A green chameleon logo

Description automatically generated

**PORT SCANNING**

​​

**TABLE OF CONTENTS**

1-SUMMARY……………………………………………………………………………………..

2-INTRODUCTION……………………………………………………………………………..

3- TOOLS USED………………………………………………………………………………..

4-SCOPE OF TESTING………………………………………………………………………….

5-RESULTS…………………………………………………………………………………………

6-CONCLUSIONS……………………………………………………………………………….

7-REFERENCES……………………………………………………………………………………

**EXECUTIVE SUMMARY**

The location can also be a local address because the JavaScript code can send a WebSocket request to any address. Businesses may try to open a socket for each request by running them on various local ports. The server can determine whether a port is open by timing how long it takes to receive a response. An active listening port will respond to a request right away, whereas an inactive port will take a lot longer to respond (until timeout). You may ask yourself, what is the purpose of port scanning for businesses? Most companies use port scanning to safeguard their checkout pages. They wish to confirm that the person making the requests is authentic. Businesses will test a number of known ports that are known to be used by trojans or by remotely controlled applications in order to identify compromised hosts. Companies can determine whether a service is safe to allow a user to log in or make a payment by obtaining a risk score for each service on the client host.

**INTRODUCTION**

Finding open ports on a network that might be receiving or sending data is known as port scanning. In order to find vulnerabilities, it can also be used to send packets to particular ports on a host and examine the responses. It is necessary to first compile a list of all active hosts and map those hosts to their IP addresses in order to perform this scanning. A network scan is the first step in this process, which is known as host discovery. Finding the arrangement of IP addresses, hosts, and ports is the aim of port and network scanning in order to accurately identify open or vulnerable server locations and assess security levels. Network and port scanning can both show whether security controls, like a firewall, are in place between the server and user device.

**PROTECTION AGAINST PORT SCANNING**

Until it can be demonstrated that port scanning was done on purpose to violate someone's privacy or gain unauthorised access, it is not a crime. As we mentioned above, it is typically used to strengthen security and safeguard websites. Undoubtedly, port scanning leaves a negative impression on a lot of users, particularly since it occurs without the users' permission. Businesses should, at the absolute least, notify visitors to the website about port scanning and update their privacy and terms and conditions pages. Businesses should be aware that every instance of client-side code, particularly from applications from third and fourth parties that use your website, has the ability to port scan users and perform these actions. In the event that their application or service is compromised, your user environments are exposed, and you won't even be aware that anything has changed.

Reflectiz offers a thorough dashboard of all JavaScript code activity and maps all third- and fourth-party apps that are installed on your website in minute detail. You can identify problems with digital applications instantly and track the data they are accessing and the locations to which they are sending.

**TECHNIQUES OF PORT SCANNING**

There are several techniques for port scanning, depending on the specific goal. It’s important to note that cybercriminals will also choose a specific port scanning technique based on their goal, or attack strategy.

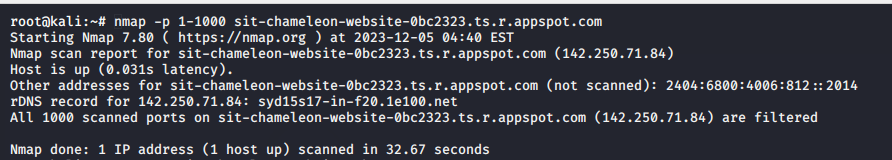
Listed below are a few of the techniques and how they work are as follows-

Ping scans: Ping scans are the most basic type of port scan. A ping is used in a network to check if a network data packet can be sent to an IP address without any problems. Ping scans are automated blasts of multiple internet control message protocol (ICMP) requests sent to various servers in an attempt to elicit responses. IT managers can use this method to troubleshoot or to disable the ping scan by utilising a firewall, which prevents attackers from using pings to locate the network.

SYN or half-open scans: Attackers can use a half-open scan, also known as a SYN (short for synchronise) scan, to find out a port's status without creating a complete connection. This scan only sends a SYN message and doesn’t complete the connection, leaving the target hanging. It’s a quick and sneaky technique aimed at finding potential open ports on target devices.

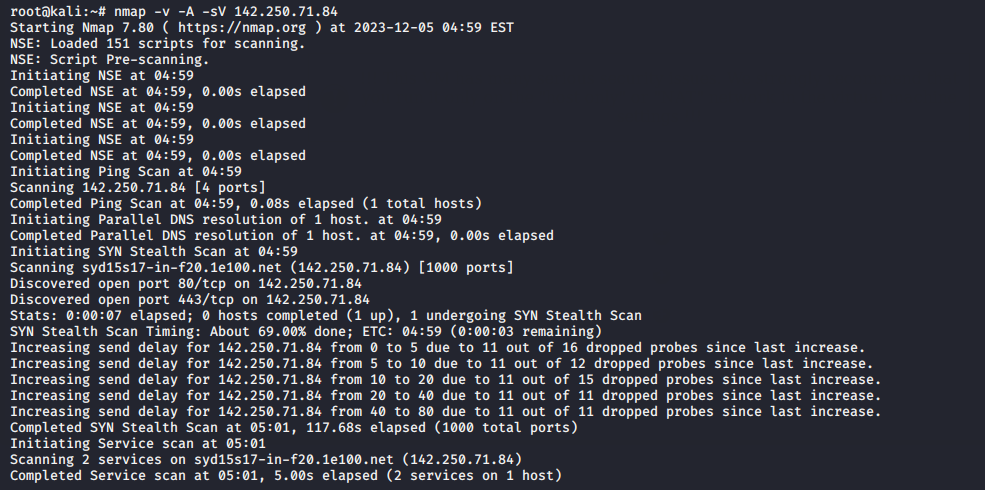
**RESULTS**

For the port scanning I have scanned all the ports which are opened for the chameleon website and here are the results which can be find in the below screenshots , I have used different types of the commands as can be seen in the below screenshots



A computer screen shot of a computer code

Description automatically generated



A screenshot of a computer program

Description automatically generated

**A screen shot of a computer

Description automatically generated**

**CONCLUSION**

In conclusion, TCP was used for the majority of the scans, and TCP SYNs dominated the traffic. Another protocol we observed was UDP, albeit it was not very common. Simple vertical or horizontal scans made up the majority of the scans; vertical scans predominated by a factor of almost two. Every port was scanned at least once, though not many of the probes came from even the most frequently scanned ports. The scan sources were distributed widely, with a preference for heavily populated regions of North America and Europe. While the vertical scans varied, the majority of the horizontal scans were sequential. We noticed a lot of variation in the scan time.

**REFERENCES**

1- www.avast.com. (n.d.). *What is port scanning and how does it work? | Avast*. [online] Available at: https://www.avast.com/en-au/business/resources/what-is-port-scanning#pc.

2- Team, R. (2022). *Port Scanning: What Does it Mean and How Can You Protect Yourself?* [online] Reflectiz. Available at: https://www.reflectiz.com/blog/port-scanning/.

‌