Automatic Port Scanner

Moona Olakara Mohammed
Dept of Computer Science Engineer
Nehru College of Engineering & Research Centre
Palakkad, India

Abstract:- In a computer network, an attack is an attempt to destroy or steal unauthorized information or make use of information as an asset. One of the attacks is a reconnaissance attack considered as the first step of a computer attack. This type of attack is mostly done by a black hat, an expert in the programmer, by scanning the internal network devices and gather vulnerability information. In this paper, shows the identification of open ports and services through the network and available IP on the network are possible to attack.

Keywords:- *Open Ports, Nmap tool, Automatic Scanner, IP.*

I. INTRODUCTION

Rising technologies overall the world is increasing day by day. The Internet is a massive interconnection that connects the global wide area network throughout the world. The network connection is used for various activities such as emails, downloading files, etc., and also new techniques propages through different filed in different activities. As increase massive network definitely gives some loopholes or unfold sports activities in the back of the internet. These sport activities may start from the basic terminology named as Intrusion Detection System or port scanner, as scan the entire network to find out ports attempt to attack which is called hacking in usual words but it is one type reconnaissance attack said by researchers.

On the other hand, a large number of computer iliteracy people are getting unaware of the loopholes present withinin the Operating Systems, networking protocols, software applications that are used on day to day . Many of them are freely easy to use available activities on the web in which many cash in of those loopholes to realize unauthorized access to a system. To further complicate the item most folks don’t follow good security practices, making the work of computer criminals even easier. but it is one type reconnssaince attack.

As a result of the massive usage of computer networks everywhere the planet, network security has become one of the a world big challenge for today’s network engineers and system administrators is to develop various methods capable of detecting attempts to compromise the integrity and availability of the network. This area of research is named Intrusion Detection Systems (IDS). Port scanning is considered a dangerous network intrusion method for locating exploitable communication channel. There is a large number of 65,535 TCP and UDP ports. Ports are ranges from 0 to 1024 are well-known ports .ranges from 1024 to 49151are dynamic ports and ranges from 49151 to 65,535 are private ports . Some of the ports are not harmful while others form malicious cause in the network. Ports scanning uses a reconnaissance method to scan all internal network devices to determine open ports and services. Port scanning is an essential part of the network security technique as it reveals the possible security vulnerabilities in the target system. Thus computer security is the major threat to the technology world. Computer security, is the protection of computer systems and networks from the vulnerability, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

The main objective of this system is to build an automatic port scanning technique to scan the entire network ports of the targeted system giving the information about the target hosts, the listening ports, and the services running on the ports. There are many network scanning tools to develop and remedy vulnerabilities in the network. these networking tools are disclosed to public which can be used by intent hackers and attackers for a malicious cause. One of the tools is analyzed in my system is the Nmap tool. As a result of scanning the host, identify the open ports and services as well as the associated IP.

This next section shows the way to introduce this system by researching various material, section III introduce the idea of new system , section IV explains the overall and future of the system.

II. RELATED WORKS

Many researchers have proposed various techniques to detect open ports for reducing vulnerabilities in computer security. The researcher in [1] specifies to detect intrusions, including port scanning. More specifically, the authors propose various techniques that correspond to both the misuse detection and anomaly detection. In [2], the authors used a large amount of the different TCP control packets as input for Back Propagation algorithm so as to detect port scans. The learning phase was supported by a training set that contains normal traffic and port scanning attacks.

In [3] the authors outline the several approaches of scanning of target system windows XP sp0 with the usage of the Nmap tool. Authors used Nmap for finding the IP with localhost OS and also target remote host OS. The authors additionally used some alternatives of Nmap which changed into providing us extra data approximately open ports. The complete work is on nmap and the assaults will be achieved on the virtual device (VMware). Kali Linux is the interface of the use of the Nmap tool. Nmap is used in reconnaissance or information-collecting phases that is the primary phase of any penetration phase.

In [4] the researcher specified and aligned the web assessment with three standards of security like confidentiality, integrity, and availability (CIA). In [5] the creator depicts the procedure of infiltration testing of those applications. The objective of such testing is to differentiate application blemishes and vulnerabilities and to propose an answer to mitigate.

In [6], the creator proposed a detecting scanning attack supported the amount of ICMP error messages that are generated when the scanner tries to attach to an open port. Hence, no algorithm was used for identifying the IPs. Alternatively, variety of a flag was produced when the amount of ICMP error messages exceeds a predefined threshold. symbolic logic was utilized. In [7] for detecting distributed port scans. In such a situation of misuse detection, the authors propose a two-stage rule induction algorithm, called the PNrule. within the first phase, the algorithm learns the P-rules that cover most of the intrusive examples while within the second, it discovers N-rules used to eliminate false positives. Another technique called CREDOS was suggested; it uses the ripple down rules to overfit the training data at the start then prune them to enhance the generalization capability.

In [8] the researchers depict network security censoring devices to address issues in the Albaha University network. The technique pen-testing tools use Nessus and Metasploit tools to get the vulnerability of a site. In [9] the creator for the examination was to offer recognizable proof of vulnerabilities and attacks for the protection of surveillance camera frameworks. The examination demonstrates that the vulnerability of reconnaissance cameras had numerous vulnerabilities in which there is earnestness for circulating cautions and best practice rules.

In [10] the researcher's main objective is to demonstrate pen testing which will automatically and manually detect the vulnerability that is occurring on web site pages by using Nmap for both inactive and active ports. In [11] the researcher provides a comparison of the security of virtualization, inclusive of detection, and escaping the environment. They describe a method to demonstrate if a digital system could also be detected and compromised, based upon totally preceding studies. Finally, this technique is employed to assess the security of virtual machines.

Within the anomalous detection category, the researcher in [12] bring out various techniques called, the Local Outlier Factor (LOF), the Mahalanobis-distance Based Outlier Detection, and Nearest Neighbor (NN) Approach. The output of those machines may be a decision-making device that depends on features processing from a time window or a connection window to classify scanners from normal users [13].

In [14] the creator proposed an anomaly detection technique based upon the k-means clustering algorithm so as to differentiate an attack from normal traffic. A close approach suggested in [15] considers an outsized amount of knowledge rather than windowed data. It utilizes a electronic database management system (MySQL); to perform OLAP like operations (group by) using SQL statements. However, this approach scales poorly to the rise within the request rate at the server and can incur delays which may largely exceed network delays.

In [16] the author reasons to collect all of the required records to comfort the information earlier than real assault consequences of the system, at some point of the port scanning and various sports were completed ultimately where the report could be made to verify the development of the device to be a more secure purpose. In [17] the authors, being able to certify and verify the communication of the security level within a certain device is crucial for his or her acceptance. Towards this end, the creator proposes a security certification the methodology implemented for IoT to empower different stakeholders with the power to realize security solutions for large-scale IoT services in an automatic system.. It also supports transparency on the IoT security level system to the consumers because the methodology able to provides a label together with the main results of the certification procedures [18].

In [19], the author describes how to port scanning problem can be a text-book data mining problem. They define features, data labeling procedure, data transformation for the gathered traffic, and the choice of the classifier (named Rapper). In [20] researchers classify an anomaly score separately to a source IP based on the number of failed connection attempts it has made. It operates under some process that the port scanners will induce more failed connections. Therefore, this approach's performance depends greatly on the chosen thresholds and therefore the definition of the failed connection. The author in [21] uses likelihood-based detection to detect whether a connection is normal or represents a scan. However, since the access is prediction is failed towards normal traffic (99% of the time), therefore algorithm results in a high percentage of false positives. While another most anomaly detection system based on traffic analysis, SPICE [22], utilizes entropy like a function to check whether the accessed port is probable or not, with a lower probability inducing more information. The algorithm calculates the sum of the negative log-likelihood of destination IP/Port pairs until it reaches the desired threshold. On the other hand, one scan on a single port may result during a false positive. Finally, the present state-of-the-art for scan detection is Threshold Random Walk (TRW) proposed in [23]. It follows a specific function technique that the source's connection history performing sequential hypothesis testing. The hypothesis testing is sustained until enough evidence is gathered to declare the source either scanner or normal

In [24] the author's proposed overall framework integrates a government system into a sensible city in ensuring various security such as user privacy, information security, and mutual trust and confidence. Acitizen-centered, business-focused, and environment-aware government system will cause greater transparency and convenience, higher revenue and efficiency, and less corruption and operational overhead. In [25] authors proposed a realistic and sensible cyber warfare testbed using XenServer hypervisor, commodity servers, and open-source tools. Testbed supports cyber-attack and defense scenarios, malware containment, exercise logs, and analysis to develop tactics and methods.

In [26] the creator proposed SPS tool can become a crucial asset within the securing of computer systems, it's by no means an entire solution to computer security. It simply provides some diagnostic information to assist the user, SA, and security professional in identifying potential security risks on computer systems and therefore the capability to secure further their computing resources. The author in [27] reasons Scan rates dropped dramatically through Tor. Using Proxychains prevented Nmap from using multiple processes so it could not scan many ports a second.

In [28] the creator details Basically targeted protocols for fingerprinting are TCP, UDP, and ICMP. The parameters of offset of the packets being sent and revived are a vendor (OS) specific and therefore the similarity and difference between these parameters help the tools to spot our OS easily the essential need is to prevent unknown packets from an unknown source that are targeted to scan our system -that is to prevent the SCAN. While in[29] another researcher have describes Securing the network may be a major concern lately. Although the open-source is taken into account to be secure but still data transmitted over the network isn't safe. Some reconnaissance tools, scanning tools, packet sniffing tools, and firewall rules are presented during this paper to know the threats, attacks, and vulnerabilities of the network. Nessus [30], the open-source vulnerability scanner, produces comparable results with more information about the particulars of the vulnerabilities related to the ports that are open.

III. METHODOLOGY

Port scanning may be an introduction scanning. this comes under reconnaissance attack which considered the first computer attack. Port scanning aims at open ports during a system. These open ports are employed by attackers to hold out attacks and exploits. There are large numbers of tools to scan for open ports. However, only a few tools are present to detect open port. The goal of this project is to find out open port scanning attempts and find out information about the machine from where port scan attempts were made.

Port scanning involves sending a message to every port, one at a time. the type of response received indicates whether the port is in use and may, therefore, be probed for weakness. Portscanning has legitimate uses in managing networks as used by the crackers as well as are often malicious in nature if some hackers are trying to find a security breach within the computer system on the network. Some examples of port scanners or ports canning tools are Nmap, Foundstone Vision, and Portscan 2000. Among them, NMap claims the particular standard within the security industry thanks to its all-round capabilities in port scanning.

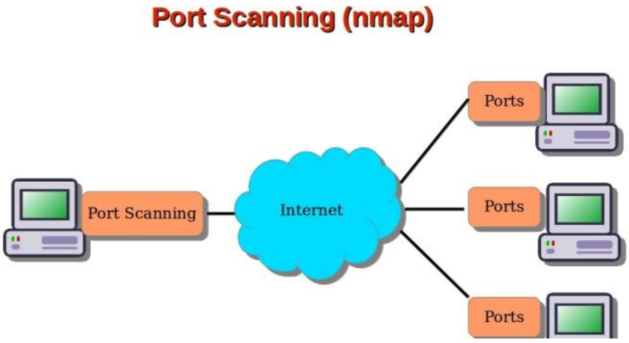

Fig 1:- Port Scanner Topology

Here in this paper, we've implemented a port scanning utility that may perform the various scans and provides standard results about the port states, services running, and IP hosts. The implementation of the utility is done in“Python” programming language and various functions of the python tool scapy are employed for the development of packets and other networking functionalities. We describe various port scanning methods and standard results in demonstrating the success of our research for scanning the ports. The aim of our research is to create a port scanning utility which will scan the ports of the target systems giving the knowledge about the target hosts, the listening ports, the filtered ports, and therefore the services running on the ports. We aim to realize the scanning of the ports by implementing the various port scanning techniques discussed within the standard tool for port scanning, Nmap.

Reconnaissance is taken into account the first pre-attack phase and maybe a systematic plan to locate, gather, identify, and record information about the target. The hacker seeks to find out the maximum amount of information as possible about the victim. This first step is taken into account a passive operation. This involves activities like operation, determining the network range, identifying active machines, finding open ports, and access points.

It performs scans in an aggressive manner by scanning one port after another for the specified range. They establish a full connection to the target machine and inspect whether the port is open. due to the complete connection establishment, it's possible to detect their presence. Thus when an outsized number of SYN packets arrive to request for a connection from one IP address at multiple ports of the target machine, it indicates that a brute force scanner is getting used to seem for open ports. Multiple packets are sent to scan multiple networking IPs and ports over the network. Figure 2 shows the process of attack in the network.

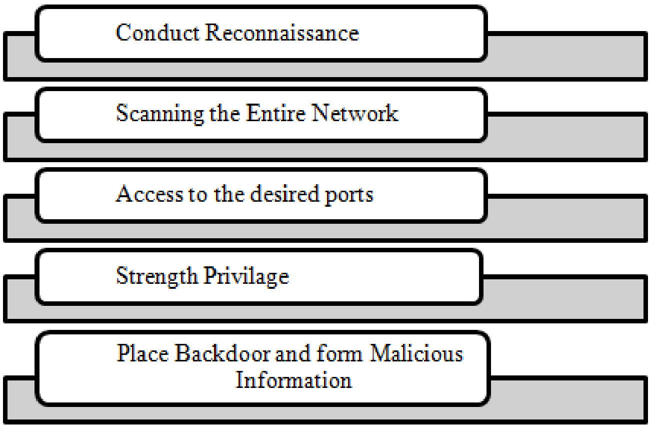
Conduct Reconnaissance
Scanning the Entire Network
Access to the desired ports
Strength Privilage
Place Backdoor and form Malicious Information

Fig 2:- Attack Process

The beginning of the attack starts from a packet that was directed to open ports that perform reconnaissance. After which the scanning of the whole network acknowledged the available open ports for purposes of attack. Mainly two sorts of open ports are UDP and TCP ports. If these ports are available, it's so on enter the specified ports to access the system and increase the strength of attack through attempt port. If the intruder anonymous access the network it paces backdoor by installing some malicious software or other malicious script injected to the system

A. *Experiment Analysis*

Services have assigned ports in order that a client can find the service easily on a foreign host. for instance , telnet servers listen at port 23, ssh on port 22, HTTP on port 80, and SMTP (Simple Mail Transport Protocol) servers listen at port 25. Client applications, sort of a telnet program or mail reader, use randomly assigned ports typically greater than 1023. Six Different Port States are recognized:

- Open: An application is accepting TCP connections, UDP datagrams, or SCTP associations on this port very actively. Finding these is typically the primary goal of port scanning. Security analysts know that each open port is a starter for the attack. Open ports are also interesting for nonsecurity scans because they show services available to be used on the network.
- Closed: A closed port is accessible, but there's no application listening thereon. they will be helpful in showing that a number is abreast of an IP address and as a part of OS detection
- Filtered: Filtering prevents its probes from accessing the port. The filtering could be from an obsessive firewall device, router rules, or host-based firewall software. Filters generally drop the packets without responding. These ports cause the scan to undertake, again and again, thus slows down the scanning.
- Open — Filtered: This state arrives when the scan is unable to work out whether the port is open or filtered. this happens for scan types during which open ports give no response.
- Closed — Filtered This state has arrived when the scan is unable to work out whether a port is closed or filtered.

The pair (IP address, port number) is named a socket and represents an endpoint of a TCP connection. to get TCP service, a connection must be explicitly established between a socket on the sending machine and a socket on the receiving machine. TCP connections are thus identified by its two endpoints, that is(socket1, socket2).

B. *Network ScanningTool*

The network scanning tools detect the devices that are active on the network and identifies information like an OS on the devices, the version of the detected devices. It performs a UDP and TCP SYNNmap is an open-source utility for network and security auditing.

- Nmap: Additionally, Nmap scans an outsized network at high speed. Nmap uses IP packets to work out what services those hosts are offering, which hosts are available on the network, what sort of operating systems (and OS versions) they're running, which sort of packet filters/firewalls are in use, and variety of other characteristics. Also, it can operate altogether major operating systems and is feasible to use both a graphical and console version. Nmap may be a network scanning tool that's most generally used.

C. *Ports*

Generally, an outsized number of machines are connected to a network and run services that use TCP or UDP ports for communication.

- UDP Scan: During the sort of scan, a variety of packets reach the destination and it doesn't scan complete the3-way TCP connection. UDP Internet Control Message Protocol (ICMP) port is an unreachable scanning port of a couple of UDP scans. UDP may be a connectionless protocol, so it’s difficult to scan the TCP because UDP ports aren’t required to reply to probes.
- SYN Scan: In this sort of scan, a variety of packets with only the SYN flag set reach the destination. It doesn't complete the 3-way TCP connection establishment handshake and terminates the connection after the victim replies with an SYN/ACK indicating an open port. This scan is often identified if there is an outsized number of packets with the SYN flag in them coming from one host. An attacker’s host request a connect() supervisor call instruction to each interesting port on the target machine. If the port is listening, connect() will be established; otherwise, the port and therefore the service is unavailable. This attack scheme is fast and doesn’t require any special privileges; however, the port scanner can easily detect and block this attack at the target system.

D. Work Specification

This system works under the control of the admin and therefore the network system. Firstly admin sends an invitation to determine the connection. After the approval of reference to the server, the admin executes the automated port scan using the Nmap tool by giving the target host IP address and scan the TCP SYN or UDP. If any open ports are found within the network.

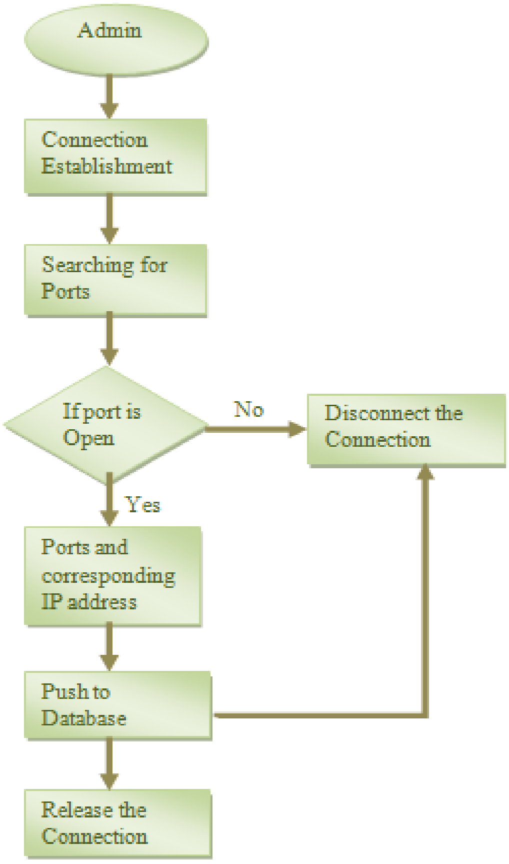

Fig 3:- Scan Detection

It pushed into the file along side services related to it, else disconnect the connection. These open ports and services are stored within the database. Along with the open ports, IP could also find using this system related to these open ports and services. for instance port 20, 21 are the ports used during a classic FTP connection between client and server. 22 is that the OpenSSH server port employed by default most Unix/Linux installations.23 is devoted to the Telnet application server that receives connections from any Telnet client. If any of the open ports found within the network it means there would be possible of attack coming from these ports. To find the IP related to this open ports, we scan the whole subnet to spot the available IP like open port 20 is found while scanning the network with Nmap tool and its services is FTP to spot which IP address associate ith open orts scan the whole subnet and therefore the result IP address would be 192.168.14.10

This technique basically about the thanks to scan the local database of services of any remote system connected to the Server with the help of IP/TCP Address of the system connected thereto server. The scanner involves a module for testing connections (the Connect page) and the handling of the local database of services (the Services page). After a hacker runs a port scanner on your system they know what services you've accepting connections. With this information, they're going to begin attempting to require advantage of these services to urge unauthorized access to your system.

IV. ADVANTAGES

A port scanner may be a software application designed to probe a network host for open ports. this is often often employed by administrators to verify the safety policies of their networks and by hackers to spot running services on a number with the view to compromising it. The knowledge gathered by a port scan has many legitimate uses including network inventory and therefore the verification of the safety of a network. Port scanning can, however, even be wont to compromise security. Many exploits depend on port scans to find open ports and send specific data patterns in an effort to trigger a condition referred to as a buffer overflow. Nmap is that the best port scanner; it can do various other things too but are the most focus here to scan port.

- ➢ Any system within the LAN are often scanned by the authorized users
- ➢ It is compatible with many of the OS
- ➢ It is especially provide security.
- ➢ Extremely active in TCP/UDP port scanning tools.Service/OS detection capabilities
- ➢ Various output formats that have been parsed and processed of results defined in various programs.
- ➢ Copious documentation on usage techniques and scripts
- ➢ Perform fast DNS lookup and scan a variety of IPs

V. CONCLUSION

The technological benefits of the port scanner is to watch and enhance the performance of the system and supply security to the system. employing a port scanner we will scan multiple ports simultaneously by using the concept called multithreading, and also determine malicious IP addresses which may be an effort to attack by this point are going to be saved. Mainly port scanners are utilized in firewalls also because the main server to detect the connected device that has been opened to find the open ports in order that the firewall and server can protect our system from threats that attack through these open ports. we will scan our own system with none help from an internet server and that we don’t require any additional software to use.

This system is predicated on automated port scanning during which an individual doesn't skill to scan the ports, he could know the essentials of the database then easily acknowledged the open ports, services, and related to IP address. this might help to require action before an attack attempt. In future administration is going to be given rights to shut the open ports of the clients. Time limit is going to be given for every and each open port, if the port isn't closed the specified time it'll be closed automatically. It can be extended to online port scanner

For future work, we decide to design our method on larger traffic data within a time limit and determine the probability of network vulnerability for our method. We also decide to propose solutions for the distributed port scanning which is barrier to the entire ports that an unknown access to the system form a technique after port scanning that's employed by attackers to cover the scanning activity

ACKNOWLEDGMENT

This research is supported greatly from the guidance of Nehru College of Engineering and Research Centre. I am also grateful to countless others who provided assistance and advice throughout the project. But chiefly I am indebted to the participants in this study, who were extremely generous with their time and knowledge, and who made this research possible.

REFERENCES

[1]. P. Dokas, L. Ertoz, V. Kumar, A. Lazarevic, J. Srivastava and P. Tan, “Data mining for network intrusion detection”, In Proc. 2002 NSF Wrokshop on Data Mining, p. 21-30.

[2]. B. Soniya and M. Wiscy, "Detection of TCP SYN Scanning Using Packet Counts and Neural Network," Signal Image Technology and Internet Based Systems, 2008. SITIS '08. IEEE International Conference, pp.646-649, Nov. 30 2008-Dec. 3 2008 doi: 10.1109/SITIS.2008.33

[3]. Kaur, Gurline, and Navjot Kaur. "Penetration Testing--Reconnaissance with NMAP Tool." International Journal of Advanced Research in Computer Science 8, no. 3 (2017).

[4]. [2] Iyamuremye, Blake, and Hisato Shima. "Network security testing tools for SMEs (small and medium enterprises)." In 2018 IEEE International Conference on Applied System Invention (ICASI), pp. 414-417. IEEE, 2018

[5]. Gupta, Bhushan B. "Requirements Based Web Application Security Testing–A Preemptive Approach!." (2017).

[6]. H.U. Baig and F. Kamran, "Detection of Port and Network Scan Using Time Independent Feature Set," Intelligence and Security Informatics, 2007 IEEE , pp.180-184, 23-24 May 2007 doi: 10.1109/ISI.2007.379554

[7]. J. Kim and J. Lee , "A slow port scan attack detection mechanism based on fuzzy logic and a stepwise policy," Intelligent Environments, 2008 IET 4th International Conference, pp.1-5, 21-22 July 2008

[8]. Holík, Filip, and Sona Neradova. "Vulnerabilities of modern web applications." In 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1256-1261. IEEE, 2017.

[9]. Alzahrani, M. E. "Auditing Albaha University Network Security using inhouse Developed Penetration Tool." In Journal of Physics: Conference Series, vol. 978, no. 1, p. 012093. IOP Publishing, 2018.

[10]. Cusack, Brian, and Zhuang Tian. "Evaluating IP surveillance camera vulnerabilities." (2017).

[11]. Ibrahim, Adamu Bin, and Shri Kant. "Penetration Testing Using SQL Injection to Recognize the Vulnerable Point on Web Pages." International Journal of Applied Engineering Research 13, no. 8 (2018): 5935-5942.

[12]. P. Dokas, L. Ertoz, V. Kumar, A. Lazarevic, J. Srivastava and P. Tan, “Data mining for network intrusion detection”, In Proc. 2002 NSF Wrokshop on Data Mining, p. 21-30.

[13]. [10] L. Ertoz, E. Eilertson, A. Lazarevic, P. N. Tan, P. Dokas, V. Kumar and J. Srivastava, "Detection of novel network attacks using data mining," In Proc. of Workshop on Data Mining for Computer Security, 2003.

[14]. H. Yang, F. Xie and Y. Lu; , "Research on Network anomaly Detection Based on Clustering and Classifier," Computational Intelligence and Security, 2006 International Conference , pp.592- 597, Nov. 2006 doi: 10.1109/ICCIAS.2006.294204

[15]. S. Jahr, "Slow portscanning detection," Internet: http://www.ztian.org/docs/slow_portscanning_detection.pdf, Nov. 2005 [Mar. 22, 2010].

[16]. Donaldson, Scott, Natalie Coull, and David McLuskie. "A methodology for testing virtualisation security." In Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2017 International Conference On, pp. 1-8. IEEE, 2017.

[17]. Hussain, Muhammad Zunnurain, Muhammad Zulkifl Hasan, and Muhammad Taimoor Aamer Chughtai. "Penetration testing in system administration." International Journal of Scientific & Technology Research 6, no. 6 (2017): 275-278.

[18]. Matheu-García, Sara N., José L. Hernández-Ramos, Antonio F. Skarmeta, and Gianmarco Baldini. "Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices." Computer Standards & Interfaces 62 (2019): 64-83.

[19]. G. J. Simon, H. Xiong, E. Eilertson and V. Kumar, "Scan detection: A data mining approach," In Proceedings of the Sixth SIAM International Conference on Data Mining, 2006, pp. 118–129.

[20]. P. A. Porras and A. Valdes, "Live traffic analysis of TCP/IP gateways," in NDSS, 1998,

[21]. C. Leckie and R. Kotagiri, "A probabilistic approach to detecting network scans," In Proceedings of the Eighth IEEE Network Operations and Management Symposium (NOMS 2002), 2002, pp. 359-372.

[22]. S. Staniford, J. A. Hoagland and J. M. McAlerney, "Practical automated detection of stealthy portscans," Journal of Computer Security, vol. 10, pp. 105-136, 2002.

[23]. J. Jung, V. Paxson, A. Berger and H. Balakrishnan, "Fast portscan detection using sequential hypothesis testing," In Proceedings of 2004 IEEE Symposium on Security and Privacy, 2004, pp. 211-225

[24]. Yang, Longzhi, Noe Elisa, and Neil Eliot. "Privacy and security aspects of E-government in smart cities." In Smart Cities Cybersecurity and Privacy, pp. 89-102. Elsevier, 2019.

[25]. Chandra, Yogesh, and Pallaw Kumar Mishra. "Design of Cyber Warfare Testbed." In Software Engineering, pp. 249-256. Springer, Singapore, 2019.

[26]. Kocher, Joshua E., and David P. Gilliam. "Self port scanning tool: providing a more secure computing environment through the use of proactive port scanning." 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05). IEEE, 2005.

[27]. Rohrmann, R., Patton, M. W., & Chen, H. (2016, September). Anonymous port scanning: Performing network reconnaissance through Tor. In 2016 IEEE Conference on Intelligence and Security Informatics (ISI) (pp. 217-217). IEEE.

[28]. Kalia, S., & Singh, M. (2005, November). Masking approach to secure systems from operating system fingerprinting. In TENCON 2005-2005 IEEE Region 10 Conference (pp. 1-6). IEEE.

[29]. Mandal, N., & Jadhav, S. (2016, March). A survey on network security tools for open source. In 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC) (pp. 1-6). IEEE.

[30]. Nessus,http://www.nessus.org/index.php