Pentesting Cheatsheet

Port Scanning/Version Detection Tools

- nmap
- masscan

SNMP Enumeration Tools

- onesixtyone
- snmpwalk

SMB Enumeration Tools

- enum4linux
- smbclient
- smbmap

SMB Concepts

- Checking for Null Sessions
- Reading/Writing to the filesystem

FTP Concepts

- Checking for anonymous login
- Reading/Writing to the filesystem

Web Application Enumeration Tools

- Burp Proxy Suite
- Nikto
- Gobuster
- Dirsearch
- Netcat
- Wpscan (for Wordpress)
- Joomscan (for Joomla)
- SQLmap

Web Application Concepts

- Banner grabbing for Webserver
- Application version discovery
- Dirbusting
- Testing for SQL injection
- Testing for LFI/RFI
- Subdomain enumeration
- Command injection

Vulnerability/Exploit Research

- Google
- ExploitDB
- Searchsploit
- CVE Database

Working with Exploits

- GNU Compiler Collection (gcc)
- msfvenom

File Transfers

- netcat
- wget
- powershell
- SMB
- FTP

Exploitation

- Metasploit (msfconsole)
- Google

Brute Forcing

- Hydra
- Medusa
- John the Ripper
- Hashcat

Privilege Escalation Enumeration Tools

- Linux priv checker
- Linenum.sh
- Windows Exploit Suggester
- Privilege Escalation Checklists
    - Windows – Fuzzy Security
    - Nix – Gotmilk
- Metasploit Gather/Post/Auxiliary modules

Privilege Escalation Concepts

- Services running as Root or System
- SUID/GUID Binaries
- Kernel exploits