What is port scanning?

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

This scanning can't take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan.

The goal behind port and network scanning is to identify the organization of IP addresses, hosts, and ports to properly determine open or vulnerable server locations and diagnose security levels. Both network and port scanning can reveal the presence of security measures in place such as a firewall between the server and the user's device.

After a thorough network scan is complete and a list of active hosts is compiled, port scanning can take place to identify open ports on a network that may enable unauthorized access.

It's important to note that network and port scanning can be used by both IT administrators and cybercriminals to verify or check the security policies of a network and identify vulnerabilities — and in the attackers' case, to exploit any potential weak entry points. In fact, the host discovery element in network scanning is often the first step used by attackers before they execute an attack.

As both scans continue to be used as key tools for attackers, the results of network and port scanning can provide important indications of network security levels for IT administrators trying to keep networks safe from attacks.

What is port scanning?

What are ports and port numbers?

Computer ports are the central docking point for the flow of information from a program or the Internet, to a device or another computer in the network and vice versa. Think of it as the parking spot for data to be exchanged through electronic, software, or programming-related mechanisms.

Port numbers are used for consistency and programming. The port number combined with an IP address form the vital information kept by every Internet Service Provider in order to fulfill requests. Ports range from 0 to 65,536 and basically rank by popularity.

Ports 0 to 1023 are well known port numbers that are designed for Internet use although they can have specialized purposes as well. They are administered by the Internet Assigned Numbers Authority (IANA). These ports are held by top-tier companies like Apple QuickTime, MSN, SQL services, and other prominent organizations. You may recognize some of the more prominent ports and their assigned services:

Port 20 (UDP) holds File Transfer Protocol (FTP) used for data transfer

Port 22 (TCP) holds Secure Shell (SSH) protocol for secure logins, ftp, and port forwarding

Port 53 (UDP) is the Domain Name System (DNS) which translates names to IP addresses

Port 80 (TCP) is the World Wide Web HTTP

Numbers 1024 through 49151 are considered “registered ports” meaning they are registered by software corporations. Ports 49,151 through 65,536 are dynamic and private ports - and can be used by nearly everyone.

What are the protocols used in port scanning?

The general protocols used for port scanning are TCP (transmission control protocol) and UDP (user datagram protocol). They are both data transmission methods for the internet but have different mechanisms.

While TCP is a reliable, two-way connection-based transmission of data that relies on the destination's status in order to complete a successful send, UDP is connectionless and unreliable. Data sent via the UDP protocol is delivered without concern for the destination; therefore, it is not guaranteed that the data will even make it.

Using these two protocols, there are several different techniques for performing port scans.

What are the different port scanning techniques?

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:

Ping scans: The simplest port scans are called ping scans. In a network, a ping is used to verify whether or not a network data packet can be distributed to an IP address without errors. Ping scans are internet control message protocol (ICMP) requests and send out an automated blast of several ICMP requests to different servers to bait responses. IT administrators may use this technique to troubleshoot, or disable the ping scan by using a firewall — which makes it impossible for attackers to find the network through pings.

Half-open or SYN scans: A half-open scan, or SYN (short for synchronize) scan, is a tactic that attackers use to determine the status of a port without establishing a full 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.

XMAS scans: XMAS scans are even quieter and less noticeable by firewalls. For example, FIN packets are usually sent from server or client to terminate a connection after establishing a TCP 3-way handshake and successful transfer of data and this is indicated through a message "no more data is available from the sender." FIN packets often go unnoticed by firewalls because SYN packets are primarily being looked for. For this reason, XMAS scans send packets with all of the flags — including FIN — expecting no response, which would mean the port is open. If the port is closed, a RST response would be received. The XMAS scan rarely shows up in monitoring logs and is simply a sneakier way to learn about a network's protection and firewall.

What type of port scan results can you get from port scanning?

Port scan results reveal the status of the network or server and can be described in one of three categories: open, closed, or filtered.

Open ports: Open ports indicate that the target server or network is actively accepting connections or datagrams and has responded with a packet that indicates it is listening. It also indicates that the service used for the scan (typically TCP or UDP) is in use as well.

Finding open ports is typically the overall goal of port scanning and a victory for a cybercriminal looking for an attack avenue. The challenge for IT administrators is trying to barricade open ports by installing firewalls to protect them without limiting access for legitimate users.

Closed ports: Closed ports indicate that the server or network received the request, but there is no service "listening" on that port. A closed port is still accessible and can be useful in showing that a host is on an IP address. IT administrators should still monitor closed ports as they could change to an open status and potentially create vulnerabilities. IT administrators should consider blocking closed ports with a firewall, where they would then become "filtered" ports.