**1. Nmap (Network Mapper)**

* **Overview**: Nmap is one of the most popular and versatile network scanning tools. It is primarily used for discovering hosts and services on a network by sending packets and analyzing the responses.
* **Key Features**:
  + **Host Discovery**: Identifies live systems on a network.
  + **Port Scanning**: Detects open, closed, or filtered ports on target systems.
  + **Service and Version Detection**: Determines the service running on a port and its version.
  + **OS Detection**: Identifies the operating system and its version running on the target host.
  + **Scripting Engine (NSE)**: Automates a wide range of network tasks, including vulnerability detection.
* **Usage Example**: nmap -sV <target IP> (for service version detection).

**2. Netdiscover**

* **Overview**: Netdiscover is a simple and efficient ARP scanner designed to find active hosts on a local network. It is often used in networks where traditional discovery methods (such as DNS queries) do not work.
* **Key Features**:
  + **ARP Scanning**: Uses Address Resolution Protocol to identify active devices.
  + **Passive Mode**: Can be used to silently discover hosts without actively probing the network.
  + **Lightweight**: Ideal for quick scans in LAN environments without excessive overhead.
* **Usage Example**: netdiscover -r 192.168.1.0/24 (to scan a specific IP range).

**3. Hping3**

* **Overview**: Hping3 is a packet crafting tool that allows users to create and send custom packets for network scanning, firewall testing, and even DoS simulations. Unlike Nmap, Hping3 offers low-level packet manipulation.
* **Key Features**:
  + **ICMP, TCP, and UDP Scanning**: Supports various protocols to analyze network response.
  + **Firewall Testing**: Can help determine the rules and behavior of firewalls by sending different types of traffic.
  + **Custom Packet Creation**: Allows detailed customization of headers and payloads for advanced testing.
  + **Traceroute Functionality**: Includes a traceroute mode to map network paths.
* **Usage Example**: hping3 -S -p 80 <target IP> (to scan port 80 using TCP SYN packets).

**Conclusion**

Nmap, Netdiscover, and Hping3 are all powerful tools for network discovery and scanning, each suited for different types of assessments. Nmap offers robust features for comprehensive scanning and analysis, Netdiscover excels in lightweight ARP scanning on local networks, and Hping3 provides advanced capabilities for custom packet crafting and firewall testing. Together, they provide a versatile toolkit for network reconnaissance and security testing.