2022

ARP POISONING
BLM 4011 Bil. Sis. Güv.

ON KALI LINUX (VM)

Contents

Figures Table

What you are expected to do: By reviewing this document and other resources, you are expected to have a good understanding of ARP Poisoning. You should come to the laboratory with your computer that has the Kali Linux operating system installed or by preparing an environment where you can run the applications that come with this system. You should be able to perform an ARP Poisoning attack on another operating system running a virtual machine. Before starting the attack, you should be able to predict the changes that will happen after the attack and show the state before the change. After the attack, you should be able to explain what happened. It should show whether we can perform some operations on the target machine after the attack and observe these operations from the attacking machine.

Note: Wireshark application, that has also been mentioned in this document, can be used to monitor network traffic, and apackets website can be used to visualize traffic.

Ne yapmanız bekleniyor: Bu dökümanı ve gerekli başka kaynakları inceleyerek, ARP Poisoning konusuna hakim olmanız beklenmektedir. Sanal makine uygulamalarından birini kurabilmeli, bilgisayarınızdaki Kali Linux işletim sistemini kullanarak veya bu sistemle birlikte gelen uygulamaları çalıştırabilecek bir ortamı bilgisayarınızda hazırlayarak laboratuvara gelmelisiniz. Sanal makinede çalıştırdığı bir başka işletim sistemine ARP Poisoning saldırısı yapabilmeli. Saldırıya başlamadan önce, saldırı sonrası olacak değişiklikleri önceden belirtmeli ve değişmeden önceki hallerini gösterebilmelisiniz. Saldırı sonrasında neler gerçekleştiğini açıklayabilmelisiniz. Saldırı sonrası hedef makinede bazı işlemler yapıp, bu işlemleri saldıran makineden gözlemleyip gözlemleyemeyeceğimizi göstermelisiniz.

Not: Ağ trafiğini izleyebilmek için dokümanda kullanılan wireshark, ve trafiği görselleştirebilmek için apackets web sitesi kullanılabilir.

Brief Explanation of ARP Poisoning

(ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address, and vice versa. Most commonly, devices use ARP to contact the router or gateway that enables them to connect to the Internet.

Any device on the network can answer an ARP request, whether the original message was intended for it or not.

For example, if Computer A "asks" for the MAC address of Computer B, an attacker at Computer C can respond and Computer A would accept this response as authentic.

ARP poisoning is when an attacker sends falsified ARP messages over a local area network (LAN) to link an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is linked to an authentic IP address, the attacker can receive any messages directed to the legitimate MAC address. As a result, the attacker can intercept, modify or block communicates to the legitimate MAC address.

Since the attacker puts itself between the target and the router, this attack type is also called Man in the Middle (MitM) attack.

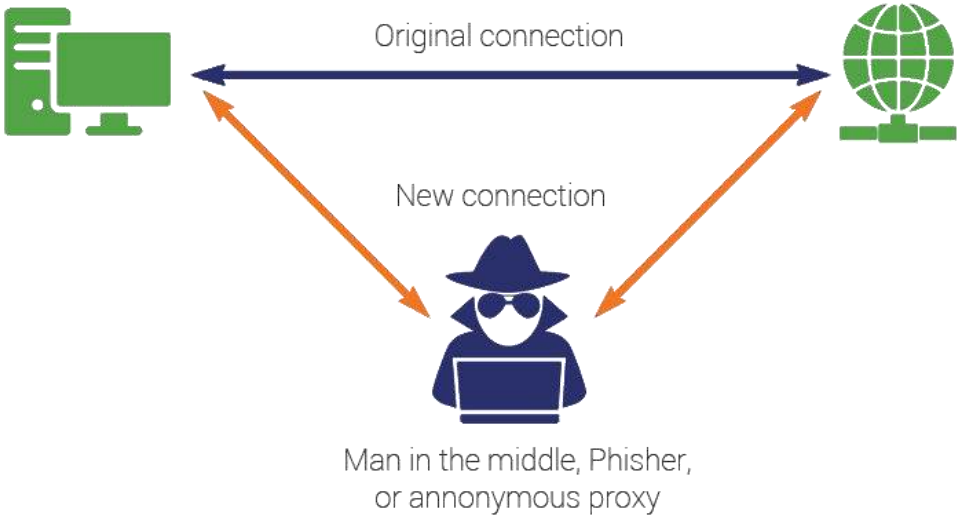

Figure 1: Man in the Middle attack or ARP Poisoning

ARP Attack Testing

To test this attack safely, we can download a piece of software that lets us emulate a computer inside our computer.

Installing Virtual Box (optional)

There are a few Virtual machine programs out there, but Virtual Box was what used in this document.

From the website https://www.virtualbox.org/ one can download and use Virtual Box freely.

For this laboratory application, the attacker machine will be a Kali Linux virtual machine while the target will be a standard Windows computer. For testing purposes, we will also build this target PC into the virtual box.

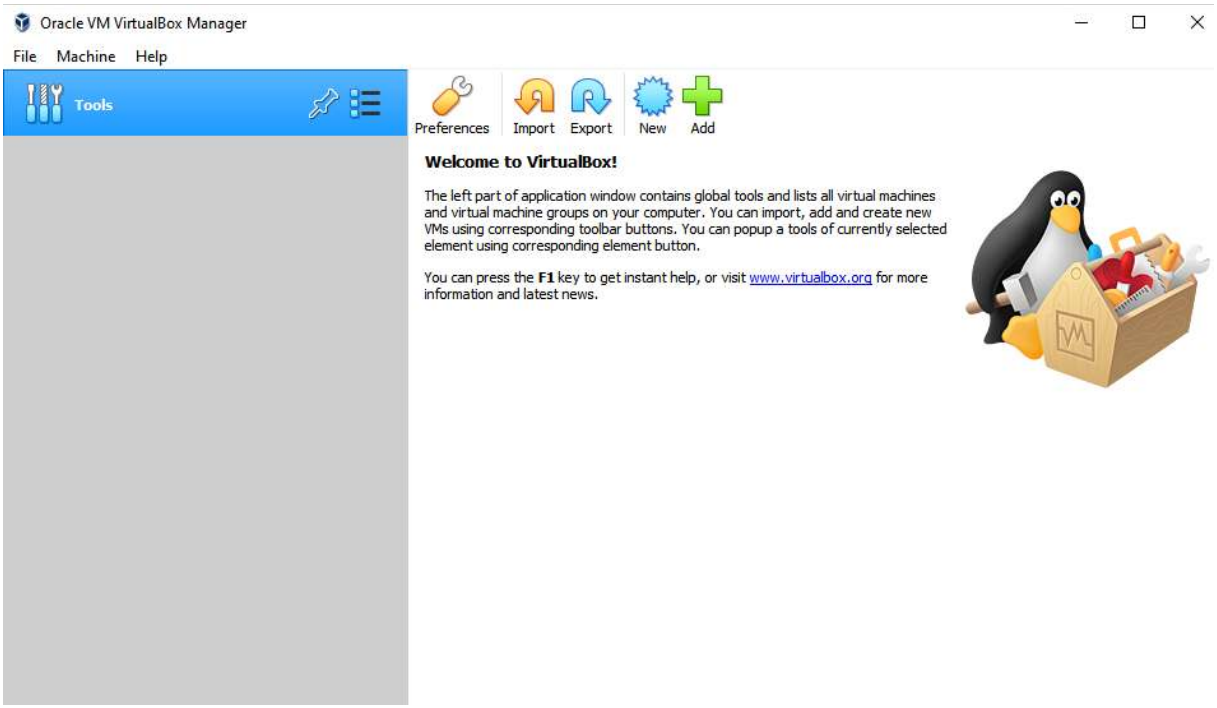

Figure 2: Virtual Box interface

By clicking new, a window will pop up. From there name the VM as target to eliminate confusion later. For this lab it will be a 32 bits windows 10 machine (you can download the iso file from Microsoft website).

From the window after naming the VM, press next and you can allocate a memory to this VM. From this window you can decide how much RAM you are willing to give to this VM from your physical PC. 1GB of RAMs is enough for this application. After that, click next and it will ask for creating a virtual hard disk. The default selection here is creating a virtual hard disk. Leave it at that and click create. Then another window will ask about the hard disk type. Default selection here is VDI. Leave it at that and it will ask about memory allocation. Leave it at the default selection, which is dynamically allocated, and it will ask for a storage space. 50GB is more than enough for this application. Finally clicking create, our VM is ready, except for operating system.

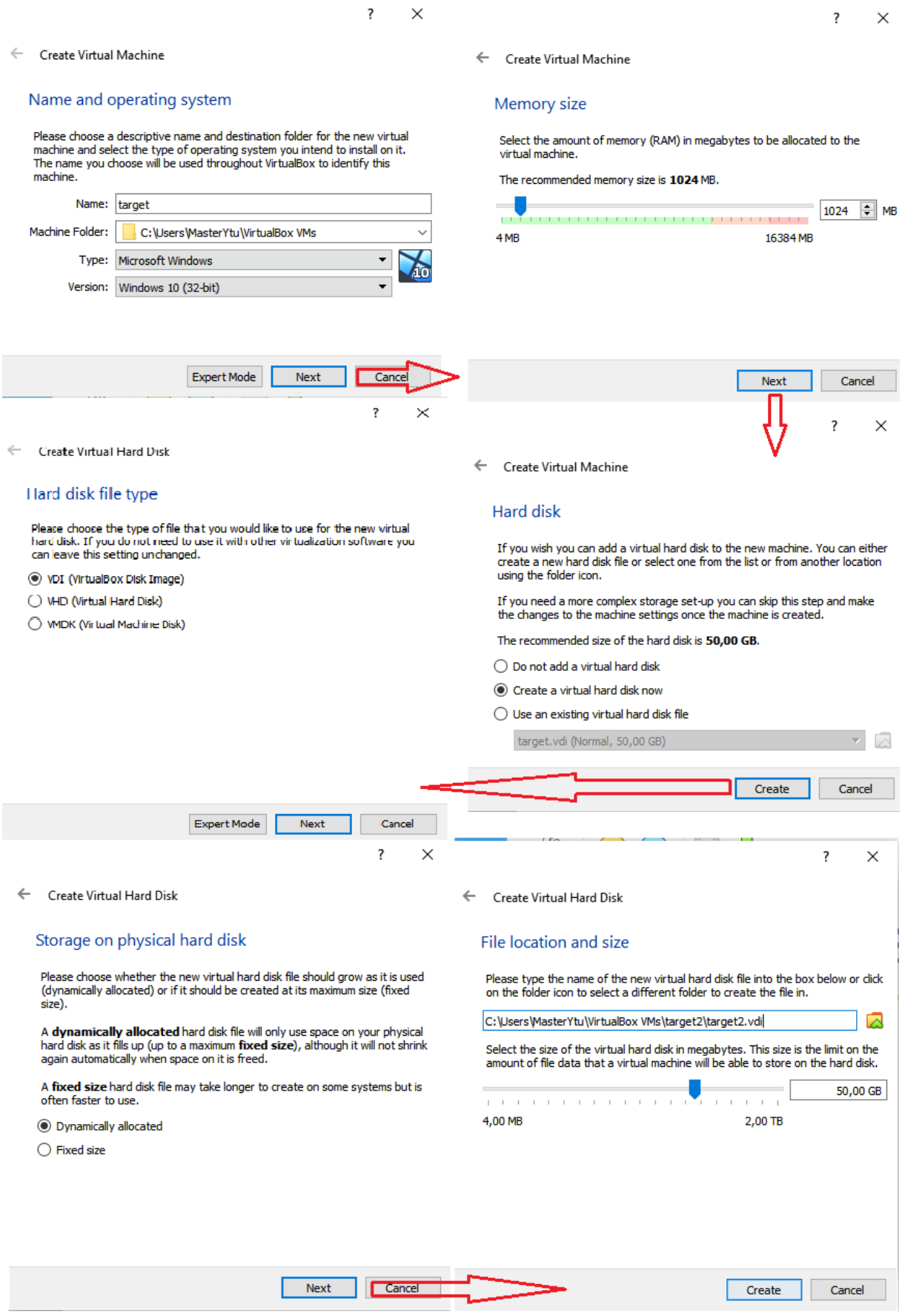

Figure 3: steps of creating a Virtual Machine

Upon first running your VM, it will ask for an operating system. Browse for the win10 iso file you downloaded before and select it. After the necessary setup procedures, out target PC is ready to go.

Installing Kali Linux (on a virtual machine)

From the website https://www.kali.org/ downloading the virtual machines version, it will download a ready-to-use virtual machine version kali linux on your computer.

From the Figure 2 simply clicking on “add” and selecting the downloaded “virtualbox machine definition” file, it will be ready to use.

With the installation of both target and attacker, we should have a sight like this:

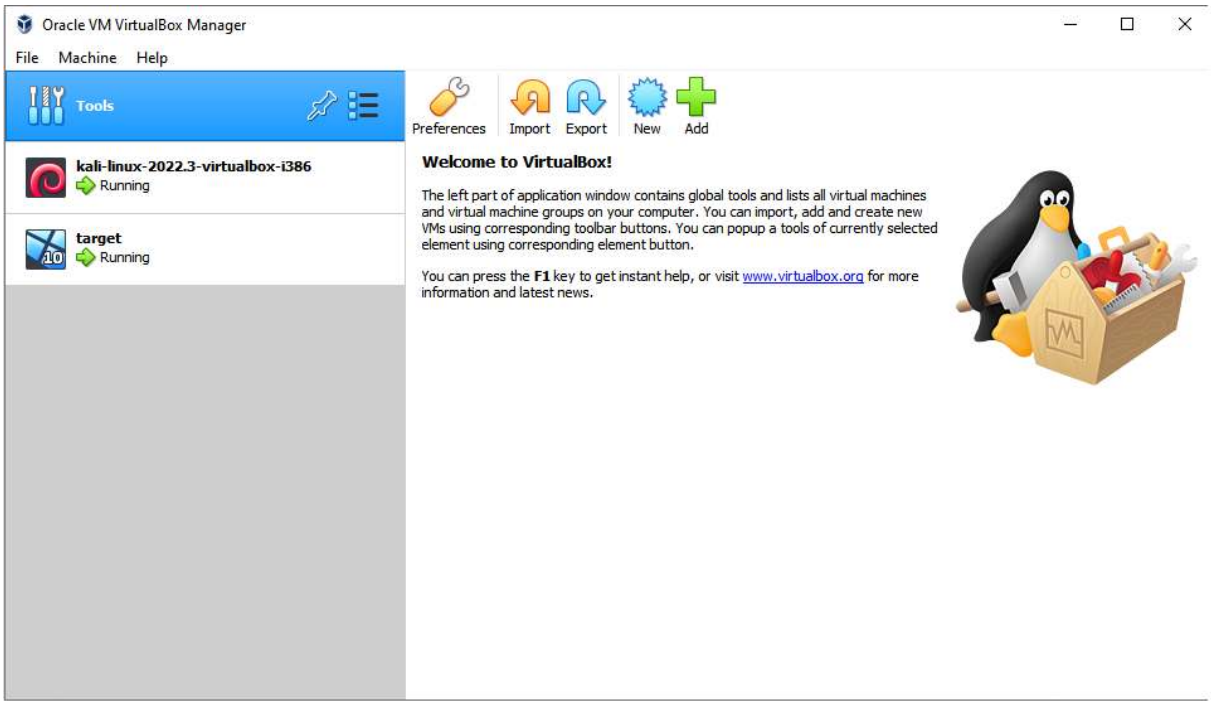

Figure 4: attacker and target as virtual machines

Initiating the Attack

Before starting to attack the target, we should change the network settings of attacker and target. To do that, click on the target>settings>network>attached to: [nat -> bridged].

And we should do the same thing for the attacker.

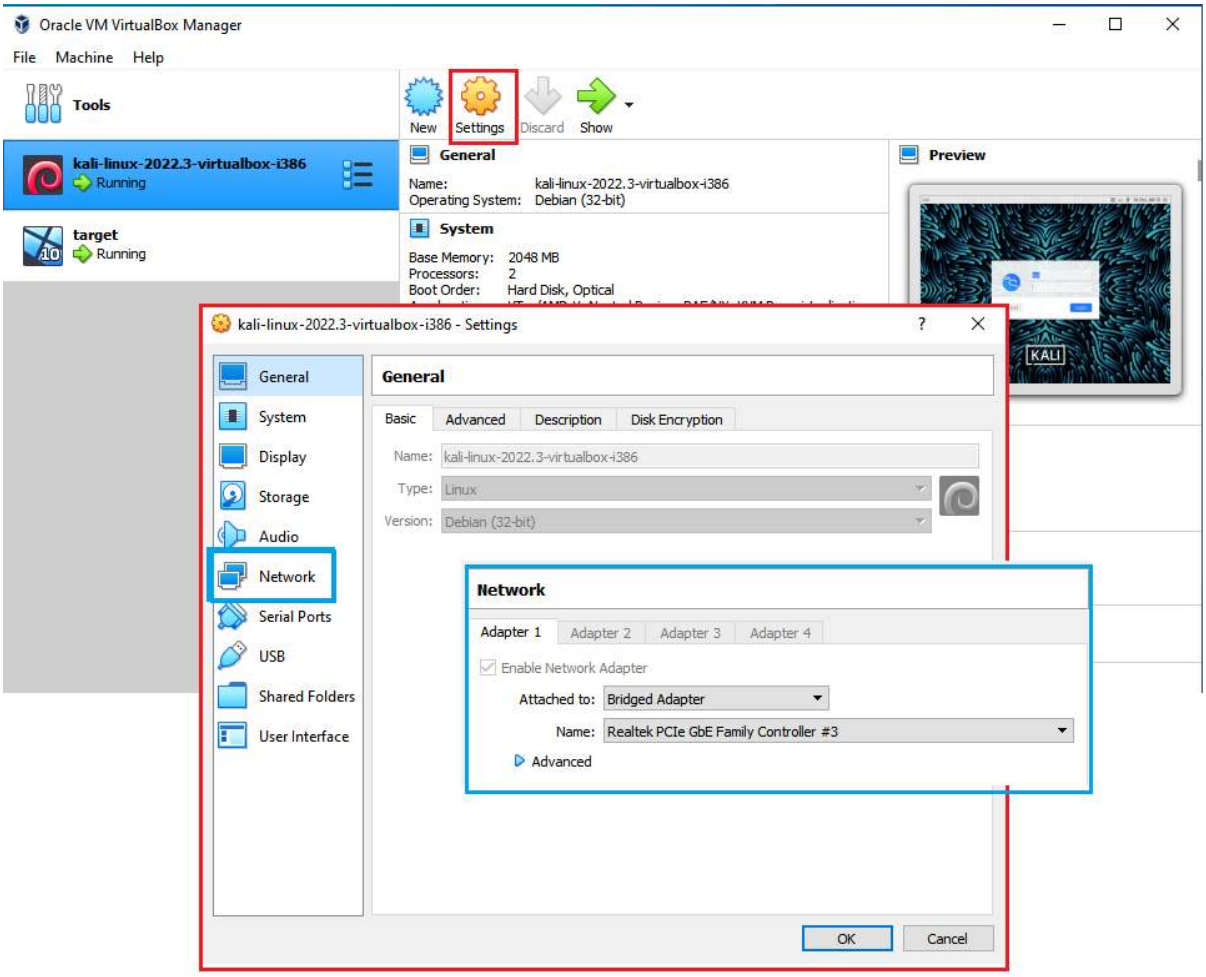

Figure 5: changing network settings of virtual machines

Target Info

To get the IP address of the target (in this example, windows), search>cmd>{ipconfig}.

This search will yield to a similar window shown down below:

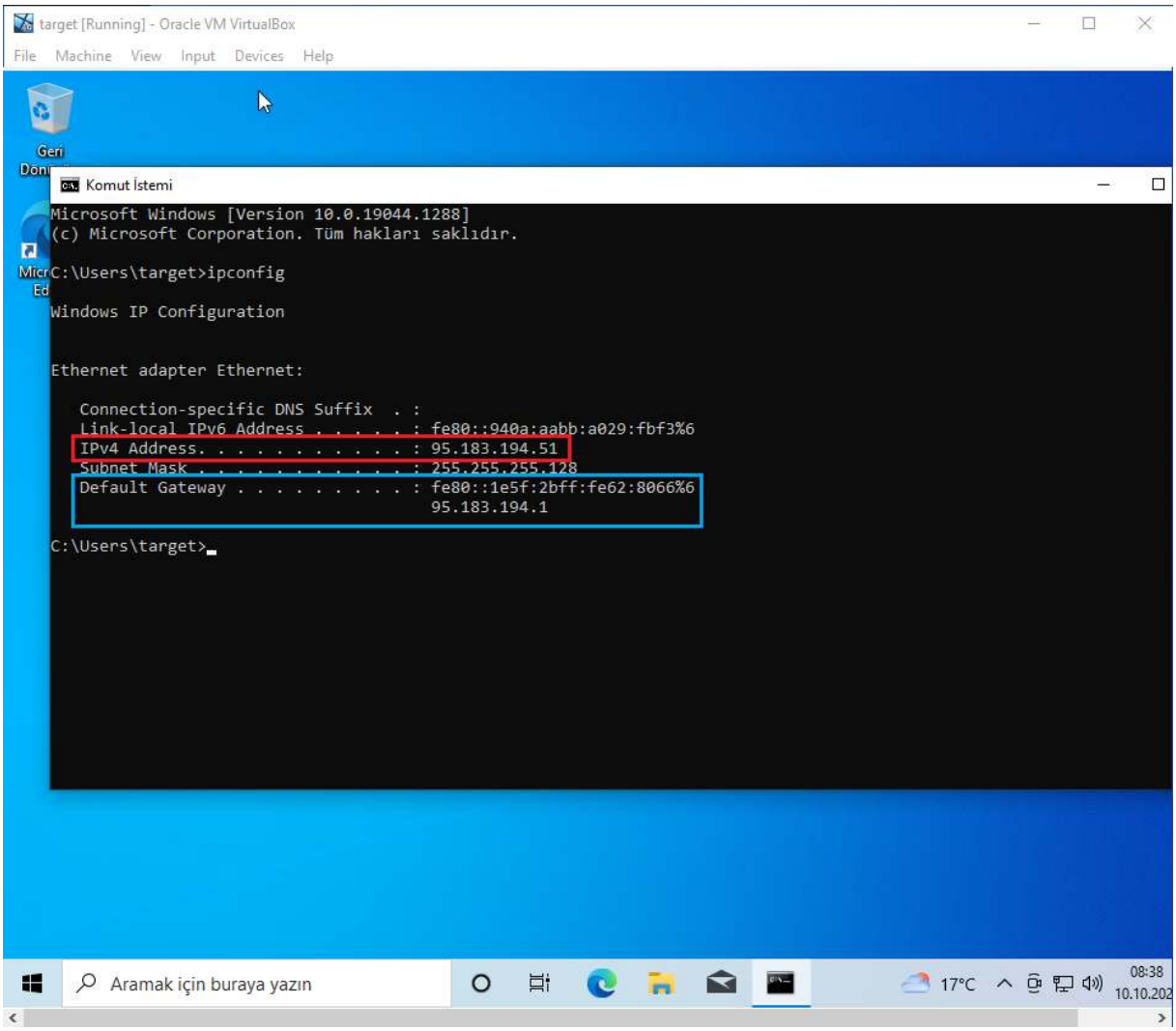

Figure 6: red line marks the ip of the virtual machine target while blue line marks the ip address of the default gateway or router

Using the same command window, we can also see the mac address of the gateway by typing {arp -a}

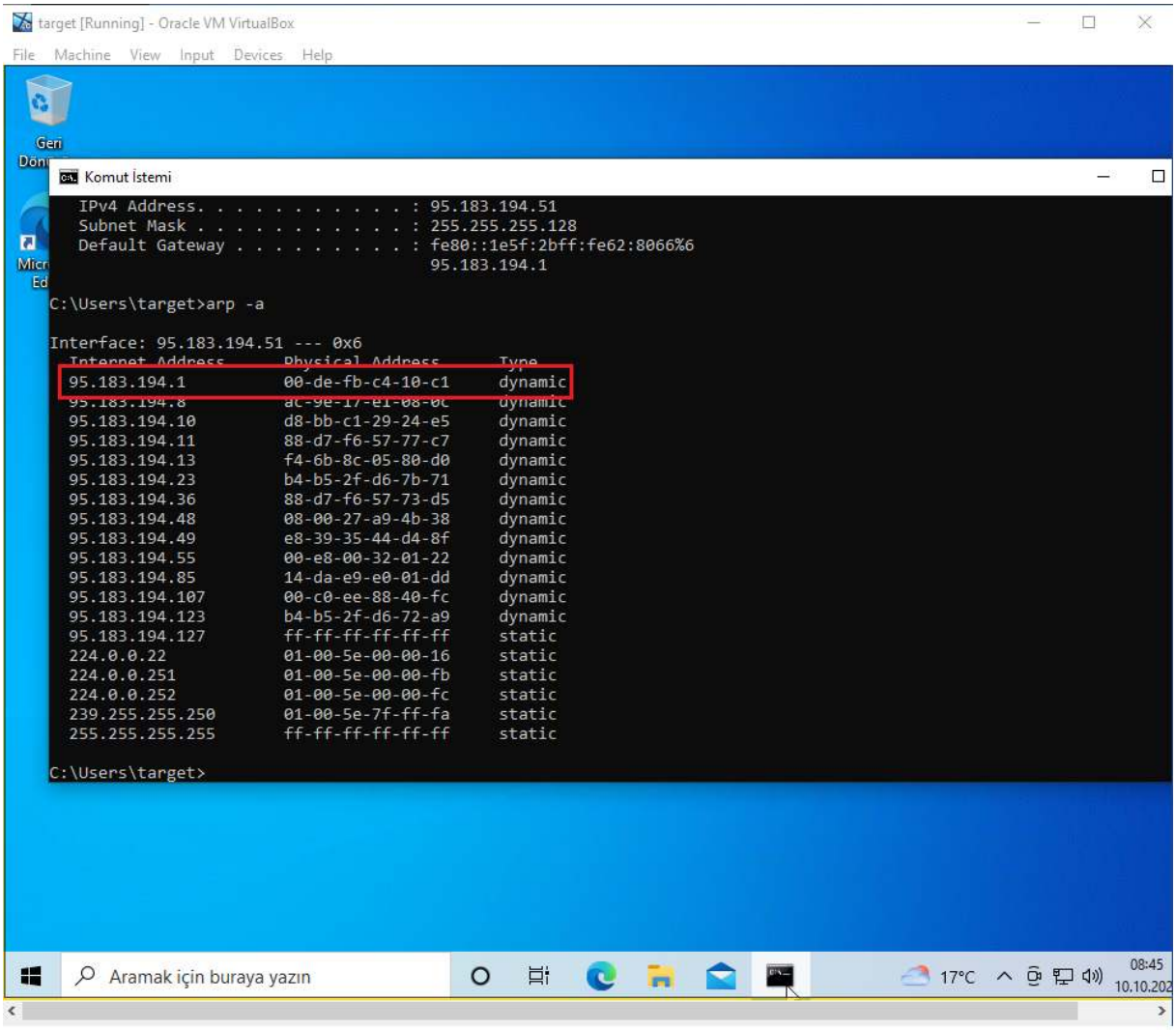

Figure 7: following the ip address of the gateway (95.183.194.1) we can see its mac address. Red line marks the mac address of the router

Attacker Info

To get the ip address of the attacker (kali), root terminal emulator> (it would ask the password) > {ifconfig}

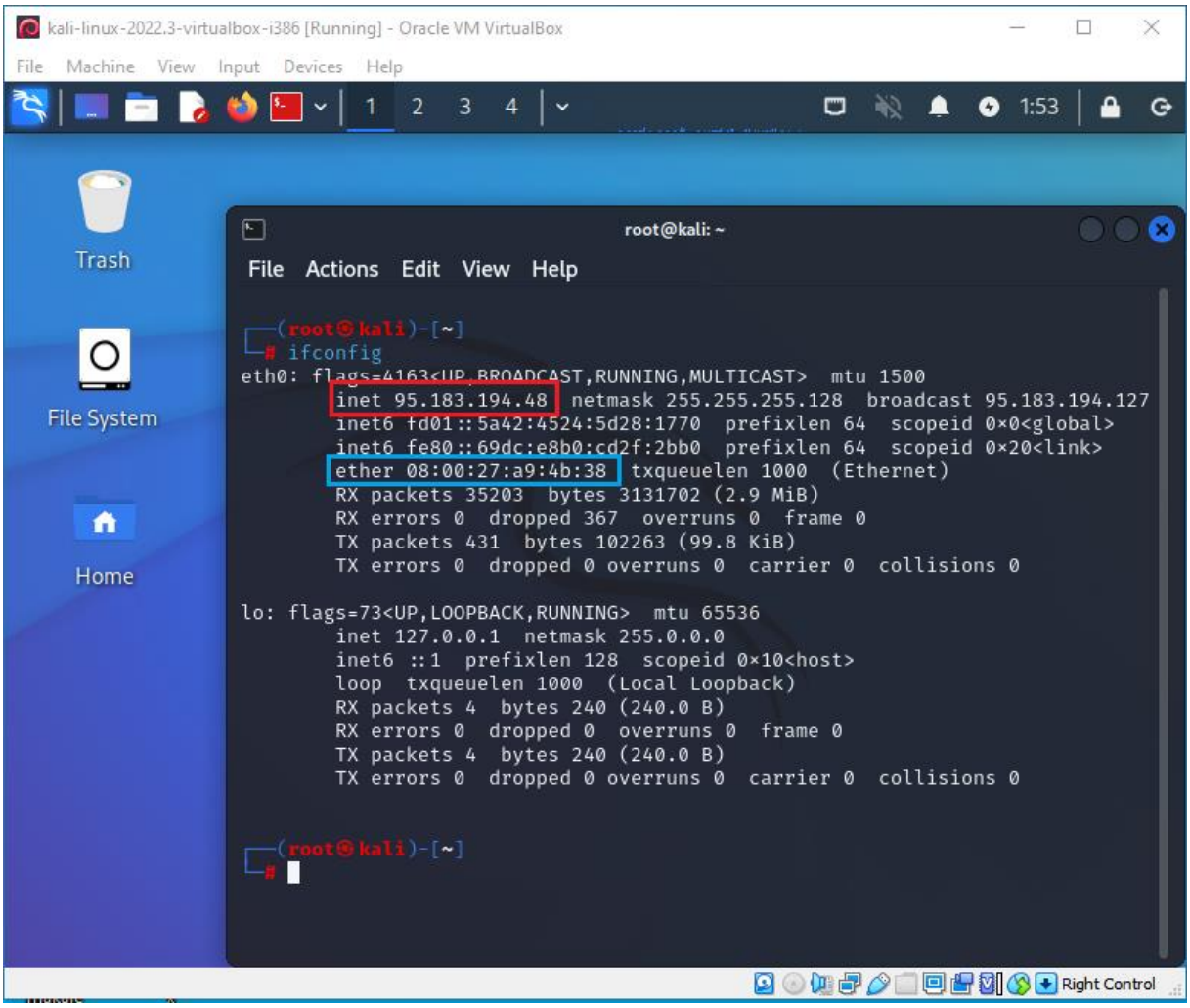

Figure 8: red line marks the ip address of the attacker, and blue line marks the mac address of it

Ettercap as an Attack Tool

This distribution of kali linux supports graphical version of Ettercap. To access Ettercap, go to Applications>sniffing & spoofing > Ettercap-graphical (here it might ask for a password).

This will start Ettercap.

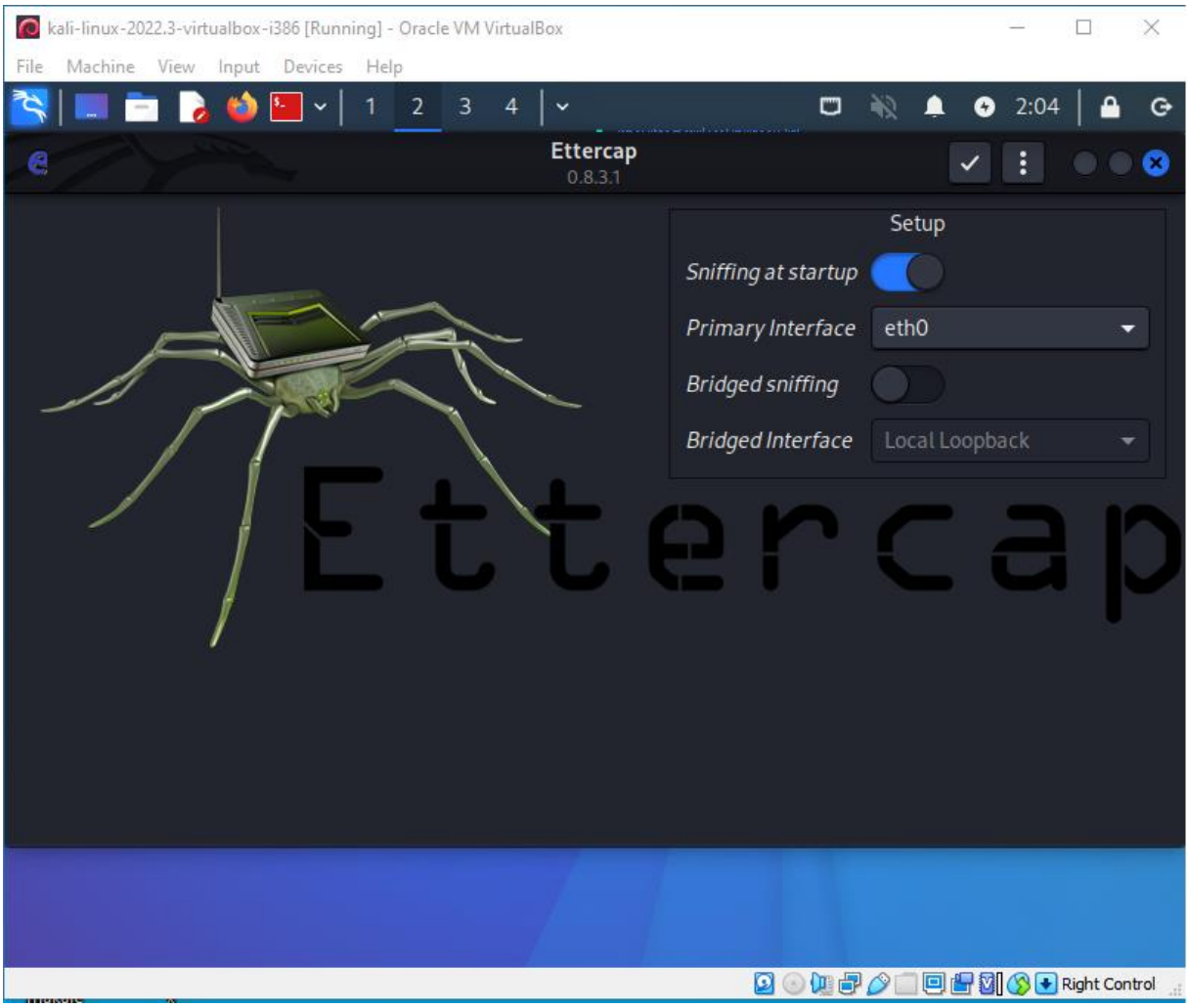

Figure 9: ettercap interface

Sniffing at startup will allow Ettercap to scan the network at start hence allowing us to see the host list.

To access the host list, see the image down below:

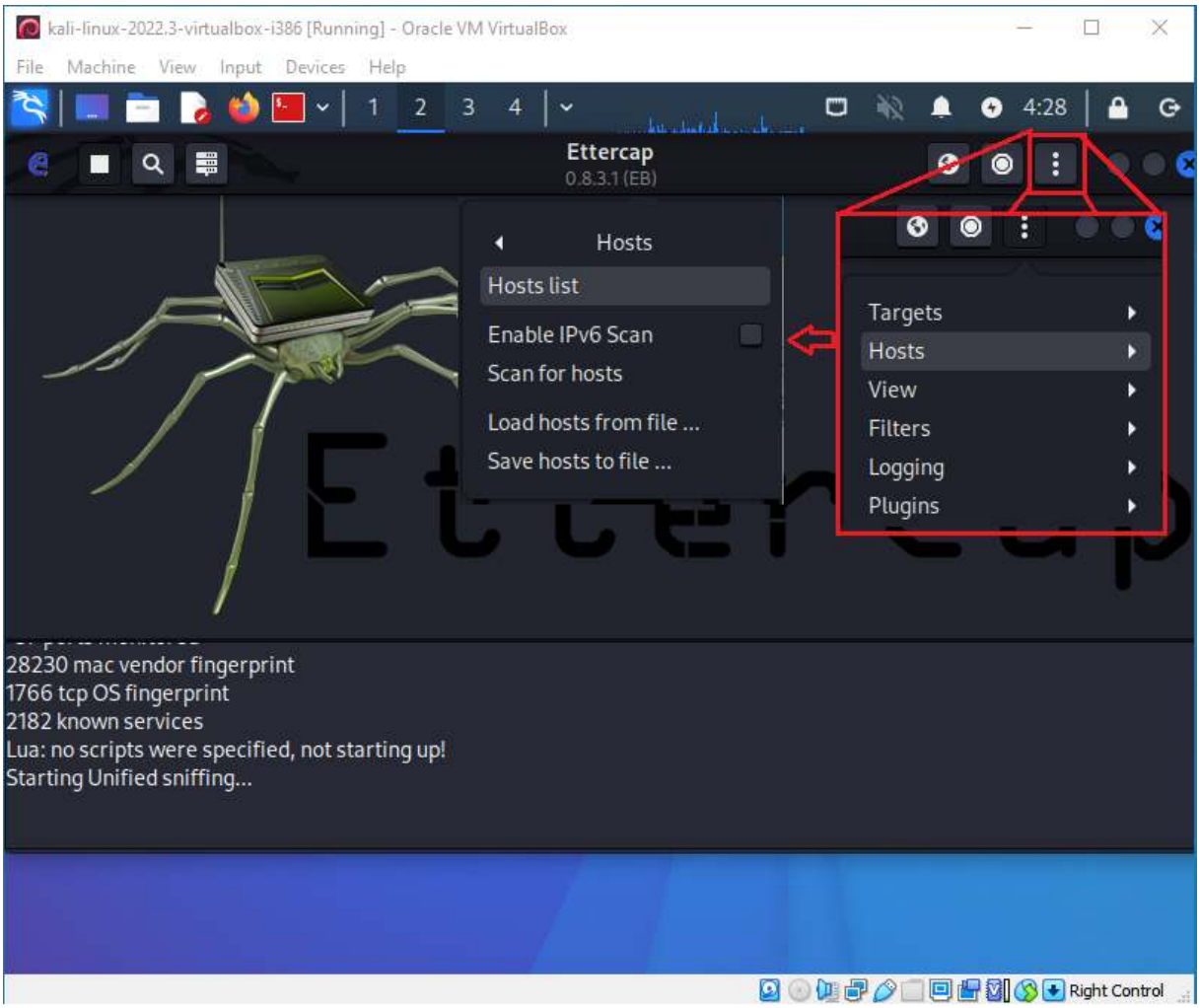

Figure 10: 1) click on the three dot on upper right corner. 2) click on hosts. 3) click on hosts list

We can also scan for hosts from here as shown in the Figure 10.

This will reveal the hosts list as shown in the image down below:

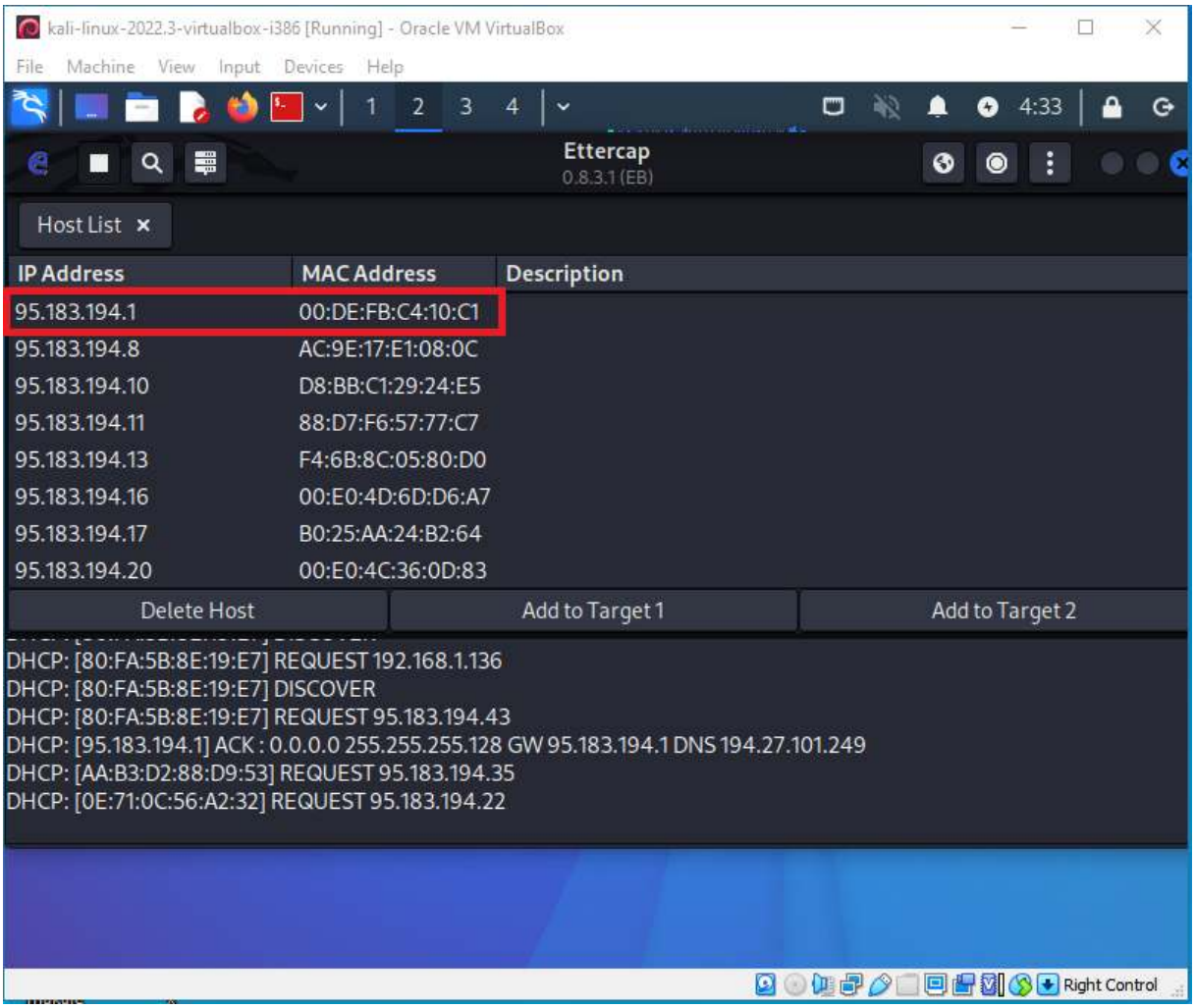

Figure 11: hosts that were revealed in the sniffing. You can also scan for hosts from the previous menu

From this host list we can see our targer's IP address as well as the ip address of the router. If you pay attention to Figure 11, both the ip number and mac address of the default gataway is marked with red. Scrolling down reveals the ip of the targer as seen down below:

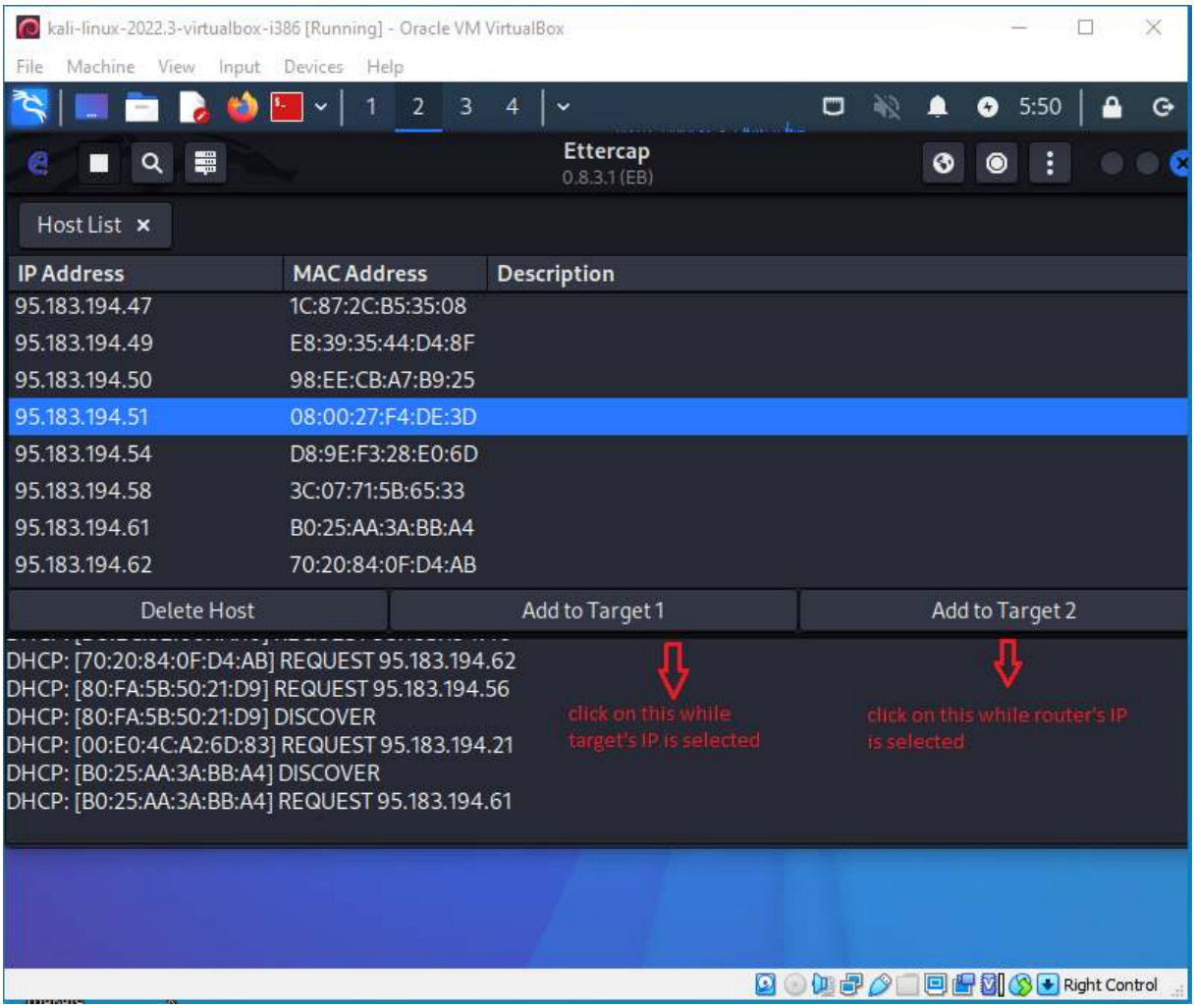

Figure 12: IP address of the target can be seen on the hosts list

To start the ARP poisoning (or MITM) attack, simply add your target as target 1, and add the router as target 2.

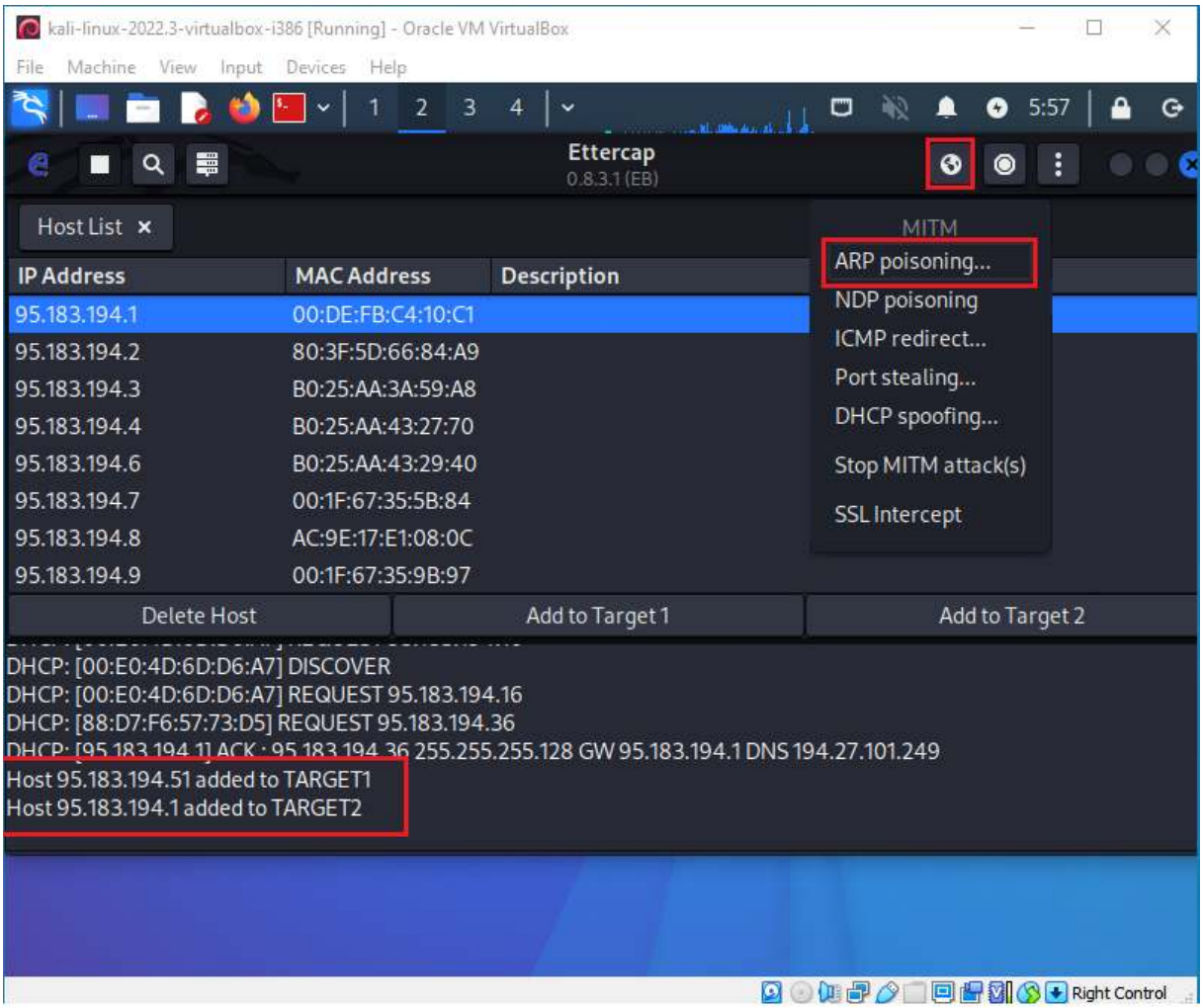

Figure 13: adding target as target 1 and router as target 2

After adding your targets press on MITM menu and select ARP poisoning. This will conclude our attack.

Aftermath

After applying steps discussed above, time to check the target. Again, with typing “ipconfig” and “arp -a” on the command window, we can observe recently - attacked target.

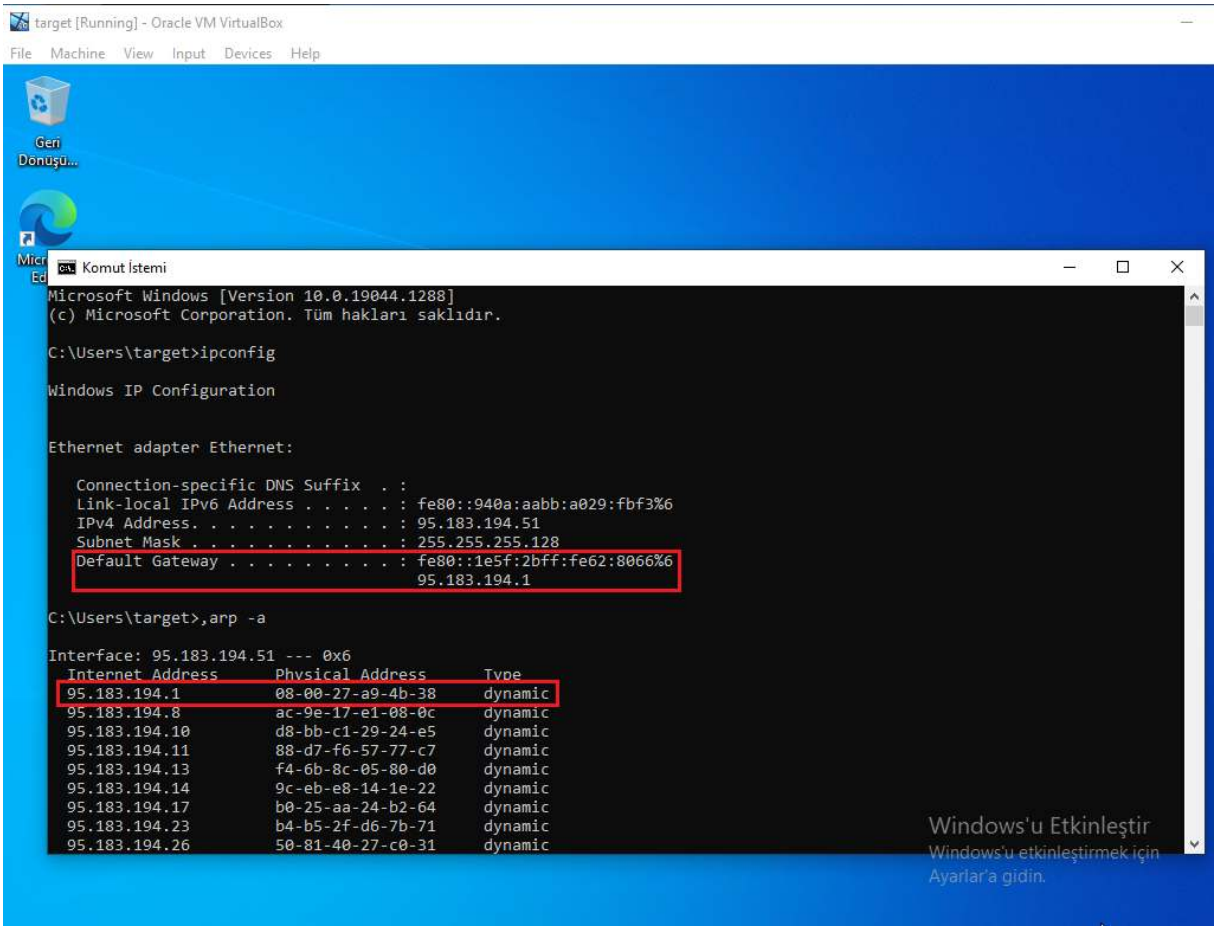

Figure 14: after ARP poisoning attack the ARP cache of the target

After observing the router MAC address, we can see that the MAC address changed from “00-DE-FB-C4-10-C1” (see Figure 7) to “08-00-27-A9-4B-38” which was the MAC address of the attacker (see Figure 8).

Monitoring the Target with Wireshark

Wireshark is the world’s foremost and widely-used network protocol analyzer. (Wireshark · Go Deep.). This program comes with kali linux. To open it, applications>{wireshark}.

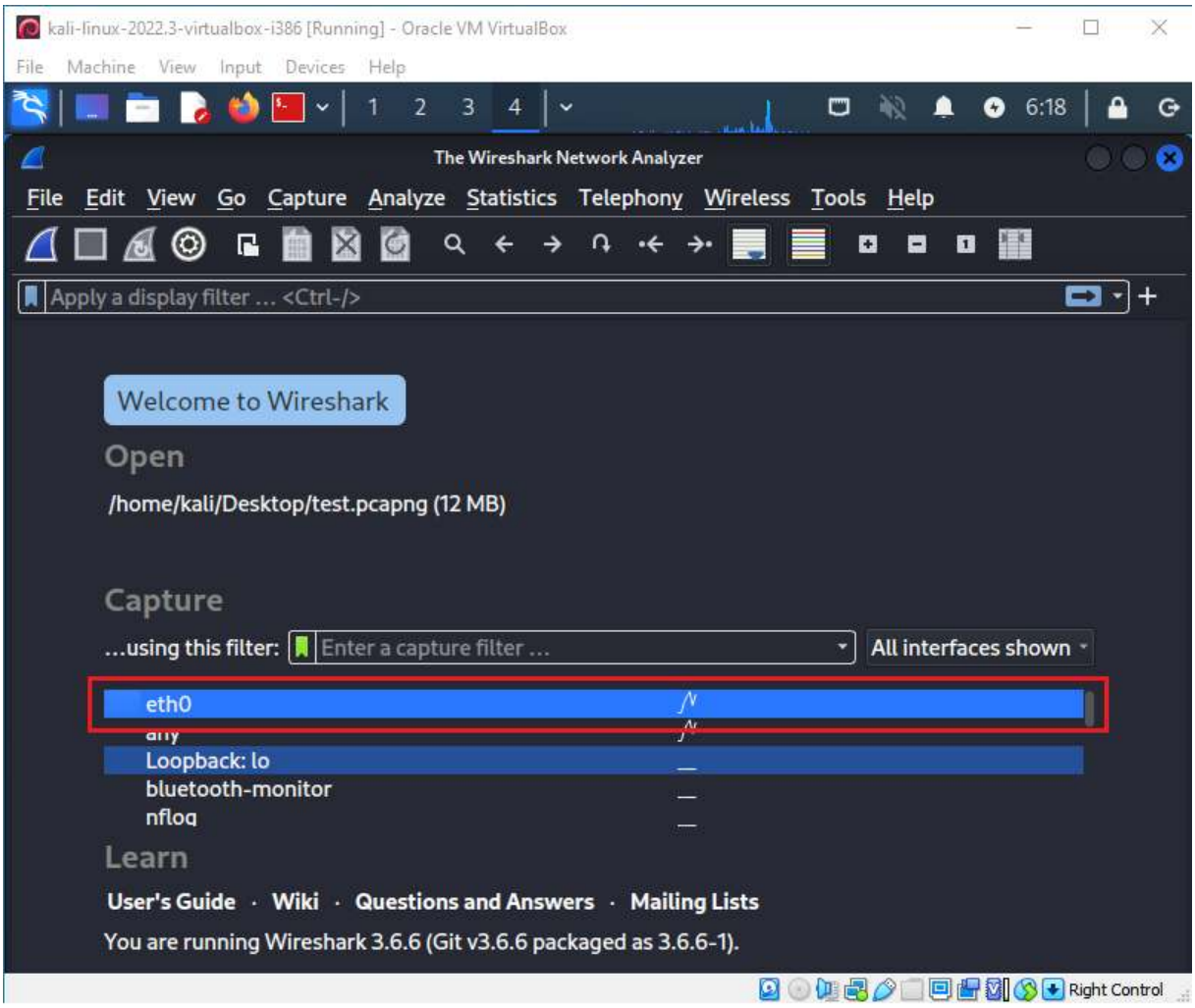

Figure 15: wireshark interface

Click on the name you see on the “primary interface” (see Figure 9) on the ettercap interface. This will start the listening of the network.

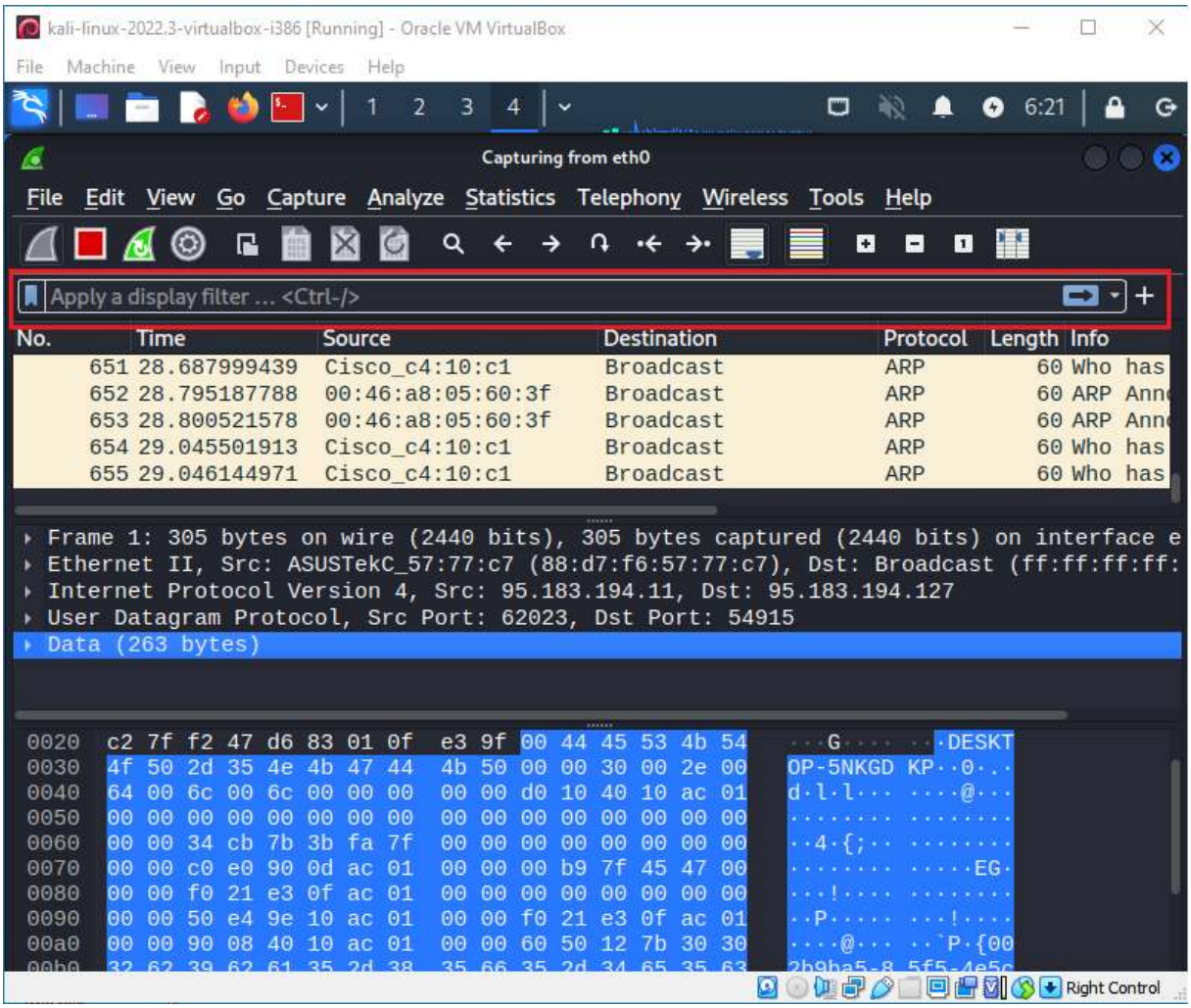

Figure 16: you can apply filters with the red-marked panel

Wireshark listens to all the network, but we are only interested in out terget. So using the filter option we can focus solely on the target.

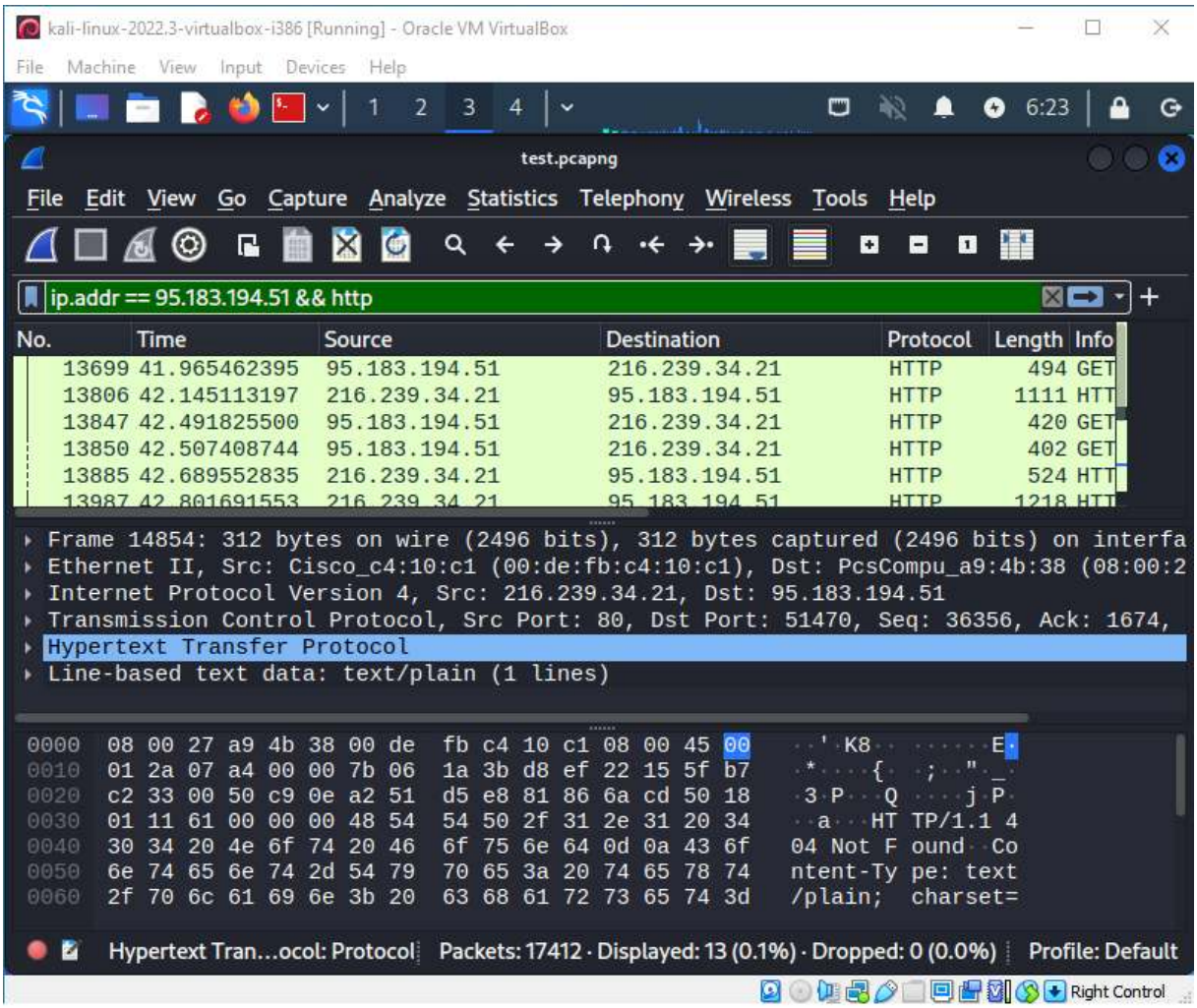

Figure 17: filtering the wiretapping by the address and protocol

With this filter we are only seeing network traffic from the target and further filtering with the http protocols only. Since HTTPs protocols are encrypted, listening to those traffic is useless.

View the Conversation

Using a website called “apackets.com” we can take a look at what we gathered by attacking the target.

First, save the network trafic of that target from wireshark as pcapng file.

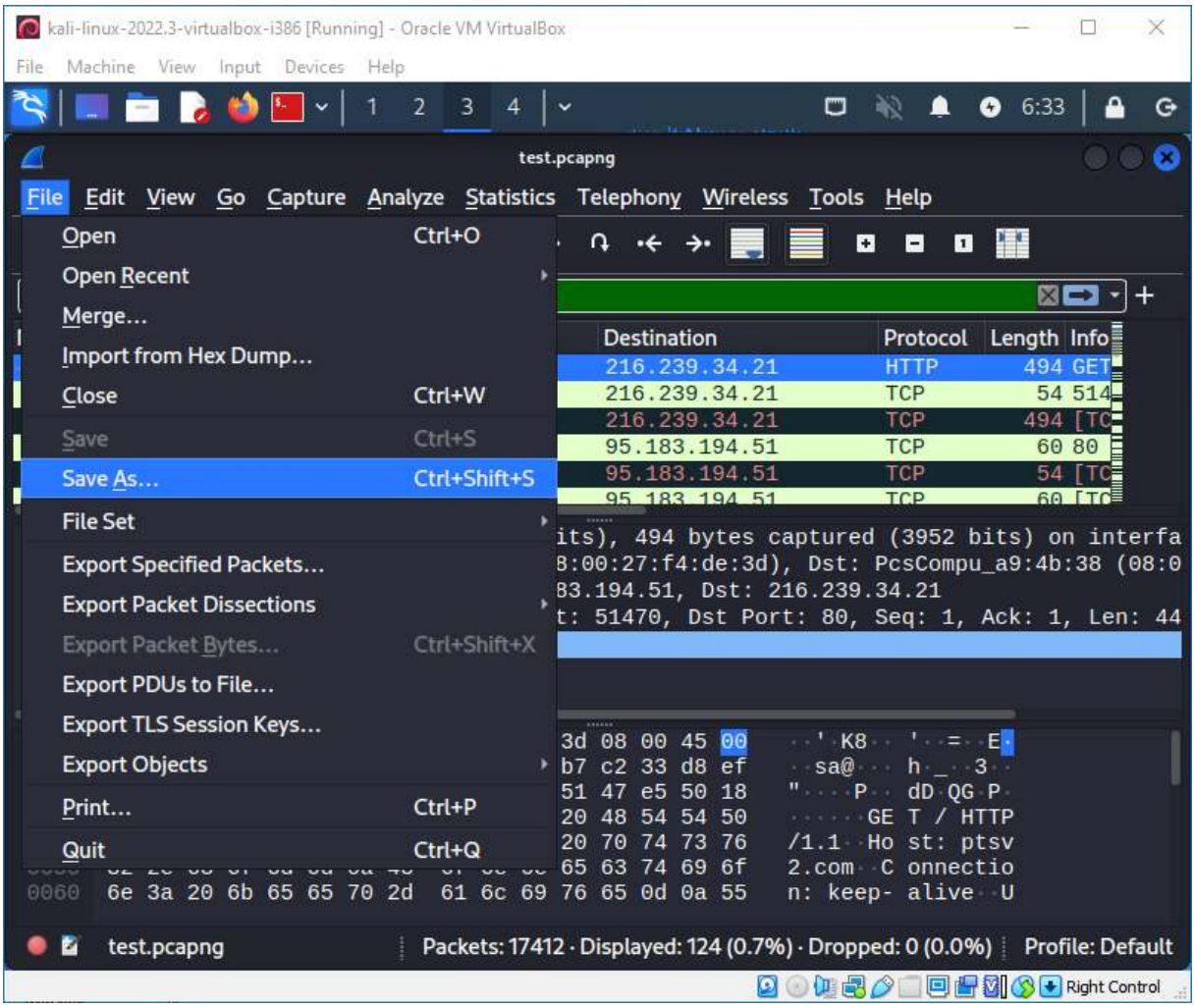

Figure 18: save the capture as pcapng file

Then go to the website “apackets.com”

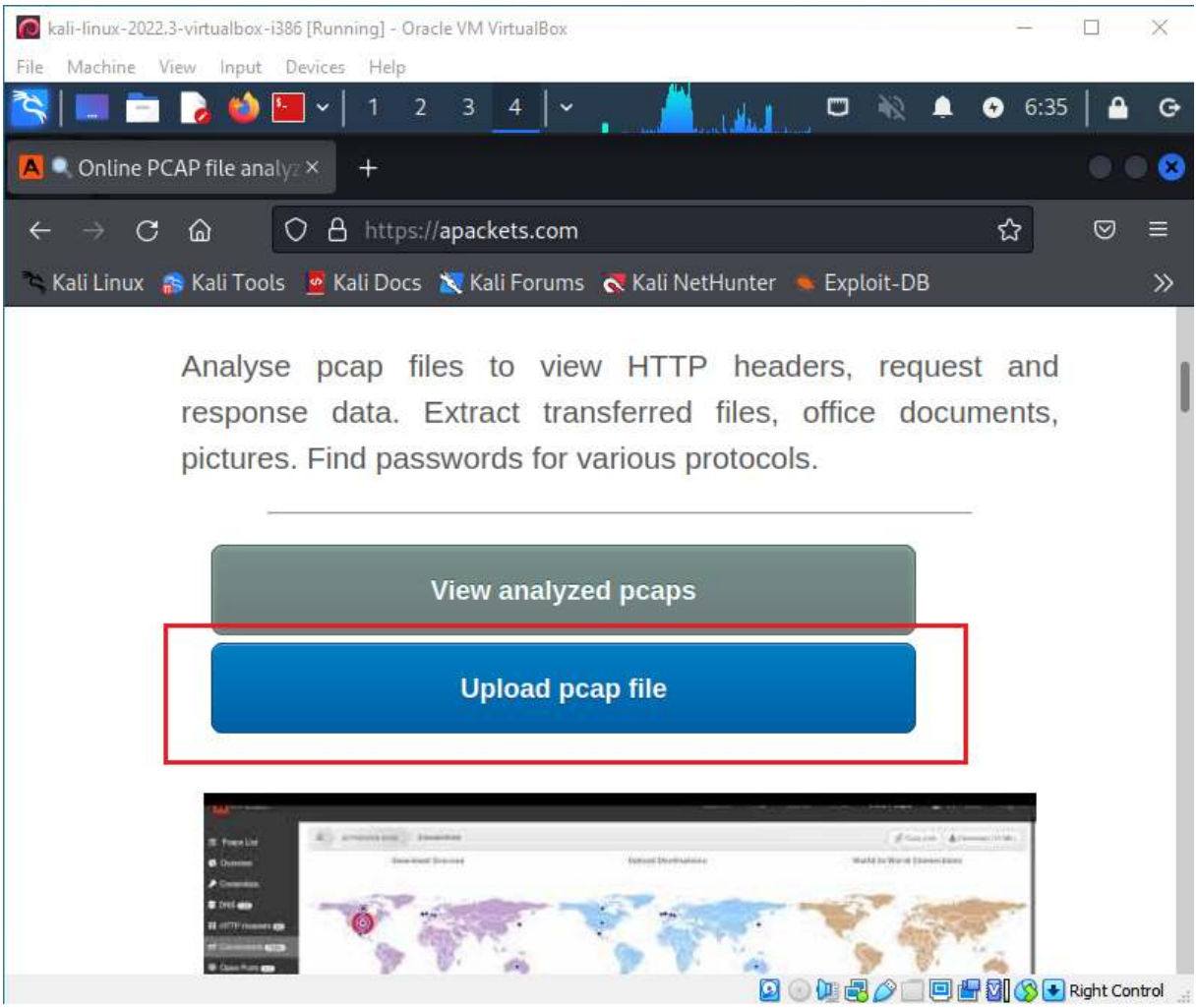

Figure 19: apackets.com to analyze the captured traffic

Upload the saved file and view report. From here the attacker can check various things such as websites the target connected to, requested the target sent, responses the target got etc.

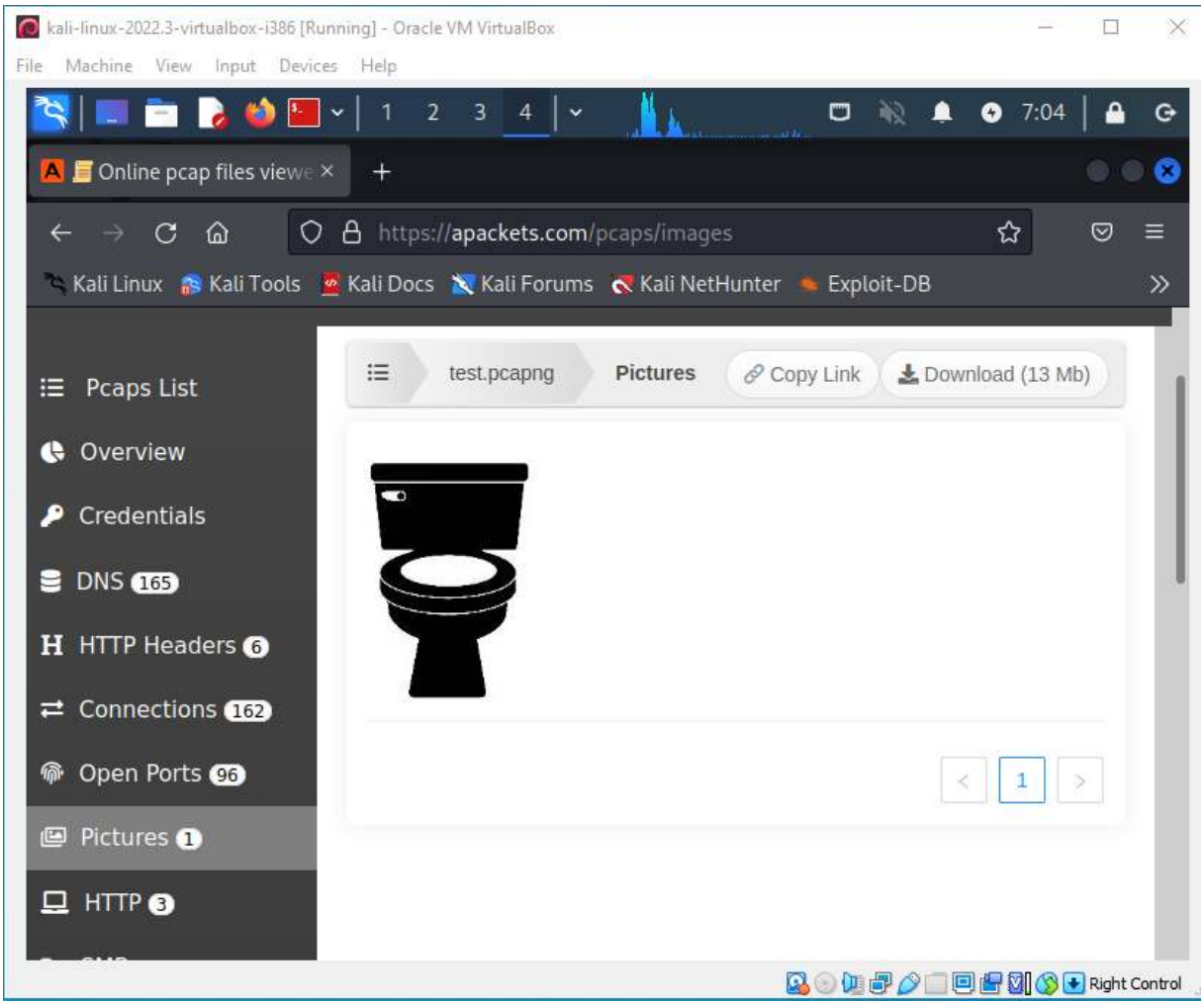

Figure 20: attacker can even chek some pictures the target viewed. This is the logo of the website http://ptsv2.com/

Since the attacker can only see HTTP connections clearly, for test purposes one of the HTTP websites [PTS - V2 (ptsv2.com)](ptsv2.com) was wisited. The logo of the website can be seen in Figure 20 above.