### **Step 1: Planning and Reconnaissance**

1. **Define Scope and Rules of Engagement**
   * Understand what is allowed and what is off-limits in your test.
   * Get written permission to test the target systems.
2. **Identify Objectives**
   * Define your goals: Are you testing for data theft, system compromise, or privilege escalation?
3. **Gather Intelligence (Passive Reconnaissance)**
   * Use tools like **Maltego**, **Spiderfoot**, and **Tor Browser** to gather OSINT (Open Source Intelligence) on the target.
   * Identify subdomains, employee details, email addresses, and associated infrastructure.

### **Step 2: Active Reconnaissance**

1. **Footprinting**
   * Use tools like **Dnsrecon** and **FOCA** to map the network and extract sensitive metadata.
2. **Perform Email Tracking**
   * Tools like **EmailTrackerPro** can help trace email interactions and understand communication paths.
3. **Map the Network**
   * Use tools like **Nmap** and **Rustscan** to identify live hosts, open ports, and running services.

### **Step 3: Vulnerability Scanning**

1. **Scan Networks for Vulnerabilities**
   * Use **Nessus** or **Sniper** to identify weak points in the target infrastructure.
2. **Analyze Services**
   * Check for misconfigurations or outdated software using **Nmap Scripts** or **MegaPing**.

### **Step 4: Enumeration**

1. **Gather Detailed Information**
   * Use tools like **Advanced IP Scanner**, **NetBIOS Enumerator**, and **SMBeagle** to enumerate shared resources, users, and services.
2. **Active Directory Enumeration**
   * Use tools like **LDAP Explorer** or **Active Directory Explorer** to gather information on directory structures.
3. **SNMP Enumeration**
   * Tools like **SoftPerfect Network Scanner** can extract details from network devices.

### **Step 5: Exploitation**

1. **Target Vulnerabilities**
   * Use tools like **Metasploit** or scripts from **Github** to exploit identified vulnerabilities.
   * For web applications, use tools like **Wpscan** or **Dirsearch**.
2. **System Hacking**
   * Leverage tools like **CrackMapExec**, **Impacket**, and **winPEAS** for privilege escalation or system compromise.
3. **Password Cracking**
   * Use tools like **John the Ripper**, **Hashcat**, or **RainbowCrack** to brute-force or crack hashes.

### **Step 6: Post-Exploitation**

1. **Establish Persistence**
   * Use tools like **SharPersist** or **Havoc** to maintain access.
   * Deploy keyloggers or backdoors where ethical and allowed.
2. **Clear Tracks**
   * Use tools like **Clear\_Event\_Viewer\_Logs** to hide your activities (only for simulation in ethical hacking scenarios).

### **Step 7: Reporting**

1. **Document Findings**
   * Include all vulnerabilities, steps to exploit them, and screenshots of your process.
   * Highlight the business impact of the vulnerabilities.
2. **Provide Recommendations**
   * Suggest actionable steps for remediation, such as patching, configuring firewalls, or improving security protocols.

### **Step 8: Cleanup**

1. **Remove Backdoors**
   * Ensure all tools, scripts, and access points are removed from the target environment.
2. **Validate Fixes**
   * Retest vulnerabilities to confirm they are resolved.
3. **Return Access**
   * Hand over control and conclude the test.

## **1. Footprinting (Reconnaissance)**

### **Tools and Explanation:**

1. **EmailTrackerPro**: Tracks email headers to identify sender's IP, routing paths, and metadata. Useful for investigating phishing attacks or mapping sender locations.
2. **FOCA**: Extracts metadata from public documents (e.g., PDFs, Word files) to uncover sensitive details like usernames, server paths, and software used.
3. **Maltego**: A visual link-analysis tool to map out relationships between people, organizations, domains, and more.
4. **Github**: A repository for open-source projects; used to discover leaked credentials, sensitive files, or misconfigured projects.
5. **Dnsrecon**: Enumerates DNS records and zones. Identifies subdomains, records, and potential DNS misconfigurations.
6. **GRecon**: Automated Google hacking tool to identify indexed sensitive information.
7. **Holehe**: Checks if email addresses are registered on various platforms for OSINT purposes.
8. **Photon**: A web crawler for extracting data such as URLs, files, and metadata from a website.
9. **Sherlock**: Searches for a username across multiple social media platforms.
10. **Spiderfoot**: Comprehensive OSINT automation for domain, IP, and user data.
11. **Tor Browser**: Allows anonymous browsing and recon in the deep web.
12. **Traceroute Tools**: Identifies the route taken by packets to a destination to map network topology.
13. **Path Analyzer Pro**: Advanced traceroute tool with network performance metrics.
14. **Web Data Extractor**: Extracts emails, phone numbers, and other structured data from web pages.
15. **HTTrack Website Copier**: Mirrors entire websites for offline analysis.

### **Order of Use:**

1. **Holehe, Sherlock** (social footprinting)
2. **Github** (code and credential leaks)
3. **Dnsrecon, Photon, Spiderfoot** (network and domain reconnaissance)
4. **FOCA, Maltego** (metadata and relationship mapping)
5. **HTTrack Website Copier, Web Data Extractor** (site mirroring)
6. **Tor Browser** (deep web exploration)
7. **Traceroute Tools, Path Analyzer Pro** (network mapping)

## **2. Scanning Networks**

### **Tools and Explanation:**

1. **Wireshark**: Captures and analyzes network traffic in real-time.
2. **Rustscan**: A fast port scanner with integration options for further analysis.
3. **Angry IP Scanner**: Lightweight and fast scanner for live hosts and ports.
4. **MegaPing**: Multi-purpose tool for ping sweeps and host discovery.
5. **NetScanTools Pro**: Comprehensive suite for network discovery and analysis.
6. **Nmap**: Industry-standard port scanner and network mapper.
7. **Colasoft Packet Builder**: Crafts and sends custom network packets.
8. **sx-Tool**: An advanced network scanning tool.
9. **Packet Crafting Tools**: Tailored network packets for testing firewalls or IDS/IPS.

### **Order of Use:**

1. **Rustscan, Angry IP Scanner, MegaPing** (initial host discovery)
2. **Nmap, NetScanTools Pro** (detailed port and service enumeration)
3. **Wireshark** (traffic analysis)
4. **Colasoft Packet Builder, Packet Crafting Tools** (advanced testing)

## **3. Enumeration**

### **Tools and Explanation:**

1. **Advanced IP Scanner**: Scans network for live devices, IP addresses, and shared resources.
2. **RPCScan**: Identifies exposed Remote Procedure Call services.
3. **SuperEnum**: Automates enumeration tasks like SMB and LDAP discovery.
4. **Active Directory Explorer**: Visualizes and queries Active Directory structures.
5. **NetBIOS Enumerator**: Scans for NetBIOS shares and services.
6. **SMBeagle**: Enumerates SMB shares and permissions.
7. **SoftPerfect Network Scanner**: Finds shared resources and network vulnerabilities.

### **Order of Use:**

1. **Advanced IP Scanner** (basic discovery)
2. **SuperEnum, NetBIOS Enumerator** (shared resources)
3. **RPCScan** (Windows-specific enumeration)
4. **SMBeagle, Active Directory Explorer** (AD and SMB enumeration)

## **4. Vulnerability Analysis**

### **Tools and Explanation:**

1. **Nessus**: Comprehensive vulnerability scanner for networks and systems.
2. **Sniper**: Automated pentesting tool with recon, enumeration, and exploit modules.

### **Order of Use:**

1. **Nessus** (network-wide vulnerability scan)
2. **Sniper** (targeted pentesting)

## **5. System Hacking**

### **Tools and Explanation:**

1. **Active Directory Tools**: CrackMapExec, Rubeus for AD enumeration and exploitation.
2. **Impacket**: Tools for lateral movement and post-exploitation.
3. **winPEAS**: Searches for privilege escalation paths.
4. **LinEnum**: Enumerates Linux systems for privilege escalation.

### **Order of Use:**

1. **Impacket** (initial foothold)
2. **winPEAS, LinEnum** (privilege escalation)
3. **Active Directory Tools** (AD-specific exploitation)

## **6. Social Engineering**

### **Tools and Explanation:**

1. **Dark-Phish, Shellphish**: Automates phishing site creation.
2. **Social Engineer Toolkit (SET)**: Simulates phishing and other SE attacks.

### **Order of Use:**

1. **SET** (preparation)
2. **Dark-Phish, Shellphish** (phishing execution)

## **7. Post-Exploitation (Covering Tracks)**

### **Tools and Explanation:**

1. **Clear\_Event\_Viewer\_Logs**: Removes event logs from Windows.
2. **PowerSploit**: Post-exploitation framework for persistence and cover tracks.