T2022_10 What are port scan attacks, and how can we avoid them? (25th May 2022)

What is port scanning

A port scan is a technique for identifying which ports are open on a network. Port scanning is similar to knocking on doors to determine whether somebody is home, since computer ports are used to transfer and receive information

This technique allows attackers to locate vulnerability that can be exploited to gain access to networks. This poses an issue since critical information can be traversing through the network from these ports.

According to the SANS Institute, port scanning is one of the most common tactics attackers use to locate services hackers can exploit to gain entry into a computer network.

Attackers can get the following information from port scanning:

- What services are available?
- Who is the owner of the services?
- If anonymous logging is permitted,
- What services on the network require authentication?

How Port Scan Attacks Work

When a hacker uses a port scan attack to explore your system, each port will answer in one of three ways: "open," "closed," or "not responding at all." A port that is open, or "listening," will react to a port scan request, telling the hacker that your device is on the other end. A closed port will also respond, but will reject the request

Even a refused request demonstrates that a device is hiding behind the scanned IP address. A firewall usually blocks ports if they do not respond at all. Blocking ports, on the other hand, is against the TCP/IP rules of conduct, therefore your firewall might not block every port on your device. Instead, it will set some ports to "closed," which means the device will still be detected by a scan.

Port Scanning Types

It's critical to understand the various sorts of port scans used by hackers to secure your network against them.

- Vanilla scan is a basic port scanning strategy that tries to connect to all 65,536 ports at the same time.

- SYN scan: Also called a half-open scan, this sends a SYN flag to the target and waits for a SYN-ACK response.
- Ping scans: The simplest port scanning technique is the ping scan. ICMP (internet control message protocol) requests are another name for them. Ping scans conduct a series of ICMP requests to several servers in the hopes of receiving a response.
- Christmas tree scans (XMAS scans) and financial institution scans (FIN scans) are more distinct attack tactics.
- XMAS scans get their name from a series of flags that are switched on within a packet and appear to blink like a Christmas tree when viewed in a protocol analyzer like Wireshark. This type of scan transmits a series of flags that, if answered, can reveal information about the firewall and the state of the ports. A FIN scan involves an attacker sending a FIN flag to a specific port, which is commonly used to end an established session. The attacker can use the system's response to determine the volume of activity and gain information into the organization's firewall usage.
- FTP bounce scan: This approach allows the sender to hide their location by bouncing a packet via an FTP server.
- Sweep scan: This preliminary port scanning technique sends traffic to a port across several computers on a network to identify those that are active. It does not share any information about port activity but informs the sender whether any systems are in use.

How to Protect Yourself from Port Scanning

1. Firewalls: A firewall can prevent unauthorized access to a network. It controls ports and their visibility, as well as detects when a port scan is in progress before shutting it down.

2. TCP wrappers: These enable administrators to permit or deny access to servers based on IP addresses and domain names.

3. Uncover network holes: port scanners can be used to determine other open ports required.

The Guyana National CIRT recommends that users and administrators review these recommendations and implement them where necessary.

References

- *What is a Port Scan?* (2022, May 5). *Retrieved from* Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan

- *What Is A Port Scan? How To Prevent Port Scan Attacks? . Retrieved from* Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-port-scan#:%7E:text=A%20port%20scan%20is%20a,being%20used%20by%20an%20organization.