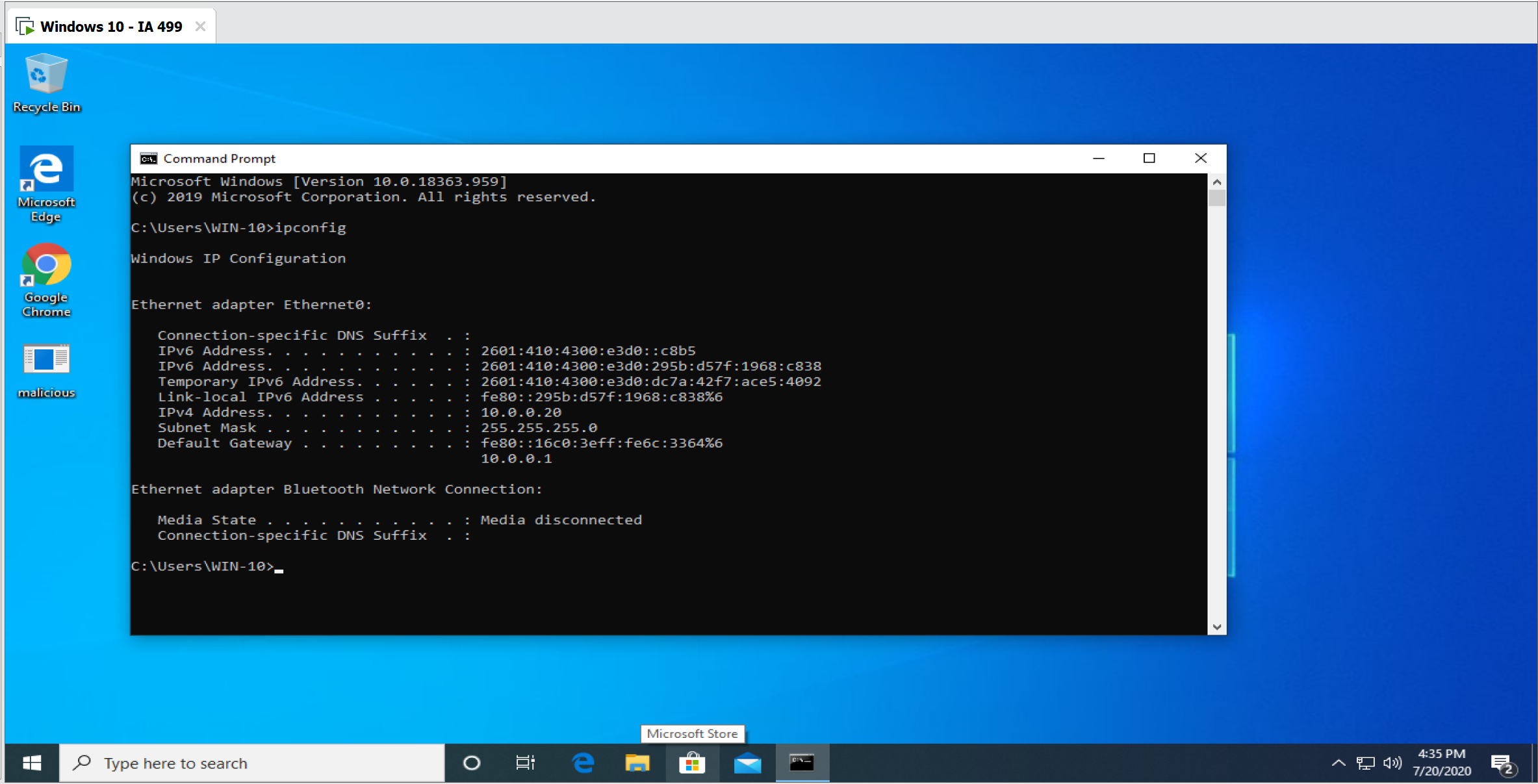
Vulnerability Analysis Lab

\*Names or letters in quotations are an example and are meant to be replaced with your own information.

Kali has many tools built into it specifically meant for analyzing networks and devices. These tools can be used to search for ip addresses or vulnerabilities and gather general system information. Three of these tools are Nmap, Nikto, and Legion.

Before starting the pen-testing, it’s best to download and install Kali Linux as a virtual machine on a Type 2 Hypervisor using either VMware, Hyper-V, or Virtual Box. Kali can be downloaded from <https://www.kali.org/downloads/>. It is recommended to install the 64-Bit version of Kali and allocate two cores of the processor, 4GB Ram, and at least 40 GB storage space, but this will come down to the specification of the host system. A second virtual machine will be needed for conducting the analysis on. This will be the victim computer. It is recommended that the victim machine is running a Windows 10 OS, which is what this lab used. Both the Kali and victim virtual machines should have their network adapters set to “Bridge” connection.

Boot up the victim computer and note down the ip address. On Windows 10, this can be done by selecting the start button at the lower left corner of the screen, type cmd in the search bar, opening command prompt (cmd), and using the **ipconfig** command.



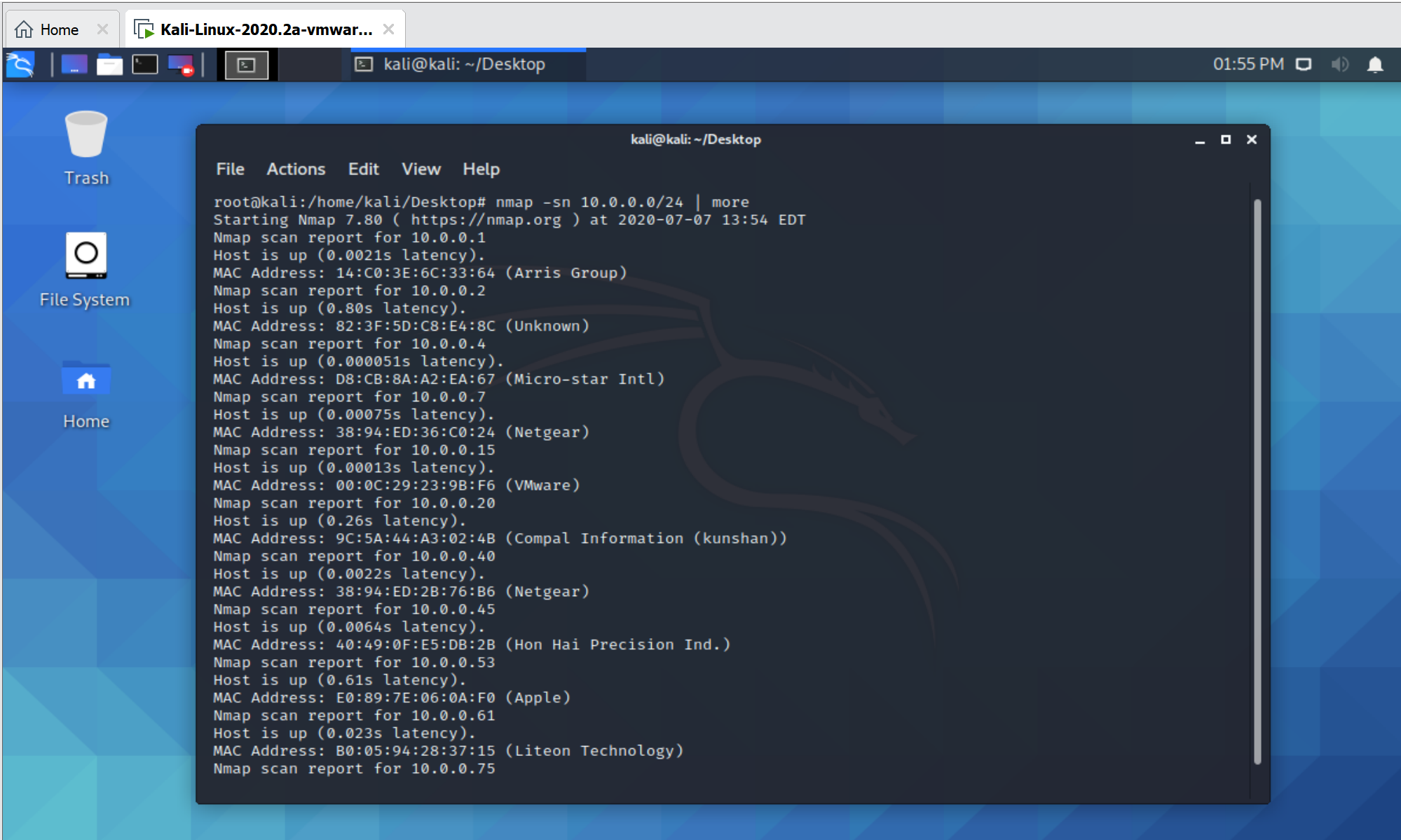
The ip address of the Kali machine should also be noted by navigating to the terminal and using the command **sudo ifconfig**. Test the connection between the two virtual machines by pinging each ip address from each VM. It’s also best to install any new updates to Kali beforehand with the command: **sudo apt-get update**.

Nmap:

Kali comes with Nmap already built in, but if for any reason it needs to be installed, it can be done with the terminal and inputting in the command **sudo apt-get install nmap**. If the user is logged in as root, then the sudo expression is no longer needed.

Nmap can be used to search for a specific range of ip addresses within a network. This can be done in the terminal using the command **sudo nmap -sn (“ip range or network”)**, with the “ip range or network” being the network of which is being searched through followed by the subnet mask slash notation. This command can be piped to **more** tooutput per page.

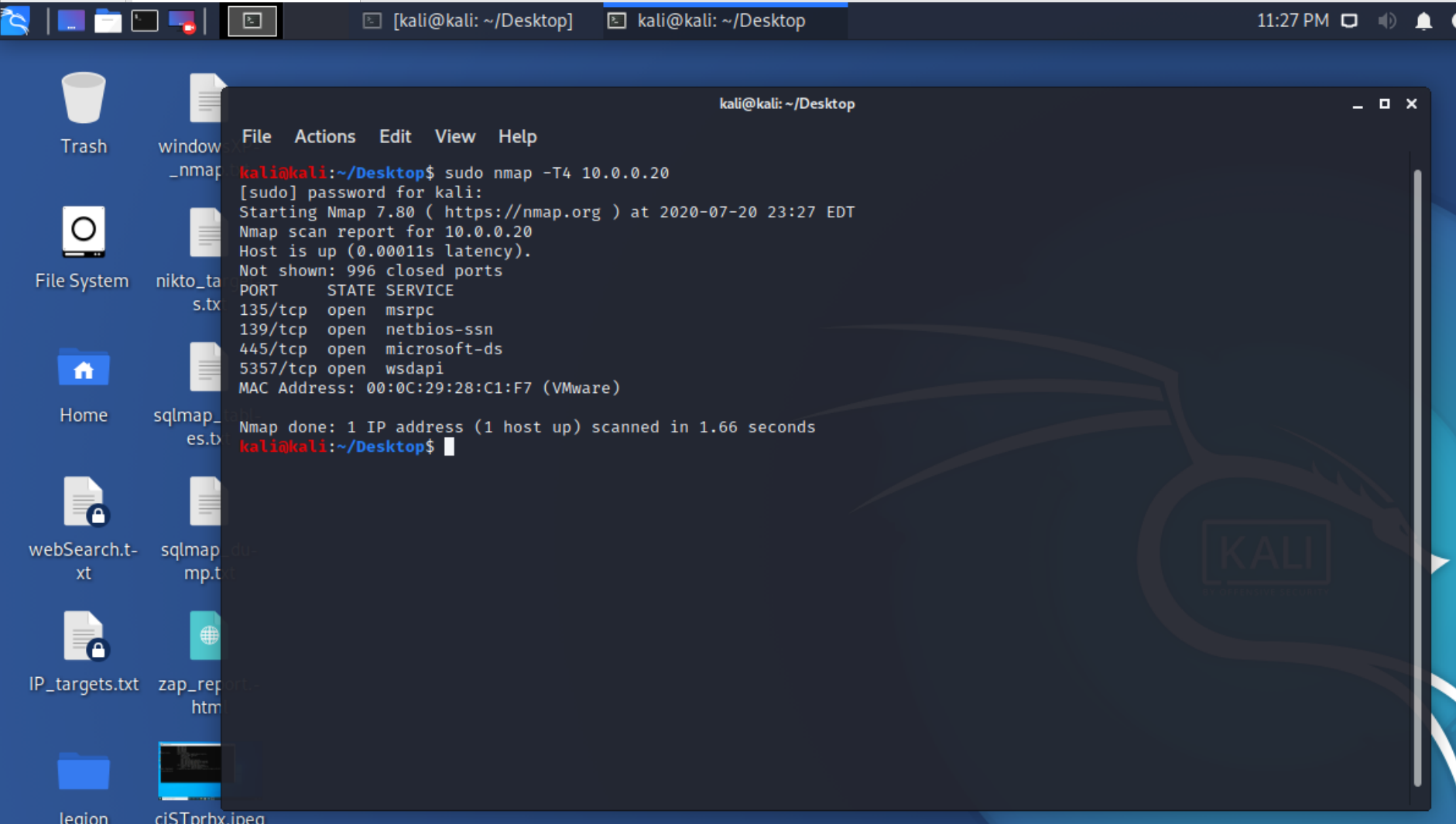
Example: nmap -sn 10.0.0.0/24 | more



Here, Nmap will discover multiple ip addresses that are in use, including the victim PC. Next, we can have Nmap directly target the victim’s ip address, **sudo nmap -T4 (“ip address”)**.

This command will scan the target IP address for any open ports. The timing option, -T4, will speed up the scan from the default scan speed. Timing can be useful for alerting or not alerting the firewalls or other security systems.

Example: sudo nmap -T4 10.0.0.20



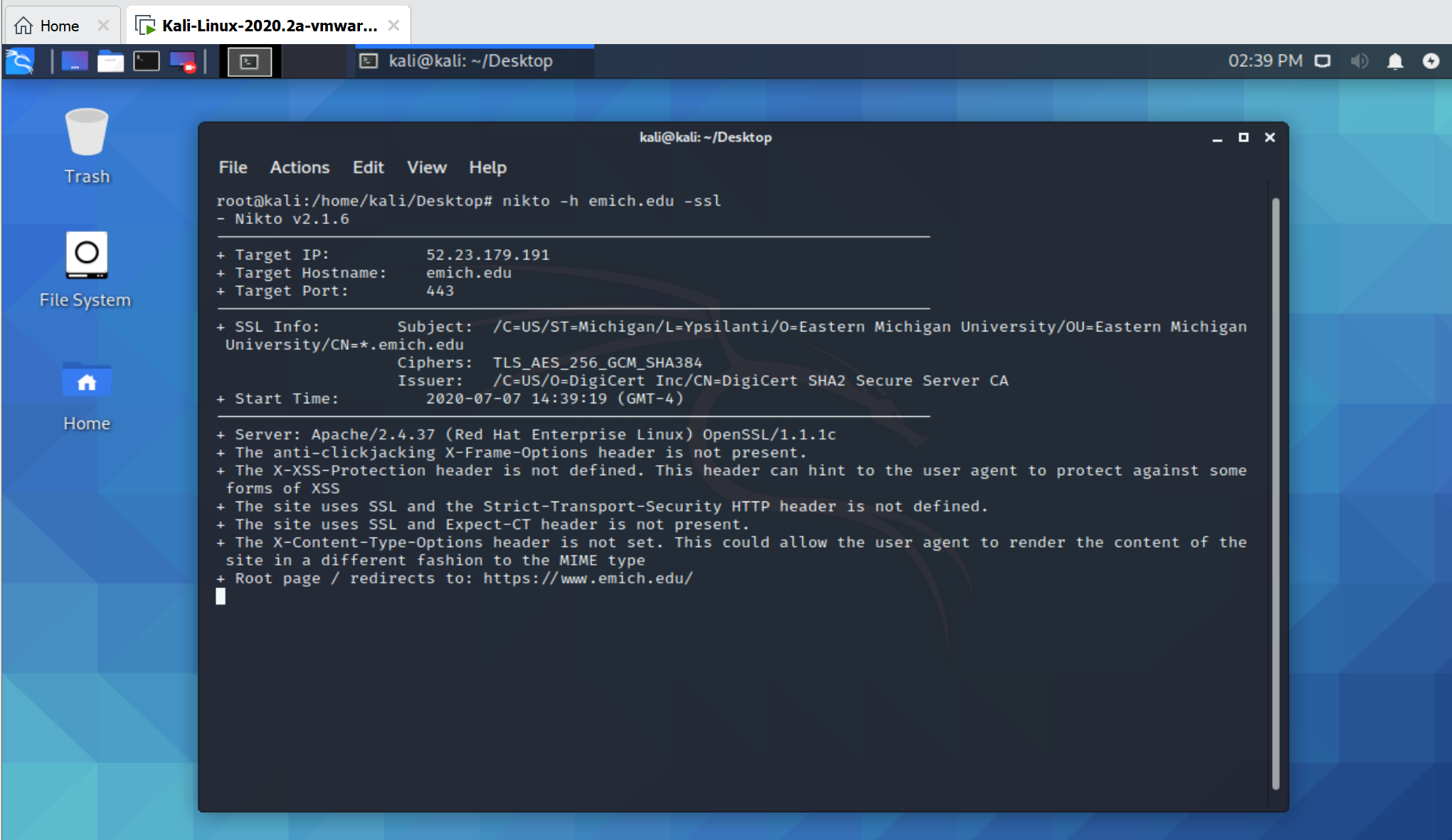
Here, Nmap was able to determine that ports 135 (MSRPC), 139 (NETBIOS-SSN), 445 (MICROSFT-DS), and 5357 (wsdapi) are all open with 996 other ports being closed. Depending on the victims’ system and the services currently running, different ports may be displayed as open or closed. This information can also be saved to a text file with the command **sudo nmap -T4 (“ip address”) > (“name”.txt)**,if needed.

Nikto:

Nikto is another vulnerability scanner mostly meant to target web servers. Again, Nikto should already be installed on Kali by default, but the command **sudo apt-get install nikto** will install it to the system if needed. Afterwards, install the ipcalc function: **sudo apt install ipcalc**.

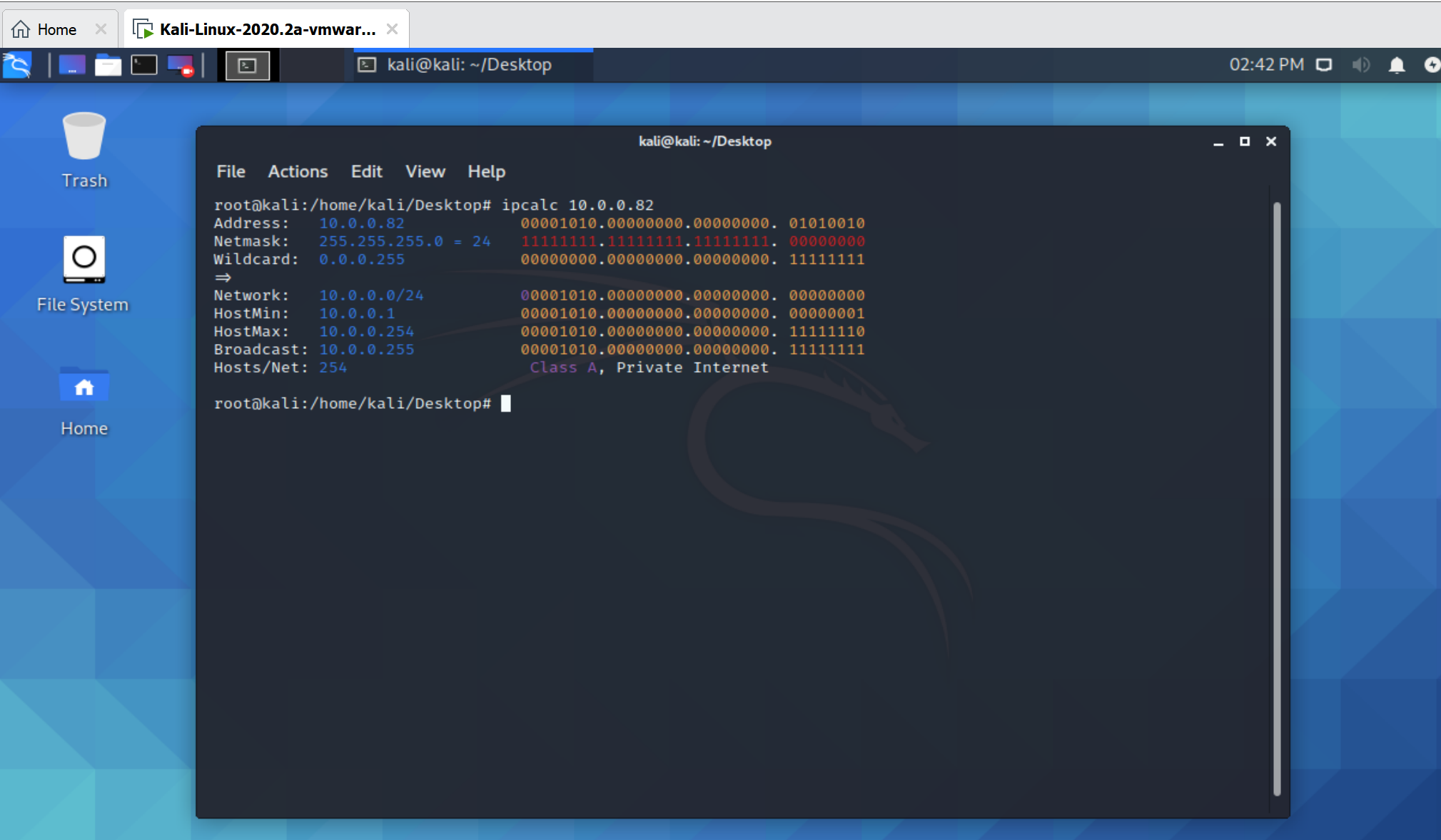
The **sudo nikto -help** command will retrieve all the options that can be used to nikto. For now, test nikto by scanning a web server over port 443 with the command **sudo nikto -h (“ip address or hostname”) -ssl**.

Example: nikto -h emich.edu -ssl



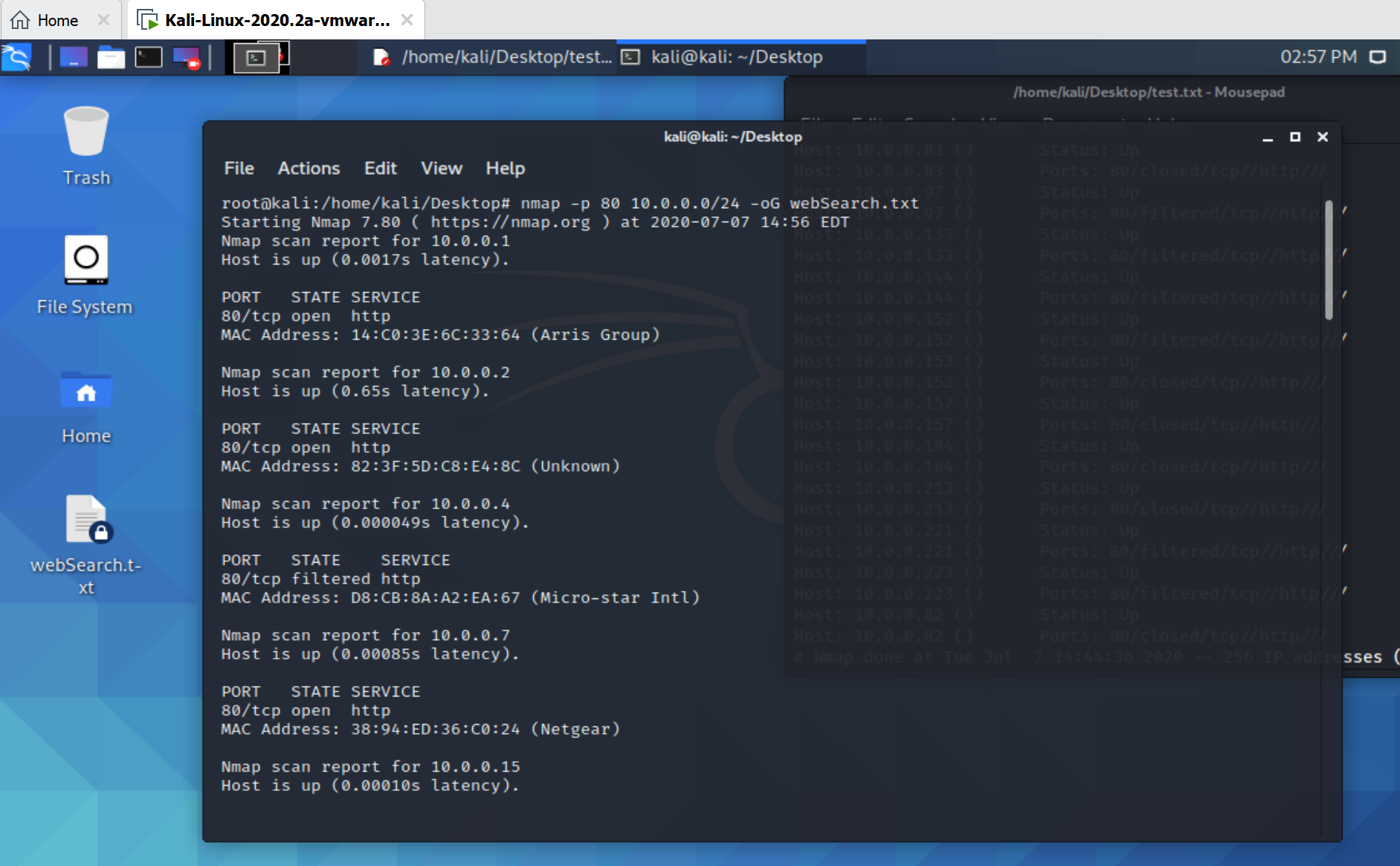
This give us information about the ip address, ciphers, and the issuer of the certificates. Next, we can use to the ipcalc command to find some information about our own network using the command **sudo ipcalc (“ip address”)** with the ip address being from the Kali virtual machine.

Example: ipcalc 10.0.0.82



This gives information about the network and the subnet mask. We can then scan for any web servers on the network, specifying for port 80 and sending the output to a text file using Nmap: **sudo nmap -p 80 (“ip range/network”) -oG (“name”.txt)**.

Example: nmap -p 80 10.0.0.0/24 -oG webSearch.txt

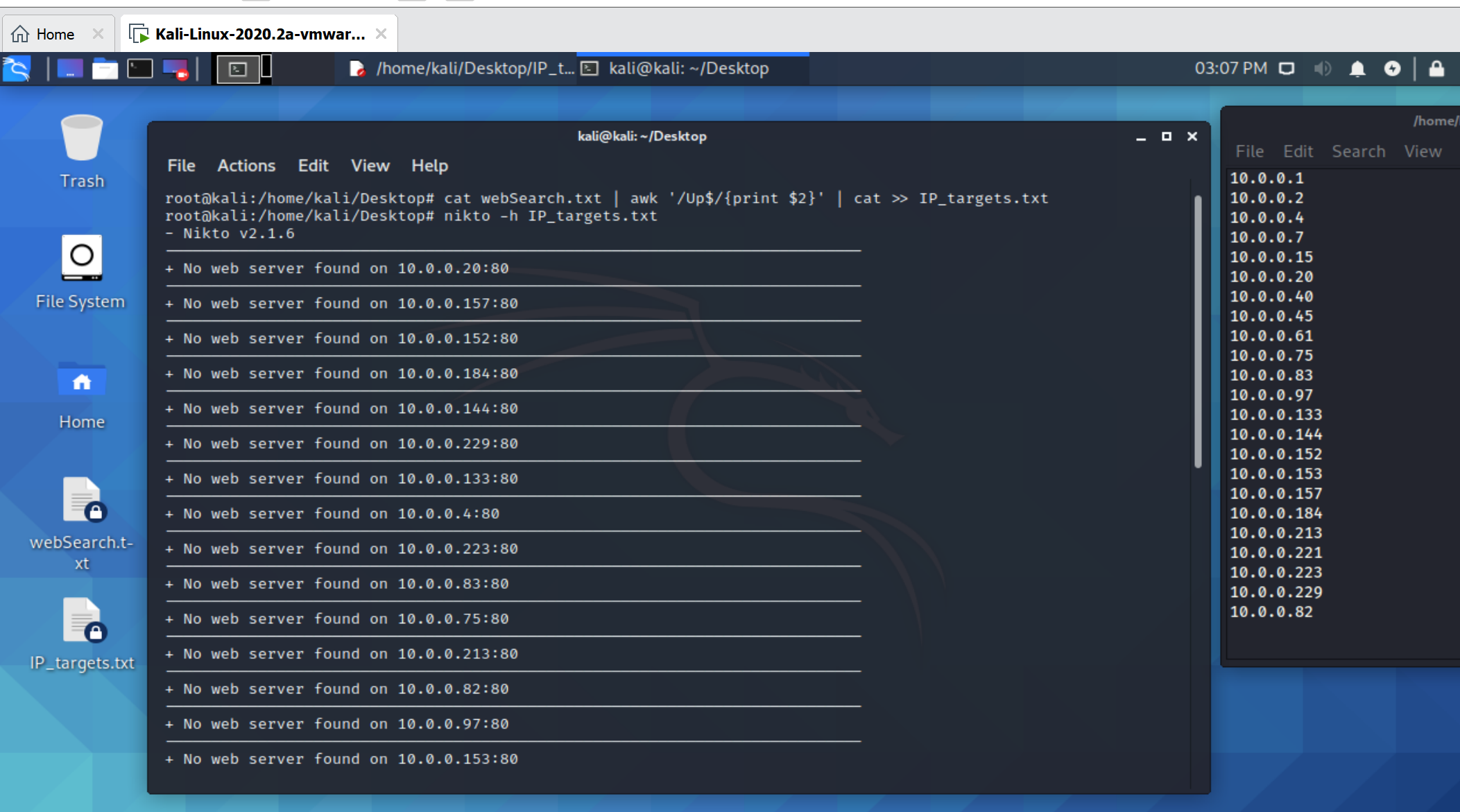


We can then filter out all the information, leaving only the ip address using the Linux command **awk** and sending it to a new text file: **cat (“name”.txt) | awk ‘/Up$/{print $2}’ | cat >> (“name”.txt)**.

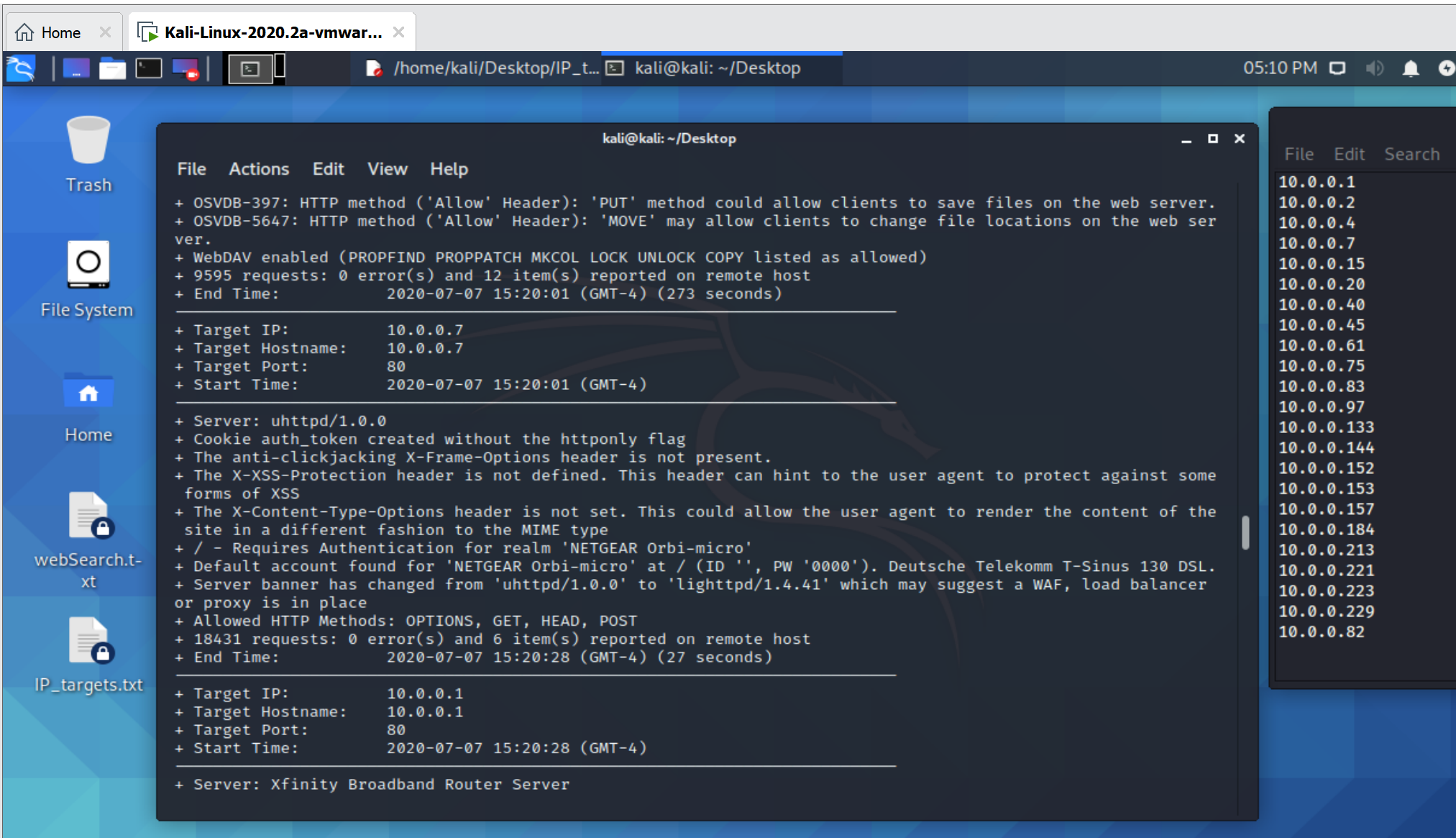
Example: cat webSearch.txt | awk ‘/Up$/{print $2}’ | cat >> IP\_targets.txt

We can then use this text file to target the ip address with Nikto: **sudo nikto -h (“name”.txt)**.

Example: nikto -h IP\_targets.txt



Nikto will display which ip addresses are web servers and which are not.



Nikto is a useful tool to quickly gather information on web servers to find their ip addresses and see the type of platforms they are running.

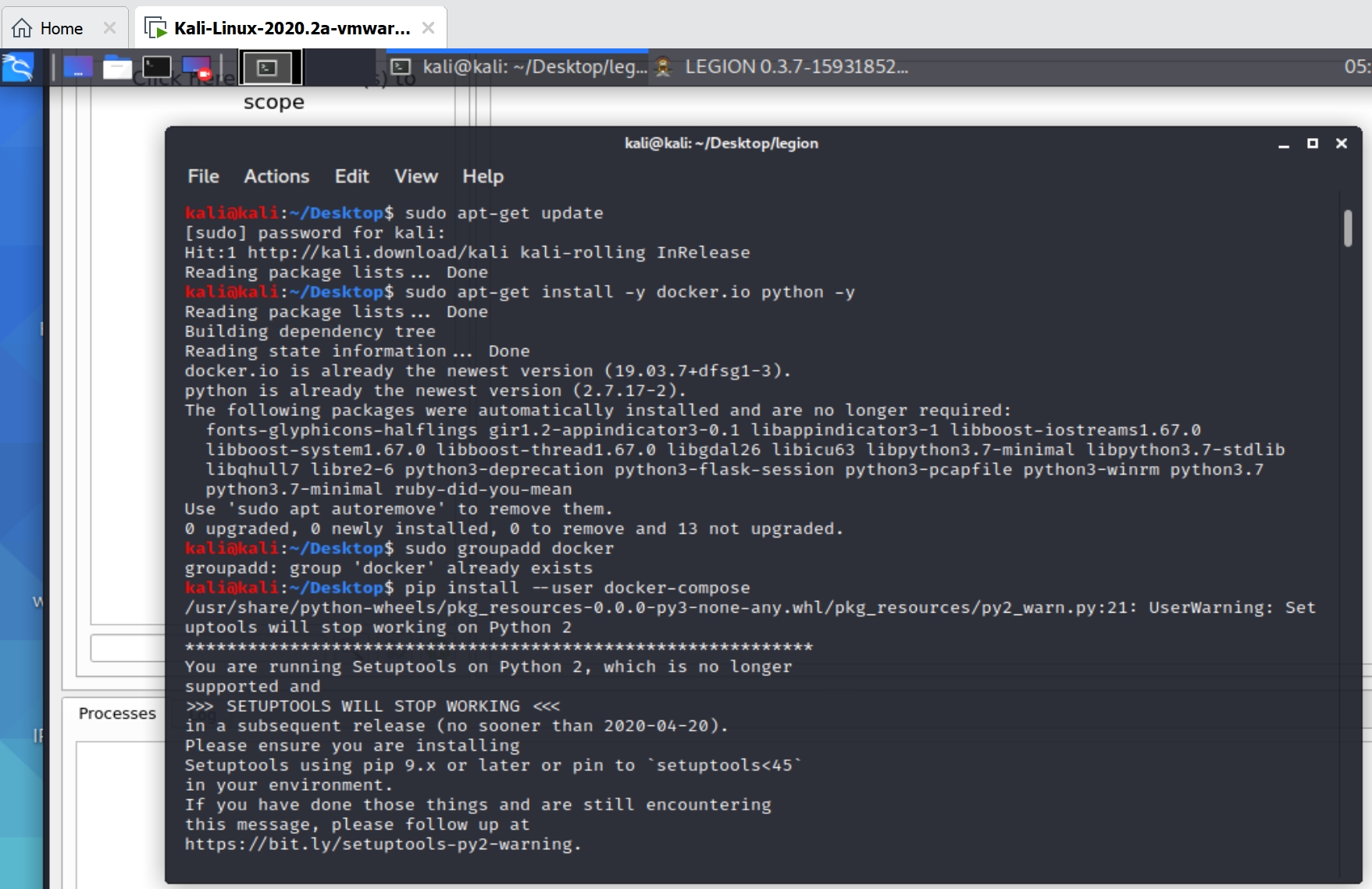
Legion:

Legion is another open-source framework that comes in both a command line and GUI format. It can be used for reconnaissance and to search for any vulnerabilities just like the previous tools. If you haven’t updated Kali recently, you can do so now, otherwise you can install Legion using the following command in the right order:

**sudo apt-get install -y docker.io python-pip -y**

**sudo groupadd docker**

**sudo pip install --user docker-compose**



Next, Legion will have to be cloned form the Github repository using the command:

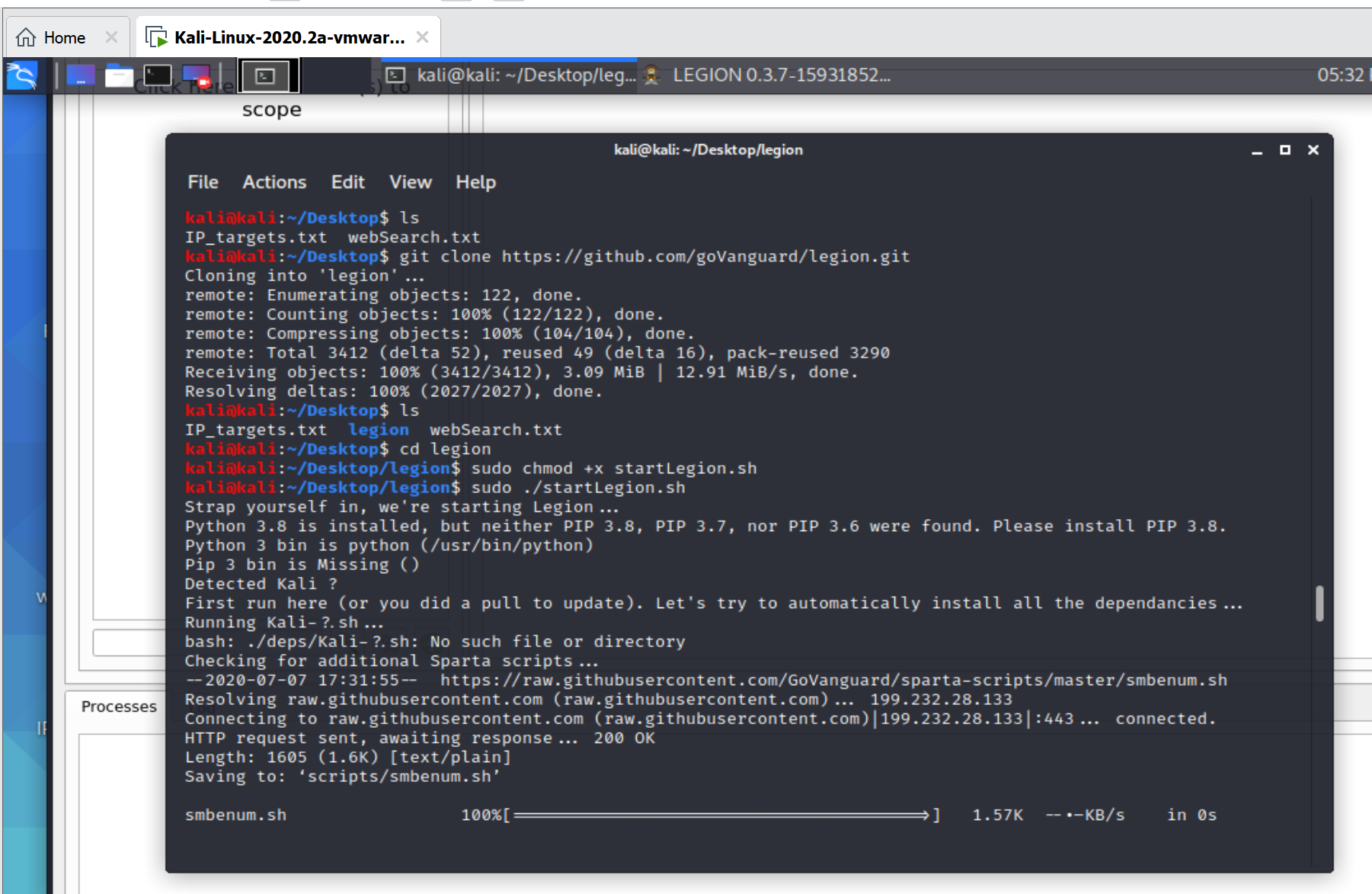
**sudo git clone** **<https://github.com/GoVanguard/legion.git>**

Once this completes, navigate to the docker folder and change the file permissions for the “runIt.sh” file to allow the user to execute the file. Afterwards, go ahead and the run the “runIt.sh” file. This can be done using the listed commands:

**cd legion**

**sudo chmod +x startLegion.sh**

**sudo ./startLegion.sh**



This will open a window for the GUI version of Legion which we can use to search and target ip addresses within a network. Being that we already know our victim’s ip address, let’s target that. Navigating to the left side of the screen and making sure that the “Hosts” tab within the “Scan” tab is selected, click within the window that displays “Click here to add host(s) to the scope” to open up a new window and add in your victim’s ip address. It is possible to change the type of scan by modifying the options here. If not already selected, change the following to those displayed below and select submit:

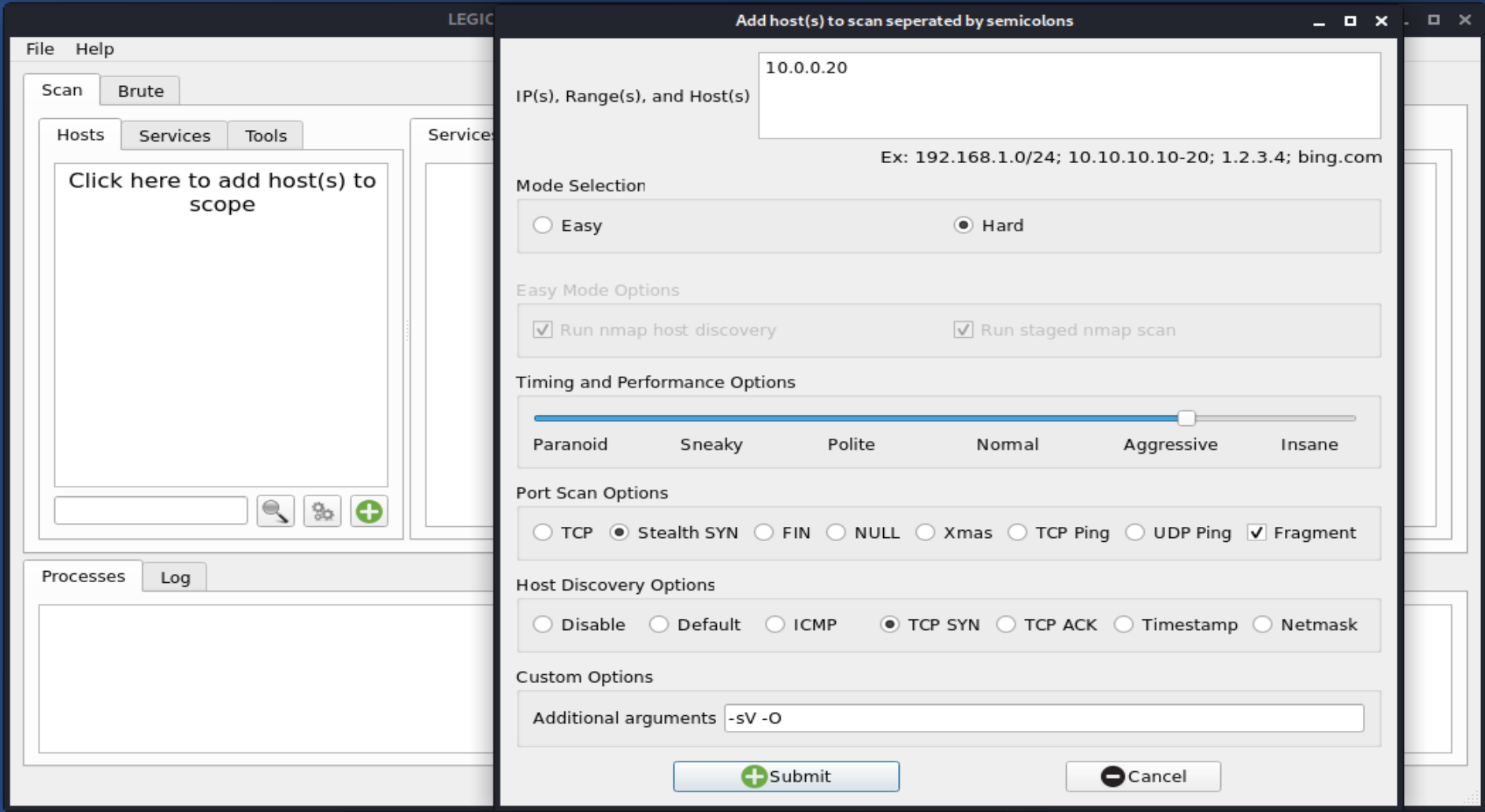
Mode Selecting: **Hard**

Timing and Performance Options: **Aggressive**

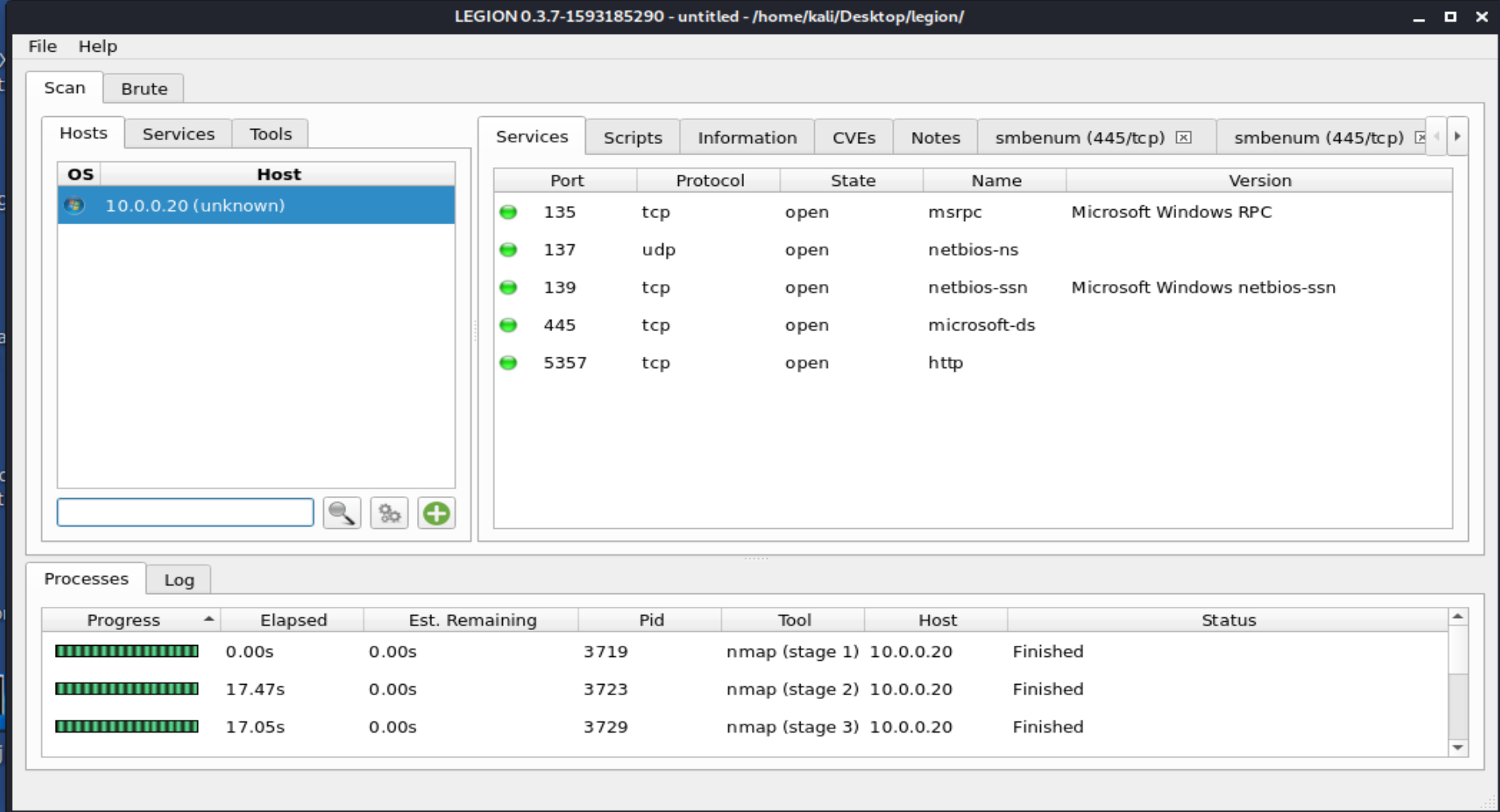
Port Scan Options: **Stealth SYN**

Host Discovery Options: **TCP SYN**

Additional Arguments: **-sV -o**



Like Nmap, Legion will display all the open network ports on the targeted ip address within the “Services” tab, which can be exploited using exploitation tools such as Metasploit.



Other than network ports, Legion provides additional data, such as the “Information” tab which displays the operating system running on the targeted machine or the “CVEs” tab which will show any common vulnerabilities that Legion had discovered regarding the target ip address.

All three of these vulnerability analyses tools, Nmap, Nikto, and Legion, are great tools used by professional pen-testers. These are tools can be used near the beginning of a pen-test to discover ip addresses on a network or to discover any open network ports and vulnerabilities on a target system, which can then be exploited using other industry tools.