NETWORK SECURITY CHECK AND ANALYSIS TOOL FOR THE DEVICE AVAILABLE IN A NETWORK RANGE

Revanth Lagadapati[1]

[1]School of Computer Science of Engineering, Lovely Professional University, Punjab, India.

---***---

Abstract - *This is the web-application implemented with the aim to combine the implementation of different processes like identification of devices in a particular ip range, scanning & finding vulnerable ports and generate the reports. This tool used to scan the devices which are in the network range for any available open ports and some protocols like FTP, Telnet, SSH, TCP, SMTP, After the exploitation done, this tool will generate a report of the device and the ports which are open or not and can be exploited or not. In this paper, we propose a united framework under single web application instead of separate tool for each and every process (identification, scanning and reporting) like 'zenmap' is only used for scanning the devices in particular ip range. And Nmap for port identification. In today's world, network security became a common need for every person who is using the technical device, and daily we are watching many organizations data is being leaked by attackers. For any organization this is the reason why network security playing a vital role, particularly data theft or data loss is the main reason for this and comprisable ports are the main source for attackers. This web-application discussed in this paper will help more number of people who are going to be the victims for data theft. As maximum number of attackers use metasploit framework as their tool and compromise victims' PC, So, with the help of this application report, people come to know that their PC is vulnerable and take precautionary measures like updating or changing OS.*

Key Words: Network security, Port Identification, vulnerability, GNUNetCat, IP Range.

1.INTRODUCTION

Nowadays, it's really tough task to protect our data from attackers than protecting money and valuable things. So network security became very essential in everyone's life. Little technical knowledge like being updated will help everyone regarding security. Cyber criminals mainly focus on ports in hosts, so , it's important to get to know that our system is in absence of vulnerable ports or our system is compromised. So, here we came up with a web application which will help people with less technical knowledge can identify their PC is vulnerable or not.

2. MODULES

The whole project consists of three modules.

1. Identification of the devices
2. Scanning and finding the vulnerable ports
3. Report generation

2.1 Identification of devices:

This is the module which finds the devices connected in the IP range of the network, for that first physically we are going to the particular network which we want to scan and we start running this web application. Then a GUI will appear and it will ask for IP range limit, i.e., starting Range and Ending Range. With the help of the background process i.e., importing the sub processes in python it will display the connected devices IP Addresses.

2.2 Scanning and finding the vulnerable ports:

From the above process, after getting the IP addresses of the devices we will use **GNUNetCat** as the background tool and find the ports of the devices. This complete process will be running in the background where this tool is connected as the backend tool. This process will display all available ports in every device connected in that range.

2.3 Report generation:

After scanning and getting displayed on the screen, this application will particularly pick the devices which are having vulnerable ports and generate a report. Web-application will compare pre given vulnerable ports and the ports displayed after scanning. And it will add that particular device which is having vulnerable ports.

3. IMPLEMENTATION

As we already know, every device has its own MAC address. meanwhile every device in a network has its own IP address. Here, our application will use that exact IP address and use router as a network pathway and implements port scanning for all devices connected with that network

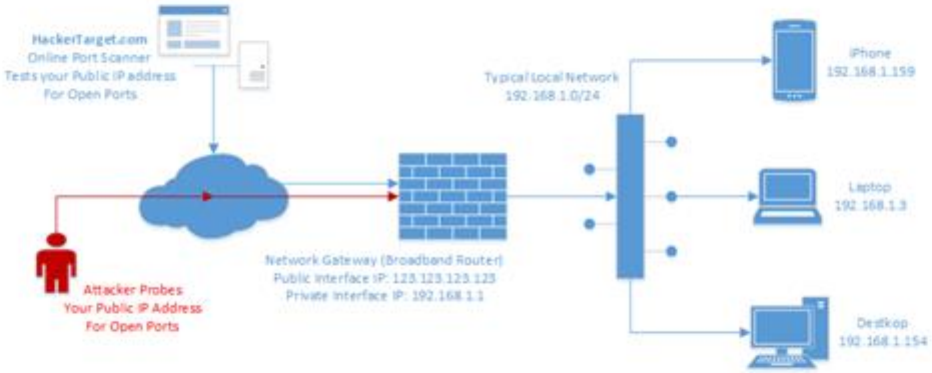

Diagram 1: Devices connected in a network.

After getting the available devices by using GNUNetCat as a backend tool in the background of our web-application and scan vulnerable ports.

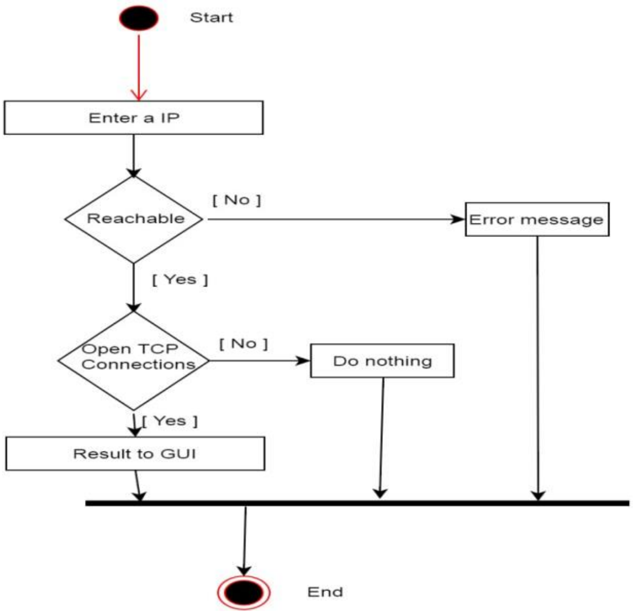

Diagram 2: flowchart for port scanning.

After port scanning as we mentioned above in modules, there will be a compression of given vulnerable ports with ports after scanning and it will give a report if they match.

4.. CONCLUSIONS

The preparation of this web-application used for port scanning is beneficial for many organizations and in many cases. We have done experiment on different networks and for different IP ranges, and we got success rate of almost 90 percent. If they are not using any Proxys or VPNs. This gives the solution for using different modules and getting various results under one web-application.

REFERENCES

[1]. A brief description of port scanning through web link https://nmap.org/book/man-port-scanning-techniques.html

[2]. https://www.geeksforgeeks.org/port-scanner-using-python/

[3]. A book named Network Mapping and Network scanning – Renee B. Williams

[4]. An article https://www.avast.com/business/resources/what-is-port-scanning

[5]. Network Scanning Cookbook: Practical network security 7 Kindle Edition written by Sriram Jetty.

[6]. Hands on Ethical Hacking and Network defense written by Michael T. Simpson, Kent Backman, and James Corley

[7]. A book named ‘A Simple Port Scan – Practical Packet Analysis’ – from O’Reilly

[8]. An article https://www.tripwire.com/state-of-security/featured/common-basic-port-scanning-techniques/

[9]. An article from www.sciencedirect.com , Port Scanning – an overview.