Kali Linux Commands

1. Basic System Commands

ls: List files and directories in the current directory.
ls -l: List with detailed information.
ls -a: Show all files, including hidden files.
ls -la
cd: Change directory.
Example: cd /home/user/Documents
pwd: Print the current working directory.
mkdir: Create a new directory.
Example: mkdir new_directory
rmdir: Remove an empty directory.
rm: Remove files or directories.
rm -rf: delete anything forcefully
Example: rm -rf file.txt
For directories: rm -rf directory_name
touch - create empty file
cp: Copy files or directories.
Example: cp file1.txt file2.txt
mv: Move or rename files or directories.
Example: mv oldname.txt newname.txt

2. **Network Commands**

ifconfig: Display network interfaces and configuration (older command, replaced by ip in newer systems).
ip a: Display network interfaces and IP addresses.
arp -a - show arp table of the LAN
ip n - alternative for arp
route - show the routing deating for network
ip r - alternative for route
ping: Send ICMP echo requests to test network connectivity.
Example: ping google.com
fping: alternative for ping
netstat: Show network connections, routing tables, and interface statistics.
Example: netstat -antp
ss -pultn: alternative for netstat
netdiscover -r ip --> to discover live hosts in Local Area Network (LAN)
nmap: Network scanning tool (commonly used in Kali Linux for security testing).
Example: nmap -sP 192.168.1.0/24 (Ping scan of the entire subnet)
fping -a -g IP/24: alternative for netdiscover
arp-scan -l : alternative command for netdiscover

nbtscan -r IP/24 - alternative command for netdiscover
nmap -sn IP/24 : alternative command for netdiscover

3. Package Management

apt update: Update package list from repositories.
apt upgrade: Upgrade all installed packages.
apt install [package_name]: Install a new package.
Example: apt install nmap
apt remove [package_name]: Remove a package.
Example: apt remove nmap
apt purge (pakage name): remove all the files related to the package.
apt search [package_name]: Search for a package.

4. User Management

whoami: Show the current logged-in user.
id: Display user ID and group ID.
sudo: Run a command with superuser privileges.
Example: sudo apt install nmap
adduser: Add a new user.
Example: sudo adduser newuser
passwd: Change the password of a user.
Example: sudo passwd newuser

5. Text File Editing

nano: Simple text editor.
Example: nano file.txt
vim: Advanced text editor (more complex than nano).
Example: vim file.txt
echo "any input" > save_file.txt - save output using > symbol.
Leafpad or mousepad or gedit

6. Searching for Files
find: Search for files and directories.
Example: find /home/user -name "*.txt" (Find all .txt files in the user's home directory)
locate: Find files by name (requires database update).
Example: locate file.txt
grep: Search for text patterns in files.
Example: grep "pattern" file.txt (Search for the string "pattern" in file.txt)

7. System Shutdown and Reboot

reboot: Restart the system.

shutdown -h now: Shut down the system immediately.
poweroff: Power off the system.

8. nmap basic commands:

-sV - for version detection
-sU - scan for UDP ports
-sT - scan for TCP ports
-p- : scan all the 65,535 ports
-p80,22,2222 - scan for specific port
-sS - SYN scan
-O - Operating system scan
-A - Aggressive scan or ALL scan
-vv - verbose
-sC - default script scan

9. Enumeration Tools:

nmap -A -p- IP - to find all info and vulnerability details using IP
dnsrecon -d domain - get info of a dns server
dnsenum / nslookup - alternative command for dnsrecon
enum4linux - to find the vulnerabilities on linux machine
nbtstat -A IP - detail info about remote NetBIOS names & associated IP address table from a specific target
theHarvester -d google.com -l 200 -b baidu/linkedin - get email id

SMB Enumeration:
metasploit : auxiliary/smb/smb_version
smbclient -N -L \\\\IP\\ - get info on samba server
smbclient \\\\IP\\server_name - login to any smb server

10. Web Application Pentesting Tools:-

nmap -A -p- IP
whatweb domain/IP - to know what technology that server is using
nikto -p 80,443 -h domain/IP - to find the vulnerabilities of a website or web applications
sslscan IP - to find the ssl/tls version and vulnerabilities
wpscan -u domain: scan wordpress for vulnerability

Directory Bruteforce:
dirbuster (gui)
dirb <URL>
dirbuster -u domain -w wordlist.txt
gobuster dir -u domain -w wordlist.txt
gobuster dns -d domain -w wordlist.txt

Dirsearch -u domain

Subdomain Enumeration:
assetfinder --subs-only domain
amass enum -d domain
gau google.com
subfinder -d domain.com -all -silent
sublist3r -d google.com
sublist3r -d target.com -b -w /path/to/wordlist.txt

exiftool -n image.jpg - find metadata