Penetration Testing Tools Cheat Sheet

A quick reference guide to essential penetration testing tools, commands, and techniques for cybersecurity professionals.

Reconnaissance Tools

Nmap (Network Mapper)

Description: Nmap is a powerful network scanning tool used for discovery and security auditing.

Basic Usage: `nmap <target>`

Syntax:
`-sS`: TCP SYN scan (stealth scan)
`-sV`: Version detection
`-O`: OS detection
`-p`: Port specification (e.g., `-p 80,443`)
`-A`: Aggressive scan (OS detection, version detection, script scanning, and traceroute)

Examples:
`nmap -sS <target>`: Perform a SYN scan to identify open ports.
`nmap -sV <target>`: Determine service versions running on open ports.
`nmap -O <target>`: Identify the operating system of the target.
`nmap -p 1-1000 <target>`: Scan ports 1 to 1000.

NSE Scripts: Nmap Scripting Engine (NSE) allows for advanced vulnerability detection and exploitation.

Example:
`nmap --script vuln <target>`: Use vulnerability scanning scripts.

Output Interpretation: Understand the scan results to identify open ports, services, and potential vulnerabilities.

Whois

Description: Whois is a query protocol used to retrieve registration information of domain names or IP addresses.

Basic Usage: `whois <domain>` or `whois <IP address>`

Purpose: Obtain contact information, registration dates, and nameserver details.

Example:
`whois example.com`: Retrieve Whois information for the domain example.com.

Nslookup

Description: Nslookup is a network administration tool used to query the Domain Name System (DNS) to obtain domain name or IP address mapping information.

Basic Usage: `nslookup <domain>`

Purpose: Verify DNS records, troubleshoot DNS resolution issues.

Example:
`nslookup example.com`: Retrieve IP address associated with example.com.

Vulnerability Scanning Tools

Nessus

Description: Nessus is a comprehensive vulnerability scanner used to identify security weaknesses in systems and applications.

Key Features:

- Vulnerability detection
- Configuration auditing
- Compliance checks

Usage:

1. Install and configure Nessus.
2. Define scan targets and policies.
3. Launch scans and analyze reports.

Report Interpretation: Understand the severity levels and remediation steps for identified vulnerabilities.

OpenVAS

Description: OpenVAS is an open-source vulnerability scanner that provides comprehensive vulnerability management.

Key Features:

- Vulnerability scanning
- Asset discovery
- Compliance reporting

Usage:

1. Install and configure OpenVAS.
2. Define scan targets and policies.
3. Launch scans and review reports.

Benefits:

- Open-source and customizable
- Regularly updated vulnerability tests

Nikto

Description: Nikto is a web server scanner that identifies potential security vulnerabilities in web applications.

Basic Usage: `nikto -h <target>`

Syntax:
`-h`: Target host
`-p`: Target port
`-ssl`: Force SSL mode

Examples:
`nikto -h example.com`: Scan example.com for vulnerabilities.
`nikto -h example.com -p 8080`: Scan example.com on port 8080.

Output Analysis: Review the scan results to identify potential security issues, such as outdated software, default configurations, and common vulnerabilities.

Web Application Testing Tools

Burp Suite

Description: Burp Suite is a comprehensive web application security testing tool used for intercepting, analyzing, and manipulating HTTP traffic.

Key Components:

- Proxy: Intercepts HTTP/S traffic
- Scanner: Automated vulnerability scanning
- Intruder: Customizable attack tool

Usage:

1. Configure Burp Suite as a proxy.
2. Intercept and analyze web application traffic.
3. Use the scanner to identify vulnerabilities.
4. Employ the intruder to perform customized attacks.

Benefits:

- Interception and modification of requests
- Automated vulnerability scanning
- Extensibility via plugins

OWASP ZAP

Description: OWASP ZAP (Zed Attack Proxy) is an open-source web application security scanner and intercepting proxy.

Key Features:

- Intercepting proxy
- Automated scanning
- Fuzzing capabilities

Usage:

1. Configure ZAP as a proxy.
2. Intercept and analyze web application traffic.
3. Use the scanner to identify vulnerabilities.
4. Perform manual testing and fuzzing.

Advantages:

- Open-source and free to use
- Active community support
- Extensible with plugins

SQLmap

Description: SQLmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities.

Basic Usage: `sqlmap -u <target>`

Syntax:
`-u`: Target URL
`--dbs`: Enumerate databases
`--tables`: Enumerate tables
`--columns`: Enumerate columns
`--dump`: Dump data

Examples:
`sqlmap -u "http://example.com/vuln.php?id=1" --dbs`: Enumerate databases.
`sqlmap -u "http://example.com/vuln.php?id=1" --tables -D <database>`: Enumerate tables in a specific database.
`sqlmap -u "http://example.com/vuln.php?id=1" --columns -T <table_name> -D <database>`: Enumerate columns in a specific table.

Exploitation: Use SQLmap to exploit SQL injection vulnerabilities and retrieve sensitive data.

Exploitation Tools

Metasploit Framework

Description: Metasploit is a powerful penetration testing framework used for developing and executing exploit code against a target system.

Key Modules:

- Exploits: Code to take advantage of vulnerabilities
- Payloads: Code to execute on the target system
- Auxiliary: Support modules for scanning and reconnaissance

Usage:

1. Launch Metasploit console (`msfconsole`).
2. Search for and select an appropriate exploit.
3. Configure the exploit parameters (e.g., target IP, port).
4. Choose a payload to execute on the target.
5. Run the exploit.

Commands:

- `search`: Search for exploits, payloads, and modules
- `use`: Select a module
- `show options`: Display module options
- `set`: Set module options
- `exploit`: Run the exploit

Social Engineering Toolkit (SET)

Description: SET is an open-source penetration testing framework designed for social engineering attacks.

Key Features:

- Spear-phishing attacks
- Website cloning
- Credential harvesting

Usage:

1. Launch SET.
2. Select an attack vector (e.g., spear-phishing).
3. Configure attack parameters (e.g., email templates, target lists).
4. Launch the attack.

Ethical Considerations: Use SET responsibly and with proper authorization.

Hydra

Description: Hydra is a parallelized login cracker which supports numerous protocols to attack.

Basic Usage: `hydra <target> <protocol> <options>`

Syntax:
`-L`: Username list
`-P`: Password list
`-vV`: Verbose mode
`-t`: Number of threads
`<protocol>`: ssh, ftp, smtp, etc.

Examples:
`hydra -L user.txt -P pass.txt ssh://<target>`: Brute-force SSH login using provided lists.
`hydra -l <username> -P pass.txt ftp://<target>`: Brute-force FTP login for a specific user.

Legal and Ethical Use: Always ensure you have explicit permission before attempting to crack logins on a system.