Cheat Sheet for comprehensive CompTIA PenTest+

1. Pre-Engagement Interactions

- **Scope Definition:**
  - **Objectives:** Clearly define the goals of the engagement.
  - **Deliverables:** List expected reports, findings, and recommendations.
  - **Rules of Engagement:** Document legal and ethical boundaries.
  - **Communication Plan:** Establish contact points and escalation paths.
- **Legal Considerations:**
  - **NDA (Non-Disclosure Agreement):** Ensure confidentiality.
  - **Authorization:** Obtain written permission from stakeholders.
  - **Data Handling:** Define how data will be stored, processed, and destroyed.

2. Information Gathering

- **Active Reconnaissance:**
  - **Ping Sweep:** `nmap -sn <target_range>`
  - **Port Scanning:** `nmap -p- <target>`
  - **Service Enumeration:** `nmap -sV <target>`
  - **OS Detection:** `nmap -O <target>`
- **Passive Reconnaissance:**
  - **WHOIS Lookup:** `whois <domain>`
  - **DNS Enumeration:** `dig <domain>`
  - **Social Media:** Gather information from public profiles.
  - **Search Engines:** Use `site:` operator in Google.
- **Tools:**
  - **Nmap:** Network scanning and enumeration.

  - **Shodan:** Internet-wide device search engine.

  - **TheHarvester:** Email, subdomain, and host enumeration.

  - **Recon-ng:** Full-featured reconnaissance framework.

3. Vulnerability Analysis

- **Manual Testing:**

  - **OWASP Top 10:** Focus on critical vulnerabilities.

  - **Fuzzing:** Use tools like `ffuf` or `Burp Suite` for input testing.

  - **Code Review:** Analyze source code for vulnerabilities.

- **Automated Scanning:**

  - **Nessus:** Comprehensive vulnerability scanner.

  - **OpenVAS:** Open-source vulnerability assessment tool.

  - **Qualys:** Cloud-based vulnerability management.

- **Configuration Review:**

  - **Checklists:** Use CIS benchmarks.

  - **Network Diagrams:** Verify security controls.

  - **Patch Management:** Ensure systems are up-to-date.

4. Exploitation

- **Exploit Selection:**

  - **ExploitDB:** Search for known exploits.

  - **Metasploit:** Use `search` command to find exploits.

  - **CVE Details:** Check for specific vulnerabilities.

- **Exploit Execution:**

  - **Metasploit:** `use <exploit>`, `set options`, `exploit`

  - **Manual Exploits:** Compile and run custom exploits.

  - **Post-Exploitation:** Use `meterpreter` for further actions.

- **Privilege Escalation:**

  - **Local Exploits:** Use `local_exploit_suggester` in Metasploit.
  - **Kernel Exploits:** Check for outdated kernel versions.
  - **Misconfigurations:** Exploit weak file permissions.

5. Post-Exploitation

- **Persistence:**
  - **Backdoors:** Create persistent access points.
  - **Scheduled Tasks:** Use `at` or `cron` jobs.
  - **Registry Keys:** Modify registry for persistence.
- **Data Exfiltration:**
  - **Encrypted Channels:** Use `SSH` or `SSL` tunnels.
  - **Steganography:** Hide data within other files.
  - **Exfiltration Tools:** Use `C2` frameworks like `Cobalt Strike`.
- **Lateral Movement:**
  - **Pivoting:** Use `sshuttle` or `socat` for tunneling.
  - **Pass-the-Hash:** Use `mimikatz` to move laterally.
  - **Exploit Trust Relationships:** Abuse domain trusts.

6. Reporting

- **Structure:**
  - **Executive Summary:** High-level overview.
  - **Technical Findings:** Detailed vulnerability descriptions.
  - **Remediation:** Step-by-step fixes and recommendations.
  - **Appendices:** Include raw data, logs, and tools used.
- **Visual Aids:**
  - **Charts:** Use pie charts for vulnerability distribution.
  - **Tables:** Summarize findings and remediation steps.
  - **Screenshots:** Capture critical evidence.

- **Tools:**
  - **Word/Excel:** For structured reports.
  - **Markdown:** For quick documentation.
  - **Jira/Confluence:** For collaborative reporting.

7. Tools and Resources

- **Penetration Testing Frameworks:**
  - **Metasploit:** Comprehensive exploitation framework.
  - **Cobalt Strike:** Advanced C2 and post-exploitation tool.
  - **Burp Suite:** Web application security testing.
- **Network Tools:**
  - **Wireshark:** Packet analysis.
  - **Tcpdump:** Command-line packet capture.
  - **Netcat:** Network utility for reading/writing network connections.
- **Exploitation Tools:**
  - **Mimikatz:** Credential extraction.
  - **John the Ripper:** Password cracking.
  - **Hydra:** Brute-force tool for various protocols.
- **Vulnerability Databases:**
  - **CVE Details:** Search for specific CVEs.
  - **NVD (National Vulnerability Database):** Comprehensive vulnerability information.
  - **ExploitDB:** Repository of exploits and vulnerable software.

8. Best Practices

- **Documentation:**
  - **Thorough Notes:** Document every step and finding.
  - **Version Control:** Use Git for tracking changes.

  - **Backup:** Keep backups of all data and findings.

- **Ethical Considerations:**

  - **Respect Privacy:** Avoid unnecessary data exposure.

  - **Transparency:** Keep stakeholders informed.

  - **Legal Compliance:** Follow local laws and regulations.

- **Continuous Learning:**

  - **Stay Updated:** Follow security blogs and forums.

  - **Hands-On Practice:** Regularly practice with labs and CTFs.

  - **Certifications:** Pursue advanced certifications like OSCP, CEH.

9. Common Pitfalls

- **Scope Creep:**

  - **Avoid:** Expanding scope without permission.

  - **Solution:** Regularly review and confirm scope.

- **Lack of Communication:**

  - **Avoid:** Not keeping stakeholders informed.

  - **Solution:** Establish clear communication channels.

- **Incomplete Reporting:**

  - **Avoid:** Missing critical details in the report.

  - **Solution:** Use checklists and templates.

10. Advanced Techniques

- **Evasion Techniques:**

  - **AV Evasion:** Use tools like `Veil-Evasion`.

  - **Firewall Bypass:** Use `ICMP` tunneling.

  - **Sandbox Detection:** Identify and evade sandbox environments.

- **Custom Exploits:**

  - **Buffer Overflow:** Write custom exploits for known vulnerabilities.

  - **Shellcode:** Develop custom shellcode for specific targets.

  - **ROP Chains:** Use Return-Oriented Programming for exploitation.

- **Advanced Post-Exploitation:**

  - **Fileless Attacks:** Use PowerShell or WMI for stealth.

  - **DLL Hijacking:** Exploit DLL loading mechanisms.

  - **Credential Dumping:** Use `Mimikatz` for advanced credential extraction.

11. Resources for Further Learning

- **Books:**

- "The Web Application Hacker's Handbook" by Dafydd Stuttard
- "Metasploit: The Penetration Tester's Guide" by David Kennedy

- **Online Courses:**

  - **Cybrary:** Free and paid courses on penetration testing.

  - **Udemy:** Comprehensive courses on various penetration testing topics.

- **Communities:**

  - **Reddit:** r/netsec, r/AskNetSec

  - **Twitter:** Follow security researchers and experts.

- **Conferences:**

  - **DEF CON:** World's largest hacker conference.

  - **Black Hat:** Premier security conference.

  - **BSides:** Community-driven security conferences.

12. Legal and Ethical Considerations

- **Legal Frameworks:**

  - **GDPR:** Data protection regulations in Europe.

  - **HIPAA:** Health information privacy in the U.S.

  - **CFAA:** U.S. Computer Fraud and Abuse Act.

- **Ethical Guidelines:**

  - **Respect Privacy:** Do not access or disclose personal information.

  - **Do No Harm:** Avoid causing disruptions or damage.

  - **Transparency:** Clearly communicate findings and methods.

- **Professional Standards:**

  - **(ISC)^2 Code of Ethics:** Guidelines for security professionals.

  - **CREST:** Standards for penetration testing and security services.

13. Post-Engagement Activities

- **Debriefing:**

  - **Stakeholder Meeting:** Discuss findings and recommendations.

  - **Lessons Learned:** Identify areas for improvement.

- **Follow-Up:**

  - **Remediation Verification:** Ensure fixes are implemented correctly.

  - **Continuous Monitoring:** Set up ongoing security monitoring.

- **Documentation:**

  - **Final Report:** Submit a comprehensive report.

  - **Archiving:** Store all documentation securely.

14. Tips and Tricks

- **Automation:**

  - **Scripts:** Automate repetitive tasks with Python or Bash.

  - **Frameworks:** Use frameworks like `Pupy` for multi-platform C2.

- **Stealth:**

  - **Low-and-Slow:** Avoid detection by performing actions slowly.

  - **Covert Channels:** Use covert channels for communication.

- **Resourcefulness:**

  - **Google Dorks:** Use advanced search techniques for recon.

  - **OSINT:** Leverage open-source intelligence tools.

15. Common Command Line Shortcuts

- **Navigation:**

- `cd`: Change directory.
- `ls`: List directory contents.
- `pwd`: Print working directory.

- **File Management:**

- `cp`: Copy files and directories.
- `mv`: Move or rename files and directories.
- `rm`: Remove files or directories.

- **Network:**

- `ping`: Send ICMP ECHO_REQUEST to network hosts.
- `traceroute`: Trace the route to a network host.
- `netstat`: Display network connections, routing tables, interface statistics.

- **Text Processing:**

- `grep`: Search text with patterns.
- `awk`: Pattern scanning and processing language.
- `sed`: Stream editor for filtering and transforming text.

16. Common Metasploit Commands

- **Core Commands:**

- `help`: Display help menu.
- `search`: Search for exploits.
- `use`: Select a module.
- `set`: Set module options.
- `exploit`: Run the exploit.

- **Post-Exploitation:**

- `sessions`: List active sessions.
- `migrate`: Migrate to another process.
- `getsystem`: Attempt to elevate privileges.

- **Auxiliary Modules:**

- `auxiliary/scanner/`: Various scanning modules.
- `auxiliary/dos/`: Denial of service modules.

17. Common Nmap Commands

- **Basic Scanning:**

- `nmap -sP <target>`: Ping scan.
- `nmap -sS <target>`: SYN scan.
- `nmap -sV <target>`: Service version detection.

- **Advanced Scanning:**

- `nmap -O <target>`: Operating system detection.
- `nmap -A <target>`: Aggressive scan.
- `nmap -p- <target>`: Scan all ports.

- **Scripting:**

- `nmap --script <script_name> <target>`: Run NSE scripts.
- `nmap --script vuln <target>`: Run vulnerability scripts.

18. Common Wireshark Filters

- **Protocol Filter:**

- `tcp`: Filter TCP packets.
- `udp`: Filter UDP packets.
- `http`: Filter HTTP packets.

- **Source/Destination Filter:**

- `ip.src == <source_ip>`: Filter by source IP.
- `ip.dst == <destination_ip>`: Filter by destination IP.

- **Port Filter:**

- `tcp.port == <port_number>`: Filter by TCP port.
- `udp.port == <port_number>`: Filter by UDP port.

- **Advanced Filter:**

- `http.request.method == "GET"`: Filter HTTP GET requests.
- `ssl.handshake.type == 1`: Filter SSL client hello packets.

19. Common Burp Suite Shortcuts

- **Proxy:**

- `Ctrl+R`: Forward intercepted request.
- `Ctrl+Shift+R`: Drop intercepted request.
- `Ctrl+I`: Intercept is on/off.

- **Intruder:**

- `Ctrl+I`: Start attack.
- `Ctrl+E`: Clear payloads.
- `Ctrl+P`: Paste payloads.

- **Repeater:**

- `Ctrl+R`: Send request to Repeater.
- `Ctrl+Shift+R`: Send to Intruder.
- `Ctrl+Shift+T`: Send to Sequencer.

20. Common Python Libraries for PenTesting

- **Requests:**

- `pip install requests`: HTTP library for making requests.
- Example: `requests.get('http://example.com')`

- **Scapy:**

- `pip install scapy`: Packet manipulation library.
- Example: `send(IP(dst="192.168.1.1")/ICMP())`

- **Impacket:**

- `pip install impacket`: Network protocols library.
- Example: `smbclient.py <domain>/<user>:<password>@<target>`

- **Paramiko:**

- `pip install paramiko`: SSH2 protocol library.
- Example: `ssh = paramiko.SSHClient()`

21. Common PowerShell Commands

- **File System:**

- `Get-ChildItem`: List directory contents.
- `Copy-Item`: Copy files and directories.
- `Move-Item`: Move files and directories.

- **Network:**

- `Test-Connection`: Ping a remote host.
- `Get-NetIPConfiguration`: Get network configuration.
- `Invoke-WebRequest`: Make HTTP requests.

- **Security:**

- `Get-Process`: List running processes.
- `Get-Service`: List services.
- `Get-EventLog`: Retrieve event logs.

22. Common Linux Commands

- **File System:**

- `ls -la`: List all files, including hidden ones.
- `cp -r <source> <destination>`: Copy directories recursively.
- `mv <source> <destination>`: Move or rename files.

- **Network:**

- `ifconfig`: Display network interface configuration.
- `route`: Display or modify the IP routing table.
- `netstat -an`: Display active network connections.

- **Security:**

- `chmod <permissions> <file>`: Change file permissions.
- `chown <user>:<group> <file>`: Change file owner and group.
- `sudo`: Execute a command as another user.

23. Common Windows Commands

- **File System:**

- `dir`: List directory contents.
- `copy <source> <destination>`: Copy files.
- `move <source> <destination>`: Move files.

- **Network:**

- `ping <target>`: Send ICMP echo requests.
- `ipconfig`: Display network configuration.
- `netstat -an`: Display active network connections.

- **Security:**

- `tasklist`: List running processes.
- `sc query`: List services.
- `eventvwr`: Open Event Viewer.

24. Common SQL Injection Techniques

- **Basic Injection:**

- `' OR '1'='1`: Bypass authentication.

- `UNION SELECT`: Combine results from multiple queries.

- **Error-Based Injection:**

- `1=1`: Trigger an error to extract information.
- `UNION SELECT NULL`: Detect number of columns.

- **Blind Injection:**

- `AND 1=1`: True condition.
- `AND 1=2`: False condition.

- **Time-Based Injection:**

- `AND SLEEP(5)`: Delay response to detect injection.

25. Common XSS (Cross-Site Scripting) Techniques

- **Stored XSS:**

- `<script>alert('XSS')</script>`: Inject script

By Ahmed Baheeg Khorshid

ver 1.0