A green chameleon logo

Description automatically generated

XMAS, FULL AND SYN SCAN of Chameleon Website

​​

​

Contents

[Introduction: 3](#_Toc152695450)

[Tools used: 3](#_Toc152695451)

[Scope of Testing 3](#_Toc152695452)

[Methodology 3](#_Toc152695453)

[Results 5](#_Toc152695454)

[XMAS Scan 5](#_Toc152695455)

[SYN Scan: 5](#_Toc152695456)

[Full Scan: 6](#_Toc152695457)

[Conclusion - Where to from here? 6](#_Toc152695458)

[References: 7](#_Toc152695459)

# Introduction:

Nmap, the free and open-source network scanner, used for exploring the hidden world of connected devices. It's like having an x-ray vision for networks, revealing the intricate details of open ports, services, and even vulnerabilities lurking beneath the surface.

# Tools used:

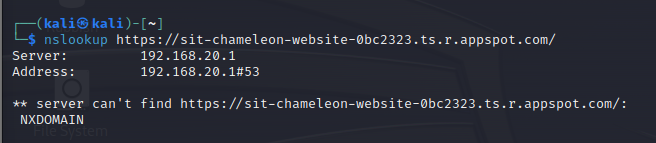
* Kali Linux
* Terminal
* NMAP

# Scope of Testing

The scope of this testing is to scan the Chameleon website using the following scans XMAS, FULL AND SYN SCAN.

The Chameleon website can be found here: <https://sit-chameleon-website-0bc2323.ts.r.appspot.com/>

To get the actual IP of the website I performed an nslookup command in Kali Linux. This allowed me to find the website’s IP address if order to perform the NMAP scans.



# 

# Methodology

1. Pre-scanning:

* Target discovery: Needed to know the website IP
* Port selection: determined the type of scans to be used (full, XMAS, SYN)

2. Inputting the scans:

* The packets are sent to the target system's IP address and designated ports.

3. Receiving responses:

* SYN/ACK: Indicates an open port.
* RST (reset): Indicates a closed port.
* No response: Can mean either open or filtered, requiring further investigation.

4. Interpreting results:

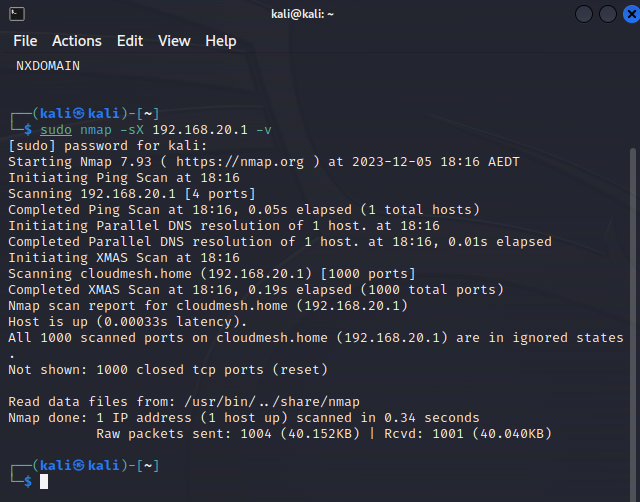
* Based on the responses, Nmap classifies ports as open, closed, filtered, or sometimes unfiltered

5. Output and analysis:

# Results

## XMAS Scan

An XMAS scan was performed on the Chameleon website. This scan identifies listening ports on a targeted system by sending a specific packet. An Xmas scan sets three TCP flags: FIN, PSH, and URG.

The XMAS scan found that all 1000 ports were scanned and that there was 1000 closed tcp ports. This means that all 1000 scanned ports responded with a closed TCP RST packet. In other words, none of the ports were open or listening for connections.

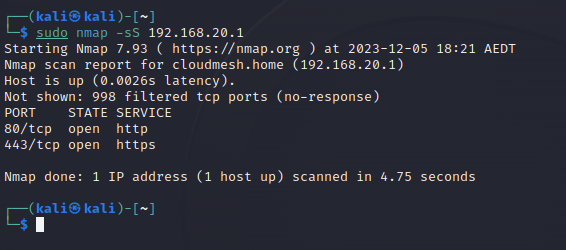
## SYN Scan:

A SYN scan, also known as a TCP SYN scan or half-open scan, is a popular technique used in network scanning with Nmap to identify open ports on a target system. The scan showed that there were two open ports, those ports being port 80 and port 443 were open.

Having ports 80 and 443 open in a Nmap scan is significant because these ports are commonly associated with specific services.

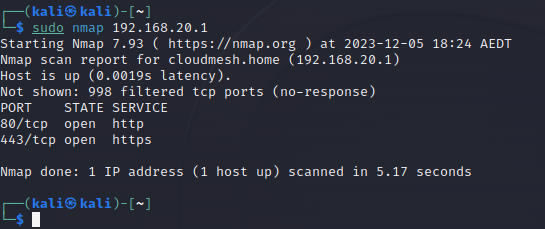
Port 80 is the default port for HTTP traffic, meaning unencrypted web communication. If port 80 is open, it indicates that the target system likely hosts a website or web application accessible through a normal web browser.

Port 443 is the default port for HTTPS traffic, which is encrypted HTTP. If port 443 is open, it suggests the presence of a secure website or web application that uses encryption for data protection.



## Full Scan:

Below performed was a basic “full” scan of the Chameleon website. It showed similar data to the SYN scan showing port 80 and port 443 being open with everything else being close.



# Conclusion - Where to from here?

From the scans, it appears that all ports are closed, except for the necessary ones such as Port 80 and Port 443. Meaning, that all required ports that don’t need to be open are closed. Keeping TCP ports closed during a Nmap scan minimises attack surfaces, hides sensitive information, reduces resource strain, closes the chance of reconnaissance attempts, and enforces least privilege. It's a simple but powerful way to tighten your network security and keep the bad actors out.

# References:

<https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/>

<https://nmap.org/book/man-port-scanning-techniques.html>