Cheat Sheet for Certified Ethical Hacker (CEH)

Certified Ethical Hacker (CEH) Cheat Sheet

1. Introduction to Ethical Hacking

- **Definition**: Ethical hacking involves legally breaking into computers and devices to test an organization's defenses.

- **CEH Domains**: 20 major domains covered in the CEH certification.

- **Ethical Hacker's Code of Conduct**:

- Obtain proper permission.
- Define the scope of the test.
- Maintain confidentiality.
- Do not cause damage.
- Report vulnerabilities.

---

2. Reconnaissance

- **Passive Reconnaissance**:

  - **Tools**:

    - **Whois**: Domain information.

    - **Nslookup/Dig**: DNS queries.

    - **Google Dorks**: Advanced search queries.

    - **Shodan**: Internet-connected device search.

  - **Techniques**:

- Social media profiling.
- Public records search.

- **Active Reconnaissance**:

  - **Tools**:

    - **Nmap**: Network scanning.

- **Nikto**: Web server scanning.
- **TheHarvester**: Email and subdomain gathering.

- **Techniques**:

- Ping sweeps.
- Port scanning.

---

3. Scanning and Enumeration

- **Network Scanning**:

- **Nmap Commands**:

- `nmap -sP <target>`: Ping scan.
- `nmap -sS <target>`: SYN scan.
- `nmap -sV <target>`: Version detection.
- `nmap -O <target>`: OS detection.

- **Masscan**: High-speed network scanner.

- **Port Scanning**:

- **Types**:

- TCP Connect Scan.
- SYN Scan.
- UDP Scan.

- **Tools**:

- **Nmap**: `nmap -sU <target>` for UDP scan.
- **Unicornscan**: Fast UDP and TCP port scanner.

- **Enumeration**:

- **Tools**:

- **Nmap**: `nmap -sC <target>` for script scanning.
- **Enum4linux**: Windows and Samba enumeration.
- **Nbtscan**: NetBIOS name enumeration.

- **Techniques**:

- DNS enumeration.
- SMB enumeration.
- LDAP enumeration.

---

4. Vulnerability Analysis

- **Tools**:
  - **Nessus**: Comprehensive vulnerability scanner.
  - **OpenVAS**: Open-source vulnerability assessment tool.
  - **Qualys**: Cloud-based vulnerability management.
- **Techniques**:
  - **CVE**: Common Vulnerabilities and Exposures.
  - **CVSS**: Common Vulnerability Scoring System.
  - **Exploit Databases**:
    - **Exploit-DB**: Search for known exploits.
    - **Metasploit**: Exploit framework.

---

5. System Hacking

- **Gaining Access**:
  - **Brute Force**:
    - **Tools**:
      - **Hydra**: Online password cracking.
      - **John the Ripper**: Offline password cracking.
  - **Exploitation**:
    - **Metasploit**: `msfconsole` for launching exploits.
    - **Searchsploit**: Search for exploits in Exploit-DB.
- **Maintaining Access**:

- **Backdoors**:
  - **Metasploit**: `exploit/multi/handler` for reverse shells.
  - **Webshells**: PHP, ASP, etc.
- **Persistence**:
  - **Registry Keys**: Add startup entries.
  - **Scheduled Tasks**: Create scheduled tasks.
- **Covering Tracks**:
  - **Logs**:
    - **Linux**: `/var/log/` directory.
    - **Windows**: Event Viewer.
  - **Tools**:
    - **Logtamper**: Modify log files.
    - **Metasploit**: `timestomp` for modifying file timestamps.

---

6. Malware Threats

- **Types**:
  - **Viruses**: Self-replicating.
  - **Worms**: Self-replicating without host file.
  - **Trojans**: Disguised as legitimate software.
  - **Ransomware**: Encrypts data and demands ransom.
  - **Spyware**: Collects information without consent.
- **Tools**:
  - **Cuckoo Sandbox**: Automated malware analysis.
  - **YARA**: Malware identification tool.
  - **VirusTotal**: Online malware analysis.

---

7. Sniffing

- **Tools**:
  - **Wireshark**: Network protocol analyzer.
  - **Tcpdump**: Command-line packet analyzer.
  - **Ettercap**: Man-in-the-middle attack tool.
- **Techniques**:
  - **ARP Spoofing**: Redirect traffic.
  - **DNS Spoofing**: Redirect DNS queries.
  - **SSL Stripping**: Downgrade HTTPS to HTTP.

---

8. Social Engineering

- **Types**:
  - **Phishing**: Deceptive emails.
  - **Pretexting**: Creating a scenario.
  - **Baiting**: Offering something enticing.
  - **Tailgating**: Following someone into a secure area.
- **Tools**:
  - **SET (Social-Engineer Toolkit)**: Phishing and social engineering framework.
  - **King Phisher**: Phishing campaign tool.
- **Prevention**:
  - **Training**: Regular security awareness training.
  - **Multi-Factor Authentication**: Additional layer of security.

---

9. Denial of Service (DoS)

- **Types**:

- **Ping of Death**: Sending oversized ICMP packets.
- **SYN Flood**: Overwhelming the target with SYN requests.
- **Smurf Attack**: Amplifying ICMP requests.
- **Teardrop Attack**: Fragmented IP packets.

- **Tools**:
- **Hping3**: Custom packet crafting.
- **LOIC (Low Orbit Ion Cannon)**: Distributed DoS tool.
- **Slowloris**: Slow HTTP request attack.

---

10. Session Hijacking

- **Types**:
- **Passive Hijacking**: Sniffing sessions.
- **Active Hijacking**: Injecting malicious code.

- **Tools**:
- **Ettercap**: Man-in-the-middle attack tool.
- **Bettercap**: Comprehensive network hacking tool.

- **Prevention**:
- **HTTPS**: Encrypted sessions.
- **Session Expiry**: Regular session timeouts.

---

11. Evading IDS, Firewalls, and Honeypots

- **IDS/Firewall Evasion**:
- **Fragmentation**: Splitting packets.
- **Source Routing**: Defining the route.
- **Proxy Chains**: Multiple proxies.

- **Honeypots**:
  - **Types**:
    - **Low-Interaction**: Limited interaction.
    - **High-Interaction**: Full system simulation.
  - **Tools**:
    - **Kippo**: SSH honeypot.
    - **Dionaea**: Multi-protocol honeypot.

---

12. Hacking Web Servers

- **Tools**:
  - **Nikto**: Web server scanner.
  - **Dirb**: Directory brute-forcing.
  - **Burp Suite**: Web vulnerability scanner.
- **Techniques**:
  - **Directory Traversal**: Accessing restricted directories.
  - **File Inclusion**: Including remote files.
  - **Misconfigurations**: Improper server settings.

---

13. Hacking Web Applications

- **Tools**:
  - **OWASP ZAP**: Web application security scanner.
  - **Burp Suite**: Comprehensive web vulnerability scanner.
  - **SQLmap**: Automated SQL injection tool.
- **Techniques**:
  - **XSS**: Cross-Site Scripting.

- **CSRF**: Cross-Site Request Forgery.
- **File Upload Vulnerabilities**: Uploading malicious files.

---

14. SQL Injection

- **Types**:
  - **In-Band**: Same channel for attack and data retrieval.
  - **Blind**: No direct output.
  - **Out-of-Band**: Different channel for data retrieval.
- **Tools**:
  - **SQLmap**: Automated SQL injection tool.
  - **Havij**: Automated SQL injection tool.
- **Prevention**:
  - **Prepared Statements**: Use parameterized queries.
  - **Input Validation**: Validate and sanitize inputs.

---

15. Hacking Wireless Networks

- **Tools**:
  - **Aircrack-ng**: Wireless security suite.
  - **Kismet**: Wireless network detector.
  - **Reaver**: WPS brute-force tool.
- **Techniques**:
  - **WEP Cracking**: Weak encryption.
  - **WPA/WPA2 Cracking**: Dictionary and brute-force attacks.
  - **Evil Twin**: Fake access point.

---

16. Hacking Mobile Platforms

- **Tools**:
  - **MobSF (Mobile Security Framework)**: Mobile app security testing.
  - **APKTool**: Reverse engineering Android APKs.
  - **Jadx**: Dex to Java decompiler.
- **Techniques**:
  - **Reverse Engineering**: Analyzing app binaries.
  - **Man-in-the-Middle**: Intercepting mobile traffic.
  - **Exploiting Vulnerabilities**: Known app vulnerabilities.

---

17. IoT and OT Hacking

- **Tools**:
  - **Shodan**: IoT device search engine.
  - **Metasploit**: Exploiting IoT vulnerabilities.
  - **Firmware Analysis**: Binwalk, Firmadyne.
- **Techniques**:
  - **Default Credentials**: Exploiting default settings.
  - **Firmware Analysis**: Extracting and analyzing firmware.
  - **Network Protocols**: Exploiting insecure protocols.

---

18. Cloud Computing

- **Tools**:
  - **CloudSploit**: Cloud security scanner.
  - **ScoutSuite**: Multi-cloud security auditing.
  - **Nessus**: Vulnerability scanner for cloud environments.
- **Techniques**:

- **Misconfigurations**: Improper cloud settings.
- **Data Leaks**: Exposed storage buckets.
- **IAM Misconfigurations**: Weak identity and access management.

---

19. Cryptography

- **Types**:
  - **Symmetric Encryption**: Single key for encryption and decryption.
  - **Asymmetric Encryption**: Public and private keys.
  - **Hashing**: One-way encryption.
- **Tools**:
  - **OpenSSL**: Command-line tool for encryption.
  - **Hashcat**: Password recovery tool.
  - **John the Ripper**: Password cracking tool.
- **Techniques**:
  - **Brute Force**: Trying all possible keys.
  - **Dictionary Attack**: Using wordlists.
  - **Rainbow Tables**: Precomputed hash values.

---

20. Post-Exploitation Techniques

- **Privilege Escalation**:
  - **Linux**: Exploiting SUID binaries.
  - **Windows**: Exploiting service misconfigurations.
- **Data Exfiltration**:
  - **Exfiltration Over C2**: Using command and control channels.
  - **Exfiltration Over Alternative Protocol**: Using different protocols.

- **Persistence**:
  - **Scheduled Tasks**: Creating scheduled tasks.
  - **Registry Keys**: Adding startup entries.

---

21. Reporting and Documentation

- **Components**:
  - **Executive Summary**: High-level overview.
  - **Technical Details**: Detailed findings.
  - **Remediation Recommendations**: Steps to fix vulnerabilities.
  - **Appendix**: Supporting documents.
- **Tools**:
  - **Word/Excel**: Standard documentation tools.
  - **LaTeX**: Professional document formatting.
  - **PenTest-Tools**: Automated report generation.

This cheat sheet provides a comprehensive overview of the essential concepts, tools, and techniques covered in the Certified Ethical Hacker (CEH) certification. Use this as a quick reference guide to navigate through the various domains of ethical hacking.

By Ahmed Baheeg Khorshid