

07/05/24

(4/8) Tools of the Trade: Linux and SQL

⇒ MODULE 1:- [Intro to operating systems]
↳ relationship b/w OS, hardware, and software, and become familiar with functions of OS

↳ GUI - Graphical User Interface

↳ CLI - Command Line Interface

⇒ MODULE 2:- [The Linux OS]

↳ Uses in cybersecurity

↳ Linux architecture and distributions

↳ Linux shell

⇒ MODULE 3:- [Linux commands in the Bash shell]

↳ Navigate and manage file system

↳ help in new linux cmds

⇒ MODULE 4:- [Databases and SQL]

↳ Query a database

↳ SQL to communicate with db

↳ SQL can join multiple tables.

➔ MODULE 1 :

➔ The wonderful world of Operating Systems:-

⇒ Operating system : (OS)

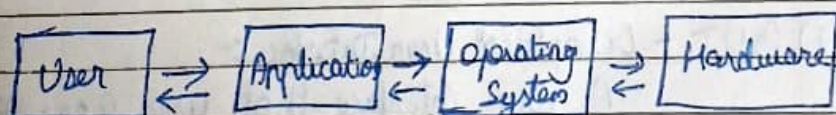
The interface between computer hardware and the user.

⇒ Hardware:

The physical components of a computer

- Windows
- macOS
- Chrome OS
- Android
- iOS
- Legacy operating systems
- Linux

➔ The operating system at work:-



⇒ Application:

A program that performs a specific task.

⇒ Booting a computer :

Click power switch

↳ BIOS or UEFI is activated

↳ Unified Extensible Firmware Interface

↳ has loading instructions

↳ activate the bootloaders

↳ boots the OS

⇒ Virtual Machine :

A VM is a virtual version of a physical computer.

⇒ Benefits of using Virtual Machines :-

(1) Security

(2) Efficiency

- KVM - Kernel based VM ⇒ hypervises
 - ↳ help manage virtual machines
 - ↳ available in linux distros

⇒ The User Interface

⇒ User Interface :

A program that allows the user to control the functions of the operating system.

- (i) GUI - Graphical User Interface
- ⇒ (ii) CLI - Command Line Interface

(i) GUI - Graphical User Interface :-

A user interface that uses icons on the screen to manage different tasks on the computer.

(ii) CLI - Command Line Interface :

A text based user interface that uses commands to interact with the computer.

- CLI is more flexible and powerful than GUI
 - CLI → customization
- Advantages of CLI in cybersecurity :-
- Efficiency
 - History file

➡ Module - 2 :-

➡ Linux

➡ All about Linux

⇒ Linux:

An open-source operating system

⇒ Components of Linux:

- (1) • User
- (2) • Applications
- (3) • Shell
- (4) • Filesystem Hierarchy Standard
- (5) • Kernel
- (6) • Hardware

(1) ⇒ User:

The person interacting with a computer.

(2) ⇒ Applications:

A program that performs a specific task

(3) ⇒ Shell:

The command-line interpreter

(4) ⇒ Filesystem Hierarchy Standard: [FHS]

The component of the Linux OS that organizes data.

(5) ⇒ Kernel:

The component of the Linux OS that manages processes and memory.

(6) ⇒ Hardware:

The physical components of a computer.

⇒ Linux distributions :- (Different versions of Linux)

⇒ Parent Distributions :-

- Red Hat Enterprise Linux (CentOS)
- Slackware (SUSE)
- Debian (Ubuntu and KALI LINUX)

⇒ Penetration test :-

A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications and processes.

⇒ Penetration testing tools in KALI LINUX :

- (1) Metasploit
- (2) Burpsuite
- (3) John The Ripper

⇒ Digital forensics :-

The practice of collecting and analyzing data to determine what has happened after an attack.

⇒ Digital forensics tools in KALI LINUX:

- (1) tcpdump
- (2) Wireshark
- (3) Autopsy

⇒ Package Managers:

It is a tool that helps users install, manage, and remove packages or applications. Linux uses multiple package managers. apt → debian and yum → redhat package manager.

⇒ The shell:

⇒ Shell:

The command-line interpreter

⇒ Command:

An instruction telling the computer to do something.

• Shell provides the user with a CLI

• commands → shell → computer
from user ← process

⇒ types of shell:

- bash (Bourne-Again Shell)
- zsh
- csh
- ksh
- tcsh

⇒ Standard input :

Information received by the OS via the command line

⇒ echo :

A linux command that outputs a specified string of text.

⇒ String data :

Data consisting of an ordered sequence of characters.

⇒ Standard output :

Information returned by the OS through the shell.

- mukundan@user1:~\$ echo hello
hello

⇒ Standard error :

Error messages returned by the OS through the shell.

⇨ MODULE - 3 :

⇨ Navigate the linux file systems :

⇒ Security analysts :

- Work with server logs
- Navigate, manage and analyse the file remotely.
- Verify and configure users and group access
- Give authorization and set file permissions.

⇒ Bash :

The default shell in most linux distributions.

⇒ Argument : (in Linux)

Specific information needed by a command.

⇒ Root directory :-

The highest-level directory in linux

⇒ Core common commands for navigation and reading files :

- pwd - prints the working directory
- ls - displays the names of files and dire in the current working dir
- cd - navigate b/w directories

- cat - displays the content of a file
- head - displays the just the beginning of a file
(by default 10 lines)

→ Standard FHS directories:

- (1) /home : Each user gets their own homedir
- (2) /bin : this dir stands for 'binary'
→ contains binary files and executables.
(these are files that contain a series of codes a comp needs to follow to run programs)
- (3) /etc : stores the system configuration files
- (4) /tmp : this directory stores many temporary files
→ used by hackers because anyone in the system can modify data in these files
- (5) /mnt : this stores media, such as USB drives and hard drives

- tail - displays the end of a file
(by default last 10 lines) → used to read most recent log files

head docs.txt

head docs.txt -n 5

head -n 5 docs.txt

- less - the less cmd returns the content of a file one page at a time

➡ Manage file content in Bash:

⇒ grep:

Searches a specified file and returns all lines in the file containing a specified string.

what we want to search
grep OS updates.txt
grep _____ updates.txt

⇒ Piping:

Sends the standard output of one command as standard input to another command for further processing

cat _____ txt | grep hi

⇒ find:

This cmd searches for directories and files that meet specific criteria

→ file name
→ file size
→ last modified



⇒ -name, -iname, -mtime, -mmin

case sensitive

case insensitive

lastly modified (days)

last modified (min)

find /home/madhura/Downloads -iname "*.git"
find " " -mtime -3

last 3 days

- ⇒ `mkdir` - creates a new directory
- ⇒ `rmdir` - removes or deletes a directory
- ⇒ `touch` - creates a new file
- ⇒ `rm` - removes or deletes a file
- ⇒ `mv` - moves a file or directory to a new location
- ⇒ `cp` - copies a file or directory into a new location

• Ex:

`rmdir oldreports`

`mkdir rgt`

`touch hey123.txt`

`rm hey123.txt`

`mv .txt /home/midhun/does`

`cp .txt /home/midhun/ haha`

⇒ nano: (file editor)

It is a command line file editor.

→ Authenticate and authorize users:

⇒ Permissions:

The type of access granted for a file or directory.

⇒ Authorization:

The concept of granting access to specific resources in a system.

⇒ Permissions in Linux:

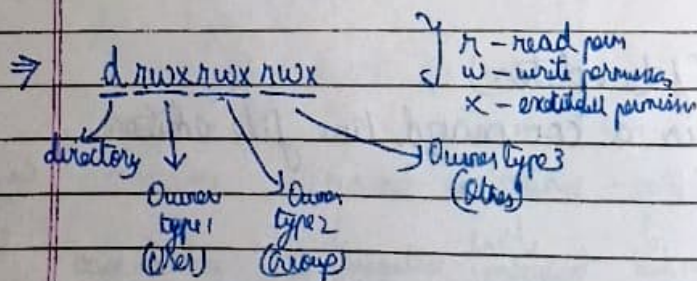
- (1) Read (r)
- (2) Write (w)
- (3) Execute (x)

⇒ Types of Owners:

- (1) User

⇒ Types of Owners:

- (1) User (u)
- (2) Group (g)
- (3) Other (o)



⇒ Options:

Modify the behaviour of the command.

- ls -l :-
displays permissions to files and directories
- ls -a :-
displays hidden files
- ls -la :-
displays permissions to files and directories, including hidden files
- $\begin{array}{cccc} _ & _ & _ & _ \\ \text{rw} & _ & _ & _ \\ \text{--} & \text{--} & \text{--} & \text{--} \end{array}$
 ↓ ↓ ↓ ↓
 type user group other

⇒ chmod :- (change mode)

used to change permissions on files and directories.

Ex: chmod $\overset{\text{add permission}}{\text{g+w}}, \overset{\text{remove permission}}{\text{o-r}} \text{ access.txt}$
 ↓ ↓
 group other

• chmod $\text{g+w}, \text{o-r} \text{ access.txt}$

~~chmod $\text{g+r}, \text{r}$~~

- chmod $\text{u+r}, \text{g+r}, \text{o+r} \text{ sample.txt}$
- chmod $\text{u+rw}, \text{g+rw}, \text{o-rwx}$

• "=" can also be used for overwriting existing permissions, for instance, if the user previously had write permission, these write permission are removed after you specify only read permissions with "=".

chmod $\text{u=r}, \text{g=r}, \text{o=r} \text{ login-session.txt}$

⇒ Root user: (or superuser)

A user with elevated privileges to modify the system.

⇒ Problems with logging in as root:

- Security risk
- Irreversible mistakes
- Accountability

⇒ Sudo: (superuser do)

Temporarily grants elevated permissions to specific users.

⇒ useradd:

Adds a user to the system.

- `sudo useradd rep2`
- ~~`sudo useradd midhu`~~ ^{on → additional gpps} _{eg → primary gip}

⇒ userdel: `sudo userdel -g security midhu`

Deletes a user from the system

- `sudo userdel rep3`

⇒ usermod:

Modifies existing user accounts

- `sudo usermod -g executives midhu`

⇒

⇒ chown:

Changes ownership of a file or directory

- `sudo chown midhu access.txt` ←

→ becomes the owner of

• Note:

* `sudo useradd -g security midhu`



creates a new user and assigns security as their primary group.

-g ⇒ primary groups

-G ⇒ additional groups

* `sudo usermod -g executive midhu`



changes midhu's primary group to executive

-g ⇒ primary grp

-G ⇒ additional grp

-a ⇒ (only used with -G) appends the user to an existing group

* `sudo usermod -a -G marketing midhu`

-d ⇒ changes the user's home directory

-l ⇒ changes the user's login name

-L ⇒ Locks the account so the user can't login.

→ Get help in Linux :-

⇒ man : (manual)

Displays information on other commands and how they work.

- man usermod

⇒ whatis :

Displays a description of a command on a single line

- whatis tail

⇒ apropos :

Searches the manual page descriptions for a specified string.

- apropos password
- apropos -a change password

⇒ MODULE 4 :-

⇒ Introduction to SQL and Databases :-

⇒ Database :-

An organised collection of information or data.

⇒ Spreadsheets :

- Designed for a single user or a small team
- Store less data

⇒ Databases :

- Accessed by multiple ~~times~~ people simultaneously
- Store massive amounts of data.
- Perform complex tasks while accessing data.

⇒ Relational database :

A structured database containing tables that are related to each other.

⇒ Primary key :-

A column where every row has a unique entry.

⇒ Foreign key :

A column in a table that is a primary key in another table.

• Note :

There can be only one primary key in a table, but there can be multiple foreign keys in a table.

⇒ SQL : [Structured Query Language]

A programming language used to create, interact with, and request information from a database.

• Query :

A request for data from a database table or a combination of tables.

⇒ Log :

A record of events that occur within an organisation's systems.

⇒ SQL queries :

→ SELECT :

Indicates which columns to return

→ FROM :

Indicates which table to query.

- `SELECT employees id, device id FROM employees;`
- `SELECT *`
`FROM employees`
- `SELECT customerid, city, country`
`FROM customers;`

⇒ ORDER BY :

It sequences the records returned by a query based on specified column or columns. This can be in either ascending or descending order.

• SELECT *
 FROM employees
 ORDER BY city; } ascending { SELECT cust_id, cust_name
 FROM customers
 ORDER BY cust_id;

• SELECT *
 FROM employees
 ORDER BY city DESC; } descending

• SELECT *
 FROM employees
 ORDER BY country, city; } Sorting based on
 multiple columns

⇒ Filtering :

Selecting data that ~~match~~ match a certain condition.

⇒ Operator :

A symbol or keyword that represents an operation.

⇒ WHERE :

Indicates the condition for a filter.

• SELECT * FROM employees WHERE country = "USA";

⇒ LIKE:

Used with WHERE to search for a pattern in column

- `SELECT * FROM log-in-attempts WHERE country LIKE 'US%';`

↙ This displays records which contain "US" in them, returning US & USA

⇒ Wildcard symbols:

A wildcard is a spl character that can be substituted with any other character.
most used ⇒ %, & _

a% → are, apple, a

a_ → as, an, a7

a__ → agd, ant, a1c

%a → agar, ha, ba, pizza

_a → ma, ba, la

% a% → Again, back, a

a → car, ban, ea7

⇒ More SQL filters

⇒ Common data types:

(i) String

(ii) Numeric

(iii) Date and time

⇒ String data :-

Data consisting of an ordered sequence of characters.

⇒ Numeric data :-

Data consisting of numbers.

⇒ Date and time :-

Data representing a date and/or time

⇒ Operators :

- = • >=
- > • <=
- <
- < > - not equal ⇒ • !=

• SELECT *

FROM log_in_attempts
WHERE Time > '18:00';

⇒ BETWEEN :

An operator that filters for numbers or dates within a range.

• SELECT *

FROM log_in_attempts

WHERE patch_date BETWEEN '2021-03-01' AND '2021-09-03';

both are included

⇒ AND:

Specifies that both conditions must be met simultaneously.

• SELECT * FROM machines
WHERE OS = 'Windows' AND UI = 2;

⇒ OR:

Specifies that either condition can be met.

• SELECT * FROM machines
WHERE OS = 'Linux' OR OS = 'MacOS';

⇒ NOT:

Negates a condition

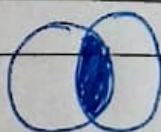
• SELECT * FROM machines
WHERE NOT OS = 'Windows';

⇒ SQL joins:

⇒ INNER JOIN:

Returns rows matching on a specified column that exists in more than one table.

• SELECT * FROM employees
INNER JOIN machines ON employees.employee_id = machines.id



⇒ Outer

⇒ Outer joins:

(i) ~~LEFT~~

⇒ Outer joins:


(i) LEFT JOIN

(ii) RIGHT JOIN

(iii) FULL OUTER JOIN


(i) LEFT JOIN :-

Returns all of the records of the first table, but only returns rows of the second table that match on a specified column.



(ii) RIGHT JOIN :-


Returns all of the records of the second table, but only returns rows from the first table that match on a specified column.



(iii) FULL OUTER JOIN :-

Returns all records from both tables

Note :- same syntax as INNER JOIN for all OUTER JOINS



⇒ Aggregate functions:

- Count
- Sum
- Avg

learn syntax (copy)

Ex: SELECT ^{SUM}
COUNT (of column name)
^{AVG}
FROM customers;

COUNT (column name)
56