



University of Dhaka
Dept. of Computer Science and Engineering
Professional Masters in Information and Cyber
Security (PMICS) Program

CSE 808 - Information Infrastructure Protection

Linux and Useful Tools for Cyber Security

Lab Class 1 – Manual

Conducted by: Md. Shakhawat Hossain Robin

Introduction to Linux

Linux is an open-source Unix-like operating system-based family on the Linux kernel, and the OS kernel was first published on 17 September 1991 by Linus Torvalds. Typically, Linux is packaged as the Linux distribution, which contains the supporting libraries and system software and kernel, several of which are offered by the GNU Project.

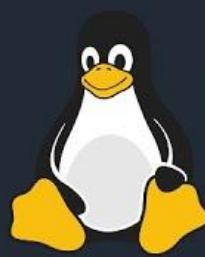
Why Linux is important for cybersecurity

- **Open Source:** Linux's open-source nature enables transparency and community-driven security auditing.
- **Built-in Security Features:** Linux distributions come with strong security features like access control and regular updates.
- **Flexibility:** Linux allows customization and deployment of specialized security measures.
- **Powerful Command-line Tools:** Linux provides powerful command-line tools for efficient execution of security tasks.
- **Reliability:** Linux serves as a robust platform for cybersecurity operations, ensuring system and network security.



Why Linux is popular

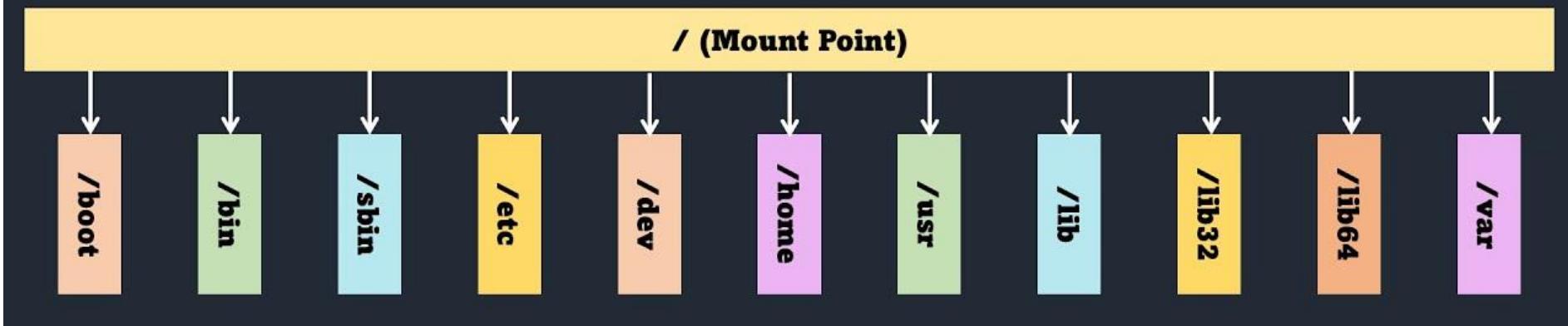
- **Open Source Philosophy:** Linux's open-source nature allows for free distribution, modification, and sharing, fostering a collaborative community-driven development model.
- **Stability and Reliability:** Linux is known for its stability and reliability, making it a preferred choice for mission-critical systems and servers.
- **Customization:** Linux offers a high degree of customization, enabling users to tailor the operating system to their specific needs and preferences.
- **Security:** Linux's security architecture and strong permission controls make it inherently more secure compared to other operating systems.
- **Cost-Effectiveness:** Linux is often available free of cost, making it an attractive option for organizations looking to minimize software licensing expenses.
- **Performance:** Linux is optimized for performance, offering efficient resource utilization and scalability across various hardware platforms.
- **Community Support:** Linux benefits from a large and active community of developers, users, and enthusiasts who provide support, contribute to development, and share knowledge.
- **Compatibility:** Linux supports a wide range of hardware architectures and devices, ensuring compatibility with diverse computing environments.
- **Enterprise Adoption:** Many businesses and organizations worldwide rely on Linux for their infrastructure needs, driving its popularity in enterprise environments.
- **Innovation:** Linux is at the forefront of technological innovation, with constant updates, advancements, and support for emerging technologies.

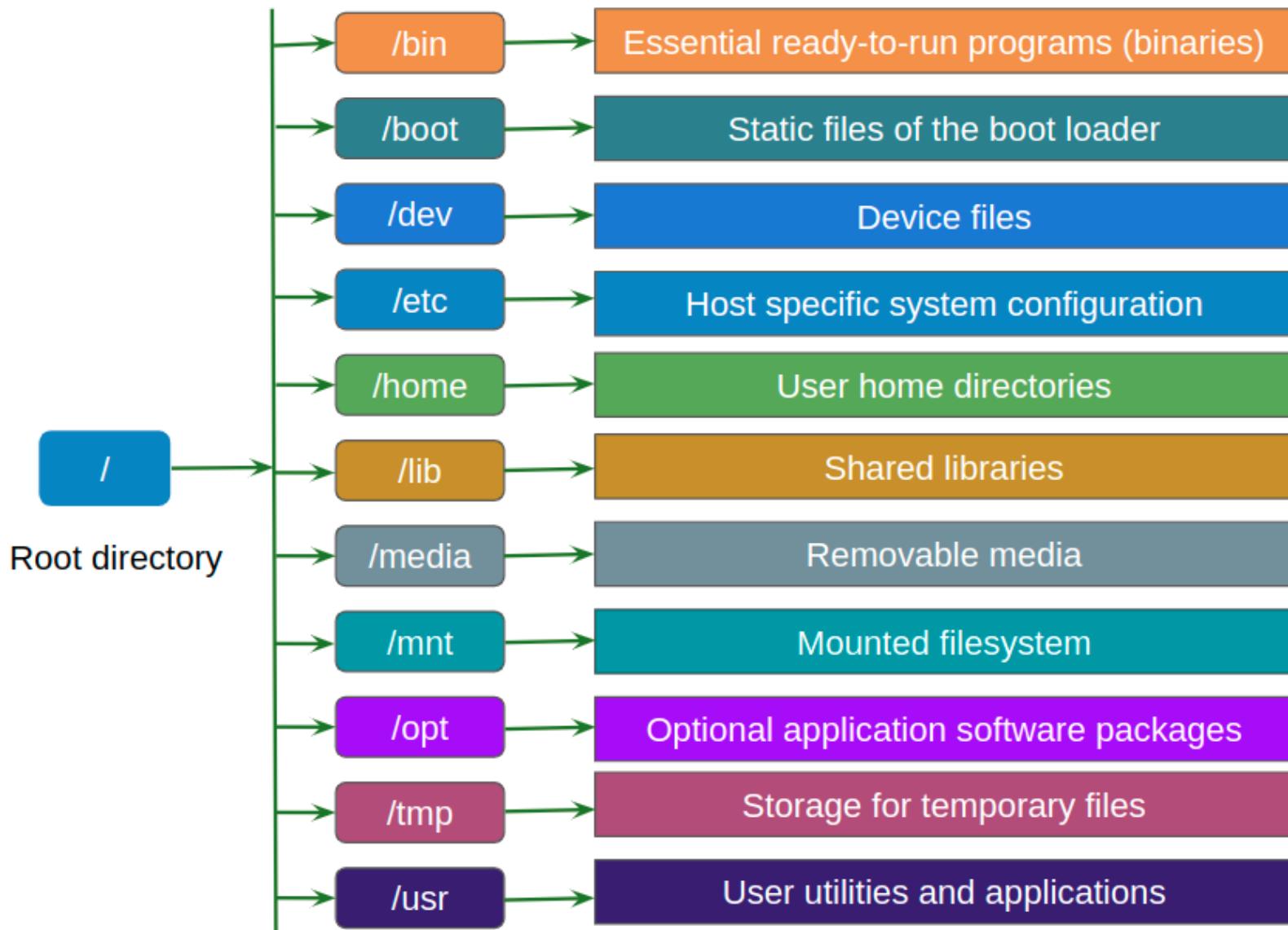


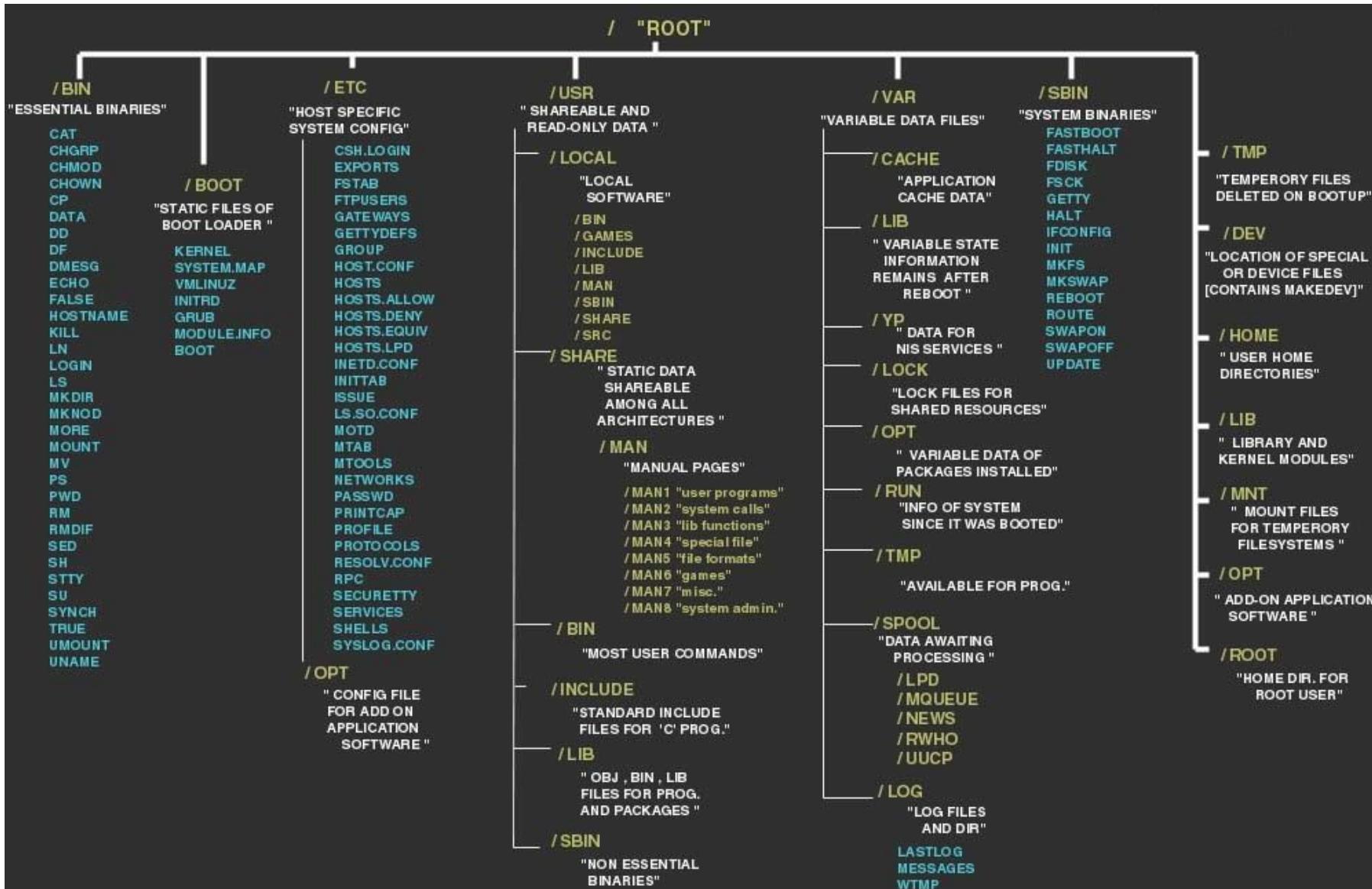
LINUX File System

Understanding

KALI LINUX







Basic Linux Commands

File Operations	
<code>ls</code>	Lists all files and directories in the present working directory
<code>ls -R</code>	Lists files in sub-directories as well
<code>ls -a</code>	Shows hidden files
<code>ls -al</code>	Lists files and directories with detailed information like permissions, size, owner, etc.
<code>cd directoryname</code>	Changes the directory
<code>cd ..</code>	Moves one level up
<code>pwd</code>	Displays the present working directory
<code>cat > filename</code>	Creates a new file
<code>cat filename</code>	Displays the file content
<code>cat file1 file2 > file3</code>	Joins two files (file1 and file2) and stores the output in a new file (file3)
<code>touch filename</code>	Creates or modifies a file
<code>rm filename</code>	Deletes a file
<code>cp source destination</code>	Copies files from the source path to the destination path
<code>mv source destination</code>	Moves files from the source path to the destination path

<code>find / -name filename</code>	Finds a file or a directory by its name starting from root
<code>file filename</code>	Determines the file type
<code>less filename</code>	Views the file content page by page
<code>head filename</code>	Views the first ten lines of a file
<code>tail filename</code>	Views the last ten lines of a file

Directory Operations and permission

<code>mkdir dirname</code>	Creates a new directory in the present working directory
<code>rmdir dirname</code>	Deletes a directory
<code>cp -r source destination</code>	Copies directories recursively
<code>mv olddir newdir</code>	Renames directories
<code>find / -type d -name dirname</code>	Finds a directory starting from root
<code>chmod octal filename</code>	Change the permissions of file to octal, which can be between 0 (no permissions) to 7 (full permissions)
<code>chown ownername filename</code>	Change file owner
<code>chgrp groupname filename</code>	Change group owner

Process Operations	
<code>ps</code>	Displays your currently active processes
<code>top</code>	Displays all running processes
<code>kill pid</code>	Kills the process with given pid
Networking	
<code>ping host</code>	Ping a host and outputs results
<code>whois domain</code>	Get whois information for domain
<code>dig domain</code>	Get DNS information for domain
<code>netstat -pnltu</code>	Display various network related information such as network connections, routing tables, interface statistics etc.
<code>ifconfig</code>	Displays IP addresses of all network interfaces
<code>ssh user@host</code>	Remote login into the host as user
<code>scp</code>	Transfers files between hosts over ssh
<code>wget url</code>	Download files from the web
<code>curl url</code>	Sends a request to a URL and returns the response

<code>traceroute domain</code>	Prints the route that a packet takes to reach the domain.
<code>mtr domain</code>	<code>mtr</code> combines the functionality of the <code>traceroute</code> and <code>ping</code> programs in a single network diagnostic tool.
Archives and Compression	
<code>tar cf file.tar files</code>	Create a tar named <code>file.tar</code> containing files
<code>tar xf file.tar</code>	Extract the files from <code>file.tar</code>
<code>gzip file</code>	Compresses file and renames it to <code>file.gz</code>
<code>gzip -d file.gz</code>	Decompresses <code>file.gz</code> back to file
<code>zip -r file.zip files</code>	Create a zip archive named <code>file.zip</code>
<code>unzip file.zip</code>	Extract the contents of a zip file
Text Processing	
<code>grep pattern files</code>	Search for pattern in files
<code>grep -r pattern dir</code>	Search recursively for pattern in dir
<code>command grep pattern</code>	Pipe the output of command to grep for searching
<code>echo 'text'</code>	Prints text

<code>sed 's/string1/string2/g' filename</code>	Replaces string1 with string2 in filename
<code>diff file1 file2</code>	Compares two files and shows the differences
<code>wc filename</code>	Count lines, words, and characters in a file

Disk Usage

<code>df</code>	Shows disk usage
<code>du</code>	Shows directory space usage
<code>free</code>	Show memory and swap usage
<code>whereis app</code>	Show possible locations of app

System Info

<code>date</code>	Show the current date and time
<code>cal</code>	Show this month's calendar
<code>uptime</code>	Show current uptime
<code>w</code>	Display who is online
<code>whoami</code>	Who you are logged in as

<code>uname -a</code>	Show kernel information
<code>df -h</code>	Disk usage in human readable format
<code>du -sh</code>	Disk usage of current directory in human readable format
<code>free -m</code>	Show free and used memory in MB
Package Installations	
<code>sudo apt-get update</code>	Updates package lists for upgrades
<code>sudo apt-get upgrade</code>	Upgrades all upgradable packages
<code>sudo apt-get install pkgname</code>	Install pkgname
<code>sudo apt-get remove pkgname</code>	Removes pkgname
Search and Find	
<code>locate filename</code>	Find a file by its name. The database updated by <code>updatedb</code> command.
<code>whereis programname</code>	Locate the binary, source, and manual page files for a command.
<code>which commandname</code>	Shows the full path of (shell) commands.
Compression / Archives	
<code>tar -cvf archive.tar dirname/</code>	Create a tar archive.

<code>tar -xvf archive.tar</code>	Extract a tar archive.
<code>tar -jcvf archive.tar.bz2 dirname/</code>	Create a compressed bz2 archive.
<code>tar -jxvf archive.tar.bz2</code>	Extract a bz2 archive.

Useful Tools for Cyber Security

Network Security Tools:

- Nmap : Network mapper for discovering hosts and services on a network.
- Wireshark : Network protocol analyzer useful for network forensics and traffic analysis
- Tcpdump : Capture and analyze network traffic on Unix-like systems
- NetworkMiner : Open source network forensic analyzer useful for investigating traffic
- Snort : Open source intrusion detection and network monitoring system
- Aircrack-ng : A suite of wireless network security tools used to assess Wi-Fi network security.
- Ettercap : Network sniffing and Man-in-the-Middle (MitM) attacking tool

Vulnerability Assessment and Penetration Testing Tools:

- Nessus : Vulnerability scanner - Nessus
- OWASP ZAP : Web application security scanner - OWASP ZAP
- Burp Suite : Web vulnerability scanner and proxy tool
- Acunetix : Web vulnerability scanner - Acunetix
- Metasploit : Penetration testing framework
- OpenVAS : Open-source vulnerability scanner
- SQLMap : SQL injection and database takeover tool - SQLMap
- DirBuster : Directory brute-forcing tool - DirBuster
- Nikto : Web server scanner - Nikto

Encryption and Cryptography Tools:

- GnuPG : Implementation of the OpenPGP standard - GnuPG
- TrueCrypt/VeraCrypt : Disk encryption software - VeraCrypt
- OpenSSL : Cryptography toolkit - OpenSSL
- PuTTY : SSH and Telnet client – PuTTY
- AES Crypt : A file encryption software that uses the (AES) algorithm to secure files and folders.
- PGP : A data encryption and decryption program that provides cryptographic privacy and authentication

Password Recovery and Cracking tools

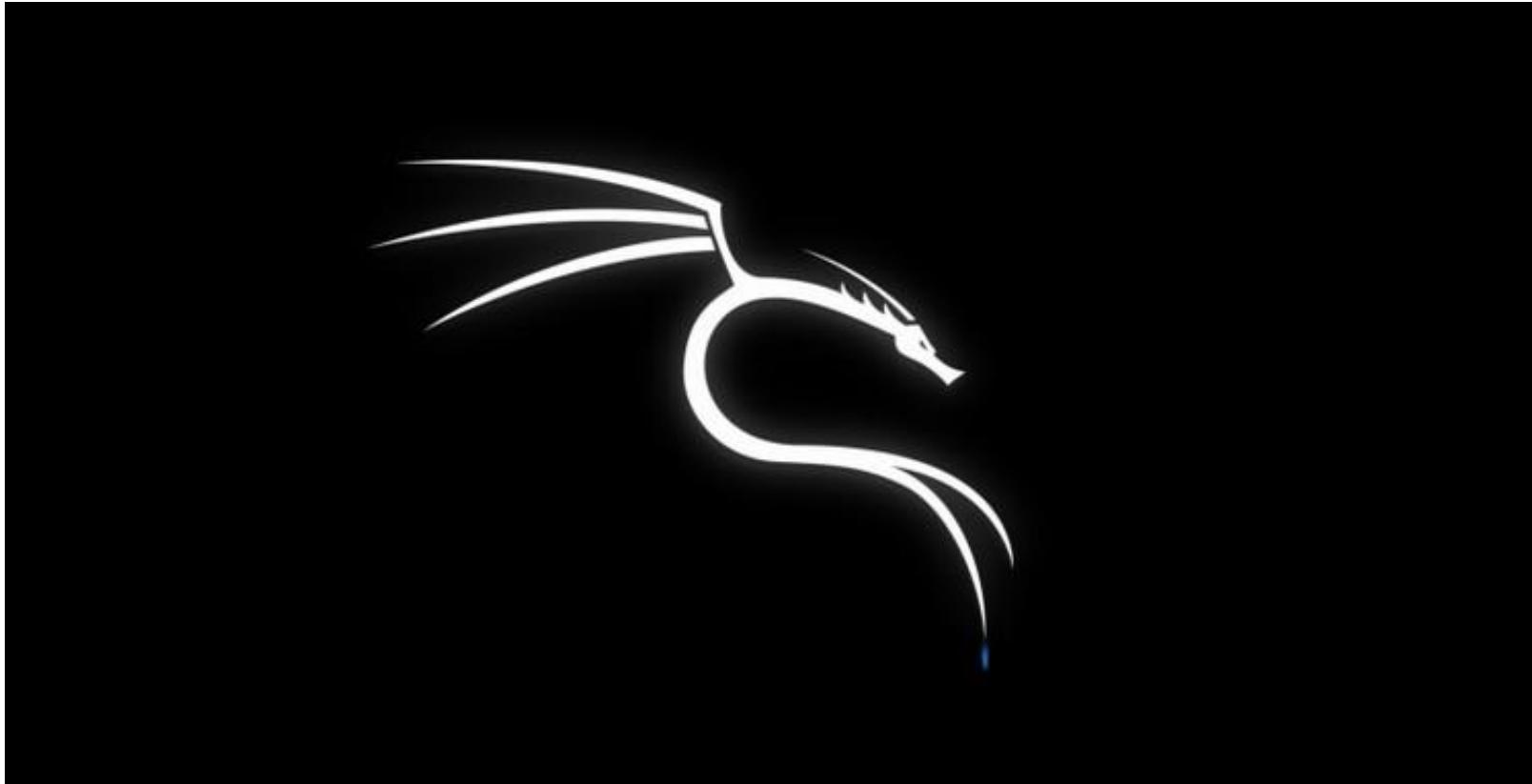
- John the Ripper : A fast password cracker, available for Unix, macOS, Windows, DOS, BeOS, and OpenVMS.
- Hashcat : An advanced password recovery utility for Windows, macOS, Linux, and BSD systems.
- Hydra : A parallelized login cracker that supports SSH, FTP, HTTP(S), Telnet, SMB, and more.
- Medusa : A speedy, parallel, and modular login brute-forcer for HTTP, HTTPS, FTP, SMB, Telnet, etc.
- Ophcrack : A Windows password cracker based on rainbow tables.

Endpoint Monitoring and Troubleshooting Tools:

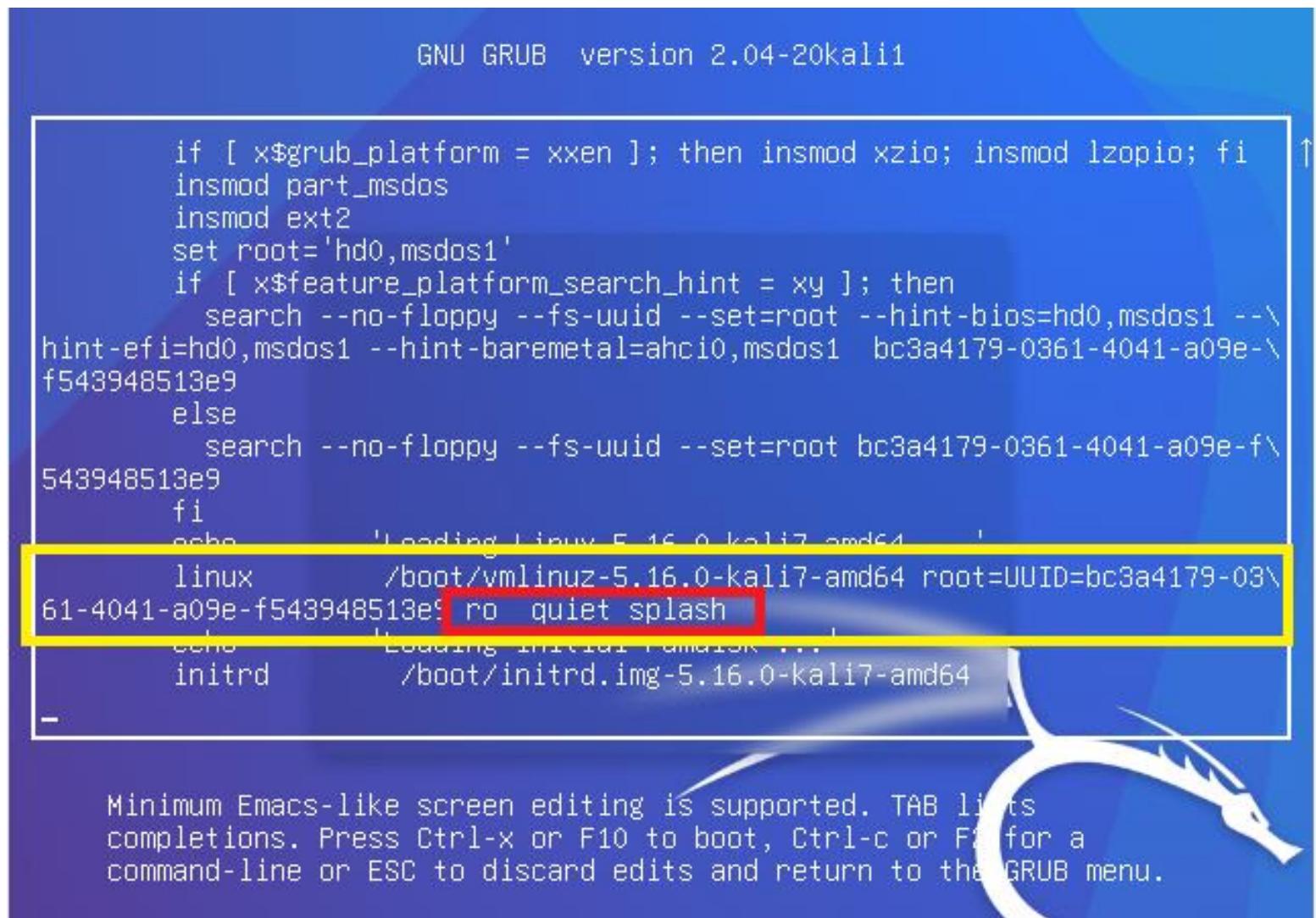
- Sysinternals Suite : Suite of Windows system utilities monitoring and troubleshooting Windows-based systems.

Linux Password Breaking

Step 1: Reboot the machine and Press “e” during boot



Step 2: Now go to the line linux, and remove **ro quiet splash** and write here **rw init=/bin/bash/**



The image shows a GRUB boot menu interface. At the top, it says "GNU GRUB version 2.04-20kali1". Below that is a large block of shell script code used to determine the root device and search for the kernel. In the middle of the screen, there is a highlighted yellow box containing the kernel command line options. The line "linux /boot/vmlinuz-5.16.0-kali7-amd64 root=UUID=bc3a4179-0361-4041-a09e-f543948513e9 ro quiet splash" is specifically highlighted with a red rectangle. Below this line, the "initrd" option is listed as "/boot/initrd.img-5.16.0-kali7-amd64". At the bottom of the screen, there is a message about Emacs-like screen editing and instructions for exiting the menu.

```
GNU GRUB version 2.04-20kali1

if [ $grub_platform = "xen" ]; then insmod xzio; insmod lzopio; fi
insmod part_msdos
insmod ext2
set root='hd0,msdos1'
if [ $feature_platform_search_hint = "xy" ]; then
    search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --\
hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 bc3a4179-0361-4041-a09e-\
f543948513e9
else
    search --no-floppy --fs-uuid --set=root bc3a4179-0361-4041-a09e-f\
543948513e9
fi
echo "Loading Linux 5.16.0-kali7-amd64..."
linux /boot/vmlinuz-5.16.0-kali7-amd64 root=UUID=bc3a4179-03\
61-4041-a09e-f543948513e9 ro quiet splash
echo "Loading initial ramdisk..."
initrd /boot/initrd.img-5.16.0-kali7-amd64
-

```

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F11 for a command-line or ESC to discard edits and return to the GRUB menu.

Step 3: press **CTRL+X** or **F10** (it will save the setting and reboot the system)

Step 4: Now a new terminal will appear, here type the command: **ls /home** and hit enter, now see the available user name and pick one which you want to reset.

Step 5: **passwd <username_which_you_want_to_reset>** and hit enter. Now set the password as you want.

```
root@none:~# ls /home
invento kali robincyber
root@none:~# passwd robincyber
New password:
Retype new password:
passwd: password updated successfully
root@none:~# _
```

Step 6: **reboot -f** (For force reboot the system)

Now you have successfully break the password of your kali linux machine

Thanks to all