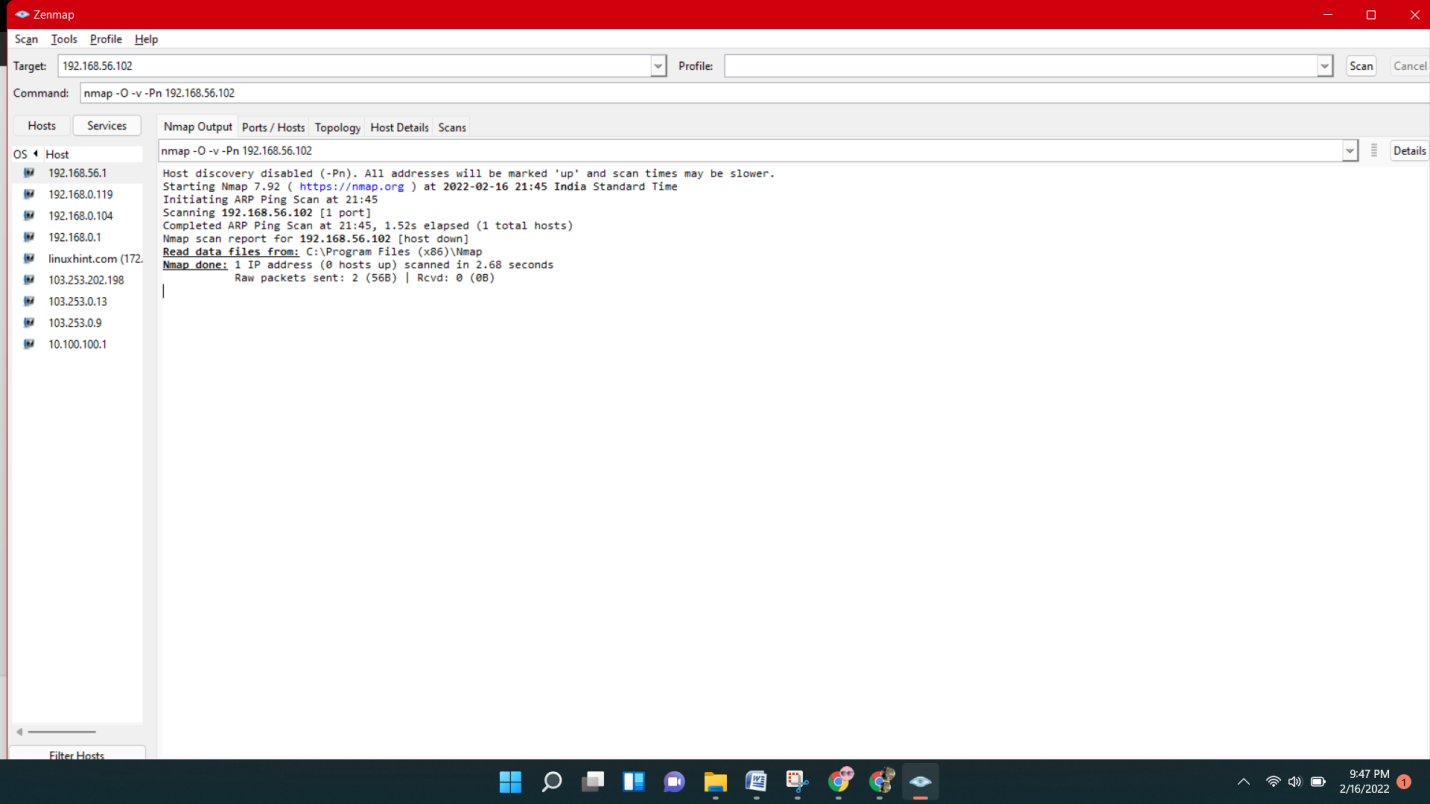
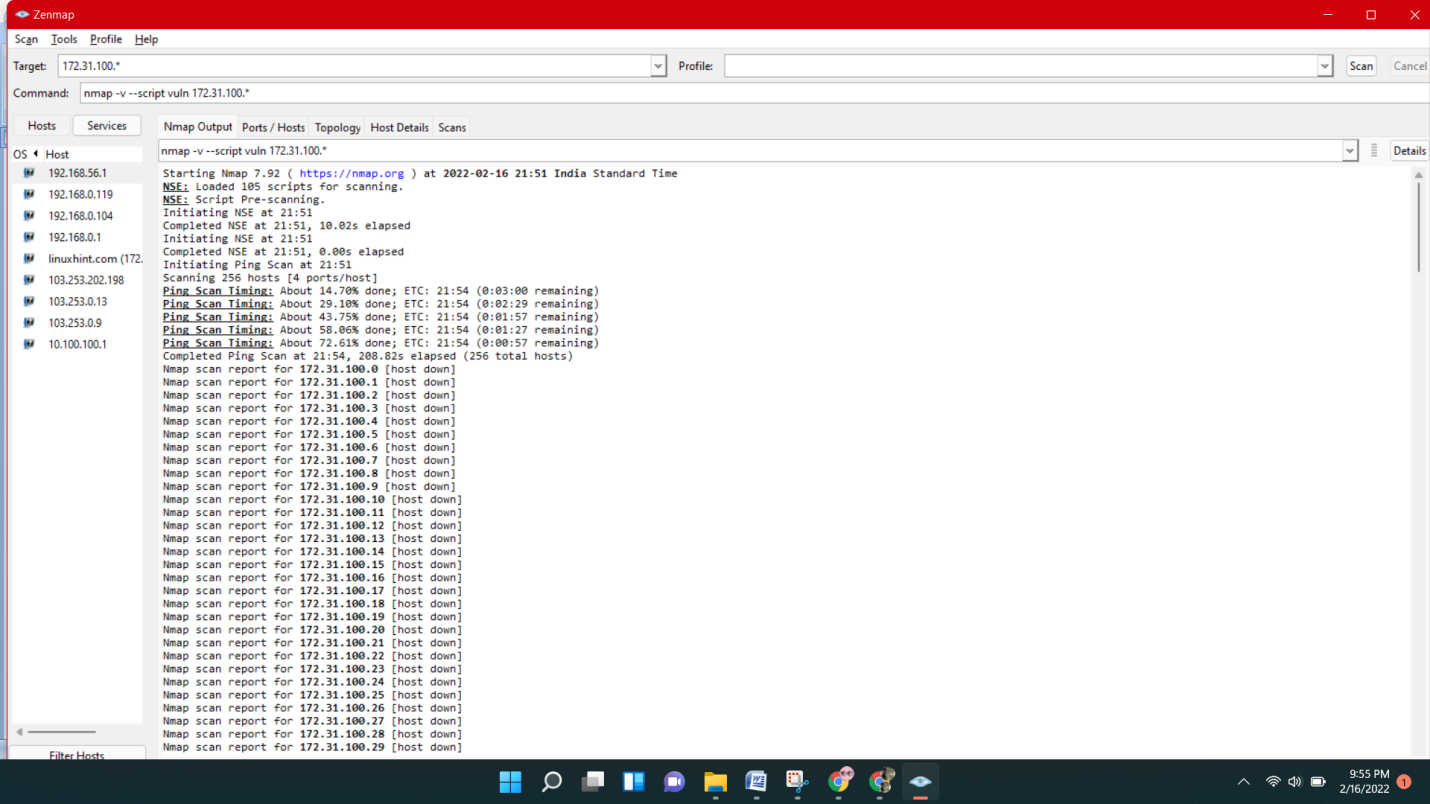
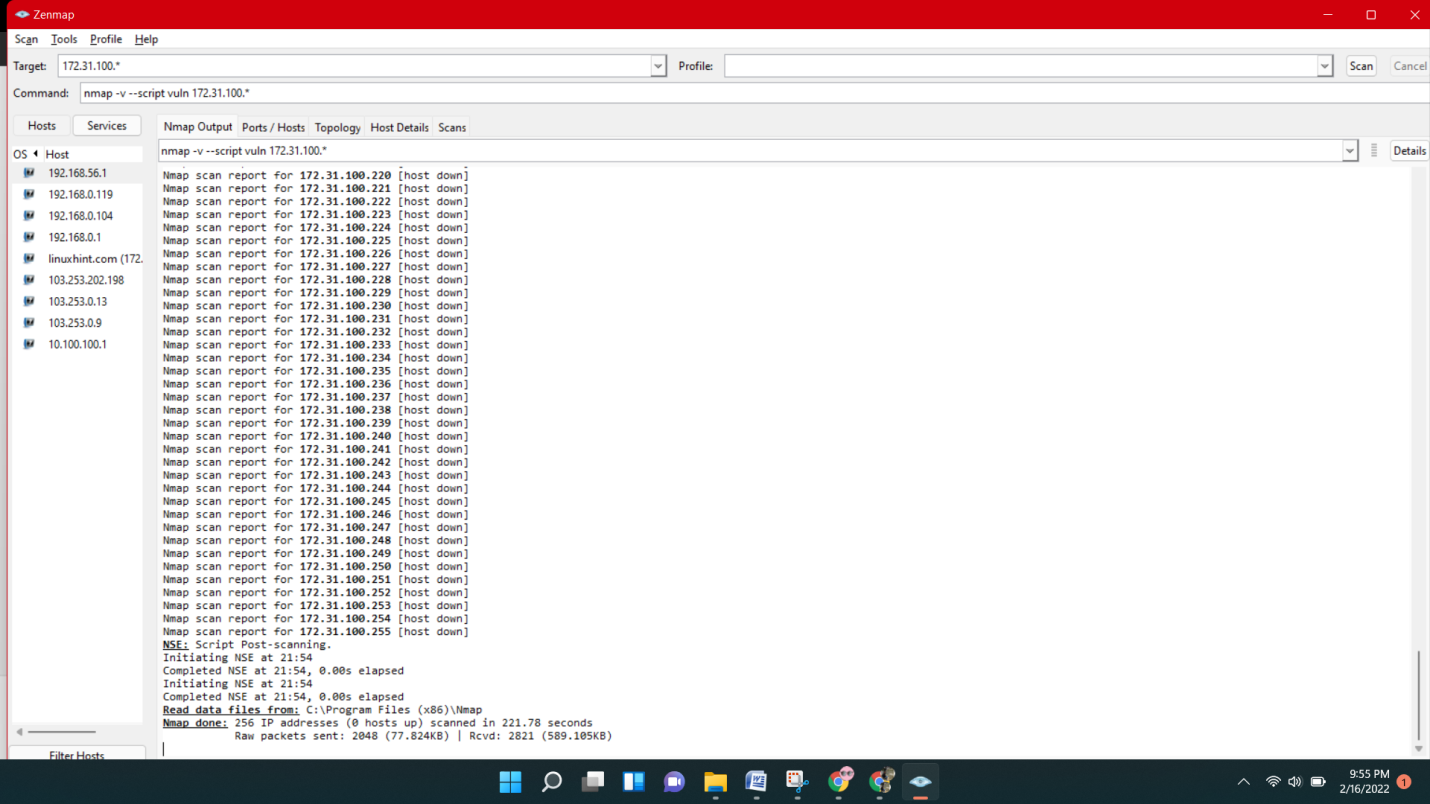
1. Another way to find potential zombie candidates for Idle scans:



## Scanning Ranges for Vulnerabilities

The following example shows the wildcard implementation to scan a whole octet’s range

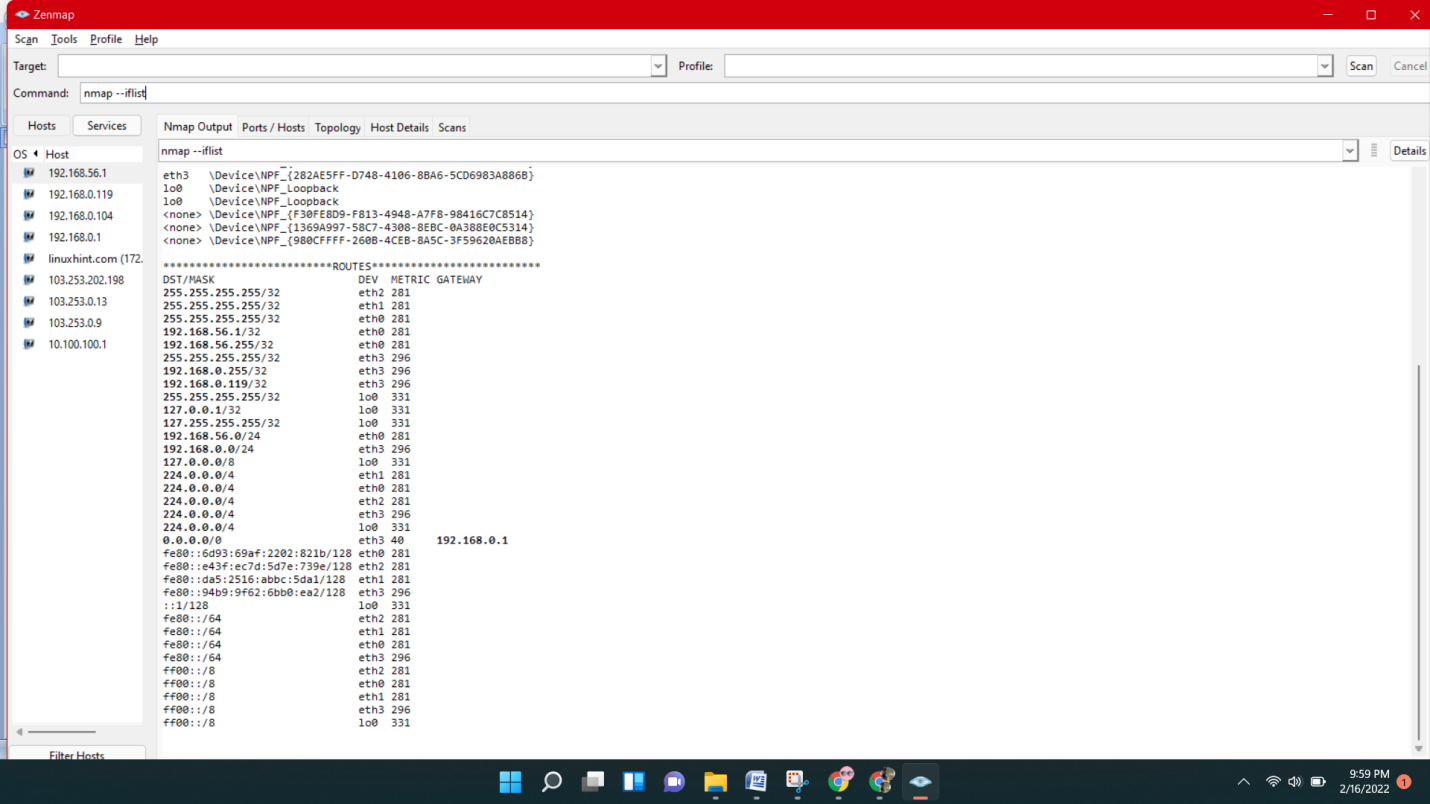




## Show host interfaces and routes

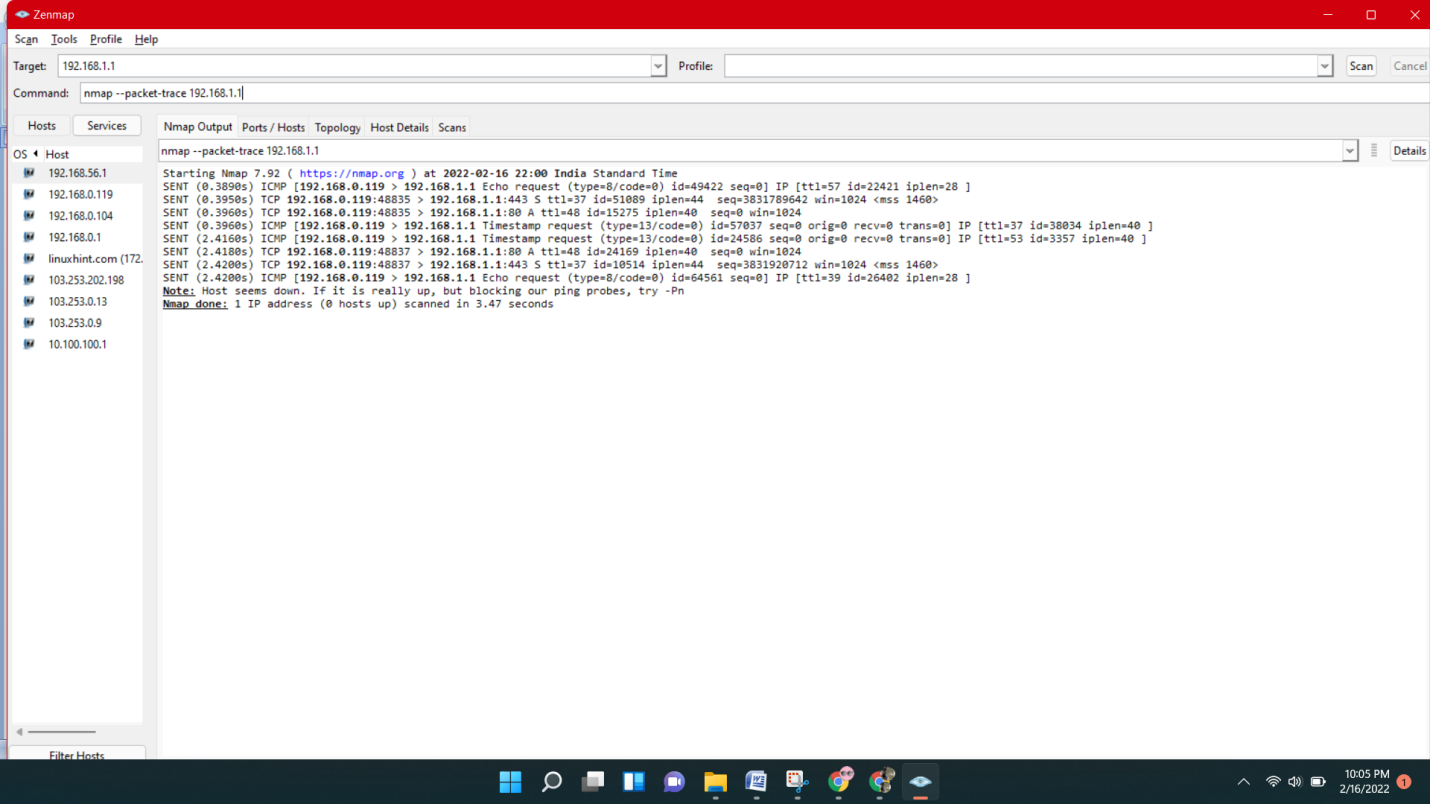
This is useful for debugging ([ip command](https://www.cyberciti.biz/faq/howto-linux-configuring-default-route-with-ipcommand/) or [route command](https://www.cyberciti.biz/faq/what-is-a-routing-table/) or [netstat command](https://www.cyberciti.biz/faq/linux-unix-open-ports/) like output using the nmap command on Linux)

nmap --iflist



## Show all packets sent and received

nmap --packet-trace 192.168.1.1



## detect remote operating system with the help of nmap

## 

## 

## Scan for IP protocol

This type of scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines:

nmap -sO 192.168.1.1

