Threat assessment of ping sweeps and port scans

Engineering, Computer Security

Threat Assessment of Ping Sweeps and Port Scans Ping sweeps and port scans are two techniques that a malicious computer user such as a hacker can utilize to compromise an Enterprise networks security and gain access to their proprietary data. For example, private email messages can be forwarded to a rogue destination email address: Done by installing a virus program into a user's email client through a discovered active computers open TCP/IP IMAP port (port number 143) that is not being currently used by that user (Clarke, 2008).

The virus then could take advantage of security vulnerabilities in that users email client program and forward emails from that users inbox over to another destination email address without them knowing about it. Therefore, in light of such exploits as just described it is vitally important to address and mitigate the security problem to an Enterprise network from ping sweeps and port scans that can be incurred from outside sources by the use of strong Firewall protections. To better comprehend the danger that ping sweeps and port scans can represent here is a more detailed explanation of each of these techniques.

Ping sweeps First, a ping is a computer network utility tool using the Internet Control Message Protocol (ICMP) to send multiple data packets to a target host device such as server, workstation, or printer to establish whether that host device on a network is actively present (turned on, or active) and able to communicate. If the target host device in question sends back a reply then that device is determined to indeed be active on the network. So therefore, a ping sweep is number of pings that are executed to determine which out of a range of IP addresses map over to live host devices (Rouse, 2005).

To perform this task there are several available software tools to choose from, such as fping, gping, and Nmap for UNIX systems. Also, there is Rhino9’s Pinger software and SolarWinds Ping Sweep for Windows systems. After using such a tool a malicious user can know which host devices on a network are actively available and then proceed to performing a technique called a port scan to try to gain access to those devices. Port Scanning Port scanning is technique used to identify any open or closed Transmission

Control Protocol (TCP) or User Datagram Protocol (UDP) networkcommunicationports or services on a network host device. For example, port number 110 is assigned to Post Office Protocol three (POP3) for email client application communications on a network. There can be up to 65, 000 ports any one computer or host device and any unused open ports as determined by a port scan may allow a malicious user unauthorized access to it. This is akin to an open window in a house whereas a burglar can gain access to it (" Facts about port,").

Also, accessive port scanning can lead to a denial of service (DoS) attack and not allow authorized users to access their data. Finally, there are again several utility tools available to perform port scanning such as Nmap as mentioned previously or SolarWinds Port scanner. Firewall To mitigate the security threat posed by ping sweeps and port scans it is highly recommended that firewall protection on all network hosts devices should be enabled to close any unused ports to protect them from unauthorized access.

Also, is recommended that the use of a firewall server to protect the network from any outside intruders be used as well. In conclusion, ping sweeping and port scanning can threaten the security of a Business Enterprises network and steps to handle security should be implemented to mitigate as much as possible any possibility that any data is kept confidential, that its integrity remains intact, and is always available.