A green chameleon logo

Description automatically generated

**OPEN PORT REPORT**

**TABLE OF CONTENTS**

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

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

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

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

5-RECOMMENDATION OF OPEN PORTS……………………………………………

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

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

**EXECUTIVE SUMMARY**



Definition: On a computer or server, an open port is a particular endpoint or channel that is open for communication. It is frequently connected to the User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) ports.

Port numbers: Port numbers are unique numerical values that are used to identify ports. While registered ports (1024 to 49151) and dynamic or private ports (49152 to 65535) are used for a variety of applications, well-known ports (0 to 1023) are reserved for particular services.

**INTRODUCTION**



An open port is a software-defined value that identifies a network endpoint. Any connection made on a TCP/IP network has a source and destination port that are used with the respective IP addresses to uniquely identify the sender and receiver of every message (packet) sent.

Ports are essential to any TCP/IP-based communication—we simply can’t do without them. Misconfigured ports and port vulnerabilities provide threat actors with a dangerous backdoor into the environment. A strong security posture hinges on understanding how ports are being used and how they are being secured. This counts double when those ports are internet-facing, as they are nearly always in the Cloud. I’ll provide an overview of ports, how they are used, some important risks to be aware of, and how to mitigate port-related cybersecurity risks across your environment.

The majority of people are aware that an IP address is a way to "uniquely" identify a system on a network. Currently, the most widely used IP address format is 192.168.1.1, which consists of four octets separated by full stops. This is a component of IPv4, the fourth version of the protocol. The addressing scheme of IPv6, the subsequent version, is far more extensive and consists of eight 16-bit hexadecimal values separated by colons, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Since IPv6 also uses ports, which we won't cover in this blog post, the following also applies to it.

**TOOLS USED**



Nmap (Network Mapper):

* Description: Nmap is a powerful and versatile open-source tool for network discovery and security auditing. It supports a wide range of scanning techniques and is known for its flexibility and efficiency.
* Features:
* Host discovery
* Port scanning (TCP, UDP)
* Version detection
* Scriptable interactions

Masscan:

* Description: Masscan is an open-source, high-speed port scanner designed for large-scale network scans.
* Features:
* Extremely fast scanning
* Asynchronous scanning
* IPv4 and IPv6 support

**SECURITY RISKS OF OPEN PORTS**



While being essential for enabling networks to work as they do, ports can offer opportunities for would-be attackers.

For example, open ports can contribute toward system identification. Historically, open ports (the default port configuration of a new system installation) offered a fingerprint of ports that could reveal much about the system being investigated. Today, this is less the case, as operating systems default to being tightly locked down at install and non-essential ports only opened as necessary. However, what the services on those necessarily open ports reveal about your system can be surprising.

There are many tools that can scan a target IP address (or range of IP addresses) and report back on ports that are ‘open’, which means that the port has software listening for traffic on it. These tools are easy to use and readily available. Some example port scanners include Nmap, Netcat, Advanced Port Scanner, and many others—including most vulnerability scanners. There are literally thousands of port scanners to choose from, though Nmap, first released in 1997, is undoubtedly the best known. While port scanners are useful tools for IT security practitioners, they also provide valuable information for threat actors.

Below is the output of an Nmap scan against the Nmap’s team test target (scanme.nmap.org). This shows the kind of information you can expect to uncover. While this is a single target, Nmap accepts multiple targets in several formats, including lists and CIDR notation.

**RECOMMENDATION OF OPEN PORTS**

In the chameleon website we have the plenty of open ports in which I have used two of them for the attacks, in my point of view the recommendation of the chameleon website open ports I will suggest that the following things as mentioned below-

**Regularly Scan Network Ports**

We need to execute a process on our clients' networks that looks for potentially harmful open services, like unencrypted legacy ports, so that administrators can disable them or swap them out for a secure version. Every port on every managed device is evaluated once a week to identify which ones need to be restricted because they pose a risk.

**Ports of Access Employing a VPN (Virtual Private Network) for Security**

Your IP address is hidden by a Virtual Private Network (VPN), which routes it through a remote server that is kept up to date and specifically configured by the VPN host. Thus, when you browse the internet using a VPN, the VPN server becomes your data source. This means that the websites you visit and the data you enter are private and unknown to your ISP and other third parties.

A computer screen with white text

Description automatically generated

**Use multi-factor Authentication**

A graphic of a cell phone plus a lock

Description automatically generated

MFA (Multi-factor authentication) is a security mechanism that needs several ways of authentication from distinct categories of credentials to validate a user's identity for a login or other transaction. Multifactor authentication combines two or more separate credentials: what the user knows, such as a password; what the user owns, such as a security token; and what the user is, which is verified using biometric means. Multi-factor authentication (MFA) dramatically aids in the security of an open service. Even if there is a credential leak or a brute-force attempt, the miscellaneous attackers will be faced with an additional code or authentication technique that they cannot bypass.

**Best Practices to Secure Ports and Reduce Threat Exposure**

The more pointed and targeted an attack, the less opportunities to prevent or detect the attack at any stage. Those few markers that may exist are within the purview of the attacker to cleanse.

What can you do to minimize the port-related risks in your environment? Let’s look at best practices for hardening and securing ports.

1. Enumerate and understand your open ports

The first step entails discovery. Identify and list all your open ports, and continuously check for any port-related configuration changes. However, just as importantly, you will need to understand and document all port usage across your environment. This information provides a baseline for port security.

2. Close any port not actively needed

This can be a challenge, as the operation of the system may depend on a potentially vulnerable port being open. If that’s true, then Option #2 is appropriate.

3. Restrict port access to specific source IP addresses (or ranges)

This practice is always applicable and offers the best option when Option #1 isn’t available. Not everyone in your environment needs access to the terminal/console of your critical servers—or any of your servers. Restricting access to only the IP range used by your admins and relevant systems (using the service on that port) will minimize the risk profile for the environment.

If you have remote workers who need access to systems, implement a Secure Remote Access (SRA) solution to get them to those systems. Don’t open the perimeter to allow that access, however confident you might be in your VPN configuration and management skills. It only takes one mistake or a previously unknown vulnerability to lead to a major breach.

**CONCLUSION**



Awareness of Security-Network administrators and security experts need to be aware of open ports in order to recognise potential threats and vulnerabilities. Risk Reduction-By seeing possible vulnerabilities and fixing them before they can be exploited, routinely monitoring and managing open ports helps reduce security risks. Tools for Port Scanning-Nmap, Massan, and other specialised tools make it easier to identify open ports and support security evaluations. But when using such tools, authorisation and ethical considerations are crucial.

REFERENCES

1- www.beyondtrust.com. (n.d.). *What is an Open Port & What are the Security Implications? | BeyondTrust*. [online] Available at: https://www.beyondtrust.com/blog/entry/what-is-an-open-port-what-are-the-security-implications.

‌2- www.youtube.com. (n.d.). *How To Check Open/Close Ports of Any Website Using PowerShell*. [online] Available at: https://youtu.be/QJWkff3\_a3I [Accessed 9 Dec. 2023].

‌3-Pandey, P. (2022). *How to Make Open Ports Secure?* [online] Scaler Topics. Available at: https://www.scaler.com/topics/how-to-make-network-ports-secure/.

‌

‌