Dom Moore
Zenmap

Overview

The network mapping tool Nmap is an open-source utility commonly used in network discovery (“enumeration” inoffensive terms) and security auditing.

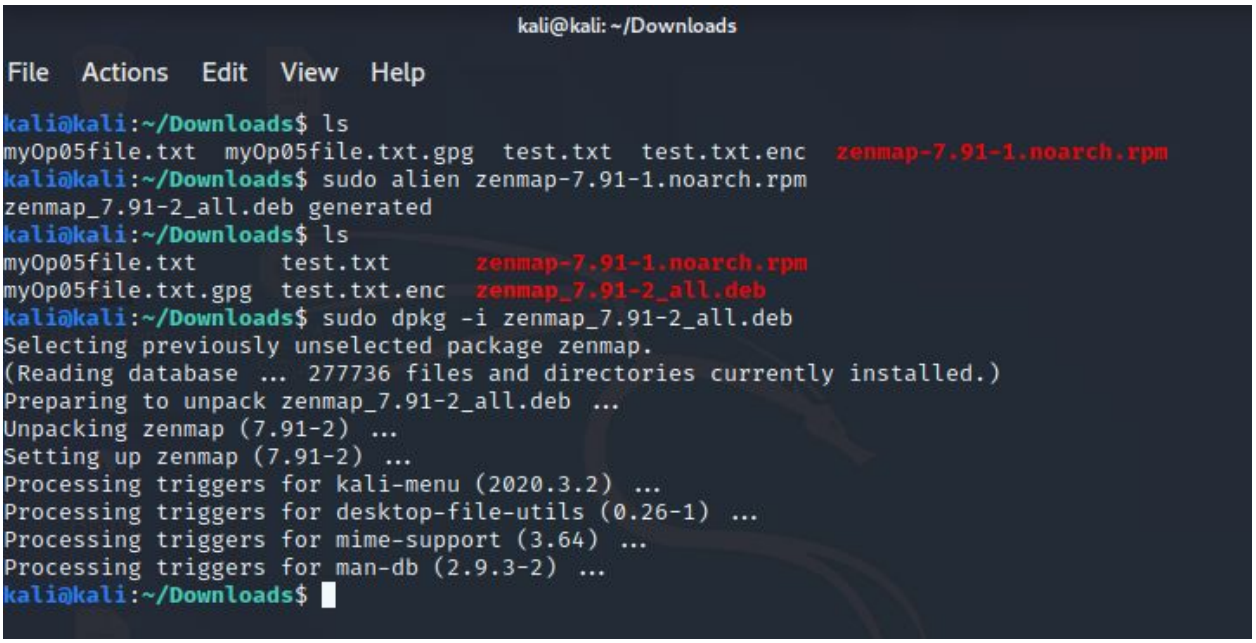
Part 1: Staging Zenmap

Step 1- download Optional Zenmap GUI (all platforms): zenmap-7.91-1.noarch.rpm

Step 2- run these commands:

- apt-get update apt-get install alien
- Go to your downloads folder cd Downloads
- sudo alien "name of the downloaded package.rpm"
- sudo dpkg -i "name of a converted package.deb"

Install Zenmap

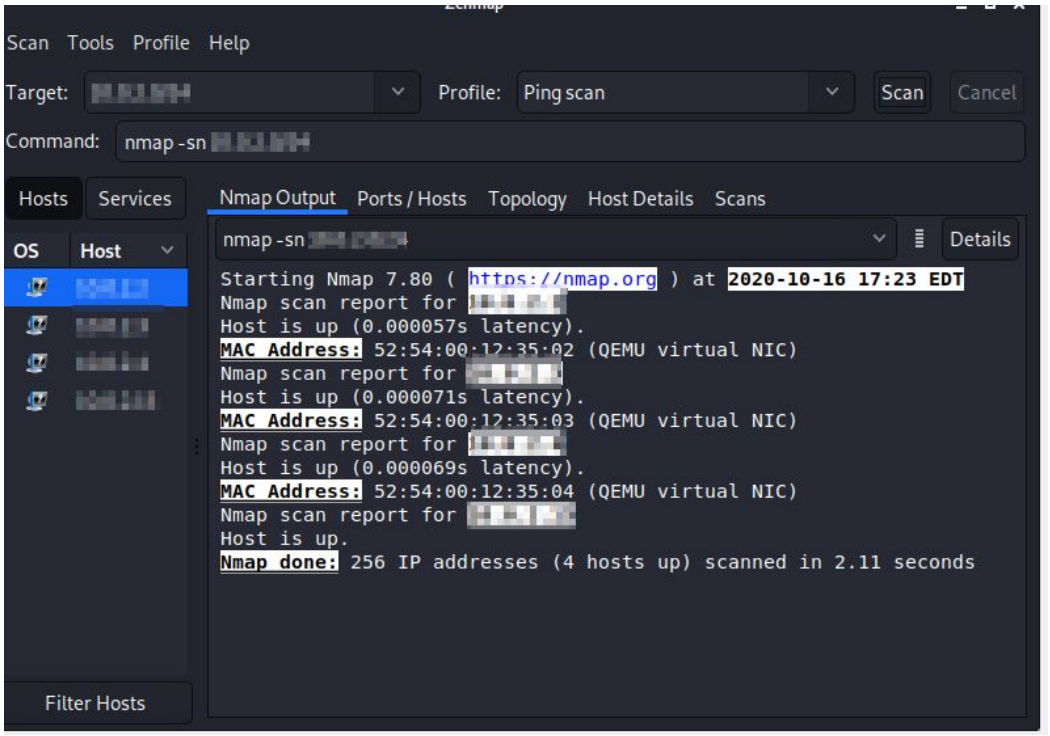


Part 2: Network Scanning with Zenmap

For each of the scans requested below:

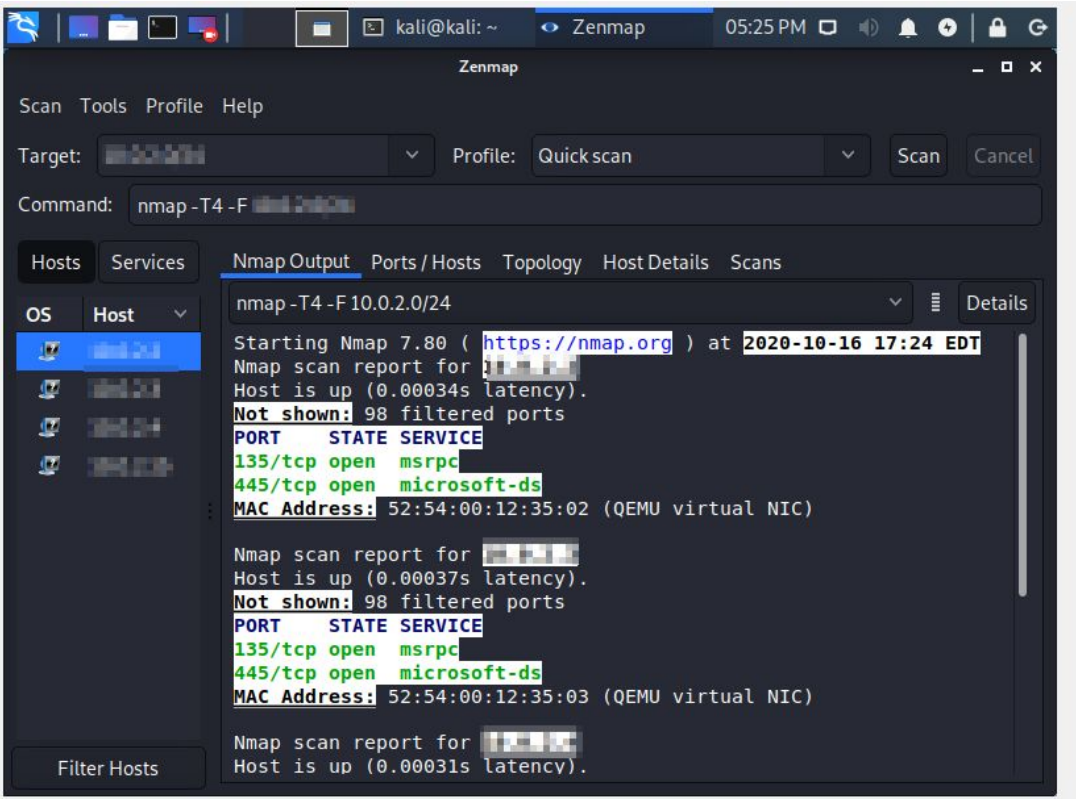
- Ping scan: **Command: nmap -sn**
    - What does this scan do in technical terms?
        - This command executes a ping scan on the target IP only but does not perform a port scan.
    - Was the scan correct?
        - The scan performed did execute as expected; it detected the four devices within the network and determined if the network was up or down.
    - Why/why not?
        - Yes, it identified that there are four devices it provided validation of those VM, it also shows that it scanned the other IP addresses within the range.

Ping scan



- Quick scan: **nmap -T4 -F**
    - What does this scan do in technical terms?
        - Scans the top 100 most common TCP ports
    - Was the scan correct?
        - Yes
    - Why/why not?
        - The Quick scan displays that there are 98 ports that are not shown, and displays the two TCP that it was able to pick up within the network.

Quick scan

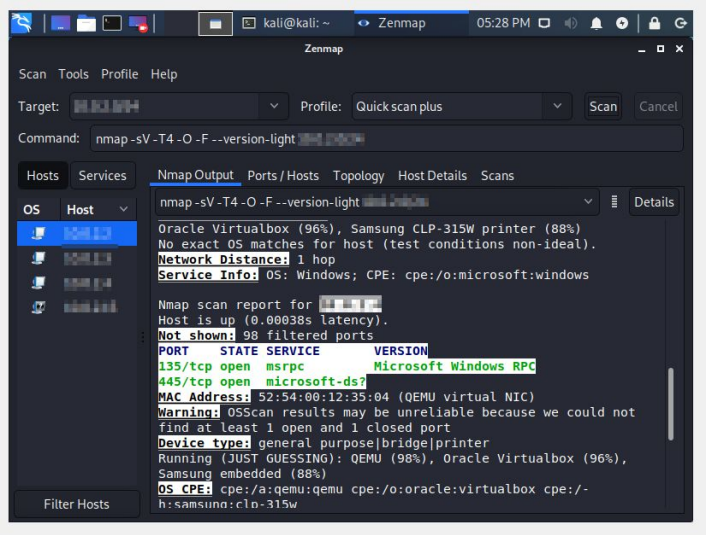


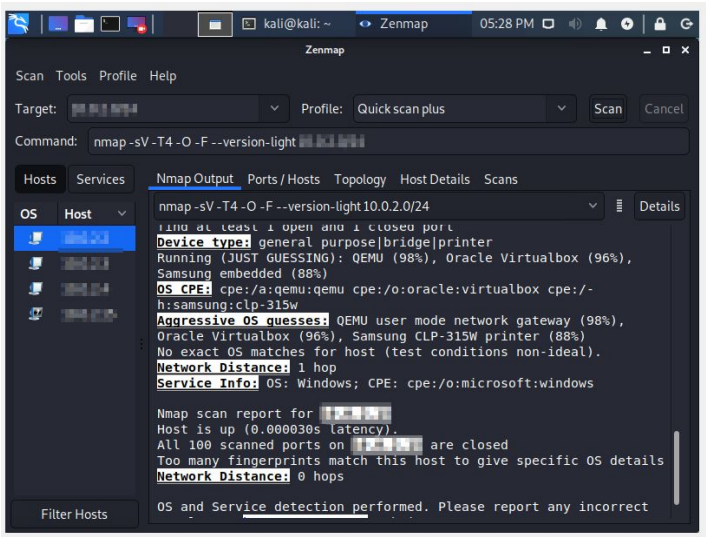
Port 143: Internet Msg Access Protocol is an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection

Port 445: TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer and Leaving port 445 open leaves Windows machines vulnerable to a number of trojans and worms.

- Quick scan plus: **Nmap -sV -T4 -O -F –version-light**
    - What does this scan do in technical terms?
        - The plus version of the QS is that it adds the os information to the results.
    - Was the scan correct?
        - Yes
    - Why/why not?
        - This scan performed the scans on the 100 ports included that os as well more details about the system such as the origin of the VM's

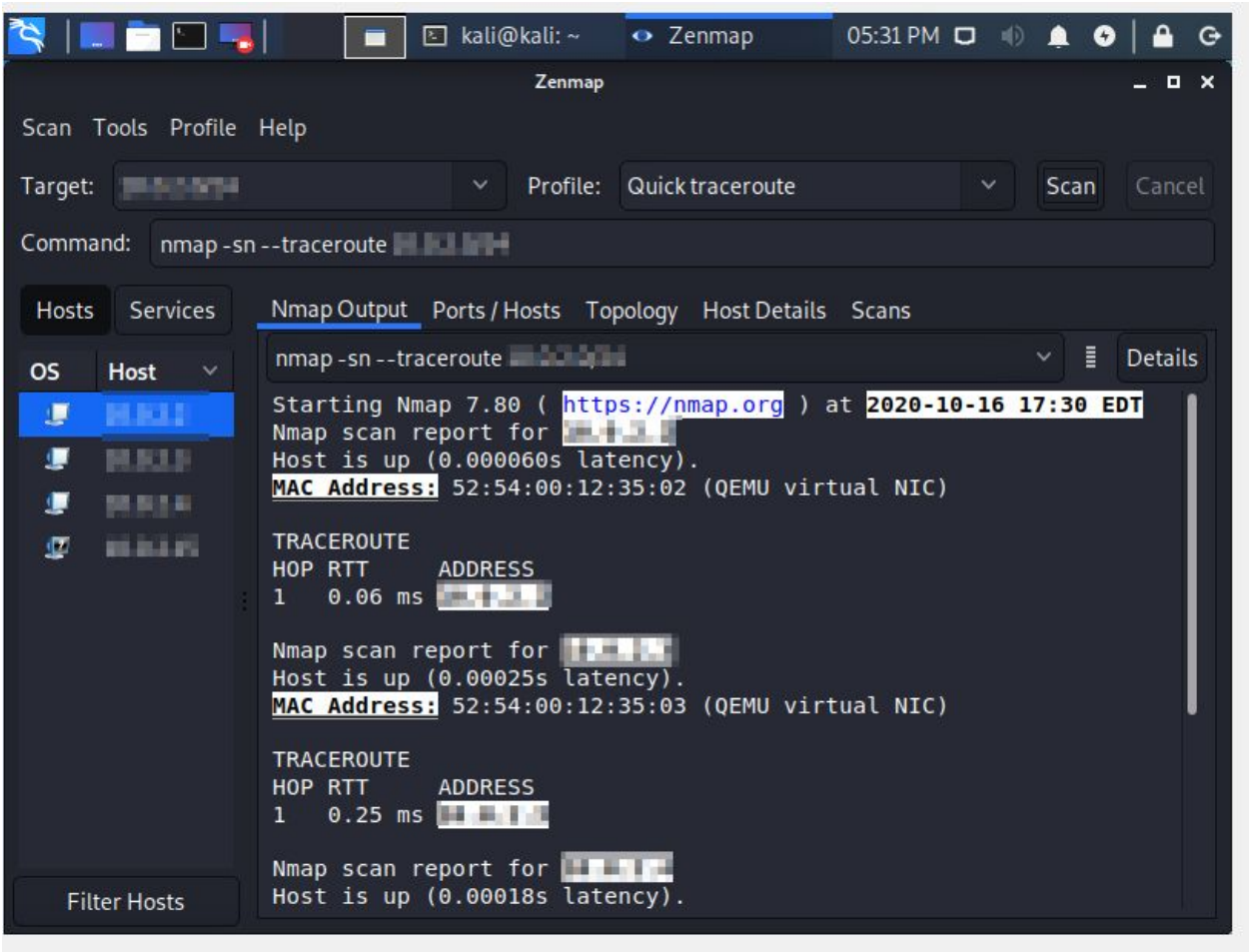
Quick scan plus





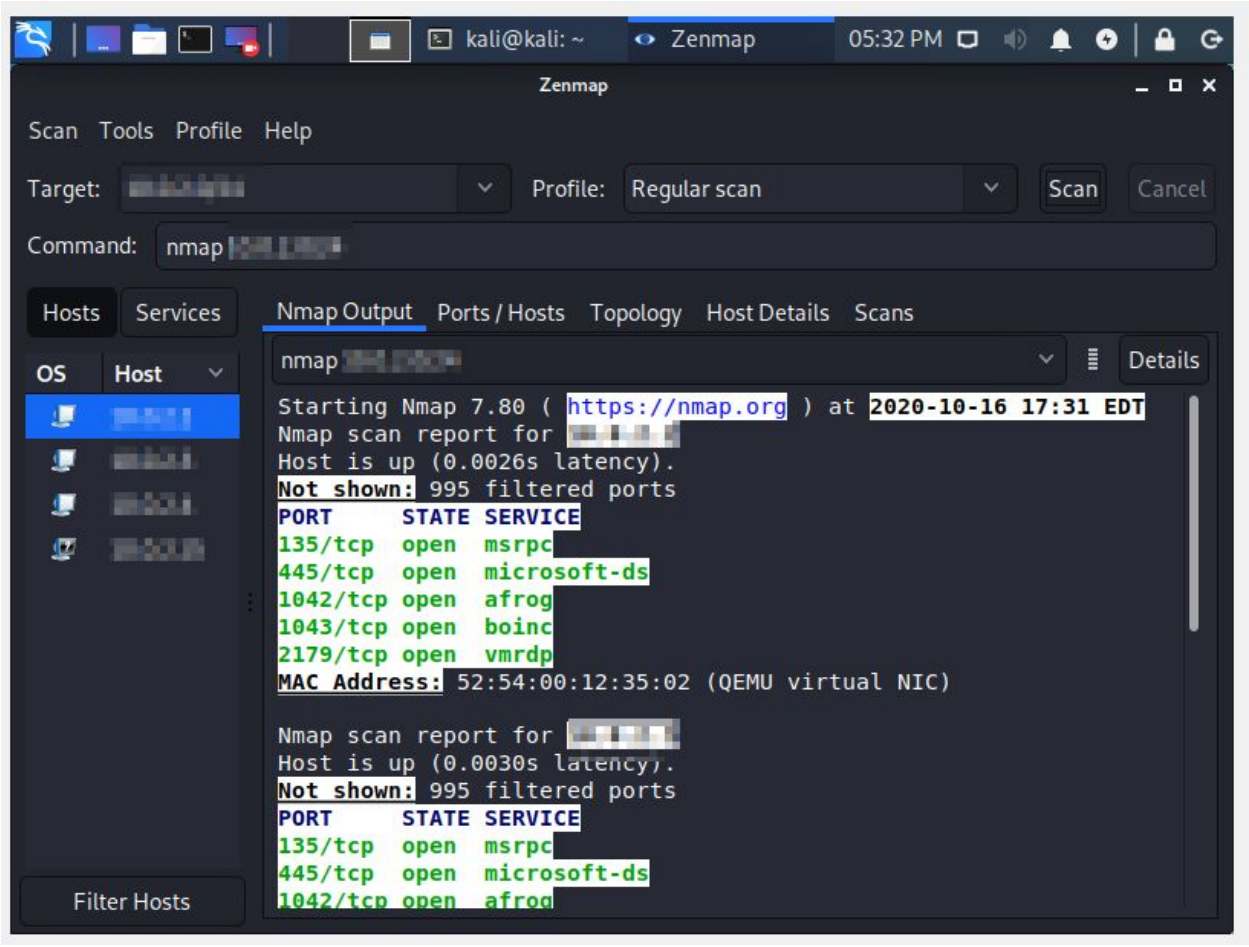
- Quick traceroute: **nmap -sn –traceroute**
    - What does this scan do in technical terms?
        - This command scans for all routers and host within the network by sending ICMP packages to all devices on the network
    - Was the scan correct?
        - Yes
    - Why/why not?
        - This command identifies the devices on the network and defines the number of hops identified as the path was determined.

Traceroute



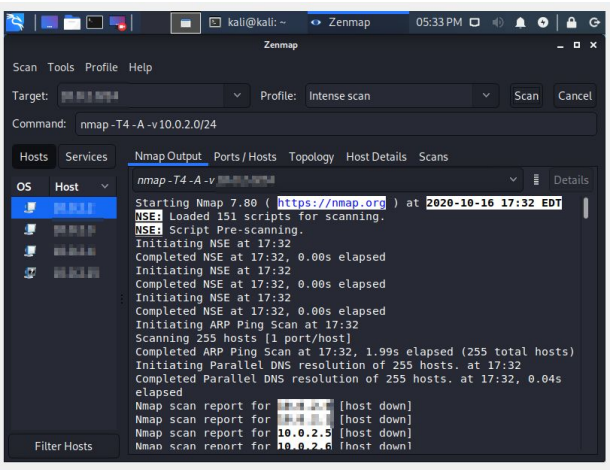
- Regular scan: **nmap**
    - What does this scan do in technical terms?
        - This means it will issue a TCP SYN scan for the most common 1000 TCP ports, using ping request
            - Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP)
            - synchronize, SYN is a TCP packet sent to another computer requesting that a connection be established between them
    - Was the scan correct?
        - Yes
    - Why/why not?
        - This command executed as expected; it displays the ping attempts and displays the TCP ports that were discovered within the scan as well as the mac address associated with the target.

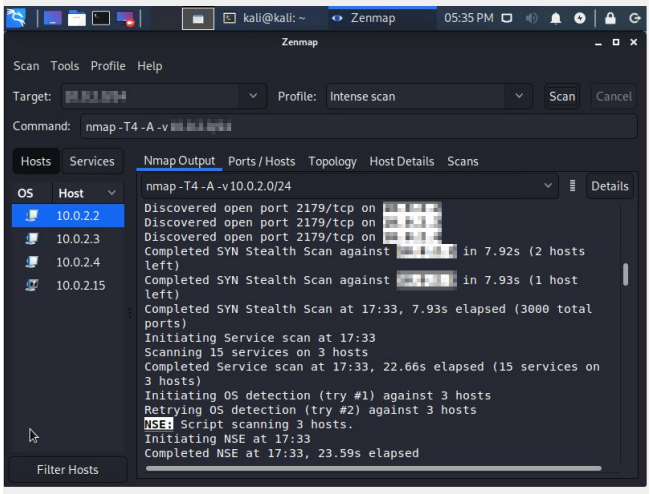
Regular scan

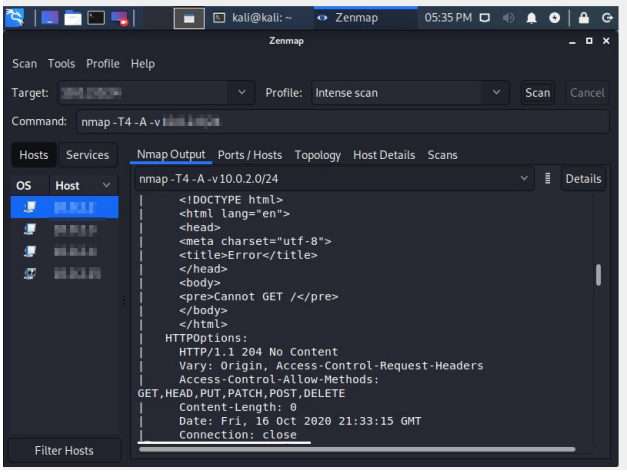


- Intense scan: **nmap -T4 -A -v**
    - What does this scan do in technical terms?
        - This command uses a t4 modifier for a fast scan of TCP ports with attempts to determine os and version os host.
    - Was the scan correct?
        - Yes
    - Why/why not?
        - This executed as expected returning both hosts that were running and host that was done, as well as the number of attempts to determine version and os.

Intense scan



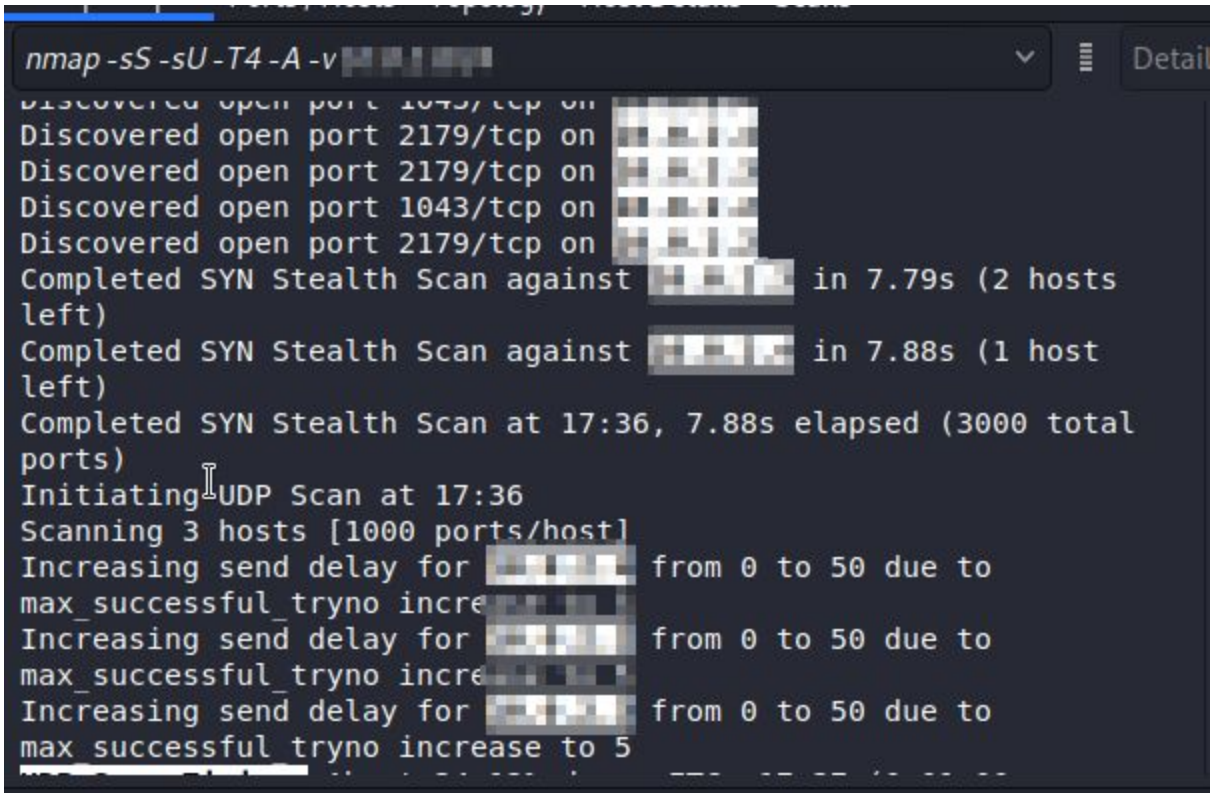




Intense scan plus UDP: **nmap -sS -sU -T4 -A -v**

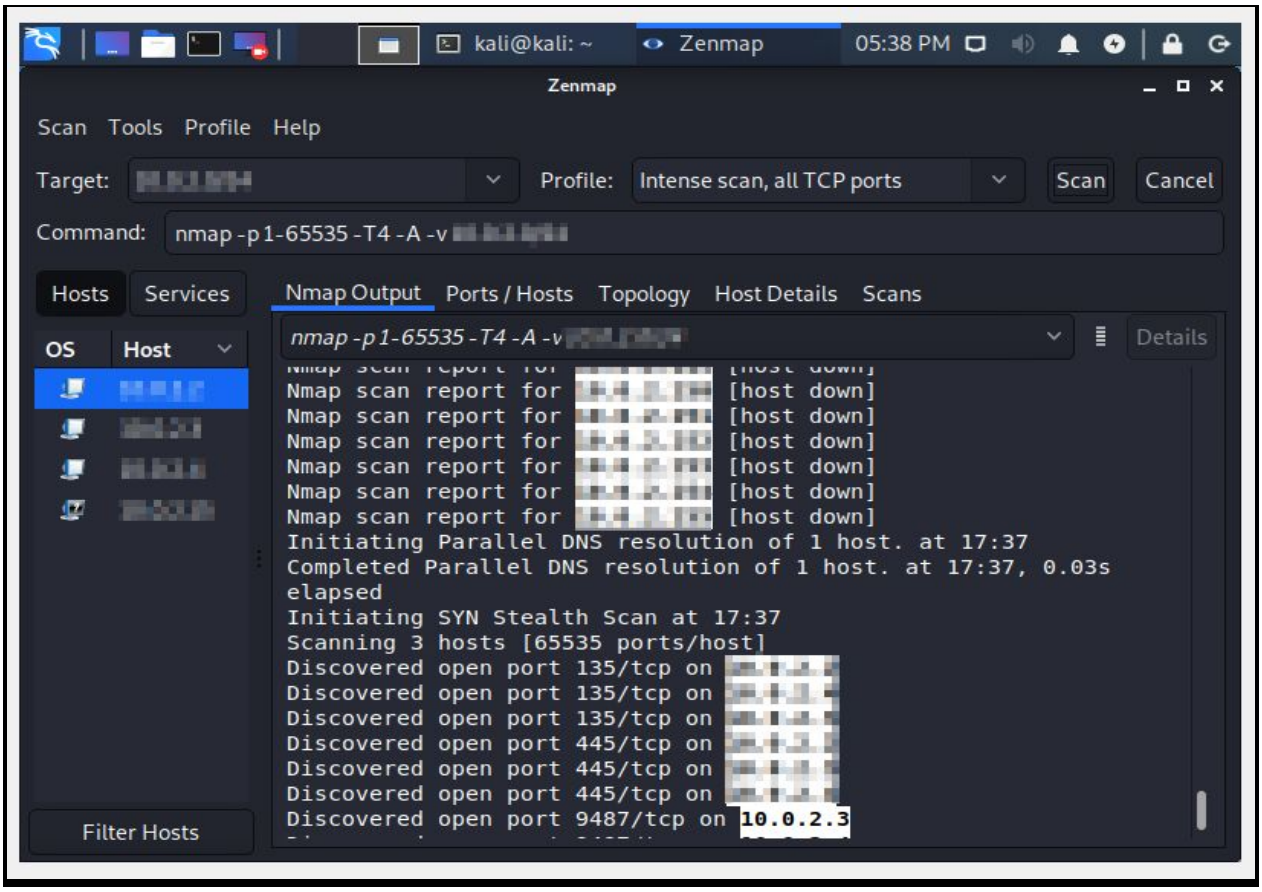
- What does this scan do in technical terms?
  - This command responds similarly to the intense scan with the added feature of UDP port scans
    - User Datagram Protocol (UDP), DP, computer applications can send messages, in this case, referred to as *datagrams*, to other hosts on an Internet Protocol
- Was the scan correct?
  - Yes
- Why/why not?
  - This executed as expected displaying both TCP and UDP attempts that the number of hosts identified.

Intense scan plus/ UDP



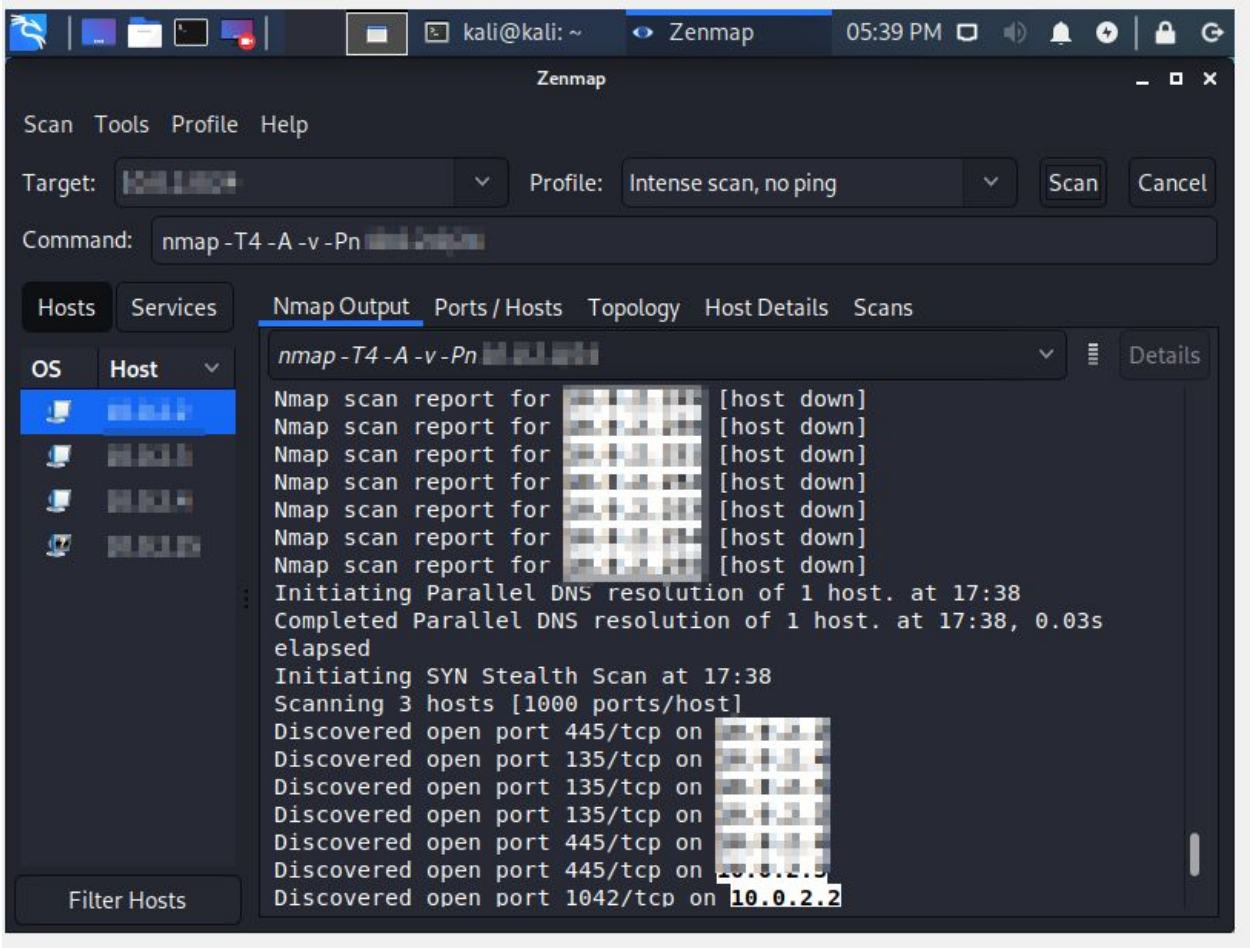
- Intense scan, all TCP ports: **nmap -p 1-65535 -T4 -A -v**
    - What does this scan do in technical terms?
        - Scans a list of 1000 most common protocols between 1 -65535 including all TCP ports
    - Was the scan correct?
        - Yes
    - Why/why not?
        - This command executes as expected showing all 65535 attempts focusing on TCP open and closed ports.

Intense scan / Tcp



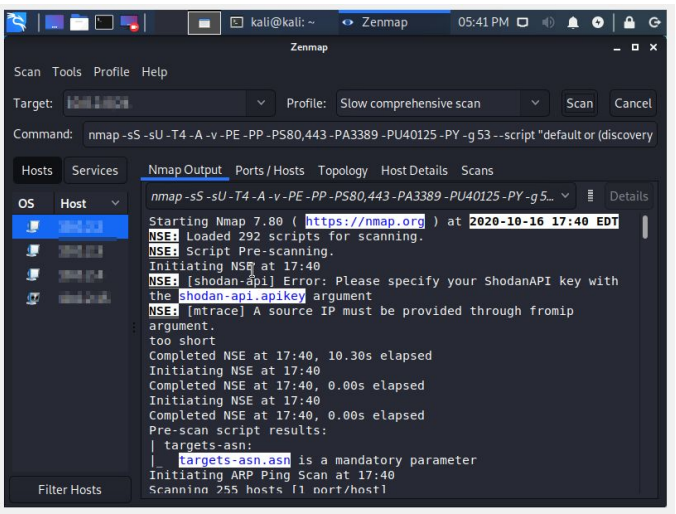
- Intense scan, no ping: **-T4 -A -v -Pn**
    - What does this scan do in technical terms?
        - This performs the same functions as the intense scan with the expectation that the target is up, and does not send ICMP packets
    - Was the scan correct?
        - Yes
    - Why/why not?
        - Command worked as expected not displaying any ICMP request

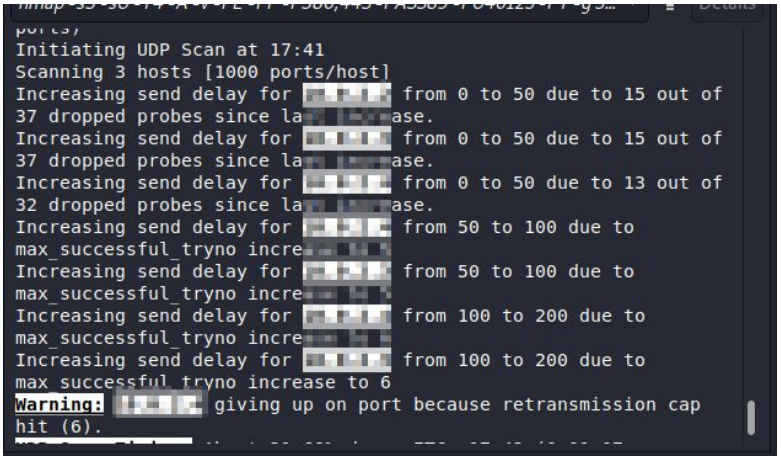
Intense scan / no ping



- Slow comprehensive scan: **-sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53**
    - What does this scan do in technical terms?
        - This command scans for TCP, UDP, and SCTP and puts a lot of effort to identify the host within the network trying to identify os and host and could be time-intensive, taking over an hour to complete
    - Was the scan correct?
        - Yes
    - Why/why not?
        - Yes, this performed a very thorough scan taking over an hour and many attempts to identify host ports connected with each port.

Slow comprehensive





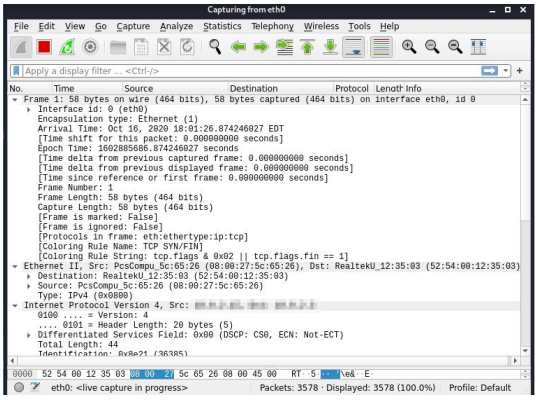
Part 3: Sniffing ICMP Packets with Wireshark

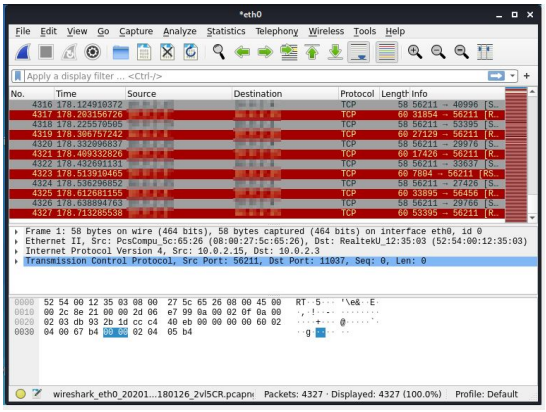
Step 1- Launch Wireshark from Kali Linux (it's part of Kali).

Step 2- Begin sniffing.

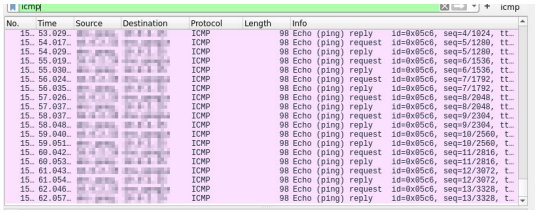
Step 3 - Filter the view to ICMP packets only

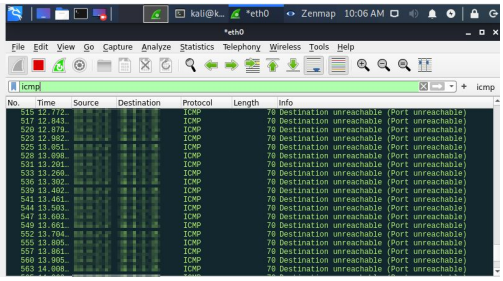
Wireshark



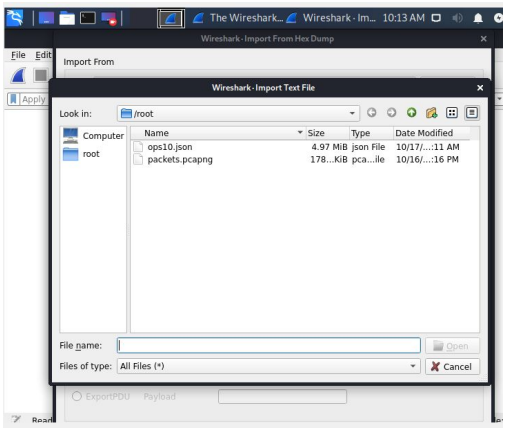


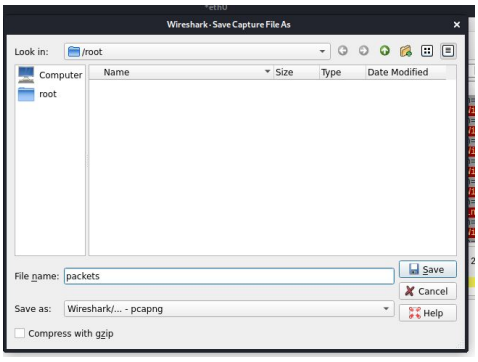
Icmp





File





Part 4: Reporting

Compile your findings in an organized fashion.

- Create a **Scans Performed** table with three columns: Scan Type, Scan Results, Actual.
    - Populate the table with your results.
- Create a **Service Enumeration** table with three columns: Server IP Address, Ports Open, and Service/Banner.
    - Populate the table with your results.
    - Indicate above the table your network range with CIDR block notation.

Scans performed table