

**Nmap:**

* Almost always used in penetration testing
* An open-source tool used to discover hosts and services on a computer network, creating a map of the network's structure
* Operates by sending packets to target hosts and analyzing responses
* Can take hours when pinging target outside home network
* Scans 1000 most common ports. Can scan all 65000 with correct flag

Can scan individual IPs, website addresses, IP ranges  
  
  


**Syn Scan:**

* nmap -sS, Only initiates Syn portion of 3-way TCP handshake   
  

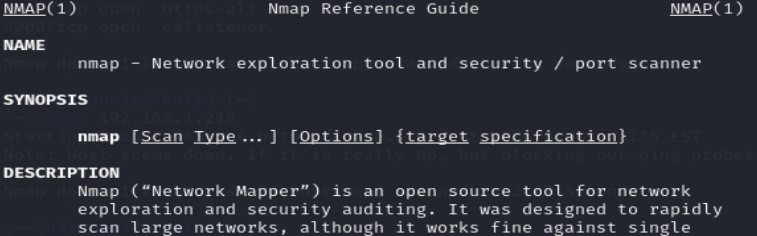
**TCP Connect Scan:**

* nmap -sT, performs normal 3-way handshake connection request (**Leaves more trace and is easily detected)**  
  

**UDP Scan:**

* nmap -sU, scans UDP ports
* These are often left unguarded as UDP scanning is slower and more difficult   
  

**Accessing NMP Manual**

* Open terminal and type man nmap
* Explains nmap scans in detail along with help menu and detailed explanations  
    
  

**Operating System Scan**

* Can use Nmap to determine operating system of target machine - **need** an open port   
  

**Version Discovery**

* Useful in learning what versions of software are running so we can look it up online and see if there are any known vulnerabilities **- need** an open port
* Default intensity of scan is 7 but can change from 0-9  
    
  

**Aggressive Mode**

* Enable to automatically scan for OS, versions, and script scanning  
  

**Host Availability Scan**

* Using this will allow you to scan a range of IP addresses on a network to determine which hosts are connected to internet without scanning their ports  
  

**Scan Single Port**

* Can use this to scan for a specific port on target machine  
  