ETHICAL HACKING OF PUBLIC NETWORK

Zakia Ben Youss Gironda and Aparicio Carranza

Computer Engineering Technology

18th Annual City Tech Poster Session

ABSTRACT

Restaurants, malls and coffee areas provide public free WiFi access to attract customers due to its flexibility and feasibility. These type of networks have been popular among the public in recent years; however, it is understood that they create a major threat. User's personal information of the network can be easily be targeted by hackers. Our objective is to assess the weakness of the public network. The objectives will be achieved by creating a sniffer packet from a primary Linux based device. We will then use the primary device to hack information from our secondary device connected within the same network. The Python Programming Language will be used along with some popular beginner libraries such as an SCAPY, IMPACKET and LIBNMAP.

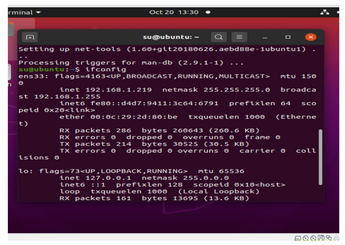
INTRODUCTION

- **The purpose of this project is to assess the security of public networks.**
- **we will discuss in debt the Linux environment set up of the devices that we will use for our project.**
- **We will explain the differences between private and public networks, and how Public Networks are venerable to threats and easily targeted by Hackers [1] to steal passwords, credit card information, etc.**
- **We will then discuss this eavesdrop on signal/packets process that is referred to as Sniffing and discuss how it is coded, structured and how the hacking of sensitive information is achieved.**
- **We will construct a sniffer packet using Python language to target a device B from a device A connected within the same public network and discuss the implementation steps of the attack.**

IMPLEMENTATION/TOOLS

Virtual Machine Set up

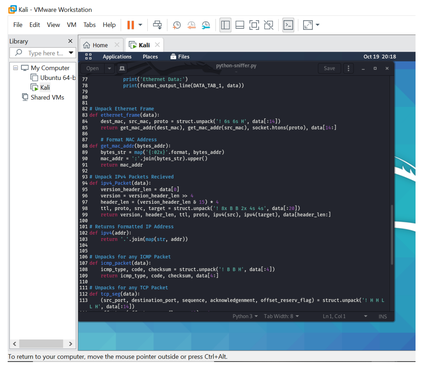
- **Installing VMware**
- **Installing Linux OS Kali**
- **Setting up root password for root privileges**
- **Installing Python Libraries such as *SCAPY, IMPACKET and LIBNMAP***

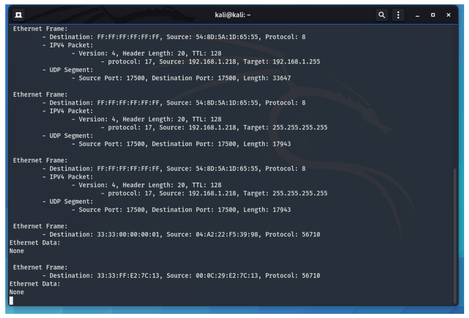


METHOD

- **Sniff passively all wireless traffic packets using SCAPPY. Each packet received goes into a function for processing.**
- **interrogate and extract data from each packet using IMPACKET which is one of the popular packet manipulation libraries**
- **There are three types of wireless (aka. 802.11) packet: management, control, and data. Extract the key fields from the Radiotap headers and write these along with the current timestamp to an in-memory queue.**

PROJECT RESULTS





Current results show sniffing of all raw available data. The next step involves unpacking the data and process the information

CONCLUSION

- **Open networks connections are vulnerable and give Hackers access to sniff out information that passes between the user of the network and the websites visited [2]. The information sniffed can consist of sensitive and private details of browsing activities, account logins and password, credit card information and purchase transactions.**
- **Public malls and coffee shops that provide open networks for their users need to reinforce their digital security.**

REFERENCES

[1] Us.norton.com. 2020. The Do's And Don'ts Of Using Public Wi-Fi. [online] Available at: https://us.norton.com/internetsecurity-wifi-the-dos-and-donts-of-using-public-wi-fi.html

[2] Nield, D., 2020. How To Stay Safe On Public Wi-Fi. [online] Wired. Available at: https://www.wired.com/story/public-wifi-safety-tips/