**NAME**: ADWAIT S PURAO

**UID**: 2021300101

**BATCH**: B2

**AIM**: Network Scanning using Open-Source Tools - NMAP

**EXPERIMENT** **NO**.: 10

**THEORY**:

# What is Nmap and why do you need it on your network?

Nmap, short for Network Mapper, is a free and open-source tool used for vulnerability checking, port scanning and, of course, network mapping. Despite being created back in 1997, Nmap remains the gold standard against which all other [similar tools](https://www.networkworld.com/article/3304424/alternatives-to-nmap-from-simple-to-advanced-network-scanning.html), either commercial or open source, are judged.

Nmap has maintained its pre-eminence because of the large community of developers and coders who help to maintain and update it. The Nmap community reports that the tool, which anyone [can get for free](https://nmap.org/download.html), is downloaded several thousand times every week.

Because of its flexible, open-source code base, it can be modified to work within most customized or heavily specialized environments. There are distributions of Nmap specific to Windows, Mac and Linux environments, but Nmap also supports less popular or older operating systems like Solaris, AIX or AmigaOS. The source code is available in C, C++, Perl and Python.

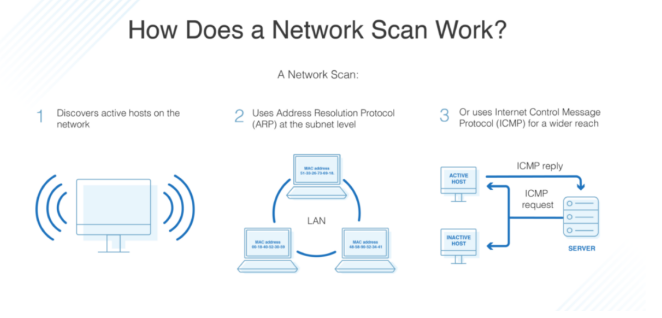
## What is Zenmap?

To deploy Nmap, users originally had to have some advanced programming skills, or at least know their way around console commands or non-graphical interfaces. That changed recently with the introduction of the [Zenmap tool](https://nmap.org/zenmap/) for Nmap, which adds a graphical interface that makes launching the program and analysing the returned output it generates much more accessible.

Zenmap was created to allow beginners to use the tool. Like Nmap, Zenmap is free, and the source code is both open and available to anyone who wants to use or modify it.

Here are some of the capabilities that are enabled by Zenmap: Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. And the results of recent scans can be stored in a searchable database.

## How does Nmap work?



The heart of Nmap is port scanning. How it works is that users designate a list of targets on a network that they want to learn information about. Users don’t need to identify specific targets, which is good because most administrators don’t have a complete picture of everything that is using the potentially thousands of ports on their network. Instead, they compile a range of ports to scan.

It’s also possible to scan all network ports, although that would potentially take a lot of time and eat up quite a bit of available bandwidth. Plus, depending on the type of passive defences that are in use on the network, such a massive port scan would likely trigger security alerts. As such, most people use Nmap in more limited deployments or divide different parts of their network up for scheduled scanning over time.

In addition to setting up a range targets to be scanned, users can also control the depth of each scan. For example, a light or limited scan might return information about which ports are open and which have been closed by firewall settings. More detailed scans could additionally capture information about what kind of devices are using those ports, the operating systems they are running and even the services that are active on them. Nmap can also discover deeper information, like the version of those discovered services. That makes it a perfect tool for finding vulnerabilities or assisting with patch management efforts.

Controlling the scans used to require console commands, which of course means that some training was required. But the new Zenmap graphical interface makes it easy for just about everyone to tell Nmap what they want it to discover, with or without formal training. Meanwhile, professionals can continue to use the console commands they always have, making it a useful tool for both experts and novices alike.

## Is Nmap a security risk?

While one could make the argument that Nmap is a perfect hacking tool, many of the deeper scan activities require root access and privileges. Someone from outside can’t just point Nmap at a target network they don’t have permission to access and have it magically uncover vulnerabilities for them to exploit. Not only that, but the attempt would likely trigger a critical security alert by any defensive or network monitoring tools.

That is not to say that Nmap could not be dangerous in the wrong hands, especially if deployed by a turncoat system administrator or someone using stolen credentials. This was demonstrated in the 2016 Oliver Stone movie Snowden (another film that featured Nmap) about the accused traitor Edward Snowden.

## What does Nmap do?

When used properly, Nmap can be invaluable for both optimizing and protecting networks and information. All of the return data sent back by ports scanned using Nmap is collected and complied by the program. Based on that information, there are several key activities that most people use the tool to help accomplish. They include:

**Network Mapping:** This is the core reason why Nmap was created and remains one of the top uses. Called host discovery, Nmap will identify the types of devices actively using scanned ports. This includes servers, routers, switches and other devices. Users can also see how those devices are connected, and how they link together to form a network map.

**Port Rules Discovery:**Nmap can easily tell, even with a low-level scan, if a port is open or closed by something like a firewall. In fact, many IT professionals use Nmap to check their work when programming firewalls. They can see if their policies are having the desired effect, and if their firewalls are working properly.

**Shadow IT Hunting:**Because Nmap discovers the type and location of devices on a network, it can be used to identity things that should not be there at all. These devices are called [shadow IT](https://www.networkworld.com/article/2997152/five-ways-shadow-it-in-the-cloud-hurts-your-enterprise.html) because their presence on a network isn’t officially authorized, or sometimes may be intentionally hidden. Shadow IT can be dangerous because such devices are not part of a security audit or program. For example, if someone secretly places an Xbox game server on a corporate network, not only will that potentially drain bandwidth, but could act as a springboard for an attack, especially if it’s not maintained with all the latest security patches.

**Operating System Detection:**Nmap can discover the types of operating systems running on discovered devices in a process called OS fingerprinting. This generally returns information about the name of the vendor of the device (Dell, HP, etc.) and the operating system. With a deeper Nmap scan, you can even discover things like the patch level of the OS and the estimated uptime of the device.

**Service Discovery:**The ability to discover services elevates Nmap above the level of a common mapping tool. Instead of simply discovering that a device exists, users can trigger a deeper scan in order to find out what roles discovered devices are performing. This includes identifying if they are acting as mail server, a web server, a database repository, a storage device or almost anything else. Depending on the scan, Nmap can also report on which specific applications are running, and what version of those applications are being used.

**Vulnerability Scanning:**Nmap is not a dedicated vulnerability scanning tool in that it does not maintain a database of known vulnerabilities or any kind of artificial intelligence that could identify potential threats. However, organizations that regularly ingest security information from threat feeds or other sources can use Nmap to check their susceptibility to specific threats.

For example, if a newly uncovered vulnerability only affects a certain application or service running an older version of the software, Nmap can be used to check to see if any programs currently operating on network assets meet those conditions. If anything is found, then presumably IT teams could prioritize getting those systems patched as quickly as possible to eliminate the vulnerability before an attacker could discover the same thing.

## What is the future of Nmap?

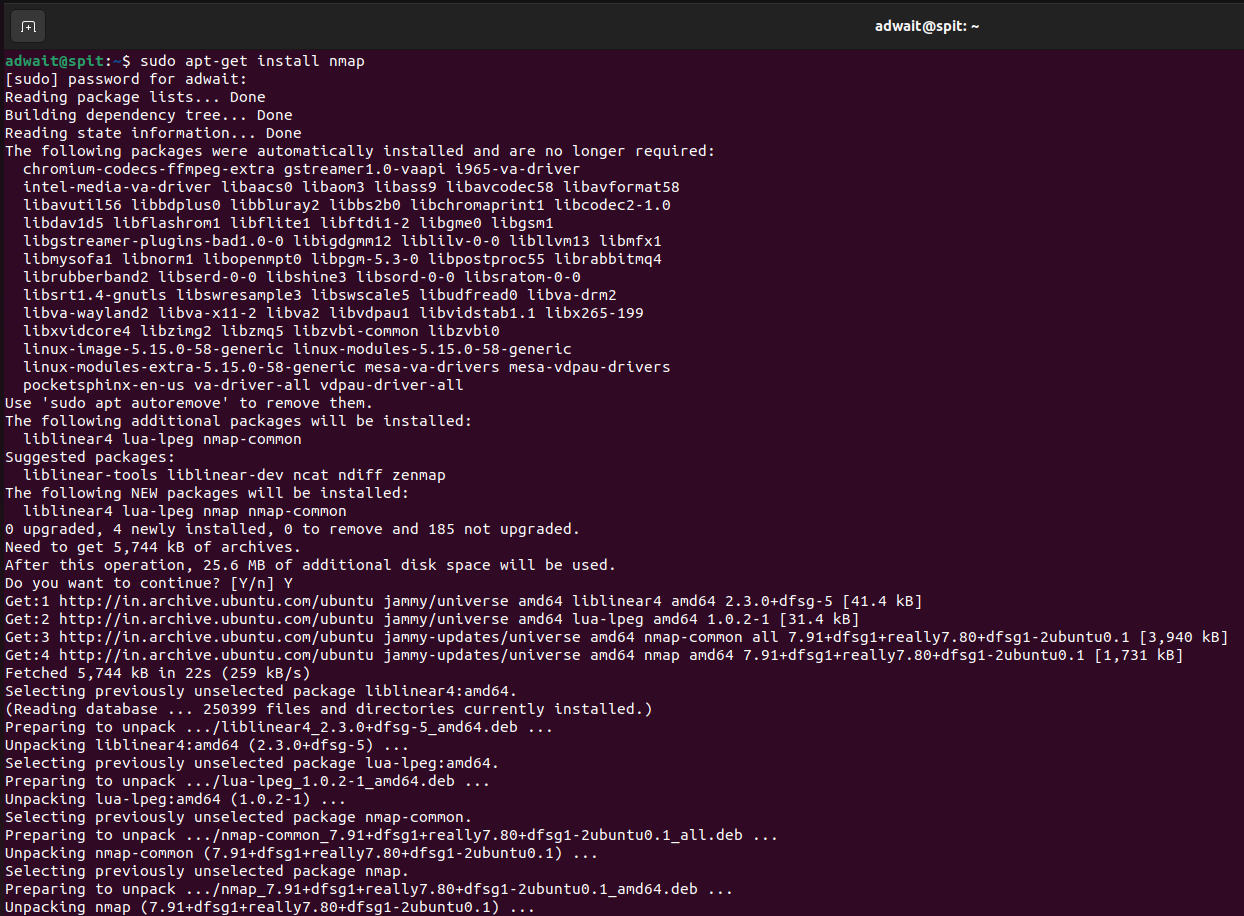
Although the Nmap tool is 25 years old, it continues to evolve. Like other seemingly ancient technologies [such as Ethernet](https://www.networkworld.com/article/3657734/what-is-ethernet.html) or [Spanning Tree](https://www.networkworld.com/article/3654828/what-is-the-spanning-tree-protocol.html), it is well maintained by an active community of experts that keep it relevant and up to date. And in the case of Nmap, that community includes its very active creator, who still goes by his Fyodor guise online.

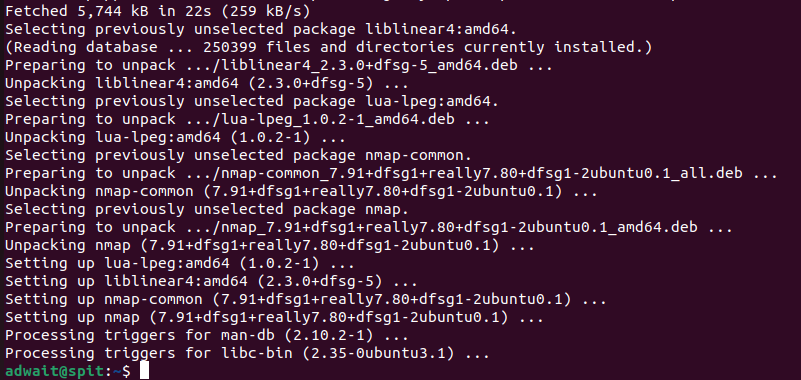
Other advancements like the new Zenmap tool make it even more useful, especially for those who don’t like working with console or command lines. The graphical interface for Zenmap allows users to quickly set up targets and configure desired scans with just a few clicks. That will help Nmap find an even bigger user base.

And finally, while there are many other tools these days that can perform similar functions, none of them have the proven track record of Nmap. Not only that, but Nmap has always been completely free and [ready to download](https://nmap.org/download.html). Because of all of these factors, it’s almost a sure thing that Nmap will be just as useful and relevant over the next 25 years as it has been for past quarter century.

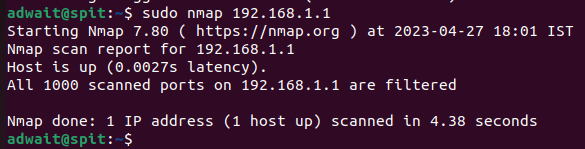
**Screenshots**:

• Installing NMAP

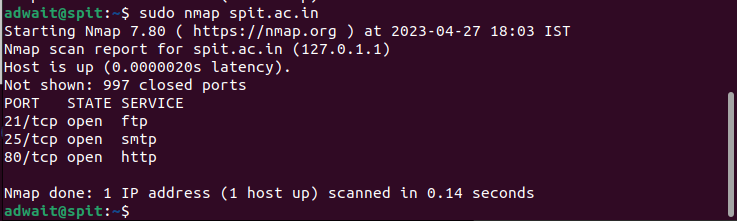




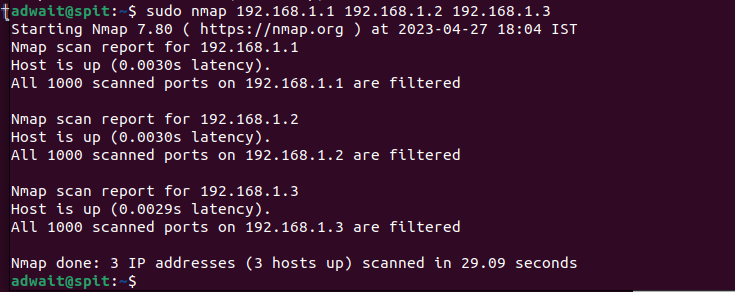
• Single



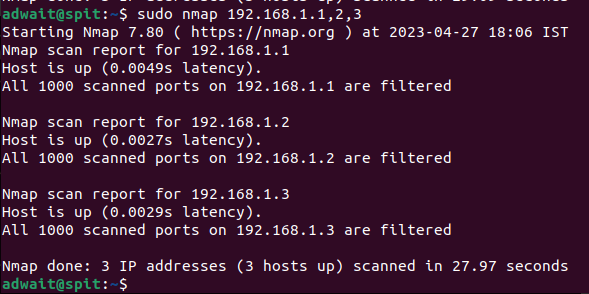
• Server name



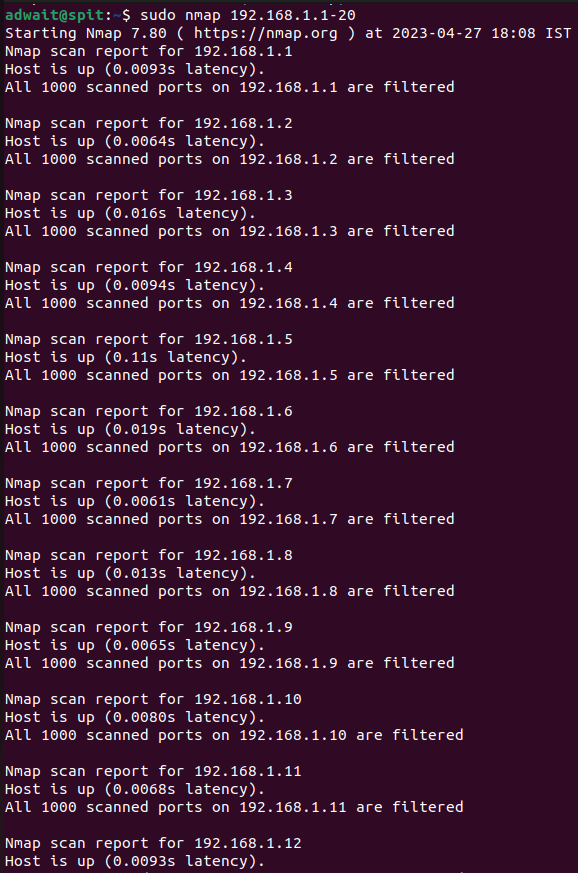
• 2-3 addresses

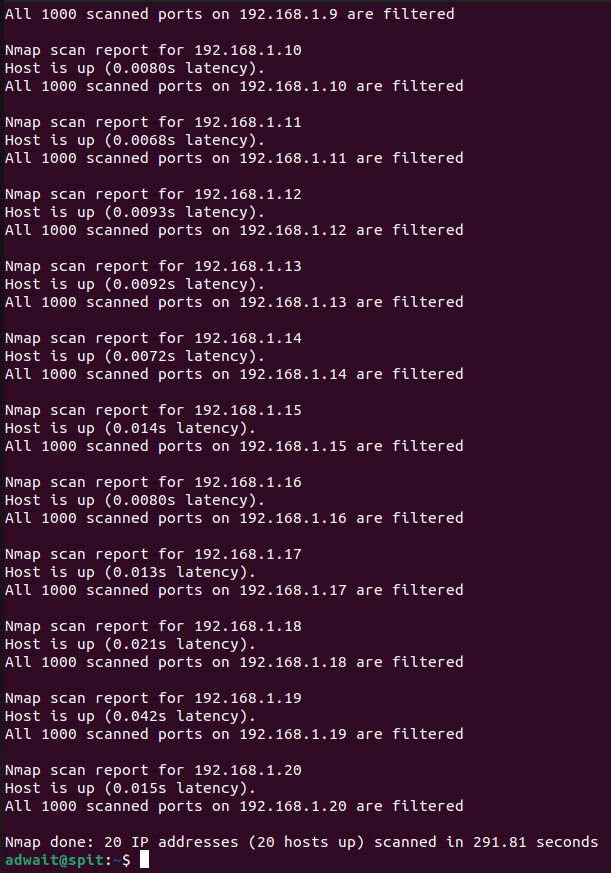


• Range of IP Addresses



• Range of IP address

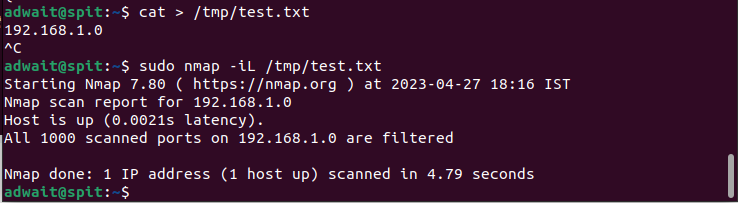




3: Read list of hosts/networks from a file (IPv4):

• The -iL option allows you to read the list of target systems using a text file. This is useful to

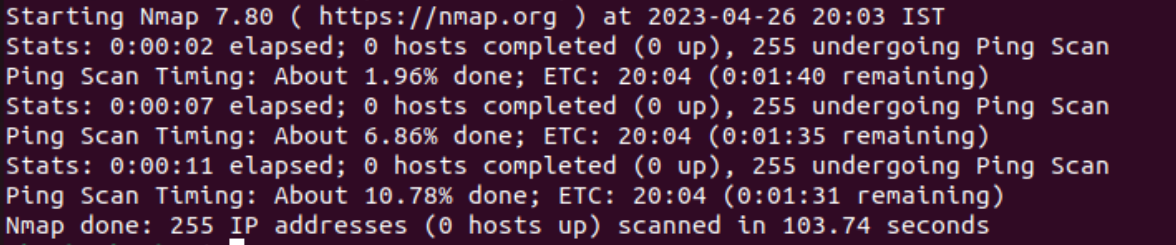
scan many hosts/networks.



4: Excluding hosts/networks (IPv4):

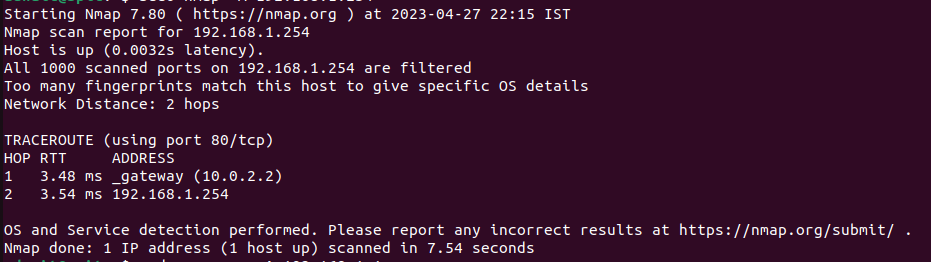
When scanning many hosts/networks you can exclude hosts from a scan:



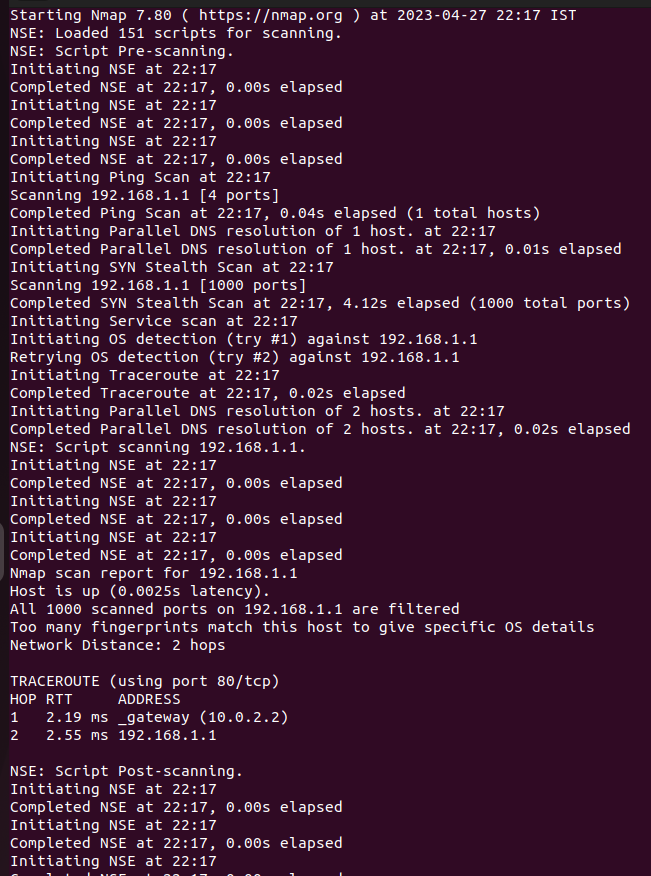


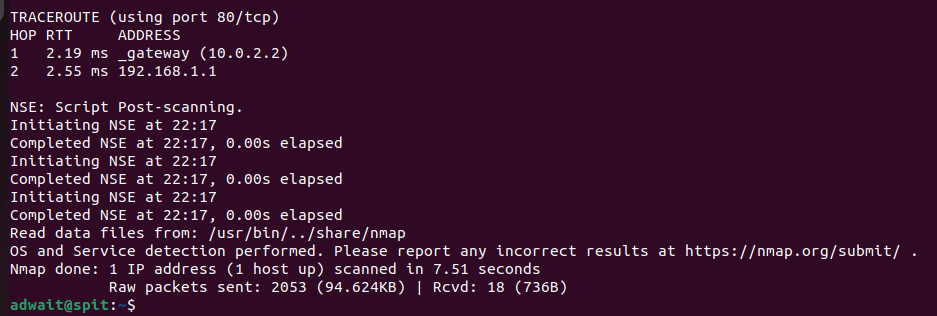
5: Turn on OS and version detection scanning script (IPv4):





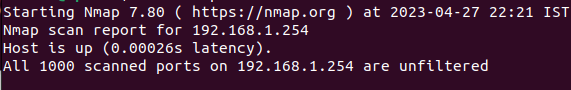




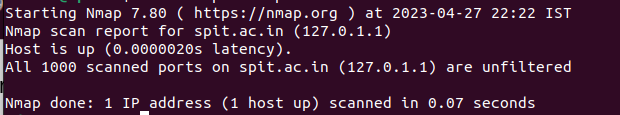


6: Find out if a host/network is protected by a firewall:



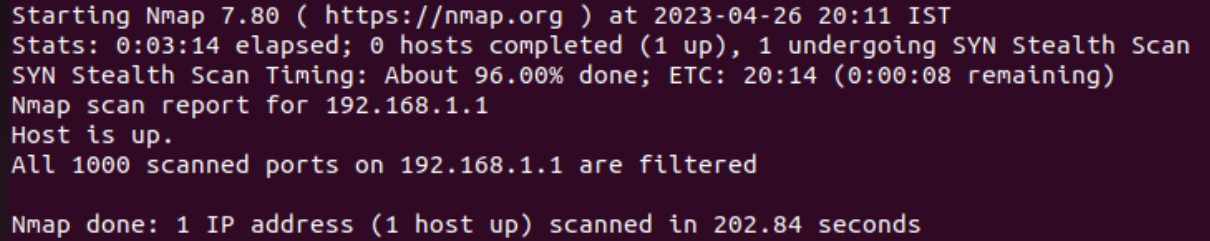




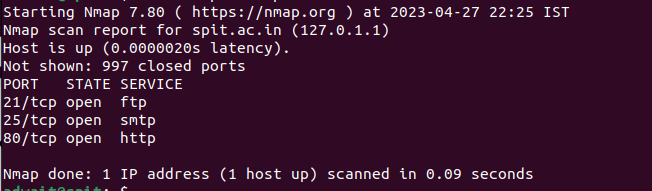


7: Scan a host when protected by the firewall



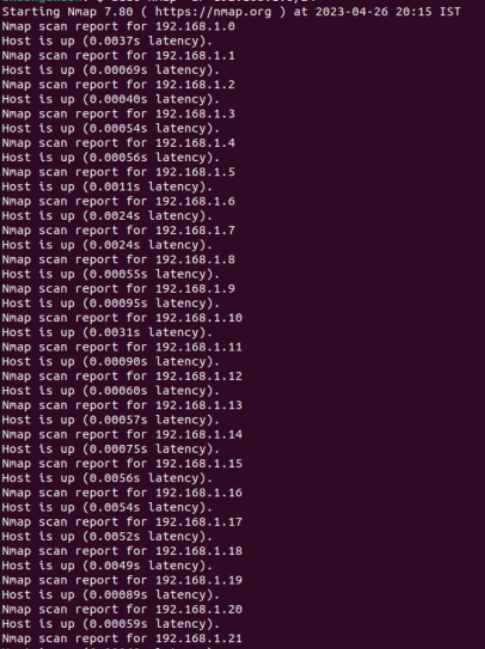


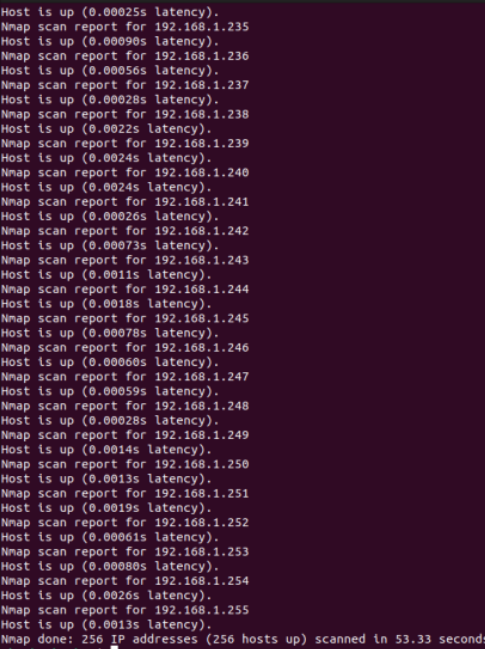




8: Scan a network and find out which servers and devices are up and running

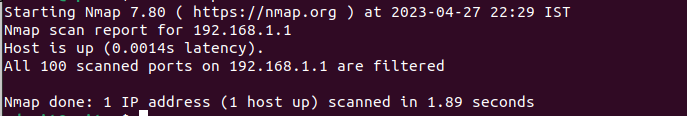






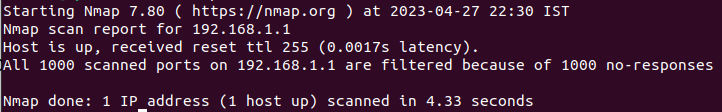
9: How to perform a fast scan?



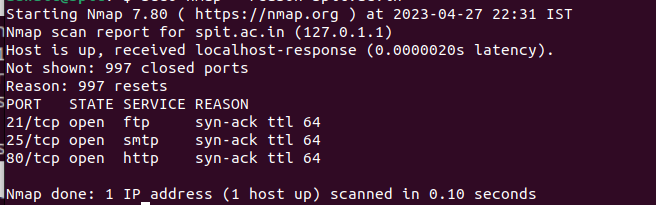


10: Display the reason a port is in a particular state





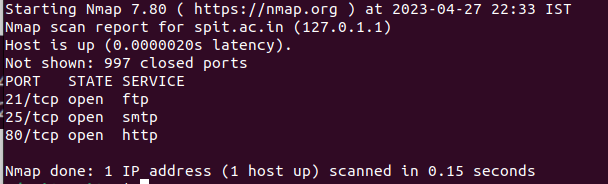




11: Only show open (or possibly open) ports



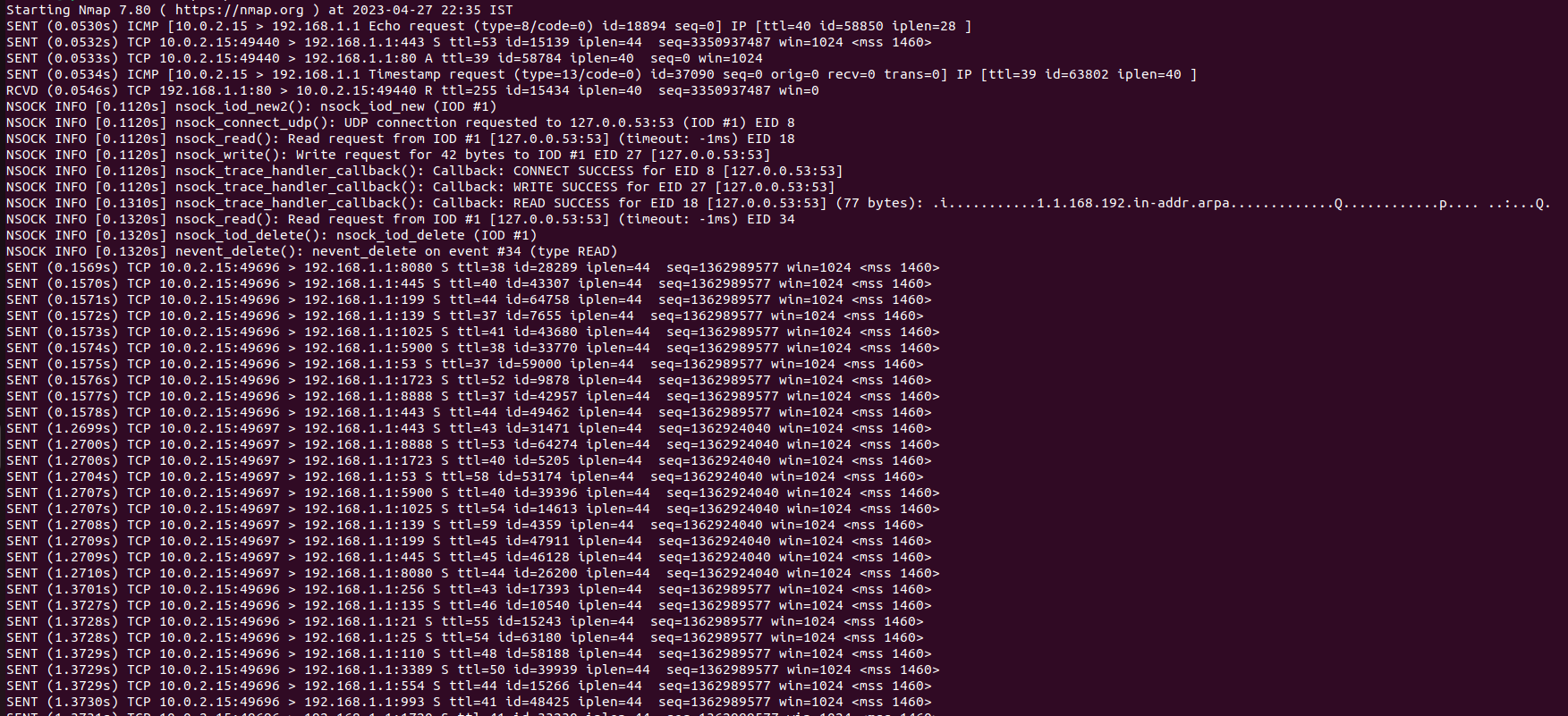


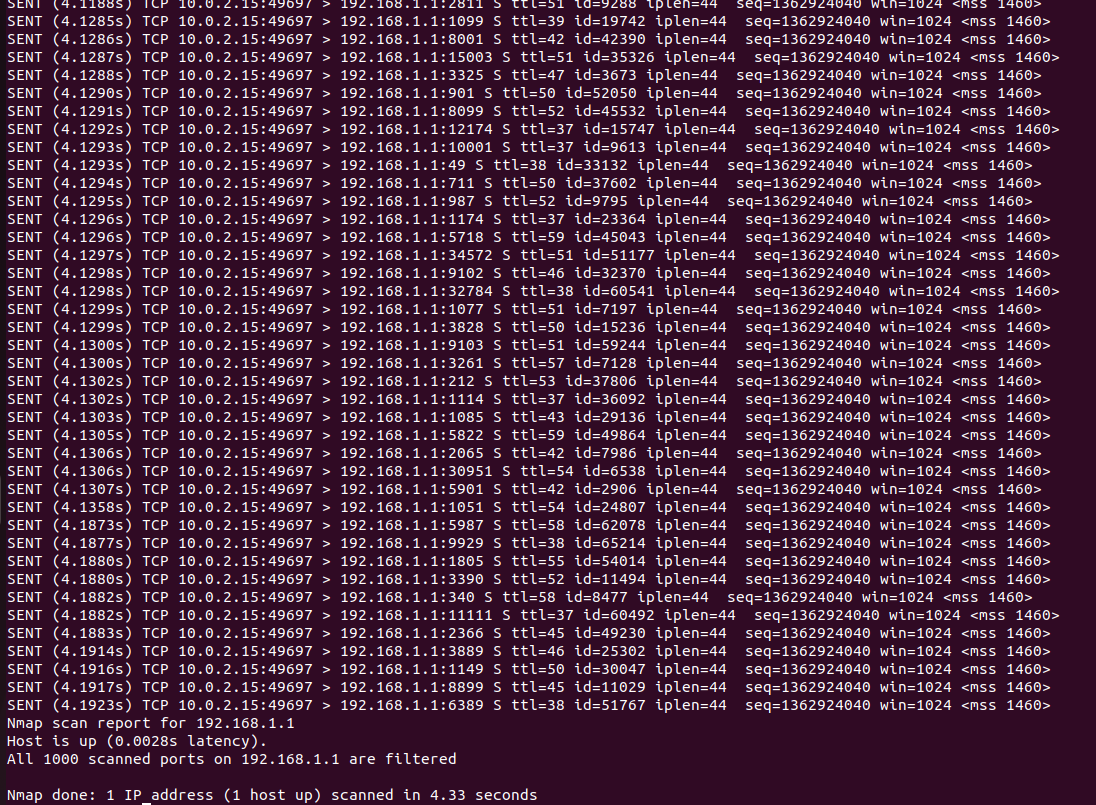


12: Show all packets sent and received

On address

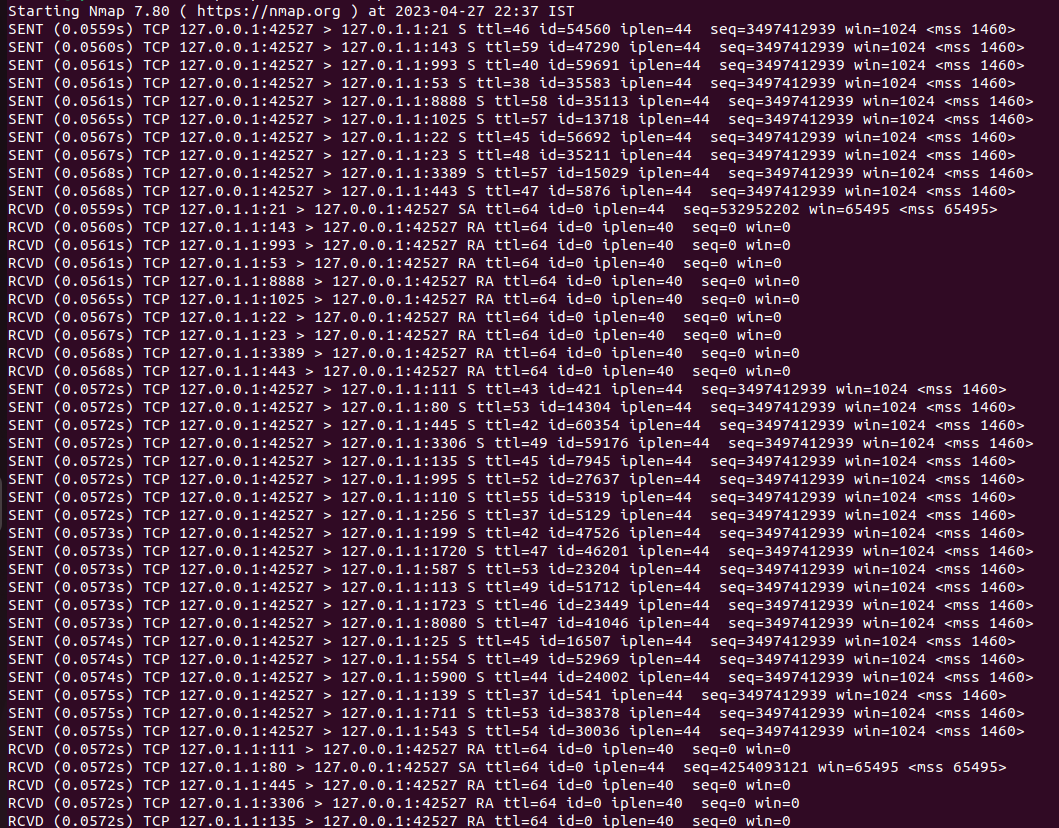


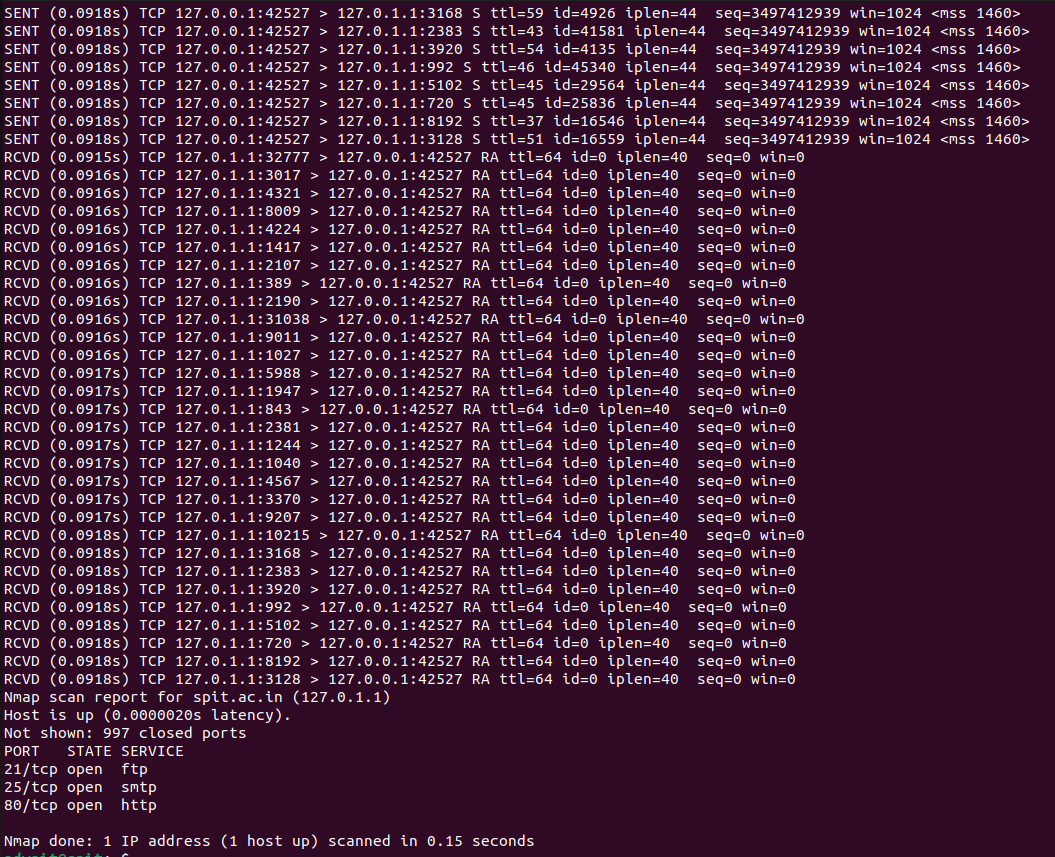




On Server:

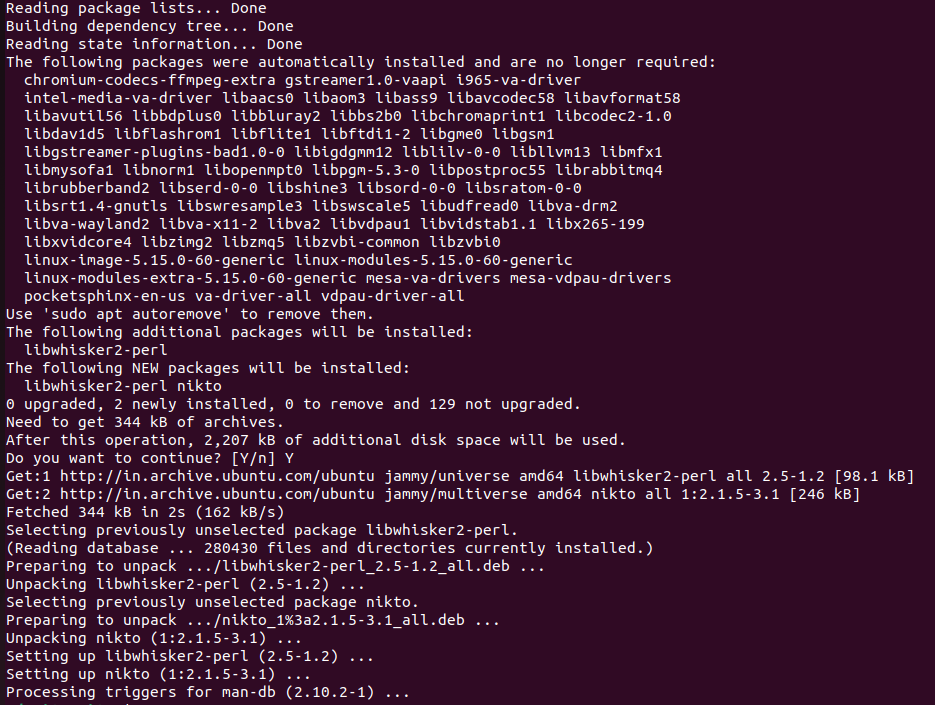




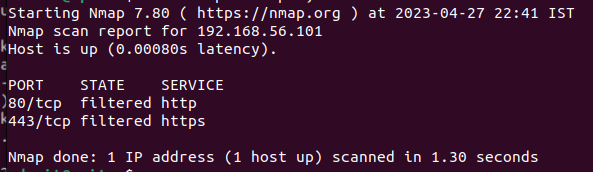


Web Server Scanning













**Conclusion:**

In the experiment, we gained a comprehensive understanding of the Nmap package and its capabilities. Nmap proved to be a valuable tool in scanning and analyzing networks by detecting the operating system, identifying open ports, and services running on the target system. We also learned about web scanning using nikto, which allowed us to identify potential security risks and vulnerabilities in web applications. Overall, this experience provided us with valuable hands-on experience in using Nmap and nikto, two powerful tools for network and web security professionals.