

Host discovery

Masscan and Zmap are fast and can quickly find which hosts are online. We use both tools to find which hosts are online. Masscan for TCP and Zmap for UDP.

General info

Nmap is more accurate and is used to find more detailed information. Two general Nmap scans are performed to gather service version information, vulnerabilities based on software versions and OS information.

Specific scans

Nmap is also used for even more detailed scans employing various options and scripts. The blue links under the ports can be clicked to see which options were used.

TCP port scans

On specific ports with scripts.

UDP port scans

On specific ports with scripts.

External scans

External scans are scans using external tools that provide functionality that Nmap scripts do not offer. Nmap is still used for host detection and a custom Nmap script is written for these external tools.

