Sig•Mal

Meeting 3

Port Scanning

- Used by Network Administrators for **NETWORK MAPPING** or **NETWORK SECURITY**

→ Can also be used by hackers to find **EXPLOITS**

→ Extremely popular technique for Discovering Services

Port Scanning +

+ Often the first step for reconnaissance.

→ Process of sending packets to specific ports on host and analyzing the responses to learn about services running.

Types of Port Scans

1. Basic Port Scan → Sending a designated packet to a port
2. TCP Connect → Figures out if the machine is listening on a port (Determines port availability)
3. Strobe Scan → Used by hackers to exploit port. Scanning on a more constricted level and disclosure of the username of the TCP Connection.
4. Stealth Scan → Undetected by networking audit tools and firewalls. However, if it makes a connection it will log an error message. There is no data associated with the connection. (Will however be seen on WireShark)

From: SpamLaws

Port Scanning Responses

1

Open, Accepted:

The computer responds and asks if there is anything it can do for you.

2

Closed, Not Listening:

The computer responds that “This port is currently in use and unavailable at this time.”

3

Filtered, Dropped, Blocked:

The computer doesn’t even bother to respond, it has no time for shenanigans.

VARONIS

5 Basic Port Scanning Techniques

Ping Scan

The simplest port scans are ping scans. You are looking for any ICMP replies, which indicates that the target is alive.

TCP Half Open

One of the more common and popular port scanning techniques is the TCP Half-Open port scan, sometimes referred to as SYN scan.

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.

UDP

UDP is the other half of our "hallway" and some standard services – DNS, SNMP, DHCP for example - use UDP ports instead of TCP ports.

Stealth Scanning

Sometimes a hacker wants to run a port scan that is even quieter and less obvious than the other kinds of scans. TCP includes some flags that allow you to do just that.

VARONIS

LIVE DEMO TIME

Head-to-Head Code Games

Two groups will be competing for a single goal, but will try to outdo each other in the improvements.

Goal: Make a “pimped” out Port Scanner

Rules:

- → Everyone on the team must contribute to the Github
- → When it comes time to present… the leaders can’t. (Must be the members)
- → As far as the code, “free range”. No Rules on how the code is built