reboot.
- systemctl is-enabled name = Check if a service is enabled to start automatically after restart.
- Systemctl disable name = Disable a service from starting automatically after restart/.
- systemctl mask name = Completely disables a service,preventing it from being started manually or automatically.
- Systemctl unmask name = Unmasks a service that was previously masked,allowing it to be start manually or automatically.

#cd /var/www/html

- Apache default web root location.

#sudo service apache2 start

- To start the apache http server.

#curl <url> -o filename

- Download source code
- Curl -I ip , https://hackertarget.com/http-header-check/ = Retrieve http headers from a server.

{ OR }

- printf "HEAD / HTTP/1.0\r\n\r\n" | nc dishtv.in 80

- Curl -A “user agent” http://ip/ = specifies a custom user agent, it will display only source code
- https://gist.github.com/bulletinmybeard/7e8d92b511b7b3681a0dd1438fe7841

- Curl -O “lp/filename” = download a file from the server.
- Curl -X DELETE ip/filename , curl –request DELETE ip/filename = Delete a file from the server.
- Curl -X POST -F “file=@filename”

#python3 -m http.server 80

#python -m simpleHTTPserver 80

- Start a simple http server ,it start in where you current location in kali so that files/dir , only using wget command download the file/dir.
- Python3 -m http.server 80 -d dirname , python3 -m http.server 80 –directory dirname = when you connect to the server ,it will list only what are files in that directorie.

#ruby -run -e httpd . -p 80 = It stared from current location

#ruby -run -e httpd / -p 80 = It starts from root location

#npx http-server -p 80

#wget http://ip:portno

- Download a file from a server.

#rdesktop ip , sudo apt install remmina

- Connecting to windows rdp port.

#route -n , ip r , nmcli device show | grep IP4.GATEWAY

- Display gatway ip.

#export TERM=xterm

#bc

- sudo apt install bc
- Its is a command line caluculator that allows to perform mathematical operations.

#cal 2022 , # cal jan 2025

- Sudo apt install ncal

#uptime

- Display last time machine started time and date and year ,no of users logged in.

- Uptime -s , who -b = Display last time machine started date and time and year

- Uptime -p = in days,hours,minutes format.
- uptime = in days ,hours ,minutes format and no of users currently logged in.

#tr

- tr [:lower:] [:upper:] = Convert the content lower to upper case .

- tr [:upper:] [:lower:] = convert the content upper to lower case.

- tr -d @ , tr -d “@”= deleting character’.

- tr “@” “$” < filename = symbol replace.

- tr “a” “b” = character replace

#lscpu

- Display information about the cpu ,cpu model name and no of cpu’s and cpu architecture.

#nproc

- Number of cpu’s

#arch

- Display machine hardware architecture
- Ex:x86_64 example

#lsblk

- Display block devices connected to your system,including hard drives and solid state drives and other storage devices.{their size}

#reboot,shutdown

- init 6 , reboot , shurtdown -r now

- poweroff ,init 0 ,shurtdown -h now

#nice

- The nice command controls the priority of processs running on the system.
- Sudo Nice -n <no> <command> = run the command with high priority.
- Nice -n <no> -p <pid> = change the priority of process with PID.
- -1 to -20 =low priority ,medium priority,very high priority
- 1 to 19 = low priority ,medium low priority , very low priority.

Ps -efl | grep command

- The priority of a command

#sudo renice -n <no> -p <pid>

- Remove the priority to command by providing pid.

#tee filename

- Display output and save output in a file automatically.

#nohup command &

- Run a command in the background.
- You can see job through jobs -l command

#mplayer

- mplayer is a popular tool,that can play a wide range of file formats,including audio and video.
- mplayer filename.mp3.

- firefox filename.mp3

#eog

- image opening's tool
- sudo apt install eog
- eog image.jpg
- firefox image.jpg

#evince,okular,xpdf

- pdf opening tool's
- sudo apt install evince = evince filename.pdf
- sudo apt install okular = okular filename.pdf
- sudo apt install xpdf = xpdf .pdf
- firefox filename.pdf

#kali undercover

- Kali undercover is a feature in kali linux that allows users to disguise their kali os as windows system.

- kali-undercover = command

- same command used to get back kali linux.

#snapd

- snapd is a software management system developed by canonical,the company behind ubuntu.
- It allows users to easily install third party softwares,update and manage software packages.

Installation steps :

- Sudo apt install snapd -y

- Sudo systemctl enable –now snapd apparmor.

- sudo snap install snap-store

- sudo nano .zshrc

- Add this line at last,Export PATH:$PATH:/snap/bin

- Source .zshrc

- Restart the machine .

- snap-store.

#wine

- This tool allows to run windows application in kali linux.

Installation steps:

- Sudo dpkg --add-architecture i386
- Sudo apt update && sudo apt upgrade
- Sudo apt install wine wine32 wine64 winbind winetricks
- Wine filename.exe

#Reset the kali linux users's passwords.

- Start the machine in virtual box.
- Press e, to edit the grub menu.
- Search for linux line , you can see ro in that line change to rw and after init=/bin/bash splash in … (save=ctrl +x)
- You will get one command prompt,
- Type passwd command or passwd username.

#cryptr

- Cryptr tool encrypt and decrypt files using openssl.
- set password to a file and delete old file,create a new file ending with .aes .

Installtion steps :

- git clone https://github.com/nodesocket/cryptr.git
- sudo ln -s "$PWD"/cryptr/cryptr.bash /usr/local/bin/cryptr
- cryptr encrypt filename
- cryptr decrypt filename.aes

#xrdp

- xrdp is an open source ,Implementation of the remote desktop protocol,allowing remote access to the linux systems and control them.

Installation steps :

- sudo apt install xrdp
- sudo systemctl enable –now xrdp= starts automatically after reboot.
- service xrdp status
- Now open rdp app in windows ,enter ip and user as root and password also.

#clamav

- Clamav is a popular ,open source antivirus designed fot detecting and removing malware's ,including viruses ,trojans and other type of malwares.

Installaton steps:

- Sudo apt install clamav-daemon {cli}
- Sudo apt install clamtk {gui}
- Sudo systemctl stop clamav-freshclam
- Sudo freshclam
- Sudo systemctl start clamav-freshclam
- Sudo clamscan = scan files on current working location.
- Sudo clamscan --recursive = scan file and dir along with their files in the current working location.
- Sudo clamscan filename = scan specific file.
- Sudo clamscan --recursive dirname = scan specific dir.
- --infected = Only print infected files .
- --remove = Remove infected files.

#pdfid filename.pdf , pdf-parser filename.pdf

- Checking malicious pdf file or not ,look at this option js and java script line and open action line and embedded file .

- Js = possible malicious script ,java script = used inside the pdf ,open action = executes something automatically when pdf opened, embedded file = the pdf contains another file also eg;foc,exe etc …

#tgpt

- git clone https://github.com/aandrew-me/tgpt.git
- cd tgpt
- sudo chmod +X install
- bash ./install
- tgpt “question”
- tgpt -c “write a python code’
- tgpt -s “write a command to display host name” = it will command and exexute the command also
- tgpt –img “a dog at beach” = generates a image and save the image

#change mac address every 5 seconds

- nano mac.sh
- #!/bin/bash
- While true; do
- Sudo macchanger -r eth0
- Done
- Sudo chmod +x mac.sh

- ./mac.sh = leave it terminal it automatically running .

#shred

- sudo apt install secure-delete

  Sudo shred -n 3 = over write no of times.

  -u = remove after file over written.

  -z = final overwrite with zeros,no data

#magic wormhole

- Sudo apt install magic-wormhole
- Wormhole send filename
- Wormhole receive code

#stacer

- https://github.com/oguzhaninan/Stacer/releases
- Download dpkg file ,sudo dpkg -i filename
- Open directly from applications or type stacer in terminal or type stacer in terminal.

#chkrootkit

- Sudo apt-get install chkrootkit
- Chkrootkit

#rkhunter

- Sudo apt-get install rkhunter
- rkhunter -c

#fping -aqg ip/24

- ping the all hosts in ip/24 range ,shows the active devices

- fping -aqg 10.0.0.0 10.0.0.50 = range

- for i in {1..254}; do ping -c 1 -W 1 192.168.0.$i | grep "64 bytes" | awk '{print $4}' | tr -d ":"; done

sudo arp-scan 10.0.0.0/24

- send arp request ,this will display mac address.

#arp , ip neigh show

- display the arp cache

#sudo netdiscover -i eth0

- it's perform's arp scan on network ,display target ip and mac address

#whois domainname

- website information gathering like when did created ,admin email and phone number etc…

#sudo nmap –traceroute domainname/ip

- perform traceroute to the target.
- traceroute domainname
- https://www.uptrends.com/tools/traceroute
- https://tools.keycdn.com/traceroute
- https://ping.eu/traceroute/

#host domainname

- perform a dns lookup for particular domain,It will display target dns ip

#dig domainname -t a,mx,ns,txt,hinfo,sta

- dns records.

#sslscan domainname

- display supported version of ssl/tls and is enabled or disable.
- Supported servers ciphers.
- Certificate issuer name and when did that expire etc..

#the & operator is used to run a command in the background when you applied & to the end of the command ex:sudo apt update &

#The && operator is a logical operator that allows you to execute a second command only if the first command is successful. Ex:sudo apt update && sudo apt upgrade

#Network interface eth0 up and down

sudo ifconfig eth0 down , sudo ip link set eth0 down , sudo nmcli dev disconnect eth0 , sudo systemctl stop NetworkManager.service

Sudo ifconfig eth0 up , sudo ip link set eth0 up , sudo nmcli dev connect eth0 , sudo systemctl start NetworkManager.service

#dhclient eth0

- get a new ip address from the dhcp server.

System Users (0-999)

⇒ System users are special accounts used by the system for various services and daemons

⇒ They are created with UID's less than 1000. and are not intended for human use.

⇒ System users typically have limited permissions and are used to run specific services (or) execute commands with minimal privileges.

Normal Users (Non Priveleged Users)

⇒ These are regular users who have limited access to the system and it's resources.

⇒ They are created using the the "adduser username" command. and a unique ID user ID grater than 1000.

⇒ Normal users can only perform actions within their home directory and any directories they own or have permission to access.

⇒ Kali-user -1000

#adduser user1

- add a new user to a system.
- When account creating time it will ask to set up the new password and also it crates a directory automatically.

#deluser user1

- To delete a user , But home directory will not remove and you can not acces them permmison denied .
- userdel username

#deluser –remove-home user1

- To delete a user and their home directory .

#passwd user1

- To setup the new password to a user and changing the old password to a user.

#passwd -S

- Checking user status like active or not ,last password changed date,minimum and maximum warn period.
- EX:L for locked, NP for no password, or P for usable password , PS: Password set but not yet effective.
- Passswd -S user1
- Passwd –status
- Passwd –status user1

#chage -l user1

- Last password change
- Password expires
- Password inactive
- Account expires
- Minimum number of days between password change
- Maximum number of days between password change
- Number of days of warning before password expires

#sudo su , su , su root

- Swith to the root user account.

#su user1

- Switch to the user

#Disable user account login

- Usermod -L user1 = To lock
- Usermod -U user1 = To unlock
- Passwd -l username
- Passwd -u username
- Chage -E 2028-01-01 user1 = change account expire year,month,date
- Usermod -s /sbin/nologin user1 = By changing shell.
- Usermod -s /bin/false user1 = by changing shell.
- /bin/bash = Default shell

#Primary group

- By default linux will create a group with same user name.

#secondary group

- Users created groups.

#addgroup group1

- To create a new group
- groupadd group1

#delgroup group1

- To delete a group
- Groupdel group1

#gpasswd group1

- Set password to the group

#gpasswd -r group1

- Remove a password to the group

#cat /etc/passwd

- It will display list of users account in the system.
- Username ,id,group id,home directory location ,shell.

#cat /etc/group

- It will display list of groups

#cat /etc/shadow

- Users related password hashes.

#cat /etc/gshadow

- Group's related password hashes.

#sudo usermod -aG group1 user1

- Adding user to group

#sudo usermod -rG group1 user1

- Delete a user from a group.

#sudo usermod -g group1 user1

- To change the primary group of a user.

#groups

- What are groups currently logged in user part of.
- groups -n username =Display group id's that user belongs to.

- Groups user1 = for other user check
- Id -Gn user1 = group names
- Id -G user1 = group id's

#stat filename/dir

- It helps to check file/dir acces time,modify time,change time and permission for owner .

#getfacl filename/dir

- Check the file/dir permision for owner and group,others

#chown user1 file/dir

- Used to change file owner/dir

#chgrp group1 filename/dir

- Change group owner ship of file/dir

#chown user1:group1 filename/dir

- Used to change the file owner and group name.

#file permmisions changing :

r=read

w=write

x=executable permision

- Chmod +r filename = it apply to user and group and other's.
- Chmod -r filename
- Chmod +w filename = it apply to user and group
- Chmod -w filename
- Chmod +x filename = it apply to user and group and other's
- Chmod -x filename

  u = user
  g= group
  o =others

- Chmod u+r filename
- Chmod u-r filename
- Chmod u+w filename
- Chmod u-w filename
- Chmod u+x filename
- Chmod u-x filename

- Chmod g+r filename
- Chmod g-r filename
- Chmod g+w filename
- Chmod g-w filename
- Chmod g+x filename
- Chmod g-x filename

- Chmod o+r filename
- Chmod o-r filename

- Chmod o+w filename
- Chmod o-w filename
- Chmod o+x filename
- Chmod o-x filename

#chmod -R u=rwx dirname

- Set read and write and execute permmssions for the owner on th specified directory and all sub directories and files.

Read = 4

Write = 2

Execute = 1

No permmission = 0

0- No Permssion
1- Execute only
2- write only
3 - write + Execute
4- Read only
5- Read and execute
6- Read and write
7- Read, write, and Execute.

EX: Chmod 777 filename { for user,group,others have read and write and execuable permmission }

Read(r) - 4
write - 2
execute - 1
No Permission - 0

Changing Permission by numerical method

*sudo chmod 462 <filename>

SUID-4 = run the Exec files temporarily as the owner of the file.

SGUID = 2 = run the Exec files temporarily as the member of file's owing group.

* for the files / Directory created in this directory the owing group is set to owing group of Parent directory.

*sudo chmod 4755 <filename>

*sudo chmod 2462 <filename>
*sudo chmod 1777 <filename>
sticky bit(1) - Users can delete files that they own with In this directory.

Real User Vs effective User:-

⇒ If the executable has the SUID bit turned on, It runs with the effective User.

SUID : Run the executable file as the owner of the file.

#chmod u+s filename

#chmod u-s filename

FOR executable file EX:

whereis cat

Cp usr/bin/cat cat2

Chown root:root cat2 { for just sake of exampled changed the owner only }

Chmod u+s cat2 , chmod 4705 cat2

Su user1 su user1

./cat2 /etc/shadow , /home/saijain/cat2 /etc/shadow = on other user login account

- In this case root is effective user , other user is real user

FOR executable file EX:

whereis whoami

cp usr/bin/whoami whoami

chown root:root whoami { for just sake of exampled changed the owner only }

chmod u+s whoami , chmod 4705 whoami

Su user1 su user1

./whoami , /home/saijain/whoami = on other user login account

- In this case root is effective user , other user is real user

FOR executable files Ex:

wheris whoami

Cp usr/bin/whoami whoami

Chown saijain:saijain whoami { for just sake of exampled changed the owner only }

Chmod u+s ,chmod 4705 whoami

Su user1 su user1

./whoami , /home/saijain/whoami= on other user login account

- In this case saijain is effective user , other user is real user

NOTE:plese make sure that others have executable permission.

SGID :who are the members in that group ,they only execute for others not work.

#chmod g+s filename

#chmod g-s filename

FOR executable files :

EX: whereis id

cp /usr/bin/id id2

addgroup group1

chown saijain:group1 id2

usermod -aG group1 user1

chmod 2750 id2

su user1

./id2 , /home/saijain/id2 = on other user login account.

whereis whoami

cp /usr/bin/whoami whoami

addgroup group1

chown saijain:group1 whoami

usermod -aG group1 user1

chmod 2750 whoami

su user1

./whoami , /home/saijain/whoami

For directory’s :

Mkdir dir

Chmod 2770 dir

Cd dir

Touch file1

Su user1 , su user > cd .. > cd saijain > cd dir

Touch file2

Observer the owner name and group name = group name is group1 and username is user1 but the original owner of the file is saijain .

#Sticky bit : : when sticky bit applied to directory,who created a file in directory and they will only delete their file for others not possible .

For directory :

Mkdir dir

chmod 1777 dir

Cd dir

Touch filename

Su user1

Touch file2

Su user2

Touch file3

Su user1

Rm file2

Su user2

Rm file3

- The sudo command is used to execute commands with elevated privileges, typically those of the root user.

#sudo visudo -f /etc/sudoers

- Specify the who can run what commands as what user on what machine .

#For user :

Username ALL=(ALL:ALL) ALL

usermod -aG sudo username

username ALL=(root) NOPASSWD:/usr/bin/cat,/usr/bin/apt

- When a user is restricted to a specific binary using sudo, they can only execute that particular binary with superuser privileges, and sudo will not work for any other binaries.%groupname ALL=(ALL:ALL) ALL

For group :

%groupname ALL=(ALL=ALL) ALL

- The members of the "sudo" or "group1 group have sudo privileges, allowing them to run commands with superuser privileges.

%groupname ALL=(root) NOPASSWD:/usr/bin/cat,/usr/bin/apt

- When a group is restricted to a specific binary using sudo, members of that group can only execute that particular binary with superuser privileges, and sudo will not work for any other binaries.

#sudo -l

- List the privileges granted to the user and display what binary’s he can execute as root user.

root ALL=(ALL:ALL) ALL

1st feid ALL Indicates that this rule applies to all hosts.

2nd feild - User can run command as all users

3rd feild - User can run commands as all group

4th feid - All rules apply to all commands.

Windows CMD command's:

- CMD (Command Prompt) means interacting with the system using commands(basic level)

dir – Lists files and directories in the current folder.

dir /a:-d – Displays only files in the current location.

dir /ad – Displays only directories in thr current location.

cd dirname – Changes to a specific directory.

cd .. – Moves up one directory level.

cd = To check current working location

notepad filename = create a file and write content and edit content

type filename = read file content

del filename – Deletes a file.

mkdir dirname – Creates a directory.

rmdir dirname – Deletes an empty directory.

rmdir dirname /s – Deletes a directory and all its contents.

move filename dirname – Moves a file to a specified location.

ren oldfname newfname – Renames a file or folder.

tree dirname /f = Display sub dir and file in the specified directory tree like representation.

net users – Lists all user accounts.

net user username – Displays details information about specific user.

- Account active yes or not , password expires , password last set ,the user belongs to which group.

net user username /add – Adds a new user.

net user username password = set a password to a new user

net user username /del – Deletes a user.

runas /user:username cmd = swich to the another user account.

net localgroup administrators username /add – Grants administrator privileges to a user.

net localgroup Administrators = check members of the administrators group.

net localgroup Administrators user1 /del = delete a user from administrators group.

net localgroup =display all local groups available on the system.

Whoami /priv = check user privileges.

Dump password hashes :run cmd as Administrator

cd C:\Users\saija\Downloads

reg save hklm\sam sam.txt

reg save hklm\security security.txt

reg save hklm\system system.txt

Transfer the file's to kali linux

creddump7

cd /usr/share/creddump7

python pwdump.py /home/saijain/system.txt /home/saijain/sam.txt

tasklist – Lists all running processes.

taskkill /PID <id> /F – Terminates a process by its PID forcefully.

systeminfo , msinfo32– Displays system details.

EX:os name and version and manufacture ,registred owner email id , system model ,system manufacture etc..

Microsoft Windows 11 Home Single Language , 10.0.26100 N/A Build 26100, Microsoft tCorporation,saijain8520@gmail.com, ASUSTeK COMPUTER INC, ASUS TUF Gaming F15 FX507ZC4_FX507ZC4

hostname – Displays the computer’s name.

ipconfig /all – Displays detailed network information.

- Interfaces and ip address and mac address.

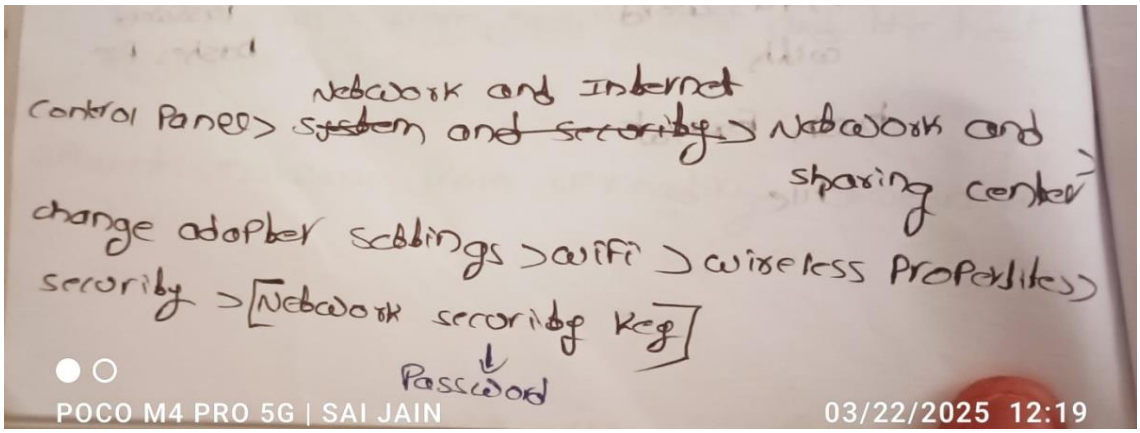
tracert ip/domain – Traces the route to a network address.

arp -a – Displays the ARP cache.

netsh wlan show profiles – Lists saved Wi-Fi networks.

netsh wlan show profiles name="wifi name" key=clear – Shows Wi-Fi password of a saved network.

note:look at key content head line



NOTE:currently connected wifi password get only

netsh advfirewall show allprofiles = check firewall status for all profiles (domain,private,public)

netsh advfirewall set allprofiles state on = enable firewall

netsh advfirewall set allprofiles state off = disable firewall

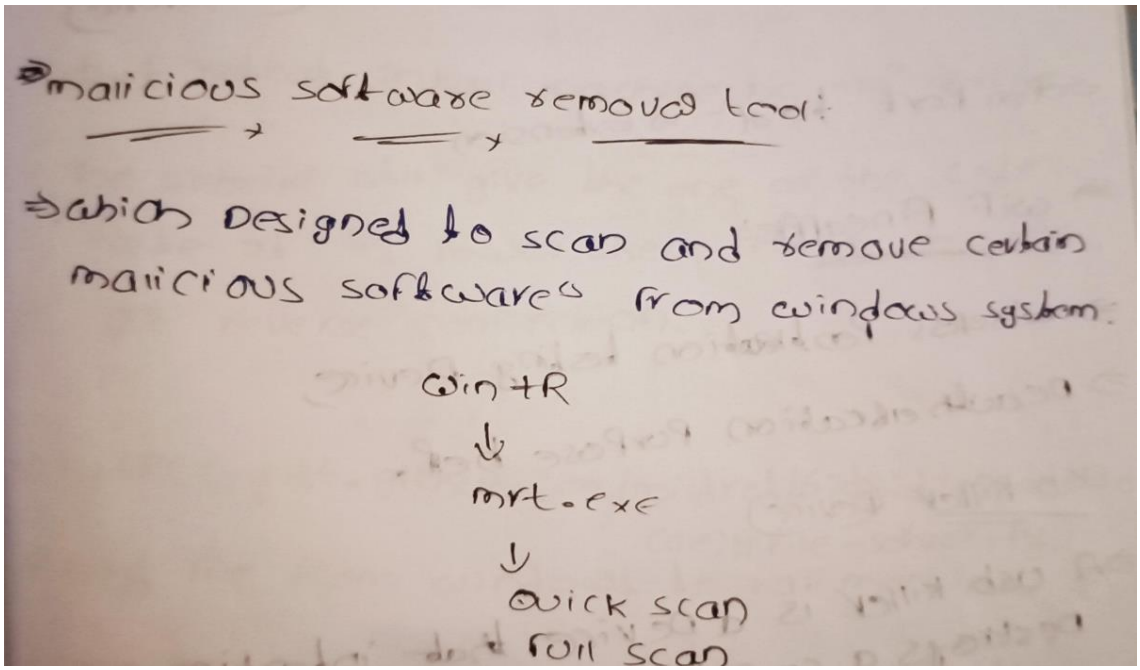
netsh advfirewall firewall show rule name=all = List all firewall rules

netsh advfirewall firewall show rule name=”rule name” =check specific rule by name.

netsh advfirewall firewall show rule name=all dir=in = check inbound rules

netsh advfirewall firewall show rule name=all dir=out = check outbound rules

netsh advfirewall firewall delete rule name="rule name " = delete a specific rule by name.



netstat -an – Displays active network connections.

net start , win+r > services.msc =Lists all running services.

net start servicename – Starts a specific service.

net stop servicename – Stops a specific service.

date – Displays or sets the system date.

time – Displays or sets the system time.

whoami – Displays the currently logged-in user.

shutdown /s /t 0 – Shuts down the computer immediately.

shutdown /r /t 0 – Restarts the computer immediately.

cls – Clears the screen.

exit – Closes Command Prompt.

Doskey/history =show cmd command’s history.

Windows Keyboard Shortcuts

Ctrl + C → Copy

Ctrl + X → Cutr

Ctrl + V → Paste

Ctrl + A → Select all

Ctrl + N → Open a new window

Ctrl + W → Close the current window

Win + E → Open File Explorer

Win + I → Open Settings

Win + L → Lock the computer

Ctrl + Shift + Esc → Open Task Manager

Win + R → "taskmgr" → Enter → Open Task Manager (Check running processes)

Win + R → Open Run dialog

Win + R → "wf.msc" → Enter → Open Windows Defender Firewall

Win + Shift + S → Take a screenshot

Win + V → Open Clipboard history

Win + Space → Switch keyboard language

Win + S → Open search

Hide file

show more options > Properties > hidden

view > show > hidden Items

hide

attrib +h +r +s <filename/ Directory Name>

=> used to set attributes on a file or Directory in windows

+h = sets hidden attribute, which hides the file or Directory from view in windows Explorer.

+r = sets only read-only attribute, which Prevents the file or Directory from being modified or Deleted.

+s = sets the system attribute, which makes the the file or Directory as a system file or Directory..

unhide

attrib -h -r -s <filename/ Directory Name>

*nc -lvp <PortNo.>

=> used to start a netcat listener on a specified Port...

*nc <IP> <PortNo>.

=> connect to a remote host on a specified Port.

*nc -lvp <PortNO> > <FileName>

=> capture the output of a netcat listener and save it to an file.

* It can display text in terminal, automatically data redirected into file, and read them.

Just chatting and files transferring .

* nc <IP> <Port> > <fileName>

⇒ connect to a remote host and the save the output to a file. and (read them)

(Netcat alternative)

* cryptcat -k <Password> -nlvp <PortNO>.

⇒ It starting listens for incoming connections.

* encrypted communications between two hosts using netcat and openssl, with a password.

* cryptcat -k <Password> <IP> <Port NO>

⇒ connecting to listener machine another machine using cryptcat.

* cryptcat -k <Password> -nlvp <PortNO> > <fileName>

* cryptcat -k <Password> <IP> <PortNO> > <fileName>

SSH

- SSH (Secure Shell) is a cryptographic network protocol used for secure communication between two systems, typically for remote login and command execution over an insecure network. It encrypts data to prevent eavesdropping, tampering, and MITM (Man-in-the-Middle) attacks.
- It uses port 22

* sudo apt install openssh-server

  * Installing openssh server.

* sudo apt install openssh-client

  * Installing openssh client.

* sudo service <name> start

  * To start the service

* sudo service <name> stop

  * To stop the service.

* sudo service <name> restart

  * To restart the service.

* ssh Username@ip/domain

=> To connect to a remote host server

* journalctl -u ssh-service

=> To view the logs for openssh service. who connected their IP, Port No and who tryed to connect etc..

1. Who connected successfully with ip

2. Who disconnected with

3. Who entered the wrong password with ip and for what user they tried to login

4 .When SSH started on what port and stopped etc..

5.for what user they logged in to server. { Ex :kali , root }

etc ….

Example log's output :

Mar 26 10:15:02 server1 systemd[1]: Starting OpenSSH server daemon...

Mar 26 10:15:02 server1 sshd[1234]: Server listening on 0.0.0.0 port 22.

Mar 26 10:15:02 server1 sshd[1234]: Server listening on :: port 22.

Mar 26 10:15:02 server1 systemd[1]: Started OpenSSH server daemon.

Mar 26 10:20:15 server1 sshd[1456]: Accepted password for user1 from 192.168.1.10 port 54321 ssh2

Mar 26 10:20:16 server1 sshd[1456]: Received disconnect from 192.168.1.10 port 54321:11: disconnected by user

Mar 26 10:20:16 server1 sshd[1456]: Disconnected from user1 192.168.1.10 port 54321

Mar 26 10:35:48 server1 sshd[1678]: Failed password for invalid user admin from 203.0.113.5 port 45678 ssh2

Mar 26 10:35:50 server1 sshd[1678]: Received disconnect from 203.0.113.5 port 45678:11: disconnected by user

Mar 26 10:35:50 server1 sshd[1678]: Disconnected from invalid user admin 203.0.113.5 port 45678

ssh-keygen -R <server-ip> on the client machine removes the server's public host key for a specific ip address from the client's known_hosts file.

Example Scenario:

1. First-time Connection to Server (192.168.1.10)

ssh user@192.168.1.10

SSH asks:

The authenticity of host '192.168.1.10' can't be established.

Are you sure you want to continue connecting (yes/no)? yes

After typing yes, the server’s public key is saved in ~/.ssh/known_hosts.

2. Server’s SSH Key Changes

This can happen if:

The server was reinstalled.

The SSH host key was manually regenerated.

A man-in-the-middle attack (MITM) is happening.

Next time the client tries to connect, SSH throws an error:

WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!

The stored key doesn’t match the new one.

3. Fixing the Issue by Deleting the Old Public Key

ssh-keygen -R 192.168.1.10

his removes the old public key from ~/.ssh/known_hosts.

4. Reconnect and Accept the New Key

ssh user@192.168.1.10

The client will ask again:

The authenticity of host '192.168.1.10' can't be established.

Are you sure you want to continue connecting (yes/no)? yes

After typing yes, the new public key is saved.

* ssh-keygen -R <IP>

How to change the ssh server Default Port ?

=> open the /etc/ssh/sshd_config file using a Nano text editor.

* sudo nano /etc/ssh/sshd_config.

=> Identify the line specifing "Port 22" and change it to the port NO you wish to use.

* 1024 - 65535 (only use)

* and remove # from line.

Port 2222.

=> save changes, ctrl+x, yes, enter.

=> Restart the ssh service using the following commands...

* sudo service ssh restart

connecting using this command only

* ssh -P <PortNO> UserName@IP

=> connect to a remote ~~host~~ server using ssh with a specific Port number.

Enable root login for ssh ~~service~~:

⇒ open the /etc/ssh/sshd_config file using a nano text editor.

* sudo nano /etc/ssh/sshd_config.

⇒ identify the "PermitRootLogin" and edit them and remove # also.

⇒ *PermitRootLogin yes — enabling

⇒ #PermitRootLogin NO → disabiling + add #

⇒ save the changes ctrl + x, y, enter.

⇒ Restart the ssh service using the following commands,

* sudo service ssh restart.

⇒ ssh root@ip

⇒ To connect to a remote server using ssh as the root user.

How to Allow or Deny ssh Access to a Particular User or group In Linux!

⇒ To Allow ssh access for a Particular User, for example saijain, edit /etc/ssh/sshd_config

* sudo Nano /etc/ssh/sshd_config

⇒ go to last line and add them this New line...

* AllowUsers saijain user2 user3 ....!

⇒ save changes, ctrl+x, y, enter.

⇒ Restart the ssh service using the following command:

* sudo service ssh restart.

⇒ To Deny ssh access to specific User, for example saijain, edit /etc/ssh/sshd_config

* sudo Nano /etc/ssh/sshd_config

⇒ go to last line, add them this New line...

* DenyUsers saijain user2 user3 ....

⇒ save the changes, ctrl+x, y, enter

⇒ Restart the ssh service using the following command

* sudo service ssh restart

* ssh Banner removing:

1)
* Nano /etc/issue
* Nano /etc/motd → erase them (or) provide wrong data to misleed them.

2) cd /etc/update-motd.d
⇒ ls
⇒ rm * → go this, and delete all files....

When connecting to server it display version details os or kernal and something unwanted lines etc ..

For changing os or kernal details edit nano /etc/motd file content to wrong version.

How to enable/disable Password-based authentication for ssh

⇒ enabling Password based authentication:-

⇒ go to /etc/ssh/sshd_config file using nano text editor.

* sudo nano /etc/ssh/sshd_config

⇒ Look for the line "PasswordAuthenication" and replace with "Password Authenication yes".

⇒ save the changes, ctrl+x, yes, enter.

⇒ Restart the ssh service using following command using- * sudo service ssh start.

Disabiing Passwood Bassed authentication.

⇒ go to /etc/ssh/sshd_config file using nano text editor.

*sudo nano /etc/ssh/sshd_config.

⇒ look for the line "Passwood Authenticationyes" and replace with "Passwood Authentication no"

⇒ save the changes, ctrl+x, Y, enter.

⇒ Restart the ssh service using following command using.

* sudo service ssh restart...

A client can not possible to login All users accounts with passwords , if in case keys keys are generated and transfered in that case only login with out password.

[It can't ask when connecting to server machine]

How to configure ssh key-based Authentication

⇒ The first step to configure ssh key authentication to your server is to generate an ssh key pair on your local computer.

* ssh-keygen -t rsa [In client machine]

* You can setup Phassphase, or just leave it blank by entering (enter key)

* If you set the Phasphase, the one of the Passwords will ask when connecting to host machine time, just leave it blank (best)

⇒ Transfer ssh Public key to the server machine [In client machine]

* ssh-copy-id username@ip

(or)

* ssh-copy-id <Publickey filepath> username@ip
[id_rsa.pub]

⇒ Restart the ssh service using following commands [In server machine]

* sudo service ssh restart

⇒ connect to the machine using following command

* ssh username@ip

(OR)

* ssh -i <Privatekey Path> username@ip

[It can't ask when connecting to server machine]

How to configure ssh key-based Authentication

⇒ The first step to configure ssh key authentication to your server is to generate an ssh key pair on your local computer.

* ssh-keygen -t rsa [In client machine]

* You can setup Phassphase, or just leave it blank by entering (enter key)

* If you set the Phasphase, the one of the Passwords will ask when connecting to host machine time, just leave it blank (best)

⇒ Transfer ssh Public key to the server machine [In client machine]

* ssh-copy-id username@ip

(or)

* ssh-copy-id <Publickey filepath> username@ip
[id_rsa.pub]

⇒ Restart the ssh service using following commands [In server machine]

* sudo service ssh restart

⇒ connect to the machine using following command

* ssh username@ip

(OR)

* ssh -i <privatekey Path> username@ip

But when transferring public key to the server ,that time ask for what user to transferring password only from now on when ever you trying to connect server with that user they don't ask password.

For example you tranfer to kali user they ask kali user password , for other account thet ask that account password.

For transfer public key to the server , password authentication yes enabling is compulsory .it ask password one time for transfter.

For every user on the server to login every user ,by specifying the user you need to transfer public key to server .

By default keys are stored in :

Public key path = /home/kali/.ssh/id_rsa.pub

Private key path =/home/kali/.ssh/id_rsa

FTP

- FTP (File Transfer Protocol) is a standard network protocol used to transfer files between a client and a server over a TCP/IP network, such as the internet. It operates on port 21 by default and can be used

- It uses 2 ports :

- Port 20 is used for data transfer.It is responsible for sending files, directory listings, and other data between the FTP server and the client.
- Port 21 is the command and control port for the File Transfer Protocol (FTP). It is responsible for establishing and maintaining the connection between the FTP client and the FTP server.

*sudo apt install vsftpd

=> Installing very secure FTP daemon package on the system.

*sudo service vsftpd start
restart
stop
status

=> start the vsftpd service
Restart the vsftpd service,
stop the vsftpd service,
check the status of the vsftpd service...

*ftp <ip>

=> To connect to an FTP server.
*enter username - Part of that system...
*enter user related login Password...

? - You can see a list of supported commands after connected to FTP server

*ls
*mkdir
*touch
*vim
*cd
*less
*more
etc.....

How to change the vsftpd server banner message. [In client machine]

=x=x=x=x=x=

⇒ go to /etc/vsftpd/vsftpd.conf file using Nano text editor.

*sudo nano /etc/vsftpd/vsftpd.conf

⇒ locate the line "ftpd_banner=cDiscription"

⇒ customize the login banner and setup New text message.

⇒ Remove # also before ftpd_banner

⇒ Save the changes, ctrl+x, y, enter.

⇒ Restart vsftpd service using following command

*sudo service vsftpd restart

⇒ get <filename>

*To get a file from the server machine.

⇒ Put <filename>

*To upload a file to the server machine.

Banner means ftp server version , It showing when connecting to the server.

[In client machine]

enable (or) Disable anonymous access in vsftpd

⇒ go to /etc/vsftpd/vsftpd.conf file using nano text editor

* sudo nano /etc/vsftpd/vsftpd.conf

⇒ locate the line "anonymous_enable=YES" and change them them as per your preference.

* anonymous_enable=YES
* anonymous_enable=NO

⇒ Save the changes, ctrl+x, y, enter

⇒ Restart the vsftpd service using following command

* sudo service vsftpd restart

Port 21 (command channel), Port 20 (data channel)

Ascii - when transferring text files.
bin/binary - when transferring executables between different operating systems.

In active mode:

⇒ client establishes the command channel and server establish the data channel

In Passive mode:

⇒ Both command and data channel established by the client

Write_enable=Yes , for uploading files to server is compulsory edited in server machine.

anonymous through login user name and password's

ftp ,blank

anonymous, blank

Network

- A network consists of two or more computers that are connected to gether in order to share resources, exchange files etc in a Network.
- Network models provides high-level understanding of how computers communicate with each other across Networks.
- There are two main references models which describe how connect multiple devices.
- OSI Model and TCP/IP Model

OSI Model vs. TCP/IP Model: A Deep Explanation

1. OSI Model (Open Systems Interconnection Model)

- Developed by ISO (International Organization for Standardization).
- Has 7 layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
- Theoretical model that helps understand how networking works in layers.
- Rarely used in real-world implementation, mainly for learning purposes.

2. TCP/IP Model (Transmission Control Protocol/Internet Protocol Model)

- Developed by the U.S. Department of Defense (DoD).
- Has 4 layers: Network Interface, Internet, Transport, and Application.
- Practical model used in real-world networks, including the Internet.
- Designed for real communication protocols like TCP, IP, UDP, etc.