Network Security Lab (MITM & Honeypot)

Author: Cesar Rodriguez Morales
Advisor: Dr. Jeffrey Duffany
Department Electrical & Computer Engineering and Computer Science Department

Abstract

Many people on the IT environment knows that internet can be a dark and dangerous place; featuring viruses and cyber attacks. But the rest of the people across the internet not think that are really exposed to be attacked. This project aims to uncover some of these threats and reveal just how vulnerable the internet can be. This project involves the implementation of a honeypot (a device designed to attack and observe the cyber attackers behavior) and to analyze cyber attacks to see what is going on in the dark underworld of the internet.

Key Terms : HonneyPot, MITM, Cyber-Attacks, Threats, Security, Vulnerabilities, Internet.

Introduction

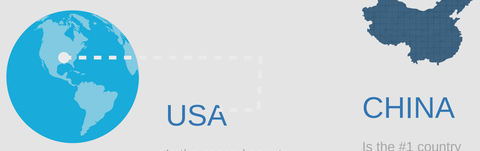
To introduce this project is necessary identify that the main focus for this project is the behavior and analysis of threat through the building a honeypot to research cyber-attack techniques and will also use the famous "man in the middle" to see the importance of use a secure WIFI connection..

-MAIN FOCUS

Is the network behavior across the internet.

Background

The term Cybersecurity includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection. From here on viruses went, well, viral and dominated the headlines. The Melissa and ILOVEYOU viruses infected tens of millions of PCs, causing email systems around the globe to fail, all with little strategic objective or clear financial motivation. These threats led to the development of antivirus technology in order to spot the signature of the virus and prevent it from executing. Equally as important, these threats also played a huge role in driving the awareness of computer users of the risks of reading emails from untrusted sources and opening their attachments.



USA

Is the second country most affected by cybercrime.

CHINA

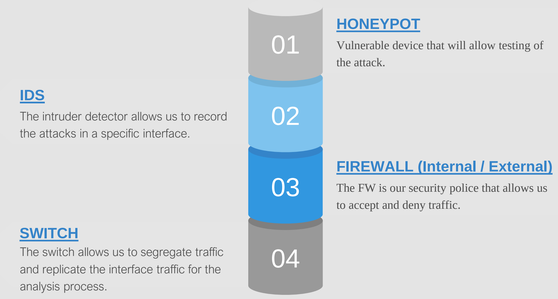
Is the #1 country most affected by cybercrime.

Problem

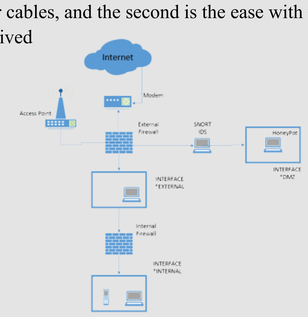
The importance of this project is to be able to see more clearly how vulnerable we are and we dangerous can be the public WIFI. This creates a big problem since many of the users who surf through the internet are not properly protected. In certain cases they only have a free antivirus program that does not include all the necessary tools.

Methodology

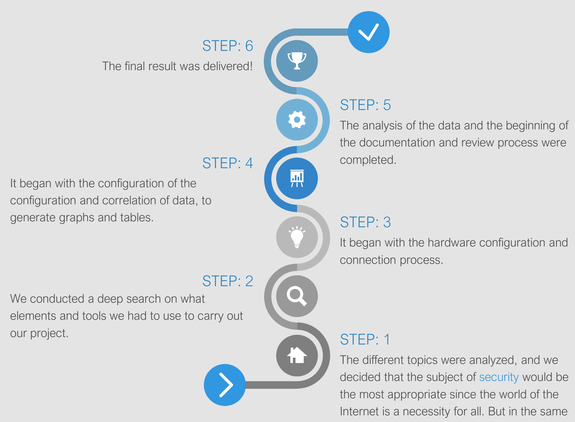
The central idea of this research project is to create a security laboratory that is composed of 5 main elements: (Honeypot, IDS, Internal Firewall, External Firewall, Switch).



The diagram that was created was strategically designed to apply with both tests. For this reason, we use the integration of an access point in which the port mirror was made. This has 2 advantages, the first is that it allows you to connect multiple devices without the need for cables, and the second is the ease with which users can be deceived

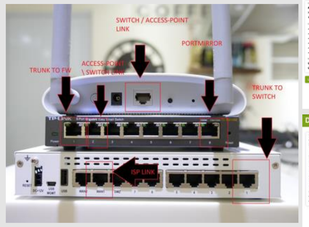


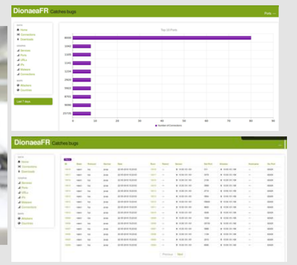
To carry out tests with MITM there are many tools on platforms such as KALI LINUX that allow us to obtain data without users perceiving it. For project purposes I will use the Wireshark tool for the ability to capture traffic and for the ease with which it can be obtained by any user as it is completely free. To perform these tests, I will use the NMAP tool to verify its behavior through the port mirror.



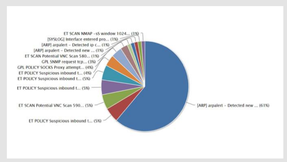
Results and Discussion

For this stage of results, as we had foreseen, our HoneypPot did not manage to collect the necessary data for our project and it is time to implement stage D and attack our HoneyPot and see its behavior.



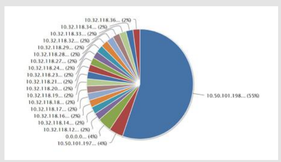


After completing the attack on our vulnerable machine we were able to obtain 10,018 events reported by our HoneyPot with the highest concentration of events on port 8080. What was expected because it is a vulnerable HoneyPot in this type of ports contrary to distributions like KIPPO that are focused on ssh port (22).

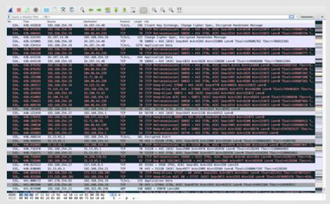


Another important analysis was the verification of the attack sensors. In this way we were able to reach the conclusion that the signature with the most record was [ARP] arpalert with 61% over the others.

No less important, it was the registry of IP addresses that attacked the system. In this case it was already expected that the IP (10.50.101.198) was in the number 1 position. This is due to the attacks made with this IP from Kali Linux.



One of the easiest way to deceive a user is by giving a free wifi signal just like the food and demos places do. Users think that they are safe but do not know how easy they can be deceived without knowing it. For this reason, the configured ports mirror interface is powered by an access point to which I will remotely connect pretending to be a regular user.



In just 4 minutes you can get a capture of over 53,000 packages. Using the Wireshark tool. Captures were also made at the terminal level with the TCPDUMP command **(sudo tcpdump -i eh4 -nnvvv vlan and host 192.168.254.23**).

These captures were in PCAP format which allows us to analyze them with the different data analysis programs with the same Wireshark. It is important to mention that the interface used was l eht4 which is configured as promiscuous for monitoring.

Conclusions

In conclusion mode, I can conclude by reaffirming that time is the key to investigations. The initial motive of this project was the creation of the honeypot with the hope of being able to analyze natural events in which real patterns could be created on which to base research and develop new defenses. In addition, the use of DIONAEA and SNORT was phenomenal because it can interact with two powerful tools. Even with this fact, I can analyze the functionality of the tools and their response to common attacks. I cannot say that it was a failure because the amount of information that can be learned was immense what from the professional point of view made me increase my level of knowledge in areas where I had not been involved. In conclusion it was a great learning and implementation experience.

Future Work

As a future plan, I want to be able to establish the honeypot at a level of development in which I can be exposed to the internet for more time in order to obtain more accurate data on which I can develop appropriate security methods. In addition to my future plans is the use of other detection tools such as SURICATA and SPLUNK to integrate syslog services. I would also like to integrate other Honeypots with different vulnerabilities like KIPPO for SHH we're brute-force attacks are very common.

Acknowledgements

I would like to acknowledge all the people that contributed on the survey and to Dr. Jeffrey Duffany with his guidance during the project.

References

[1] British Computing Society: Code of Conduct. http://www.bcs.org/category/6030.
[2] British Computing Society, The Chartered Institute for IT. http://www.bcs.org/.
[3] Brute force attack image. http://lightningbase.com/security/wordpress-bruteforce-attack/.
[4] Data Protection Act 1998. http://www.legislation.gov.uk/ukpga/1998/29/contents.
[5] Dionaea, catches bugs. http://dionaea.carnivore.it/.
[6] Distributed denial-of-service attack image. http://www.betterhostreview.com/tag/ddos-attackprotected-hosting.