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.

Filtered ports: Filtered ports indicate that a request packet was sent, but the host did not respond and is not listening. This usually means that a request packet was filtered out and/or blocked by a firewall. If packets do not reach their target location, attackers cannot find out more information. Filtered ports often respond with error messages reading “destination unreachable” or “communication prohibited.”

Port Scanning Techniques

Nmap is one of the most popular open-source port scanning tools available. Nmap provides a number of different port scanning techniques for different scenarios.

Ping Scanner

The simplest port scans are ping scans. A ping is an Internet Control Message Protocol (ICMP) echo request – you are looking for any ICMP replies, which indicates that the target is alive. A ping scan is an automated blast of many ICMP echo requests to different targets to see who responds. Ping scans aren’t technically port scanning techniques, as the best you can get back is that there is a computer on the other end, but it’s related and usually the first task before you do a port scan.

Administrators usually disable ICMP (ping) either on the firewall or on the router for external traffic, and they leave it open inside the network. It’s quick and easy to turn off this functionality and make it impossible to scout the network this way. However, ping is a useful troubleshooting tool, and turning it off makes tracking down network problems a little more difficult.

TCP Half Open

One of the more common and popular port scanning techniques is the TCP half-open port scan, sometimes referred to as an SYN scan. It’s a fast and sneaky scan that tries to find potential open ports on the target computer.

SYN packets request a response from a computer, and an ACK packet is a response. In a typical TCP transaction, there is an SYN, an ACK from the service, and a third ACK confirming message received.

This scan is fast and hard to detect because it never completes the full TCP 3 way-handshake. The scanner sends an SYN message and just notes the SYN-ACK responses. The scanner doesn't complete the connection by sending the final ACK: it leaves the target hanging.

Any SYN-ACK responses are possibly open ports. An RST(reset) response means the port is closed, but there is a live computer here. No responses indicate SYN is filtered on the network. An ICMP (or ping) no response also counts as a filtered response.

TCP half-open scans are the default scan in NMAP.

TCP Connect

This port scanning technique is basically the same as the TCP Half-Open scan, but instead of leaving the target hanging, the port scanner completes the TCP connection.

It's not as popular a technique as the TCP half-open. First, you have to send one more packet per scan, which increases the amount of noise you are making on the network. Second, since you complete the target's connection, you might trip an alarm that the half-open scan wouldn't.

Target systems are more likely to log a full TCP connection, and intrusion detection systems (IDS) are similarly more likely to trigger alarms on several TCP connections from the same host.

The advantage of the TCP connect scan is that a user doesn't need the same level of privileges to run as they do to run the Half-open scan. TCP connect scans use the connection protocols any user needs to have to connect to other systems.

UDP

UDP scans are slower than TCP scans, but there are plenty of exploitable UDP services that attackers can use, DNS exfiltration, for example. Defenders need to protect their UDP ports with the same voracity as their TCP ports.

UDP scans work best when you send a specific payload to the target. For example, if you want to know if a DNS server is up, you would send a DNS request. For other UDP ports, the packet is sent empty. An ICMP unreachable response means the port is closed or filtered. If there is a service running, you might get a UDP response, which means the port is open. No response could mean that the port is open or filtered.

One more logical use of a UDP scan is to send a DNS request to UDP port 53 and see if you get a DNS reply. If you do get a response, you know that there is a DNS server on that computer. A UDP scan can be useful to scout for active services that way, and the Nmap port scanner is preconfigured to send requests for many standard services.

Difference Between TCP and UDP

TCP and UDP are the two most common protocols in use for Internet Protocol (IP) networks. Transmission Control Protocol (TCP) is a nice orderly transaction protocol: TCP sends each packet in order, complete with error checking, verification, and a 3-way handshake to confirm each packet is successful.

UDP doesn't have any error checking but tends to be faster. Live streaming and online video games often use UDP for this reason. UDP is a connectionless protocol, so programs that use UDP just send the data – and if you miss a packet, you will never get it again.

Stealth Scanning

Some port scans are easier to detect than others, so defenders need to know about these TCP flags that allow attackers to make their port scans difficult to detect.

When you send a port scan with a packet and the FIN flag, you send the packet and not expecting a response. If you do get an RST, you can assume that the port is closed. If you get nothing back, that indicates the port is open. Firewalls are looking for SYN packets, so FIN packets slip through undetected.

The X-MAS scan sends a packet with the FIN, URG, and PUSH flags and expects an RST or no response, just like the FIN scan. There isn't much practical use for this scan, but it does make the packet resemble a Christmas tree, so there is that.

You can also send packets with no flags, called a NULL packet, and the response is either an RST or nothing.

The good thing – for the hacker – about these scans is that they don't usually show up in logs. More recent Intrusion Detection Software (IDS) and, of course, WireShark will catch these scans. The bad news is that if the target is a Microsoft OS, you will only see closed ports – but if you do find an open port, you can assume that it's not a Windows machine. The most significant advantage of using these flags is that they can slip past firewalls, which makes the results more reliable.

Additional Scanning Techniques

The scans we discussed are the most common, but this is not an exhaustive list. Here are some more scans and the reasons to run them:

TCP ACK scan: to map firewall rulesets

TCP Window scan: can differentiate open ports from closed ports but only works on a minority of systems

–scanflags: for the advanced user that wants to send their custom TCP flags in a scan, you can do that in Nmap

Port Scanning Tools

1.Nmap

2.Solarwinds Port Scanner

3.Netcat

4.Advanced Port Scanner

5.NetScan Tools

How can cybercriminals use port scanning as an attack method?

According to the SANS Institute, port scanning happens to be one of the most popular tactics used by attackers when searching for a vulnerable server to breach.

These cybercriminals often use port scanning as a preliminary step when targeting networks. They use the port scan to scope out the security levels of various organizations and determine who has a strong firewall and who may have a vulnerable server or network. A number of TCP protocol techniques actually make it possible for attackers to conceal their network location and use “decoy traffic” to perform port scans without revealing any network address to the target.

Attackers probe networks and systems to see how each port will react — whether it’s open, closed, or filtered.

For example, open and closed responses will alert hackers that your network is in fact on the receiving end of the scan. These cybercriminals can then determine your operation's type of operating system and level of security.

As port scanning is an older technique, it requires security changes and up-to-date threat intelligence because protocols and security tools are evolving daily. As a best practice approach, port scan alerts and firewalls should be used to monitor traffic to your ports and ensure malicious attackers do not detect potential opportunities for unauthorized entry into your network.

How to Detect a Port Scan?

There are a few different techniques to detect port scans, which could be attempts to scan your network for vulnerabilities.

One is a dedicated port scan detector software application, like PortSentry or Scanlogd.

Netcat includes port scanning functionality as well as the ability to create a simple chat server or program different packets for testing purposes.

Intrusion detection systems (IDS) are another way to detect port scans. Look for an IDS that uses a wide variety of rules to detect the various kinds of port scans that aren't merely threshold-based.

Why Should You Run a Port Scan?

You should run port scans proactively to detect and close all possible vulnerabilities that attackers might exploit.

Proactive port scanning is a good habit that you should repeat on a regular schedule. Also, review and audit all open ports to verify they are being used correctly and that any applications that do use open ports are secure and protected from known vulnerabilities.

Implications of Running a Port Scan

Here are some caveats to running port scans. Some services or computers might fail from a port scan. This is for internal systems more so than internet-facing systems, but it can happen.

Running port scans without authorization can be considered an aggressive action, and if you are on a shared network, you might scan a system that isn't under your control, which isn't good.

Port scans are a critical part of building a good defense from cyberattacks. Attackers are using port scans, as well. You need to beat them to the punch and close down possible attack vectors and make their lives as difficult as possible.

Protecting the perimeter is only part of the battle, however. You need to protect and monitor your data with the same vigilance you protect and monitor your ports. Varonis Data Security Platform helps you protect your data by building internal barriers to your most sensitive data and then monitoring all activity that could impact that data.