What is Nmap?

Nmap ,short for Network Mapper, is a network discovery and security auditing tool. It is known for its simple and easy to remember flags that provide powerful scanning options. Nmap is widely used by network administrators to scan for:

- Open ports and services
- Discover services along with their versions
- Guess the operating system running on a target machine
- Get accurate packet routes till the target machine
- Monitoring hosts

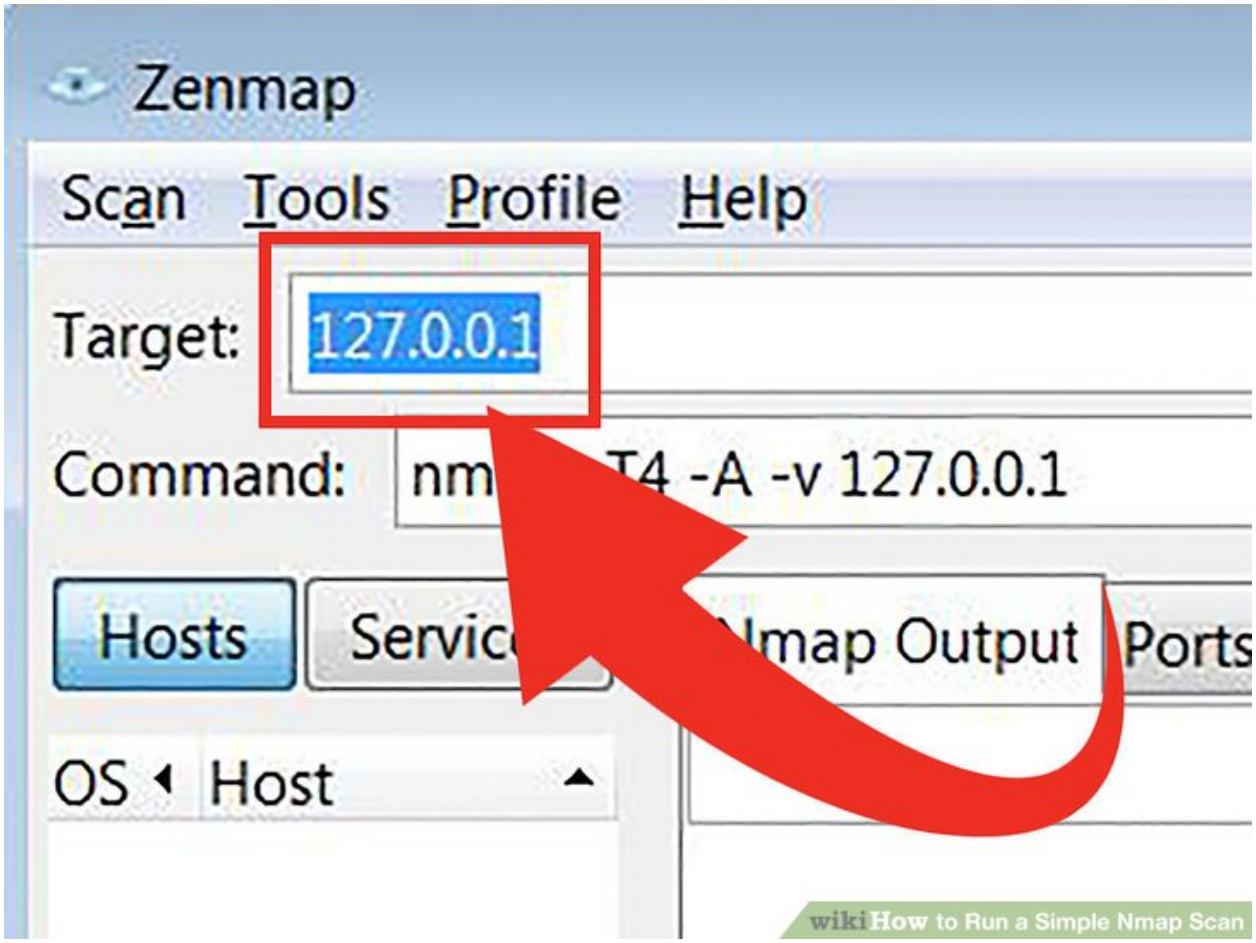
Nmap is a network mapper that has emerged as one of the most popular, free network discovery tools on the market. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

Common Nmap Functions

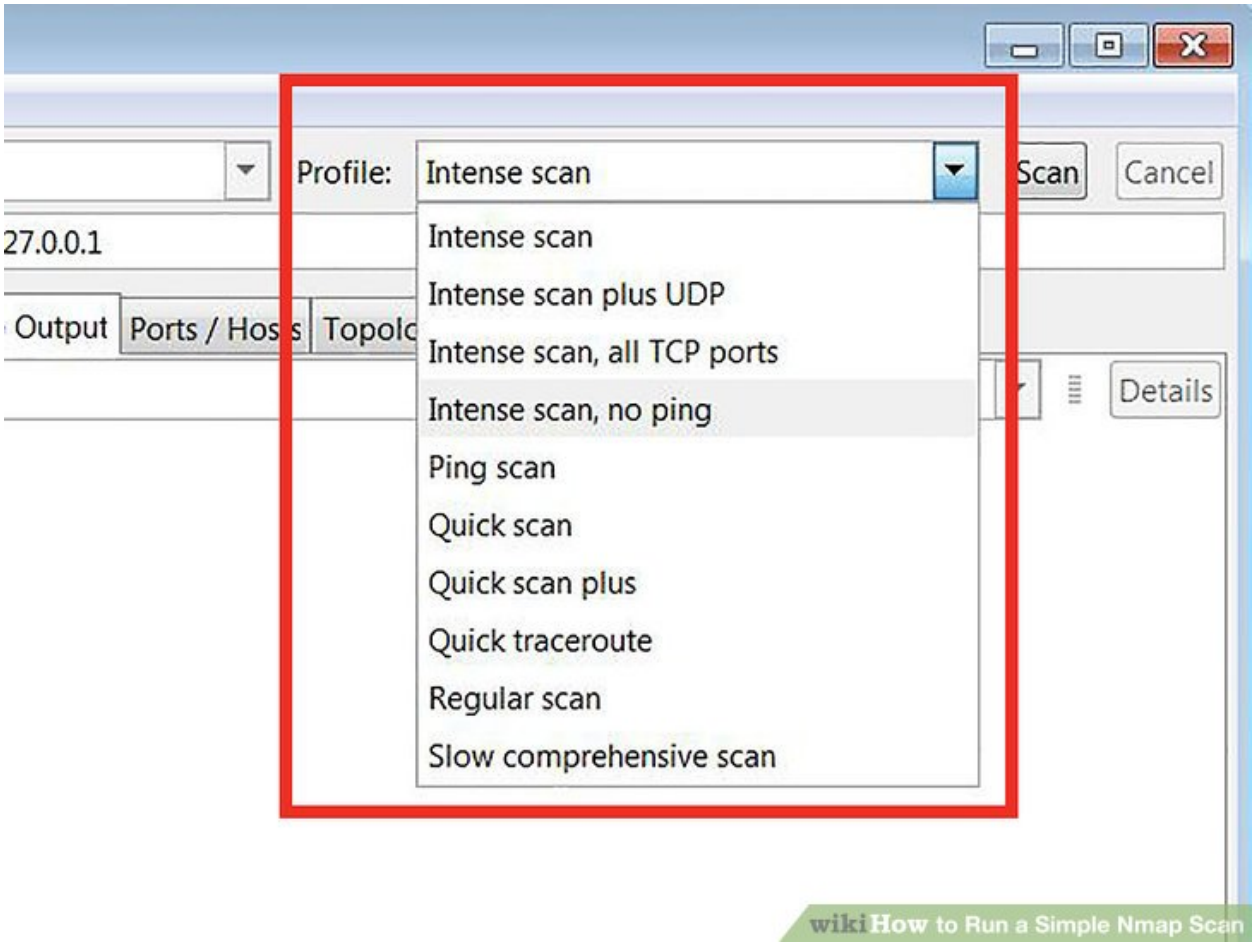
- Ping Scanning
- Port Scanning
- Host Scanning
- OS Scanning
- Scan Top Ports
- Output to Files
- Disable DNS Resolution

VARONIS

Using Zenmap GUI in windows



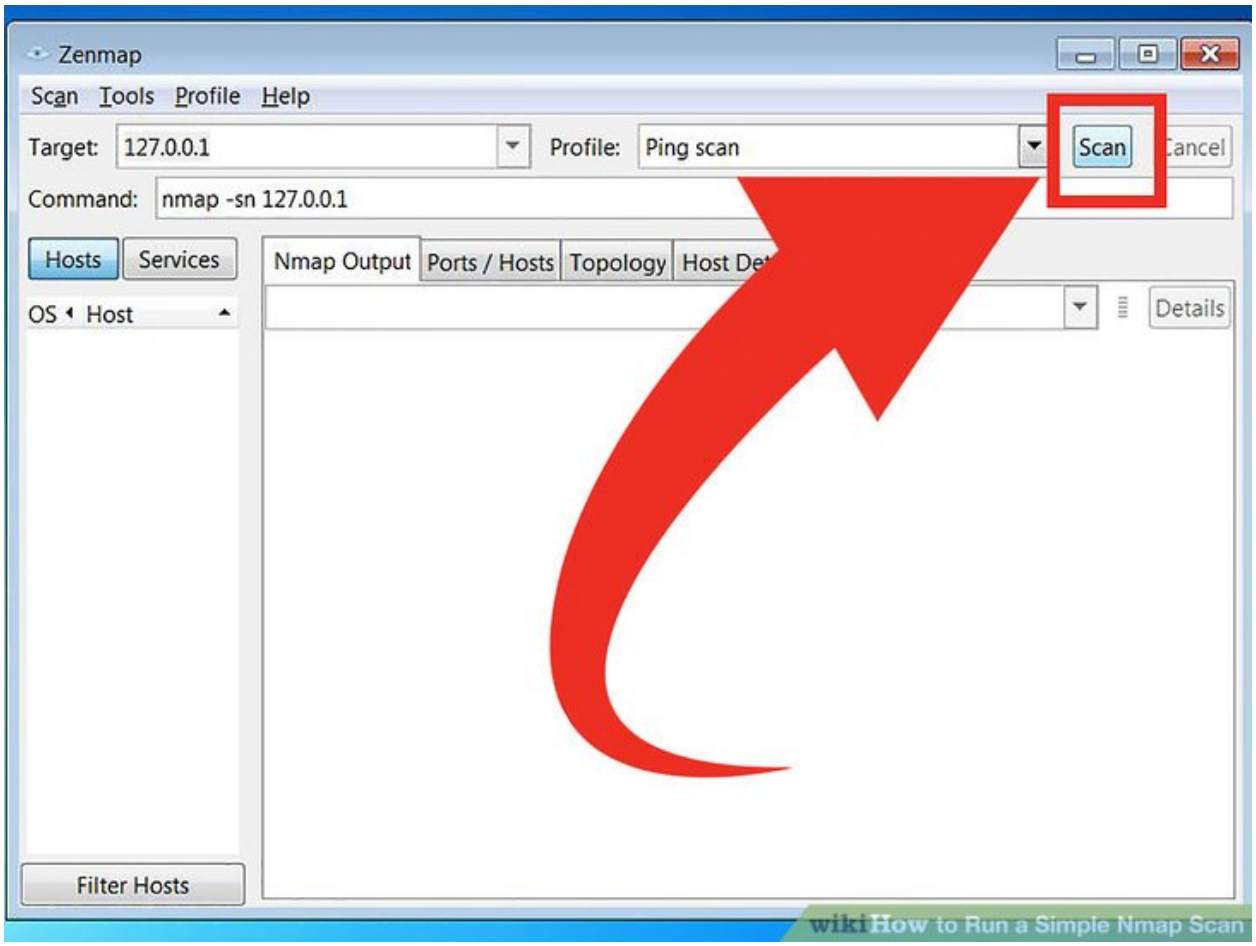
Enter in the target for your scan. The Zenmap program makes scanning a fairly simple process. The first step to running a scan is choosing your target. You can enter a domain (example.com), an IP address (127.0.0.1), a network (192.168.1.0/24)

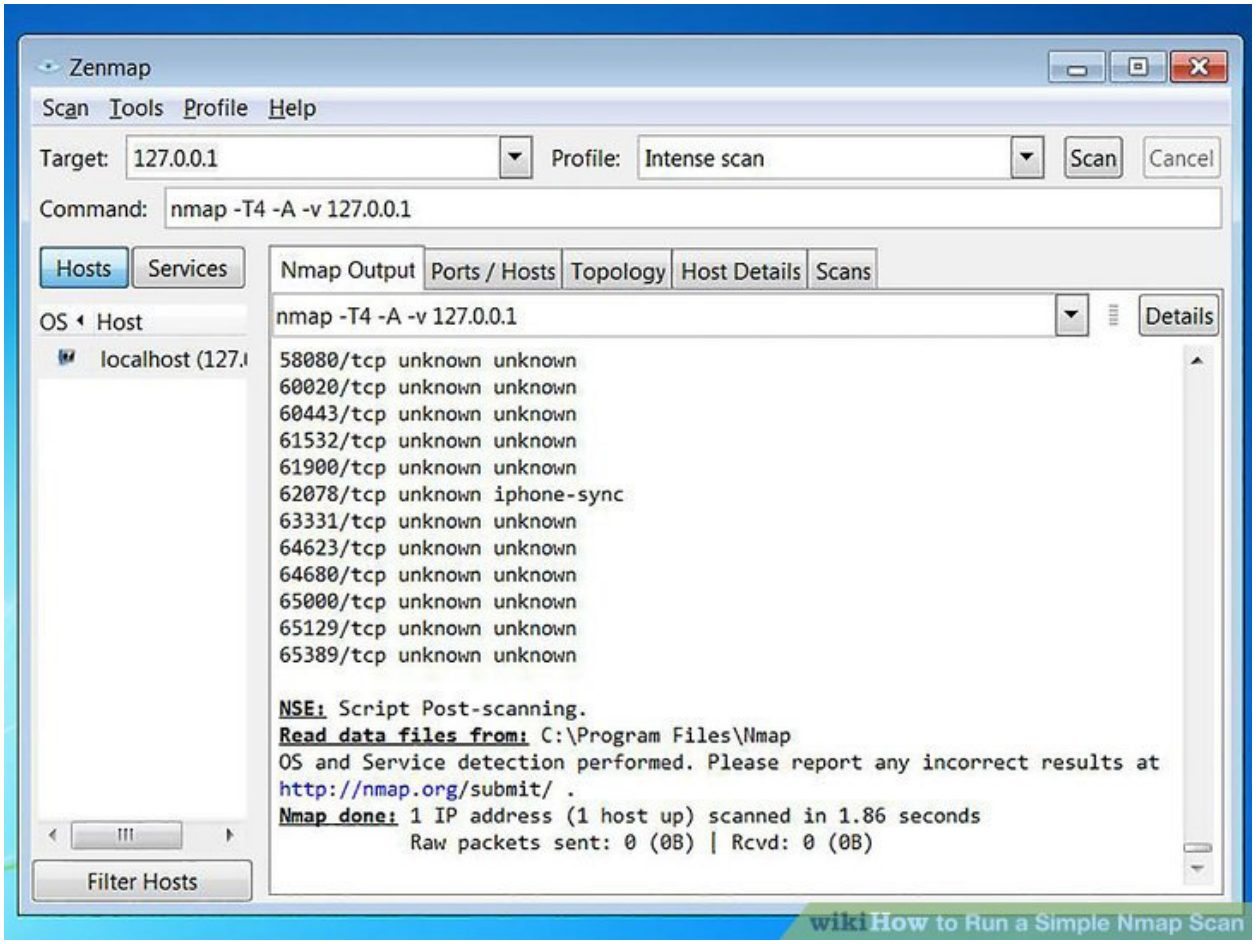


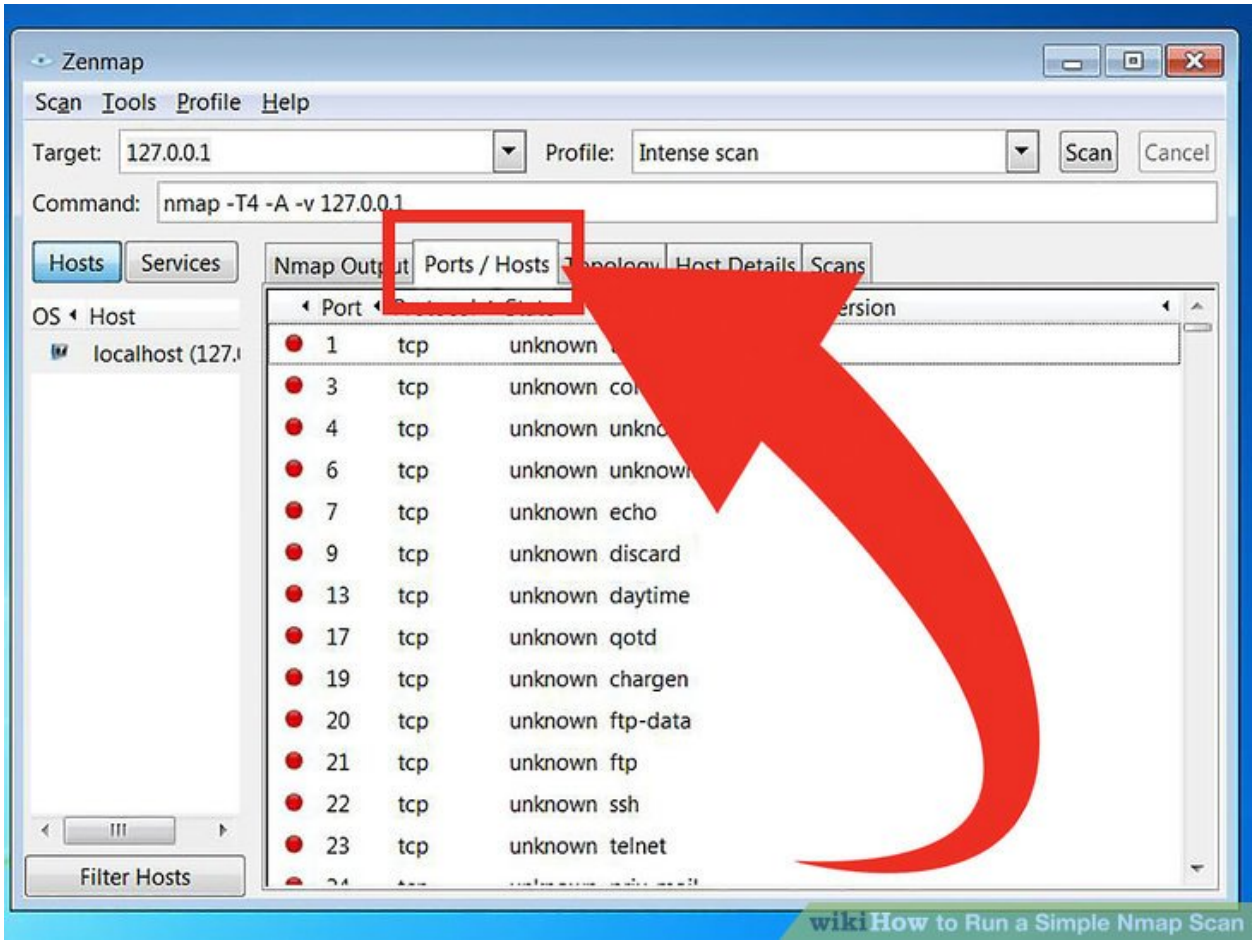
- **Intense scan** - A comprehensive scan. Contains Operating System (OS) detection, version detection, script scanning, traceroute, and has aggressive scan timing. This is considered an intrusive scan.
- **Ping scan** - This scan simply detects if the targets are online, it does not scan any ports.

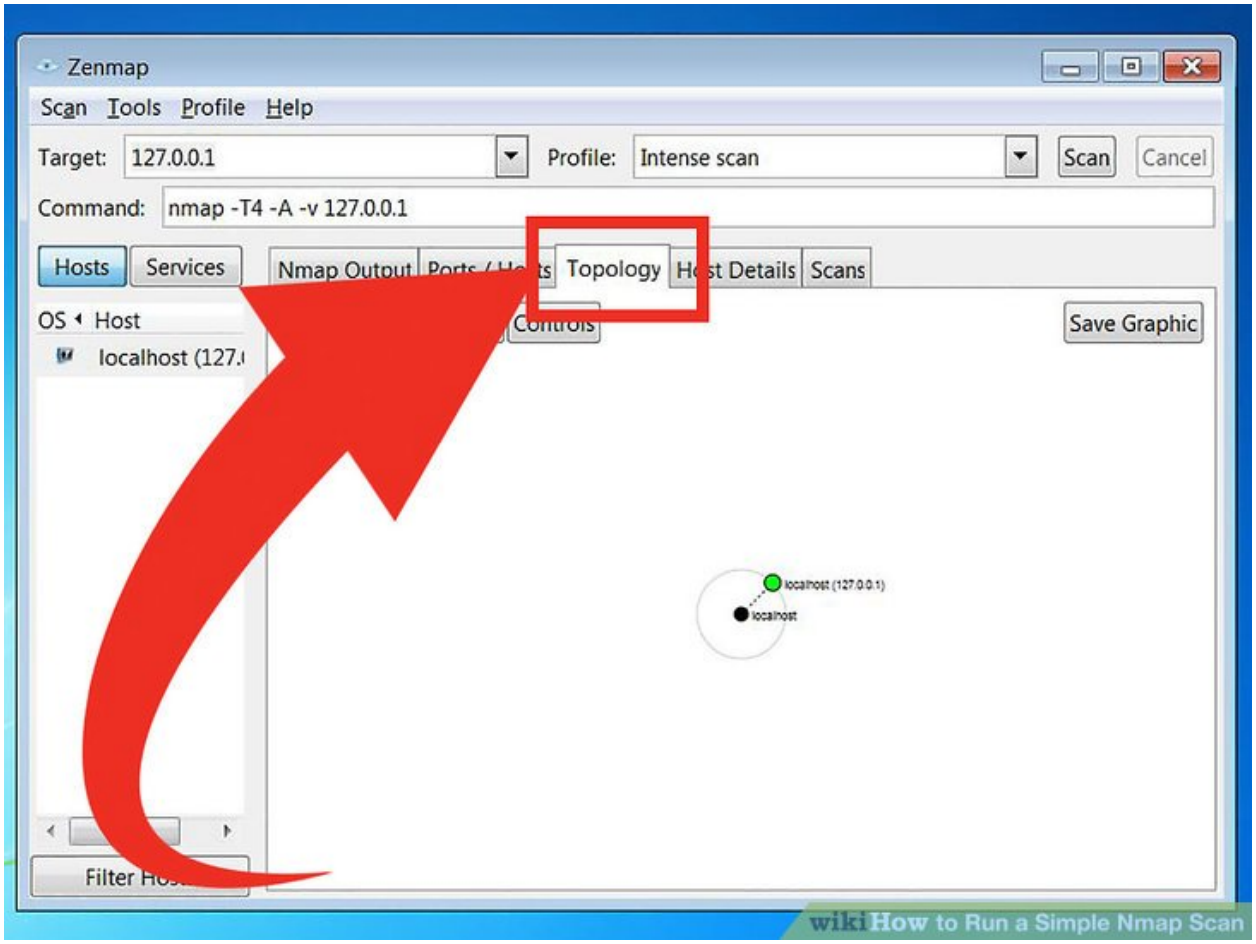
- **Quick scan** - This is quicker than a regular scan due to aggressive timing and only scanning select ports.
- **Regular scan** - This is the standard Nmap scan without any modifiers. It will return ping and return open ports on the target.

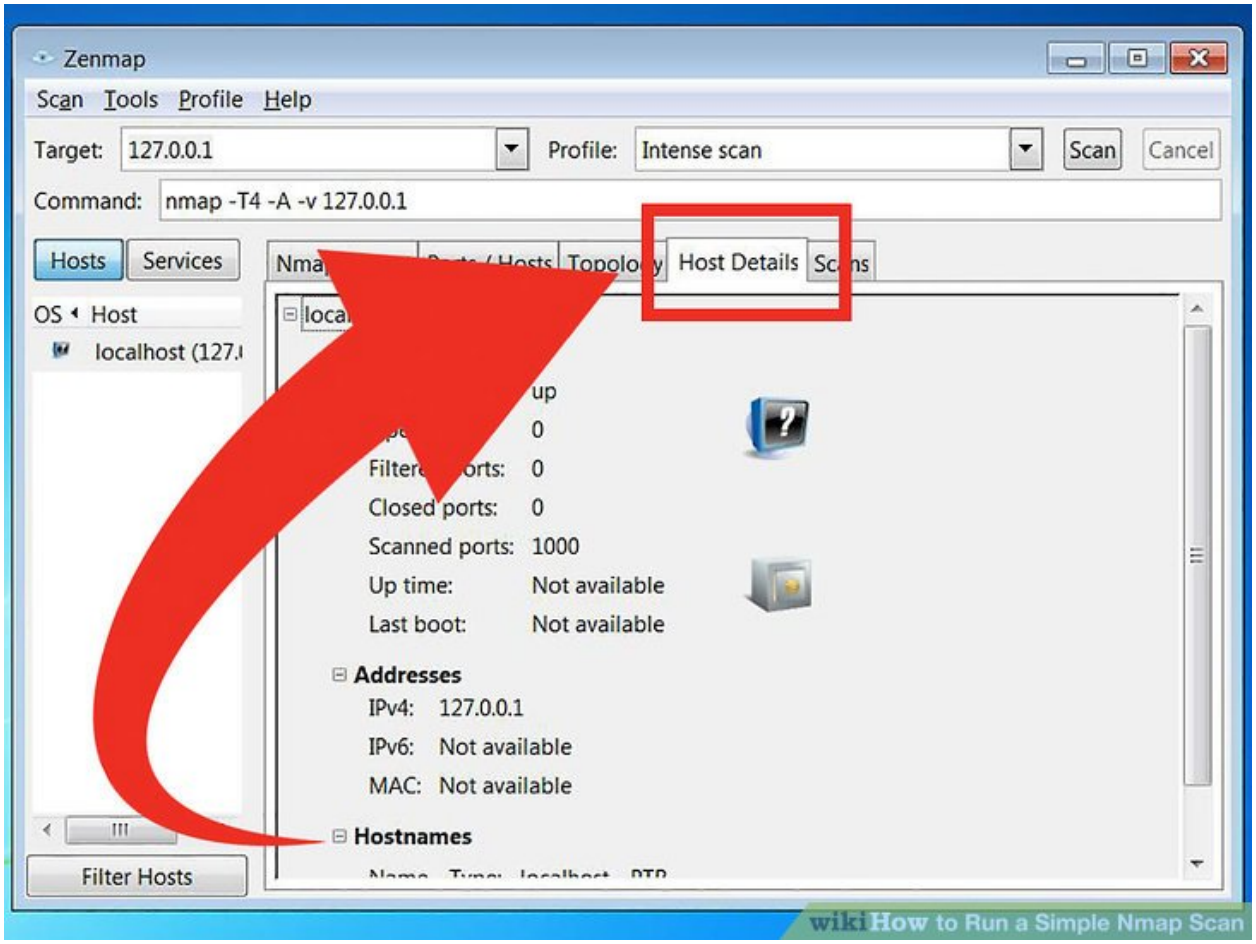
Click Scan to start scanning. The active results of the scan will be displayed in the Nmap Output tab. The time the scan takes will depend on the scan profile you chose, the physical distance to the target, and the target's network configuration.



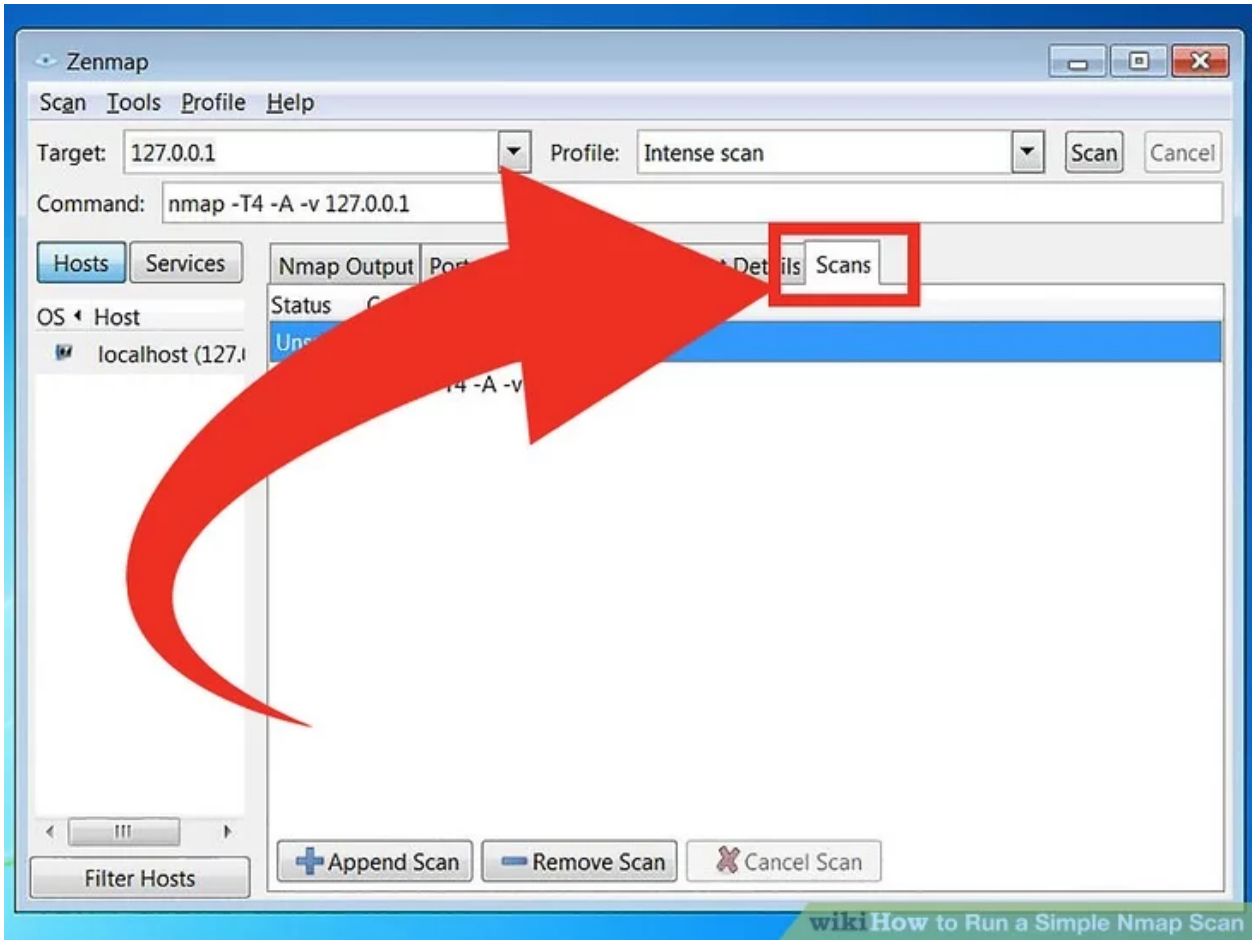

Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 127.0.0.1
Hosts
Services
OS Host
localhost (127.
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 127.0.0.1
Details
58080/tcp unknown unknown
60020/tcp unknown unknown
60443/tcp unknown unknown
61532/tcp unknown unknown
61900/tcp unknown unknown
62078/tcp unknown iphone-sync
63331/tcp unknown unknown
64623/tcp unknown unknown
64680/tcp unknown unknown
65000/tcp unknown unknown
65129/tcp unknown unknown
65389/tcp unknown unknown
NSE: Script Post-scanning.
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
wikiHow to Run a Simple Nmap Scan


Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 127.0.0.1
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS Host
localhost (127.
Port
Version
1 tcp unknown
3 tcp unknown
4 tcp unknown
6 tcp unknown
7 tcp unknown echo
9 tcp unknown discard
13 tcp unknown daytime
17 tcp unknown qotd
19 tcp unknown chargen
20 tcp unknown ftp-data
21 tcp unknown ftp
22 tcp unknown ssh
23 tcp unknown telnet
Filter Hosts
wikiHow to Run a Simple Nmap Scan


Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 127.0.0.1
Hosts
Services
Nmap Output
Topology
Scans
OS Host
localhost (127.
Save Graphic
localhost (127.0.0.1)
localhost
wikiHow to Run a Simple Nmap Scan



Scans - This tab stores the commands of your previously-run scans. This allows you to quickly re-scan with a specific set of parameters.



Nmap Commands

Scanning Techniques

Flag	Use	Example
-sS	TCP syn port scan	nmap -sS 192.168.1.1
-sT	TCP connect port scan	nmap -sT 192.168.1.1
–sU	UDP port scan	nmap –sU 192.168.1.1
–sA	TCP ack port scan	nmap –sA 192.168.1.1

Host Discovery

Flag	Use	Example
-Pn	only port scan	nmap -Pn 192.168.1.1
-sn	only host discover	nmap -sn 192.168.1.1
-PR	arp discovery on a local network	nmap -PR 192.168.1.1
-n	disable DNS resolution	nmap -n 192.168.1.1

Port Specification

Flag	Use	Example
-p	specify a port or port range	nmap -p 1-30 192.168.1.1
-p-	scan all ports	nmap -p- 192.168.1.1
-F	fast port scan	nmap -F 192.168.1.1

service Version and OS Detection

Flag	Use	Example
-sV	**detect the version of services running**	**nmap -sV 192.168.1.1**
-A	**aggressive scan**	**nmap -A 192.168.1.1**
-O	**detect operating system of the target**	**nmap -O 192.168.1.1**

Scanning Multiple Hosts

Nmap has the capability of scanning multiple hosts simultaneously. This feature comes in real handy when you are managing vast network infrastructure.

- Write all the IP addresses in a single row to scan all of the hosts at the same time
- nmap 192.164.1.1 192.164.0.2 192.164.0.2

Web links

Installation link for windows

https://nmap.org/download.html

Process that happen in windows

https://www.wikihow.com/Run-a-Simple-Nmap-Scan