

Host discovery

Masscan and Zmap are fast and can quickly find which hosts are online. A scan is performed checking the top 250 TCP ports and certain UDP ports. These hosts are then passed onto Nmap.

Specific scans

Nmap is more accurate and is used to find more specific information. Various options and scripts are employed for this. The blue links can be clicked to see which options were used.

General info

Two general Nmap scans are performed to gather service version information, vulnerabilities based on software versions and OS information.

TCP port scans

On specific ports with scripts

UDP port scans

On specific ports with scripts

