Discussion-2 TCP/IP Ports can be easily exploited

Discussion Topic:

TCP/IP Ports can be easily exploited.
Do you think scanning them is helpful?
How would you handle it without becoming intrusive or impacting performance?

My Post:

Hello class,

TCP/IP ports are used by devices and applications on a network to communicate. In other words, they act as a gateway for devices, programs, and networks to broadcast information and communicate (Kolaric, 2024). However, as communication gateways, their open nature makes them vulnerable to exploitation by malicious actors. One potential solution to mitigate this risk is to regularly scan open ports. This post examines the efficiency and feasibility of scanning open TCP/IP ports, that is whether it helps secure them or creates more problems than it solves.

Before exploring port scanning, it is important to understand why TCP/IP ports are vulnerable in the first place. For example:

- Unsecured (legacy) services, protocols, or ports such as 21 (FTP), 23 (Telnet), 110 (POP3), 143 (IMAP), and 161 (SNMPv1 and SNMPv2) are vulnerable because the protocols using these ports do not provide authentication, integrity, or confidentiality (cjs6891, n.d.).
- Attackers often target default ports, that is ports used by services with default configurations such as databases like SQL Server and MySQL (ports 1433, 1434, and 3306), as well as services such as SSH (port 22), and HTTP (port 80). These ports are targeted because they are well-known and widely used as default ports for databases, services, and some applications.
- Even secure protocols such as HTTPS (port 443) are vulnerable to attacks like cross-site scripting (XSS) and SQL injections, which exploit weaknesses that are part of web applications (Techa, 2024).

Attackers use various approaches to exploit open TCP/IP ports' vulnerabilities. Methods such as credential brute-forcing (repeatedly trying to login with different login credentials), spoofing and credential sniffing (impersonating legitimate users to intercept and steal sensitive information), exploiting application vulnerabilities (listening on open ports to gain control of systems or steal data), and denial-of-service (DOS) (flooding open ports with traffic, overwhelming a system) (Murphy, 2023).

With so many potential threats targeting open TCP/IP ports, a potential proactive solution to mitigate this risk is TCP/IP port scanning. TCP/IP port scanning is a technique, a software, that runs a port scan on a network or server to identify which ports are open and listening (receiving information) as well as revealing the location or presence of network security devices, like firewalls (Paloalto, n.d.). This technique is also called fingerprinting. Fingerprinting can help identify open ports and the services running on them, revealing potential suspicious activities. For example, multiple unauthorized access or login attempts and the presence of unknown services. Port scanning can be used to verify that security devices are in place, functioning correctly, and that only authorized ports are open. It can also map active hosts and those hosts to their IP addresses revealing unknown IP addresses and active hosts, as well as detecting unauthorized changes to the network configuration. Therefore, port scanning can be used as a proactive security tool for identifying and addressing security vulnerabilities within a network.

However, if used too aggressively port scanning can interfere with another security system such as Intrusion Detection Systems (IDS) triggering unwanted security alerts. It can also impact network performance by consuming network bandwidth and resources. Thus, it is essential to balance the use of port scanning with the appropriate frequency and scope of the scans. It is also essential to use the appropriate tools and techniques that are best suited to the specific characteristics of the network. Below is a table describing some of those tools and techniques.

Table 1

Tools and Techniques for Port Scanning

Tool/Technique	Description	Benefits/Risks
Nmap	An open-source port scanner with various scan types and options for customization.	Widely used and versatile, but can be detected if not used carefully.
SYN Scanning (-sS)	A scan type that avoids completing TCP connections, reducing the chances of detection.	Less intrusive than other scan types, but may not be as accurate in identifying all open ports.
Masscan	A fast and scalable port scanner designed for scanning large networks.	Efficient for large-scale scans, but requires careful configuration to avoid overwhelming systems.
RustScan	An open-source tool that enhances Nmap by speeding up the scanning process.	Can significantly reduce scan times, but may increase the risk of detection if not used cautiously.
Nessus	A commercial vulnerability scanner that can also perform non-intrusive port scans.	Provides vulnerability assessment capabilities, but can be expensive.
TCP Connect Scans	These scans complete the TCP handshake, making them more reliable but potentially more intrusive.	Easier to implement but may trigger security alerts. Different TCP scan types require different levels of privileges. For example, TCP connect scans require fewer privileges compared to half-open scans.
UDP Scans	These scans are used to identify open UDP ports, which are often used for services like DNS.	Essential for security assessments, but generally slower than TCP scans. While UDP scans are generally slower than TCP scans, they are essential for identifying vulnerabilities in UDP-based services, such as DNS.

Note: Data from NMAP (n.d) and Kost (2024).

To summarize, TCP/IP port scanning is a proactive technique for assessing and improving network security. However, if used too aggressively port scanning can interfere with security systems and impact network performance. Therefore, it is essential to define the appropriate scope and frequency of scans and to select the right tools and techniques that are best suited to the specific characteristics of the network. When used properly port scanning can play a role in mitigating the risks associated with open TCP/IP ports and strengthen the overall security of a network.

-Alex

References:

cjs6891 (n.d.). Cisco CCNA Cyber Ops SECFND 210-250, Section 3: Understanding Common TCP/IP Attacks. *E17_blog*. GitHub. https://cjs6891.github.io/el7_blog/texts/cisco-ccna-cyber-ops-secfnd-3/#:~:text=Examples%20of%20insecure%20services%2C%20protocols,authenticity%2C%20integrity%2C%20and%20confidentiality.

Kolaric, D. (2024, June 5). *Identifying secure and unsecured ports and how to secure them*. All About Security. https://www.all-about-security.de/identifying-secure-and-unsecured-ports-and-how-to-secure-them/

Kost, E. (2024, November 18). *Top 5 Free Open Port Check Tools in 2024 | UpGuard*. https://www.upguard.com/blog/best-open-port-scanners

Murphy, D. (2023, December 11). *Open Port Vulnerabilities: How to Secure Open Ports*. Lepide Blog: A Guide to IT Security, Compliance and IT Operations. https://www.lepide.com/blog/how-to-secure-open-ports-from-vulnerabilities/

NMAP Org. (n.d). *TCP SYN (Stealth) Scan (-sS) | Nmap Network Scanning*. https://nmap.org/book/synscan.html#:~:text=TCP%20SYN%20(Stealth)%20Scan%20(,it%20never%20completes%20TCP%20connections.

Paloalto (n.d.). *What is a Port Scan?* Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan#:~:text=Running%20a%20port%20scan%20on,revealing%20the%20presence%20of%20security&text=Port%20scanning%20plays%20a%20crucial,can%20signal%20potential%20security%20vulnerabilities.

Schrader, D. (2024, September 23). Identifying common open port vulnerabilities in your network. Netwrix. https://blog.netwrix.com/open-ports-vulnerability-list

Techa, M. (2024, November 11). Understanding common ports used in networks for TCP and UDP usage. Netwrix. https://blog.netwrix.com/common-ports