All about Nmap

While there are many advanced monitoring tools that can help network administrators in port scans and detect network vulnerabilities, Nmap is still considered a standard tool. Why is that?

While there are many advanced monitoring tools that serve as a great help to network administrators in port scanning and detecting network vulnerabilities, Nmap is still considered a standard tool. ink. Why is that?

Network administrators, IT managers and security experts have been, and will face a never-ending battle on the battlefield named cyber security.They will have to constantly check their network to find out the harmful agents as well as the hidden security holes.While there are currently a number of monitoring utilities available to assist professionals in network mapping and security control, Nmap is the number one choice for flexibility and portability. These practices have made it awidely recognizedport scanning and security vulnerabilityworldwide.

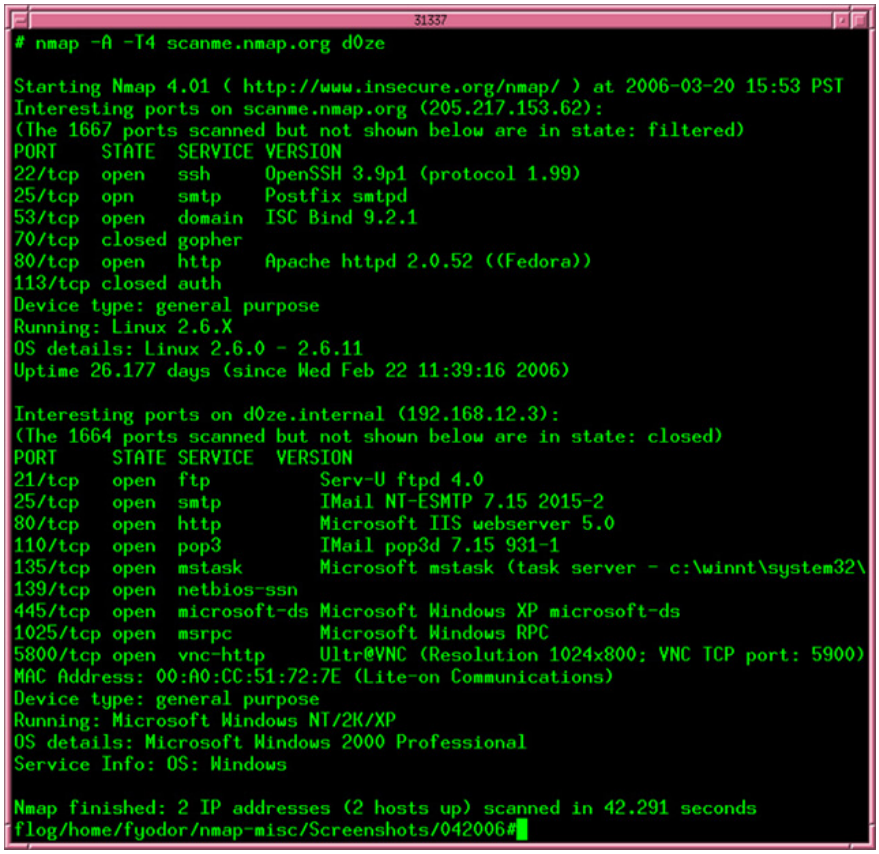
All about Nmap

What is Nmap?

Nmap (full name Network Mapper)is a security tool developed by Floydor Vaskovitch.Nmap isopen source, free, used forport scans and security holes.Network administrators use Nmap to determine which devices are running on their systems, as well as find out which servers are available and the services they provide, and search for them. open ports and detect security risks.

Nmap can be used to monitor individual servers as well as large network clusters including hundreds of thousands of devices and multiple subnets.

Although Nmap has been constantly developed, improved over the years and extremely flexible, its platform is still a port scanning tool, gathering information by sending raw packets to system ports. system.It then listens and analyzes the responses and determines whether those ports are opened, closed, or filtered in some way, such as a firewall.Other terms used to refer to port scanning include port detection (discovery) or port enumeration (enumeration).



Nmap in port scan

The data packets sent by Nmap return IP addresses and other related data, allowing you to identify network attribute types, provide you with network records or diagrams and allow you to create an evaluation list of hardware and software in that network.

Different network protocols use different types of packet structures.Nmap uses layer protocols including TCP (transmission control protocol), UDP (user query protocol), and SCTP (flow control protocol), as well as support protocols such as ICMP (Internet control message protocol, used to send error messages).

Different protocols serve different purposes and system ports.For example, UDP's low resource costs are well suited to real-time online video streaming, where you'll sacrifice some lost data packets in exchange for speed, while videos are Non-real-time streams on YouTube will be cached and slower using TCP, although this protocol is more reliable.

Along with many other features, the basic port scanning and packet capture capabilities (packet-capture -packet blockingfeaturethat is passing or moving through a specific computer network)of Nmap are also constantly being upgraded. upgrade, improve.

Gordon Lyon, author of Nmap, shared in an email response to software queries that his company is now focusing on upgradingNpcappacket capture featuredriversand libraries for Windows. ."It makes Nmap faster and more powerful on Windows and is also being used by many other applications. We have released eight releases of Npcap this year," Gordon Lyon said.

Nmap and the path to success

Nmap was written on C ++ platform and was first introduced with the source code in Phrack magazine in September 1997. It was later expanded with C, Perl and Python.Author Gordon Lyon used the pseudonym Fyodor Vaskovitch.Fyodor Vaskovitch said he chose this pseudonym because he was impressed after reading Fyodor Dostoevsky's notes from the Underground.

Throughout the years since its launch, Nmap has benefited from the growing contribution of the growing fan community and developers, and now the application has a number of downloads up to thousands of times every day.Along with support from the tech world, Nmap has been well known among the public, who do not have much network security expertise through movie movies.In these films Nmap has become a breakthrough tool for directors along with the acting of stars like Rihanna and Kate Mara.Nmap made its first appearance in the movie The Matrix Reloaded, in which Trinity character Carrie-Anne Moss portrayed her impressive ability to unlock security using the Nmap software correctly.

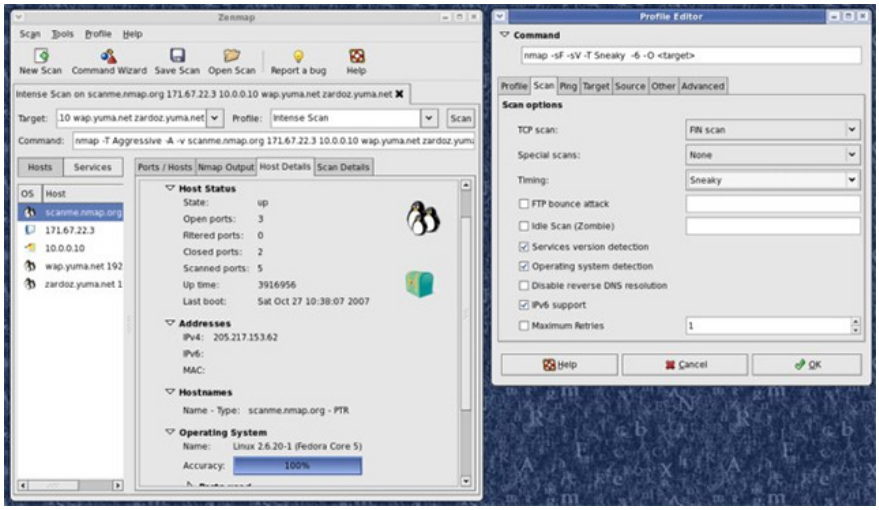
What operating systems does Nmap work on?

One of the reasons for Nmap's widespread popularity is that it can be used on many different operating systems.It works on Windows and macOS and is supported on Linux distributions including Red Hat, Mandrake, SUSE and Fedora.It also works well on other operating systems including BSD, Solaris, AIX and AmigaOS.

How to use Nmap

It is not difficult to find a range of free network monitoring utilities as well as free open source vulnerability scanning tools available for network administrators and security controllers.However, what makes Nmap stand out as an information technology tool that any network manager needs to know is its flexibility and power.In addition to the basic function of Nmap as port scanning, it also provides users with a range of related features including:

1. **Network mapping** : Nmap can identify devices that are active on the network (also known as server detection), including servers, routers and how they are physically connected. how.
2. **Operating system detection (OS detection)**: Nmap can identify the operating systems of devices running on the network (also known as OS fingerprinting), while providing information about providers and operating systems. base, software version and even estimate the device's uptime.
3. **Service discovery (Service discovery)** : Nmap can not only identify servers that are operating on the network, but also determine which services they are providing.Can be mail, web or name servers.As well as identifying specific applications and versions of the software they are running.
4. **Security auditing** : Nmap can find out which version of the operating system and application is running on network servers, thereby allowing network administrators to identify general weaknesses that correspond to Specific vulnerabilities.For example, if the network administrator receives vulnerability alerts in each specific version of the application, he can perform a network scan to determine if the software version is running on the network. No and take steps to patch or update the relevant servers.In addition, scripts can automate tasks such as detecting specific vulnerabilities.



Use Nmap for local networks

Running Nmap is often the best way to discover the 'size' of the network and the number of devices connected to it. The "fast" Nmap **(-F)** scan on the network can create a list of all IP addresses belonging to the server that operates on the network, along with some additional information.

```
sudo nmap -F 192.168.0.0/24 Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-1
```

The amount of information on the local network that Nmap can collect is impressive, including the MAC address and the manufacturer of the connected device, the operating system that the device is using and the version of any service. running on the device. After knowing how many devices are on the network and (almost) knowing which devices they are, the next step is to scan and check the devices on the network you are interested in.

Another important function of Nmap is to allow port scanning of each device or IP address range, including multiple devices. This allows an attacker to find out the details of each device detected on the network, including information about open ports and service running. Port is the port that another device can connect to, so finding a range of services running on open ports can be a huge benefit to hackers, especially if one of the devices used an outdated version and vulnerable.

Use Nmap for remote networks

In addition to scanning local networks, Nmap can also display information about remote networks. In fact, you can run Nmap on the site you want to test and it will parse and get the IP address associated with that site's domain name.

```
nmap -F wonderhowto.com Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-11 23
```

After retrieving the IP address and noting the open port numbers, Nmap can then indicate that the operating system **(-O)** is being used to store a remote site.

```
sudo nmap -O 104.193.19.59 Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-10
```

Finally, users can even learn about software versions that are running on open ports. If you see a port vulnerable to attack, it can make your work on the network much easier. Using the previously discovered IP address, users can perform a different scan than the **-sV** parameter **,** indicating that **httpd 2.0** is being used on the target computer.

```
sudo nmap -sV 104.193.19.59 Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-1(
```

These details - the IP address of a remote site or server, the operating system running on the device and the version of any application running on the open ports discovered - is everything the hacker Need to start attacking devices on the network.

What you need

To use Nmap, you will need a system that supports it. Fortunately, Nmap is a cross-platform application, works on Windows, Linux and macOS, preinstalled on many systems. Even if you don't have this tool, it's easy to install.

You will also need a network to connect and scan to try these techniques, but note that scanning is often referred to as a 'prelude' for an attack and needs to be scrutinized. This means that if your job is to monitor suspicious behavior, scanning the entire network is a great way to get the most panoramic view.

Step 1: Configure Nmap to scan a target

To run basic scanning, users can specify specific target IP addresses to scan. One of the basic but most informative scans is to run Nmap, specify the destination IP address and then enter **-A** to enable operating system detection, version detection, script scanning and follow watch.

```
sudo nmap 104.193.19.59 -A Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-10
```

Even for a single goal, a basic scan can bring a lot of information. Here, the example is simply scanning the IP address for the **WonderHowTo.com** domain **.** The tool can run with a device on a local network, such as a router or a remote server, such as the **WonderHowTo.com** host **.**

Step 2: Calculate the subnet and scan a specific range to find the device

To identify other devices on the local network, it is useful to calculate the subnetwork range. This is the range of IP addresses that can be provided to devices on the network and is a signal that it is possible to scan all IP addresses of devices on the network.

A useful tool to do this is **IPcalc.** This tool will get the IP address (easily found by entering **ifconfig** or **ip a** in the terminal window) and calculating the subnet range based on that. The tool will provide a sequence of numbers like **"192.168.0.0/24",** specifying a range of IP addresses. In the example below, the subnet is calculated as **127.0.0.0/24.**

```
ipcalc 127.0.0.1 Address: 127.0.0.1 01111111.00000000.00000000. 00000001 Netmark
```

To include information about the services running on the device found, users can open the terminal window and enter the following command, in addition to your network range (where using **"172.16.42.0/24"** in For example). Scanning is a bit slow, so you can use the **-F** flag instead of **-A** to perform faster scans for the most popular ports.

```
nmap 172.16.42.0/24 -A Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-11 23:
```

Basically, we're running Nmap without arguments, except for the **-A** flag **.** We will see the same output as above, showing the devices detected and the services running on them.

Another handy tool to explore the network is arp-scan. Sometimes it is possible to display devices that Nmap misses. We can use Nmap to perform ARP scans with query **-PR, which is** quite fast and active in bringing online servers back.

```
nmap -PR 192.168.0.0/24 Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-12 06
```

Step 3: Create a list of target active servers

Now, you will calculate all IP addresses that can appear on the local network and discover them by scanning **-F** (fast), by running Nmap without arguments except for the **-A** flag to scan. slow, but for more information or with **-PR** is able to quickly scan a local network to find active servers.

Finally, if you want to create the detected TXT file of the server, you can use the command below to create the list, avoiding having to scan the entire network the next time. For example, to scan devices with port 80 open and save them to the list, you can use some Linux tools and flag **-oG "greppable output"** to filter the output that Nmap provides.

By running **nmap -p 80 -oG - 192.168.0.0/24** (network range is replaced by a specific case), you can add **| awk '/ 80 / open / {print $ 2}' >> port80.txt** to export the IP address of detected devices into TXT file named **"port80.txt."**

```
nmap -p 80 -oG - 192.168.0.1 | awk '/80/open/ {print $2}' >> port80.txt cat port8
```

Here, the **awk** command is searching for lines containing the port number and the **"open"** result **,** with the second string in each line (in this case, the IP address) stored by the cat command into a new file named **port80. txt**

Step 4: Determine the operating system on the detected devices

One of the most useful things to know about a device discovered on the network is the operating system it is running. Here, we can get the target TXT list already in the previous step and scan the operating system, requiring root permissions. You can use the **-O** flag to scan the operating system and the **-iL** flag to tell Nmap the device you want to read from the target server's TXT file.

```
sudo nmap -O -iL port80.txt Password: Starting Nmap 7.60 ( https://nmap.org ) at
```

This tactic allows users to get as much information as possible about the operating system from any target list that wants to run, whether the target is an intranet or the list of IP addresses of the site.

The next step is to explore the versions of applications running on open ports. This may indicate that a port running the software is outdated and has a vulnerability already detected. To do this, use the **-sV** flag **.**

```
sudo nmap -sV 192.168.0.2 -D 192.168.0.1,192.168.0.2,192.168.0.3 Starting Nmap 7
```

Here, we will find some very specific information about the server, making it possible to identify an attack from 'eavesdrop' software through the portal.

Step 5: Advanced scanning solutions

Occasionally, users will have trouble scanning the network because the ping sent by Nmap is blocked by the firewall on the router. This can make the user mistakenly think that there is no device on the network (though it is in fact available). To avoid this, you can include the **-Pn** flag **,** to sometimes allow direct connection to devices and get feedback.

If you are scanning on a network that does not want to be detected, you can perform a test with the **-D** flag to make it difficult to detect who is scanning on the network. The process will look like the command below and require root access.

```
sudo nmap -sS 192.168.0.2 -D 192.168.0.1,192.168.0.2,192.168.0.3 Password: Starti
```

If you need more information about what's going on, you can press a key while the scan is taking place to get some information on how to proceed or add the **-v** parameter to increase the level of detail (amount information that the script provides). In general, you can continue to add more v- **v** depending on the level of desire to find out more information about what's happening.

```
Initiating ARP Ping Scan at 07:18 Scanning 192.168.0.1 [1 port] Completed ARP Pi
```

Here, we can see the reason reported for active port 80 allows us to decide which part of the scanning process will give us the necessary information or be ignored. As mentioned, you'll see everything that the scan is doing and this can create a lot of output for complex scans.

The first time searching for something about the network can be very difficult for beginners, whether they are learning about the network exploit for the first time or simply trying to find a network router.

Keep in mind, although scanning the network is a great idea to run on a private network and see what is connected, this may not be allowed on the network at work or other networks that you do not own. . If an employer actually detects suspicious behavior online, your behavior can easily be considered a threatening action if there is no good reason to do so.

One of the best things about Nmap is that it can create scripts with options like **-oG** and can be used to provide information to other tools. So, if you ever imagine building a tool to find other devices on the same network, Nmap might be what you're looking for.

Nmap commands for beginners

One of the great things about using Nmap is that new users have little knowledge of the system or the network can still start with simple commands to perform basic scans, while experts have can take advantage of more complex commands to get a more detailed view of the entire network.

What you get when you use Nmap is basically the list of targets you have scanned, along with the associated information associated with those goals.The information you receive will depend on how you perform the scan.In other words, it depends on the commands you have used.

The scanning process does not necessarily generate much traffic but depends on the commands used.Scanning all ports on all systems will not bring much effect, mainly because only a small number of available ports will be used at the same time (one system can have 65,535 TCP ports and 65,535 UDP ports).Various options allow finetuning or extended scanning.For example, in defining service versions, available options include:

1. **sV (allows version detection)**

2. **version-intensity (set the scanning intensity)**

Scanning intensity ranges from 0 to 9. Lower intensity scans will explore common services, while higher intensity scans can determine which services are used less but will lose more More scan time.

Different commands can also allow you to specify which port or network components to scan or ignore.

Nmap Scripting Engine (NSE)

Nmap Scripting Engine (NSE) includes a command tool written in the Lua programming language to write, save and share scripts that automate different types of scans.Although often used to check for typical vulnerabilities, network infrastructures, all tasks can be automated.

Zenmap - Nmap's interface

Zenmap is the graphical interface of Nmap security scanner.This interface provides users with hundreds of different options.It allows users to do things like store information about scans and then compare them, view network topology maps, see which ports are running on the server or all of the servers above. Network and storage, scanning in the database to serve the later search process.

What's new in Nmap

The Nmap 7.70 version, released in March 2018, has provided nine new NSE scripts and provided hundreds of new operating system and service codes for the operating system and applications that detect application versions, including code that supports IPv6 and IPv4.Improvements in version 7.70 also help to detect the service version faster and more accurately.Due to the widespread use of Windows, the introduction of improvements to the Npcap Windows capture package is also offered to enhance performance and stability are particularly important steps from the publisher.

The next release of Nmap is expected to be released by the end of the third quarter or early in the fourth quarter of this year, but Lyon also noted that between the releases, scripts and new protocols that are being refined by the company. and available for user testing.

"Converting from outdated Winpcap drivers to our new Npcap system is an unprecedented big step for Windows Nmap users. We will also continue to expand and improve Nmap Scripting Engine. Now we have 591 scripts and 133 protocol libraries, you can find at https://nmap.org/nsedoc/. I feel like my brainchild is now really In fact, Nmap will turn 21 on September 1! ', Lyon said.

Is Nmap being used for unauthorized behavior?

Although port scanning is not an illegal feature, at least under US federal law, Nmap's features are definitely useful for bad-looking hackers looking for holes. Security vulnerability to exploit.Certain applications of the software, not allowed to access, if ignored, you may be fired or have legal trouble, even if you are performing a vulnerability scan because of bad purpose.

While some Nmap scans are quite light and can't turn off alerts, it's best to proceed with your authorized scans with the appropriate individuals in your organization.Note that many Nmap options, such as OS fingerprinting, require access to the original data.Therefore, when doubting about the legality of the things you want to do, especially when you work alone and without the legal team of the organization to consult, talk to a lawyer. have expertise in computer fraud and abuse.

Nmap resources

If you want to learn more about Nmap, the only and best source of information you should consult is Nmap.org.This website is maintained and handled by the author FyodorVaskovitch.Essential resources on Nmap.org and other websites include:

1. Document.
2. Nmap reference guide, detailed description of Nmap and how it works.
3. Zenmap user guide.
4. Nmap users can join the Nmap-hacker mailing list to keep track of updates. Developers interested in testing or contributing code and suggestions can subscribe to the Nmap-dev list.
5. Top 100 network security tools are voted by Nmap users.

Download Nmap where?

To download Nmap, visit here and follow the instructions.

See more:

1. 4 websites to quickly check the safety of links
2. How to hack WiFi passwords with holes on WPA / WPA2
3. How to protect your computer against a Foreshadow security vulnerability
4. Learn about DNS Cache spoofing and DNS Cache poisoning