Kali Linux Commands Cheat Sheet

Basic Linux Commands

File and Directory Management

- **ls** - List files and directories.
- **cd [directory]** - Change directory.
- **pwd** - Print the current working directory.
- **mkdir [directory]** - Create a new directory.
- **rmdir [directory]** - Remove an empty directory.
- **rm [file/directory]** - Remove files or directories.
- **cp [source] [destination]** - Copy files or directories.
- **mv [source] [destination]** - Move or rename files or directories.
- **cat [file]** - Display file contents.
- **nano [file]** - Edit files in the terminal.
- **touch [file]** - Create a new, empty file.

User Management

- **whoami** - Show the current user.
- **adduser [username]** - Add a new user.
- **passwd [username]** - Change a user's password.
- **sudo [command]** - Execute commands as a superuser.
- **su** - Switch to the superuser account.

Process Management

- **ps** - Display running processes.

APPAZON

- **top** - Show real-time process monitoring.
- **kill [PID]** - Terminate a process by its Process ID.
- **pkill [process-name]** - Terminate processes by name.

Network Commands

- **ifconfig** - Display network interfaces and configurations (deprecated; use **ip**).
- **ip a** - Show IP addresses and interfaces.
- **ping [host]** - Test connectivity to a host.
- **netstat** - Show network connections, routing tables, and statistics.
- **curl [URL]** - Fetch content from a URL.
- **wget [URL]** - Download files from a URL.

Kali-Specific Tools and Commands

Information Gathering

- **nmap [target]** - Network scanner.
- **whois [domain]** - Query domain information.
- **dnsenum [domain]** - DNS enumeration.
- **theHarvester -d [domain] -l [limit]** - Gather emails, subdomains, and names.

Vulnerability Analysis

- **nikto -h [host]** - Web server scanner.
- **wpscan --url [url]** - WordPress vulnerability scanner.
- **openvas** - Open Vulnerability Assessment System.

Exploitation Tools

- **msfconsole** - Metasploit Framework console.

- **sqlmap -u [url]** - SQL injection testing.
- **searchsploit [keyword]** - Search for exploits in Exploit-DB.

Password Attacks

- **hydra -L [userlist] -P [passwordlist] [target]** - Brute force login credentials.
- **john [file]** - John the Ripper password cracker.
- **hashcat -m [hash-mode] [hash-file] [wordlist]** - Advanced password recovery.

Wireless Attacks

- **airmon-ng** - Enable monitor mode on wireless interfaces.
- **airodump-ng [interface]** - Capture wireless packets.
- **aireplay-ng** - Inject packets into wireless networks.
- **aircrack-ng [capture-file]** - Crack WPA/WEP keys.

Sniffing and Spoofing

- **ettercap -G** - GUI-based network sniffing.
- **wireshark** - Network protocol analyzer.
- **arpspoof -i [interface] -t [target]** - ARP spoofing tool.

Post Exploitation

- **meterpreter** - Post-exploitation framework (via Metasploit).
- **beef-xss** - Browser Exploitation Framework.

Forensics

- **autopsy** - Forensic analysis tool.
- **foremost -i [image-file]** - File recovery.
- **binwalk [file]** - Analyze binary files.

Social Engineering

- **setoolkit** - Social Engineering Toolkit.

Web Application Analysis

- **burpsuite** - Web application security testing.
- **zap** - OWASP Zed Attack Proxy.

Package Management

APT Commands

- **apt update** - Update the package list.
- **apt upgrade** - Upgrade installed packages.
- **apt install [package]** - Install a package.
- **apt remove [package]** - Remove a package.

Utilities

Disk Management

- **fdisk -l** - List disk partitions.
- **mount [device] [mount-point]** - Mount a device.
- **df -h** - Display disk space usage.

Archiving and Compression

- **tar -cf [archive.tar] [files]** - Create a tar archive.
- **gzip [file]** - Compress a file with gzip.
- **unzip [file.zip]** - Extract a zip archive.

System Monitoring

APPAZON

- **dmesg** - View kernel messages.
- **uptime** - Show system uptime.

Hacking Commands Cheat Sheet

Information Gathering

- **nmap [target]** - Network scanner to discover hosts and services.
- **whois [domain]** - Query domain information.
- **dnsenum [domain]** - DNS enumeration.
- **theHarvester -d [domain] -l [limit]** - Gather emails, subdomains, and names.
- **shodan** - Search for devices on the internet (API-based).
- **maltego** - Graphical link analysis tool for gathering open-source intelligence.
- **recon-ng** - Web recon framework.

Vulnerability Scanning

- **nikto -h [host]** - Web server vulnerability scanner.
- **wpscan --url [url]** - WordPress vulnerability scanner.
- **openvas** - Open Vulnerability Assessment System.
- **nmap --script [script-name] [target]** - Run vulnerability-specific Nmap scripts.
- **searchsploit [keyword]** - Search Exploit-DB for known vulnerabilities.

Exploitation Tools

- **msfconsole** - Metasploit Framework console for exploiting vulnerabilities.
- **sqlmap -u [url]** - Automate SQL injection testing.

- **exploitdb** - Local Exploit-DB repository (via **searchsploit**).
- **commix --url [url]** - Command injection exploitation tool.
- **routersploit** - Exploitation framework for embedded devices.
- **empire** - Post-exploitation framework for PowerShell and Python agents.

Password Attacks

- **hydra -L [userlist] -P [passwordlist] [target]** - Brute force login credentials.
- **medusa -h [host] -U [userlist] -P [passwordlist]** - Brute force login testing.
- **hashcat -m [hash-mode] [hash-file] [wordlist]** - Advanced password cracking.
- **john [file]** - John the Ripper password cracker.
- **cewl --depth [level] --width [length] -w [file] [url]** - Generate custom wordlists.
- **crunch [min] [max] [charset] -o [file]** - Create password wordlists.

Wireless Hacking

- **airmon-ng** - Enable monitor mode on wireless interfaces.
- **airodump-ng [interface]** - Capture wireless packets.
- **aireplay-ng --deauth [count] -a [AP-MAC] -c [Client-MAC] [interface]** - Deauthentication attack.
- **aircrack-ng [capture-file]** - Crack WPA/WEP keys.
- **wifite** - Automated wireless network auditor.
- **reaver -i [interface] -b [BSSID] -vv** - Exploit WPS vulnerabilities.

Sniffing and Spoofing

- **ettercap -G** - GUI-based network sniffing and man-in-the-middle attacks.

- **wireshark** - Network protocol analyzer.
- **arpspoof -i [interface] -t [target]** - Perform ARP spoofing.
- **dsniff** - Password sniffing for various protocols.
- **tcpdump -i [interface]** - Packet capturing tool.
- **macchanger -r [interface]** - Randomize MAC address.

Post-Exploitation

- **meterpreter** - Metasploit post-exploitation framework.
- **beef-xss** - Browser Exploitation Framework.
- **empire** - Control machines using PowerShell or Python agents.
- **mimikatz** - Extract Windows credentials and perform post-exploitation tasks.
- **powersploit** - Post-exploitation PowerShell scripts.

Social Engineering

- **setoolkit** - Social Engineering Toolkit.
- **evilginx2** - Advanced phishing framework for man-in-the-middle attacks.
- **gophish** - Phishing campaign toolkit.

Web Application Hacking

- **burpsuite** - Web application security testing and proxy tool.
- **zap** - OWASP Zed Attack Proxy for web app scanning.
- **xsser -u [url]** - Detect and exploit XSS vulnerabilities.
- **sqlmap -u [url]** - Automated SQL injection testing.
- **nikto -h [host]** - Web server vulnerability scanner.

Exfiltration and Data Analysis

- **netcat [options]** - Transfer files or open a backdoor.
- **scp [source] [destination]** - Securely copy files over SSH.
- **binwalk [file]** - Extract hidden data from binary files.
- **foremost -i [image-file]** - File recovery and carving.

Denial of Service (DoS)

- **hping3 [target]** - Craft custom network packets for DoS/DDoS attacks.
- **slowloris [target]** - Slow HTTP DoS attack tool.
- **loic** - Low Orbit Ion Cannon for DoS.
- **ufonet** - DDoS attack tool using botnets.

Privilege Escalation

- **linpeas.sh** - Script to find privilege escalation paths on Linux.
- **winpeas.exe** - Privilege escalation auditing for Windows.
- **sudo -l** - Check available sudo privileges.
- **gtfobins** - Find privilege escalation exploits using binaries.

Cryptography and Steganography

- **gpg --encrypt --recipient [user] [file]** - Encrypt files.
- **openssl enc -aes-256-cbc -in [input-file] -out [output-file]** - File encryption.
- **stegdetect [file]** - Detect steganography in images.

- **steghide** - Embed and extract data from images or audio files.

Disclaimer: Use these commands responsibly and only in environments where you have explicit permission. Unauthorized use is illegal and unethical.

Comprehensive Guide to Kali Linux Commands and Tools

General Linux Commands

File and Directory Management

Command	Description	Example
ls	List files and directories.	**ls -la**
cd [directory]	Change directory.	**cd /home/user**
pwd	Print the current directory.	**pwd**
mkdir [directory]	Create a new directory.	**mkdir projects**
rm [file]	Delete a file.	**rm data.txt**
cp [source] [dest]	Copy files or directories.	**cp file.txt /tmp**
mv [source] [dest]	Move or rename files.	**mv oldname.txt newname.txt**

User Management

Command	Description	Example
whoami	Show the current user.	**whoami**
sudo [command]	Execute commands as superuser.	**sudo apt update**
adduser [username]	Add a new user.	**adduser hacker**

System Information

Command	Description	Example
uname -a	Show system information.	**uname -a**
uptime	Show system uptime.	**uptime**
dmesg	View kernel log messages.	**dmesg

Networking Commands

General Networking

Command	Description	Example
ifconfig	View or configure network interfaces.	**ifconfig**
ip a	Show IP addresses and interfaces.	**ip a**
ping [host]	Test connectivity to a host.	**ping 8.8.8.8**
netstat	Display network connections.	**netstat -an**

Advanced Networking

Command	Description	Example
tcpdump	Capture network packets.	**tcpdump -i etho**
nmap [target]	Network mapping and scanning.	**nmap -A -T4 scanme.nmap.org**
traceroute [host]	Trace the path packets take.	**traceroute google.com**

Package Management

Command	Description	Example
apt update	Update package list.	**sudo apt update**
apt upgrade	Upgrade installed packages.	**sudo apt upgrade**
apt install [pkg]	Install a package.	**sudo apt install wireshark**

Kali Linux Tools

Information Gathering Tools

Tool	Description	Example
nmap	Network scanner to discover hosts.	**nmap -sS 192.168.0.0/24**
whois	Query domain ownership information.	**whois example.com**
theHarvester	Gather emails, subdomains, and more.	**theHarvester -d example.com**

Vulnerability Analysis Tools

Tool	Description	Example
nikto	Web server vulnerability scanner.	**nikto -h http://example.com**
wpscan	WordPress vulnerability scanner.	**wpscan --url http://example.com**

Exploitation Tools

Tool	Description	Example
msfconsole	Metasploit Framework console.	**msfconsole**
sqlmap	SQL injection automation tool.	**sqlmap -u http://example.com**

Password Cracking Tools

Tool	Description	Example
hydra	Brute-force login credentials.	**hydra -l admin -P passwords.txt -t 4 http://example.com**
john	Password cracker.	**john hashes.txt**
hashcat	Advanced password recovery.	**hashcat -m 0 hash.txt wordlist.txt**

Wireless Attacks

Tool	Description	Example

Tool	Description	Example
airmon-ng	Enable monitor mode on Wi-Fi interface.	**airmon-ng start wlano**
airodump-ng	Capture wireless packets.	**airodump-ng wlanomon**
aircrack-ng	Crack WPA/WEP keys.	**aircrack-ng capture.cap**

Sniffing and Spoofing Tools

Tool	Description	Example
wireshark	Network protocol analyzer.	**wireshark**
arpspoof	Perform ARP spoofing.	**arpspoof -i etho -t 192.168.0.1**

Social Engineering Tools

Tool	Description	Example
setoolkit	Social Engineering Toolkit.	**setoolkit**

Forensics Tools

Tool	Description	Example
autopsy	Forensic analysis GUI.	**autopsy**
binwalk	Analyze binary files.	**binwalk firmware.bin**

Usage Examples

Example 1: Scanning a Network

```
nmap -A -T4 192.168.1.1
```

- -A: Perform OS detection, version detection, script scanning, and traceroute.

- -T4: Faster execution.

Example 2: SQL Injection Test

```
sqlmap -u "http://example.com/product?id=1" --dbs
--dbs: Retrieve database names.
```

Example 3: Cracking a WPA2 Wi-Fi Network

```
airmon-ng start wlano
airodump-ng wlanomon
aireplay-ng --deauth 10 -a [AP-MAC] -c [Client-MAC] wlanomon
aircrack-ng capture.cap
```

Disclaimer: Use these tools responsibly and only in environments where you have explicit permission. Unauthorized use is illegal and unethical.

APPAZON