A Technical investigation into port scanning using Nmap

Abdul Rahman Khan
Applied Cybersecurity
University of Sunderland
New Castle, UK

***Abstract*— The most widely used attack method for collecting information about networked devices is port scanning. This paper provides a comprehensive investigation of TCP connect scan(-sT) using Nmap, focusing on a single target machine (www.honeypot.com-192.168.100.10). The weakness of the TCP protocol layer which operates at layer 4 of the ISO model is revealed by the scan. The investigation explores the characteristics of the attack software, Nmap, and how it affects the scanning operation. Techniques for countermeasures, from configuring TCP settings to deploying hardware, are presented. To contribute to the continuous evolution of cybersecurity defenses, this investigation reports the overall effects of the scan, assesses the efficiency of the countermeasures that were used, and proposes suggestions for further investigation.**

***Keywords*—Port scanning, connect scan, Nmap, countermeasures, Cybersecurity, ISO model.**

I. INTRODUCTION

In the modern contemporary world, Network security is a significant and continuous concern. As technology evolves, so do the techniques used by ethical security experts and malicious hackers. For enterprises, the network infrastructure is vital because it provides a basis for storing data, communication, and business operations. Enterprises may suffer substantial damages because of network breaches in terms of assets such as money, and legal obligations [1]. However modern cyberthreats are frequently sophisticated, with attackers using intricate techniques to get around outdated security measures. With the rise of methods of attack, like zero-day exploits, ransomware, and social engineering it's imperative for organizations to uninterruptedly develop their security methods to effectively detect and eliminate these threats. Failing to take measures may result in financial implications and problems [1]. Identifying the vulnerabilities and unauthorized access to the system is crucial for maintaining the reliability of data and securing important systems in organizations. Port scanning, a fundamental aspect of cyber security, is a crucial technique for evaluating the strength and vulnerabilities of the system. This paper aims to carry out the technical analysis of port scanning using the Nmap tool, with a specific focus on server 192.168.100.10 (www.honeypot.com) by using the TCP connect scan(st) technique. Malicious Hackers use port scanning as one of their most popular attacks or first scan to obtain information from the network. As the attack is so common and is carried out via a command line, even an inexperienced hacker can get the data. The process of port scanning involves examining a system's IP address to identify ports that are accessible and active services [2]. The most common ports used for port scanning are TCP, UDP and ICMP [3]. Port scanning may be divided into two types based on how it is carried out. In the first case, you can scan a single-source port, which is a one-to-many scan where scanning is done on a single host The second kind of scan consists of distributed port scanning which may be carried out with a many-to-many or many-to-one model that uses many different hosts to carry out the scanning[4].

- AIM

This paper aims to perform a technical investigation of portscanning, focusing on the TCP connect scan technique using the Nmap tool. The objective of this research is to analyse the intricate details of this scanning technique, and the targeted entity is www.honeypot.com which is hosted at IP address 192.168.100.10. This study includes the working of Nmap and how it impacts network protocol. Within this research, the TCP connect scan technique is carefully examined. The most important aspect of this research includes investigating the network analysis using wireshark during the scanning process. This will explore how Wireshark captures the data and interprets the interaction between Nmap and Honeypot

II. PROTOCOL STANDARDS

Port scanning is a straightforward scan and [5] a simple method to check for services and open ports on a network is to port scan. OSI Model is followed by all systems connected to a network. There are seven layers in the OSI model of communication. In general Transport layer using ports deals with UDP and TCP connection. On the transport layer, there are many protocols

accessible. However, not all systems make use of such protocols. For limited communication sessions, ephemeral ports are utilised. Therefore port scanning is an attack that takes place at the Transport layer(4^{th} layer)[6].

A. Port States

A computer's port is the point where data is sent from one Programme to another, from the internet to other devices, or between computers[6]. It's a virtual location where network communication begins and ends. Ports are divided into 6 states, the states are as follows: Unfiltered, Filtered, Open, Closed, Open | Filtered, Closed | Unfiltered

Open: ports are accessible for the communication

Closed: This port indicates that, even for the authorised user it won't scan, indicating that the port is closed

Filtered: The network mapper may access the port, but because the probes prohibit access to the port, it cannot be established whether the port is open.

Unfiltered: Although it is accessible nmap cant detect if it is open or closed

Open | Filtered: In this, the port doesn't give any response due to which Nmap cannot identify whether the port is open or filtered

Closed | Unfiltered: whether a port is open or closed cannot be determined. It is used for IP ID idle scan

B. Port Scanning Techniques

Port scanning uses some procedures to detect the open and closed ports of the network, some of the techniques are:

1. PING SCAN: These are the most fundamental port scanning techniques, These scans are identified as ICMP(internet control message) requests. To find out if the target is present, ping scan checks for any ICMP request. If hundreds or thousands of ports are to be scanned on a machine or even on the whole subnet, it needs to check whether the target machines are accessible or not. This is the goal of ping scanners.

There are two primary methods for ping scanning:

- Making use of "real pings0", which involves ICMP echo queries being sent to potential IP addresses and reporting as up any host that responds.
- Making use of "TCP pings", which involve sending unique TCP segments to probe ports that are frequently open and unfiltered (such as port 80).

2. SYN-SCAN: Here port scanner creates IP packets and tracks responses to them. The approach is also known as "scanning using half-open connections" because a complete TCP connection is never formed here[7] Here SYN packets are produced by port scanners. A SYN-ACK packet will be sent back by the host that is being targeted if the port is open. The connection closes before the connection procedure is completed by the host scanner when it sends the RST packet

3. XMAS-SCAN: In this scanning, by transferring packets to the target device with improper flag settings, Xmas scan figures out whether ports are open[8]. Its ability to get past some firewalls and intrusion detection systems more readily than SYN scan makes it regarded as a stealth scan. firstly Nmap Xmas scan generates packets with the finish (FIN), Push (PSH), and urgent(URG) flag set. There is no set protocol for processing these kinds of packets because this flag combination is incorrect and shouldn't ever occur in regular traffic. TCP stacks will react differently to one other, In general, open ports will reject the packet and not react, whereas closed ports will respond in RST/ACK. On the other hand, some systems won't react to any packets, and certain TCP stacks will react with RST packets from any ports, including open ports. Responses to this scan will also be modified by personal firewall and packet filter.

4. *FIN-SCAN:* Certain servers can track a SYN scan of their ports. For instance, sending "fake" SYN packets to a server that is secured by closed ports or polling many ports could reveal an effort at SYN scanning and cause the server to disconnect to stop scanning. Using the FIN packet for scanning, a hacker can get beyond these security measures. When a packet with FIN arrives on a closed port, the server is supposed to reply with RST. The server should reject FIN messages sent on open ports. This distinction allows one to separate the closed port from the open port[7]. To terminate the connection that has been formed, this scan sets out a FIN Flag. The Nmap can find the firewall details and activity level on that particular port with the use of the answer[6].

5. *NULL-SCAN*: The Null scan gets its name from the fact that it sends packets to the target device with an invalid flag setting i.e. packets with all flags turned off to figure out which ports are open[8]. A null scan is also regarded as stealthy, due to its capacity to bypass firewalls and intrusion detection systems, Despite this, similar to the SYN scan, management is now more aware of this scan due to the widespread presence of scan-specific fingerprints on network-based appliances and host intrusion prevention and detection software. Open ports will reject the packets and not respond but closed ports will respond with RST/ACK. On the other hand, some systems respond to any packet with an RST packet from any port, including open ports, while some systems will not reply at all. Responses to this scan will also be modified by personal firewall and packet filter

6. TCP CONNECT-SCAN: TCP connect scan is the default type of TCP scan when the SYN scan is not accessible [9]. This situation results when a user does not have raw packet privileges. Nmap utilizes the connect system call to ask the operating system that is running to launch a connection with the target machine and port, instead of sending raw packets like many other scan types do. P2P clients, Web browsers, and most other network-enabled apps all connect via this same high-level system function. It is an aspect of the Berkeley Sockets API, a programming interface. Nmap utilises this API to get connection attempt status information instead of reading raw packet answers off the wire.

This investigation thoroughly explores the TCP connect scan, which has a significant effect on TCP and the Transmission Control Protocol (TCP) in the context of the Internet Protocol

Suite. It is pivotal to investigate the protocol standards and place TCP into the layers of the OSI (Open Systems Interconnection) model to truly comprehend the effects of the TCP connect scan.

ISO/OSI model :
OSI (Open System Interconnection) is the Open Systems Interconnection Reference Model. The OSI model, which defines the ISO International Standards Organization, illustrates seven layers of function[10]. It is an excellent starting point for those new to network technology, nevertheless, it also provides evaluation and analysis based on a range of network technologies, which makes the network less mysterious and more reasonable to follow. To provide an organized and modular approach to networking, each layer in the OSI model contains certain tasks as shown in Figure 1.

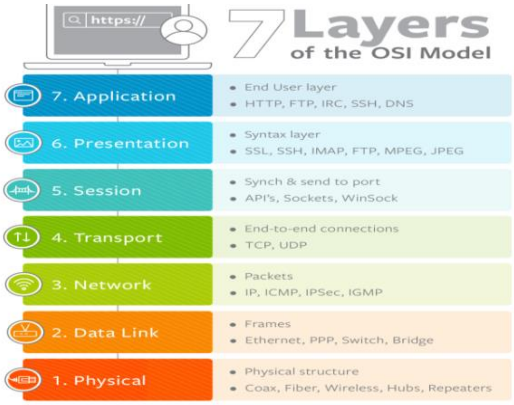

Figure 1. different layers in OSI model[12]

1. *Physical Layer:* This layer sends and receives data between the device and physical media. Hence, this layer is also stated to as the hardware layer at times. Bits are the protocol data unit for this layer. They describe the number of features, including modulation types, voltage levels, data rates and physical connectors.
2. *Data Link Layer*: Noise or interference can change the information at the physical layer, which makes the physical layer's information transmission inaccurate. By virtually removing errors in the connection between adjacent nodes, the data link layer will enhance the service that the physical layer provides[11]. In general, retransmission techniques combined with error-detecting codes or error-correcting codes are used to achieve this. In addition, buffer overflows may be avoided with the use of flow control. Framing will also be provided by the data link layer because the physical layer only manages bit transfers.
3. *Network Layer:* This is the third layer of the OSI model which is accountable for organizing and transmitting data between networks[12]. It focuses on logical addressing for data packets and routing of devices on different network
4. *Transport Layer*: It's the 4 and most important layer of the OSI model, it is also affected by the port scanning technique. The transport layer manages end-to-end protocol which increases bandwidth and data-rate speed[13]. The task of the transport layer involves segmentation of the data stream and congestion relief. TCP and UDP (User Datagram Protocol) operate at this.
5. *Session Layer:* These are some of the tasks performed by the session layer: creating connections and ensuring that they continue to function normally throughout a session[14]. The Session layer allows the establishment, termination and maintenance of sessions between applications.
6. *Presentation Layer*: The main tasks of this layer include providing or defining the encryption and data format. Conferring to the Open System Interconnection (OSI) model, the Presentation Layer is the 6th layer[15]. Since it acts as a data translator for the network, this layer is commonly referred to as the translation layer. This layer collects and modifies the data it obtains from the Application Layer to prepare it for network transmission. It is also called a syntax layer because it maintains the correct syntax for data it receives or sends to other networks. Corresponding to the relevant network protocol and architecture, the presentation layer in the OSI model serves as a translator, converting the data supplied by the transmitting node's application layer into a setup that is suitable and well-matched. When data reaches its destination computer, the presentation layer transforms it into a format that the application layer can use. In other words, when transmitted data has any problems to be read in a format that differs from the original format presentation layer essentially handles.
7. *Application Layer:* Application layer software's main task is to offer an interface through which programs may access network services[14]. The word "application layer" implies a set of functions that include file transfer, file management, email information processing, and more. It does not imply working on a specific application's network. Some of the application layer protocols include HTTP, FTP, IRC, SSH, DNS

C. TCP CONNECT(-sT) Scan and its effect on Network protocol

This research paper explores deeply the subject of TCP connect scan(-sT), which has a substantial impact on the Transmission Control Protocol (TCP) layer of the OSI model. The fourth layer of the OSI model includes TCP and UDP
TCP connection: TCP is a connection-oriented protocol[6] which stays active until the data is fully transmitted. The TCP handles the loss of data and reorders data to be delivered if there is a loss. The server receives the TCP data and responds with an ACK indicating that everything is well. This way it completes the three-way handshake
UDP connection: UDP is a connectionless protocol. To figure out whether the data reached its intended location, this protocol does not accept an ACK flag. There is no order in the packets that contain the data. No information is provided if the data is lost As a result, UDP is less reliable compared to UDP

TCP CONNECT SCAN(-sT): This is the basic scanning technique. The SYN scan and the TCP connect scan are similar, but the TCP connect scan completes a three-way handshake[16]. If the SYN scan is not supported by the system then the TCP connect scan will act as a default scan. Nmap will first send the SYN packet to the target host during this scanning. The port is

closed if the acknowledgement (ACK) and reset (RST) flags are set in the response packet. If it received SYN/ACK that indicates the port is open for communication. Nmap will then reply with ACK to complete the three-way handshake followed by RST/ACK to immediately close the communication

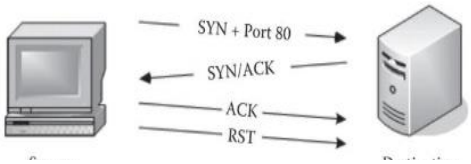

Figure 2. working principle of TCP CONNECT scan[16]

Figure.2. illustrates that it's working principle:

- Firstly, the source machine sends a SYN packet at port 80
- The destination machine then answers with a SYN/ACK packet
- The source machine again sends an ACK packet in response to the SYN/ACK packet to complete the three-way handshake
- Finally, the source machine sends the RST packet to close the connection[16].

The most significant thing here is the TCP connect scan analyses the way the TCP protocol behaves to figure out if a certain port on the target system is open or closed. It evaluates the openness and accessibility of network services by utilizing the well-established TCP connection approaches. These Techniques can also be used by attackers or ethical hackers to figure out the open ports of the network. To ensure security and unauthorized access the network security administrator must take some countermeasures. To scrutinize, the TCP connect scan greatly impacts the way the TCP protocol works. It is possible to figure out if a target machine's ports are accessible by starting a connection handshake and analyzing the response. To enhance network security and put up efficient countermeasures, it is crucial to comprehend how port scanning techniques interact with network protocols.

In conclusion, TCP connect scan(-sT) works on the Transport Layer(4 Layer) of OSI model. The transport layer manages end-to-end communication, error correction and congestion control. The TCP connect scan checks the accessibility of particular network ports on a target machine (192.168.100.10) by using features of the TCP protocol, which is an important transport layer protocol.

III. ATTACK SOFTWARE AND ITS EFFECT ON PROTOCOL

Ensuring network security is becoming more and more crucial in today's linked digital world, which has led to a closer investigation into defence-related technologies and possible risks. This section emphasizes the significance of Nmap in network security and it also demonstrates the parameters TCP connect scan uses and its effect on the scanning process. The objective is to analyze the mechanisms, configurations, and outcomes that create the impact of Nmap's TCP connect scan by looking at the attack software and how it affects the network protocol.

A. Nmap

The Nmap (network mapper) is an open-source tool for finding networks and executing security audits [17]. It is also efficient for many systems and network administrators for operations like organising service upgrades, maintaining track of host or service uptime, and assessing the network. Nmap implements innovative techniques employing raw IP packets to identify hosts on a network, the services (application name and version) they provide, the operating system (OS version) they run, the type of firewalls or packet filters they have in place, and a plethora of other details. Although it is designed to quick scan large networks it works well with a single host. More advanced functionality for vulnerability and service identification may be achieved by using Nmap scripts[18]. The four primary functions of Nmap are port scanning, host discovery, services detection, and TCP/IP stack fingerprinting. The below figure shows the scanning of www.honeypot.com (192.168.100.10

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.100.10
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-22 10:35 EST
Nmap scan report for 192.168.100.10
Host is up (0.0031s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
443/tcp open  https
```

Figure 3. Scanning of server www.honeypot.com (192.168.100.10)

VMware :

VMware virtualization permits multiple virtual machines to operate on a single physical computer, with each of them sharing the resources of the single PC under various conditions[19]. VMware is a virtual machine tool that provides a virtual PC environment that enables several instances of the working frameworks to continue operating on a single server.

B. Network analysis using Wireshark:

As a network packet analyzer, Wireshark captures packet data and displays it in as much detail as possible [20]. It is possibly one of the best open-source packet analysers accessible on the market now. Wireshark is used to troubleshoot network problems, examine security problems, to debug the protocol implementation. For evaluating the resilience of websites against security attacks, most penetration testers use Wireshark over other network protocol analyzers as it complies with international industry and educational standards. A live network's data can be simply gathered and analysed offline[21]. It is not limited to any one operating system and supports hundreds of protocols. It is also said to feature one of the strongest display filters available. Among the several functions

offered by Wireshark are the following: Compatibility with Windows and UNIX., capturing live packet data from an interface on a network., Show packets with extensive protocol details, Access and save the captured packet data.

C. Packets captured during scanning:

In this paper, Wireshark plays a significant role in capturing the packets. Nmap's communication with www.honeypot.com(192.168.100.10) may be analysed by examining the packets that were captured and collected by Wireshark during the TCP connect scan. The following are the packets captured by Wireshark during the investigation:

SYN packet: sent from the source(Nmap), It delivers the target 192.168.100.10 a SYN (synchronise) packet to start the three-way handshake. It indicates the start of a connection attempt and requests the honeypot server to confirm the synchronisation.

SYN-ACK packet: This packet is received from the target www.honeypot.com. The target replies with SYN-ACK packets which indicates that the target is ready for connection, It confirms the SYN packet sent from Nmap indicating it is ready for communication

ACK packet: this packet is again sent from Nmap, In response to the SYN-ACK packet of the target (192.168.100.10) Nmap sends the ACK (acknowledge) packet which completes the three-way handshake, establishing a connection between www.honeypot.com(192.168.100.10) and Nmap

RST packet: This packet is sent from both directions Nmap and Target which indicates that an unexpected error occurred during connection, it occurred due to firewalls and other countermeasures

FIN packet: Nmap sends the FIN packet to end the connection from the target, which indicates the end of the scanning

Examining all these packets at once provides an extensive understanding of the workings of the TCP connect scan. The connection is established via the three-way handshake, and the target's(192.168.100.10) port status is disclosed by packets. A comprehensive picture of the communication between Nmap and 192.168.100.10 is provided by the RST and FIN packets, which indicate the end of connections.

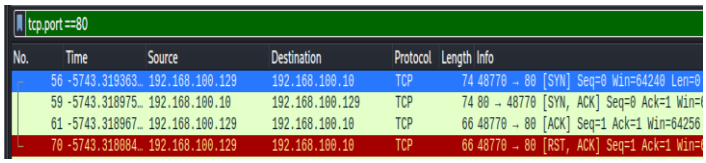

Figure 4 Wireshark capture of port 80 and Three-way handshake performance

D. TCP Connect Scan(-sT) Parameters and its effect:

The scanner makes an effort to successfully establish a TCP connection on each port using this approach. When a connection is successfully established with complete three-way handshakes, the TCP connect scanner considers that the port is open. Otherwise, it is marked as closed[22] Due to a connection attempt carried out by the port scanner, this scanning approach is effective in showing if a port is open for connection from another program. On the scanned system, however, this kind of scan is quite simple to identify. Almost usually, attempts to connect() to every port on the machine will result in a warning if the target is running a firewall or intrusion detection system[23].

The TCP connect scan uses several parameters during the attack some of them are:

-sT(TCP connect scan): This is main parameter that describes the TCP connect scan[9]. It connects to the target machine by initiating a three-way handshake. The effect of this parameter includes Stealthiness: Compared to other scan types like the SYN scan (-sS), the TCP connect scan is more noticeable. It becomes more detectable as it completes a three-way handshake Dependability: Since it establishes a connection, it guarantees that the target system responds well, providing reliable data about open ports.

-v(Verbose): This parameter provides more thorough information, the effect includes: Verbose output can help understand the scan's progress as well as gather more information about the target.

-oN(normal output): As the name suggests this parameter saves the result of the scan to a file in normal format, which helps in saving the result for further documentation

-p(port specification): The specific ports to be scanned can be selected using this parameter. For instance, using -p 1-500 will scan ports from 1 to 500. Impact: Using these parameters one can scan a specific range of ports which makes it more efficient

E Aspect of TCP Protocol exploited by TCP connect scan(-sT):

During the investigation, it was found that TCP connect scan a technique that uses Nmap to exploit specific aspects of Transmission control protocol to access the network host at target machine (192.168.100.10). This is an in-depth description of how this vulnerability occurs during the Nmap attack:

Three-way Handshake: To set up a connection with www.honeypot.com(192.168.100.10), TCP connect scan(-sT) begins the Three-way handshake, which is the very basic step in Transmission control protocol (TCP). Nmap Tcp connect scan first send the SYN packet to www.honeypot.com to start the communication, then target machine(192.168.100.10) respond backs with SYN/ACK packet, Nmap then again sends the ACK packet which completes the three-way handshake. So The three-way handshake process of TCP is exploited by TCP connect scan in this manner

Analysis of the response: if the port in the target machine 192.168.100.10 is open then target response with SYN/ACK, If the port is closed then the target sends the RST packet which indicates that the connection is rejected

Effects on Target System(192.168.100.10): Nmap's TCP connect scan uses the TCP protocol for its benefit by allowing it to communicate with the target system in a way that is likely to be authorized, conventional communication's TCP connect scan(sT) reveals the entry points and ports of the target(192.168.100.10)

Finding the port states: Nmap carefully examines the responses to figure out each probed port's available state. The target machine's(192.168.100.10) availability to establish a connection is indicated by an open port, which is signalled by a SYN-ACK response. On the other hand, a RST response indicates a closed port, which means that a connection cannot be established.
To conclude, the TCP connect scan in Nmap surreptitiously Alters the standard TCP connection protocols to secretly determine whether network ports are accessible. By adhering to the standards of TCP communication, this systematic approach not only improves the efficacy of the scan but also provides insightful information about the target system

IV. COUNTERMEASURES TECHNIQUE AND ITS EFFECTS

Implementing strong countermeasure strategies into practice is essential for enhancing network security in response to the vulnerabilities revealed by Nmap's TCP connect scan. Robust security will be required to reduce the effects of port scanning, especially when a certain machine, like www.honeypot.com (192.168.100.10), is the target. This section explores some common countermeasure techniques used in industry to mitigate the port scanning effect

Intrusion Detection System (IDS): An IDS is a hardware or software device that spots malicious activity on computer systems so that system security may be preserved[24]. IDS aims to detect various forms of malicious network traffic and computer activity that an average firewall is unable to detect. This is necessary for establishing robust security against activities that jeopardize computer systems' confidentiality, integrity, or availability. If the same IP address tries to connect to multiple ports, modern intrusion detection and prevention systems may easily stop such port scanning activity. This is a duty that even antivirus software can handle. Professional hackers attempt to use vertical distributed scanning[25]. The attacker threats are not always of the same level of risk. Some are just little irritations, but others could endanger the growth and existence of the organization[26]. Three essential elements are evident in the most harmful threats: execution speed, intensity and unexpected

Port Knocking: A series of connection attempts on various specified ports are made as part of the security practice known as "port knocking" to obtain access to a network or service[27]. It hides open ports until the proper knocking sequence is carried out, adding a layer of security. This approach assists in avoiding unauthorized access and can make it difficult for attackers to identify services that are available. As a type of access control, port knocking prevents unauthorized users from using services until they have successfully completed the proper port sequence. Port knocking hides open ports from potential attackers, making it more difficult for them to carry out reconnaissance, by maintaining ports closed until the proper port sequence is detected.

Honeypots: In network security, honeypots are a cutting-edge idea. [28]Information regarding attempted or actual intrusions into a resource is the aim of this kind of technology. For example, the time, date, the compromised IP address, the compromised OS system, or the wordlists, exploits, and instructions used after infiltration—all of these details might be drastically different. An information source known as a "honeypot" is often created with the intention of identifying and preventing any effort to gain access to an experimental system[29]. A honeynet is a system made up of many honeypots. The real system, which is a server behind the honeypot, will be secure and undamaged even if the attacker manages to breach the system or server. Instead, the hacking attempt will target the honeypot, which resembles the original server. The purpose of the honeypot is to improve whole security, based on its level of engagement, rather than to fix a server-related issue[30]. The degree of interaction between the information system and an attacker is measured by the level of engagement.

TCP wrappers: 'TCP Wrapper' is the most widely used program that supports system authorization[31]. Which service requests from which hosts should be approved or rejected in advance can be specified by the administrator. Only requests for services from hosts that are permitted are accepted. TCP Wrappers verify a host's approval before enabling access, much like a checkpoint soldier[32]. Until the client or host is authorized, TCP Wrappers comes in as the middleman and operates as the server. To authenticate hosts, TCP Wrappers make utilize of their access control functionality wrappers allow restriction to TCP services

Firewall: The first and most basic purpose of a firewall is to monitor and regulate the network traffic that is permitted to reach the network host under protection[33]. Usually, firewalls work in this way: they analyse packets, maintain track of connections being established, and filter connections based on the findings of their packet inspections and the connections they notice.

IP Tables: In the investigation, it is found that Nmap's TCP connect scan(-sT) poses a threat by establishing a three-way handshake i.e., a complete connection to 192.168.100.10. Implementing robust countermeasures like IP tables is necessary for network security
A command-line firewall tool named iptables utilizes policy chains to either allow or prohibit traffic. To match a connection when it struggles to establish itself on any given system, iptables searches through its set of rules. It falls back on the default action if it is unable to find one[34]. An essential part of Linux-based systems, IP tables can be used as a tool for managing firewalls. It enables network address translation (NAT), packet filtering rules, and packet mangling to be defined by administrators. By strategically configuring rules to regulate incoming connection requests, IP tables can be used to fight Nmap TCP Connect Scans and reduce their impact. IP table function at OSI layer 3(network)[35]. Three built-in tables are included with the IP table: FILTER, MANGLE and NAT
Packet filtering: Administrators can implement rules using IP tables to filter incoming, outgoing, and forwarded packets according to a variety of parameters, like protocols, ports, source and destination IP addresses, and more. It has the following default chain

Input: The server receives packets that are governed by the rules in this chain.
Output: This chain oversees managing the packets leaving the system.
Forward: This rule set controls how packets are routed through the server.
Network Address Translation (NAT): NAT, an approach that changes network address information in packet headers while in transit, is made easier by IP tables. NAT rules are incorporated in this table to route packets to networks that are inaccessible directly. The NAT table is used when modifying a packet's source or destination. The chains listed below are among them:
Prerouting: packets are assigned by this chain as soon as they arrive at the server.
Output: functions in the same way as the output chain that the filter table explained.
Postrouting: After a packet exits the output chain, it is possible to modify it using the rules in this chain
Packet Mangling: Administrators can alter packet content and headers by using IP tables to carry out packet mangling operations. The functionality can be helpful for traffic characteristic customization, network optimization, and the application of certain network policies. This table has the following chains: Prerouting, post-routing, Output, Input, Forward

A .Configuration of IP tables rules And TCP settings:

We can implement IP tables to block incoming connection requests to strengthen the target system (192.168.100.10) against TCP Connect Scans by Nmap. configuration includes reducing scanning attempts can be achieved by limiting access to particular source IP addresses. Rules for IP tables can be created to only allow connections from reliable sources while blocking access to others,
By setting up regulations that restrict the number of connections that may be made at once from a single source, saturation and possible denial-of-service situations brought on by port scanning can be minimised. And also It can be advantageous to set IP tables to rate limit connection requests coming from a certain IP address or range. This prevents scanning operations' frequent bursts of connection attempts from overloading the target machine.
An effective defence against Nmap TCP Connect Scans can be provided by IP tables. Strategically built and deployed, they act as an effective countermeasure, strengthening the target system's security posture.
Configuring TCP settings: this configuration plays a significant role, it involves adjusting certain TCP parameters to optimize the network security
Adjusting time-out values: The duration that a system will wait for a response before concluding that a connection attempt has failed is figured out by the timeout values. This is usually done by using the command '*sysctl1'* in Linux
Limiting connections: Preventing exhaustion of resources, port scanning and potential denial-of-service attacks can be achieved by limiting the number of concurrent connections that originate from a single source
Implementing rate limit: Rate limiting controls the rate at which connection requests are accepted from a particular source, mitigating rapid-fire connection attempts. Firewalls or network devices provide rate limit feature
TCP keep alive: sends little packets at regular intervals to guarantee that a connection is still operational. This can be configured by using parameters such as '*tcp_keepalive_time'* can be adjusted using '*sysctl'*

V. CONCLUSION AND FUTURE WORK

A technical investigation on port scanning using the TCP connect scan method has shed light on the safety consequences and vulnerabilities related to Nmap's features. A thorough understanding of the impact of attack software, countermeasure approaches, and network protocol investigation has led to a full knowledge of the scan's effects on the target server (www.honeypot.com). The target machine's(192.168.100.10) open ports and exposed services were mapped out in detail by the TCP connect scan, providing information on possible points of entry for attackers. Furthermore, the patterns of communication between www.honeypot.com and Nmap were investigated. Additionally, the formation of the TCP connect scan three-way handshake using Wireshark and its impact on the OSI 4 layer (TCP) was scrutinized
To enhance the investigation future work would include:
Advanced scanning techniques like UDP scan, FTB bounce scan, idle scan and many more. Additionally using methods for network monitoring to continually examine incoming and outgoing traffic. Deploying alerting systems that are automatic and that send out messages when they see anomalous scanning activity and putting in place automatic responses for identified scanning sources, including rate limitation or temporary blockage.

VI. REFERENCES

[1] R. Abu Bakar and B. Kijsirikul, "Enhancing Network Visibility and Security with Advanced Port Scanning Techniques," *Sensors*, vol. 23, no. 17, p. 7541, 2023.

[2] M. Shah, S. Ahmed, K. Saeed, M. Junaid, and H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool," in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, IEEE, 2019, pp. 1–6.

[3] Q. A. Al-Haija, E. Saleh, and M. Alnabhan, "Detecting port scan attacks using logistic regression," in *2021 4th International Symposium on advanced electrical and communication technologies (ISAECT)*, IEEE, 2021, pp. 1–5.

[4] M. Ring, D. Landes, and A. Hotho, "Detection of slow port scans in flow-based network traffic," *PLoS One*, vol. 13, no. 9, p. e0204507, 2018.

[5] A. Upadhya and B. K. Srinivas, "A Survey on different Port Scanning Methods and the Tools Used to perform

them," *Int J Res Appl Sci Eng Technol*, vol. 8, no. 5, 2020.

[6] R. Vadivel and S. Mayukha, "Port Scanning Mitigation Strategies for Penetration Testing: Blue Team Perspective," in *2022 International Conference on Engineering and Emerging Technologies (ICEET)*, IEEE, 2022, pp. 1–6.

[7] E. V Ananin, A. V Nikishova, and I. S. Kozhevnikova, "Port scanning detection based on anomalies," *2017 Dynamics of Systems, Mechanisms and Machines (Dynamics)*, pp. 1–5, 2017.

[8] A. Orebaugh and B. Pinkard, *Nmap in the Enterprise: Your Guide to Network Scanning*. Elsevier Science, 2011. [Online]. Available: https://books.google.co.uk/books?id=VjgezB784XIC

[9] "https://nmap.org/book/man-port-scanning-techniques.html."

[10] M. Lin and M. Jun, "Study on Understanding Manner of ISO/OSI Seven Layers Architecture [1]," *Journal of Southwest Nationalities College Natural Science Edition*, vol. 27, no. 1, pp. 35–39, 2001.

[11] L. Staalhagen, "A comparison between the OSI reference model and the B-ISDN protocol reference model," *IEEE Netw*, vol. 10, no. 1, pp. 24–33, 1996.

[12] "https://www.bmc.com/blogs/osi-model-7-layers/."

[13] D. Wetteroth, *OSI Reference Model for Telecommunications*. in McGraw-Hill telecom professional. McGraw Hill LLC, 2001. [Online]. Available: https://books.google.co.uk/books?id=DLNpjT3K4ooC

[14] Y. Li, D. Li, W. Cui, and R. Zhang, "Research based on OSI model," in *2011 IEEE 3rd International Conference on Communication Software and Networks*, IEEE, 2011, pp. 554–557.

[15] "https://www.geeksforgeeks.org/presentation-layer-in-osi-model/."

[16] R. Baloch, *Ethical Hacking and Penetration Testing Guide*. in Auerbach Book. CRC Press, 2017. [Online]. Available: https://books.google.co.uk/books?id=fKfNBQAAQBAJ

[17] P. Calderon, *Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips*. Packt Publishing Ltd, 2021.

[18] K. Chhillar and S. Shrivastava, "University computer network vulnerability management using Nmap and Nexpose," *International Journal*, vol. 10, no. 6, 2021.

[19] G. Kaur and N. Kaur, "Penetration testing–reconnaissance with NMAP tool," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 3, pp. 844–846, 2017.

[20] U. Lamping and E. Warnicke, "Wireshark user's guide," *Interface*, vol. 4, no. 6, p. 1, 2004.

[21] S. Sandhya, S. Purkayastha, E. Joshua, and A. Deep, "Assessment of website security by penetration testing using Wireshark," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, IEEE, 2017, pp. 1–4.

[22] A. Sivanathan, H. H. Gharakheili, and V. Sivaraman, "Can we classify an iot device using TCP port scan?," in *2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS)*, IEEE, 2018, pp. 1–4.

[23] A. J. Bennieston, "Nmap-a stealth port scanner." 2004.

[24] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, 2019.

[25] S. V Bredikhin, V. I. Kostin, and N. G. Scherbakova, "Detection of scanners in IP networks by the method of sequential statistical analysis," *Bulletin of NSU Series: Information Technology*, no. 4, pp. 15–35, 2016.

[26] E. A. Basinya, V. E. Khitsenko, and A. A. Rudkovskiy, "Countermeasure method against unauthorized and anonymous information system data collection," in *2019 Dynamics of Systems, Mechanisms and Machines (Dynamics)*, IEEE, 2019, pp. 1–6.

[27] F. H. M. Ali, R. Yunos, and M. A. M. Alias, "Simple port knocking method: Against TCP replay attack and port scanning," in *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, IEEE, 2012, pp. 247–252.

[28] D. Fraunholz, M. Zimmermann, and H. D. Schotten, "An adaptive honeypot configuration, deployment and maintenance strategy," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, IEEE, 2017, pp. 53–57.

[29] R. C. Joshi and A. Sardana, *Honeypots: a new paradigm to information security*. CRC Press, 2011.

[30] H. Wafi, A. Fiade, N. Hakiem, and R. B. Bahaweres, "Implementation of a modern security systems honeypot honey network on wireless networks," in *2017 International Young Engineers Forum (YEF-ECE)*, IEEE, 2017, pp. 91–96.

[31] M. Kwon, J. Hong, and Y. Cho, "Ethernet wrapper: extension of the TCP wrapper," in *Proceedings. Eighth International Conference on Parallel and Distributed Systems. ICPADS 2001*, IEEE, 2001, pp. 573–580.

[32] "https://www.giac.org/paper/gsec/445/tcp-wrappers-they/101088."

[33] W. Noonan and I. Dubrawsky, *Firewall fundamentals*. Pearson Education, 2006.

[34] "https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/."

[35] G. N. Purdy, *Linux iptables Pocket Reference: Firewalls, NAT & Accounting*. " O'Reilly Media, Inc.," 2004.