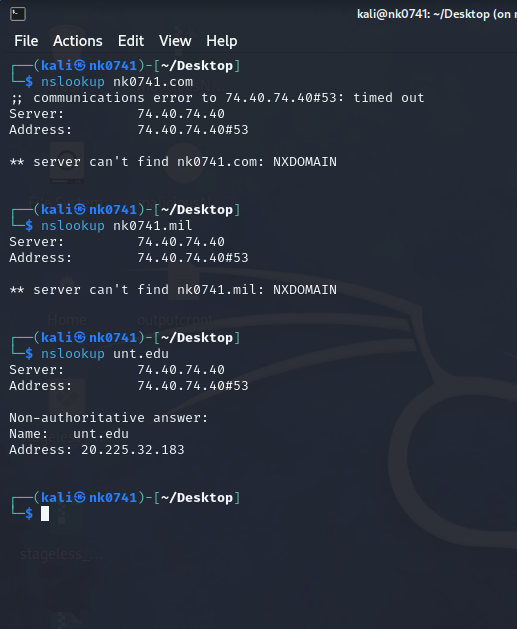
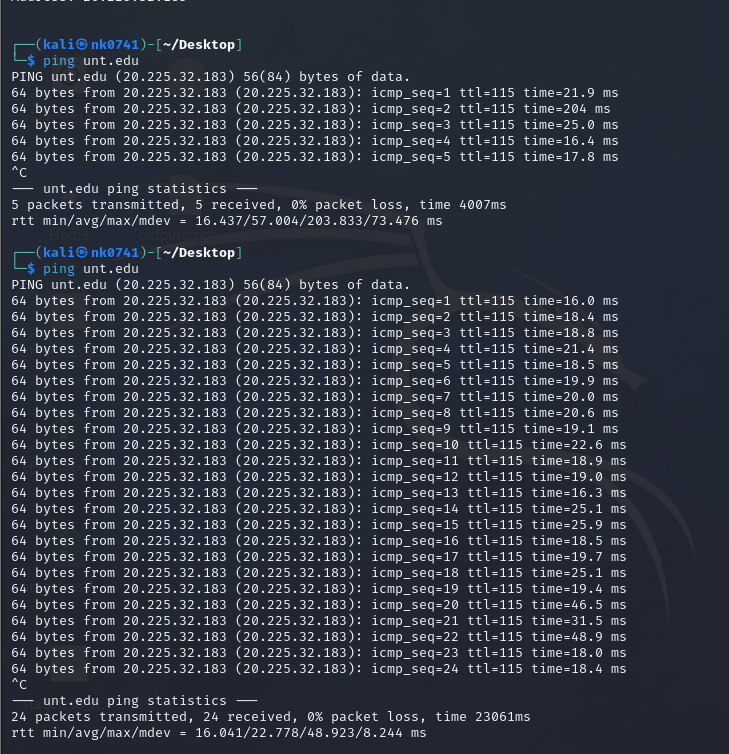
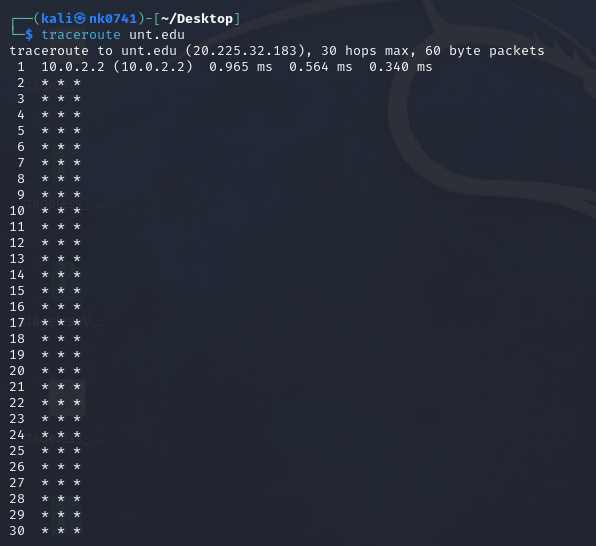
DNS resolution:



We can see the nk0741.com and nk0741.mil doesn’t have any server for them. Unt.edu has server has ip address: 20.225.32.183

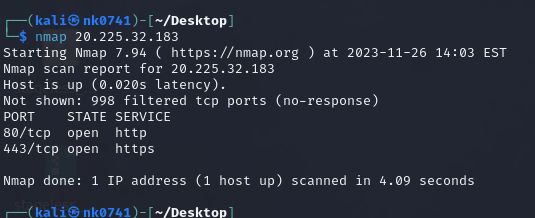
Using Ping command on unt.edu  


Using trace route on unt.edu:



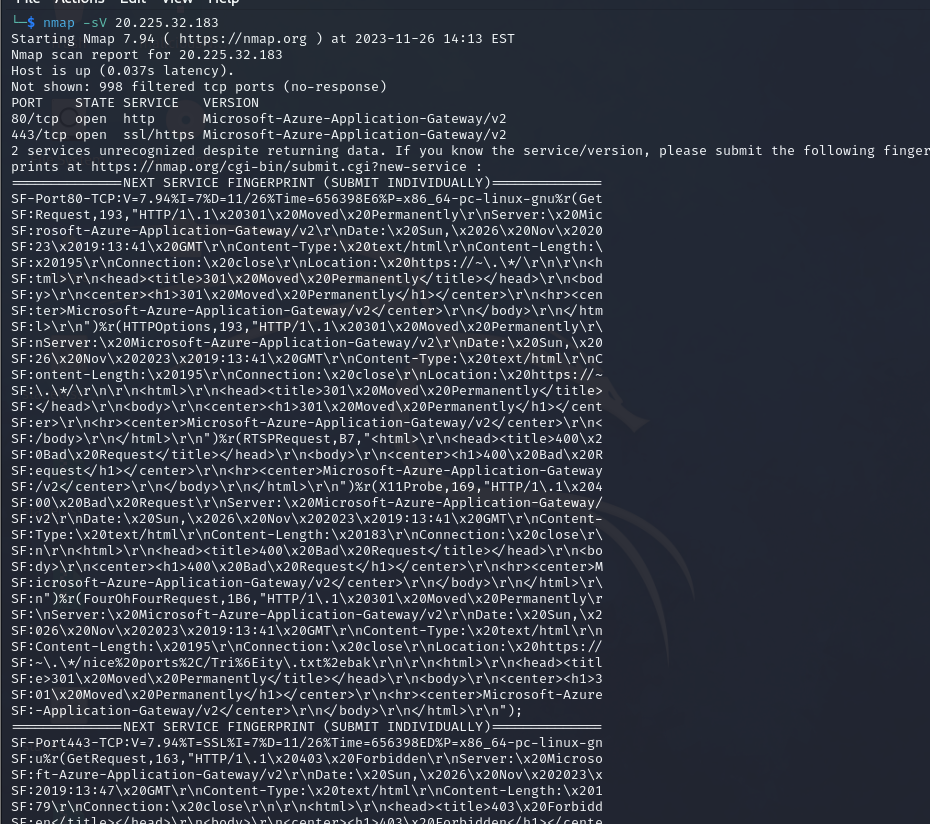
The traceroute shows a connection attempt to unt.edu (20.225.32.183) with no successful hops, likely due to network configurations blocking ICMP packets. The asterisks (\*) indicate no response received within the allotted time, possibly due to firewall settings or network congestion. The lack of specific hop details suggests the packets might be getting dropped or filtered at an intermediary network point.

Using nmap on unt.edu:



The nmap command shows that host is up and responsive with a very low latency of 0.020 seconds. The scan revealed two open ports: port 80 for HTTP and port 443 for HTTPS. Additionally, the scan found 998 TCP ports as filtered, suggesting that these ports are likely protected by a firewall or not responding to the scan. Overall, the host seems to be running web services on standard HTTP and HTTPS ports.

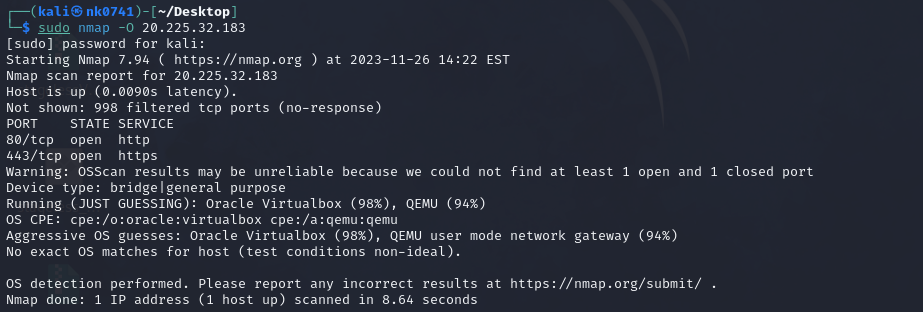
Detailed scan using nmap:



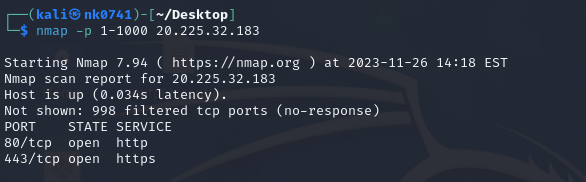
Explanation:

The Nmap scan conducted on the IP address 20.225.32.183 confirmed that the target system is active and promptly responsive, indicating a quick round-trip time (latency) of 0.020 seconds. This implies that the system is online and accessible. Regarding the ports, the scan identified two ports that are open and accepting connections: port 80 (HTTP) and port 443 (HTTPS). These ports are commonly used for web services, suggesting that the host likely hosts web servers or web-based applications utilizing HTTP and HTTPS protocols. Furthermore, the scan reported 998 TCP ports as "filtered," meaning that these ports did not respond to the scan. This situation typically occurs when ports are protected by a firewall or when the scanned ports do not provide any response, possibly indicating they are closed or not actively listening for connections.

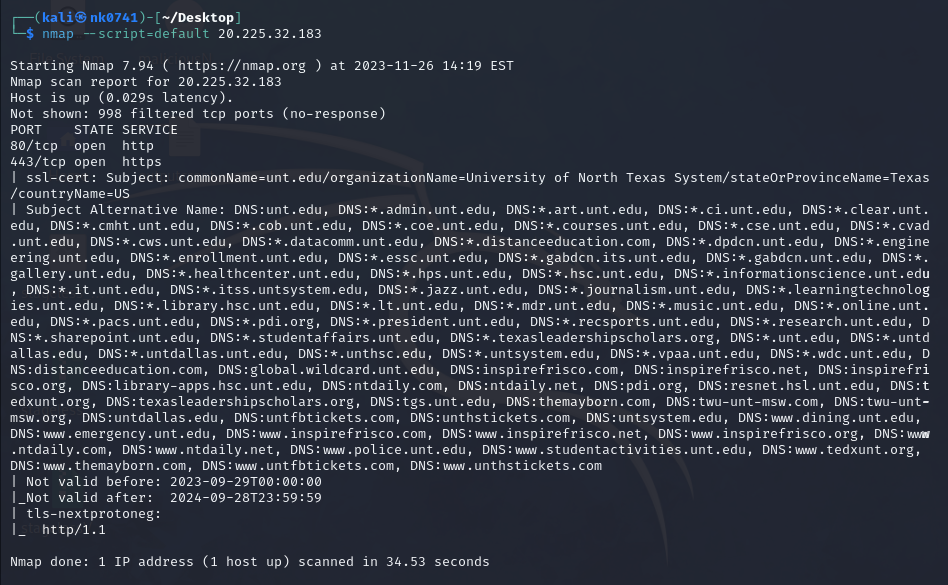
Trying to detect OS used in unt.edu using nmap: (Requires root access)



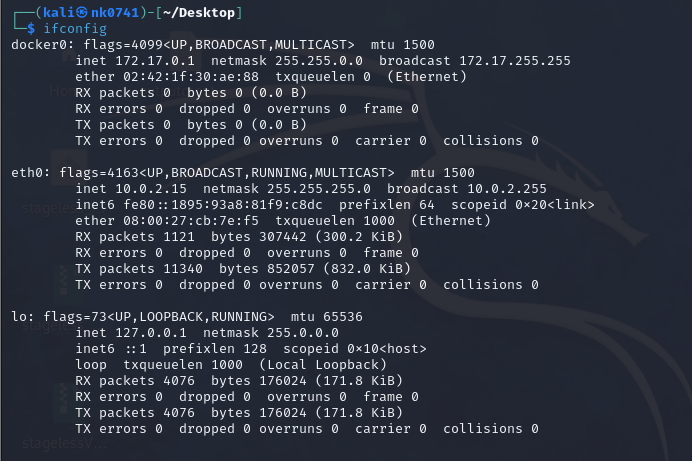
Scanning only specific ports using nmap:



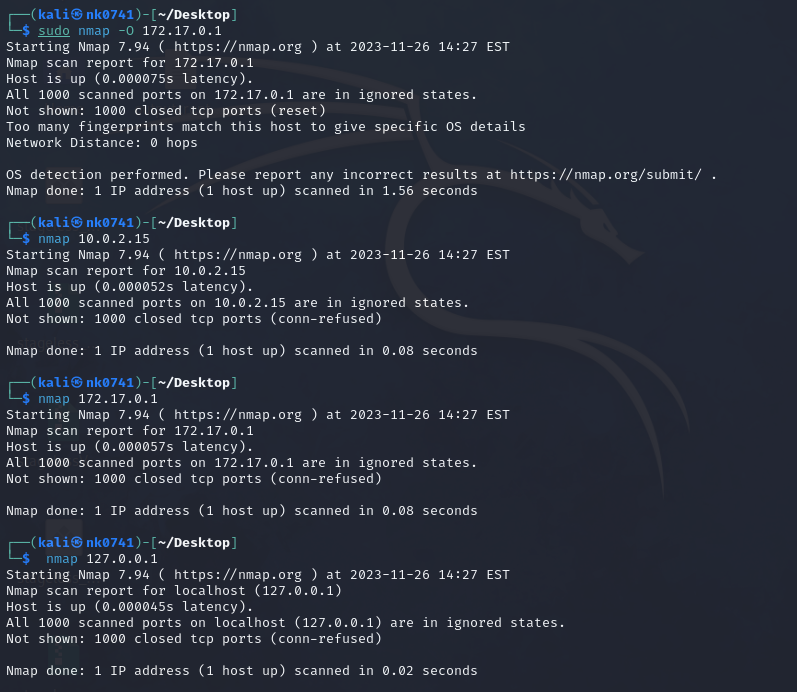
Using nmap to do the script scanning:



Using ifonfig to get machince’s ip address:



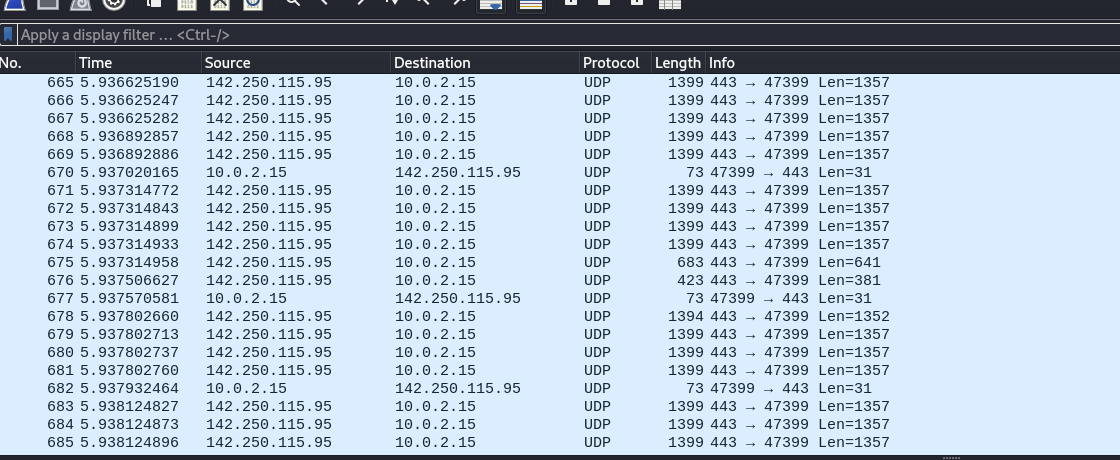
Nmap scan on local OS:



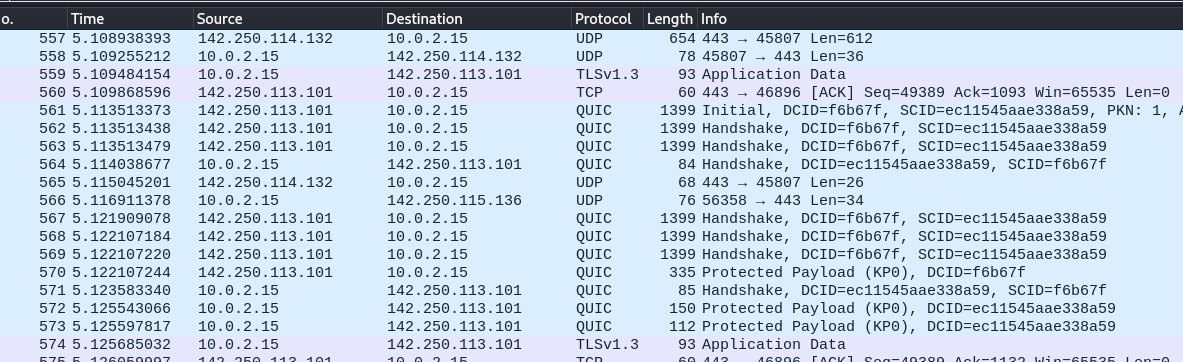
The vm has 3 ip address one for docker, other for brigded eth0 connection and last one is localhost/loopback address.

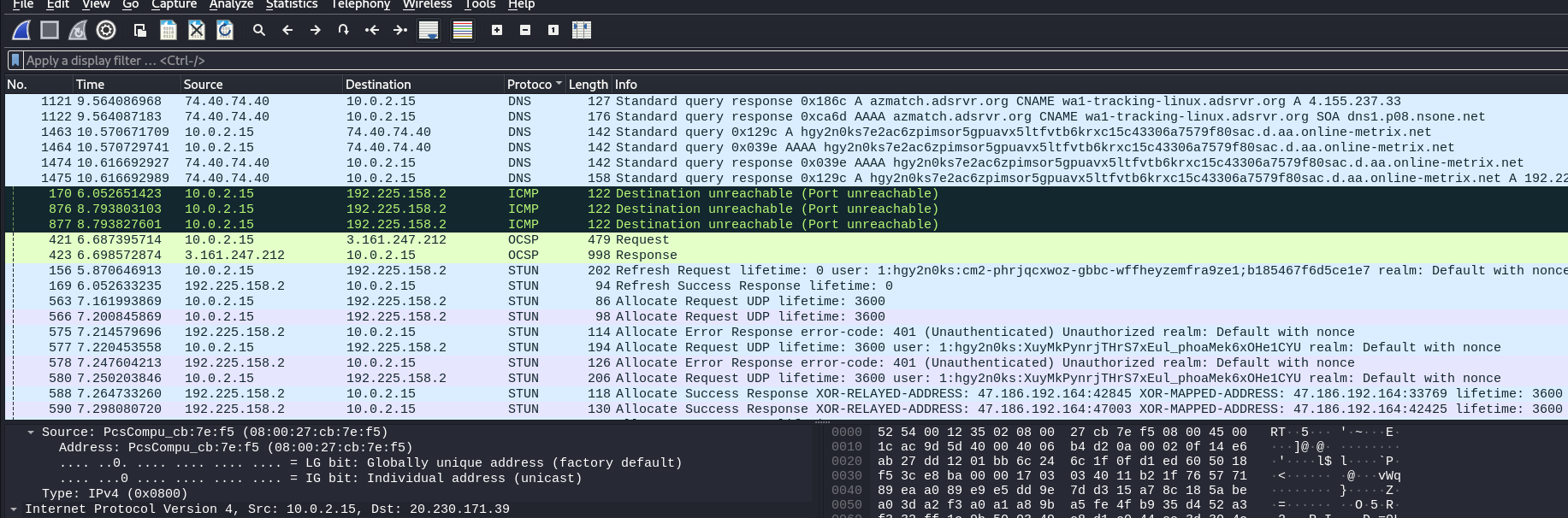
Running wireshark on youtube:

Protocol used- udp:



Protocol used- QUIC:



Running wire shark on Walmart.com  


I found many different protocols like dns, icmp, ocsp, stun, tcp, TLSv1.2, udp. It didn’t use quic protocol.