



CHAMELEON

FOR OUR SMARTER WORLD

XMAS, FULL AND SYN SCAN of Chameleon Website

Contents

Executive summary:

Introduction:

Nmap, the free and open-source network scanner, is your trusty swiss army knife 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
- Parallels

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 in order to perform the NMAP scans.

```
(kali㉿kali)-[~]  
$ nslookup https://sit-chameleon-website-0bc2323.ts.r.appspot.com/  
Server:      192.168.20.1  
Address:     192.168.20.1#53  
  
** server can't find https://sit-chameleon-website-0bc2323.ts.r.appspot.com/:  
NXDOMAIN
```

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

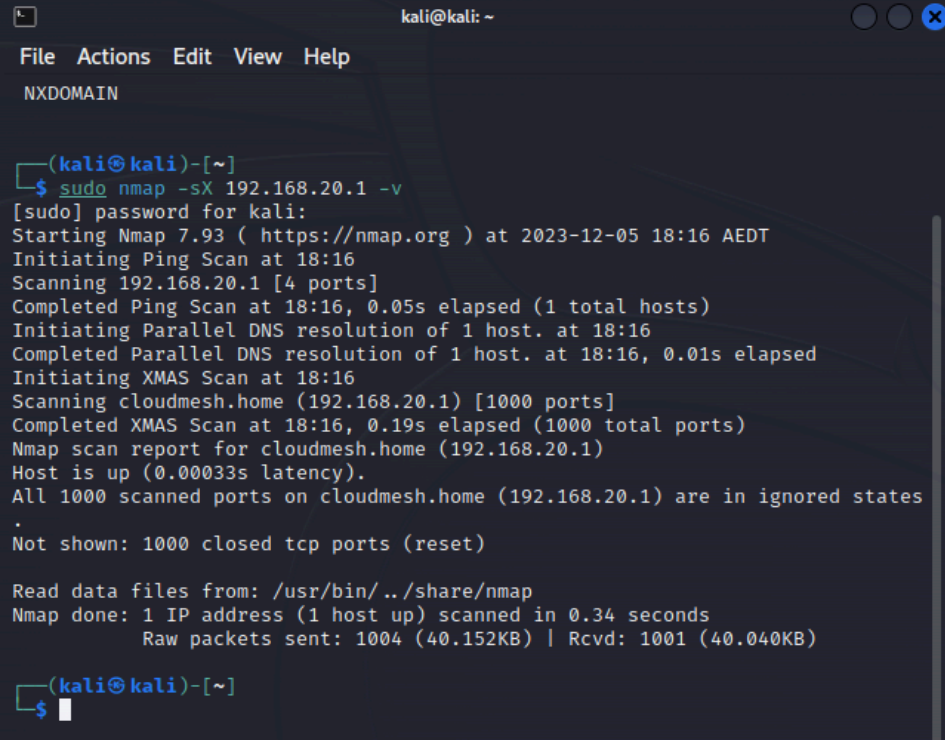
5. Output and analysis:

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.

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal content shows the execution of 'sudo nmap -sX 192.168.20.1 -v'. The output indicates a successful XMAS scan of 1000 ports on cloudmesh.home (192.168.20.1), resulting in 1000 closed TCP ports (reset). The scan took 0.34 seconds and sent 1004 raw packets. The prompt '(kali@kali)-[~]' is visible at the bottom.

```
kali@kali: ~  
File Actions Edit View Help  
NXDOMAIN  
  
(kali@kali)-[~]  
$ sudo nmap -sX 192.168.20.1 -v  
[sudo] password for kali:  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-05 18:16 AEDT  
Initiating Ping Scan at 18:16  
Scanning 192.168.20.1 [4 ports]  
Completed Ping Scan at 18:16, 0.05s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 18:16  
Completed Parallel DNS resolution of 1 host. at 18:16, 0.01s elapsed  
Initiating XMAS Scan at 18:16  
Scanning cloudmesh.home (192.168.20.1) [1000 ports]  
Completed XMAS Scan at 18:16, 0.19s elapsed (1000 total ports)  
Nmap scan report for cloudmesh.home (192.168.20.1)  
Host is up (0.00033s latency).  
All 1000 scanned ports on cloudmesh.home (192.168.20.1) are in ignored states  
.  
Not shown: 1000 closed tcp ports (reset)  
  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds  
Raw packets sent: 1004 (40.152KB) | Rcvd: 1001 (40.040KB)  
  
(kali@kali)-[~]  
$
```

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.

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.20.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-05 18:21 AEDT
Nmap scan report for cloudmesh.home (192.168.20.1)
Host is up (0.0026s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.75 seconds

(kali㉿kali)-[~]
$
```

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.

```
(kali㉿kali)-[~]
$ sudo nmap 192.168.20.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-05 18:24 AEDT
Nmap scan report for cloudmesh.home (192.168.20.1)
Host is up (0.0019s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.17 seconds

(kali㉿kali)-[~]
$
```

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>