Net Scan: Web-based Network Scanning Tool

Lee Liang Foong, Julia Juremi and Yogeswaran Nathan

Abstract--- *Cyber security has been highlighted in recent years due to the increasing number of cyber-attacks and the impact it can cause which affect national security. To improve cyber security, network scanning tools are essential where it is used for gathering information about the actual state of a system or network. Therefore, we will examine common modules included in a network scanning tool and 6 common port scanning techniques. In this paper, the differences of existing and proposed system will also be discussed where the proposed system is a web-based network scanning tool named Net Scan which is able to perform host discovery, operating system detection, open ports and services, and trace route.*

Keywords--- *TCP, SYN, ACK, Port, Scanner, ICMP, Net Scan.*

I. INTRODUCTION

As the internet continues to grow and become integral part of our lives, the number of devices connected to the Internet has been exponentially increasing. This state leads to higher degree of threats and probability of vulnerabilities in devices and network connected.

In recent years, cyber security has been highlighted due to the increasing number of cyber-attacks and the impact it can cause which affect national security. Due to that, network scanning tools have been developed to assist network administrator to detect and fix vulnerabilities in systems by network scanning.

Network scanning tools could gather devices information, which are connected to the internet such as operating system, version and open port [1]. With this information, network administrator can find vulnerabilities of those systems and come up with countermeasure to prevent or mitigate probable cyber-attacks.

Network scanning tools may include modules such as IP Scanner, Vulnerability Audit, Port Scanner, NS Lookup, and Trace Route [2]. IP Scanner is used to identify network devices and test whether the host is reachable across an IP network. This is done by sending out echo request packets to the target host and listen for echo response replies. Port Scanner uses operating system’s network functions to test whether the port is open and will terminate the connection before TCP three-way handshake completes.

NS Lookup as the name suggests, finds the name server information for domains by querying the Domain Name System. Trace Route records the path through the Internet between your computer and a specified destination computer. It also calculates and displays the amount of time each hop took. It is also used for understanding where problems are in the Internet network and for getting a detailed sense of the Internet itself [2].

Lee Liang Foong, School of Technology, Asia Pacific Institute of Information Technology. E-mail: TP041203@apu.edu.my
Julia Juremi, School of Technology, Asia Pacific Institute of Information Technology. E-mail: julia.juremi@apu.edu.my
Yogeswaran Nathan, School of Technology, Asia Pacific Institute of Information Technology. E-mail: yogeswaran.nathan@apu.edu.my

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

II. NETWORK SCANNING TOOL

Network Scanning tool gather information regarding computing systems with the aim to scan networks for vulnerabilities in the designed network [1]. These tools detect network devices and identify services on those devices by using fingerprint techniques [1].

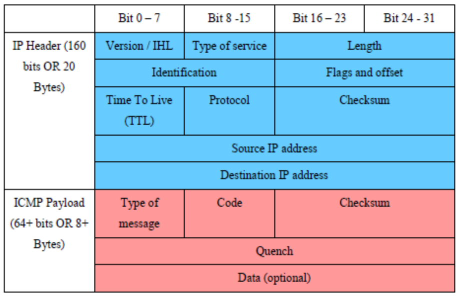
Fingerprinting technique can be classified into active fingerprinting and passive fingerprinting in accordance with method of acquiring packet information. In active fingerprinting, responses from variety of packets sent to the target network are analyzed. Depending on operating system, network device responds with modified packet which allows active fingerprinting to identify the running operating system, version of the target network device through the response packets received from target host [1].

The probability of network devices to be detected is higher using Intrusion Detection System and Intrusion Prevention System as the network devices send and receive packets directly from these systems [1]. In passive fingerprinting, packets are sniffed from TCP port which is a stealthier approach compared to active fingerprinting as it is less likely to be stopped or detected by the firewall [1].

However, this approach is relatively difficult to obtain operating system information. Passive fingerprinting identifies operating system by analyses data in the packet header while sniffing SYN or SYN/ACK packets.

2.1. IP Scanner

IP scanner is used to test whether a particular host is reachable across a network or to discover live host in a network. It can also be used to self-test network interface card of a computer, or as a speed test. This is done by sending Internet Control Message Protocol (ICMP) “echo request” packets to a target host and listen for the ICMP “echo response” replies. Round trip time of this process will be measured, and records of any packet loss will be displayed in a statistical summary [2].



	Bit 0 – 7	Bit 8 -15	Bit 16 – 23	Bit 24 - 31
IP Header (160 bits OR 20 Bytes)	Version / IHL	Type of service	Length	
	Identification		Flags and offset	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Payload (64+ bits OR 8+ Bytes)	Type of message	Code	Checksum	
	Quench			
	Data (optional)			

Figure 1: Generic Composition of an ICMP Packet

2.2 NS Lookup

Ns lookup is a computer program used in Windows and UNIX where it sends a domain name query packet to Domain Name System (DNS) servers to find DNS details which includes IP addresses of a computer, MX records for a domain and the NS servers of a domain [2]. Depending on the system of the client, the default destination of the query packet maybe local DNS server at client’s service provider, intermediate name server, or root server system for entire domain name system hierarchy.

2.3 Port Scanning

A port scanner can be either benign, when network administrator wants to check network status or applications which require ports allocation to communicate, or malign, when malicious users trying to seek or identify exploits or vulnerabilities by retrieving services information. Information gathered from port scanning can vary between active port number, target operating system, and services version. Depending on the objective of port scanning, scanning can be performed based on two main perspectives, vertically or horizontally [3].

Vertical port scan is where a range of ports are probed on a single target machine. This type of scan is performed when there is a specific target and you want to find vulnerabilities of a system.

While horizontal scan is where a set of hosts are probed for the same port [3]. This scan is performed when attackers have known of a certain exploit or vulnerabilities and they wanted to identify vulnerable victims.

Horizontal scan is much harder to be detected as it will require a global view of the targeted network or by using multiple Intrusion Detection Systems (IDS). Vertical and horizontal scans can be combined to retrieve service information for an entire network mask, this scan is known as block port scan [3]. In order to evade detection of defence mechanism placed in the target, attackers have come up with a different approach in performing scans.

One of the ways is to perform scans in a slow manner by having a long-time interval between each port probe. If the time interval is long enough to exceed IDS scan threshold, port probes will be treated as legitimate traffic [3].

Another approach is to perform distributed port scan where attackers will spoof their IP address for each port probe. Although this approach is useful to bypass defence mechanism in place, it demands lot of computational resources from attacker, like a botnet. There are many different techniques for port scanning available and the six most common port scan techniques are:

- Transmission Control Protocol (TCP) Connect Scan
- SYN Scan
- ACK Scan
- FIN Scan
- NULL Scan
- XMAS Scan

2.3.1TCP Connect Scan

TCP connect is a three-way handshake between client and server, if the handshake take place then the communication between client and server is established.

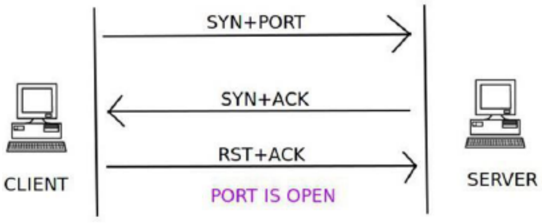


Figure 2: TCP Connect Scan with Open Port [4]

When a client tries to connect to a server on a certain port, it initializes the connection by sending a TCP packet with the SYN flag set and the port to which it wants to. If the specific port is open on the server and is accepting connections, server will respond with a TCP packet with the SYN and ACK flags set. Then the connection is established by the client sending an acknowledgement ACK and RST flag in the final handshake. If this three-way handshake is completed, then the port on the server is open.

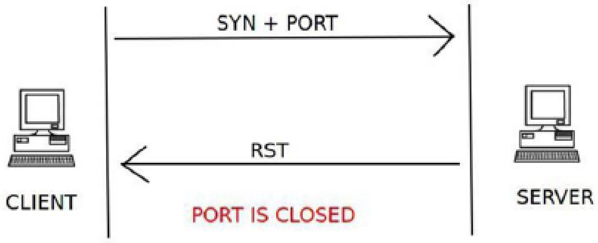


Figure 3: TCP Connect Scan with Closed Port [4]

If serverreply with an RST packet instead of a SYN-ACK packet during the second handshake, then that particular port is closed on the server.

2.3.2 SYN Scan

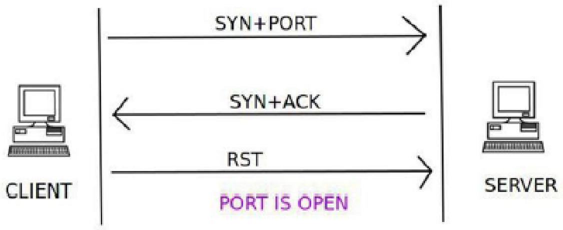


Figure 4: SYN Scan with Open Port [4]

This port scanning technique is similar to TCP connect scan where the client sends a TCP packet with the SYN flag set and the port number to connect to. If the port is open, the server responds with the SYN and ACK flags inside a TCP packet. Instead of sending an acknowledgement ACK and RST flag during the third handshake, client sends out an RST flag in a TCP packet. This technique is used to evade port scanning detection by firewalls without establishing connection during final handshake.

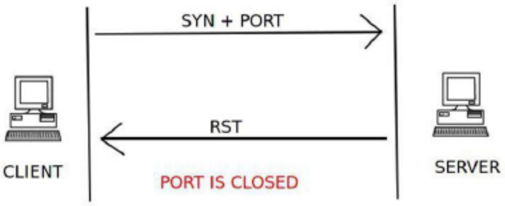


Figure 5: SYN Scan with Closed Port [4]

The closed port check is same as TCP connect scan where the server responds with an RST flag set inside a TCP packet during the second handshake.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

2.3.3 ACK Scan

TCP ACK scan is used to determine whether a stateful firewall is present on the target server or not instead of using this scan to identify open or closed state of a port. This type of scan only determines if the target port is filtered or not.

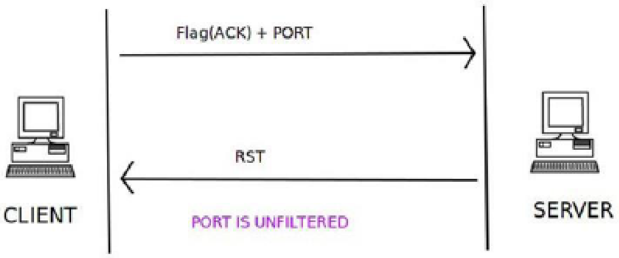


Figure 6: TCP ACK Scan with Unfiltered Port [4]

ACK flag in a TCP packet and port number is sent to the target server and if the server responds with the RSP flag inside a TCP packet then the port is unfiltered and stateful firewall is absent.

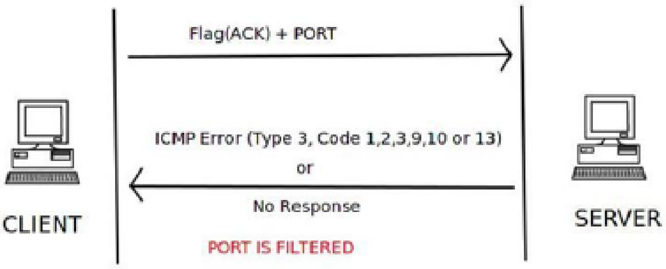


Figure 7: TCP ACK Scan with Filtered Port [4]

If the target server doesn’t respond to TCP ACK scan packet or the server responds with an ICMP packet containing ICMP type 3 or code 1,2,3,9,10, or 13 set, then the specific port is filtered which shows the present of stateful firewall.

2.3.4 FIN Scan

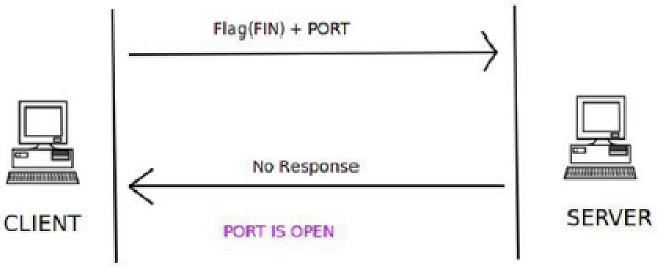


Figure 8: FIN Scan with Open Port [4]

FIN scan sends port number and TCP packet containing FIN flag to target host and if there is no response from the server, then the port is open.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

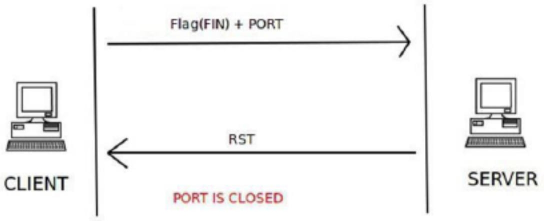


Figure 9: FIN Scan with Open Port [4]

If the target server responds with a TCP packet with RST flag for FIN scan request, then the port is closed on the server.

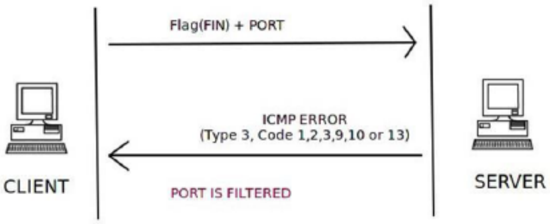


Figure 10: FIN Scan with Filtered Port [4]

If the target server responds with ICMP type 3 or code 1, 2, 3,9,10, or 13 set in reply to FIN scan request, then this shows that the port in target server is filtered and the port state can't be found.

2.3.5 NULL Scan

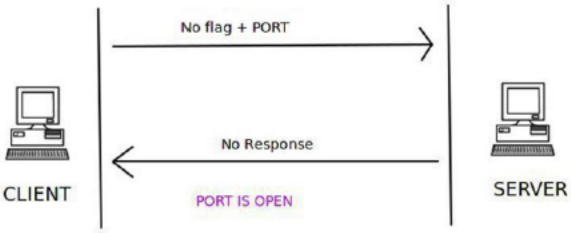


Figure 11: NULL Scan with Open Port [4]

NULL scan sends a TCP packet with no flag set and port number to the target server and if there is no response from the server, then that specific port is open.

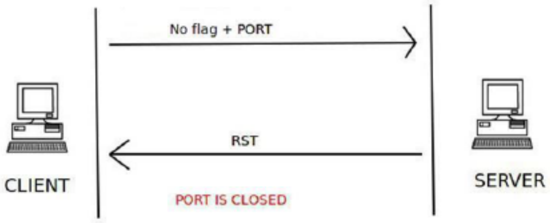


Figure 12: NULL Scan with Close Port [4]

If target server responds with TCP packet containing RST flag in response to NULL scan, then the specific port is closed.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

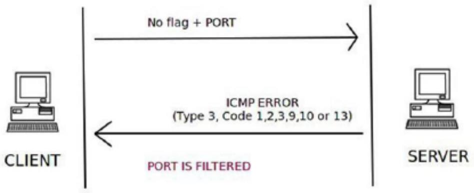


Figure 13: NULL Scan with Filtered Port [4]

If the target server responds with ICMP type 3 or code 1, 2, 3,9,10, or 13 set in reply to NULL scan request, then this shows that the port in target server is filtered.

2.3.6 XMAS Scan

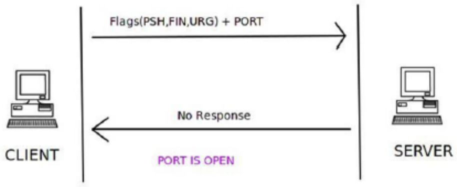


Figure 14: XMAS Scan with Open Port [4]

In a XMAS scan, a TCP packet containing PSH, FIN, and URG flags and port number are sent to the server and if the there is no response from the server, the specific port is open.

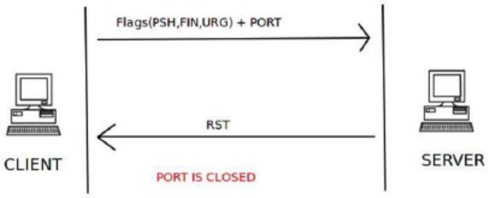


Figure 15: XMAS Scan with Closed Port [4]

If target server responds with TCP packet with RST flag, then the specific port is closed on the server.

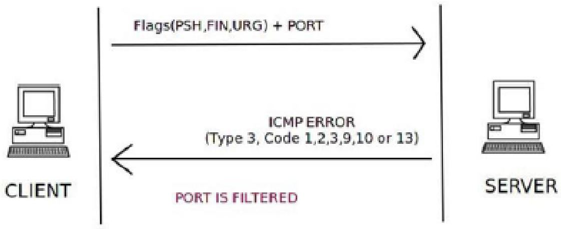
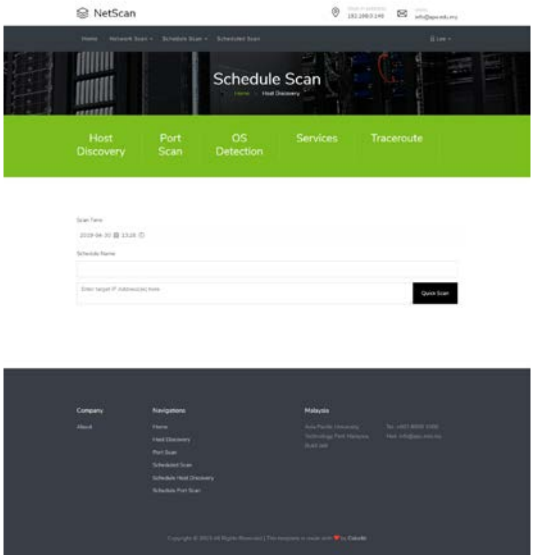


Figure 16: XMAS Scan with Filtered Port [4].

If the target server responds with ICMP type 3 or code 1, 2, 3,9,10, or 13 set in reply to XMAS scan request, then this shows that the port in target server is filtered and the port state can’t be determined.

III. DIFFERENCES BETWEEN EXISTING AND PROPOSED SYSTEM

There are some differences in the existing system which has resulted in the developer proposing a new web-based network scanning tool known as Net Scan. First and foremost, the proposed system is a web application which requires no installation, all the program data is stored in the web server, and the scanning is performed on the server side instead of user's computer. Besides that, Net Scan is easier to access compared to traditional network scanning tool, where any device with internet browser that is connected to the internet will be able to access it which includes computer, smartphones, tablets, and Android TV. Although there is an existing system known as Nmap Online Scanner [5] that is similar to the proposed system, users need to pay for every single IP address scanned. Nmap Online Scanner charges 0.30 credits for each IP address scanned and 0.05 credits for every 5 minutes over 30 minutes. For an unregistered user, 1.20 credits are given for free every day which is around 4 IP addresses scans daily and for extra credits users would have to pay minimum of 12 US dollar for 500 credits [5]. The proposed system also has additional feature to allow authenticated user schedule for network scanning. This feature is useful for users who want to scan their network at specific time for minimal traffic impact. Figure 14 shows the interface for scheduling host discovery where user is required to enter scanning time, schedule name, and IP address (es). The proposed system also allows users to manage their scan history. Figure 15 shows the interface for user's schedule where scan history and scheduled scans are listed.

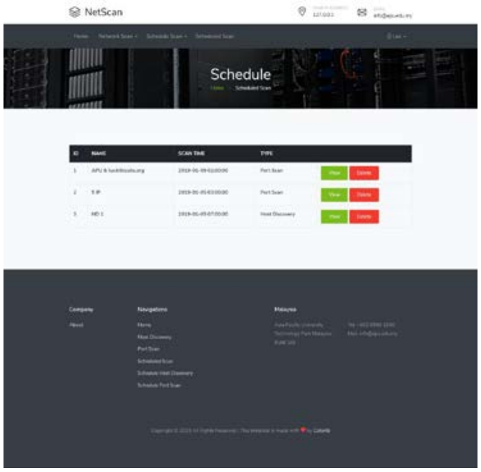


Scan Time: 2019-04-30 13:28

Schedule Name:

Enter target IP Address(es) here

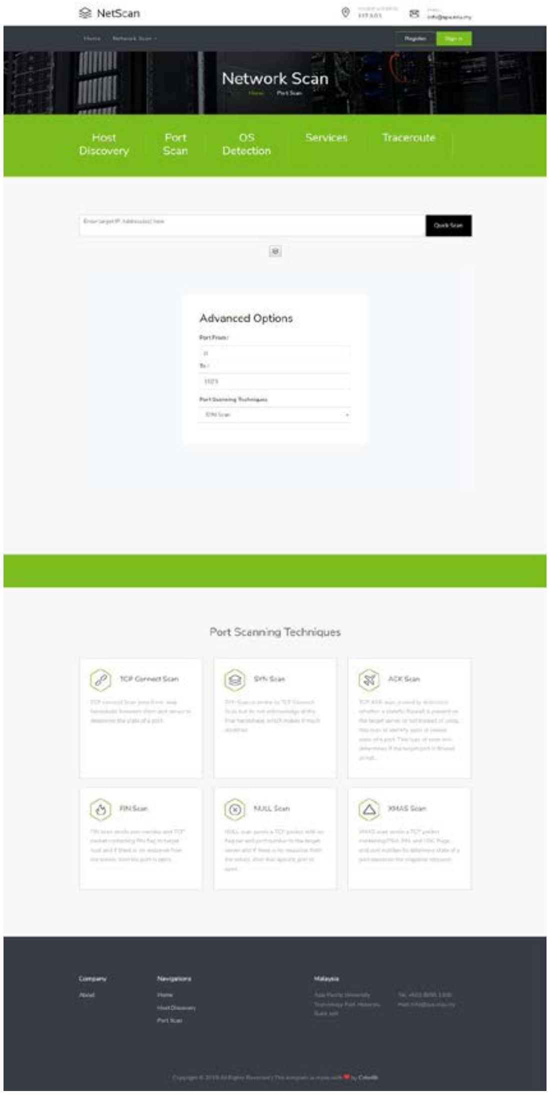
Figure 14: Net Scan Schedule Host Discovery Interface



ID	NAME	SCAN TIME	TYPE
1	APU & hackthissite.org	2019-01-09 02:00:00	Port Scan
2	5 IP	2019-01-05 03:00:00	Port Scan
3	HD 1	2019-01-05 07:00:00	Host Discovery

Figure 15: Net Scan User Schedule Interface

As for comparison with the powerful network scanning tool Nmap which support various advanced network scanning techniques [6], the proposed system is much more user-friendly. Output of the Nmap can be confusing or over complex when scan against a large network if the users do not know where to look at as the output can be hundreds of pages long depending on the size of network it was scanned against. Besides that, Nmap is a very complex tool with more than 30 options available and it may be too complex for user who have not use Nmap before. So, to really take advantage of this powerful tool, user would need to go through pages of man page and remember the correct sequence of commands. The proposed system has a more organized output and is easy to use. For quick scanning, users are required to enter target IP address(es) only where Net Scan will perform default port scanning with SYN Scan from port 0 to 1023, OS and services detection, and trace route. There are also options for users that would like to specify port range for scanning and 6 port scanning techniques to choose from. Figure 16 shows the interface for port scanning and Figure 17 shows the interface for scanning results where user can download the scan results in txt.



Advanced Options

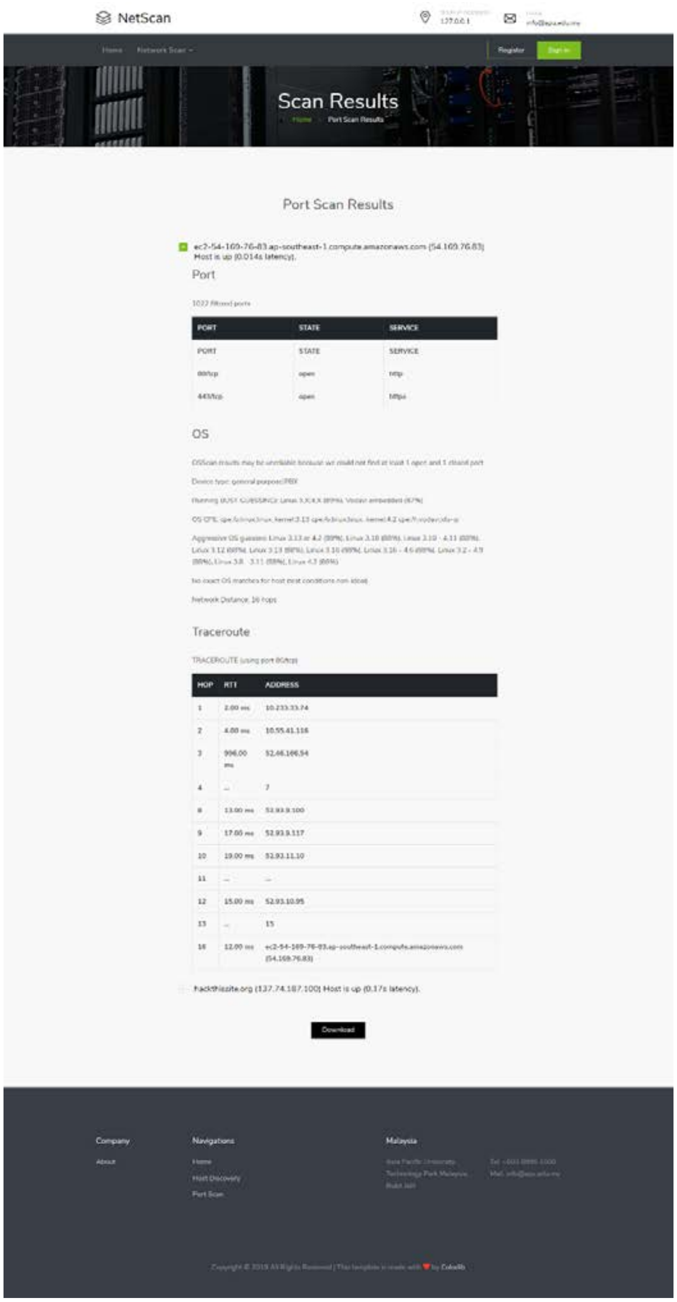
Port From : 0

To : 1023

Port Scanning Techniques: SYN Scan

Figure 16: Net Scan Port Scanning Interface

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019



Port Scan Results

☑ ec2-54-169-76-83.ap-southeast-1.compute.amazonaws.com (54.169.76.83) Host is up (0.014s latency).

Port

1022 filtered ports

PORT	STATE	SERVICE
PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

OS

OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose|PBX

Running (JUST GUESSING): Linux 3.X|4.X (89%), Vodavi embedded (87%)

OS CPE: cpe:/o:linux:linux_kernel:3.13 cpe:/o:linux:linux_kernel:4.2 cpe:/h:vodavi:xts-ip

Aggressive OS guesses: Linux 3.13 or 4.2 (89%), Linux 3.10 (88%), Linux 3.10 - 4.11 (88%), Linux 3.12 (88%), Linux 3.13 (88%), Linux 3.16 (88%), Linux 3.16 - 4.6 (88%), Linux 3.2 - 4.9 (88%), Linux 3.8 - 3.11 (88%), Linux 4.2 (88%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 16 hops

Traceroute

TRACEROUTE (using port 80/tcp)

HOP	RTT	ADDRESS
1	2.00 ms	10.233.33.74
2	4.00 ms	10.55.41.116
3	996.00 ms	52.46.166.54
4	...	7
8	13.00 ms	52.93.9.100
9	17.00 ms	52.93.9.117
10	19.00 ms	52.93.11.10
11	...	...
12	15.00 ms	52.93.10.95
13	...	15
16	12.00 ms	ec2-54-169-76-83.ap-southeast-1.compute.amazonaws.com (54.169.76.83)

□ hackthissite.org (137.74.187.100) Host is up (0.17s latency).

Figure 17: Net Scan Scan Results Interface

IV. Functionalities of the Proposed System

The aim of proposed system is to design and develop a web-based network scanning tool that is accessible and user-friendly. The objectives of proposed system include:

- To identify networked devices and test whether the target is reachable across network.
- To identify operating system version of target host.
- To identify open ports and network services running on target host.
- To identify path that a packet takes from a device to a specified destination.
- To maintain the profile and scan history of a user.

The network scanning tool can be accessed through a web browser and allow users: -

- To sign into the system.
- To logout from the system.
- To perform network scanning.
- To view and maintain network scan result.
- To delete scan history and result.

Additional features are as follows: -

- Notify user through email when scanning is done.
- Allow user to download scan results.
- Allow scheduling for rescan.

Figure 18 shows the interface for registration and Figure 19 shows the login interface of Net Scan.

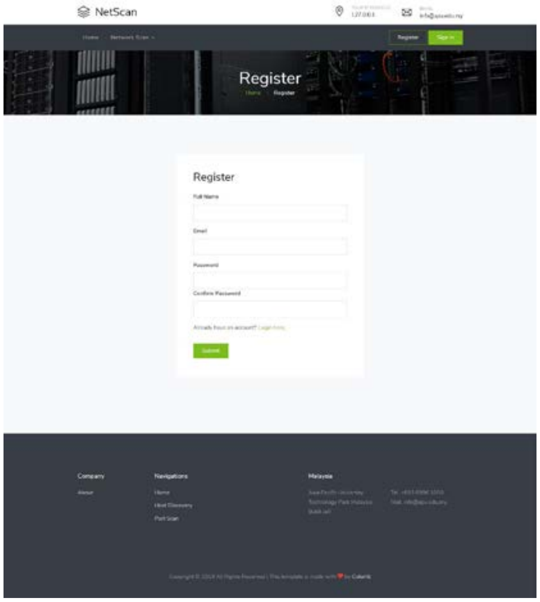


Figure 18: Net Scan Registration Interface

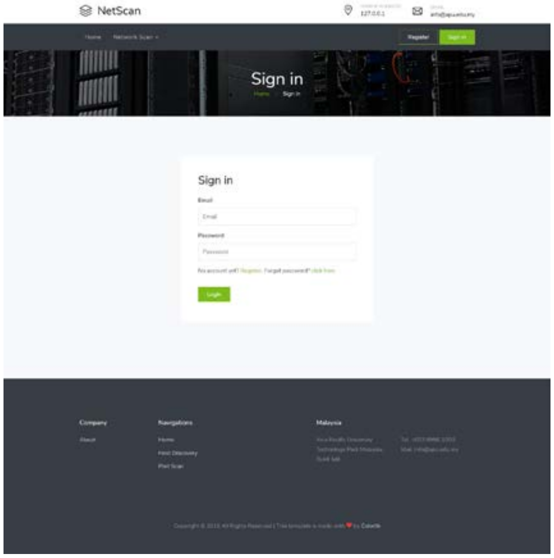
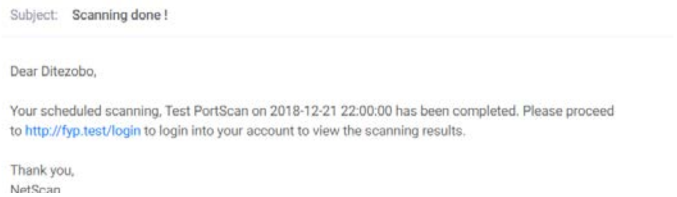


Figure 19: Net Scan Login Interface

When a scheduled scan is done, the proposed system will send an email to notify user that the scheduled scan is done. Figure 20 shows a sample email sent to user when scanning is done.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019



Subject: **Scanning done !**

Dear Ditezobo,

Your scheduled scanning, Test PortScan on 2018-12-21 22:00:00 has been completed. Please proceed to http://fyp.test/login to login into your account to view the scanning results.

Thank you,
NetScan

Figure 20: Sample Email Sent to Notify User

V. CONCLUSIONS

At the end of the project, all the aim and objectives were fulfilled successfully where users can perform host discover, port scanning, identify services running, operating system detection, and trace route and view the scan results in an organized manner. Additional features such as enable users to schedule scan at their desired time was also successfully implemented. The system was also tested, and the results shows that no bugs was found during the testing. An in-depth research was also done on network scanning tools and types of port scanning techniques. This is not perfect and have space for improvement, the first improvement can be done is to allow user to enter domain names or urls to be scanned instead of just entering IPv4 address(es). Lastly, another improvement is to provide more options for users to choose from when scanning is performed such as enable UDP scanning.

REFERENCES

[1] Sun-young Im, S.-H. S.-h. (2016). Performance Evaluation of Network Scanning Tools with Operation of Firewall. *IEEE*, 876-881.

[2] G.Murali, M. Y. K., 2011. Network Security Scanner. *IJCTA*, Volume 2, pp. 1800-1805.

[3] Igor Jochem Sanz, M. A. L. D. M. F. M. O. C. M. B. D., 2017. A Cooperation-Aware Virtual Network Function for Proactive Detection of Distributed Port Scanning. 2017 *1st Cyber Security in Networking Conference (CSNet)*, pp. 1-8.

[4] InfoSec Institute, 2013. *Port Scanning using Scapy*. [Online] Available at:https://resources.infosecinstitute.com/port-scanning-using-scapy/#gref.

[5] Online-Domain-Tools.com, 2018. Nmap Online Scanner. [Online] Available at: http://nmap.online-domain-tools.com/.

[6] NMAP.org, 2018. Nmap Security Scanner. [Online] Available at: https://nmap.org/.

[7] P. Mary Jeyanthi, Santosh Shrivastava Kumar “The Determinant Parameters of Knowledge Transfer among Academicians in Colleges of Chennai Region”, *Theoretical Economics Letters*, 2019, 9, 752-760, ISSN Online: 2162-2086.

[8] P. Mary Jeyanthi, “An Empirical Study of Fraudulent and Bankruptcy in Indian Banking Sectors”, *The Empirical Economics Letters,* Vol.18; No. 3, March 2019.

[9] Mary Jeyanthi, S and Karnan, M.: “Business Intelligence: Hybrid Metaheuristic techniques”, *International Journal of Business Intelligence Research,* - Volume 5, Issue 1, April-2014.

[10] P. Mary Jeyanthi, “INDUSTRY 4.O: The combination of the Internet of Things (IoT)and the Internet of People (IoP)”, *Journal of Contemporary Research in Management*, Vol.13; No. 4 Oct-Dec, 2018, ISSN: 0973-9785.

[11] P. Mary Jeyanthi, "The transformation of Social media information systems leads to Global business: An Empirical Survey", *International Journal of Technology and Science (IJTS),* issue 3, volume 5, ISSN Online: 2350-1111

[12] P. Mary Jeyanthi,” An Empirical Study of Fraud Control Techniques using Business Intelligence in Financial Institutions”, *Vivekananda Journal of Research* Vol. 7, Special Issue 1, May 2018, ISSN 2319-8702(Print), ISSN 2456-7574(Online).

[13] Mary Jeyanthi, S and Karnan, M.: “Business Intelligence: Artificial bear Optimization Approach”, *International Journal of Scientific & Engineering Research*, Volume 4, Issue 8, August-2013.

[14] 8. Mary Jeyanthi, S and Karnan, M.: “Business Intelligence: Optimization techniques for Decision Making”, *International Journal of Engineering Research and Technology*, Volume 2, Issue 8, August-2013.

[15] Mary Jeyanthi, S and Karnan, M.: "A New Implementation of Mathematical Models with metaheuristic Algorithms for Business Intelligence", *International Journal of Advanced Research in Computer and Communication Engineering*, Volume 3, Issue 3, March-2014.

[16] Dr. Mary Jeyanthi: "Partial Image Retrieval Systems in Luminance and Color Invariants: An Empirical Study", *International Journal of Web Technology* (ISSN: 2278-2389) – Volume-4, Issue-2.

[17] Dr. Mary Jeyanthi: "CipherText Policy attribute-based Encryption for Patients Health Information in Cloud Platform", *Journal of Information Science and Engineering* (ISSN: 1016-2364)

[18] Mary Jeyanthi, P, Adarsh Sharma, Purva Verma: "Sustainability of the business and employment generation in the field of UPVC widows" (ICSMS2019).

[19] Mary Jeyanthi, P: "An Empirical Survey of Sustainability in Social Media and Information Systems across emerging countries", *International Conference on Sustainability Management and Strategy"* (ICSMS2018).

[20] Mary Jeyanthi, P: "Agile Analytics in Business Decision Making: An Empirical Study", *International Conference on Business Management and Information Systems"* (ICBMIS2015).

[21] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence – soft computing Techniques", *International Conference on Mathematics in Engineering & Business Management (ICMEB 2012)*.

[22] Mary Jeyanthi, S and Karnan, M.: "A Comparative Study of Genetic algorithm and Artificial Bear Optimization algorithm in Business Intelligence", *International Conference on Mathematics in Engineering & Business Management (ICMEB 2012)*.

[23] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Data Mining and Optimization for Decision Making ", *2011 IEEE International Conference on Computational Intelligence and Computing Research* (2011 IEEE ICCIC).

[24] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Data Mining and Decision making to overcome the Financial Risk", 2011 *IEEE International Conference on Computational Intelligence and Computing Research* (2011 IEEE ICCIC).

[25] Dr. Mary Jeyanthi, S: "Pervasive Computing in Business Intelligence", *State level seminar on Computing and Communication Technologies.* (SCCT-2015)

[26] Dr.P.Mary Jeyanthi, "Artificial Bear Optimization (ABO) – A new approach of Metaheuristic algorithm for Business Intelligence", ISBN no: 978-93-87862-65-4, *Bonfring Publication.* Issue Date: 01-Apr-2019

[27] Dr.P.Mary Jeyanthi , "Customer Value Management (CVM) – Thinking Inside the box" – ISBN : 978-93-87862-94-4, *Bonfring Publication*, Issue Date: 16-Oct-2019

[28] Jeyanthi, P. M., & Shrivastava, S. K. (2019). The Determinant Parameters of Knowledge Transfer among Academicians in Colleges of Chennai Region. *Theoretical Economics Letters,* 9(4), 752-760.