

Ports and Its Security

Ports are another essential asset through which security can be breached. In computer science, ports are of two types - physical ports (which is a physical docking point where other devices connect) and logical ports (which is a well-programmed docking point through which data flows over the internet). Security and its consequences lie in a logical port. In this chapter, you will learn about the different measures that you need to take to protect your system through the use of ports.

DONATE

<https://googleads.g.doubleclick.net>

Latest

Show All

Table of Contents

- # [Understanding Logical Ports](#)
- # [Security of Logical Ports](#)
- # [Risky Ports and Their Attacks](#)

Understanding Logical Ports

In Computer Science, each logical connection is assigned a specific number. It ranges from 0 to 65536 in the case of UDP ports and 0 to 65535 in the case of TCP ports. These are end-points to logical connections that determine which service to use in TCP/IP or UDP. The numbering of logical ports also helps to identify which port it must send traffic to. Whenever a data communication is handled by TCP/IP as client-server architecture, it uses the TCP port 80 (or 443, which is another TCP port for https). The official port numbers are listed and assigned by the Internet Assigned Number Authority (IANA), and they divided these ports into three sub-categories:

- Well-Known Ports (0-1023)
- Registered Ports (1024 - 49,151)
- Dynamic / Private Ports (49,152 - 65,535)

Security of Logical Ports

Every logical port is subject to a threat to a system, but some of the commonly used ports receive a lot of attention from cybercriminals. Cybercriminals use vulnerability scanners and port scanning techniques for identifying opened ports on any system or server. Next, they can identify (from these open ports) what kind of services (HTTP, SMTP, FTP, DNS, SSH, Telnet, or VCN) are running and the kind of system being used by the target victim. Here's the list of potential logical ports that are the targets of cybercriminals.

- 15 Netstat
- 20/21 FTP
- 22 SSH
- 23 Telnet
- 25 SMTP
- 50/51 IPSec
- 53 DNS
- 67/68 BOOTP
- 69 TFTP

- 79/49 TACACS+
- 80 HTTP
- 88 Kerberos
- 110 POP3
- 111 Port Map
- 119 NNTP
- 123 NTP
- 137-139 NetBIOS
- 143 IMAP
- 161 SNMP
- 389 LDAP
- 443 SSL
- 445 SMB
- 500 IPSec/ISAKMP
- 520 RIP
- 546/547 DHCP
- 636 SLDAP
- 1512 WINS
- 1701 L2TP
- 1720 323
- 1723 PPTP
- 1812/13 RADIUS
- 3389 RDP
- 5004/5005 RTP
- 5060/5061 SIP

Risky Ports and Their Attacks

Here are some of the critical ports that are prone to cyber-attacks. Port 21 of TCP helps in connecting an FTP server, which carries a bunch of vulnerabilities such as anonymous authentication, directory traversal and helps in performing an XSS attack. Another port 23 (Telnet Port), is fundamentally unsafe because the data is in unmasked form and remains in plain text. Here, attackers can listen to or scrounge for sensitive data and inject commands (in the form of a Man-in-the-middle (MITM) attack).

The DNS port number 53 acts as an exit route for cybercriminals. Since DNS is rarely monitored and filtered so once the cybercriminal gets all the information required, they can use this port to get out after clearing their logs and tracks. Again, port number 80 (supports HTTP), which received browser traffic, is prone to SQL injections, cross-site scripting (XSS), cross-site request forgeries (CSRF), and buffer overruns.

So, as a security professional, it is essential to detect (by scanning for all opened ports) and close all those ports which are not in use by the server or system to prevent a security breach. Proper and updated firewalls also help check the data packets your system will send and receive over the network. The logical port blocking technique will eventually block those ports that are not used by that particular system.

DONATE

<https://googleads.g.doubleclick.net>

Latest

Show All

Next Chapter : [Network Protocols and Its Security](#) >