https://doi.org/10.46335/IJIES.2024.9.5.16 **e-ISSN: 2456-3463**
Vol. 9, No. 5, 2024, PP. 69-72

International Journal of Innovations in Engineering and Science, www.ijies.net

Model to Identify Network Devices and Ports

Ansh Gadhia[1], Utkarsh Chandekar[2], Vidyan Tidke[3], Bhakti Thakre[4]

[1, 2, 3] Student, [4]Assistant Professor
Department of Computer Science and Engineering (Cyber Security), SVPCET, Maharashtra, Nagpur, 441108

gryphongatekeepers.hacker29@gmail.com

***Received on**: 12 May, 2024* ***Revised on**: 20 June,2024,* ***Published on**: 22 June ,2024*

***Abstract -** The primary goal of this research is to analyse the depths of the private networks and at the same time, develop a project to study its association with Cyber Security.Network Trailblazzer is a Linux based tool which will help in getting access to the information of devices in a particular private network. As the threats in cyber security networks increase, this tool shall help in quick identification of the device as well as will provide the properties of the device.*

***Keywords**- Private networks, Linux, Access, Tool*

1. INTRODUCTION

Millions of computers spread across vast geographic regions are part of the massive business, academic, and governmental computer networks that exist today. It is necessary to comprehend the architecture and operation of these networks in order to be able to monitor and regulate them. The purpose of this article is to provide the reader an overview of the methods and procedures used to ascertain the composition and operation of such vast computer networks and to offer some guidance on potential visualisations of the data such as this.The recent changes in cyber security attacks and their patterns are quite renowned to the world. These change in patterns have brought upon a vast variety in attacking the networks of a system. Adapting to these changes has become a necessity. To face the new challenges head on development of compatible tools has come into high demands

In conjunction to this, the industry has long deemed etworking and cyber security[10] to be attachable domains, and it has significantly started and codified Linux-based technology. Linux is an open source, community-developed operating system (OS) for PCs, servers, mainframes, mobile devices, and embedded systems that is similar to Unix. As One of the most widely supported operating systems, it is compatible with almost all popular computer platforms, such as SPARC, x86, and ARM.

Network security is essential as organisations depend more and more on IT systems. Without proper security, organisations run the danger of irreversible system damage and reputational harm. Hardware, software, and user education are all included in layered security, which is crucial for thwarting many kinds of network assaults. This section discusses the threats to the confidentiality, availability, and integrity of network resources. Different types of network threats can arise from different sources, such as malware, unauthorized access, phishing attacks, denial-of-service (DoS) attacks, and man-in-the-middle (MitM) attacks. Preventing these network threats demands the use of effective security measures. By correctly implementing security measures, network security avoids data abuse.

2. LITERATURE REVIEW

Network Watcher: A simple tool called Wireless Network Watcher searches wireless network and shows a list of all the computers and gadgets that are currently linked to it. The following details are shown for each computer or device connected to the network: IP address, MAC address,

https://doi.org/10.46335/IJIES.2024.9.5.16 **e-ISSN: 2456-3463**
Vol. 9, No. 5, 2024, PP. 69-72

International Journal of Innovations in Engineering and Science, www.ijies.net

network card manufacturer, and (optionally) machine name.

The list of connected devices may also be copied to the clipboard and pasted into Excel or another spreadsheet programme, or it can be exported as an html, xml, csv, or text file [4].

(This is only limited to windows)

Netdiscover: When tracking, Netdiscover is an active/passive address reconnaissance tool designed primarily for wireless networks without a Dhcp server. Additionally, hub/switched networks can make advantage of it.

In addition, Netdiscover may be used to examine your network's ARP data and locate network addresses by utilising its auto scan mode, which looks for widely utilised local networks[5].

(We need to provide every detail to netdiscover; Ex: IP address)

Arp command: The Internet-to-adapter address translation tables used by the Address in Networks and communication management may be seen and altered using the arp command. The host identified by the HostName variable's current ARP entry is shown by the arp command. Using Internet dotted decimal notation, the host can be given either by name or number. Arp command works similar to the tool but sometimes it won't show all the IP addresses in a network[6].

(The output of data gained by this command has low reliability)

3. METHODOLOGY

Ifconfig: The kernel-resident network interfaces are configured using the ifconfig (interface configuration) command. It is utilised to configure the interfaces as needed during boot up. After that, it is typically utilised when system tweaking or debugging are required. This command may also be used to enable or disable a specific interface as well as assign an IP address[2] and netmask to it[3].

Ping: To ascertain the network connectivity between the host and server/host, use the PING (Packet Internet Groper) command. When a data packet with the message "PING" is sent to the given address using the IP address or URL as input, the server or host responds, and this time is logged. This is known as latency. A quicker connection is indicated by a fast ping and low latency. Ping delivers an ICMP reply message if the host is up and running, else it utilises the Internet Control Message Protocol (ICMP) to send an ICMP echo message. Milliseconds are typically used to measure ping. This ping is pre-installed on all current operating systems[3].

Nmap: The Linux command-line tool Nmap is used for security audits and network research. Network and system administrators, as well as hackers and cybersecurity enthusiasts, typically utilise this program. It has several tags which helps in identifying open or closed ports[7] of a specific IP device[1].

3.1 ALGORITHM

STEP 1: Starts with a welcome note "Welcome to Network Trailblazzer".

STEP 2: The interface displays the user "Are you on a private network?" providing the options (YES/NO).

STEP 3: If "YES", the function scans the network with a parameter yes which then scans the current IP of the device furthermore grepping out its (Host, Network no. and subnet).

STEP 4: A file named "newconfig.txt" is created. Every IP address and iteration that may exist on the private network is pinged linearly, and its availability in the network is verified.

STEP 5: Once the Verification process ends, the mac addresses of provided IPs stored in file: newconfig.txt is scanned and checked using Nmap.

STEP 6: After executing the scanning program, the network information (IP address and Mac address) is printed.

STEP 7: Following the forementioned, the tool asks the user whether they want to check the ports of any device in the available network, providing two options (YES/NO).

https://doi.org/10.46335/IJIES.2024.9.5.16 **e-ISSN: 2456-3463**
Vol. 9, No. 5, 2024, PP. 69-72

International Journal of Innovations in Engineering and Science, www.ijies.net

-

STEP 8: Upon receiving the input "YES", the program provides the data of open and closed ports in the network device via use of Nmap command.

STEP 9: The program stops its execution while displaying the results according to the inputs received.

4. FUTURE SCOPE

The tool's current burst time for scanning every device is 13 minutes. By investigating the issue of time complexity in greater depth in the future and work to minimise the burst time to as low as possible.

- To connect the tool to a Database to improve the scope of data.
- Creating a storage for storing the Static IP's
- To adjointly develop an API (Application Programming Interface) for provide an user friendly environment.

5. RESULT AND CONCLUSION

- Beyond what many now expect, the next decade's innovations in computing are bound to transform the way we conduct ourselves and improve our digital existence.

- The prototype that is being described in this article exemplifies the fundamental ideas required to verify connection across the entirety of the devices in a network.

- By iterating every IP that might possibly exist in a given network, this model is able to obtain the MAC and IP addresses of such networks. Additionally, it provides the user with information about the ports that are accessible on the devices. This would open the way for beginner hackers get better understanding of the network with which they are associated

- Subsequent researches are necessary to examine the devices more comprehensively, potentially minimising time and facilitating the integration of various devices.

- Although the benefits of the digital revolution for everyday life are abundantly apparent, they are still mostly unrealized.

REFERENCES

[1] *Nmap: https://nmap.org*

[2] *GeeksforGeeks: https://www.geeksforgeeks.org/structure-and- types-of-ip-address/*

[3] *Linux basics for hackers: getting started with networking, scripting, and security in Kali | Author: OccupyTheWeb Description: First edition | San Francisco: No Starch Press, Inc., [2018]. | Subjects: LCSH: Penetration testing (Network and computer security), Kali Linux, Hackers, Operating systems (Computers) | Chapter No. 8: Bash Scripting.*

[4] *Network Watcher: https://www.nirsoft.net/utils/wireless_network*

a. watcher.html

[5] *Netdiscover: https://www.kali.org/tools/netdiscover/*

[6] *Arp: https://www.ibm.com/docs/en/aix/7.2?topic=ar p-command*

[7] *Port and Network Scanning: https://www.varonis.com/blog/nmap-commands*

[8] *The basics of IP address: https://www.ipv4mall.com/blogs/exploring-ip-addresses-why-are-they-divided-into-four- parts/*

[9] *Padole, D. M., Kanani, P., Raut, L. E. E. N. A., Jhaveri, D., & Nagda, M. A. N. A. L. I. (2017). An Insight into IP Addressing. Oriental Journal of Computer Science and Technology, 10(1), 33-40.*

[10] *Forouzan, B. A. (2007). Data communications and networking. Huga Media.*

[11] *IPv4 – Addressing: https://www.tutorialspoint.com/ipv4/ipv4_quick_guide.html*

[12] *Public and Private IP address: https://www.iplocation.net/public-vs-private- ip-address*

[13] *Public and private IP Addresses: http://referenceswww.siliconindia.com/online-courses/tutorials/What-are-Private-and-Public- IP-Addresses-id-109.html*

[14] *Lyon, G. F. (2009). Nmap network scanning: The official Nmap project guide to network discovery and security scanning. Insecure*

[15] *McCarty, C., Molina, J. L., Aguilar, C., & Rota, L. (2007). A comparison of social network mapping and personal network visualization. Field methods, 19(2), 145-162.*