**“Port Scanning: The art of information gathering”**

***Table of Contents***

*Introduction………………………………………………………….(1)*

*Port……………………………………………………………………(2-3)*

*Well known ports…………………………………………………….(3-4)*

*Vulnerability Assessment with Port Scanning……………………(4)*

*Citations……………………………………………………………….(5)*

Daniel Rao

Feb 28th, 2021

Vince Skinner

**Port Scanning: The art of information gathering**

**Introduction**

Port scanning is a network type threat. It can be used both by good guys and attackers. The attackers actually use port scanning as a vehicle for reconnaissance. They are constantly trying to figure out how a network might work or how it might look like. While on the other hand, administrators or the people who are actually administering the system, they may actually use port scanning to verify security policies in their move to improve overall security posture. This is

what's called port scanning an internal network from within the company. However there can be people with malicious purposes who just want to get the idea of what services are offered by the company which in other words simply means scanning the ports. This type of scanning often takes place remotely via raw internet to scan all of the ports associated with the particular ip address of that company/organization. In the field of cyber security it is also known as scanning an external network host.

**Port**

A port is basically a 16 bit long address. The idea behind port scanning is to find open ports. Before we dive too much behind the idea of port scanning lets look at what a port? If we define it in simple words, a port actually occurs in the context of tcp/ip which is the standard protocol where all of the internet transactions occur. Within tcp/ip there is a notion called ip address which resides on the network layer of tcp/ip model and this is what's used to reference hosts. Inside the network layer of the tcp/ip model in addition to ip address there is something called a port.

By physical analogy imagine having a house with a physical address which will be more like an ip address, and doors being the ports. There could be several doors in a house, each serving a different purpose. Among which one of the doors may serve as a way to go out, others may serve as a door to go to the garden or inside the garage, Like each door serves different purposes very similar to that each port also serves a very specific purpose.

Now in order to be secure one may have to shut some of the doors and only use the doors that are in constant use. The best practise for any company or organization would also be shutting down the ports that are not in use and only using the ones that are in constant use by the user.

Like many doors available in the house associated with the physical address there are many ports available in a computer or a server which has an ip address and according to wikipedia, “ The registered ports are those from 1024 through 49151. IANA maintains the official list of well known and registered ranges. The dynamic or private ports are those from 49152 through 65535.

**Well known ports**

Some of the most well known ports according to opensource.com are as follows:

|  |  |
| --- | --- |
| Port Number | Usage |
| 20 | File Transfer Protocol (FTP) Data Transfer |
| 21 | File Transfer Protocol (FTP) Command Control |
| 22 | Secure Shell (SSH) |
| 23 | Telnet - Remote login service, unencrypted text messages |
| 25 | Simple Mail Transfer Protocol (SMTP) E-mail Routing |
| 53 | Domain Name System (DNS) service |
| 80 | Hypertext Transfer Protocol (HTTP) used in World Wide Web |
| 110 | Post Office Protocol (POP3) used by e-mail clients to retrieve e-mail from a server |
| 119 | Network News Transfer Protocol (NNTP) |
| 123 | Network Time Protocol (NTP) |
| 143 | Internet Message Access Protocol (IMAP) Management of Digital Mail |
| 161 | Simple Network Management Protocol (SNMP) |
| 194 | Internet Relay Chat (IRC) |
| 443 | HTTP Secure (HTTPS) HTTP over TLS/SSL |

**Vulnerability Assessment with Port Scanning**

If we can find an open port using special tools intended for scanning ports such as nmap, zenmap which is just another tool built on top of nmap that corresponds to a service running on a system and if that service happens to have a vulnerability, an attacker can easily identify the vulnerability and may find a means to exploit it.

The idea is that when we do a port scan we may not try to scan every single port which would be a lot of effort. However, we might cherry pick some of the famous ports or the ports for which we might have an exploit in mind for a particular vulnerability. Like maybe one example of a port that's famously used in attacks is port 1433 which is the port associated typically with SQL server, and SQL server is basically a database service that is run to host a database. An attacker may be able to take advantage of the exploit depending on its version or if it has already been patched.

**Citations**

<https://opensource.com/article/18/10/common-network-ports>

<https://en.wikipedia.org/wiki/Port_(computer_networking)>