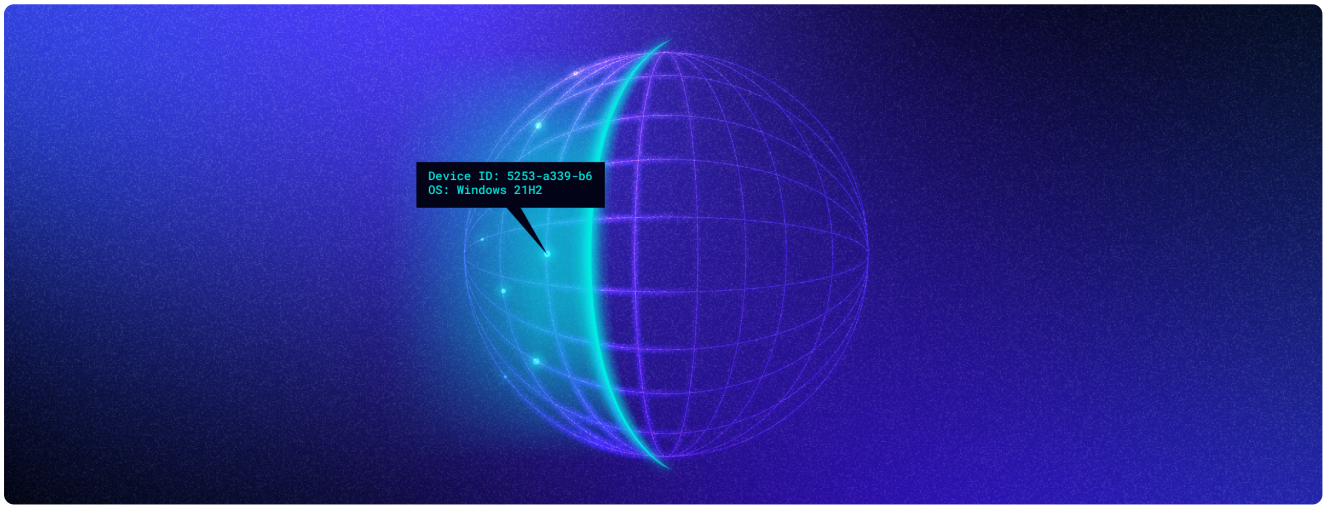
Blog / Data Security

How to Use Nmap: Commands and Tutorial Guide

Michael Buckbee

7 min read

Last updated May 4, 2022

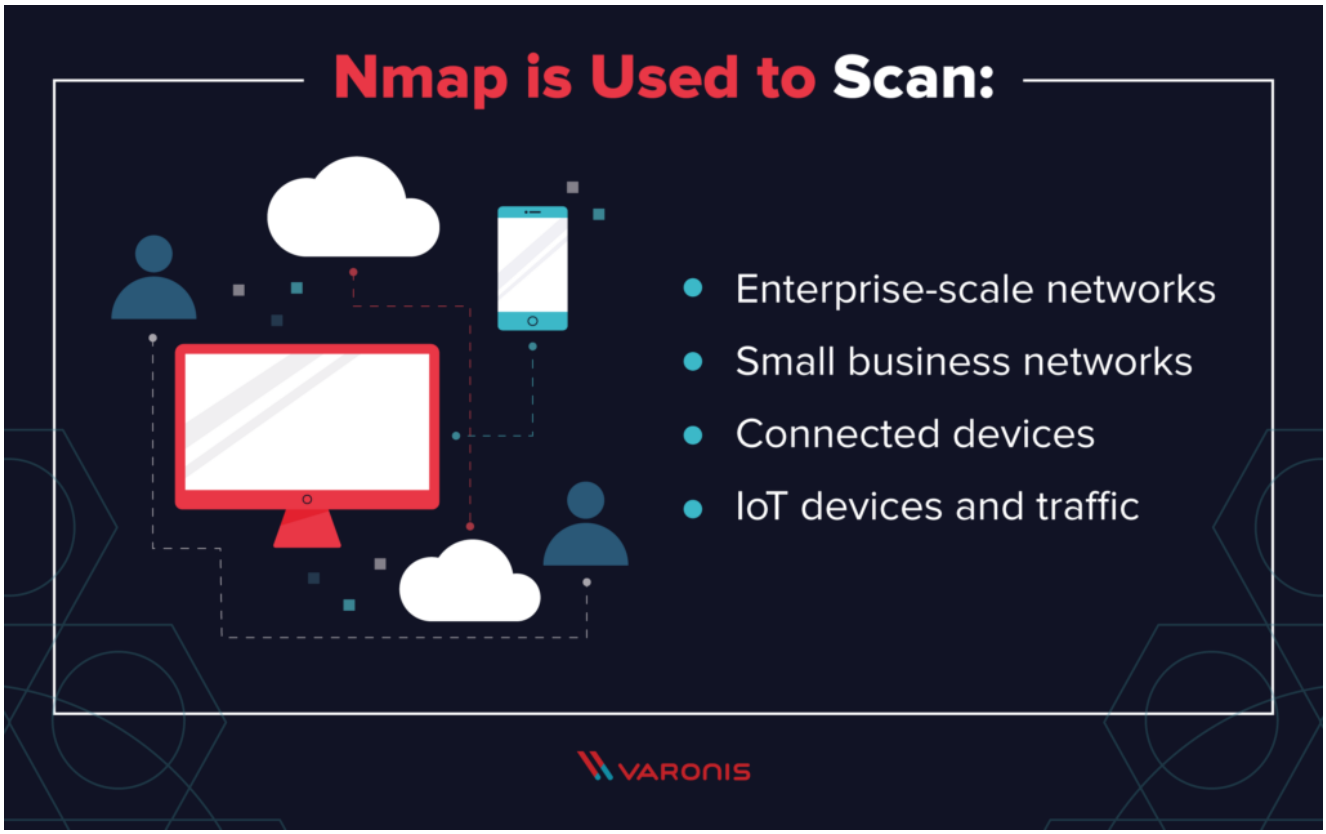


Nmap is a network mapper that has emerged as one of the most popular, free network discovery tools on the market. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection,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

A number of recent cyberattacks have re-focused attention on the type of network auditing that Nmap provides. Analysts have pointed out that the recent Capital One hack, for instance, could have been detected sooner if system administrators had been monitoring connected devices. In this guide, we'll look at what Nmap is, what it can do, and explain how to use the most common commands.

Ideally, Nmap should be used as part of an integrated Data Security Platform. Once Nmap has been used to map a network, a platform such as Varonis' Datadvantage can then be used to implement advanced access control.

What is Nmap?



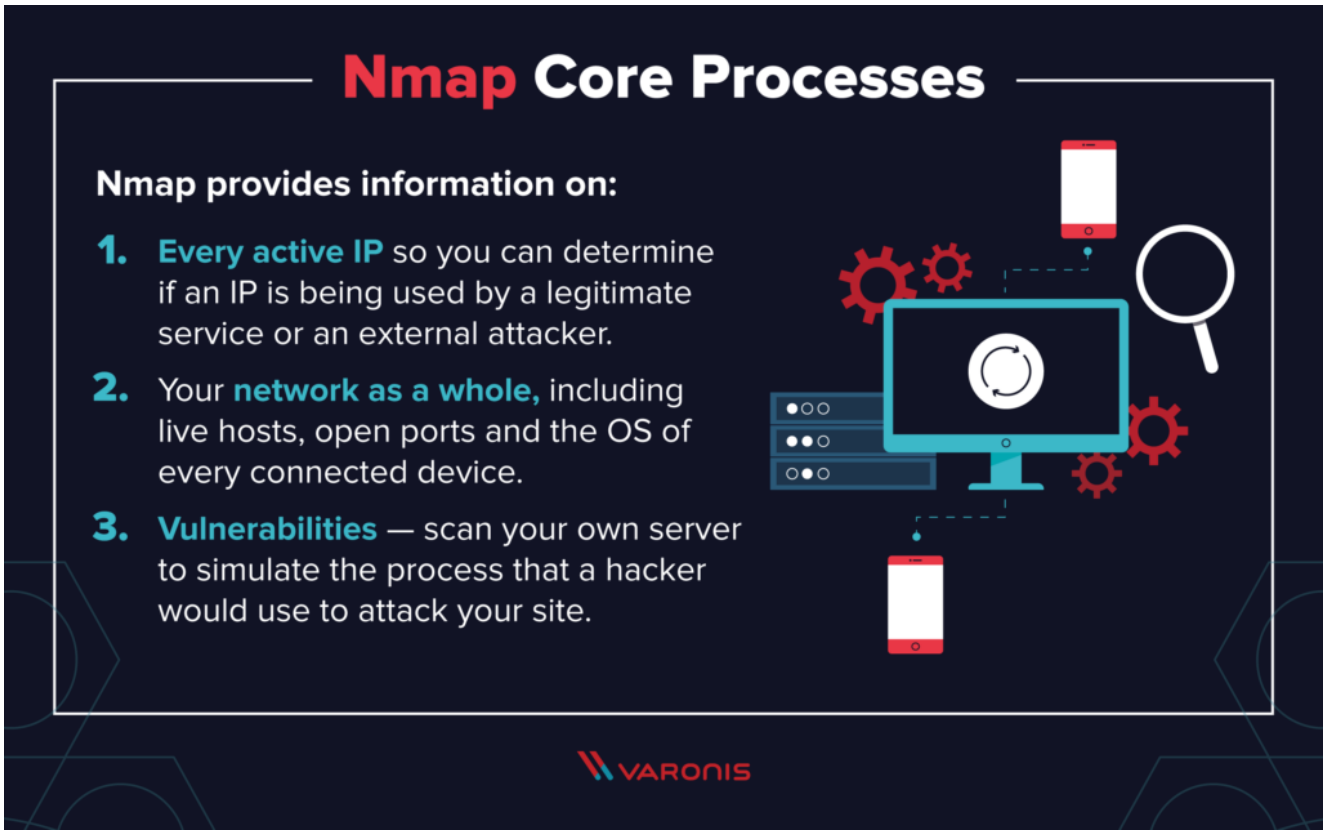
At its core, Nmap is a network scanning tool that uses IP packets to identify all the devices connected to a network and to provide information on the services and operating systems they are running.

The program is most commonly used via a command-line interface (though GUI front-ends are also available) and is available for many different operating systems such as Linux, Free BSD, and Gentoo. Its popularity has also been bolstered by an active and enthusiastic user support community.

Nmap was developed for enterprise-scale networks and can scan through thousands of connected devices. However, in recent years Nmap is being increasingly used by smaller companies. The rise of the IoT, in particular, now means that the networks used by these companies have become more complex and therefore harder to secure.

This means that Nmap is now used in many website monitoring tools to audit the traffic between web servers and IoT devices. The recent emergence of IoT botnets, like Mirai, has also stimulated interest in Nmap, not least because of its ability to interrogate devices connected via the UPnP protocol and to highlight any devices that may be malicious.

What Does Nmap Do?



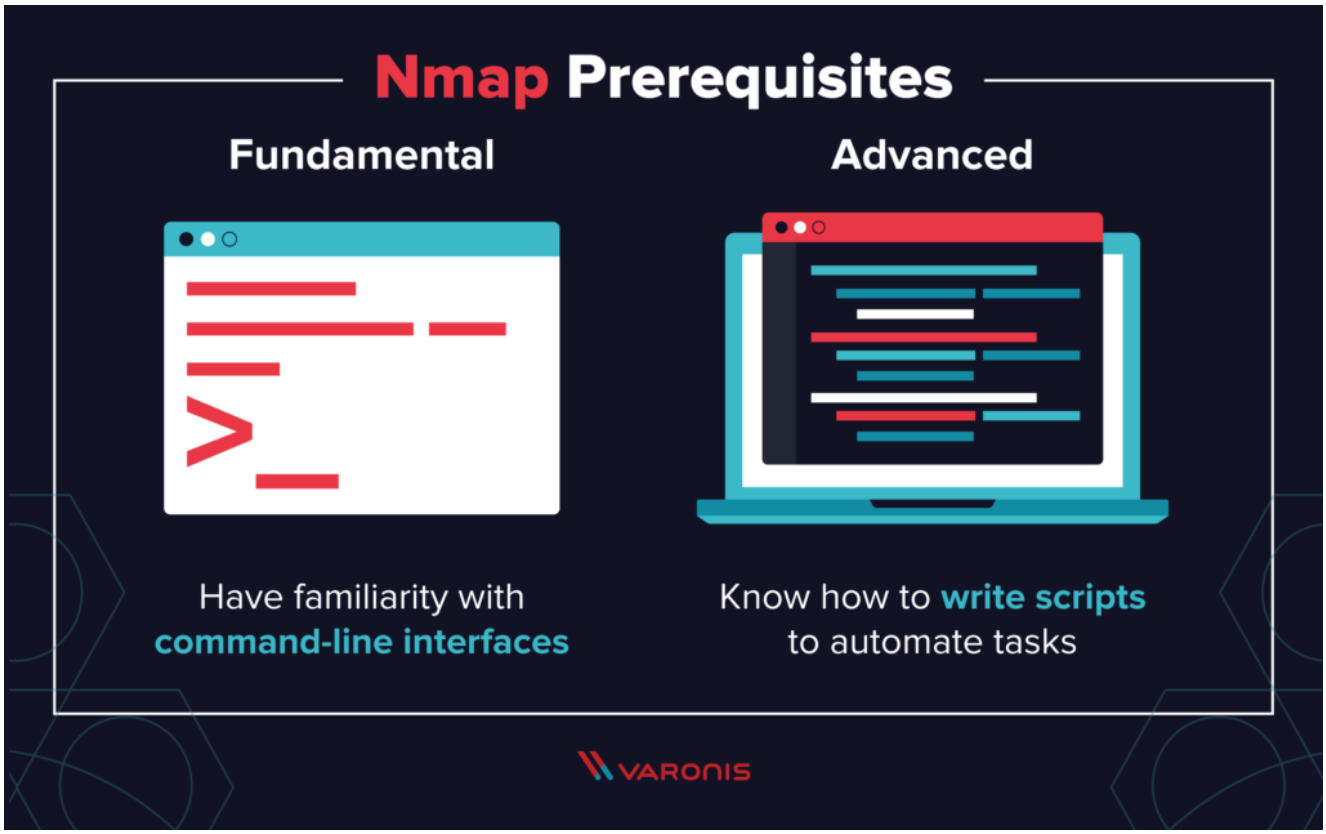
At a practical level, Nmap is used to provide detailed, real-time information on your networks, and on the devices connected to them.

The primary uses of Nmap can be broken into three core processes. First, the program gives you detailed information on every IP active on your networks, and each IP can then be scanned. This allows administrators to check whether an IP is being used by a legitimate service, or by an external attacker.

Secondly, Nmap provides information on your network as a whole. It can be used to provide a list of live hosts and open ports, as well as identifying the OS of every connected device. This makes it a valuable tool in ongoing system monitoring, as well as a critical part of pentesting. Nmap can be used alongside the Metasploit framework, for instance, to probe and then repair network vulnerabilities.

Thirdly, Nmap has also become a valuable tool for users looking to protect personal and business websites. Using Nmap to scan your own web server, particularly if you are hosting your website from home, is essentially simulating the process that a hacker would use to attack your site. “Attacking” your own site in this way is a powerful way of identifying security vulnerabilities.

How To Use Nmap



Nmap is straightforward to use, and most of the tools it provides are familiar to system admins from other programs. The advantage of Nmap is that it brings a wide range of these tools into one program, rather than forcing you to skip between separate and discrete network monitoring tools.

In order to use Nmap, you need to be familiar with command-line interfaces. Most advanced users are able to write scripts to automate common tasks, but this is not necessary for basic network monitoring.

How To Install Nmap

The process for installing Nmap is easy but varies according to your operating system. The Windows, Mac, and Linux versions of the program can be downloaded here.

> For Windows, Nmap comes with a custom installer (namp<version>setup.exe). Download and run this installer, and it automatically configures Nmap on your system.

On Mac, Nmap also comes with a dedicated installer. Run the Nmap-<version>mpkg file to start this installer. On some recent versions of macOS, you might see a warning that Nmap is an “unidentified developer”, but you can ignore this warning.

Linux users can either compile Nmap from source or use their chosen package manager. To use apt, for instance, you can run Nmap –version to check if Nmap is installed, and sudo apt-get install Nmap to install it.

Nmap Tutorial and Examples

Once you’ve installed Nmap, the best way of learning how to use it is to perform some basic network scans.

How To Run a Ping Scan

One of the most basic functions of Nmap is to identify active hosts on your network. Nmap does this by using a ping scan. This identifies all of the IP addresses that are currently online without sending any packets to these hosts.

To run a ping scan, run the following command:

```
# nmap -sp 192.100.1.1/24
```

This command then returns a list of hosts on your network and the total number of assigned IP addresses. If you spot any hosts or IP addresses on this list that you cannot account for, you can then run further commands (see below) to investigate them further.

Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to your network. Each host then responds to this packet with another ARP packet containing its status and MAC address.

To run a host scan, use the following command:

```
# nmap -sp <target IP range>
```

This returns information on every host, their latency, their MAC address, and also any description associated with this address. This can be a powerful way of spotting suspicious hosts connected to your network.

If you see anything unusual in this list, you can then run a DNS query on a specific host, by using:

```
# namp -sL <IP address>
```

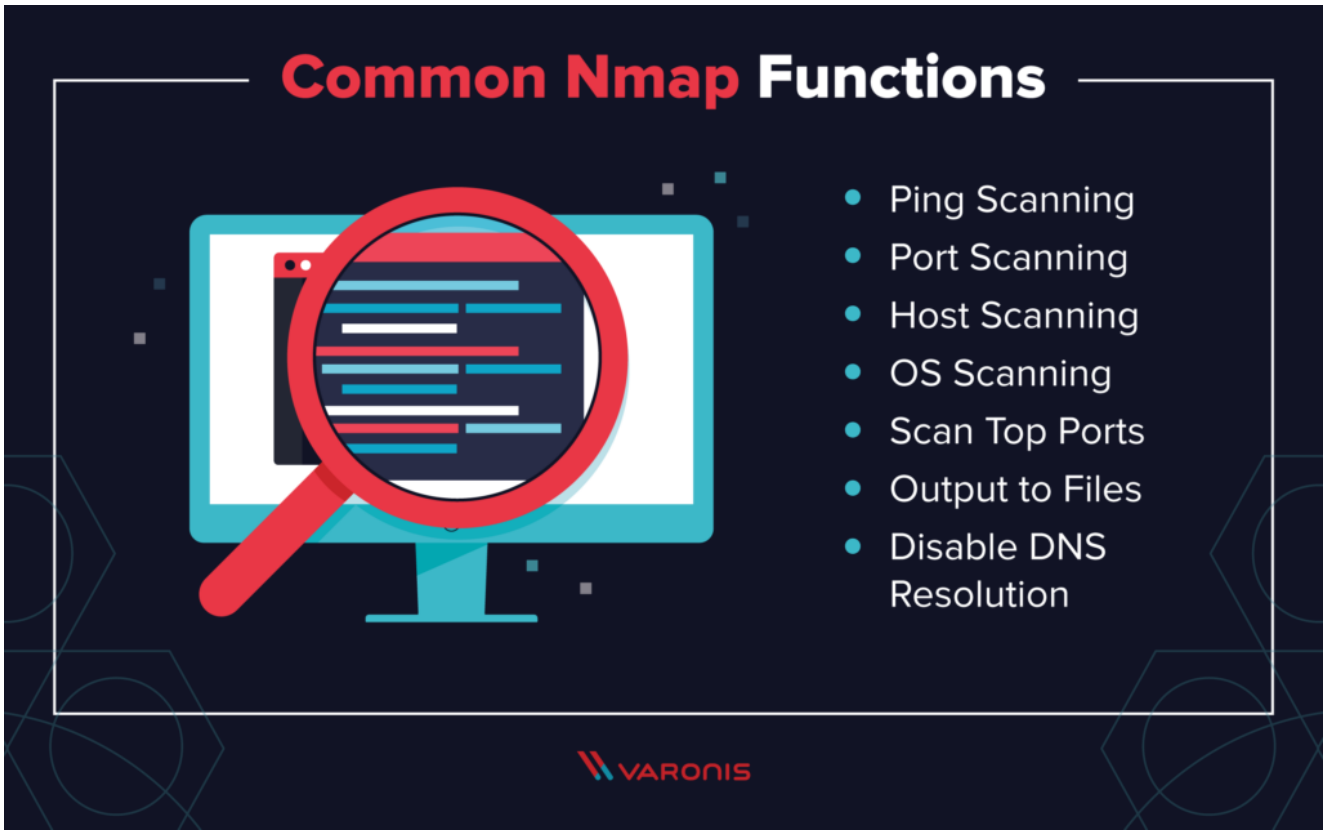
This returns a list of names associated with the scanned IP. This description provides information on what the IP is actually for.

How To Use Nmap in Kali Linux

Using Nmap in Kali Linux can be done in an identical way to running the program on any other flavor of Linux.

That said, there are advantages to using Kali when running Nmap scans. Most modern distros of Kali now come with a fully-features Nmap suite, which includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Nmap Commands



Most of the common functions of Nmap can be executed using a single command, and the program also uses a number of 'shortcut' commands that can be used to automate common tasks.

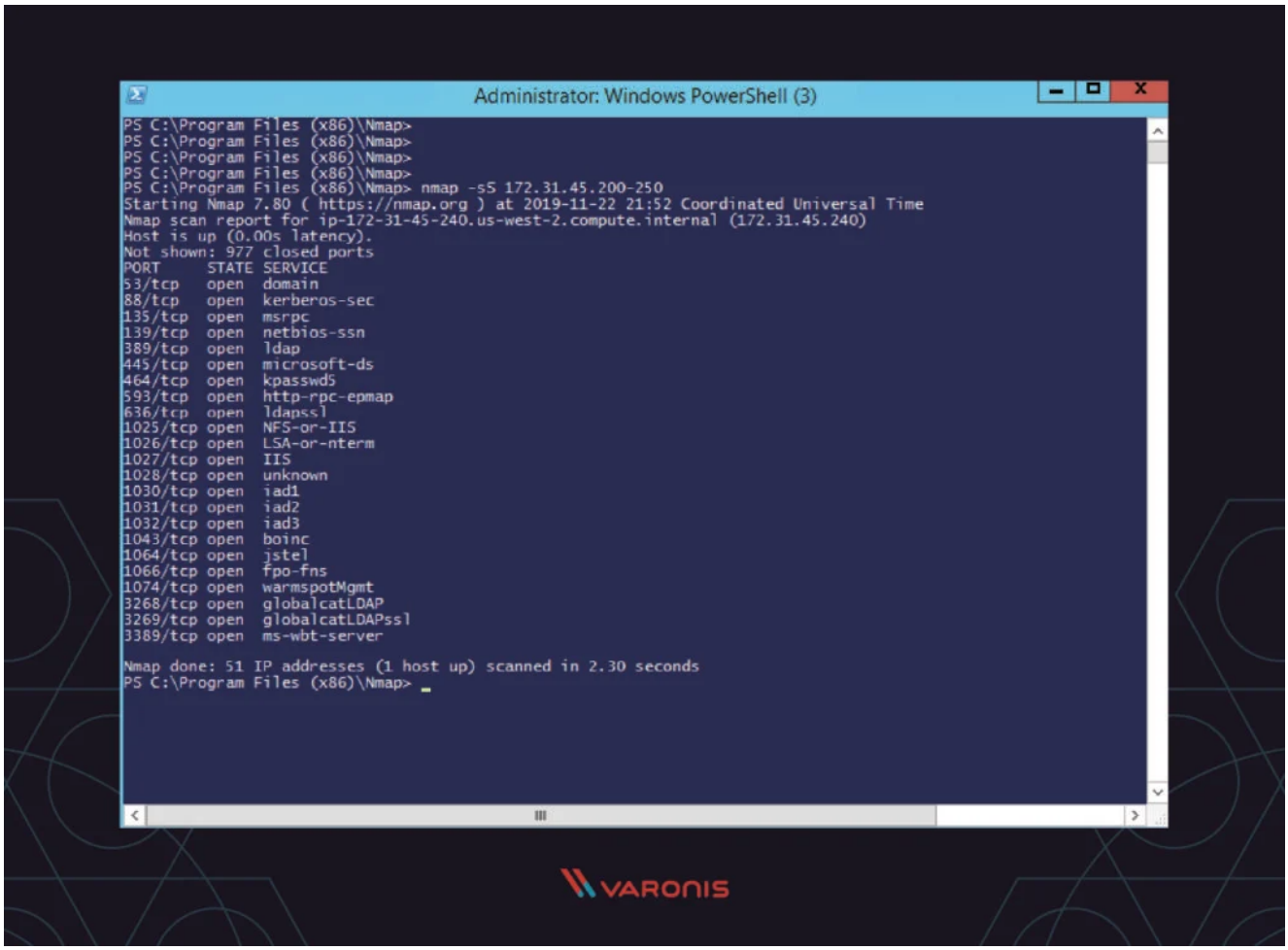
Here is a quick run-down:

1. Ping Scanning

As mentioned above, a ping scan returns information on every active IP on your network. You can execute a ping scan using this command:

```
# nmap -sp 192.100.1.1/24
```

2. Port Scanning



There are several ways to execute port scanning using Nmap. The most commonly used are these:

```
# sS TCP SYN scan

# sT TCP connect scan

# sU UDP scans

# sY SCTP INIT scan

# sN TCP NULL
```

The major differences between these types of scans are whether they cover TCP or UDP ports and whether they execute a TCP connection. Here are the basic differences:

The most basic of these scans is the sS TCP SYN scan, and this gives most users all the information they need. It scans thousands of ports per second, and because it doesn't complete a TCP connection it does not arouse suspicion.

The main alternative to this type of scan is the TCP Connect scan, which actively queries each host, and requests a response. This type of scan takes longer than a SYN scan, but can return more reliable information.

The UDP scan works in a similar way to the TCP connect scan but uses UDP packets to scan DNS, SNMP, and DHCP ports. These are the ports most frequently targeted by hackers, and so this type of scan is a useful tool for checking for vulnerabilities.

The SCTP INIT scan covers a different set of services: SS7 and SIGTRAN. This type of scan can also be used to avoid suspicion when scanning an external network because it doesn't complete the full SCTP process.

The TOP NULL scan is also a very crafty scanning technique. It uses a loophole in the TCP system that can reveal the status of ports without directly querying them, which means that you can see their status even where they are protected by a firewall.

3. Host Scanning

Host scanning returns more detailed information on a particular host or a range of IP addresses. As mentioned above, you can perform a host scan using the following command:

```
# nmap -sp <target IP range>
```

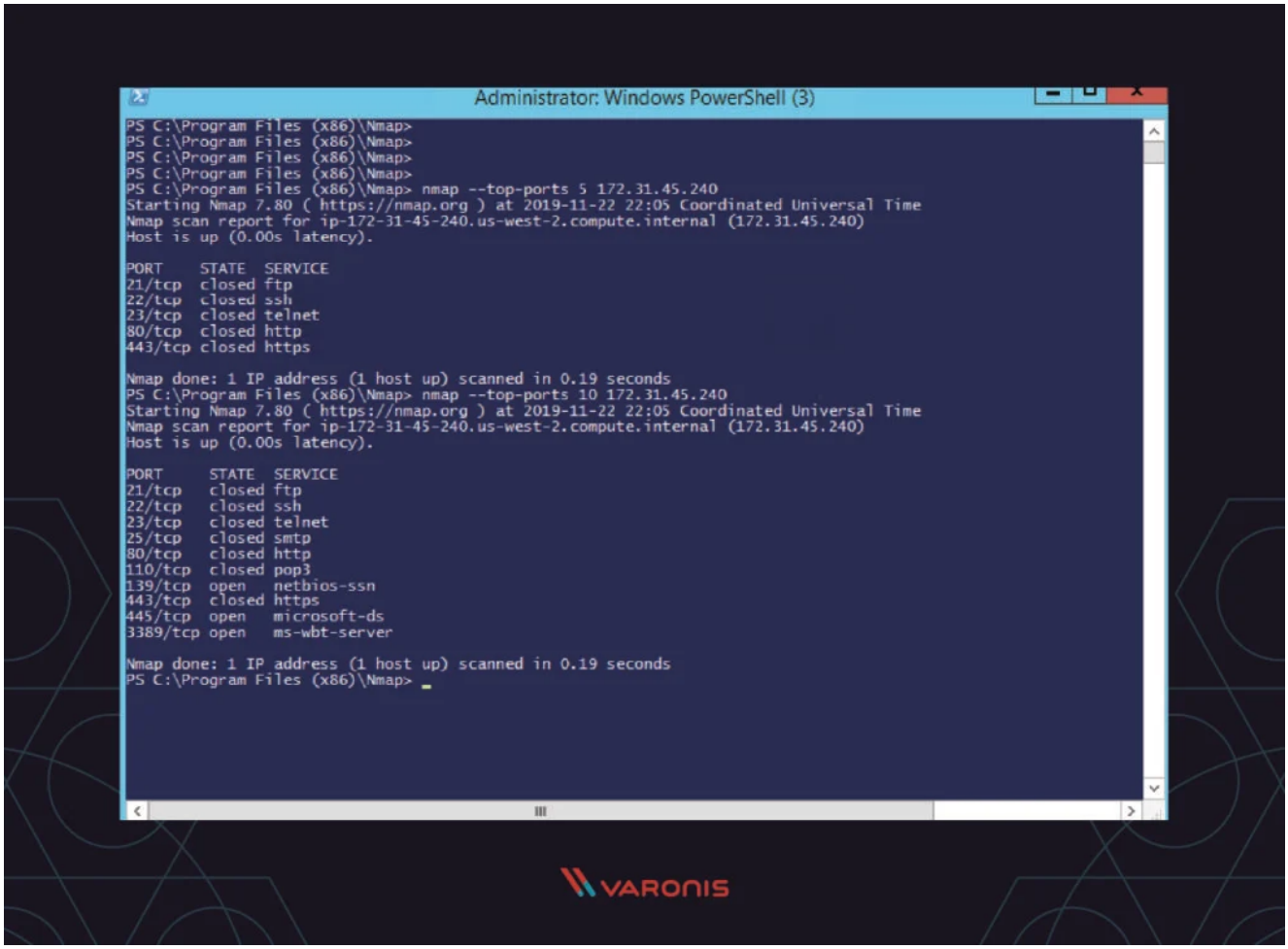
4. OS Scanning

OS scanning is one of the most powerful features of Nmap. When using this type of scan, Nmap sends TCP and UDP packets to a particular port, and then analyze its response. It compares this response to a database of 2600 operating systems, and return information on the OS (and version) of a host.

To run an OS scan, use the following command:

```
# nmap -O <target IP>
```

5. Scan The Most Popular Ports



If you are running Nmap on a home server, this command is very useful. It automatically scans a number of the most 'popular' ports for a host. You can run this command using:

```
nmap --top-ports 20 192.168.1.106
```

Replace the "20" with the number of ports to scan, and Nmap quickly scans that many ports. It returns a concise output that details the status of the most common ports, and this lets you quickly see whether you have any unnecessarily open ports.

6. Output to a File

If you want to output the results of your Nmap scans to a file, you can add an extension to your commands to do that. Simply add:

```
-oN output.txt
```

To your command to output the results to a text file, or:

```
-oX output.xml
```

To output to an XML.

7. Disable DNS Name Resolution

Finally, you can speed up your Nmap scans by using the -n parameter to disable reverse DNS resolution. This can be extremely useful if you want to scan a large network. For example, to turn off DNS resolution for the basic ping scan mentioned above, add -n:

```
# nmap -sp -n 192.100.1.1/24
```

Nmap FAQ

The commands above cover most of the basic functionality of Nmap. You might still have some questions though, so let's run through the most common ones.

Q: What Are Some Nmap Alternatives?

There are some alternatives to Nmap, but most of them are focused on providing specific, niche functionality that the average system administrator does not need frequently. MASSCAN, for instance, is much faster than Nmap but provides less detail. Umit, by contrast, allows you to run several scans at once.

In reality, however, Nmap provides all the functionality and speed that the average user requires, especially when used alongside other similarly popular tools like NetCat (which can be used to manage and control network traffic) and ZenMap (which provides a GUI for Nmap)

Q: How Does Nmap Work?

Nmap builds on previous network auditing tools to provide quick, detailed scans of network traffic. It works by using IP packets to identify the hosts and IPs active on a network and then analyze these packets to provide information on each host and IP, as well as the operating systems they are running.

Q: Is Nmap Legal?

Yes. If used properly, Nmap helps protect your network from hackers, because it allows you to quickly spot any security vulnerabilities in your systems.

Whether port scanning on external servers is legal is another issue. The legislation in this area is complex and varies by territory. Using Nmap to scan external ports can lead to you being banned by your ISP, so make sure you research the legal implications of using the program before you start using it more widely.

The Bottom Line

Taking the time to learn Nmap can dramatically increase the security of your networks because the program offers a quick, efficient way of auditing your systems. Even the basic features offered by the program – such as the ability to perform port scanning – quickly reveal any suspicious devices that are active on your network.

Using Nmap to perform frequent network audits can help you avoid becoming easy prey for hackers, whilst also improving your knowledge of your own network. In addition, Nmap provides functionality that complements more fully-featured data security platforms such as that offered by Varonis, and when used alongside these tools can dramatically improve your cybersecurity.

What you should do now

Below are three ways we can help you begin your journey to reducing data risk at your company:

1. **Schedule a demo session with us**, where we can show you around, answer your questions, and help you see if Varonis is right for you.
2. **Download our free report** and learn the risks associated with SaaS data exposure.
3. Share this blog post with someone you know who'd enjoy reading it. Share it with them via **email, LinkedIn, Reddit,** or **Facebook.**

Michael Buckbee

Michael has worked as a sysadmin and software developer for Silicon Valley startups, the US Navy, and everything in between.

View sample

Keep reading

Speed Data: When Lives Depend on Strong Security With John Mason

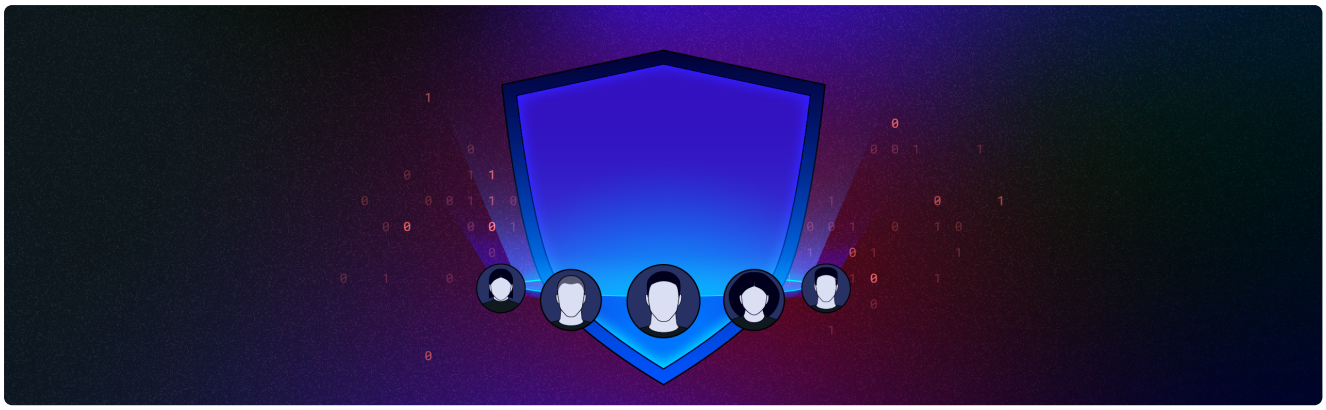
Megan Garza
January 18, 2024

Tempo Technology Services' John Mason shares why strong cybersecurity in healthcare is so critical and how organizations can combat malicious actors.

2024 Cybersecurity Trends: What You Need to Know

Lexi Croisdale
December 26, 2023

Learn more about data security posture management, AI security risks, compliance changes, and more to prepare your 2024 cybersecurity strategy.



Straight From the CISO: Top Tips for Today's Cybersecurity Leaders

Megan Garza

December 14, 2023

We've gained massive insight from our conversations with CISOs and other cybersecurity leaders. Now, we're passing along their wisdom to you.

Data Classification

Labels

Policy Pack

DatAnswers

DatAlert

Edge

Data Transport Engine

DataPrivilege

DatAdvantage Cloud

Data Classification

Cloud

Solutions

By use case

Cloud data protection

Data discovery & classification

Compliance management

Data loss prevention

Data activity auditing

DSPM

Least privilege automation

Insider risk management

Proactive incident response

Ransomware prevention

SSPM

Zero Trust

By industry

Finance

Healthcare

Federal government

Education

Manufacturing

State & local government

Integrations

Microsoft 365

On-prem data & apps

Cloud data, SaaS, & IaaS

Directory services

NAS

Network devices

Third-party apps

Why Varonis?

Case studies

Operational plan

Industry recognition

Customer success

IR & forensics team

Measurable ROI

Why Varonis SaaS

Company

About Varonis

Careers

Investor relations

Press

Corporate responsibility

Trust & security

Brand

Partners

Partner program

Partner locator

Partner portal

Service providers

Technology partners

Buy on AWS marketplace

Buy on Azure

marketplace

Resources

Resource library

Blog

Free security courses

Product training

SecurityFWD

Webinars

Events

Support

Community

Contact Us

Get a demo

Get support

+1 (877) 292-8767