## 1. Nmap (Network Mapper)

- **Usage**: Network discovery and security auditing.
- **Example**: Scanning a network to detect live hosts, open ports, and services.
    - `nmap -sS 192.168.1.1`

---

## 2. Metasploit Framework

- **Usage**: Exploitation framework used for developing and executing exploit code against a remote target.
- **Example**: Penetration testers use it to test vulnerabilities in systems.
    - Launch via terminal: `msfconsole`

---

## 3. Wireshark

- **Usage**: Network protocol analyzer for capturing and analyzing packet data in real-time.
- **Example**: Analyzing HTTP traffic or identifying suspicious network activity.
    - Start from terminal: `wireshark`

---

## 4. Hydra (THC-Hydra)

- **Usage**: Brute force login cracker for various protocols (e.g., FTP, SSH, HTTP).
- **Example**: Trying a list of passwords on a login service.
    - `hydra -l admin -P passwords.txt ssh://192.168.1.10`

---

## 5. Burp Suite

- **Usage**: Web vulnerability scanner and proxy tool used in web application security testing.
- **Example**: Intercepting HTTP requests and testing for XSS or SQL injection.
    - Launch GUI version: `burpsuite`