PORT SCAN ON CHAMELEON WEBSITE

CHAMELEON

FOR OUR SMARTER WORLD

TABLE OF CONTENTS:

INTRODUCTION

What is port scan?

Scanning for open ports is known as port scanning, and it is utilized in computer networking and cybersecurity. Network ports are virtual communication endpoints that are bound to a particular service or protocol. Port scanning is frequently conducted for various reasons, including network management, security evaluations, and troubleshooting. Here's a rundown of what port scanning entails:

PURPOSE:

In computer networking and cybersecurity, the process of looking for open ports is known as port scanning, and it is used in both of those fields. The term "network port" refers to a virtual communication endpoint that is associated with a certain kind of service or protocol. Scanning of ports is performed often for a variety of purposes, including the administration and assessment of networks and their security, as well as troubleshooting. An overview of what port scanning comprises is provided below:

TOOLS AND SOFTWARES BEING USED:

-> KALI LINUX – It is an Operating System.

-> WIRE SHARK – Tool used for capturing the traffic.

-> NMAP- It is used to scan the ports.

PROCESS:

NMAP-:

This essential command is the primary directive for starting the Nmap program, which denotes the beginning of the scanning process. It is also known as the nmap scan command.

-sS this option, which is used as a tactical decision, denotes a TCP SYN scan. A TCP SYN scan is a complex port scanning mechanism that has been painstakingly developed to determine whether or not TCP ports on the target system are accessible. Using this method, SYN packets are sent to each port, and the answers to those packets are carefully analyzed in order to determine whether or not the port in question is open or closed.

- -T4: This parameter adjusts the timing template to "Aggressive" (T4) so that the scan may be completed more quickly while still maximizing its efficiency. This decision assures that the scanning will proceed at a reasonably quick rate while also retaining its accuracy.

- -v: The verbose (-v) option is active, which provides a detailed, real-time data stream describing the course of the scan. This is an essential component for gaining a deeper understanding of the situation.

- -n: Choosing this option instructs Nmap to refrain from engaging in DNS resolution for IP addresses and hostnames. This option is accessible in the Options menu. This simplified strategy speeds up the scanning process, especially when the primary emphasis is placed just on IP addresses.

• --maximum degree of parallelism This strategic specification limits the total number of simultaneous probes to a count of 10, dictating the maximum quantity of probes that may be sent out throughout the scan. This function improves both the scan speed and the usage of available resources.

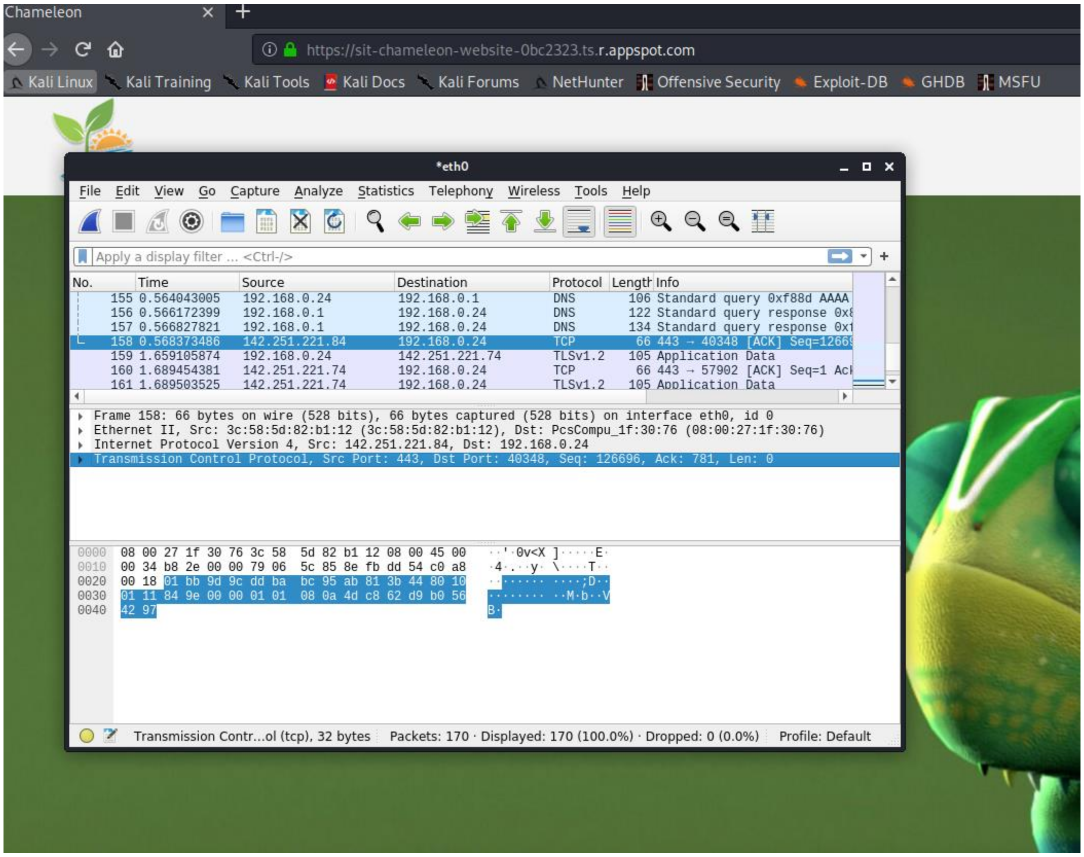
• -Pn: If you choose this setting, you will prevent host discovery from occurring on purpose. It functions on the presumption that the host is operational even if it does not react to standard host discovery probes. This is because it is designed to get around this limitation. This capability shows to be quite helpful when evaluating hosts that do not respond.

• --top-ports 100: This option painstakingly focuses the focus of the scan towards the top 100 ports that are used the most often. Nmap keeps a curated list of these ports, which allows it to refine the scan and zero in on the principal network entry points.

These tools and settings have been deliberately designed to allow a complete and efficient study of the Chameleon website's port setup. This makes it possible for potential vulnerabilities to be detected with accuracy and thoroughness.

IP ADDRESSES:

To find the IP address of the chameleon website and the Virtual Machine, I have used wireshark framework.



```
No.   Time         Source          Destination     Protocol Length Info
  155 0.564043005  192.168.0.24    192.168.0.1     DNS       106 Standard query 0xf88d AAAA
  156 0.566172399  192.168.0.1     192.168.0.24    DNS       122 Standard query response 0x8
  157 0.566827821  192.168.0.1     192.168.0.24    DNS       134 Standard query response 0x1
  158 0.568373486  142.251.221.84  192.168.0.24    TCP        66 443 → 40348 [ACK] Seq=1266
  159 1.659105874  192.168.0.24    142.251.221.74  TLSv1.2   105 Application Data
  160 1.689454381  142.251.221.74  192.168.0.24    TCP        66 443 → 57902 [ACK] Seq=1 Ack
  161 1.689503525  142.251.221.74  192.168.0.24    TLSv1.2   105 Application Data
```

```
Frame 158: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
Ethernet II, Src: 3c:58:5d:82:b1:12 (3c:58:5d:82:b1:12), Dst: PcsCompu_1f:30:76 (08:00:27:1f:30:76)
Internet Protocol Version 4, Src: 142.251.221.84, Dst: 192.168.0.24
Transmission Control Protocol, Src Port: 443, Dst Port: 40348, Seq: 126696, Ack: 781, Len: 0
```

```
0000  08 00 27 1f 30 76 3c 58  5d 82 b1 12 08 00 45 00   ··'·0v<X ]·····E·
0010  00 34 b8 2e 00 00 79 06  5c 85 8e fb dd 54 c0 a8   ·4·.··y· \····T··
0020  00 18 01 bb 9d 9c dd ba  bc 95 ab 81 3b 44 80 10   ········ ····;D··
0030  01 11 84 9e 00 00 01 01  08 0a 4d c8 62 d9 b0 56   ········ ··M·b··V
0040  42 97                                              B·
```

```
Transmission Contr...ol (tcp), 32 bytes   Packets: 170 · Displayed: 170 (100.0%) · Dropped: 0 (0.0%)   Profile: Default
```

Here we can see that IP address of the Chameleon website is 142.251.221.84 and the IP address of the virtual machine is 192.168.0.24.

-> Virtual machine IP address I.e 192.168.0.24 represents a private Internet Protocol address that has been allotted to the Kali Linux virtual machine. This address acts as the gateway via which one may do network activities while still operating inside the virtual environment.

-> Chameleon website IP address I.e 142.251.221.84 is linked to the original Chameleon site. When doing a port scan, this address is a crucial identifier of the device being probed.

COMMAND WHICH IS EXECUTED FOR THE PORT SCAN:

```
nmap -sS -T4 -v -n --max-parallelism 10 -Pn --top-ports 100
142.251.221.84
```

REFRENCE FOR THE COMMAND:

-> -sS: Starts a TCP SYN scan to locate open ports by sending packets and evaluating replies.

-> Timing template "Aggressive" (T4) optimizes scan efficiency by speeding up execution.

-> -v: "Verbose" displays scan progress data.

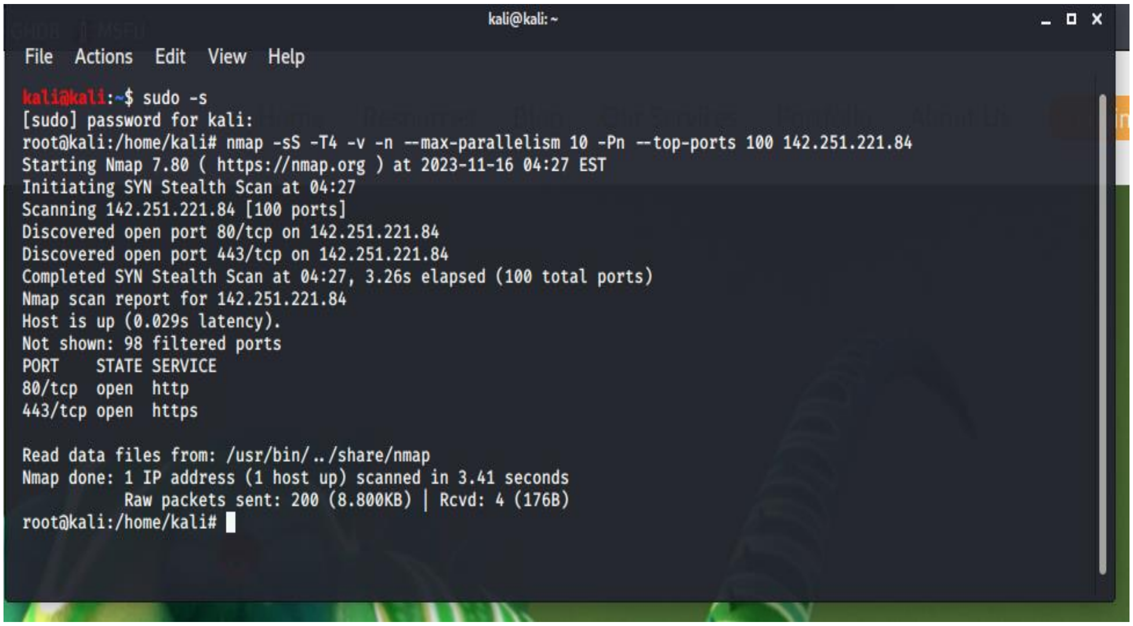
-> -n skipping DNS resolution for IP addresses and hostnames speeds up the scan and focuses on IP addresses.

-> --max-parallelism 10: This argument limits the number of concurrent probes sent throughout the scan to 10, speeding it up.

-> -Pn disables host discovery, presuming the host is functioning even if it doesn't reply to probes. This helps scan unresponsive hosts.

-> --top-ports 100: The scan targets the top 100 most commonly used ports to streamline analysis.

SCREENSHOT AFTER EXECUTING THE COMMAND:



```
kali@kali:~$ sudo -s
[sudo] password for kali:
root@kali:/home/kali# nmap -sS -T4 -v -n --max-parallelism 10 -Pn --top-ports 100 142.251.221.84
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-16 04:27 EST
Initiating SYN Stealth Scan at 04:27
Scanning 142.251.221.84 [100 ports]
Discovered open port 80/tcp on 142.251.221.84
Discovered open port 443/tcp on 142.251.221.84
Completed SYN Stealth Scan at 04:27, 3.26s elapsed (100 total ports)
Nmap scan report for 142.251.221.84
Host is up (0.029s latency).
Not shown: 98 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.41 seconds
           Raw packets sent: 200 (8.800KB) | Rcvd: 4 (176B)
root@kali:/home/kali#
```

ANALYSIS OF THE FINDINGS OF THE PORT SCAN:

The next part details the findings of the thorough port scan, providing insight into the individual open ports that were uncovered throughout the evaluation. This in-depth research highlights possible vulnerabilities inherent to these ports, which include things like out-of-date software, configuration oddities, and the availability of exploitable web apps.

In this regard, it is crucial to specify the potential security threats posed by both open and closed ports, including:

PORT 80/TCP (HTTP):

-> HTTP Port-80 is used for HTTP (Hyper Text Transfer Protocol) communication by default.

-> Data transfer protocols, such as Transfer Control Protocol (TCP), are related to this port.

-> Port 80 is widely used for the transmission of online information over HTTP, which poses a security risk. Keep in mind that just because Port 80 is exposed does not mean there is a security hole. Instead, the vulnerability depends on the web server's specific setup and the code it runs.

-> Security holes brought on by using insecure or unpatched versions of web server software. Prioritization should be given to applying security updates in a timely manner to keep the web server software up-to-date.

-> Threats that have been lying in wait due of insecure server-hosted online applications. These apps must be carefully evaluated and fortified to prevent vulnerabilities that might be used by attackers.

PORT 443/TCP (HTTPS):

-> The Hypertext Transfer Protocol Secure (HTTPS) is a protected form of HTTP in which all connections are encrypted before they leave port 443.

-> This port is also linked to the TCP protocol, which establishes an encrypted link between your browser and the websites you visit.

-> Port 443 is far more secure than Port 80, which is the fundamental difference between the two. Data may be sent via a secure connection using port 443, while plain text can be sent via port 80.

-> Problems in SSL/TLS settings that might leave the server open to security breaches. Using modern SSL/TLS protocols and ciphers is crucial to the server's security.

-> Potential security holes introduced by certificate-related problems, such as those caused by incorrectly configured SSL/TLS certificates or the use of self-signed certificates.

TO AVOID POTENTIAL DANGERS, WE SHOULD:

Several practical suggestions are made to lessen the impact of the hazards that have been discovered. Web application error handling, SSL/TLS setup improvements, and software updates are all included in these suggestions;

Web Application Security: If the site contains online apps, they should be coded securely to avoid SQL injection, XSS, and CSRF, which are all too typical web vulnerabilities. Make use of WAFs to further fortify your network's defenses against web-based assaults.

Regular system and software update:

Make that the web server software, operating system, and any third-party apps are kept up-to-date with the latest security patches and upgrades on a regular basis. Existing flaws may be lessened by installing updates promptly.

Education on security measures:

Instruct all personnel and developers responsible for the upkeep of the website on safe coding, password management, and incident response protocols.

Regular Vulnerability scanning:

In order to execute vulnerability scans and security assessments on a regular basis on the Chameleon website, you need establish a periodic timetable. Conducting regular scans may assist in identifying and addressing new vulnerabilities and threats.

--> The enhancement of the security posture of the Chameleon website, as well as the reduction of the risk of security incidents, will result from the consistent implementation of these guidelines. It is vital to do routine monitoring and take preventative actions in order to protect against the ever-evolving dangers that exist in the cybersecurity environment.

FINAL THOUGHTS:

As a result of the port scan, possible security holes in the Chameleon website have been revealed. It is important to keep ports like 80 (HTTP) and 443 (HTTPS) available for online services, but there is always a chance that your web applications might be compromised due to things like out-of-date software or incorrect setups.

The suggested suggestions provide an obvious way to improve the website's security for Chameleon. Common attacks like SQL injection, cross-site scripting (XSS), and Cross-Site Request Forgery (CSRF) may be prevented by adhering to best practices for online application security, such as installing and maintaining up-to-date software and using secure SSL/TLS setups.

The Chameleon website must take measures to prevent these problems from worsening, especially in light of the constantly shifting nature of online threats. Regular security assessments, regular monitoring, and a dedication to best practices will assist to maintaining a safe and resilient online presence. The Chameleon website, its users, and its assets will all be safer from cybercriminals if the suggestions above are implemented.

REFRENCES USED:

1. “blog.netwrix.com,” blog.netwrix.com, 2022. https://blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/

2. “What is port 80 vulnerability?” cbtnuggets.com, 2023. https://www.cbtnuggets.com/blog/technology/networking/http-80-vs-https-443
3. NetworkChunk, “ Nmap tutorial”, YouTube. Jul.09, 2020. Accessed Nov. 14, 2023. [YouTube video]. Available: https://www.youtube.com/watch?v=4t4kBkMsDbQ&t=4s
4. David Bombal, “Stealth scan and Finding vulnerabilities”, YouTube. Mar.12, 2022. Accessed Nov. 14, 2023. [YouTube video]. Available: https://www.youtube.com/watch?v=F2PXe_o7KqM
5. Matesh Linux, “Website scanning using Nmap”, YouTube. May.13, 2022. Accessed Nov. 15, 2023. [YouTube video]. Available: https://www.youtube.com/watch?v=xzWKn_Ddpxo