A Smart Network and Port Scanning Tool

Abstract

*In computer networking, a port is a communication endpoint. At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service. The most common transport protocols that use port numbers are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). Port scanning refers to the surveillance of computer ports[11], done by us when we are trying to communicate with a certain computer. We conduct port-scanning techniques in order to locate holes within specific computer ports. To be able to check whether a service is currently running on a port or how many services are running or to scan number of hosts alive in a network, where we need to ping every single IP of the network and wait for the response, seems hectic and for this particular reason, a network automation tool will come very handy for the user and as a solution to this and a lot more, we bring **DEDMAP** - a Simple but Powerful, Clever and Flexible Cross-Platform Port Scanning tool made with ease to use and convenience in mind.*

***Keywords**: Networking; TCP; UDP; Automation; Dedmap;*

1. Introduction

An interconnection of hosts(devices) to help them communicate with one another is called Networking. There are devices available to make networking possible such as Router, Hubs, Switch, and Bridge.

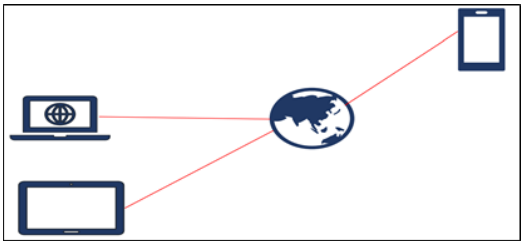

Figure 1: Depiction of Networking among devices

The sole purpose of networking is to help devices communicate with each other. But how? How can devices communicate with each other?

A very common example is When we go to someone’s house, the first thing we do is to knock on the door to check whether someone is inside or not. In the world of technology, Ports are somewhat an equivalent to “doors”. A port is a place where information is sent or received on a computer. If someone has to send data to a computer, they need to send it through the designated port.

Now to determine whether a port is open and listening (receiving message) one needs to communicate with a port and see if the services are sending back any response. Ports are software-based and managed by a computer’s operating system. Every port is associated with a specific service. They allow computers to differentiate between different kinds of traffic. Ports are standardized across all network-connected devices. Most ports are reserved for certain protocols — for example, all Hypertext Transfer Protocol (HTTP) messages go to port 80. While IP addresses enable messages to go to and from specific devices, port numbers allow targeting of specific services or applications within those devices. These open ports can be exploited through code vulnerabilities or malicious services by attackers. That is why being aware of the unused ports and closing them is considered to be the best practice to stop these attacks.[1]

2. Background Study

There are numerous tools available in the market to help with port scanning all their unique features. The top 4 best ones (according to SecurityTrails) [2] are:

(1) Nmap[3],

(2) Unicornscan,

(3) Angry IP Scan and

(4) Netcat.

There are many more tools available for scanning ports and live hosts on a network but the ones mentioned above are the most significant ones. Upon doing further research on them we found their significance as below:

2.1 Nmap:

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Nmap has evolved over the years and is extremely flexible, at heart it's a port-scan tool, gathering information by sending raw packets to system ports. It listens for responses and determines whether ports are open, closed or filtered in some way by, for example, a firewall. Other terms used for port scanning include port discovery or enumeration. [4]

2.2 Unicornscan:

Unicornscan is a new information gathering and correlation engine built for and by members of the security research and testing communities. It was designed to provide an engine that is Scalable, Accurate, Flexible, and Efficient. It is released for the community to use under the terms of the GPL license.

Features of Unicornscan are as follows:

- Asynchronous stateless TCP scanning with each of the TCP flags or flag combinations
- Asynchronous protocol-specific UDP scanning
- superior interface for measuring a response from a TCP/IP enabled stimulus
- Active and Passive remote OS and application detection
- PCAP file logging and filtering
- capable of sending packets with different OS fingerprints than the OS of the host.
- Relational database output for storing the results of your scans
- Customizable module support to fit according to the system being pentested
- Customized data set views.
- Has its TCP/IP stack, a distinguishing feature that sets it apart from other port scanners
- Comes built into Kali Linux, no need to download [5]

2.3 Angry IP Scanner:

Angry IP scanner is a very fast IP address and port scanner. It can scan IP addresses in any range as well as any their ports. It is cross-platform and lightweight. Not requiring any installations, it can be freely copied and used anywhere. Angry IP scanner simply pings each IP address to check if it’s alive, then optionally it is resolving its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be extended with plugins [6][7].

Features of Angry IP Scanner are as follows:

- Scans local networks as well as Internet
- IP Range, Random or file in any format
- Exports results into many formats
- Extensible with many data fetchers
- Provides command-line interface
- Over 29 million downloads
- Free and open-source
- Works on Windows, Mac and Linux
- Installation not required.

2.4 NETCAT

Netcat is a command line tool responsible for reading and writing data in the network. To exchange data, Netcat uses the network protocols TCP/IP and UDP. The tool originally comes from the world of Unix but is now available for all platforms. Netcat is often called the “Swiss army knife for TCP/IP”. For instance, it allows us to diagnose faults and problems that jeopardize the functionality and security of a network. Port scans, data streaming or simple data transfers can also be performed by Netcat[8][9].

Features of Netcat are as follows[10][11]**:**

- Outbound or inbound connections, TCP or UDP, to or from any ports
- Full DNS forward/reverse checking, with appropriate warnings
- Ability to use any local source port
- Ability to use any locally configured network source address
- Built-in port-scanning capabilities, with randomization
- Built-in loose source-routing capability
- Can read command line arguments from standard input
- Slow-send mode, one line every N seconds
- Hex dump of transmitted and received data
- Optional ability to let another program service establish connection.
- Optional telnet-options responder

3. Problem Identification

The whole networking concept makes no sense if devices cannot communicate with each other. Devices communicate through ports so, to communicate one needs to get in touch with the designated port of the target device. But pinging all computers on a network at once is not feasible. Neither is pinging all ports of a computer manually time-efficient. We need a tool that automatically does the job for us and is user friendly and fast.

There are numerous tools out in the market but everyone has their own cons. They do not have the required features all in one place which is why we worked up one, keeping convenience and ease in mind specially.

Our tool is named DEDMAP and the logo is given below:

Figure 2: Logo of DEDMAP

4. Proposed Model

DEDMAP is a Simple but Powerful, Clever and Flexible Cross-Platform Port Scanning tool made with ease to use and convenience in mind. Both TCP and UDP protocols have 0 to 65535 ports. These 65535 ports can be divided into the following three ranges [12][13]:

System or reserved ports: from 0 to 1023
User or registered ports: from 1024 to 49151
Dynamic or private ports: from 49151 to 65535

The features of DEDMAP are enlisted below:

- It tries to scan a target IP or range of IP's and find services that are running and listening on some ports.
- It can also scan a range of hosts to find live hosts.
- It performs both DNS and rDNS lookup.

- It performs sweep scan.
- Full Support for Android devices (via termux)

The proposed working of DEDMAP is depicted in the picture below:

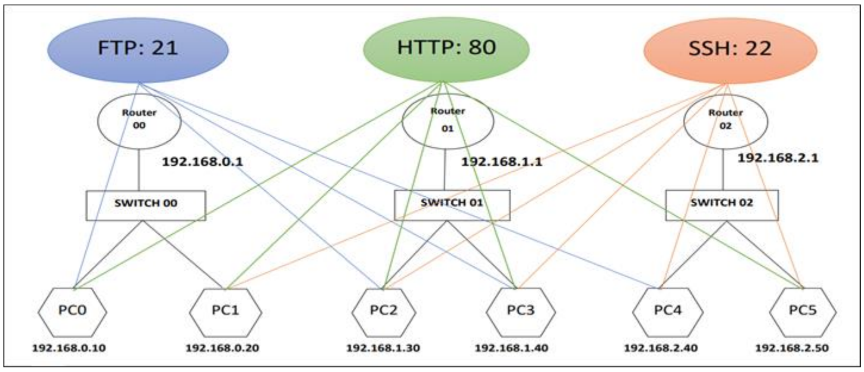

Figure 3: Depiction of Working of DEDMAP

Our tool DEDMAP is focused on automatically discovering open ports of specified targets. Consider the block diagram above, suppose user on PC0 wishes to check open ports on PC2. When the PC0 user types the command to check open ports on the target IP i.e.192.168.1.30 the output returns the port number 21,80,22 are open on the target as shown in the picture.

5. Material

Materials needed to build this tool are:

Python3:
Python 3.0 (a.k.a. "Python 3000" or "Py3k") is a new version of the language that is incompatible with the 2.x line of releases. The language is mostly the same, but many details, especially how built-in objects like dictionaries and strings work, have changed considerably, and a lot of deprecated features have finally been removed. Also, the standard library has been reorganized in a few prominent places. [14]

Pip:
pip is the package installer for Python. You can use pip to install packages from the Python Package Index and other indexes. [15]

pyfiglet:
pyfiglet is a full port of FIGlet (http://www.figlet.org/) into pure python. It takes ASCII text and renders it in ASCII art fonts (like the title above, which is the 'block' font). [16]

funcy:
A collection of fancy functional tools focused on practicality. Works with Python 2.7, 3.4+ and pypy.

numpy:
NumPy brings the computational power of languages like C and Fortran to Python, a language much easier to learn and use. With this power comes simplicity: a solution in NumPy is often clear and elegant.

colorama:
Makes ANSI escape character sequences (for producing colored terminal text and cursor positioning) work under MS Windows. [17]

6. Future Scope

With these features is can be really helpful for network automation. We have plans to make DEDMAP available for chat applications like WhatsApp and Telegram as well in near future which will allow a user to use all the features of DEDMAP in a mobile phone right from a chat application. We will also be adding a small honeypot feature in DEDMAP which will be very useful for monitoring a server for incoming traffic which can be further used as an IDS system. We are yet to fix UDP scanning. We will use multithreading to drastically improve the performance of the tool. We will test the tool and add support for windows.

7. Limitations

DEDMAP is slow as no multithreading is used in the program. UDP does not work properly as of now. The user must maintain the sequence: "dedmap [--option(s)] [target(s)]". The tool supports IP range only in the last octet .i.e 1.1.1.(1-200) . This is also a safety measure to prevent the user from scanning the ENTIRE INTERNET (1-255.1-255.1-255.1-255) and blowing up his/her NIC, RAM, CPU and HARDDISK.

8. Conclusion

DEDMAP is expected to have lots of bugs as it is at a very early stage. It has not been tested in Windows yet and will not work most probably. Some of the example (commands) that you can try out with our tool is as follows:

- dedmap 192.168.0.10
- dedmap localhost
- dedmap –d google.com yahoo.com facebook.com localhost
- dedmap google.com
- dedmap google.com yahoo.com
- dedmap 192.168.0.20 192.168.1.20 192.168.1.30
- dedmap 192.168.0.1-100 google.com (Perform a tcp scan on all the hosts without pinging to bypass firewall icmp block)
- dedmap –p 20 192.168.1.30
- dedmap –p 20,21,22 192.168.3.40
- dedmap –sm lan –p 21 192.168.0.1-255 (Perform a tcp port scan in lan mode on all the live hosts)
- dedmap –s 192.168.3.50-255
- dedmap –sr 192.168.3.40-255 (Perform a reverse dns lookup on all the live targets in the network)
- dedmap –st 192.168.0.1-255 (To scan only the hosts which are alive in the network)
- dedmap –o report.txt 127.0.0.1

We would also like to add that this tool is made for educational purpose only. Use it with/on systems or networks you own or have permission from the owner. We shall not be held responsible for whatsoever you do with this tool.

With our tool, we hope to ease out communication with ports, detecting alive hosts in a network and many more activities for the user.

References

1. Gelnaw,A. MAY 21, 2019. Open Port Vulnerabilities: What's the Big Deal?

2. Borges,E. MAY 22 2018 . Top 5 Best Port Scanners.

3. BBC News. 2003-05-19. "Matrix mixes life and hacking". Retrieved 2018-10-28.

4. Nmap.org. Retrieved 2018-10-28. "The History and Future of Nmap".

5. Younis,S. Unicornscan: A beginner's guide.

6. Keks,A. Angry IP Scanner. Github.

7. Andrew L. Angry IP Scanner 25 Jan 2021 Released on 8 Apr 2004

8. Giovanni G. (2006-11-01). "The GNU Netcat project". Retrieved 2020-03-22

9. Thomas L. (2011-03-02). "Netcat OpenBSD Cygwin Port 1.10.2.3". Daemon.de. Retrieved 2019-06-05.

10. 2008-02-14. "Netcat 1.10". nc110.sourceforge.net.

11. Chirgwin, R.(2016-02-03). "Socat slams backdoor, sparks thrilling whodunit". The Register. Retrieved 2019-06-05.

12. Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry. August 2011. sec. 6. doi:10.17487/RFC6335. RFC 6335.

13. Contract Between ICANN and the United States Government for Performance of the IANA Function, 21 March 2001, archived from the original on 2008-12-26.

14. Kuhlman, D. "A Python Book: Beginning Python, Advanced Python, and Python Exercises". Section 1.1. Archived from the original (PDF) on 23 June 2012.

15. Kollár, L. "Managing Python packages the right way". Opensource.com. Red Hat. Retrieved 23 June 2019.

16. "FIGlet FAQ". Retrieved 2013-09-19.

17. Muhimen "Colored text in terminal using Python" Jun 11, 2020

18. John,P. "RFC 793". Retrieved 29 June 2012

19. Ferranti,M. AUG 17, 2018. What is Nmap? Why you need this network mapper.

20. Mohan K, Computer Port numbers and port number classifications:, October 4, 2010