Kevin Huang

CSS 537

Lab 2: Network Scanning using nmap

01/22/2022

Task 1: Getting started with nmap

* -sn: do not do a port scan after host discovery



* -PO: sends an IP packet with the specified protocol number set in it’s IP header



* -PS: sends an empty TCP packet with the SYN flag set



* -PU: sends a UDP packet to the given ports



* -sO: determine which IP protocols are supported by target machines



* -sV: detects the version

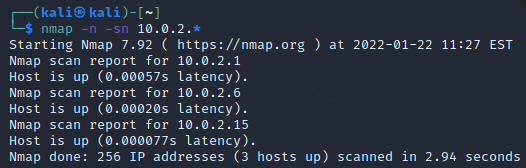


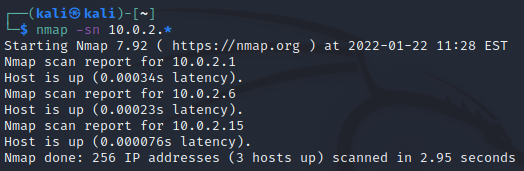
* -O: enables OS detection



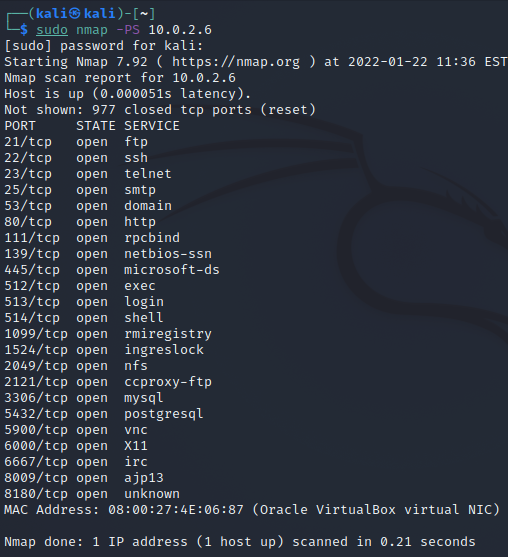
Task 2: Using nmap to conduct a reconnaissance of your network

1. The -n option is used so that the scan does not do DNS resolution. I can see that running without the -n option did not have any noticeable difference since there was no DNS resolution needed when scanning my own network.

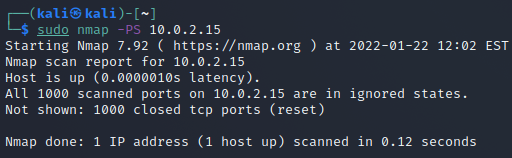




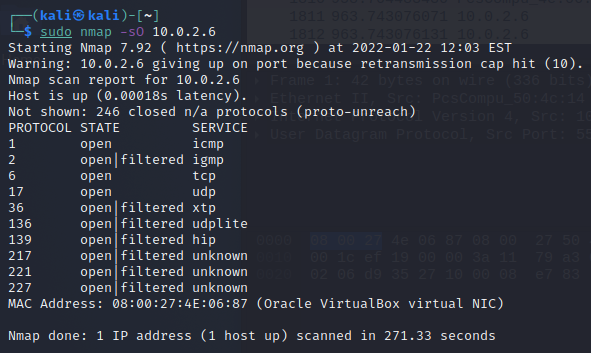
1. The other host machine that I have on the network is 10.0.2.6. I found that there are 23 open TCP ports on this host. UDP is a connectionless protocol, unlike TCP we will not get a response back for a successful request. We can attempt to ping all the UDP ports and if we get a destination unreachable meaning that the port is closed.



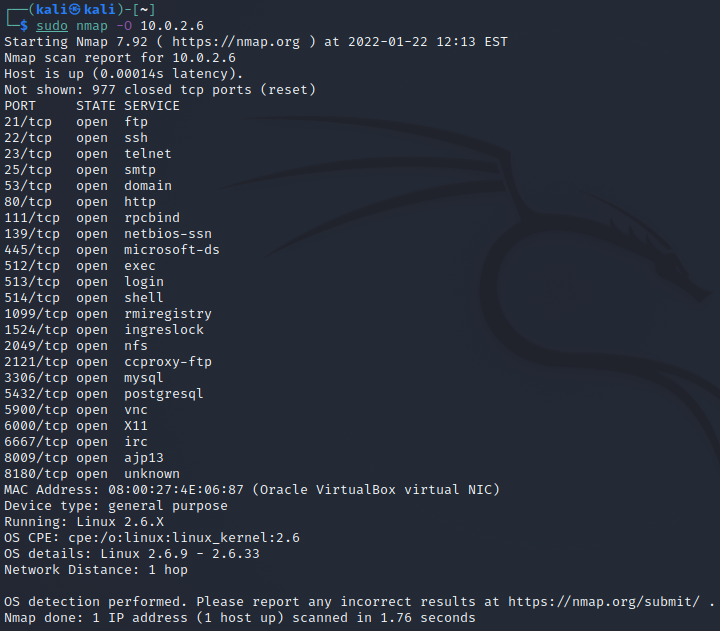
1. I was not able to identify any open ports on my own machine. It says that the 1000 scanned ports are in ignored states.

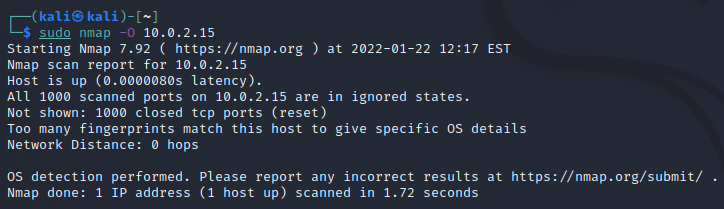


1. With the -sO scan, there were additional protocols that were found. There were new protocols found such as igmp, xtp, udplite, and hip.

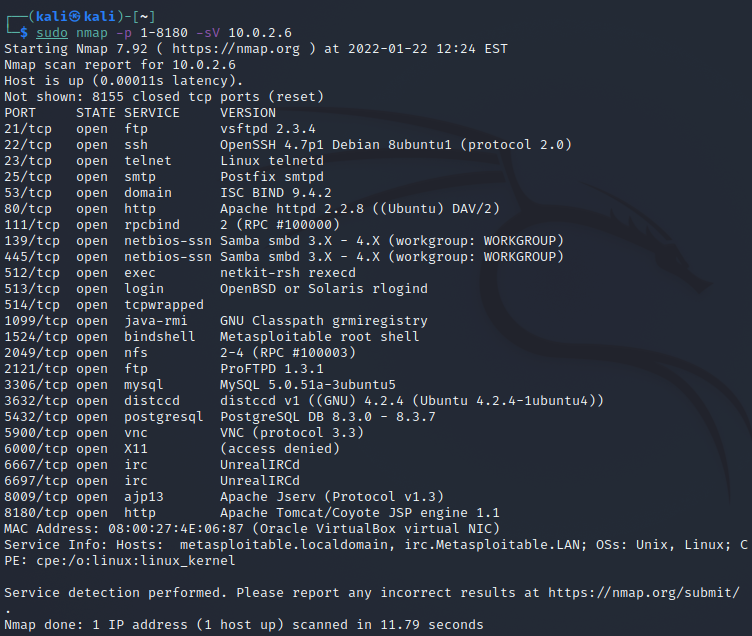


1. Using the -O option when scanning 10.0.2.6, I found that nmap thinks that it is running Linux 2.6.X. Also, it found that the MAC address is 08:00:27:4E:06:87 which matches. It was not able to find what operating system the attacker machine was running.

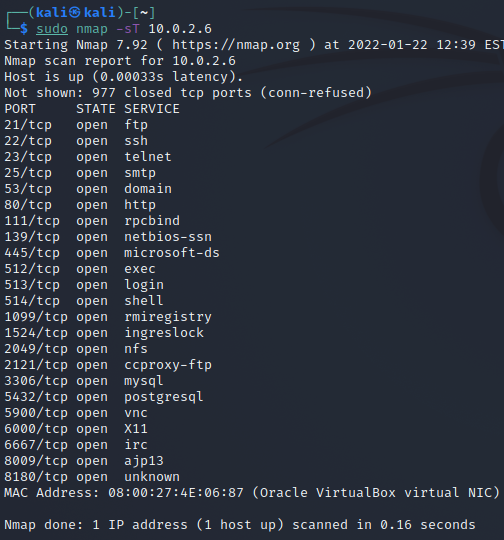




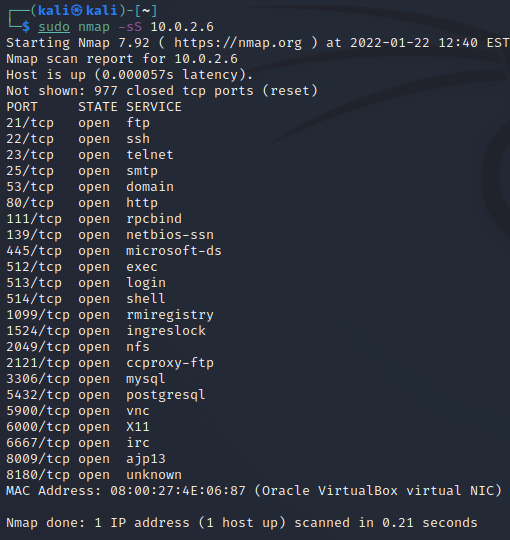
1. I found that I can specify a port range to scan with -p option. I used the version scan option -sV to scan open ports that I found previous. For SSH, the target host uses version OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0). I also found that for http, it uses Apache httpd 2.2.8 ((Ubutu) DAV/2).



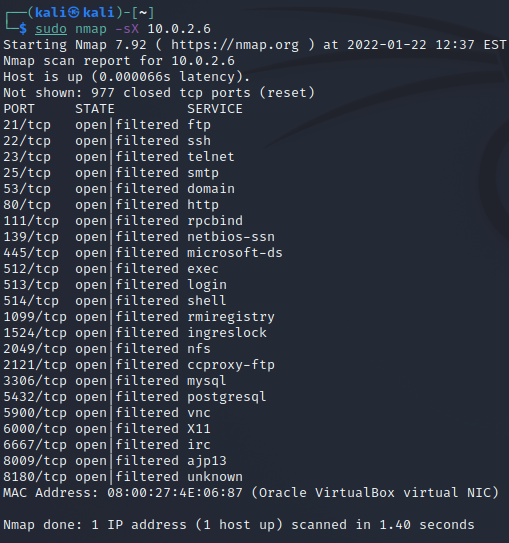
1. TCP Connect scan:



TCP SYN scan:



Xmas -sX scan:



Null scan:

