الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Projet de Fin de Cycle

En vue de l'obtention du Diplôme de Licence
Filière : Télécommunication

Présenté par

SARAOUI Lamia

&

ABDALLAH ELHIRTSI Raouf

&

YAHIAOUI Raiane

Design and implementation of a Trojan Horse "ProRat"

Proposé par : AMALO Warda & BERSALI Mahdi

Année Universitaire 2021-2022

Acknowledgment

Let us begin by thanking God the Almighty for blessing us with health and strength to make this modest work.

Secondly, we would like to express our sincere thanks to our promoter Miss Warda AMALOU, who has entrusted us with this subject and the interest she has shown in our work, which has been a great help and which has enabled us to complete this work.

At the same time, we would like to thank Mr Merouane MEHDI and Ms Zeyneb BERKAT for their help and precious advice.

We thank Mr Sami HEBIB for his guidance, moral support and encouragement, which have been a considerable contribution without which this work could not have been carried out in the right way.

Our sincere thanks also go to the members of the jury for their interest in our research by agreeing to examine our work and to enrich it with their proposals.

Finally, we would also like to thank our families and friends, and all those who participated in this work from near and far.

ملخص:

RAT(الوصول عن بعد) هو برنامج ضار يتضمن بابًا خلفيًا للتحكم الإداري في الكمبيوتر الهدف. في هذا العمل ، أجرينا سيناريو هجوم لحصان طروادة يسمح للمتسلل بالوصول إلى الجهاز المستهدف عن بُعد من خلال حصان طروادة مخفي داخل صورة أرسلها المتسلل إلى الهدف. عند تنفيذ الهدف لهذه الصورة ، سيعمل حصان طروادة في نفس الوقت. أثناء هذا التنفيذ ، سيتم تنفيذ تكامل النظام في سجلات Windows الخاصة بالبرامج الضارة. نحدد في إعدادات الشبكة عنوانIP يدويا ، الذي يربط جهازي كمبيوتر ، من خلال شبكة إيثرنت.

كلمات المفاتيح: حصان طروادة، مخترق، هجوم، متسلل، ضحية، مصاب، مستهدف، برنامج ضار، IP

Résumé :

Un cheval de Troie de type RAT (accès à distance) est logiciel malveillant qui comprend une porte dérobée pour le contrôle administratif de l'ordinateur cible. Dans ce travaille nous avons mené en place un scénario d'attaque d'un cheval de Troie qui permet au pirate d'accéder à la machine cible à distance grâce à un cheval de Troie caché à l'intérieur d'une image envoyée par le pirate à la cible. A l'exécution de cette image par la cible, cela s'exécutera en même temps. Lors de cette exécution une intégration système dans les registres de Windows du programme malveillant sera effectuée. dans les paramètres du réseau nous avons déterminé l'adresse IP manuellement, qui relie deux PC, avec un réseau Ethernet.

Mots clés : RAT, Logiciel Malveillant, Cible, Attaque, Cheval de Troie, Pirate, IP, Ethernet.

Abstract:

RAT (remote access trojan) is a malware that includes a backdoor for administrative control of the target computer. In this work we have conducted an attack scenario of a Trojan horse that allows the hacker to access the target machine remotely through a Trojan horse hidden inside an image sent by the hacker to the target. At the execution of this image by the target, the Trojan will run at the same time. During this execution a system integration in the Windows registries of the malware will be performed. In the network settings we determine the IP Address manually, which connects two PCs, through an ethernet network.

Keywords : Trojan Horse ; ProRat ; TCP/IP ; LAN ; Cyber Security ; Firewall ; OSI ; Hacker ; server ; Client ; Victim ; Infect ; Implementation ; Routing .

Table of contents

Table of contents

Chapiter 1 : Computer Network

Chapiter 2 : IT Security

Chapiter 3 : Design and Implementation

List of figures

The current world has entered into information time with the development of computer networks, while internet has become indispensable in life, work, and study, so occupying the biggest aspects of our daily lives. However, this great progress came with bigger threats; the virus attacks became increasingly popular because of the development and strengthening of internet. Various attack methods greatly endanger the property security of human beings, their personal information, credit accounts and many more; as a result, the cybersecurity emerged as a deterrent against these threats.

Our project's goal is to gain knowledge to be a network or security network administrator, thus it's a must to put yourself in the shoes of a pirate. So before being one, we have to understand how the attacks work, so that we can then find solutions for this kind of problem.

Trojan horse virus is one of the major and well-known threats, for what once stood for a brilliant trick and a masterful feat of engineering is nowadays regarded as a malicious digital pest whose sole aim is to wreak havoc on its victim's computers unnoticed. It does this by reading passwords, recording keyboard strokes or opening the door for further malware that can even take the entire computer hostage. we have to make this study to know more fundamental knowledge, communication methods, and work process to take precautionary measures to further enhance the network protection and construct harmonious network environment.

This thesis consists of three chapters:

- ✓ The first chapter is devoted to the IT network and its architectures, the OSI model and IT equipment as well as LAN and routing.
- ✓ The second chapter is reserved for computer security and malwares precising our theme which is the Trojan horse.
- ✓ The last chapter presents the client/server architecture, the ProRat software implementation and the Trojan Horse Impact in the hacked PC.

This brief concludes with a general conclusion and perspectives for remedying this kind of problem.

Introduction

certainly, in the network, many researchers started to create their own norms, but each one was different than the other, that led them to not being able to communicate; so, they found it necessary to create a unified norm that responds to all the necessities of a network to reassure a liable communication and they have chosen the OSI model.

This chapter is divided into four parts. First, a general view on the computer network. In the second part, we will talk about the OSI model, as well as the TCP protocol that interests us in our project . Then the Ethernet is presented . In the last part, the Internet protocol is detailed.

1.1. Computer Networks

1.1.1. Definition

Computer network is a system consisting of computers and other network devices working together to achieve a common goal. The purpose of the computer network is :

- Sharing resources functions such as shared use of printers, CPU , hard drive .
- Communication: eg, electronic mail, instant messaging, chat .
- access to information: for example, web browsing in order to achieve the same goal, each part of the computer network and provide service request (service) [1].

1.1.2. Local Area Network

LAN (Local Area Network). It is a set of computers belonging to the same organization and linked together in a small geographical area.

A LAN typically spans a single geographic area and provides services and applications to individuals within a common organizational structure, such as an enterprise, campus or region. As a general rule, a local network is administered by a single organisation. The administrative control that manages security and access control strategies applies at the network level [2].

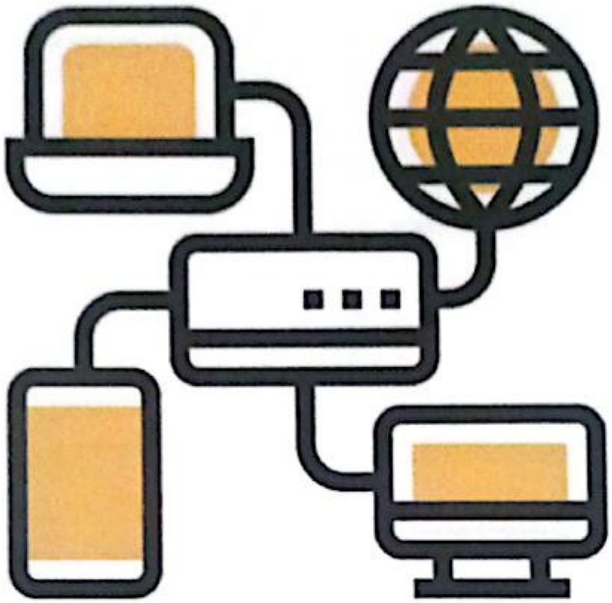

Figure 1.1. Local Area Network.

1.1.3. Representation of the Network

a. **Network card:** A network card, or LAN adapter, provides the physical connection to the network from the computer or other host device. Media that connect the computer to the network device connect directly to the network card.
b. **Physical port:** a connector or socket on a network device to which the media is connected to a host or other network device.
c. **Interface :** specialized ports on a network device that connect to individual networks. Since routers are used to interconnect networks, ports on a router are called network interfaces [3].

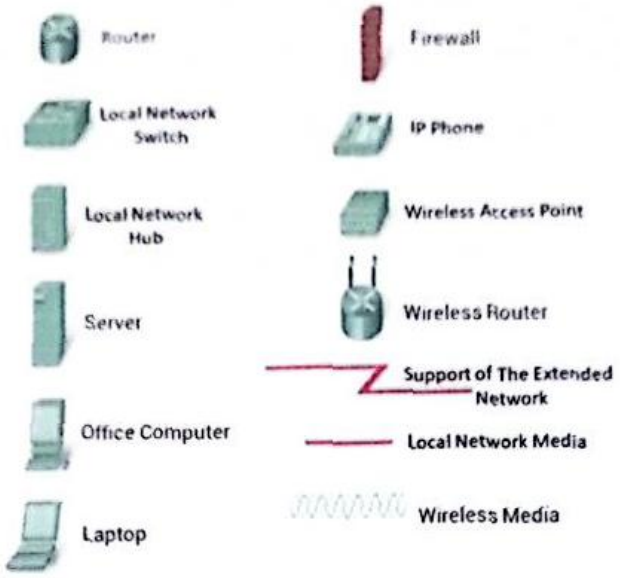

Figure 1.2. Common Data Network symbol.

1.1.4. IT Equipments

The networks are composed of a physical and software part. Peripherals and media represent the physical elements or hardware of the network. The hardware often corresponds to the visible components of the network platform [2].

A. Terminal devices:

The network devices that people are most used to are called final devices. These devices form the interface between the human network and the communications network. Some of *these end devices are:*

- Computers (workstations, laptops, file servers, web servers).
- Network printers.
- VoIP phones.
- Surveillance cameras.

In the case of a network, the final devices are called **Hosts**. A host device is either the source or the destination of a message transmitted over the network. To distinguish between

hosts, each host on a network is identified by an address. When a host starts a communication, it uses the destination host address to indicate where the message should be sent.

In modern networks, a host can act as a client, a server, or both.

- **Servers** are computers that have installed software to provide information and services to other computers on the network. The most common services are:

- File sharing.
- Access to World Wide Web information.
- E-mail.
- Sharing printers.
- E-commerce.
- Database storage.

- **Clients** are computers that have installed software (for example, a web browser) allowing them to query and display information obtained from the server. The client is generally a regular personal computer [2].

B. Intermediate devices:

In addition to the end devices that people are accustomed to rely on intermediary devices to provide connectivity, to ensure data flow across the network. These devices connect individual hosts to the network and can connect multiple individual networks to form an inter-network. These intermediate network devices include:

- Network access devices (hubs, switches and wireless access points).
- Inter-network devices (routers).
- Communication servers and modems.
- Security Peripherals (Firewall).

Managing data as it passes through the network is also one of the roles of intermediate devices. These devices use the destination host address , along with information about network interconnections, to determine the path that messages should take across the network. The processes that run on the devices on the intermediate network perform these functions:

- Regenerate and retransmit data signals.
- manage information indicating the paths that exist through the network and the inter - network.
- Advise other devices of communication errors and failures.
- Direct data to other paths in case of link failure.
- allow or refuse the data flow, depending on security settings [2].

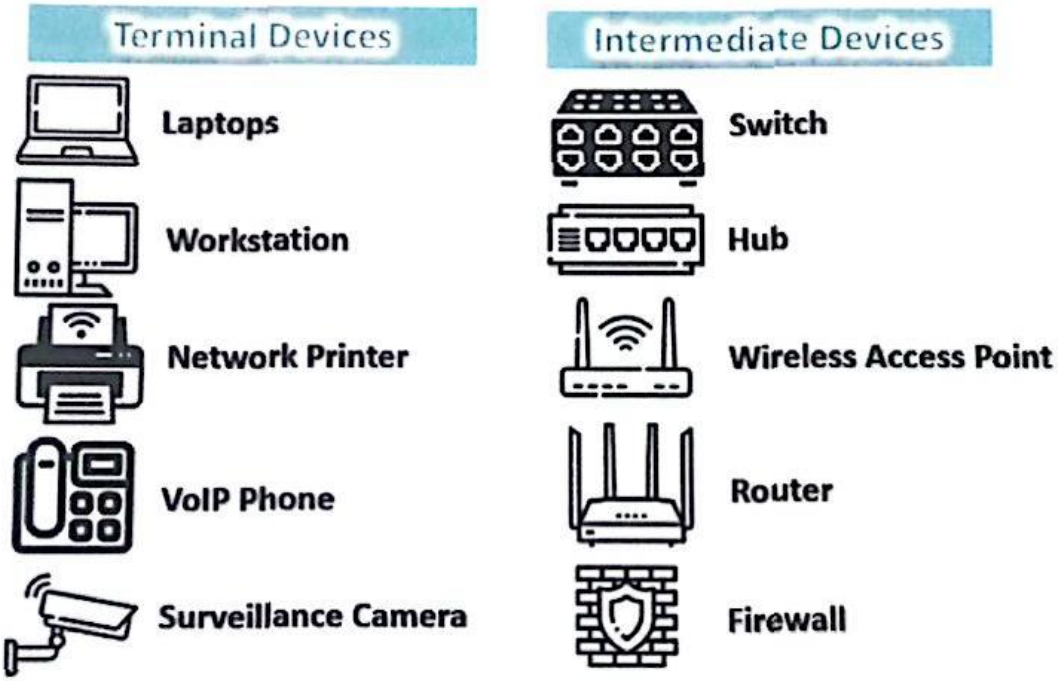

Figure 1.3. IT Equipment.

1.1.1. Network Models

i. Client/Server model

In the client/server model, the device requesting the information is named client and the device responding to the request is named server. The client and server processes are considered to be part of the application layer. The client. starts the exchange by requesting data from the server, which responds by sending one or more data streams to the client. Application layer protocols describe the format of requests and responses between clients and servers. In addition to the actual data transfer, this exchange may also require control information, such as user authentication and identification of a data file to be transferred [2].

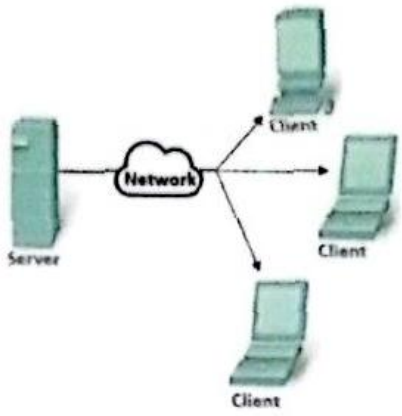

Figure 1.4. Client/Server model.

ii. Peer to Peer model

In a Peer-to-Peer network, at least two computers are connected via a network and can share resources (for example, printers and files) without having a dedicated server. Each connected end device (named homologue) can operate as a server or as a client. A computer can act as a server for a transaction while simultaneously serving as a client for another computer. The client and server roles are defined according to each request [2].

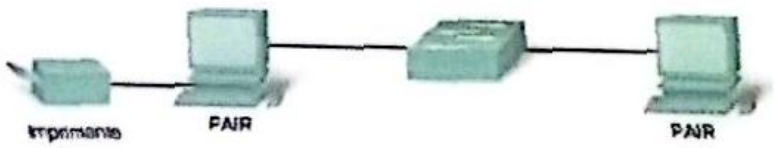

Figure 1.5. Peer to Peer model.

1.2. OSI-model

1.2.1. Definition

The Open Systems Interconnection (OSI) model is the virtual model that describes the Concept of a computer system with internal structure and technology.

OSI or in other words, Open Systems Interconnection model is a conceptual model which is used vastly in the software industry especially in the field of communication for characterizing and standardizing the functions without touching the internal structure underlying in the structure or technology [4].

1.2.1. Layers

The Open Systems Interconnection (OSI) model is divided into seven layers ; Hardware and Software layers :

a. Hardware Layers (Network access)

1. Physical Layer:

The Physical layer is the first layer of the OSI Model. In this layer there is signal encoding and cabling . It works to send individual bits from one node to another. This layer is actually responsible for the connection between two devices. Whatever data comes to this layer is converted into binary format. After the conversion, send the data to the data link layer [4].

2. Data-Link Layer:

Data-Link layer protocols describe data frame exchange methods between peripherals on a common medium [3].

b. Software Layers

3. Network Layer:

The network layer adds the concept of routing on top of the data link layer. When the data reaches the network layer, the source and destination addresses contained in each frame are examined to determine if the data has reached its final destination. When the data reaches its

final destination, Layer 3 formats the data into packets and delivers them to the transport layer. Otherwise, the network layer updates the destination address and pushes the frame down.

To support routing, the network layer maintains logical addresses, such as the IP addresses of network devices. It also manages the mapping between these logical and physical addresses. In IPV4 networks, this mapping is done via Address Resolution Protocol (ARP). IPV6 uses the Neighbour Discovery Protocol (NDP) [5].

4. Transport Layer:

The transport layer is responsible for transferring data from one location to another. It controls the reliability of communication through segmentation, flow control, and error control.

- Segmentation is the process of dividing received data into small units called segments.
- A segment is a unit of Communication In this layer.
- **Flow Control:** Flow Control is the process of controlling the amount of data being transmitted.
- **Error Control:** Transport Layer uses Automatic Repeat Request Scheme to retransmit lost or corrupted data. A group of bots called checksum is added to each segment to determine the received segment with errors [6].

Role:

The transport layer is responsible for establishing a temporary communication session between two applications and delivering data between them. An application generates data that is sent from an application on a source host to an application on a destination host. This is without regard to the destination host type, the type of media over which the data must travel, the path taken by the data, the congestion on a link, or the site of the network [7].

TCP/IP:

Short for Transmission Control Protocol/Internet Protocol, is a communication protocols suite that means a set of rules and procedures which are used for interconnecting various network devices over the internet by defining how the data should be transmitted, routed, broken into packets, addressed, and received at the destination. The TCP defines how applications can create communication channels across a network. IP defines the way each packet is addressed and routed to ensure it reaches the correct destination [7].

5. Session Layer:

The session layer sets up, coordinates and terminates conversations between applications. Its services include authentication and reconnection after an interruption. This layer determines how long a system will wait for another application to respond. Examples of session layer protocols include X.225 and Zone Information Protocol (ZIP) [8].

6. Presentation Layer:

The presentation layer translates or formats data for the application layer based on the semantics or syntax the application accepts. This layer also handles the encryption and decryption that the application layer requires [8].

7. Application Layer:

The Application Layer provides a homogeneous interface between the network and the software. this kind of interface is often called the API (Application Programming Interface) and allows you to write a program once, without taking into account any particular network type, then to use it with any network type, TCP/IP, IPX, AppleTalk, Ethernet, Token Ring or FDDI..[9].

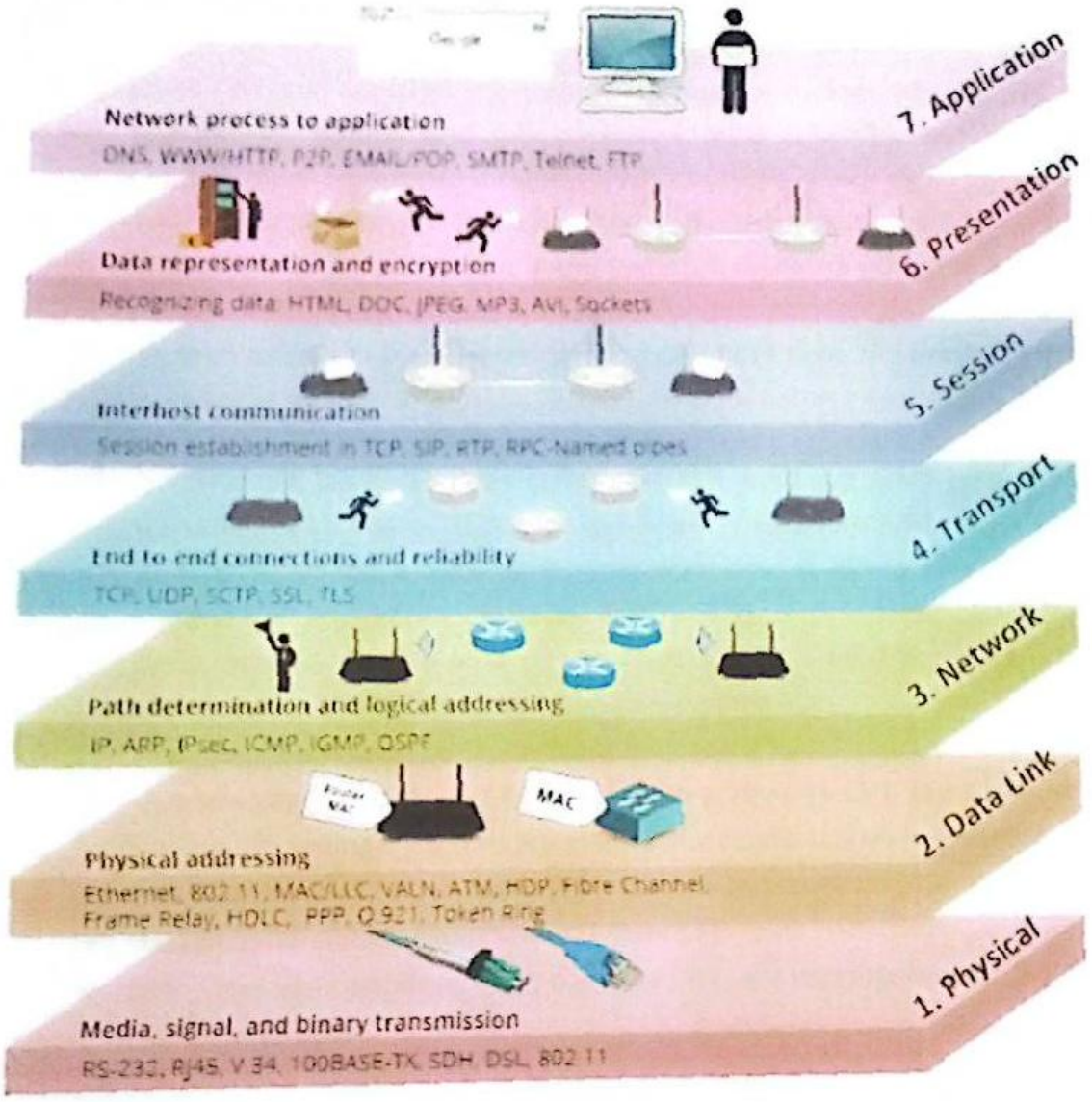

Figure 1.6. OSI Model.

1.3. Ethernet

Ethernet is a network technology, well known and very responsive , based on a bus topology, while the physical topology can be bus or star; to which several computers are connected. And the transmission is done in baseband using the Manchester code [10].

1.4. Internet Protocol

IP (Internet Protocol) specifies the technical format of packets and the addressing scheme for computers to communicate over a network. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source. IP by itself can be compared to something. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/ IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time. IP Layers The Internet protocol suite uses encapsulation to provide abstraction of protocols and services.

- Sur Internet, les ordinateurs communiquent entre eux grâce au protocole IP qui utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de 0 à 255 (4 fois 8 bits), on les note donc sous la forme xxx.xxx.xxx.xxx où chaque xxx représente un entier de 0 à 255. 2 Ces numéros servent aux ordinateurs du réseau pour se reconnaître, ainsi il ne doit pas exister deux ordinateurs sur le réseau ayant la même adresse IP.
- We have two version of IP which are IPV4 and IPV6.
- IP addresses can only communicate with addresses with the same network number, including if stations are in the same segment. This is the same number that allows the router to route the packet to the recipient [11].
- We have five classes explained in (Figure I.3).
- Each Class has a public range and private one , are represented in (Figure I.4).

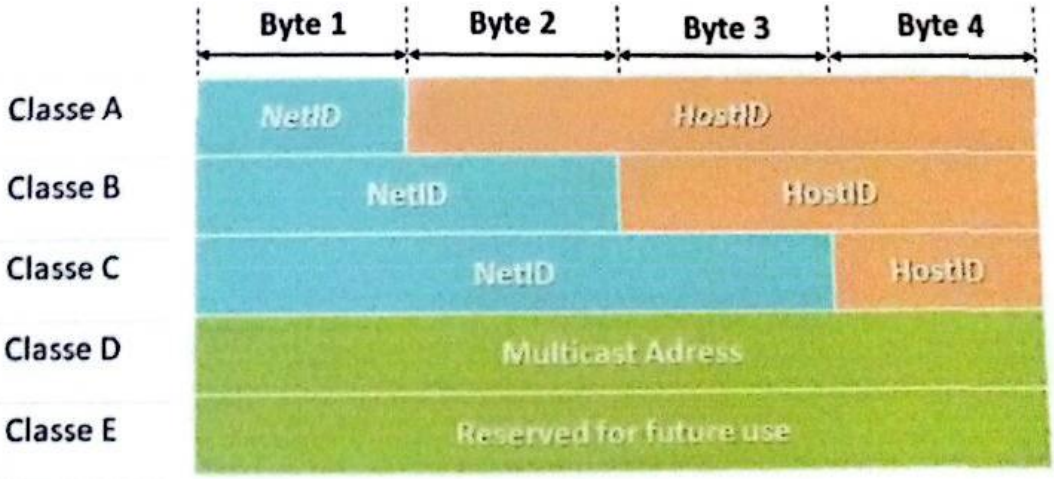

Figure 1.7. IP address classes.

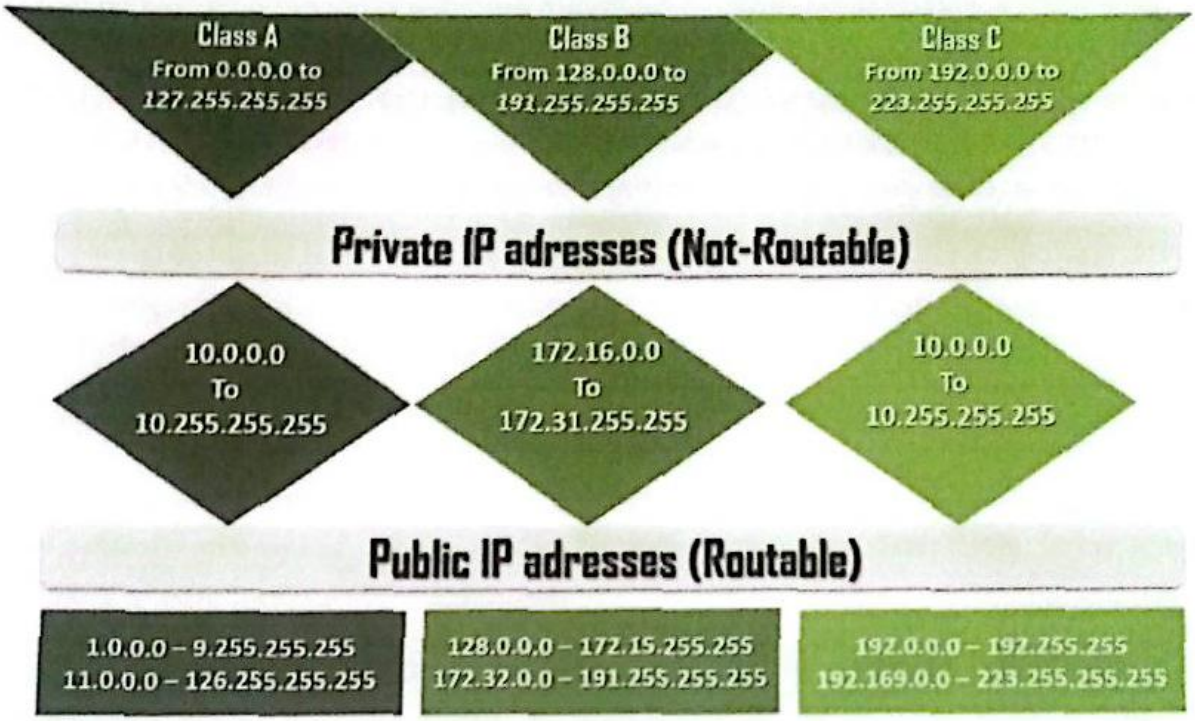

Figure 1.4. private / public IP addresses.

Conclusion

This chapter provides an overview of the OSI-based computing network for data transfer between computers. Subsequently, a detailed representation is conducted on the internet protocol.

The next chapter will cover cyber security in general and also address threats.

Introduction

Today's world depends on technology more than ever, this has resulted in a huge surge in the creation of digital data(information). This huge amount of data(information) is stored and transferred throughout the internet and different networks on a daily basis, so the need to protect this information became crucial, and that led to the emergence of cyber-security.

This chapter contains three parts. First, let's see what cyber security is. Then, we mentioned the types of malwares. finally, we will detail the Trojan horse.

2.1. Cybersecurity

Cyber security is a defensive remedy to protect virtually any internet-connected systems out of cyber-threats and attacks, its goal is the preservation of confidentiality, integrity and availability of information in the cyberspace.

In our project we are studying network security, which is the implementation of both the software and hardware mechanisms to ensure the safety of the network and the infrastructures from external danger [12].

2.1.1. Firewall

A firewall is a security device computer hardware or software that can help protect the network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your computer. Not only does a firewall block unwanted traffic, it can also help block malicious software from infecting your computer [13].

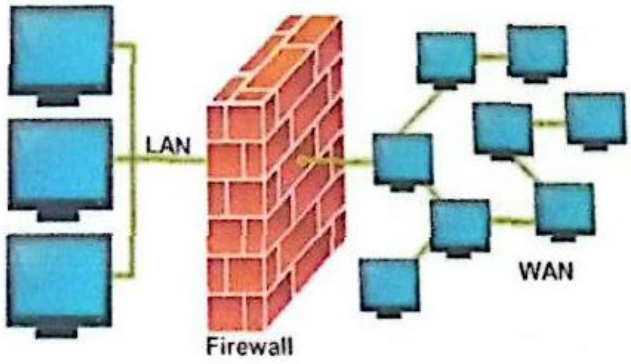

Figure 2.1. Firewall.[20]

2.1.2. Anti-virus

Antivirus software is a type of program designed and developed to protect computers from malware like viruses, computer worms, spyware, botnets, rootkits, keyloggers and such. Antivirus programs function to scan, detect and remove viruses from your computer. Most antivirus programs incorporate both automated and manual filtering abilities. The instant scanning option may check files - downloaded from the Internet, discs that are embedded into the PC, and files that are made by software installers. The programmed scanning process may likewise check the entire hard drive on a day-to-day basis. The manual scanning system enables you to check single documents or even to scan the complete network at whatever point you feel it is necessary [14].

2.2. Malwares

2.2.1. Definition

A Malware is a small and particularly malicious software that has the objective of deceiving a user and harming his computer system[15].

2.2.1. Types of malware attacks

- **Virus:** is the most common type of malware that can execute itself and spread by infecting other programs or files.
- **Worm:** can self-replicate without a host program and typically spreads without any interaction from the malware authors.
- **Spyware:** collects information and data on the device and user, as well as observes the user's activity without their knowledge.
- **Ransomware:** infects a user's system and encrypts its data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data.
- **Rootkit:** obtains administrator-level access to the victim's system. Once installed, the program gives threat actors root or privileged access to the system.
- **Backdoor:** virus or remote access Trojan (RAT) secretly creates a backdoor into an infected computer system that enables threat actors to remotely access it without alerting the user or the system's security programs.

- **Adware:** tracks a user's browser and download history with the intent to display pop-up or banner advertisements that lure the user into making a purchase. For example, an advertiser might use cookies to track the webpages a user visits to better target advertising.
- **Keyloggers:** also called system monitors, track nearly everything a user does on their computer. This includes emails, opened webpages, programs and keystrokes.[16].

2.3. Trojan Horse

2.3.1. Definition

A Trojan Horse, or Trojan Horse, is a non-self-replicating type of malware that appears to perform a desirable function, but rather facilitates unauthorized access to the user's computer system. Trojans do not attempt to inject themselves into other files like a virus, but the "payload" carried by a Trojan is unknown to the user, but it can act as a delivery vehicle for a variety of threats [17].

Figure 2.1. Trojan Horse.[21]

2.3.2. Types of Trojan Horse

- **Backdoor Trojans:** This type of Trojan allows hackers to remotely access and control a computer, often for the purpose of uploading, downloading, or executing files at will," this type will be our main subject of study". (ProPat,).
- **Exploit Trojans:** These Trojans inject a machine with code deliberately designed to take advantage of a weakness inherent to a specific piece of software.

- **Rootkit Trojans:** These Trojans are intended to prevent the discovery of malware already infecting a system so that it can affect maximum damage.
- **Banker Trojans:** This type of Trojan specifically targets personal information used for banking and other online transactions. (Ice IX, Spy Eye...).
- **Distributed Denial of Service (DDoS) Trojans:** These are programmed to execute DDoS attacks, where a network or machine is disabled by a flood of requests originating from many different sources.
- **Downloader Trojans:** These are files written to download additional malware, often *including more Trojans, onto a device.*
- **Exploit Trojans:** These devious Trojans use exploits — software tricks designed to leverage a known software or hardware vulnerability — to infect your device. Zero-day exploits target vulnerabilities that no one but the exploit creator has discovered yet.
- **Fake antivirus Trojans:** A dangerous type of scareware, fake AV Trojans pretend to detect viruses and other malware on your device, then urge you to pay for security software which is either useless or actively malicious. When you pay, the Trojan creator gets your payment details.[18]

2.3.3. Common ways to get Infected by trojans

There is no limit to how the hackers can be creative with their tactics, these are of the most common ones:

- Social engineering: a psychological technique to manipulate users into clicking on a link or downloading an app, free music or movies, that are infected.
- *Phishing email:* it is a message appearing to be from trusted source but in reality, it is an attempt to trick the user into downloading a trojan.
- Scareware: a convincing pop-up ad claiming your device is threatened and offers a solution (but secretly hides a malware) to protect your device.

2.3.4. Infectious method

In TCP/IP network, a port represents an endpoint in the establishment of a connection between computers. for the computer that acts as the server, the port number will typically Identify the type of service It Is; and so, depending on the trojan Involved, it can use one to multiple ports to established a connection between the victim's device and the hacker.

The hacker running the "client" portion establishes a connection to the IP address of a known PC that has the "server" portion installed upon it, but if the hacker doesn't have the IP address of the compromised PC, usually Initiates a series of connection to a large range of IP addresses on the internet, this one is known as "scanning", and so the unlucky user that his PC responds with his IP address to the "scan" will get hacked [19].

conclusion

In this chapter we have seen cybersecurity, malwares and our main interest Trojan Horses with their method of spreading.

In the next chapter we will create a client/server architecture and implement a ProRat Trojan and see its effects.

Chapter 3 : Design and Implementation

Introduction

In the previous chapters we explained the IT network, IT security and malware In a general way.

This last chapter Is devoted to explain how to use the trojan « ProRat 1.9 ». It will aim to explain how creates a server to control the victim's computer, the different ProRat function (once you have controlled what to do...).

3.1. Overview of the software used

The Trojan can be programmed by the hacker meanwhile there are ready softwires to be used directly. In our project we will implement a very used software called ProRat.

Overview of ProRat

ProRat has a server creator with features that allow it to be undetected by antivirus and firewall software, and also allow it to stealthily run in the background. The software runs completely in Windows, and such features include killing security software, removing and disabling system restore points, and displaying a fake error message to mislead the victims. It is often "Bound" with other file types, such as image files, and when the image file is viewed, the server is installed in the background, undetected if no antivirus software has been installed.

3.2. Material used

the materials used in our project is summarized in :

- ✓ Personal laptop (server).
- ✓ Personal laptop (client).
- ✓ 2 twisted cables with RJ45 connectors.
- ✓ Adapter(USB to RJ45).
- ✓ Router.

3.3. The Architecture

1) physical installation of two PCs, connecting the server PC with the Router via a RJ45 cable and also with the client PC using the USB-RJ45 adapter because in the server PC there is a RJ45 jack (Figure 3.1).

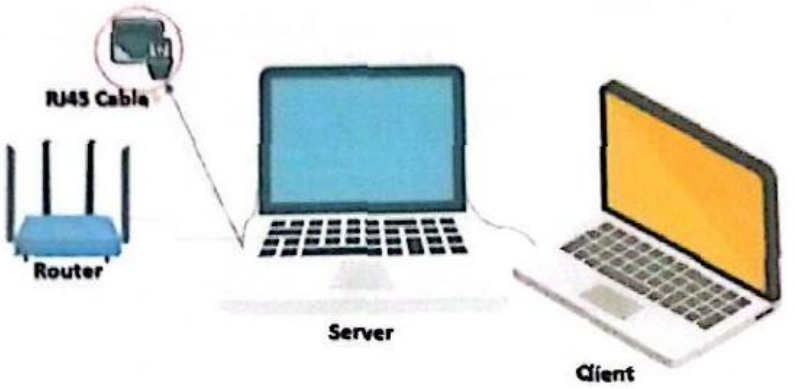

Figure 3.1. physical installation.

2) Next, the configuration of the network card (**Server**):
   - Control Panel > Center Network and Share > Change Card Parameters > Ethernet Card > Right Click > Properties (Figure 3.2).

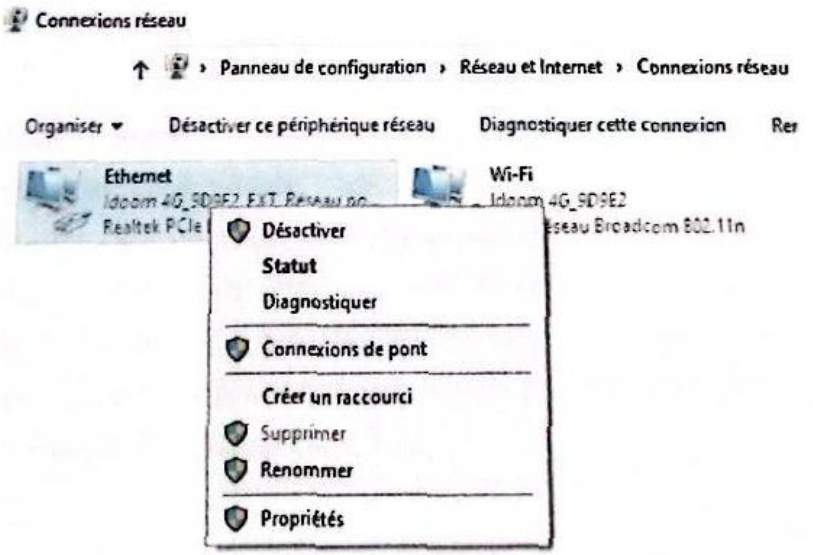

Figure 3.2. carte Ethernet.

- double click on Internet Protocol version 4 (TCP/IPV4) (Figure 3.3).

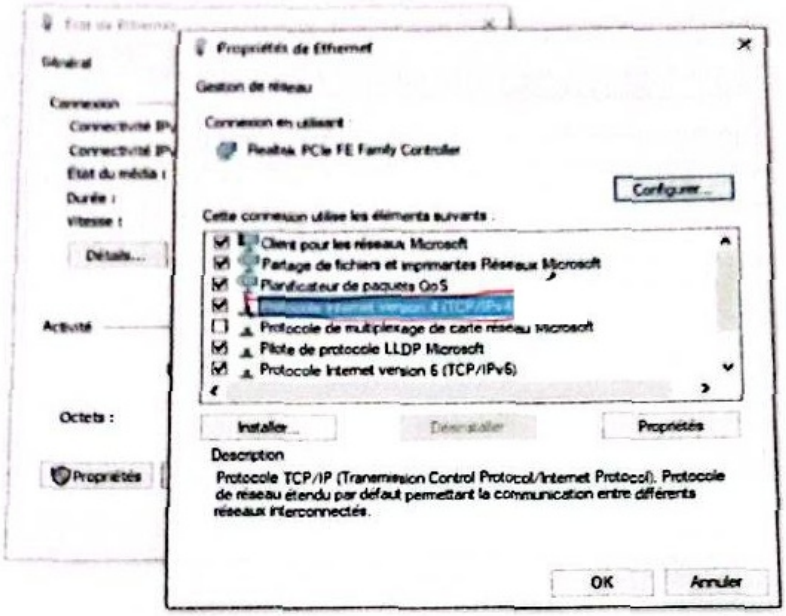

Figure 3.3. Ethernet Properties.

- chose ; use this IP address > fill (IP address , subnet mask , default gateway) > use this DNS address > fill (preferred DNS server) > ok;
  we supposed a Private IP address class C (192.168.10.1) and DNS IP address of Google(8.8.8.8) (Figure 3.4).

3) the configuration of the network card (client):
   - Control Panel > Center Network and Share > Change Card Parameters > Ethernet Card > Right Click > Properties (Figure 3.2).
   - double click on Internet Protocol version 4 (TCP/IPV4) (Figure 3.3).
   - chose ; use this IP address > fill (IP address , subnet mask) without filling default gateway > use this DNS address > fill (preferred DNS server) > ok;
     we supposed a Private IP address class C (192.168.10.2) and DNS IP address of Google (8.8.8.8) (Figure 3.4).

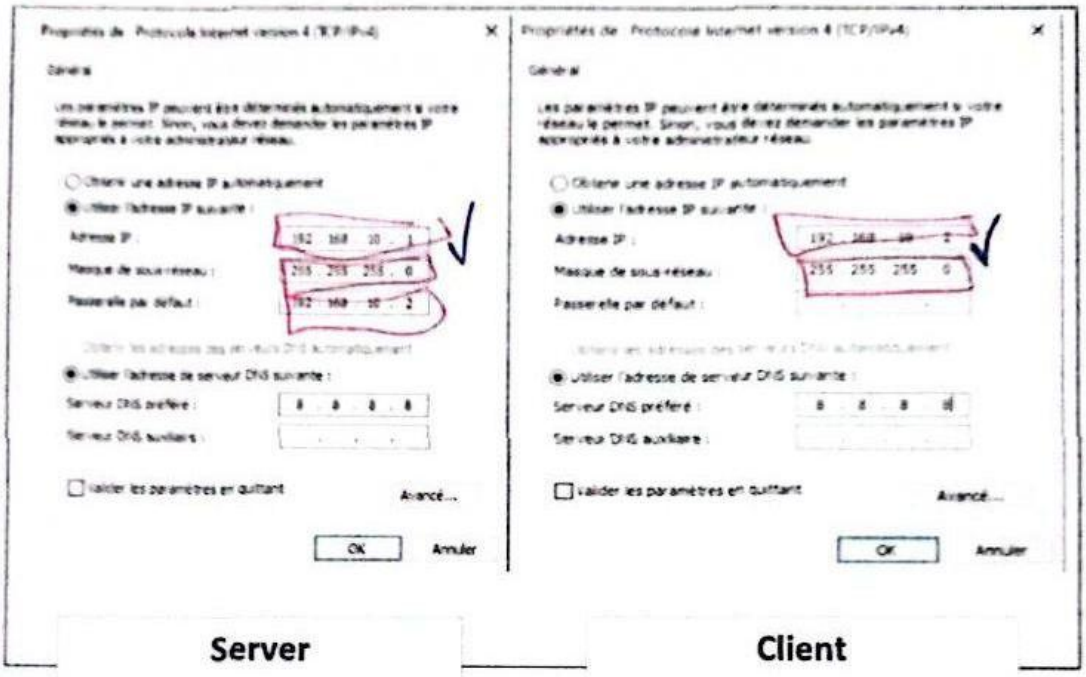

Figure 3.4. Routing.

4) disabling Firewall (this step is done for both):
Control Panel > system and security > windows defender firewall > activate or deactivate firewall > check the deactivation boxes > ok (Figure 3.5).

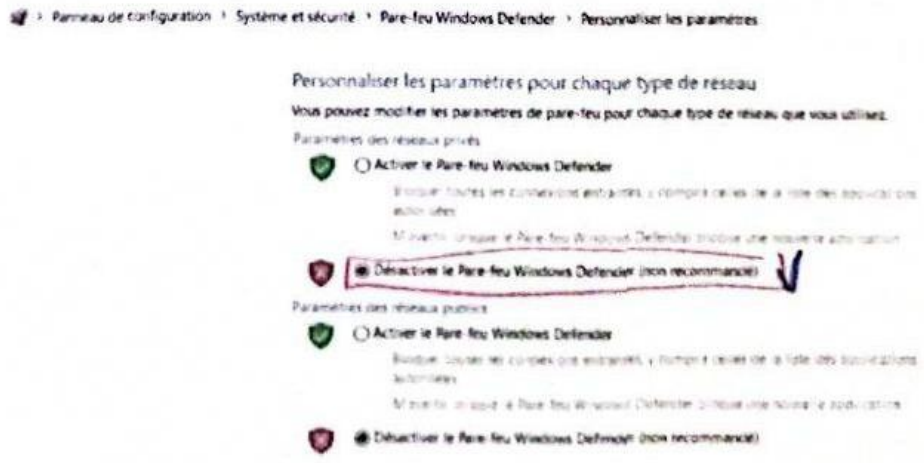

Figure 3.5. disabling Firewall.

5) checking the connection between two PCs:

- ❖ ***server:***

➢ In the search bar tape CMD then click Enter > tape **ipconfig** (shows the IP address) > ping 192.168.10.2 (when successful (Figure 3.6)).

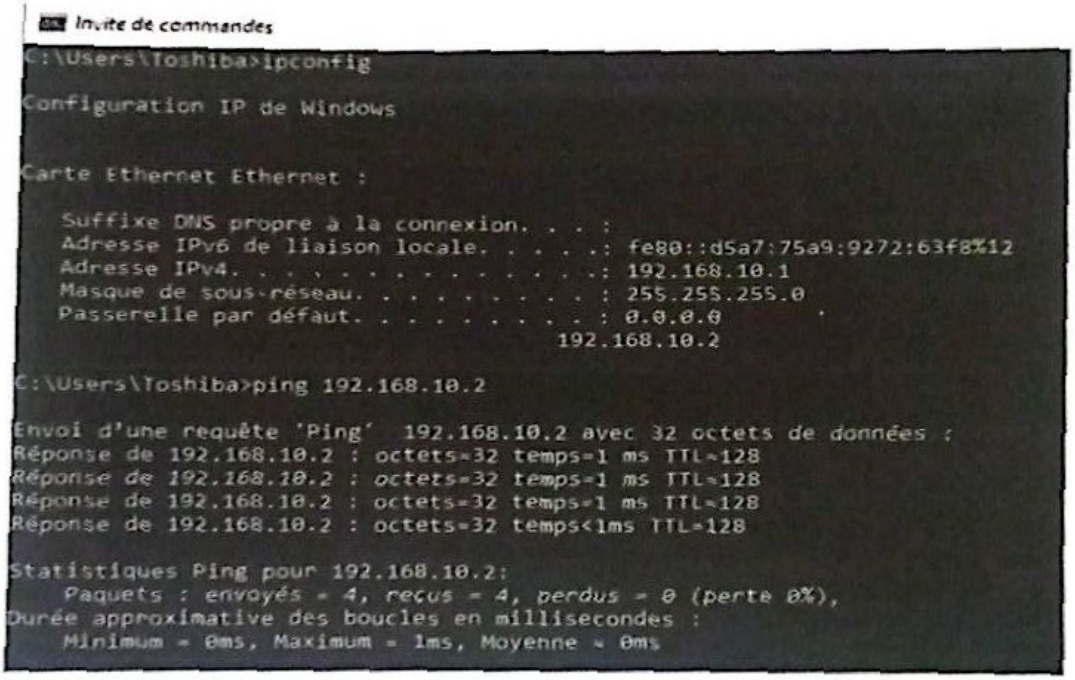

Figure 3.6. verification(Server).

- ❖ ***Client:***

➢ In the search bar tape CMD then click Enter > tape **ipconfig** (shows the IP address) > ping 192.168.10.1 (when successful (Figure 3.7)(Figure 3.8)).

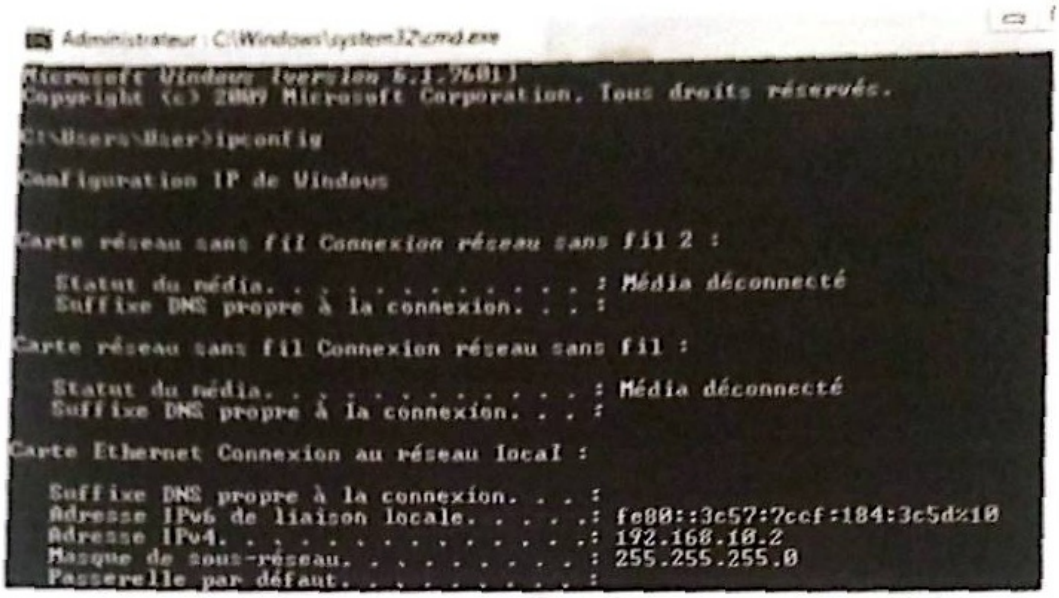

Figure 3.7. Verification1(Client).

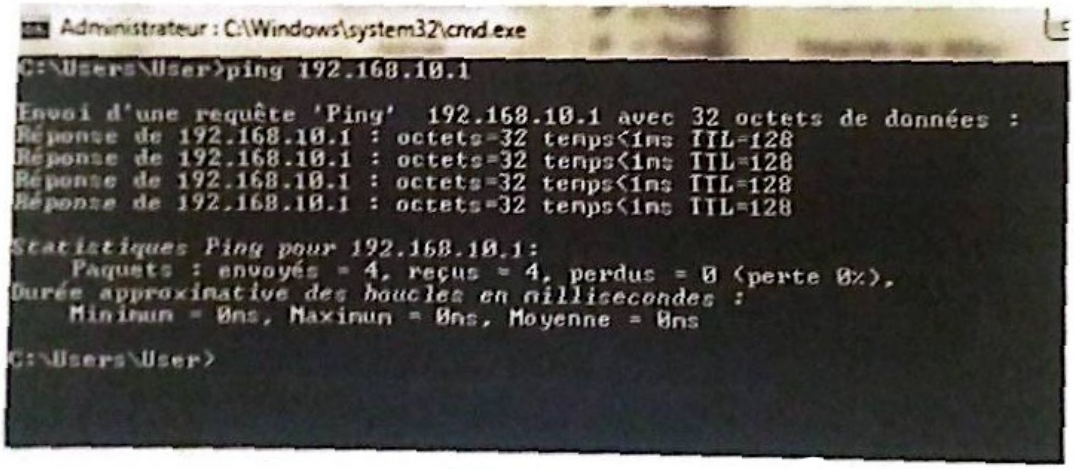

Figure 3.8. Verification2(Client).

3.4. The Implementation

1) First of all, Download ProRat.
2) Opening prorat.exe that we have downloaded (Figure 3.9).

Figure 3.9. ProRat interface.

3) A click on **Create** and then **Create ProRat Server**(Figure 3.10).

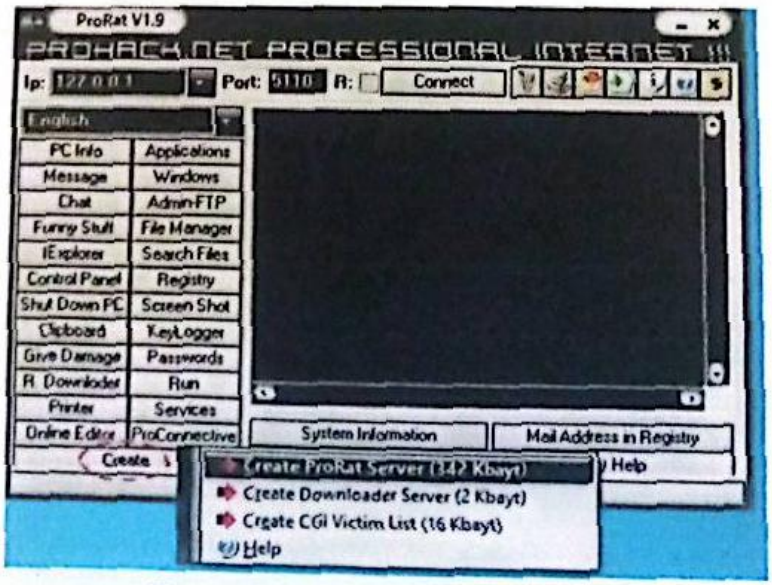

Figure 3.10. Sitting-up the server.

4) Enter our victim's host IP address In the ProRat Notification field as shown. (Figure 3.11).

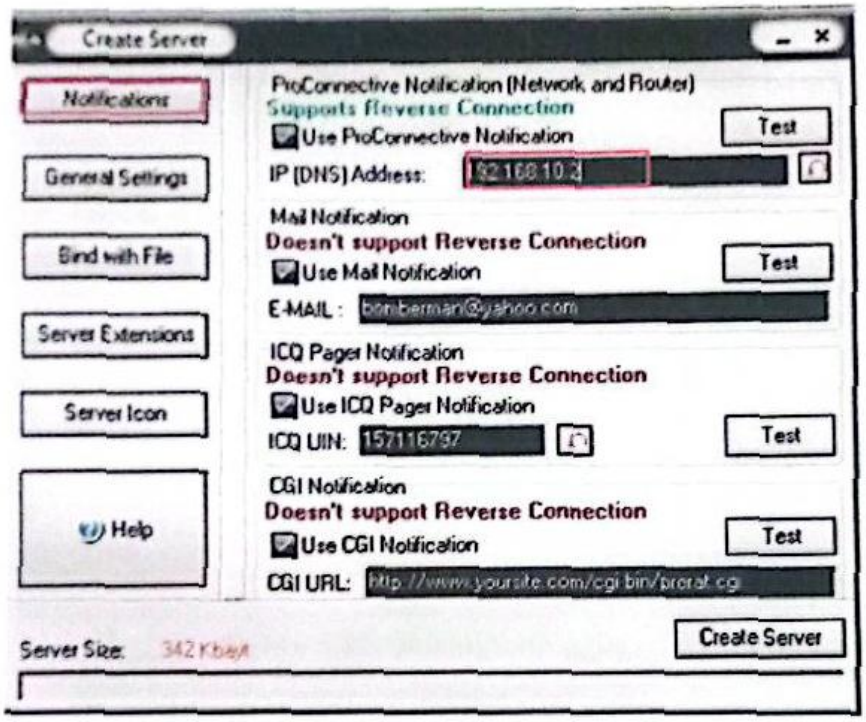

Figure 3.11. Notification button.

5) Opening **General settings.** This tab Is the most important tab. In the check boxes, we chose the **server port** the program will connect through, the **password** we entered when the victim Is infected and wanted to connect with them, and the **victim's name** (Figure 3.12).

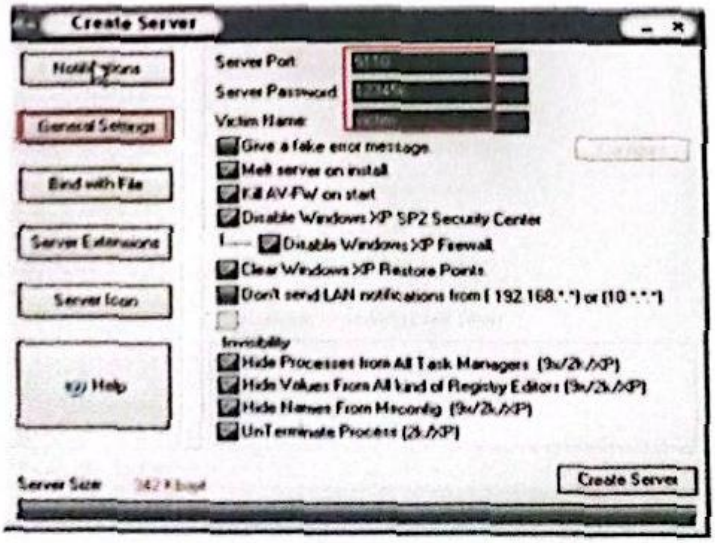

Figure 3.12. General settings button.

6) Going to the **Bind with File** button . we have the option to bind the trojan server file with another file. We selected an Image, So as to make the victim trust your file (Figure 3.13).

Figure 3.13. Binding with a file.

7) Clicking on the Server Extensions button to continue. Here we chose what kind of server file to generate. We preferred using .exe files (Figure 3.14).

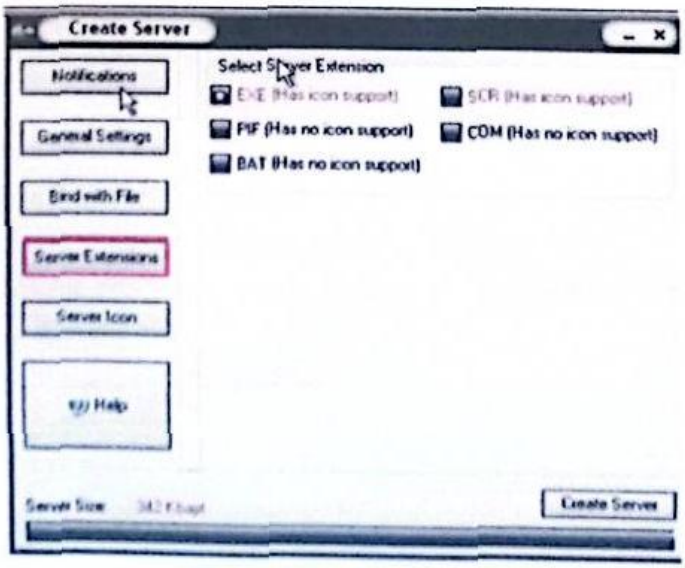

Figure 3.14. File format.

8) Choosing an Icon to our server as to keep the file hidden In **server Icon** button (Figure 3.15).
9) Then clicking on **create server** to finish sitting-up the server (Figure 3.15).
10) Sending the infected file (By uploading It In a USB-drive > sticking the USB-drive In the client's PC).

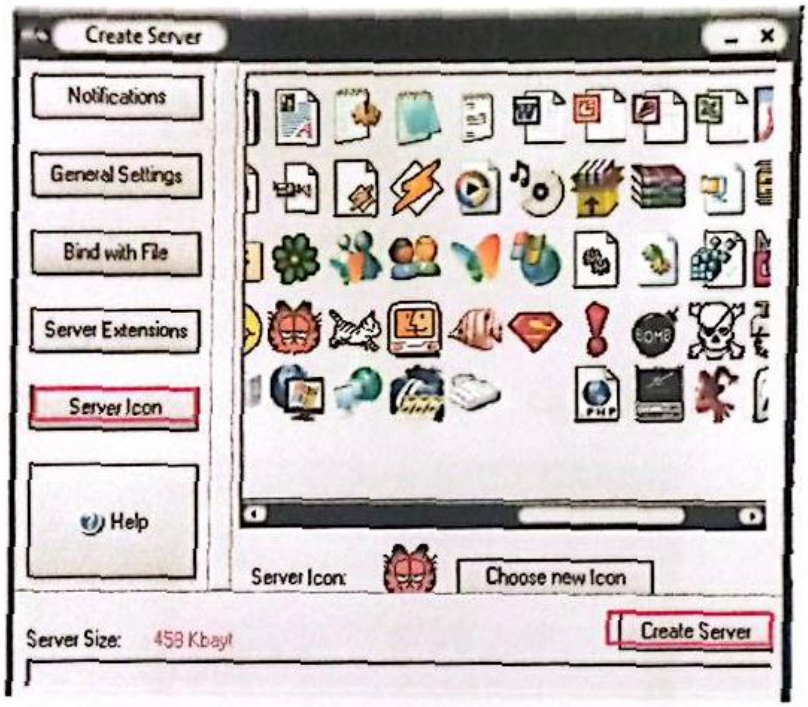

Figure 3.15. Server Icon.

3.5. Results of manipulation

After Implementing the Infected file In the victim's PC and running It, we got these results:

1) By clicking on the connect button in the ProRat, the software responds (Figure 3.16).

Figure 3.16. Software responding.

2) The hacked PC detects a suspicious activity (Figure 3.17).

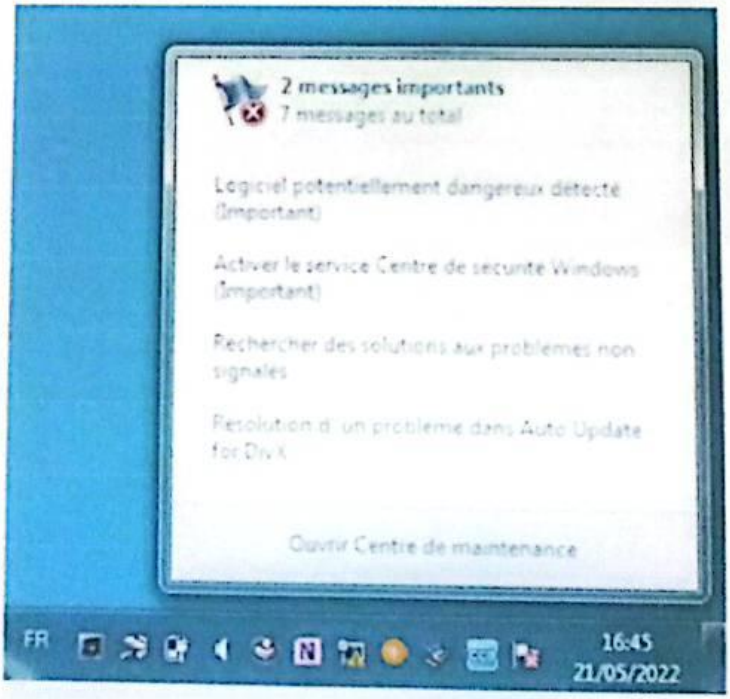

Figure 3.17. Detection.

3) We initiated the manipulation process, first, we got the hacked PC information (Figure 3.18).
Then, we start controlling the victim (The result of the manipulation is on the attached CD and in this Drive:
https://drive.google.com/drive/folders/1RoU1i7vfXxjHRl99y5pye4Her6elll5e?usp=sharing).

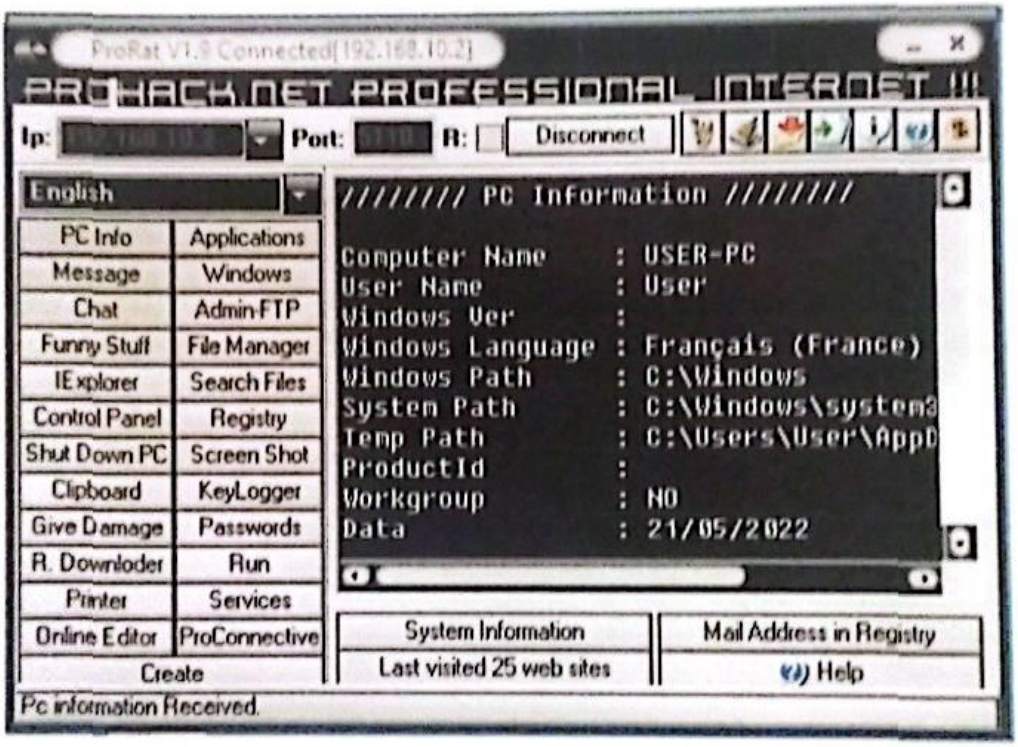

Figure 3.18. Victim's PC Information.

Conclusion

This chapter was dedicated to the implementation of used hacker software, the presentation of the results of tests performed. We started with an introduction to the work environment, the software used and the hardware used In order to manipulate the victim's PC.

We designed this work for the right cause, it aims to gain knowledge about network attacks to understand how Trojan Horse works.

In this thesis we have seen the IT network, routing, and cybersecurity and its threats. In the last part, we implemented the ProRat in a client/server architecture and we controlled the client PC seeing the changes that is made by this software.

the result of this software allows to:

- have complete control of the victim.
- extracting the victim's personal information.
- Mess-up tasks and stop them.

In perspective, we found that the Trojan Horse operation is based on the notion of ports and the means to remedy to this problem one can set up a firewall that will block all unnecessary ports because the Trojan uses a random port to access. also, we can use an anti-intrusion like Kaspersky or windows defender.. , as one can kill the malware manually in the task manager.

Bibliography

[1]. Wulandari Rahmat, « COMPUTER NETWORK », academia, https://www.academia.edu .

[2]. A.S.Mabunda, « Réseaux Informatiques », Scribd, https://fr.scribd.com, le Mar 30, 2018.

[3]. N. Rezoug, « Cours communication sur un Réseau », Université de Blida, 2017.

[4]. Pooja Gupta, «What is OSI-Model», educba , https://www.educba.com.

[5]. «The Layers of the OSI Model Illustrated», phanmemportable, https://phanmemportable.com.

[6]. Swati Tawde, «What is TCP/IP?», educba , https://www.educba.com.

[7]. sinako jail, «Transport Layer», academia , https://www.academia.edu.

[8]. Andrew Froehlich , Linda Rosencrance, Kara Gattine, «OSI model (Open Systems Interconnection)», techtarget, https://www.tachtarget.com.

[9]. Ed Tittel, «Réseaux», Dunod, Paris, 2003.

[10]. CHrist CaLderon, , «ETHERNET REDES ETHERNET», academia, https://www.academia.edu.

[11]. M.MEHDI, « Cours COUCHE 3 : LA COUCHE RESEAU », Université de Blida, 2022.

[12]. Cybersecurity, «Cyber security », Synopsys, https://www.synopsys.com.

[13]. Alison Grace Johansen, «What is a firewall? Firewalls explained and why you need one», https://us.norton.com, June 17, 2021.

[14]. Antivirus, «comodo», https://antivirus.comodo.com.

[15]. Gabriel Dabi-Schwebel, «Malware», https://www.1min30.com, 2022.

[16]. Ben Lutkevich, « Malware» , https://www.techtarget.com/ ,2022.

[17]. Antivirus, «What is a Trojan horse and what damage can it do», Kaspersky, https://www.kaspersky.com.

[18]. Antivirus, «What is a Trojan (horse) », Avast, https://www.avast.com.

[19]. Mary Atamaniuk, «what is a Trojan virus and how to prevent it», Clario, https://www.clario.com.

[20]. ASM Educational Center, «CompTIA Sec+ | Microsoft MTA Security: Firewall - ASM , Rockville , Maryland», Pinterest, https://www.pinterest.fr.

[21]. Naveen Verma, «An Introduction to the Trojan horse Virus», medium, https://medium.com, Nov 9, 2018.