**9 Best FREE IP & Ports Scanners for Open Port, IP and Service Scanning**

[GUIDES](https://www.pcwdld.com/guides)

[**Marc Wilson**](https://www.pcwdld.com/author/root) Last Updated : 01/08/2019

Doing a Network Reconnaissance helps network managers improve security by identifying weak devices that can be potentially breached. It can also allow managers to maintain a [detailed and updated diagram of the network](https://www.pcwdld.com/top-10-network-diagram-topology-and-mapping-software).

The network reconnaissance is basically **identifying live hosts and scanning ports and services**. When testing security or even hacking, port scanning becomes one of the most essential steps of a successful network exploration.

It basically helps identify open and vulnerable ports and protocols that are being used in the network. Port Scanning helps managers, testers, and hackers create a profile and gain intelligence about a target organization all while ensuring [Access to critical Systems and services are managed correctly](https://www.pcwdld.com/access-rights-manager-solarwinds).

Live open ports can lead into the services running on hosts which can become a door into the organization. Running a port/services scan can make you aware of these weaknesses. With this information in hand, a network manager can secure a firewall by closing unnecessary ports and services.

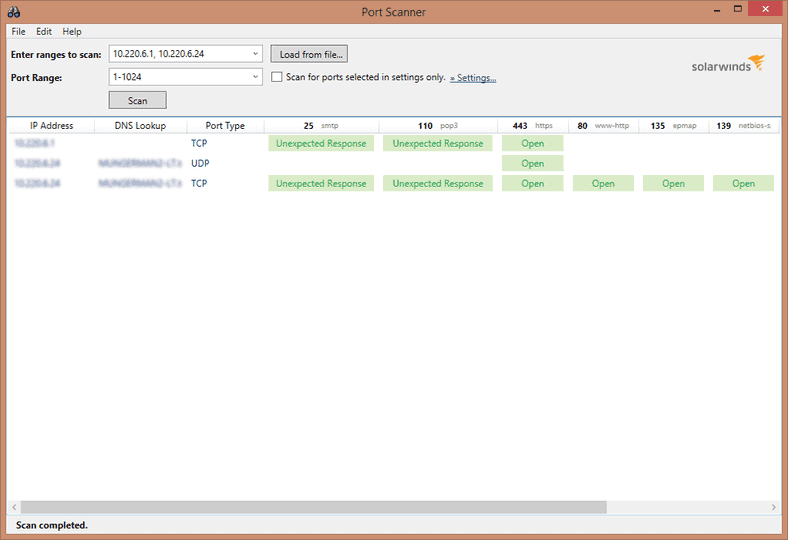
The following is a list of the **Best FREE IP Scanners for Port and Services**, including a brief description, their features and official download site.

**Here's a List of Best Free IP & Port Scanners of 2019:**

1. [SolarWinds Port Scanner](https://www.pcwdld.com/best-free-ip-scanners-port-service-scannin#SolarWinds%20Port%20Scanner)
2. [Nmap](https://www.pcwdld.com/best-free-ip-scanners-port-service-scannin#Nmap)
3. [Advanced IP Scanner](https://www.pcwdld.com/best-free-ip-scanners-port-service-scannin#Advanced%20IP%20Scanner)
4. [Angry IP Scanner](https://www.pcwdld.com/best-free-ip-scanners-port-service-scannin#Angry%20IP%20Scanner)
5. [Free IP Scanner by Eusing](https://www.pcwdld.com/best-free-ip-scanners-port-service-scannin#Free%20IP%20Scanner%20by%20Eusing)
6. [NetCat](https://www.pcwdld.com/best-free-ip-scanners-port-service-scannin#NetCat)
7. [LanSweeper IP Scanner](https://www.pcwdld.com/best-free-ip-scanners-port-service-scannin#LanSweeper%20IP%20Scanner)
8. [MyLanViewer Network/IP Scanner](https://www.pcwdld.com/best-free-ip-scanners-port-service-scannin#MyLanViewer%20Network/IP%20Scanner)
9. [Slitheris Network Discovery](https://www.pcwdld.com/best-free-ip-scanners-port-service-scannin#Slitheris%20Network%20Discovery)

There are a variety of scanners on the market which are usually online tools. But the best scanners are the ones that you run on your own devices since they allow more flexibility in the process.

**1. SolarWinds Port Scanner**

[](https://cdn.pcwdld.com/wp-content/uploads/solarwinds.png)

SolarWinds is one of the leading companies that create network and IT infrastructure monitoring software. The [SolarWinds Port Scanner](https://www.solarwinds.com/free-tools/port-scanner) is one of the “Free Download” tools that allows you to scan an IP address range or hostname and generate lists of the open, closed and filtered ports on the target network.

The software is easy to use. To begin scanning you will only configure the scan profile. To do this you must enter the target information, such as IP range, hostnames. You can also configure it to look for layer 4 ports or services such as TCP or UDP ports.

Aside from the common IP and Port scanning, SolarWinds Port Scanner can also be configured to resolve hostname with specific DNS information and it can also find the MAC address to identify the OS version.

**Common features?**

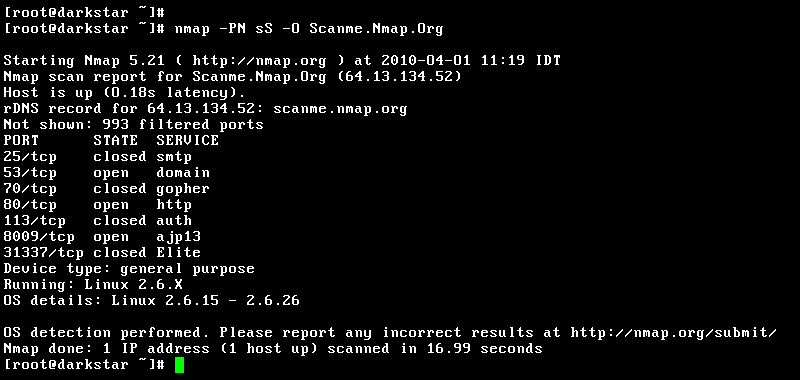
* Uses multi-threading for less overhead and faster scanning.
* Schedule scans to ensure updated data.
* All scan profiles are configured in a single window with a command line.
* Save all scan profiles for future faster scanning.
* View all the IANA port name definitions right on the application.

**Official site and where to download:**

[https://www.solarwinds.com/free-tools/port-scanner](https://www.solarwinds.com/free-tools/port-scanner?CMP=BIZ-RVW-PCWDLD-SW_WW_X_PP_PPD_FT_EN_FTLAN_SW-PORTS-X_X_X_X-Q417)

[Download Free Here!](https://www.solarwinds.com/free-tools/port-scanner?CMP=BIZ-RVW-PCWDLD-SW_WW_X_PP_PPD_FT_EN_FTLAN_SW-PORTS-X_X_X_X-Q417)

**2. Nmap**

[](https://cdn.pcwdld.com/wp-content/uploads/nmap.png)

Nmap is considered the Swiss Army Knife of hackers (ethical and not) and pen-testers.

[Nmap](https://nmap.org/download.html) stands for Network Mapper and is one of the most popular port scanners. It is an open source tool that offers a great deal of flexibility and power when it comes to performing any kind of active network reconnaissance against a target. With Nmap you can craft packets and send them to a specific target and let the software analyze the response.

For beginners, Nmap can be a little bit intimidating because there are so many different scanning combinations that get you different results.

**A very short list of what you can do with Nmap:**

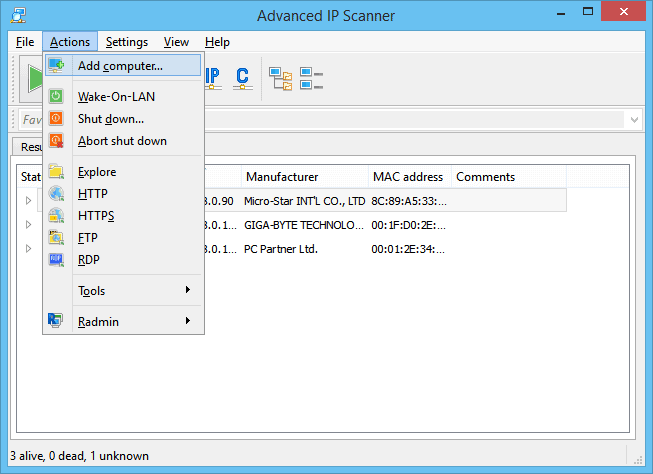
* Scan a target selection, such a single IP, a host-name, a range, etc.
* Scan a port selection, such as a single port or a range.
* Detect specific services and OSs.
* Perform NSE scripts.
* A really strong feature in Nmap is different “Port Scan Types”, such as TCP Connect, TCP SYN Scan. Below is a table with the most common TCP Scans Types that you can do in Nmap.

|  |  |
| --- | --- |
| **Scan Type** | **Description** |
| TCP Connect (-sT) | Full Three-way-handshake (SYN, SYN/ACK, ACK) |
| TCP SYN (sS) | Send SYN. RST/ACK response=not listening SYN/ACK=listening |
| TCP FIN (sF) | Send FIN, RST response=port close |
| TCP Xmas Tree (sX) | Send FIN, URG, PSH, RST response=port closed |
| TCP Null (sN) | No Flags. RST response=port closed |
| TCP ACK (PT) | Send ACK. Firewall test to verify packet filtering. |

**Official site and where to download:**

<https://nmap.org/download.html>

**3. Advanced IP Scanner**

[](https://cdn.pcwdld.com/wp-content/uploads/advanced-ip.png)

It is a portable, easy-to-use and free network scanner for Windows. [Advanced IP Scanner](http://advanced-ip-scanner.com/) is free of installation. Just press play and you’ll have one of the most robust scanners at your disposal. With Advanced IP Scanner you can see a list of network devices with information such as IP, Port, Manufacturer, MAC Address, OS, etc.

This scanner finds all the devices in a targeted scan in a matter of seconds and provides easy access to their shared resources, either through HTTP, HTTPS, FTP or even shared folders.

Another cool feature of this tool is that it detects the RDPs or Radmin ports, and it will let you manage the device remotely right from the platform.

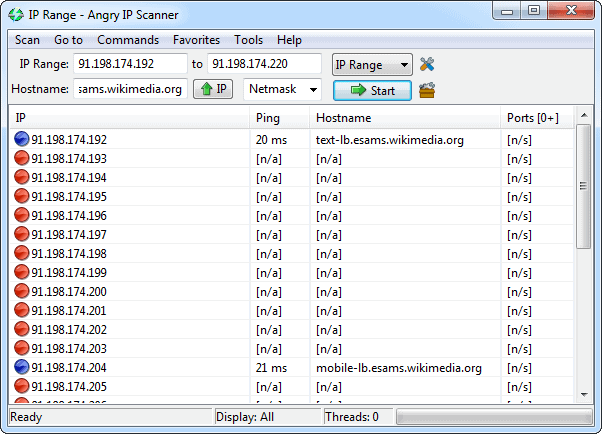
**Common features:**

* Easy access to network shares.
* Control devices via Radmin and RDP.
* Switch on/off computers remotely.
* Find the MAC addresses.
* Export all scan results to a CSV file.

**Official site and where to download:**

<http://www.advanced-ip-scanner.com/>

**4. Angry IP Scanner**

[](https://cdn.pcwdld.com/wp-content/uploads/angry-ip.png)

Angry IP Scanner (also called ipscan) is a free and open-source network scanner. The tool works on popular OSs, such as Windows, Mac OSX, and Linux. It was designed with simplicity in mind, the software is ultra-light, no installation is required (highly portable) and it is fairly easy to use.

At its most basic level, [Angry IP Scanner](https://angryip.org/) will ping the target device/network to confirm that it is alive. It can also resolve hostnames, find the MAC address, and scan ports. You can extend the amount of information received about each target with the help of plugins.

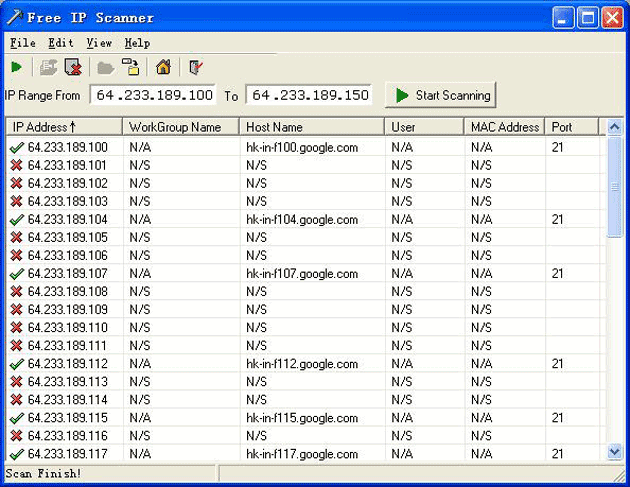
**Common features:**

* Can scan private or a public range of IP addresses. Additionally, it can get the NetBIOS information of a device, detect web servers and customize openers.
* It is able to export the results in different formats such as TXT, CSV, XML, or IP-Port list files.
* For faster scanning, the tool uses the multi-threading approach.
* By default, the tool comes with common fetchers like Ping, Host-name, and Ports but you can add more fetchers with the help of plug-ins to see more information.
* The tool runs on the GUI, but you can use the CLI to call up different options on the software.

**Official site and where to download?**

<https://angryip.org/>

**5. Free IP Scanner by Eusing**

[](https://cdn.pcwdld.com/wp-content/uploads/free-ipscanner.png)

Eusing Software creates miscellaneous free applications for windows users. Among the most popular tools is the [Free IP Scanner.](http://www.eusing.com/ipscan/free_ip_scanner.htm) This tool is a lightweight standalone scanner which can check a hundred devices per second. It is only supported by Windows OSs.

Free IP Scanner pings the IP (or range of IPs) to see who is alive. It can also translate the host-name to IP (or vice versa), find closed and open ports and get NetBIOS information. The last one can show details such as host-name, workgroup, active logged users, and the MAC address of the device. All the results obtained can be exported into a TXT file.

People like Free IP Scanner because it is simple, portable and easy to use. However, it cannot be extended with more functionality. Although the tool scans and finds ports, the entire layer 4 TCP/UDP information cannot be customized for deeper analysis.

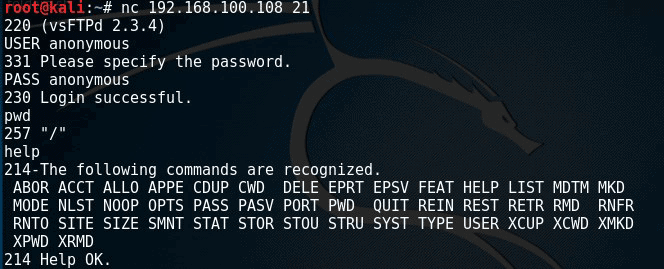
**Extra features:**

* Fast scanning using multi-threaded technology.
* Free IP Scanner can scan multiple targets per second without consuming many resources.

**Official site and where to download?**

<http://www.eusing.com/ipscan/free_ip_scanner.htm>

**6. NetCat**

[](https://cdn.pcwdld.com/wp-content/uploads/netcat.png)

A fully versatile tool preferred by most hackers like NMAP above.

[**NetCat**](http://netcat.sourceforge.net/)**is not strictly an IP Scanner, it goes well beyond that.** It is however a tiny [Unix networking analyzer](https://www.pcwdld.com/linux-network-monitor-software-and-tools) utility used by and against hackers for a large number of reasons.

It is tiny but powerful. NetCat is considered as a feature-rich networking tool used especially for debugging and investigation.

With NetCat you can create any kind of connection. It basically writes to and reads data from network connections using TCP or UDP. In other words, it can open TCP or UDP connections between two devices over any port.

The most common use for this tool is to set up reverse and bind shells, redirecting network traffic, port scanning and forwarding, debugging scripts, and service banner grabbing.

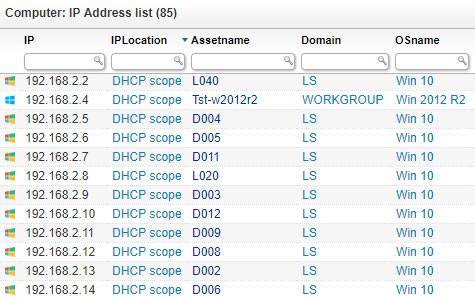
**Some features?**

* Connect to a remote system through any port or service.
* Banner Grabbing to identify the software that the target is using.
* Scan, listen and forward open ports.
* Create tunnels with specific network parameters, like source port/interface, listening port/interface and the remote host.
* Create back-doors for easy access to the target.
* Transfer files from the target

**Official site and where to download:**

<http://netcat.sourceforge.net/>

**7. LanSweeper IP Scanner**

[](https://cdn.pcwdld.com/wp-content/uploads/lansweeper.jpg)

It is a free and [powerful IT management tool](https://www.pcwdld.com/best-infrastructure-monitoring-tools-and-software) that can scan networks and find your assets. The [IP Scanner](https://www.lansweeper.com/feature/ip-scanner/) is a feature that comes integrated with LanSweeper. With the scanner, you can target a specific IP or range of IPs and get a full inventory of all computers, servers, virtual servers, [switches, routers](https://www.pcwdld.com/router-monitoring-software), printers, VoIP phones, etc. The results can be easily exported and created into a report.

People love LanSweeper because of its ability to automatically deploy scripts and commands to many devices at the same time. It uses an integrated deployment feature to automatically deploy software and execute commands on the devices shown on the inventory.

The software goes beyond scanning. It will let you get deep details through scanning, find issues and proactively fix them. The scanner grabs network information through WMI, SNMP, HTTP, FTP, SSH and other protocols.

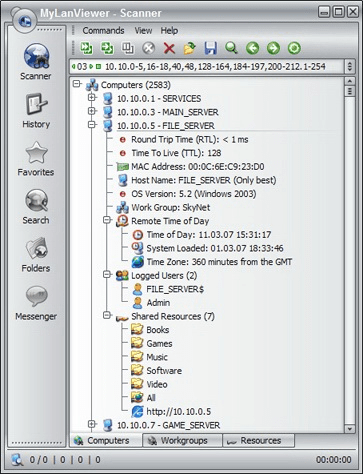
**Common features?**

* Inventorying
* Scan IP addresses automatically or on demand
* Import the results via a CSV file.
* Run custom actions such as remote shutdown.
* Wake-On-LAN Manager
* Find MAC address, logged-on users, user accounts, device up-times, etc.
* The free version lets you find detailed info of up to 100 devices.

**Official Site and where to download?**

<https://www.lansweeper.com/feature/ip-scanner/>

**8. MyLanViewer Network/IP Scanner**

[](https://cdn.pcwdld.com/wp-content/uploads/mylanviewer.png)

A comprehensive network IP Scanner for Windows OSs. On the basic level, this tool will scan the target network and will show the IP, MAC addresses, NIC vendor, OS Version, logged users, and shared folders of the wired and wireless devices found an easy-to-read list.

[MyLANViewer Network/IP Scanner](http://www.mylanviewer.com/network-ip-scanner.html) can monitor all the scanned devices (even if they are hidden), and notify you when a new device was found.

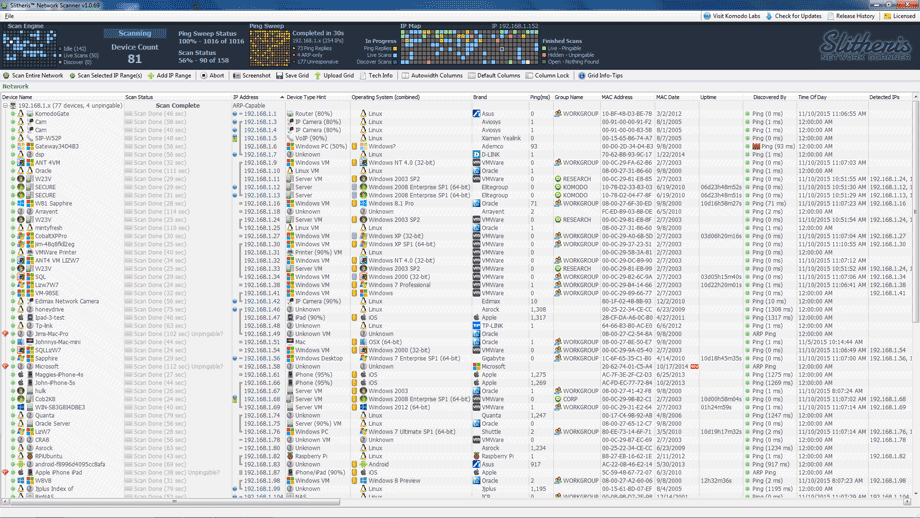
**Additional Features:**

* NetBIOS scanner
* Whois and [Traceroute tool](https://www.pcwdld.com/best-traceroute-alternative)
* Remote shutdown and Wake-On-LAN manager.
* Wireless network scanner and monitor
* Show and access shared folders
* Terminate user sessions
* Show netstat information
* Find rogue DHCP servers.

**Official Site and where to download:**

<http://www.mylanviewer.com/network-ip-scanner.html>

**9. Slitheris Network Discovery**

[](https://cdn.pcwdld.com/wp-content/uploads/slitheris.png)

Slitheris Network Discovery from Komodo Laboratories is a Windows-based premium IP scanner. The free version of this advanced network scanner allows you to find up to 50 network devices but can be extended with the premium license.

This tool takes IP scanning to a new level, it is fast and finds information that most scanners can’t. It gathers information from target network devices without needed credentials or agents. [Slitheris Network Discovery](http://www.komodolabs.com/ip-scanner/) uses multi-threaded technology to quickly find all pingable devices and uses ARP pings to discover hidden devices.

**What can Slitheris do?**

* *Real-time visual ping sweep.*It shows what the ping sweep is doing with a visual matrix.
* *OS Detection and Fingerprinting.*Identify different Windows OS versions without the need for authentication and credentials.
* *Identify different type of devices.*Find whether the device is a Printer, Virtual Machine, Mobile, Server, Workstation, etc.
* *Age determination.*Uses MAC address to determine the age of the device.
* *SMB Security.* Alarms when SMB (Server Message Block) is enabled or disabled on a device, to improve security.
* *Detects stealth devices.*The tool uses the ARP cache to find un-pingable devices.
* *Find Web GUI access devices.*The tool uses port scanning on HTTP and HTTPS to see whether a device can be accessed through Web GUI.

**Official Site and where to download:**

<http://www.komodolabs.com/ip-scanner/>

**Conclusion**

Open ports can be gateways into networks and are considered weaknesses if not treated with security in mind.

The toolbox of network and security administrators should contain a Port and Services Scanner to help them identify open ports and control vulnerabilities efficiently, before its too late.

There are many free and online scanners out there as well, But when combining portability, effectiveness, feature-richness, flexibility and cost efficiency, only the previous nine stand out.

They are free, download a copy today and scan your network. We suggest you grab several of them (as they are all Free) and give them a try – they all have different feature sets and work well when there is no internet connection available to use an online variation. We hope this list of some of the top Port Scanners help you secure your network and keep intruders out!