A green chameleon logo

Description automatically generated

**SYN AND FULL SCAN**

​​

TABLE OF CONTENTS

1-Summary

2- Introduction

3- Tools Used

4-Scope of testing

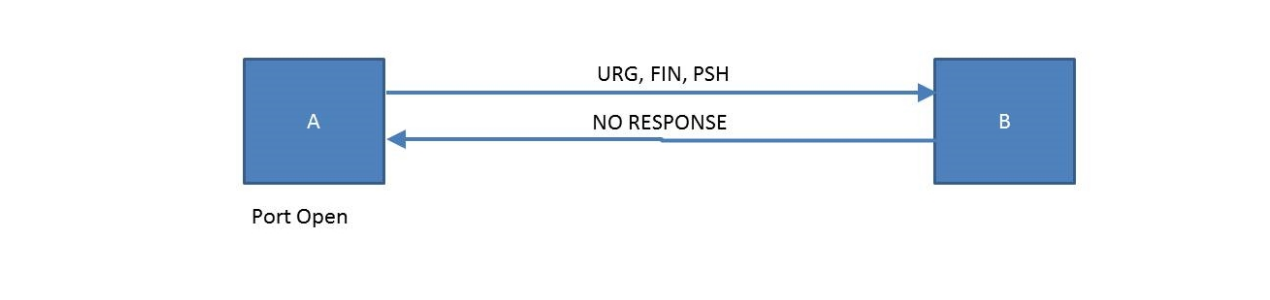
5-Results

6-Conculsions

7-References

**EXECUTIVE SUMMARY**

In this scan, the **ACK**, **SYN**, **URG**, **RST**, and **FIN** flags are all set at once on the same packet. The issue with this is that since all the flags are set, the target system may have difficulties in interpreting the packets it has received. The following diagram shows this process:



**INTRODUCTION**

A SYN scan is a type of network scanning method used by security researchers and hackers to discover open ports on a target system. It is a part of the TCP three-way handshake process, which is the method by which most TCP connections are established. The three steps in the handshake are:

SYN (Synchronize): The client sends a SYN packet to the server, indicating an intention to establish a connection.

SYN-ACK (Synchronize-Acknowledge): If the port is open, the server responds with a SYN-ACK packet, indicating that it received the SYN and is willing to establish a connection.

ACK (Acknowledge): Finally, the client sends an ACK packet, acknowledging the receipt of the SYN-ACK. At this point, the connection is established.

In a SYN scan, the attacker sends SYN packets to a range of port numbers on the target system without completing the three-way handshake. This allows the attacker to determine which ports are open without actually establishing a full connection. If a SYN-ACK is received, the attacker knows the port is open; if a RST (Reset) packet is received, the port is closed.

**TOOLS USED**

Nmap:

Description: Nmap (Network Mapper) is a powerful and widely used open-source tool for network discovery and security auditing. It supports various scanning techniques, including SYN scanning.

Command: nmap -sS [target]

Hping:

Description: Hping is a command-line tool that allows users to send custom TCP/IP packets and display their responses. It's versatile and can be used for various network-related tasks, including SYN scanning.

**SCOPE OF TESTING**

The scope of testing SYN scans, or any type of security testing, should be well-defined and conducted in an ethical and legal manner. SYN scanning is typically used for security assessments to identify open ports on a network or system, and it can help organizations understand potential vulnerabilities that could be exploited by attackers. Here are key considerations regarding the scope of testing SYN scans:

Authorized Testing:

Ensure that you have explicit authorization before conducting any SYN scans. Unauthorized scanning is not only unethical but can also lead to legal consequences.

Define Objectives:

Clearly define the objectives of the SYN scan. Identify the specific systems, networks, or applications that are within the scope of the testing.

Agreement with Stakeholders:

Communicate with relevant stakeholders, including network administrators and system owners. Obtain their approval and inform them about the testing schedule to prevent any unnecessary alarms.

Legal and Regulatory Compliance:

Ensure that the SYN scans comply with applicable laws and regulations. Some regions and industries have specific rules regarding network and system testing.

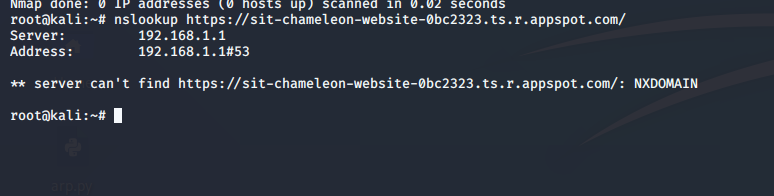
Documentation:

Document the scope, methodology, and results of the SYN scan. This documentation is valuable for internal records, audit purposes, and for explaining the findings to relevant parties.

Respect Privacy:

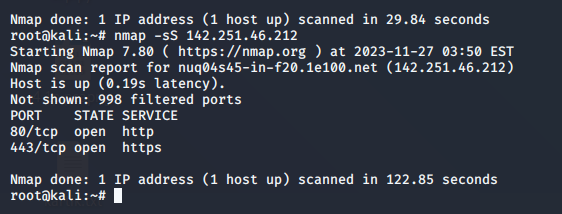
Be mindful of privacy considerations, especially when scanning systems that may contain sensitive or personal information. Avoid collecting or accessing information that is not within the scope of the testing.

Results

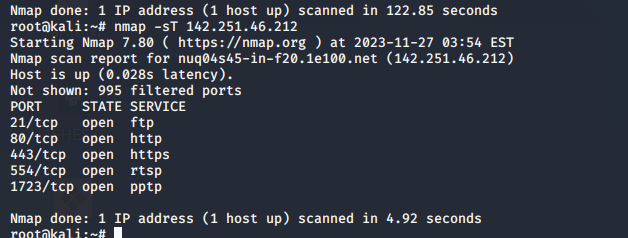


A screenshot of a computer

Description automatically generated



We can easily see that these two ports are opened of the chameleon of the website 80 and 443.This is the SYN SCAN I have done with the chameleon website and it can be seen easily that all the ports (1000) are opened.



This is of the full scan where we can see that lots of the ports are opened which can be used for the attacks such as fever attack etc and analysed these ports in the Wireshark as the traffic of them.

**CONCLUSION**

In conclusion, SYN scanning is a widely used technique in the field of network security testing and vulnerability assessment. It serves the purpose of identifying open ports on a target system, providing valuable insights into potential vulnerabilities that could be exploited by malicious actors. However, it's crucial to approach SYN scanning and any security testing activities with careful consideration and adherence to ethical and legal guidelines. Here are key points to summarize:

Purpose and Objective:

SYN scanning is employed to discover open ports on a target system or network.

The primary objective is to assess the security posture by identifying potential entry points for attackers.

Authorized and Ethical Use:

SYN scanning, like any security testing method, should only be conducted with explicit authorization from the system owner or administrator.

Ethical use involves respecting privacy, following legal guidelines, and obtaining proper consent.

References:

1-https://www.plixer.com/blog/understanding-xmas-scans/

2-TCP FIN, NULL, and Xmas Scans (-sF, -sN, -sX) | Nmap Network Scanning

3-https://subscription.packtpub.com/book/security/9781788995177/4/ch04lvl1sec39/xmas-scans