UNIVERSIDAD POLITÉCNICA DE YUCATÁN

DATA ENGINEERING

5° A

SERVER ARCHITECTURE

UNIT 3

FINAL PROJECT

ETHICAL HACKING

DANIEL GIORDANNO MAGAÑA CRUZ

PROFESSOR: ANGEL ARTURO PECH CHÉ

AUGUST 06, 2019

INDEX

INTRODUCTION

In the give document, I will talk about ethical hacking. Ethical hacking is defined as an act of intruding/penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages. The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing. Ethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the authorized person for the purpose of improving the security and defending the systems from attacks by malicious users.

What I did in this project was to make use of phishing by using many powerful tools, the first one is known as Kali Linux, which is a operative system mostly used by hackers in order to find out vulnerabilities across many things, like for example web pages, operatives systems, applications, between other among of things. The other tool I used was a Social Engineering program that is installed by default on the Kali Linux system, which has the name of setoolkit. Basically, what you can achieve with this tool is to clone a web site in order to gain access over someone and like this, you can show someone, how easy is for a cracker to gain access over your system, network, account, etc. The third tool is constitutional email that we as students have at the UPY, which is my university. I had to use social engineering in order to convince some students to get in to my server and access to the web page and by this, they were able to see their scores.

The web page that I cloned is the one named: mi-escuelamx.com/upy/acceso.asp, which is the web page that we as students use in the university in order to check our

scores and many other interesting things, and with this tool (setoolkit) I did the hard work, it allowed me to clone the whole page and by using my local IP address, a port and a local server called apache2, I was able to gain access over their accounts. The tools once I used it, it automatically detects the username and the password of someone, but only if they are connected to the same network as I am. In this case the network I was connected with was the Students network, so I am using again social engineering and gathering information, because I am knowing that most of students use this network and also I am making them to believe that I am doing some settings on the web page. But I am only showing how easy is for a cracker to gain access over your account, with the purpose of the ethical hacking and to show all this in my project.

With no having more to add, I hope you guys like this project.

MATERIALS

The materials I used in order to make this amazing practice are the following:

- Laptop of 8GB of RAM, intel i5 as the processor.
- USB 2.0: is a Universal Serial Bus (USB) standard.
- Kali Linux booted in the USB
- Setoolkit: The Social-Engineer Toolkit is an open-source penetration testing framework designed for social engineering. The Social-Engineer Toolkit (SET) was created and written by the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon. With over two million downloads, SET is the standard for social-engineering penetration tests and supported heavily within the security community.
- Institutional email: nameenrollment@upy.edu.mx
- Scores web page: mi-escuelamx.com/upy/acceso.asp
- Local IP
- Port 80
- Apache HTTP Server Project, the goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.
- Video recorder of Kali Linux

HACKING TECHNIQUES

The technique that I used in this great project is the one called phishing

Phishing is a social engineering technique used by ethical hackers, crackers and many other people in order to obtain confidential information such as usernames, passwords, credit card details, etc. by posing as reliable and legitimate communication.

The Phishing scenario is generally associated with the ability to duplicate a web page to make the visitor believe that it is on the original website, rather than the fake one. The deception is usually carried out through email and often these emails contain links to a fake website that looks almost identical to a legitimate site. Once on the fake site, unsuspecting users are tricked into entering their confidential data, which provides criminals with ample scope for scams and scams with the information obtained.

How to recognize a Phishing message

It is not always easy to recognize phishing messages by their appearance. However, faithfully reproducing the format of a company requires time and effort that criminals are not usually willing to invest. Errors, inconsistencies or misspellings are a clear indication. Also look at the sender's address.

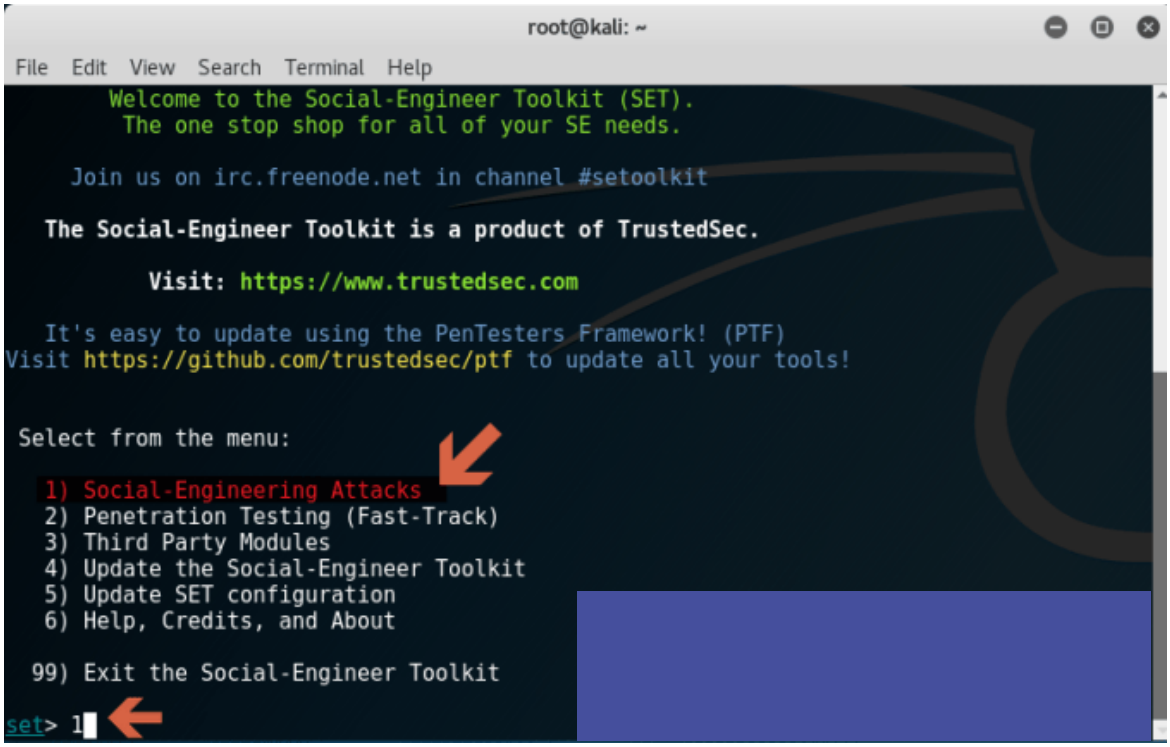
Be cautious in operations from your smartphone. The growing popularity of smartphones makes many users perform many of their efforts on their mobile. Criminals know this and try to take advantage of the loss of clarity resulting from smaller screens and lower security measures.

PROCESS OF DOING THE PHISHING BY USING SETTOLKIT

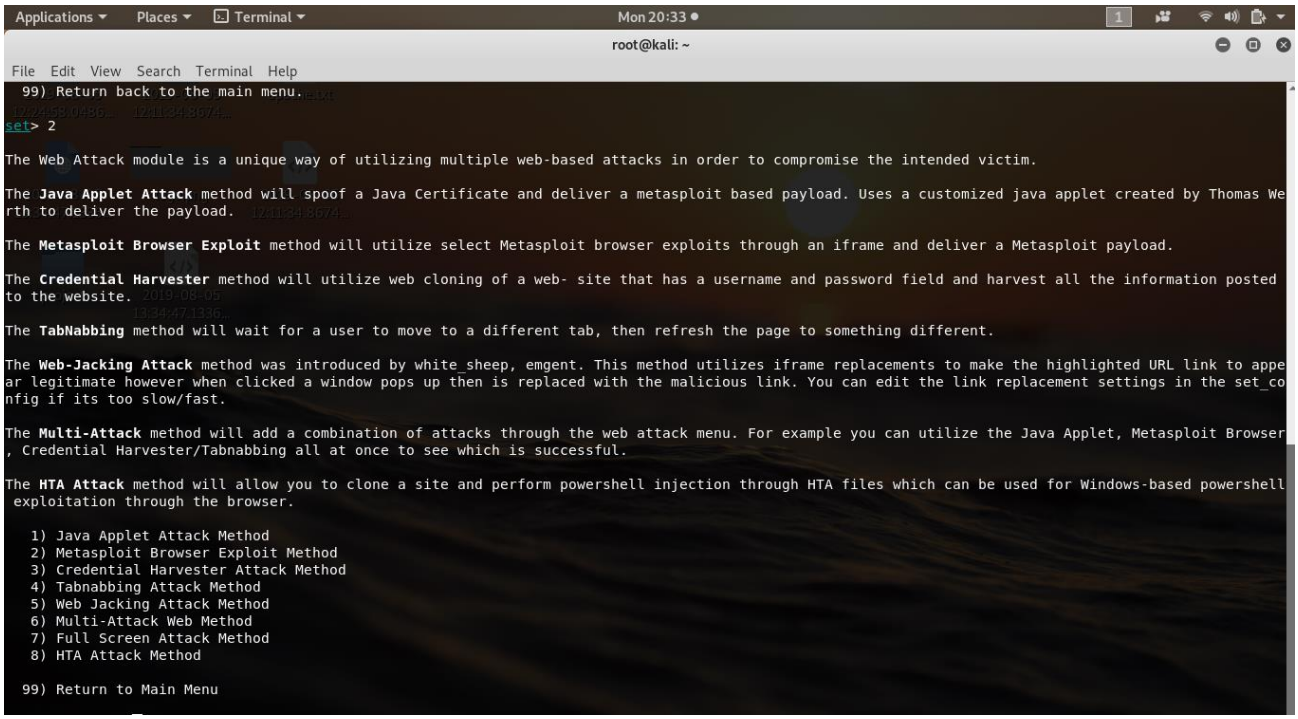
The first thing we have to do is open Kali Linux

Then we have to open a terminal and by default when you download Kali Linux, this tool is already installed there, on the terminal you have to type setoolkit and something like this, will be displayed on screen:

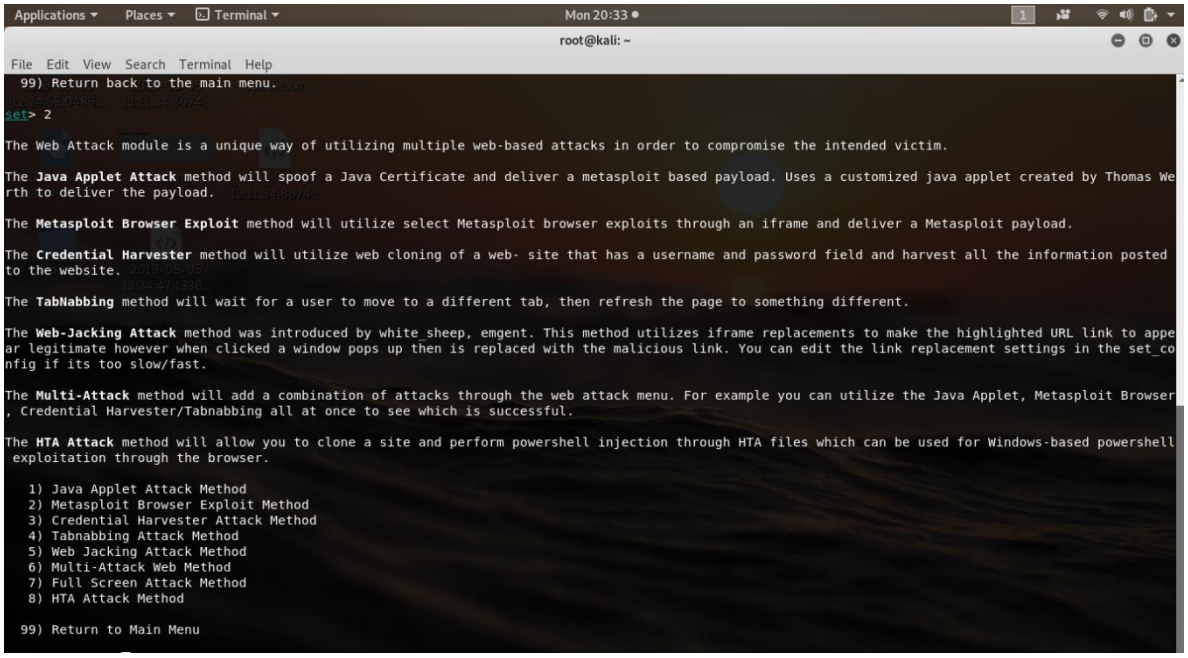
After this, we have to choose the number one, which is a Social-Engineering Attack and we type enter, something like this will be shown.



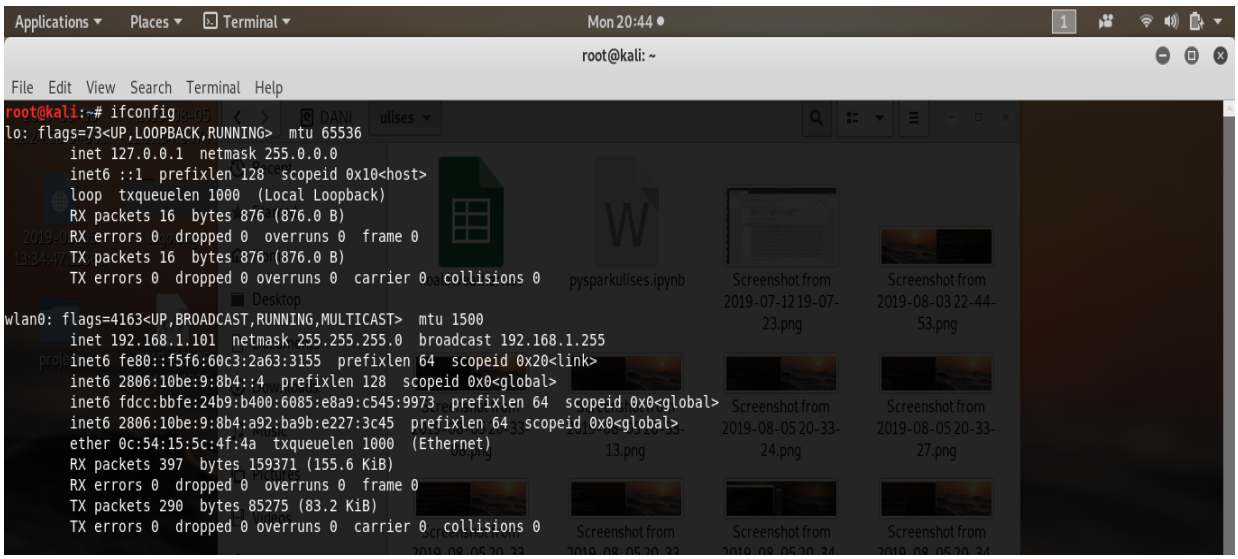
Then we choose the option number two:



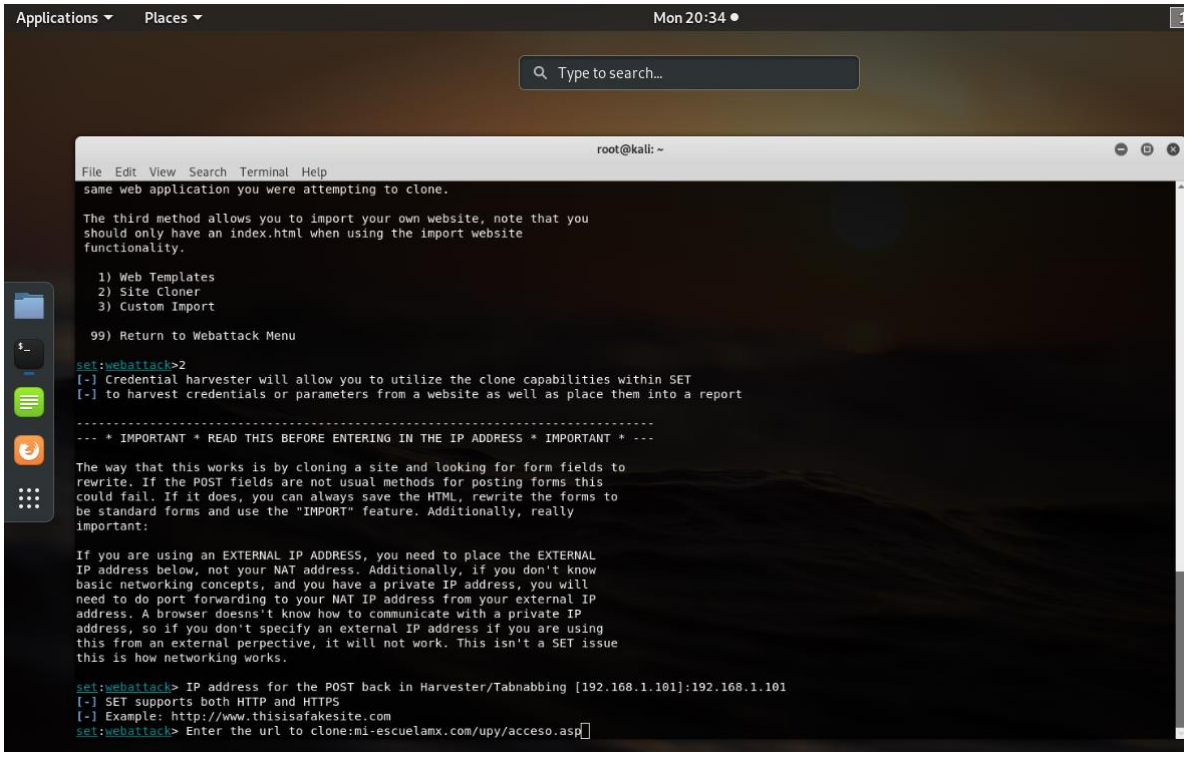
Then we choose the option number 3, which is the credentials option



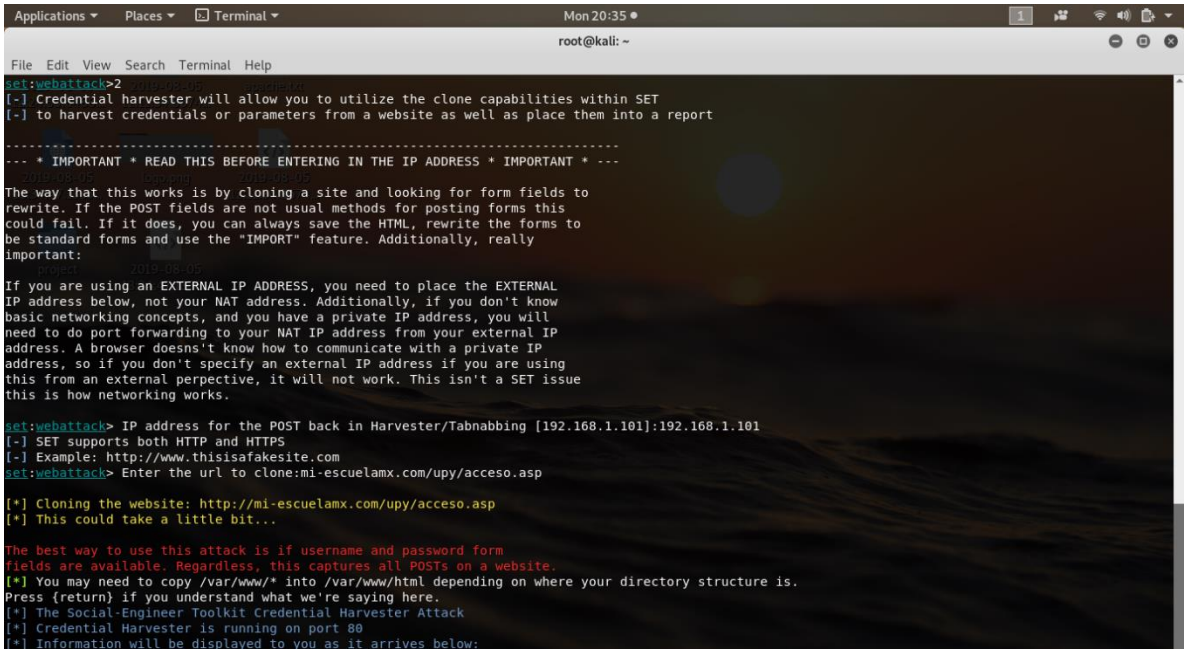
We put our local IP by opening a new tab and putting ifcongig



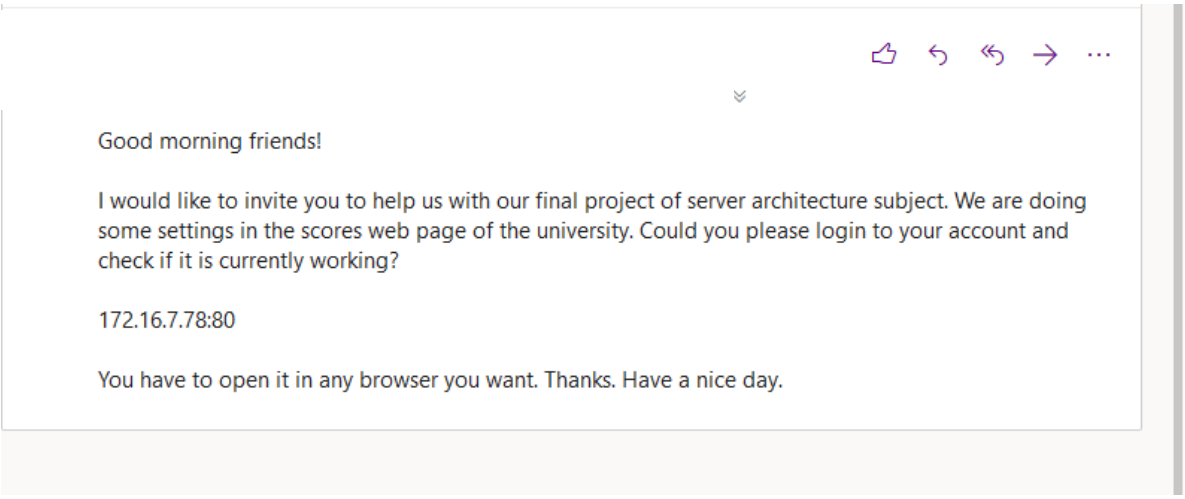
Then we clone the web page by selecting the number 2, which is the site cloner option. Here, we see it and then we put our port in which we will listen it to:



Then we put the name of the web page and it will start running



Then we send an email convincing people to open it



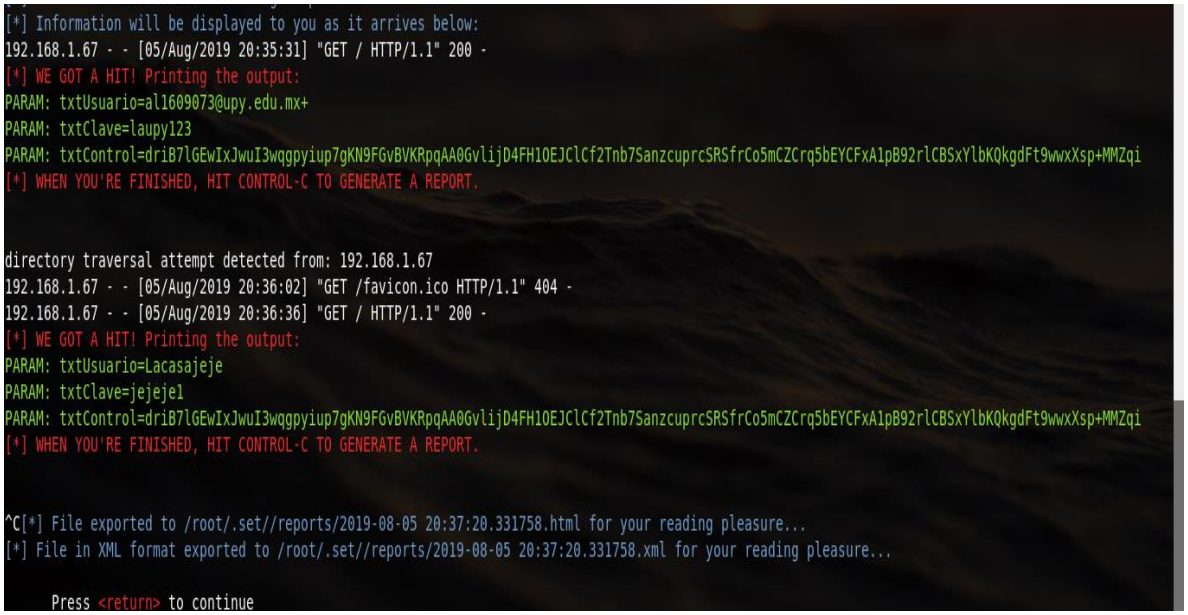
Good morning friends!

I would like to invite you to help us with our final project of server architecture subject. We are doing some settings in the scores web page of the university. Could you please login to your account and check if it is currently working?

172.16.7.78:80

You have to open it in any browser you want. Thanks. Have a nice day.

So then we have to wait until someone open it and start a session, like this:



```
[*] Information will be displayed to you as it arrives below:
192.168.1.67 - - [05/Aug/2019 20:35:31] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: txtUsuario=al1609073@upy.edu.mx+
PARAM: txtClave=laupy123
PARAM: txtControl=driB7lGEwIxJwuI3wqgpyiup7gKN9FGvBVKRpqAA0GvlijD4FH1OEJClCf2Tnb7SanzcuprcSRSfrCo5mCZCrq5bEYCFxA1pB92rlCBSxYlbKQkgdFt9wwxXsp+MMZqi
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


directory traversal attempt detected from: 192.168.1.67
192.168.1.67 - - [05/Aug/2019 20:36:02] "GET /favicon.ico HTTP/1.1" 404 -
192.168.1.67 - - [05/Aug/2019 20:36:36] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: txtUsuario=Lacasajeje
PARAM: txtClave=jejeje1
PARAM: txtControl=driB7lGEwIxJwuI3wqgpyiup7gKN9FGvBVKRpqAA0GvlijD4FH1OEJClCf2Tnb7SanzcuprcSRSfrCo5mCZCrq5bEYCFxA1pB92rlCBSxYlbKQkgdFt9wwxXsp+MMZqi
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


^C[*] File exported to /root/.set//reports/2019-08-05 20:37:20.331758.html for your reading pleasure...
[*] File in XML format exported to /root/.set//reports/2019-08-05 20:37:20.331758.xml for your reading pleasure...

     Press <return> to continue
```

RECOMENDATIONS

The recommendations to avoid and prevent this type of malicious things are the following:

As a general rule, reject attachments and analyze them even when you are waiting to receive them.

Use antivirus and firewall. These applications do not take care of the problem directly but can detect emails with Trojans or unauthorized or suspicious incoming / outgoing connections.

Never click on a link included in an email. Always try to manually enter any website.

Know that your entity, company, organization, etc., whatever you are, will never ask you for confidential information by any means, either by telephone, by fax, or by email, or through any other existing means. It is very important to highlight this point and if you receive an email of this type, ignore it and / or delete it.

Another way to know if you are really entering the original site, is that the web address of the page should start with https and not http, as is the custom. The final “S” gives us a high level of confidence that we are browsing a secure web page.

You should avoid web pages that only have the ip address like the following: 172.16.7.78:80. Because usually these ones are not s legitimate as the ones that have the domain name.

It is a good habit to verify the digital certificate that is accessed by double-clicking on the status bar lock at the bottom of your browser (currently some browsers may also display it in the top navigation bar).

Do not respond to requests for information that arrive by e-mail. When real companies need to contact us they have other ways of doing so, of which email will never be a part due to their inherent security problems.

If you have questions about the legitimacy of an email, telephone the company at a number you know in advance, never call or make contact the numbers, information that come in the messages received

Email is very easy to intercept and fall into the wrong hands, so you should never send passwords, credit card numbers or other sensitive information through this medium.

DESIGN: NETWORK SCHEMA

I made this project at the University, which is a Network of type WPA2. The name of the network is Students. I decided to connect myself to this network because most of students are connected to this one. Then I used my own laptop as a node, in other words my laptop was put as a server, because it basically received all the network traffic to my local IP and to my local port which was: 172.16.7.78:80.

REFERENCES

- Social Engineering Toolkit Phishing (cybersecurity) Loi Yang - https://www.youtube.com/watch?v=sZ8jlQPhbLU&t=115s
- Trustedsec/social-engineer-toolkit Trustedsec - https://github.com/trustedsec/social-engineer-toolkit
- Kali Linux: Social Engineering Toolkit https://linuxhint.com/kali-linux-set/
- Using the Social Engineering Toolkit In Kali Linux By - http://www.fixedbyvonnie.com/2015/06/using-the-social-engineering-toolkit-in-kali-linux/
- What Is Phishing? - Definition from Techopedia https://www.techopedia.com/definition/4049/phishing
- Infospyware Marcelo Rivero - https://www.infospyware.com/articulos/que-es-el-phishing/

CONCLUSION

After doing this whole work I got to more than one conclusion. The first one is that this doing phishing, could be seen as an easy task to make, but is not like that, because first of all, you have to find any program that could make this, also you have use social engineering, which is not something really easy. Maybe you are asking yourself, what social engineering is, well it is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

The advantage in this case was that I knew a little bit about how to use Linux and that helped me with Kali Linux. Then I did a huge research about how to implement it in my own way, which was by cloning the grades site of my school.

Phishing could turn our into something really dangerous for a normal person, because if you do not have those knowledges about how to identify a phishing, you could be lied really easily and like this, all your information could be stolen.

I also got to the conclusion that the grades web page of the school is not so secure, because it was cloned faster than others. It did not mattered that it had the s in the http (https), it was able to clone it in the same way.

It is so interesting and funny to implement this kind of phishing, because in this project I used my institutional email and many classmates logged in there and that web page did not have the domain name as it is accustom to, it only had my local IP and my listener port.