Port Scanning

Ryleigh, Jonathan, Brayon, Jayden

What is a port?

- Virtual point where network connections start and end
- Managed by computers OS
- Help differentiate between different kinds of traffic
  - Emails go to a different port than a webpage
- Port scanning is a method of determining open ports on a network & if they are receiving or sending data

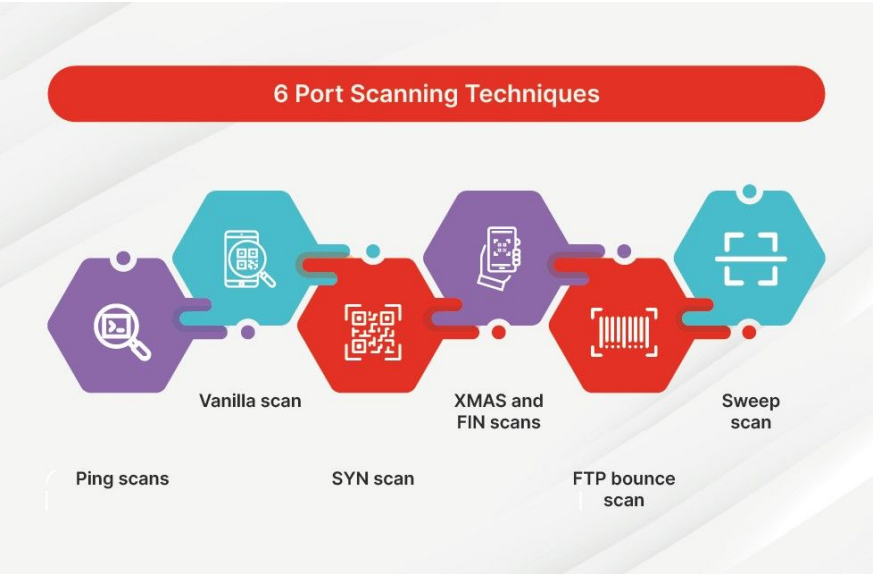
Types of Port Scanning

Many techniques:

- Ping scan, UDP scans, Stealth scans, and so on.
- Horizontal port scanning: scanning a set of IP addresses for a specific port address
- Vertical port scanning: scanning a specific IP address for multiple port addresses

How is it done?

- Port scans can be easily done with many tools
  - Most commonly used is Nmap




```
root@siteduzero:~# nmap 192.168.1.65

Starting Nmap 4.20 ( http://insecure.org ) at 2007-
01-26 00:18 CET
Interesting ports on 192.168.1.65:
Not shown: 1692 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
1234/tcp open  hotline
6112/tcp open  dtspc

Nmap finished: 1 IP address (1 host up) scanned in
5.622 seconds
root@siteduzero:~#
```

Notable Occurrences/Events

- Ebay using port scan to check for running remote access and remote support programs
  - Check for compromised computers making fraudulent purchases or financial transactions
- Ublock Origin extension blocks sites that perform port scans

Mitigation Techniques

- Shut down unused ports
- Firewalls
- TCP wrappers
  - Give administrators the ability to allow or deny access to servers based on IP addresses

References

https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/

https://www.bleepingcomputer.com/news/technology/bleepingcomputers-most-popular-tech-stories-of-2020/

https://www.fortinet.com/resources/cyberglossary/what-is-port-scan

https://www.baeldung.com/cs/port-scanning