PORT SCANNING

What is a Port Scan?

A **port scan** is a method for determining which ports on a network are open. As ports on a computer are the place where information is sent and received, port scanning is analogous to knocking on doors to see if someone is home. Running a port scan on a network or server reveals which ports are open and listening (receiving information), as well as revealing the presence of security devices such as firewalls that are present between the sender and the target. This technique is known as fingerprinting. It is also valuable for testing network security and the strength of the system's firewall. Due to this functionality, it is also a popular reconnaissance tool for attackers seeking a weak point of access to break into a computer.

Ports vary in their services offered. They are numbered from 0 to 65535, but certain ranges are more frequently used. Ports 0 to 1023 are identified as the "well-known ports" or standard ports and have been assigned services by the Internet Assigned Numbers Authority (IANA). Some of the most prominent ports and their assigned services include:

- Port 20 (udp) – File Transfer Protocol (FTP) for data transfer
- Port 22 (tcp) – Secure Shell (SSH) protocol for secure logins, ftp, and port forwarding
- Port 23 (tcp) – Telnet protocol for unencrypted text commutations
- Port 53 (udp) – Domain Name System (DNS) translates names of all computers on internet to IP addresses
- Port 80 (tcp) – World Wide Web HTTP

There are standard services offered on ports after 1023 as well, and ports that, if open, indicate an infected system due to its popularity with some far-reaching Trojans and viruses.

A port scan sends a carefully prepared packet to each destination port number. The basic techniques that port scanning software is capable of include:

- **Vanilla**– the most basic scan; an attempt to connect to all 65,536 ports one at a time. A vanilla scan is a full connect scan, meaning it sends a SYN flag (request to connect) and upon receiving a SYN-ACK (acknowledgement of connection) response, sends back an ACK flag. This SYN, SYN-ACK, ACK exchange comprises a TCP handshake. Full connect scans are accurate, but very easily detected because full connections are always logged by firewalls.
- **SYN Scan**– Also referred to as a half-open scan, it only sends a SYN, and waits for a SYN-ACK response from the target. If a response is received, the scanner never responds. Since the TCP connection was not completed, the system doesn't log the interaction, but the sender has learned if the port is open or not.
- **XMAS and FIN Scans**– an example of a suite of scans used to gather information without being logged by the target system. In a FIN scan, an unsolicited FIN flag (used normally to end an established session) will be sent to a port. The system's response to this random flag can reveal the state of the port or insight about the firewall. For example, a closed port that receives an unsolicited FIN packet, will respond with a RST (an instantaneous abort) packet, but an open port will ignore it. An XMAS scan simply sends a set

of all the flags, creating a nonsensical interaction. The system's response by can be interpreted to better understand the system's ports and firewall.

- **FTP Bounce Scan**– allows for the sender's location to be disguised by bouncing the packet through an FTP server. This is also designed for the sender to go undetected.
- **Sweep scan**– pings the same port across a number of computers to identify which computers on the network are active. This does not reveal information about the port's state, instead it tells the sender which systems on a network are active. Thus, it can be used as a preliminary scan.

Scans that are developed for the sender to go undetected by a receiving system's log are known as stealth scans and are of particular interest to attackers. Despite its popularity in this area, port scanning is a valuable tool for fingerprinting a network and for a penetration tester to assess the strength of network security.

Port Scanning is the name for the technique used to identify open ports and services available on a network host. It is sometimes utilized by security technicians to audit computers for vulnerabilities, however, it is also used by hackers to target victims. It can be used to send requests to connect to the targeted computers, and then keep track of the ports which appear to be opened, or those that respond to the request.

When a criminal targets a house for a burglary, typically the first thing he or she checks is if there is an open window or door through which access to the home can be gained. A Port scan is similar, only the windows and doors are the ports of the individual's personal computer. While a hacker may not decide to "break in" at that moment, he or she will have determined if easy access is available. Many people feel this activity should be illegal, which it is not, however, due to the fact that the potential attacker is merely checking to see if a possible connection could be made, in most areas, it is not considered a crime. However, if repetitive port scans are made, a denial of service can be created.

Hackers typically utilize port scanning because it is an easy way in which they can quickly discover services they can break into. In some cases, hackers can even open the ports themselves in order to access the targeted computer. Hackers also use port scanners to conduct tests for open ports on Personal Computers that are connected to the web.

Port Sweeping

Port sweeping is regarded by certain systems experts to be different from port scanning. They point out that port scanning is executed through the searching of a single host for open ports. However, they state that port sweeping is executed through the searching of multiple hosts in order to target just one specific open port. While Port scanning and sweeping have legitimate uses with regard to network management, unfortunately, they are used almost as frequently for the purpose of criminal activity.

A Serious Threat

Anytime there are open ports on one's personal computer, there is potential for the loss of data, the occurrence of a virus, and at times, even complete system compromise. It is essential for one to protect his or her virtual files, as new security risks concerning personal computers are discovered every day. Computer protection should be the number one priority for those who use personal computers. Port scanning is considered a serious threat to one's PC, as it can occur without producing any outward signs to the owner that anything dangerous is taking place.

Firewall Protection

Protection from port scanning is often achieved through the use of a firewall. A firewall monitors incoming and outgoing connections through one's personal computer. One technique used by firewall technology is the opening of all the ports at one time. This action stops port scans from returning any ports. This has worked in many situations in the past, however, most experts agree it is best to have all open ports investigated individually. Another approach is to filter all port scans going to one's computer. An individual can also choose to port scan his or her own system, which enables one to see the personal computer through the eyes of a hacker.

Firewalls are the best protection one can invest in with regard to port scanning. Firewalls deny outside access to an individual's personal computer. With this type of protection, a personal computer is essentially hidden from unwelcome visitors and is also protected from a variety of other hacking techniques. With firewall software, an individual is assured that his or her sensitive and personal information remains protected.

In today's age of cyber crimes, identity theft, and the myriad of other criminal activities which can be executed through electronic technology, one should never assume that he or she can be too careful. Most people who have become the victim of cyber theft, or other similar crimes, state they wish they would have paid closer attention to the tools available through which their personal computers could have been made safer, and less vulnerable to attack.