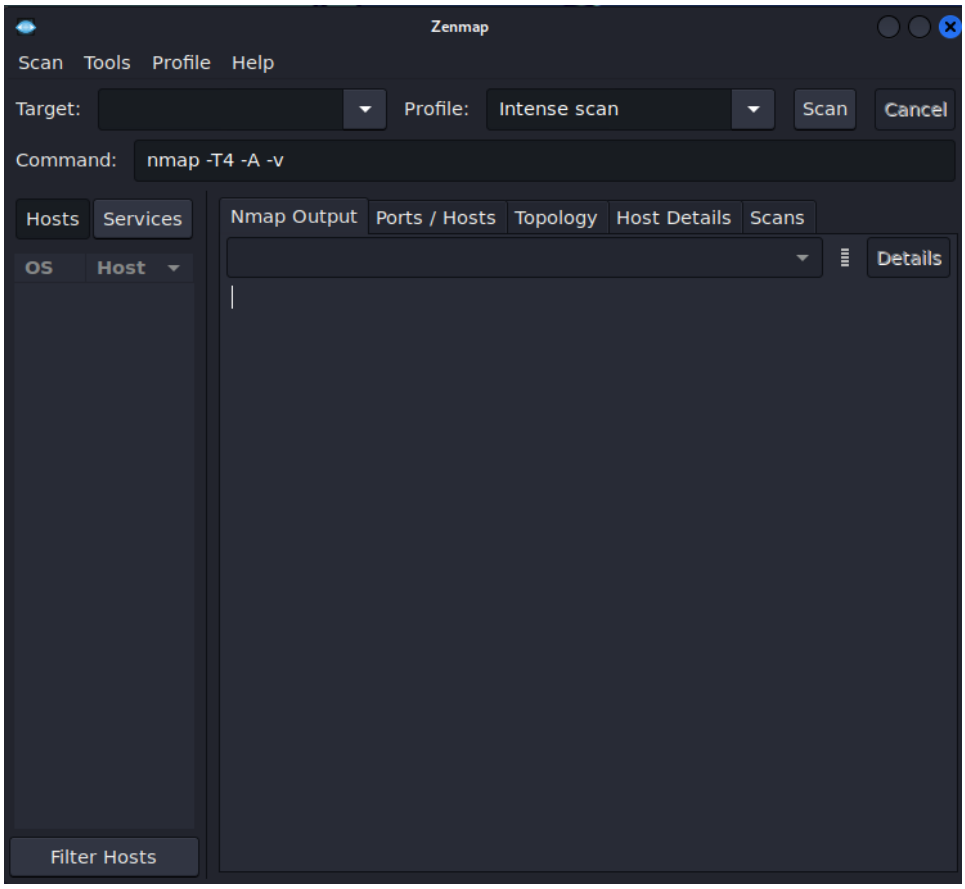
Computer Security

Lab 1 Demo: Zenmap

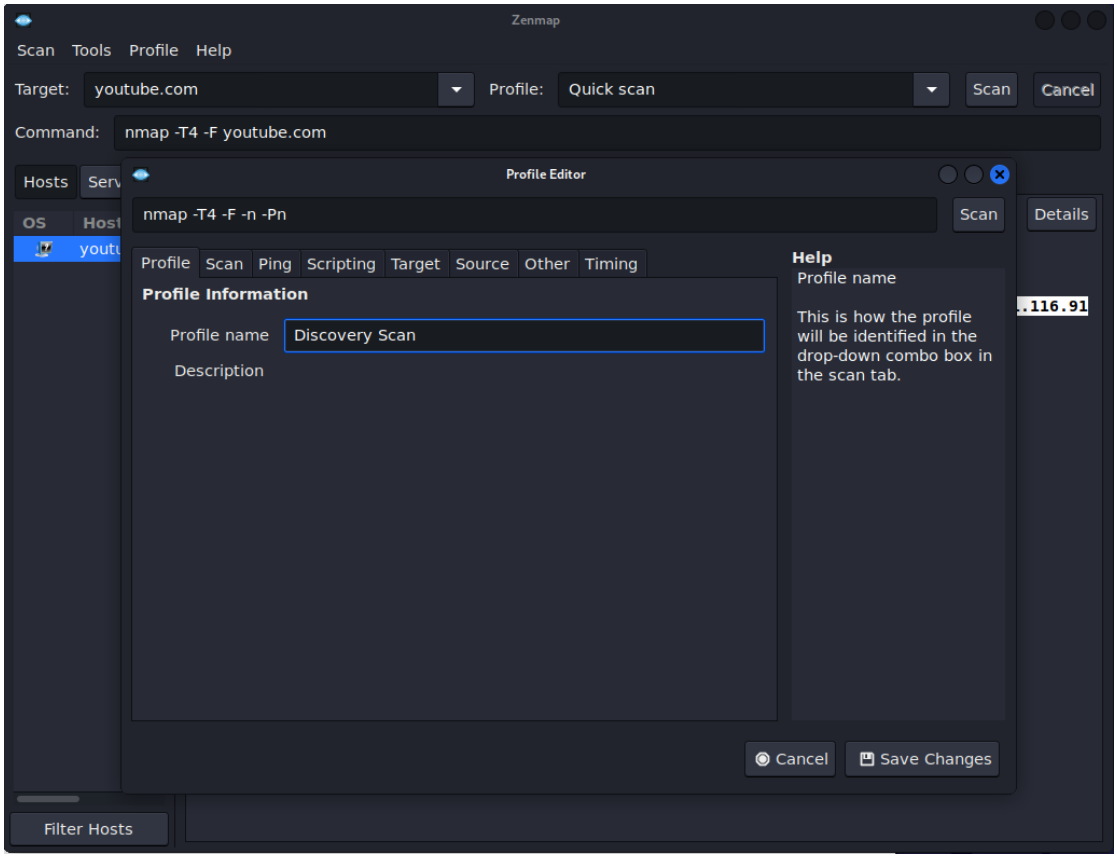
Stephanie Salgado

What is Zenmap and how is it used?

Zenmap is the GUI representation of nmap, a network mapper, and it utilizes console nmap commands. It can be launched in the terminal or by clicking on it in a desktop environment. Within Zenmap, you can select a target and profile (intense scan, quick scan, ping scan, etc.), which will also display the nmap command that would perform the same action. Alternatively, you can enter a personalized command.

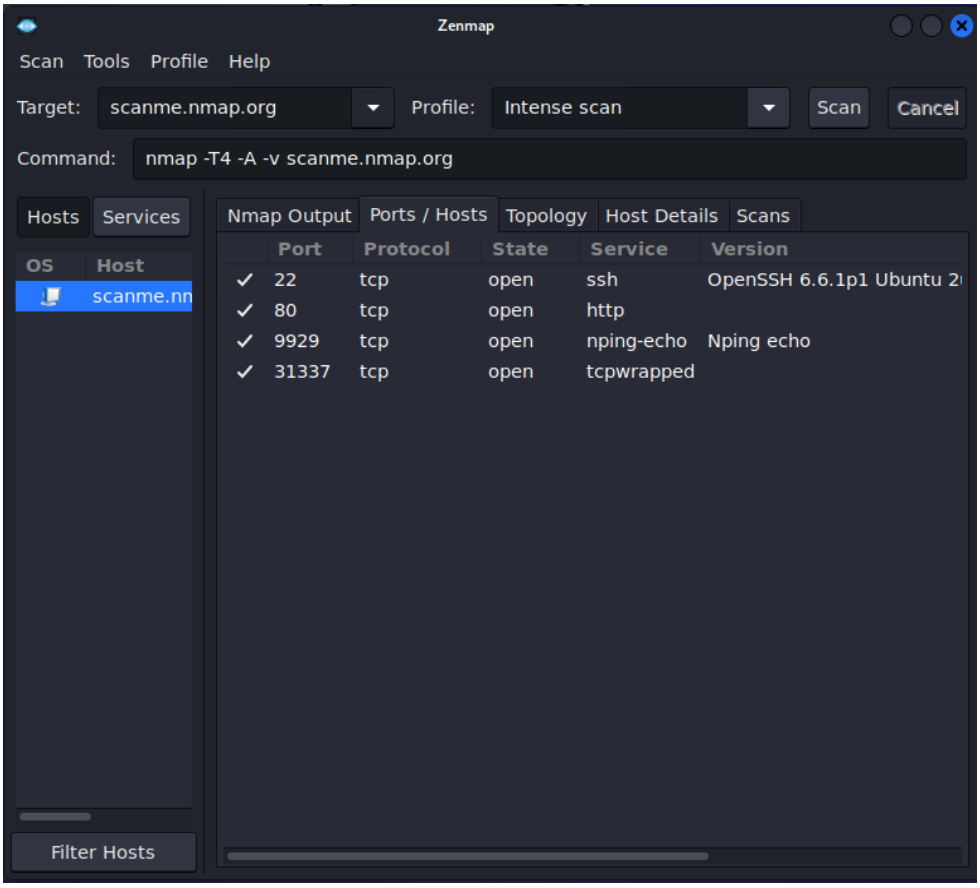


Zenmap allows you to create a new profile and add or edit commands through its “Profile Editor” accessed from the “Profile” tab; these changes are then reflected when selecting a profile. The Profile Editor allows for more customization under its tabs.

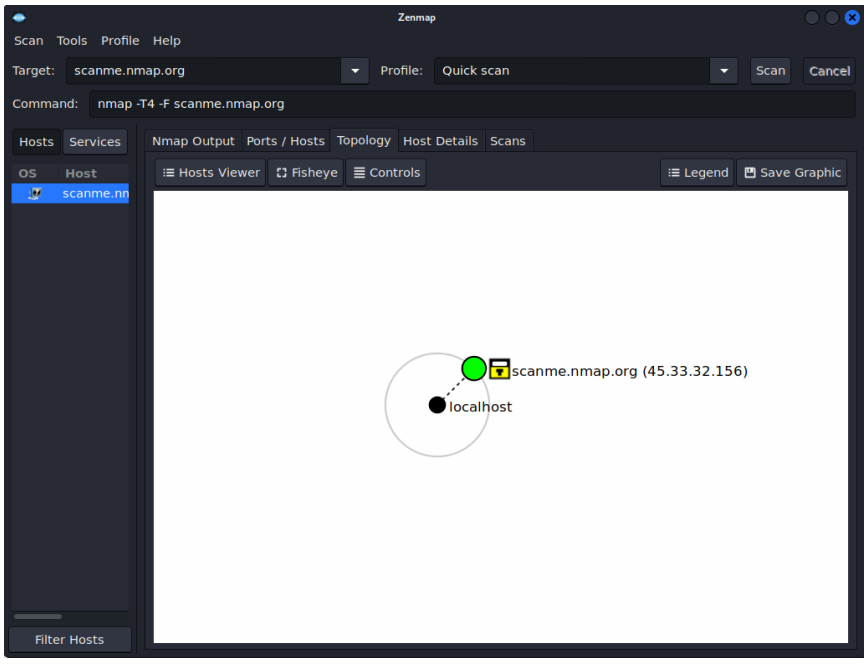


Through Zenmap, you can combine results of many scans through a feature called “scan aggregation”. The collection of these scans in an aggregated view is called a “network inventory”.

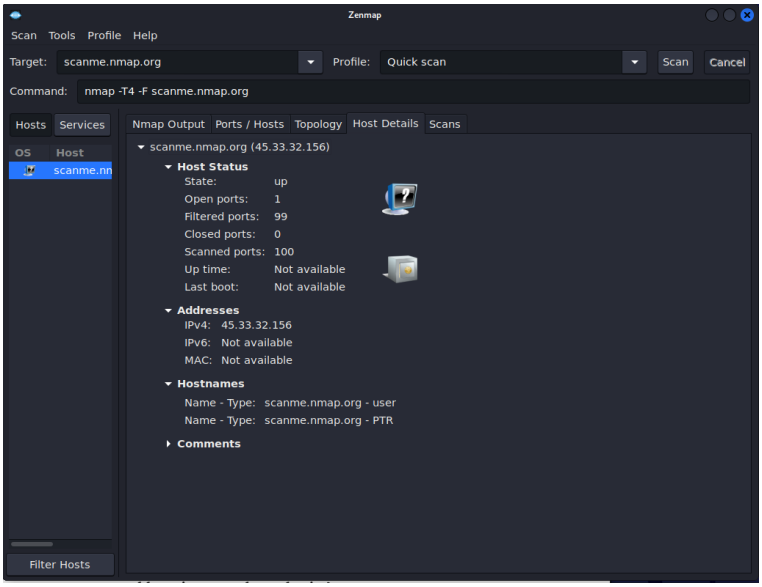
After running a scan/scans, the results are displayed in tabs which can be more intuitive and easier to understand than the nmap terminal output. By default, the selected tab is “Nmap Output” which resembles the terminal output, but the other tabs can be used to find specific information. Under the “Ports/Hosts” you can view all interesting ports and version information if available when a host is selected.



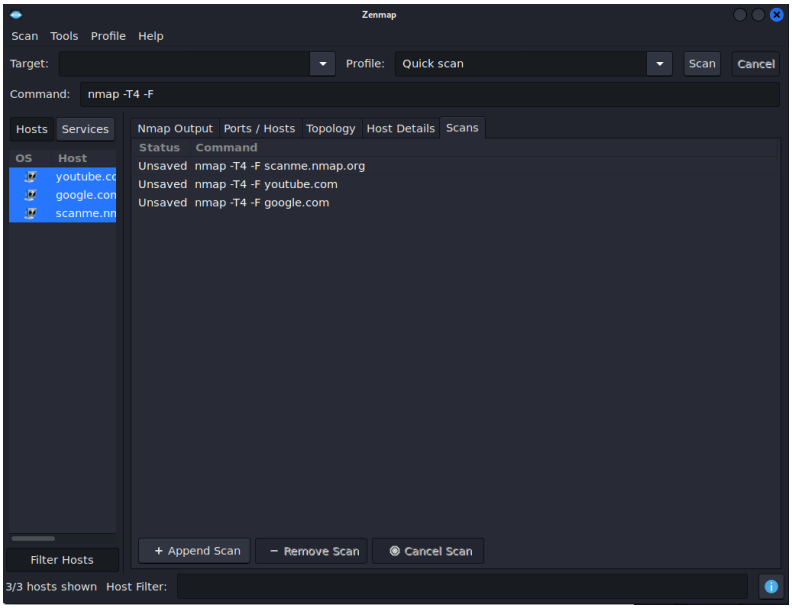
The “Topology” tab provides an interactive view of connections between hosts in a network.



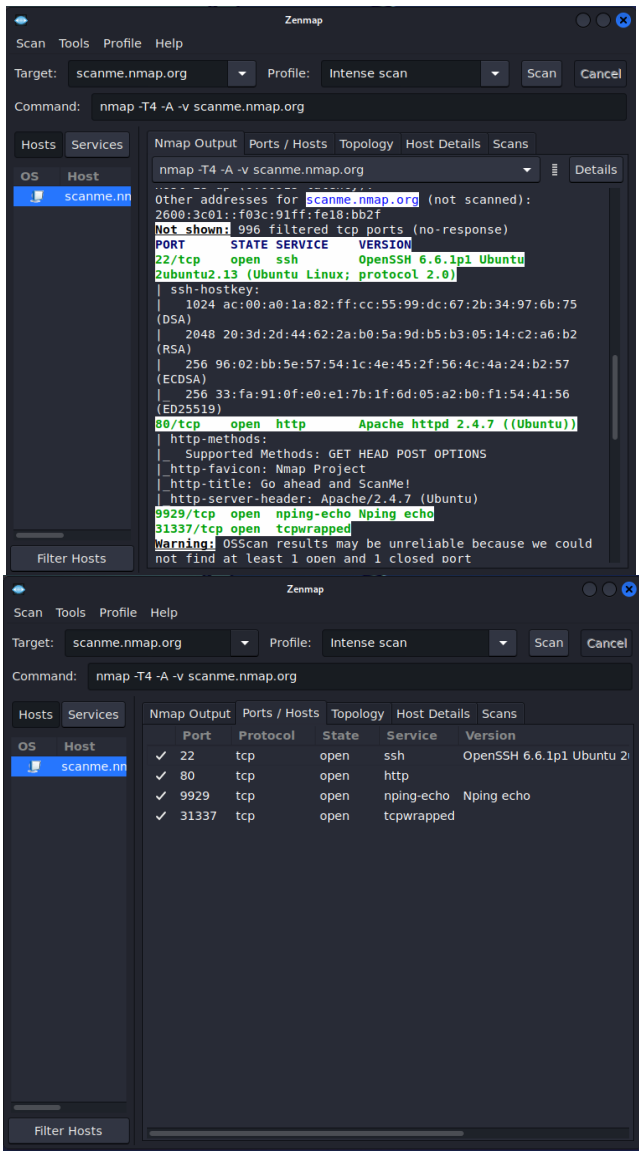
The “Host Details” tab breaks all the information about a host into a hierarchical display. The host's names and addresses, its state, and the number and status of scanned ports are displayed. When available, the host's uptime, operating system, OS icon and other associated details are shown; the closest matches are displayed when the exact OS match is not found.



The “Scans” tab displays all the aggregated scans that make up the network inventory and you can also add or remove scans.

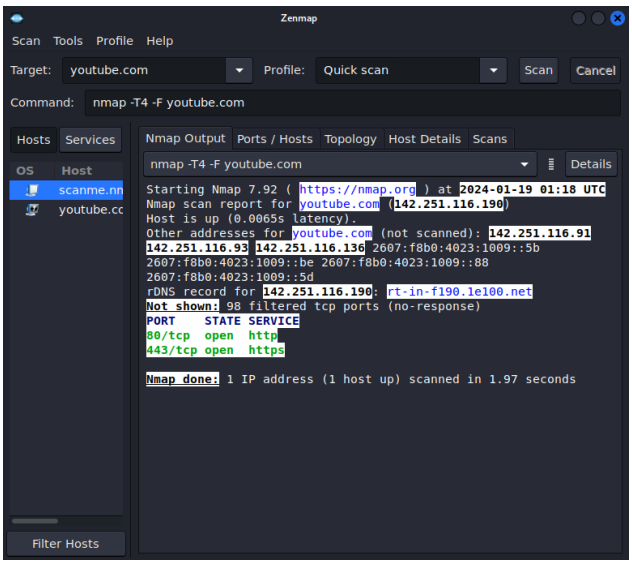


Target 1: scanme.nmap.org (Intense Scan)

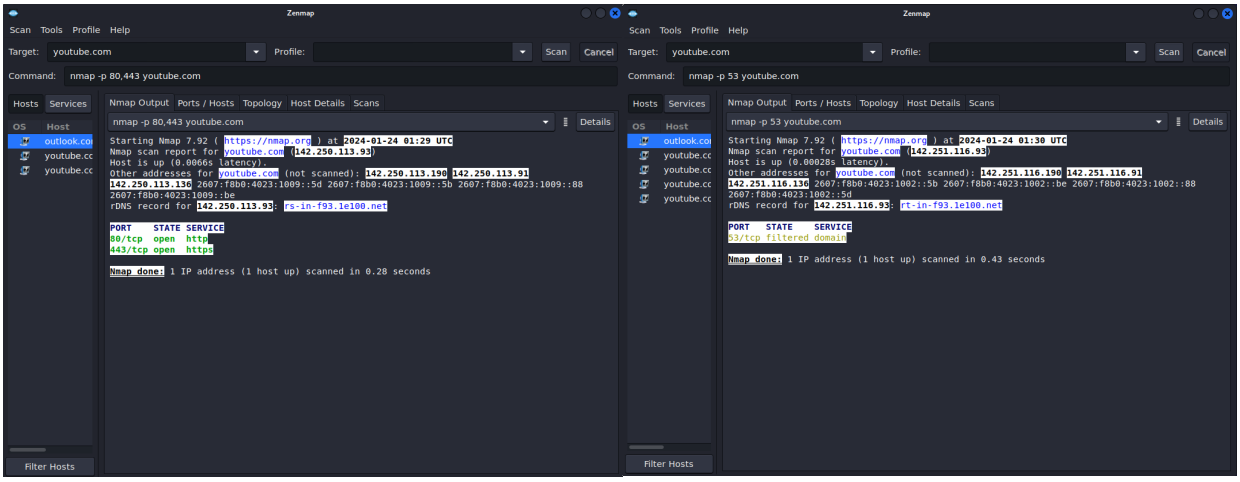


The nmap command used for an intense scan is “nmap -T4 -A -v” followed by the target host. The “-T4 '' in this command sets a timing template from 0-5, higher means faster, speeding up the scan which can be useful when providing Zenmap with a custom command. The “-A” (aggressive option) enables OS detection, version detection, script scanning, and traceroute, while “-v” increases verbosity, not to be confused with “-V” which gets the version. In this case, the host was “scanme.nmap.org”. The intense scan yielded 4 ports, their state, service and version. For example, Port 22 is tcp, open.

Target 2: youtube.com (Quick Scan)

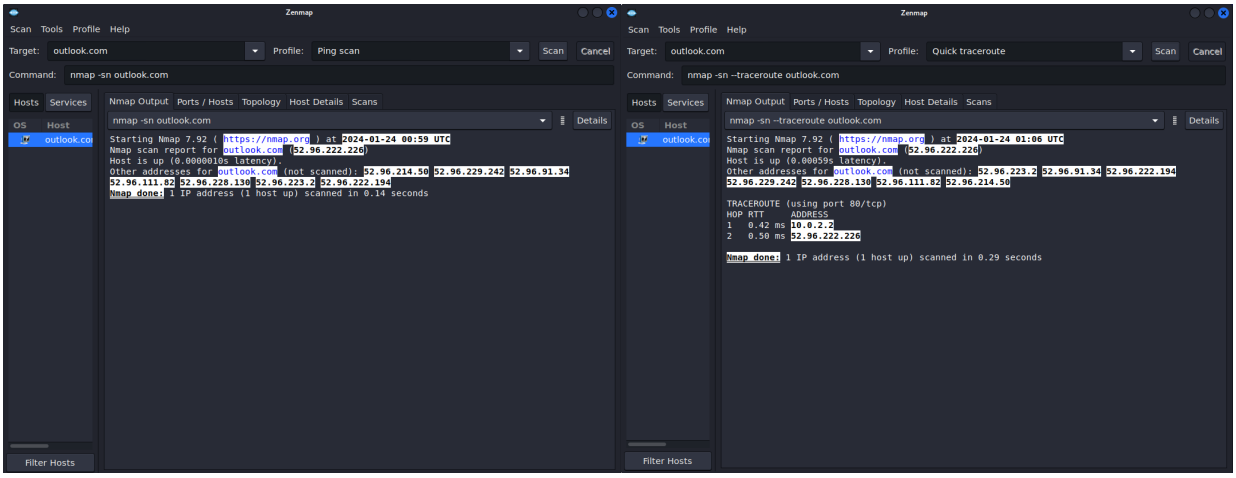


The command used for a quick scan is “nmap -T4 -F” followed by the host. In this case, the “-F” signifies a fast mode that scans for fewer ports. Quick scan on youtube yielded 2 ports. Port 80 is tcp, open and http, as is default to enable internet connection (unencrypted). Port 443 is tcp, open and https (encrypted web traffic). Nmap also allows you to scan for a specific port/ports by using “-p” followed by the port/ports you wish to find.

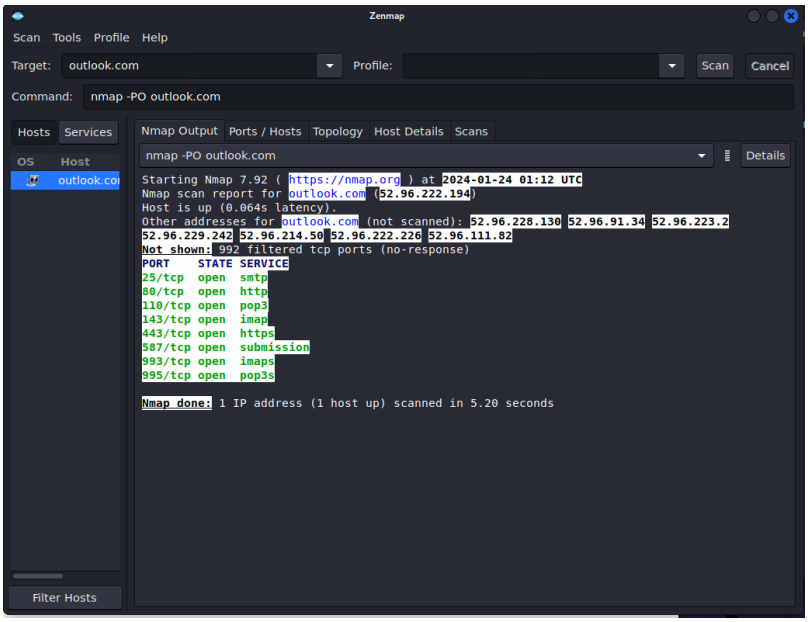


After scanning for port 53 nmap’s response for the port’s state was “filtered” which means it can not determine whether the port is open because packet filtering prevents its probes from reaching the port.

Target 3: outlook.com (Ping Scan & Quick Traceroute)

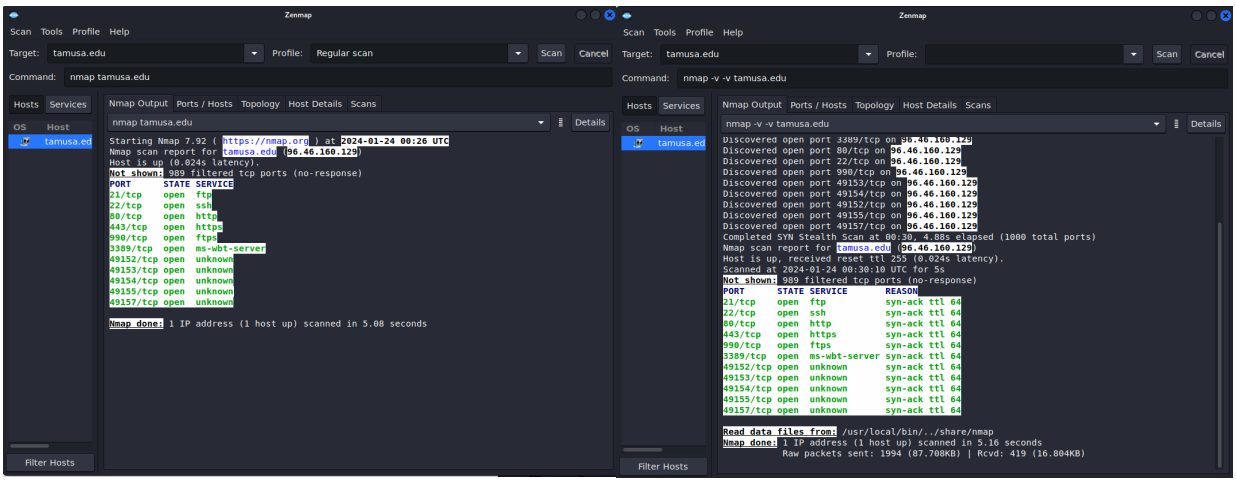


A ping scan is done with command "nmap -sn" followed by the target. "-sn" specifies a ping scan and disables port scan. Similarly a quick traceroute uses "-sn" to disable port scan and "--traceroute" to trace hop path to each host.

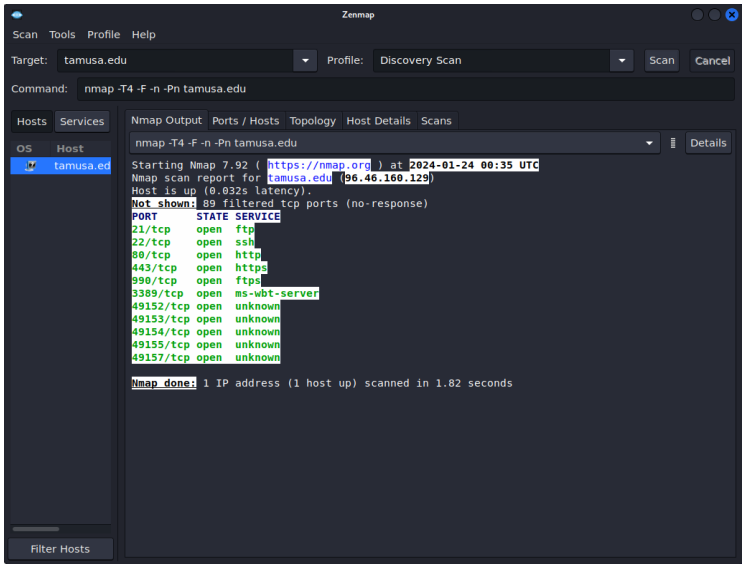


Using "-PO" does an IP protocol ping, a form of host discovery, that sends IP packets looking for either responses using the same protocol as a probe, or ICMP protocol unreachable messages which signify that the given protocol isn't supported by the destination host. Receiving either message can be used to determine if the target host is alive.

Target 4: tamusa.edu (Regular Scan & “Discovery Scan”)



Notice a regular scan is done with the simple command “nmap” followed by the target. If you’d like even more verbosity adding “-vv” would generate more as shown above. Target “tamusa.edu” has 11 open ports, of which those starting in “49” have an unknown service.



Running a custom command “nmap -T4 -F -n -Pn” which I’ve saved as “Discovery Scan '' provides the same information on the target as the “Regular Scan” while taking 4 seconds less. The “-n” in the custom command tells nmap to **never** do reverse DNS resolution on

active IP addresses found. Inversely, “-R” would tell nmap to **always** do reverse DNS resolution on target IP addresses. “-Pn” skips host discovery by treating all hosts as online.