# NMAP Commands

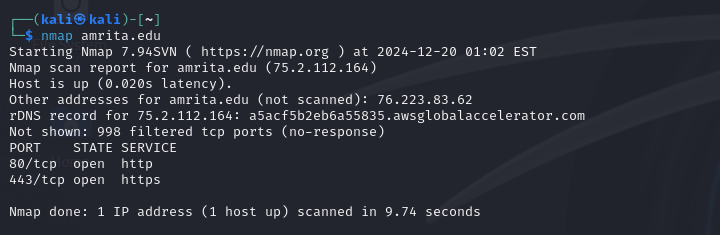
Agasthya P – CH.EN.U4CYS22004

# 

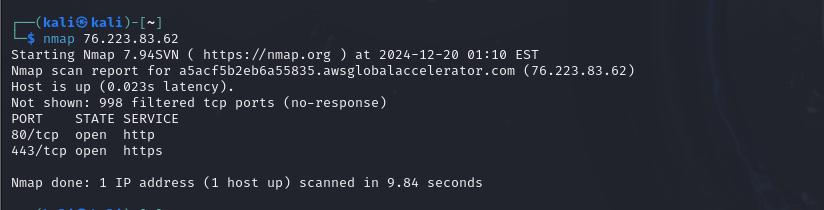
1. Scan a System with Hostname and IP Address

The Nmap tool offers various methods to scan a system. In this example, I am performing a scan using hostname as amrita.edu to find out all open ports, services and MAC address on the system.

**Scan using Hostname**

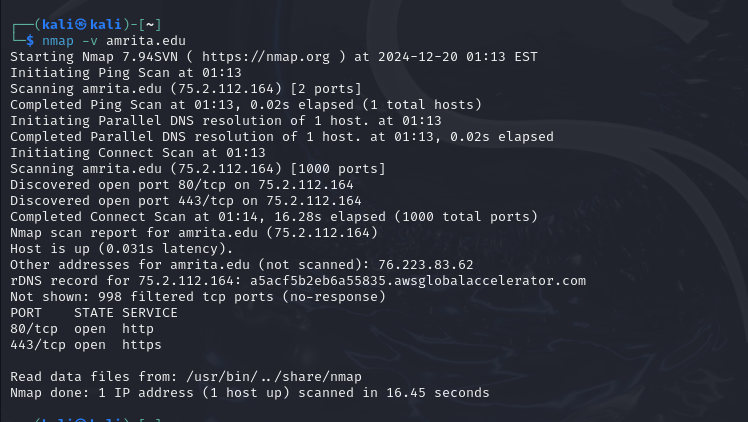


Scan using IP Address



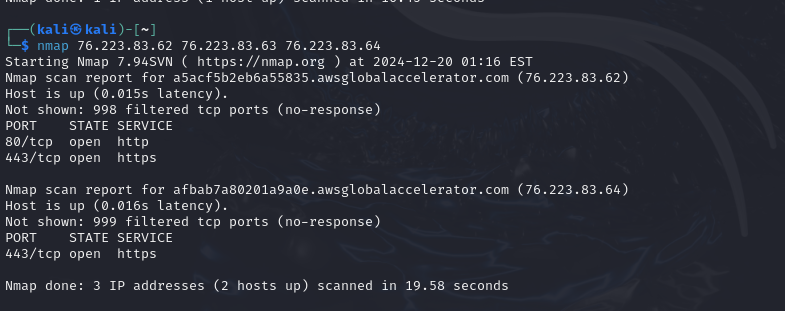
2. Scan using “-v” option

You can see that the below command with “-v” option is giving more detailed information about the remote machine.



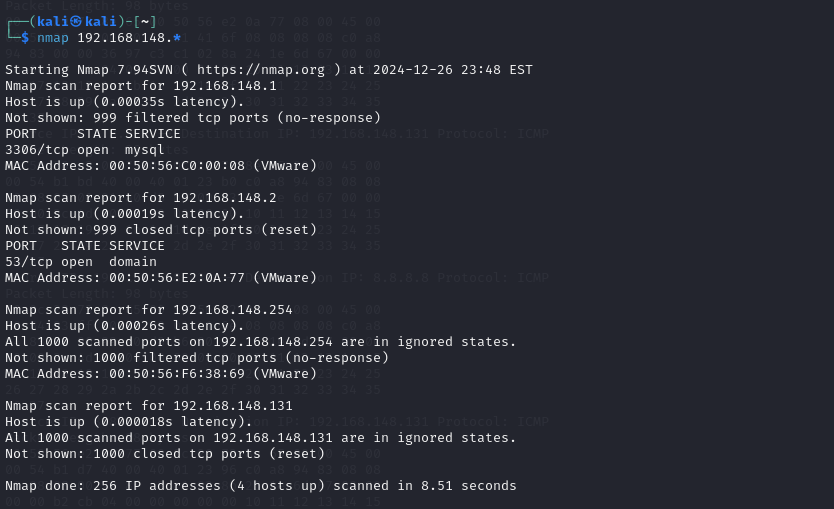
3.Scan Multiple Hosts

You can scan multiple hosts by simply writing their IP addresses or hostnames with Nmap.



4. Scan a whole Subnet

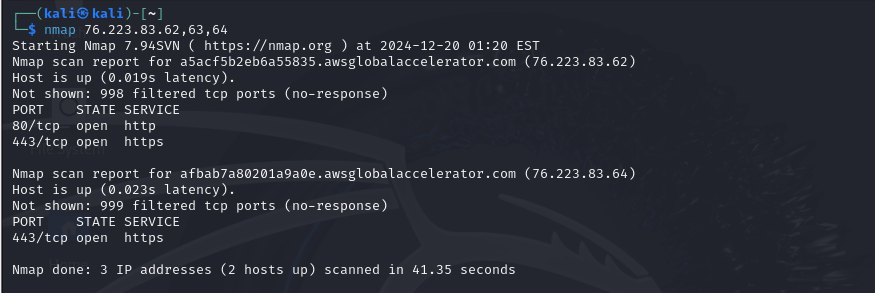
You can scan a whole subnet or IP range with Nmap by providing \* wildcard with it.



On above output you can see that nmap scanned a whole subnet and gave the information about those hosts which are Up in the Network.

5. Scan Multiple Servers using last octet of IP address

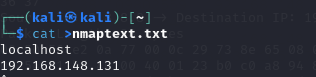
You can perform scans on multiple IP address by simple specifying last octet of IP address. For example, here I performing a scan on IP addresses 76.223.83.62 76.223.83.63 76.223.83.64.



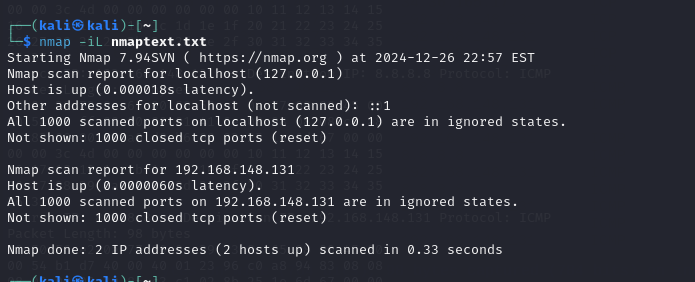
6. Scan list of Hosts from a File

If you have more hosts to scan and all host details are written in a file , you can directly ask nmap to read that file and perform scans. Let’s see how to do that.

Create a text file called “nmaptext.txt” and define all the IP addresses or hostname of the server that you want to do a scan.

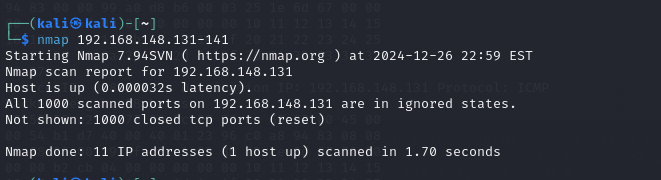


Next, run the following command with “iL” option with nmap command to scan all listed IP address in the file.



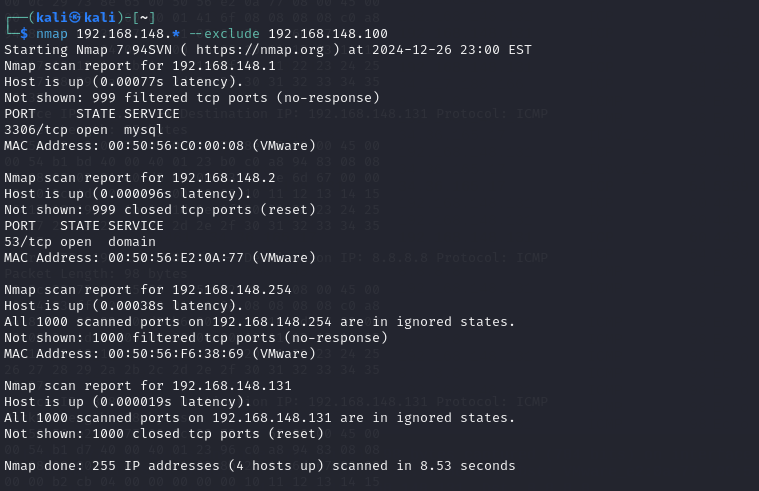
7. Scan an IP Address Range

You can specify an IP range while performing scan with Nmap.



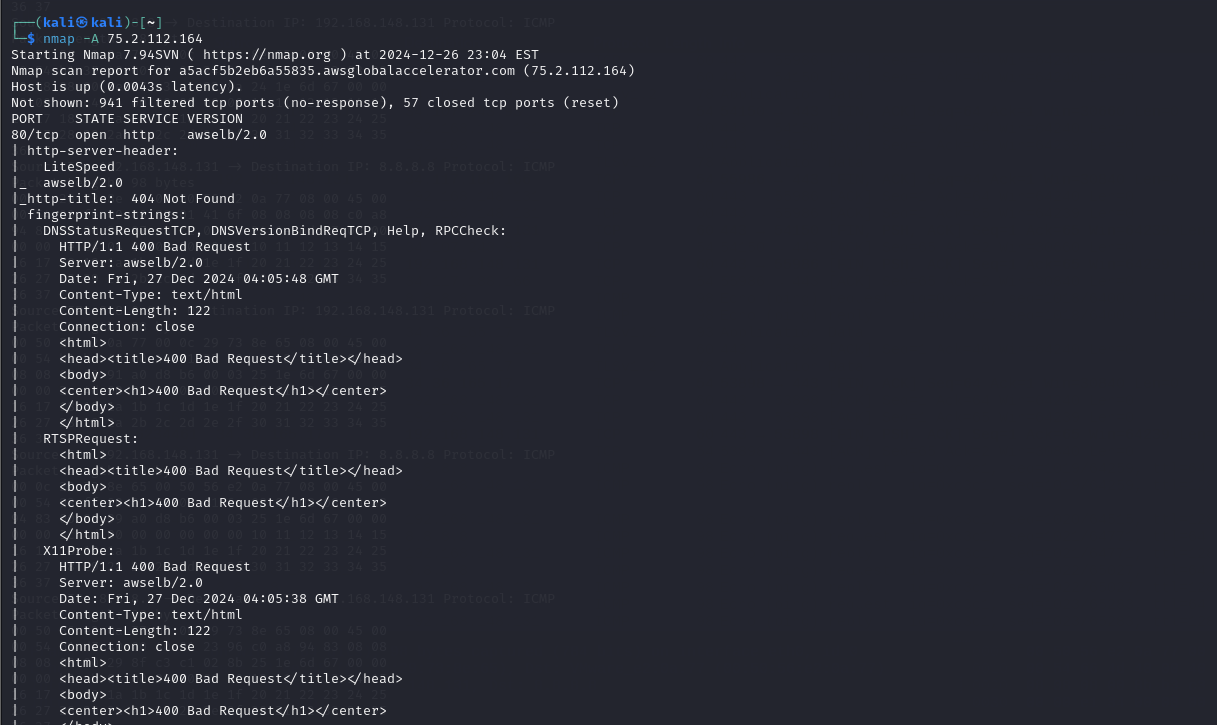
8. Scan Network Excluding Remote Hosts

You can exclude some hosts while performing a full network scan or when you are scanning with wildcards with “–exclude” option.



9. Scan OS information and Traceroute

With Nmap, you can detect which OS and version is running on the remote host. To enable OS & version detection, script scanning and traceroute, we can use “-A” option with NMAP.



In above Output, you can see that nmap is came up with TCP/IP fingerprint of the OS running on remote hosts and being more specific about the port and services running on the remote hosts.

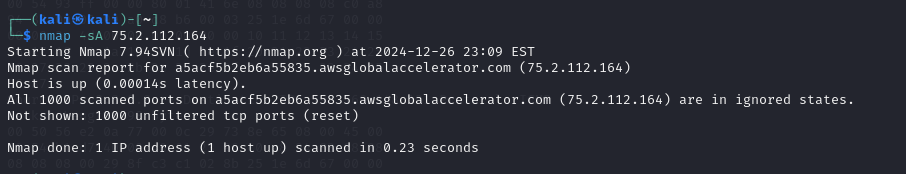
10. Enable OS Detection with Nmap

Use the option “-O” and “-osscan-guess” also helps to discover OS information.



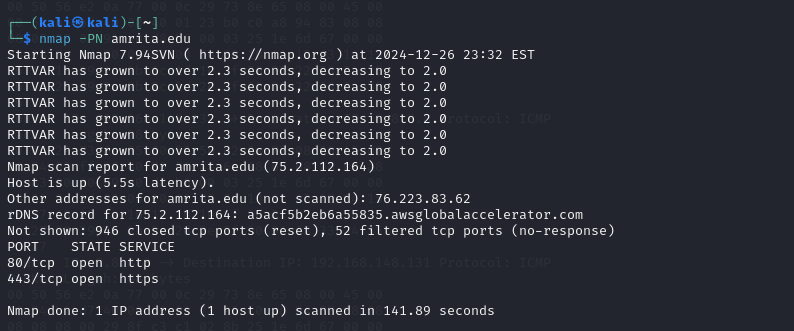
11. Scan a Host to Detect Firewall

The below command will perform a scan on a remote host to detect if any packet filters or Firewall is used by host.



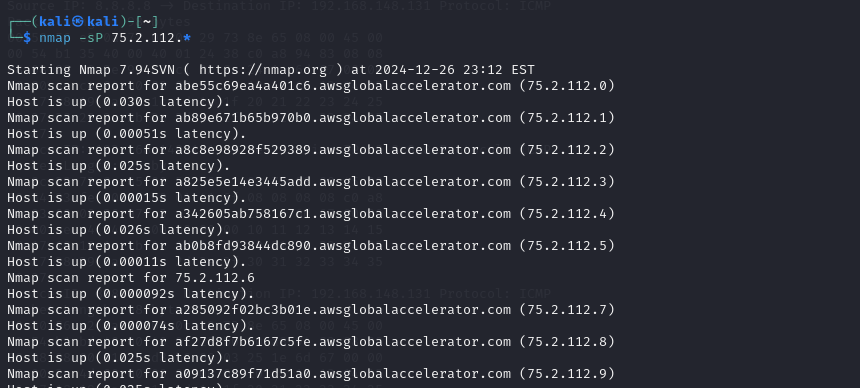
12. Scan a Host to check its protected by Firewall

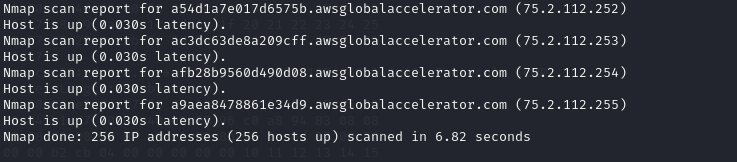
To scan a host if it is protected by any packet filtering software or Firewalls.



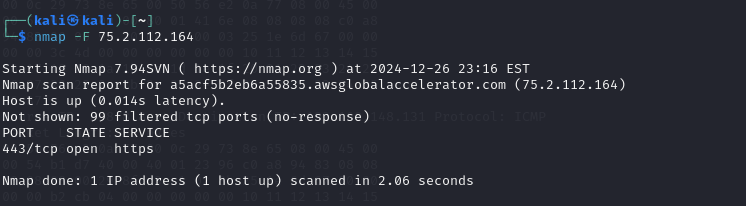
13. Find out Live hosts in a Network

With the help of “-sP” option we can simply check which hosts are live and up in Network, with this option nmap skips port detection and other things.



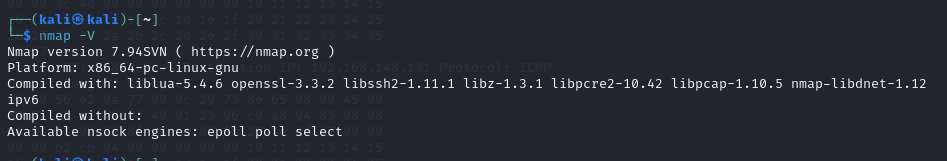


14. Perform a Fast Scan

You can perform a fast scan with “-F” option to scans for the ports listed in the nmap-services files and leaves all other ports. 

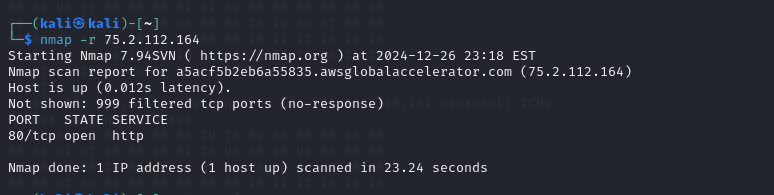
15. Find Nmap version

You can find out Nmap version you are running on your machine with “-V” option.



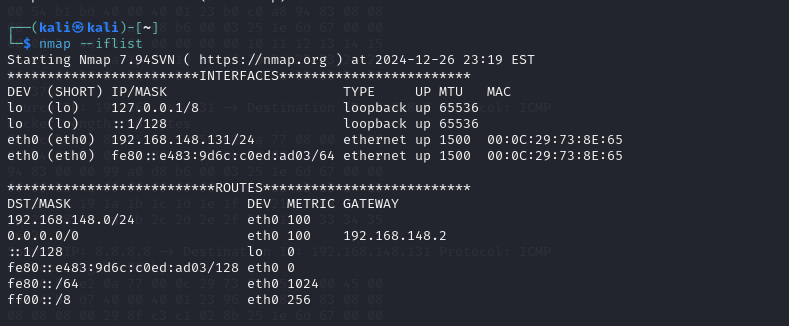
16. Scan Ports Consecutively

Use the “-r” flag to don’t randomize.



17. Print Host interfaces and Routes

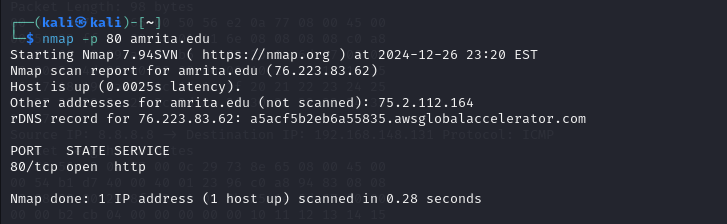
You can find out host interface and route information with nmap by using “–iflist” option.



In above output, you can see that map is listing interfaces attached to your system and their respective routes.

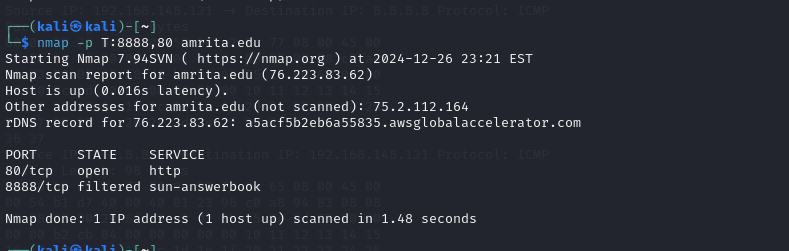
18. Scan for specific Port

There are various options to discover ports on remote machine with Nmap. You can specify the port you want nmap to scan with “-p” option, by default nmap scans only TCP ports.

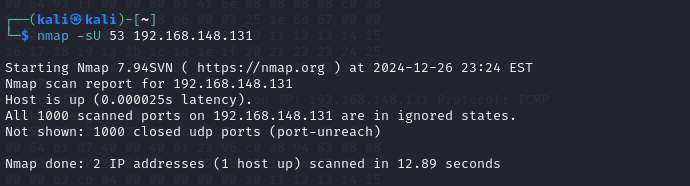


19. Scan a TCP Port

You can also specify specific port types and numbers with nmap to scan.

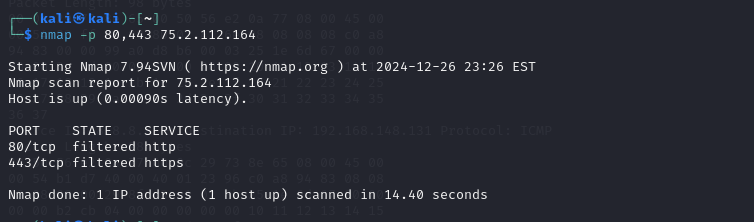


20. Scan a UDP Port



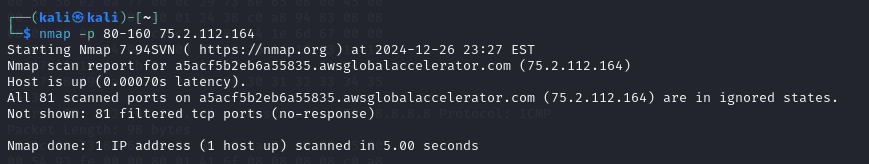
21. Scan Multiple Ports

You can also scan multiple ports using option “-p“.



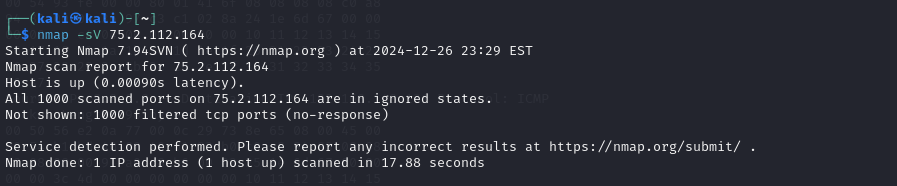
22. Scan Ports by Network Range

You can scan ports with ranges using expressions.



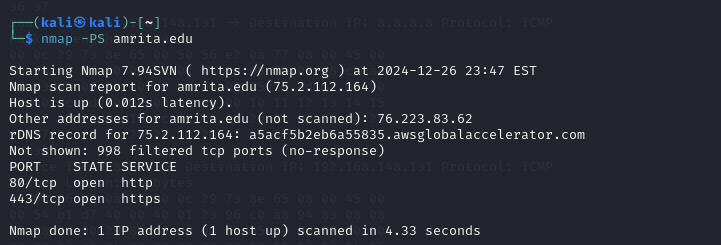
23. Find Host Services version Numbers

We can find out service’s versions which are running on remote hosts with “-sV” option.

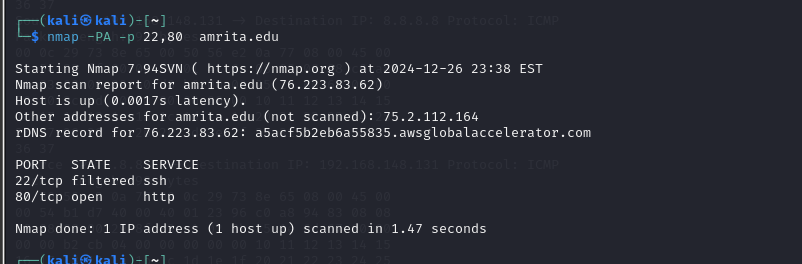


24. Scan remote hosts using TCP ACK (PA) and TCP Syn (PS)

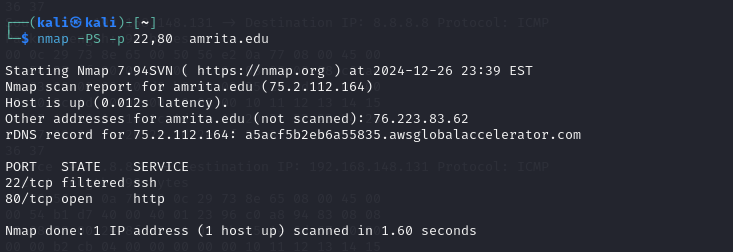
Sometimes packet filtering firewalls blocks standard ICMP ping requests, in that case, we can use TCP ACK and TCP Syn methods to scan remote hosts.



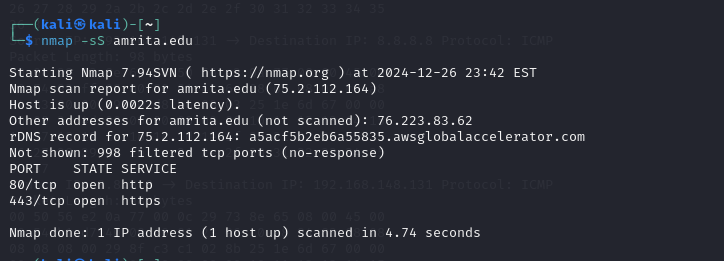
25. Scan Remote host for specific ports with TCP ACK



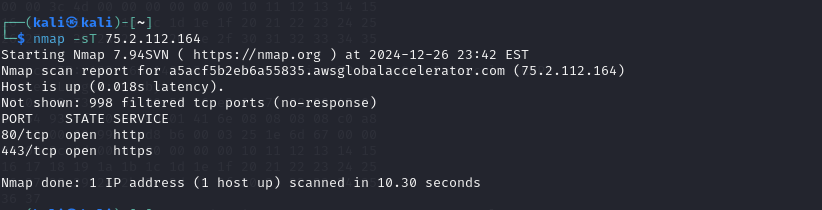
26. Scan Remote host for specific ports with TCP Syn



27. Perform a stealthy Scan



28. Check most commonly used Ports with TCP Syn



29. Perform a tcp null scan to fool a firewall

