Week 1 Case Study -

Ping Sweeps and Port Scans

Anthony Meunier

DeVry University

SEC 280

Week 1 Case Study - Ping Sweeps and Port Scans

Ping sweeps and port scans are both forms of network probes aimed at finding potential weak spots in a network’s security structure. These probes are not technically intrusions in themselves, but they are however generally used to detect and scan the network in order to find the easiest paths for intrusion methods later on. As you can imagine, even the risk of a network breach is something not to be taken lightly. Possessing the knowledge to protect yourself, and your network, ahead of time is the best method of fighting and preventing malicious attacks in the first place. Let’s explore how these probes operate and what you and your company can do to bolster the network’s security.

Ping sweeps are a simple concept and standard “pings” are even often used in the IT field for troubleshooting purposes. Ping sweeps first establish “communication” with a target server by, of course, pinging them! Usually the way these sweeps are performed is the intruder sends an ICMP ECHO to a group of network machines. The purpose for these pings is to see which machines respond and are “alive.” After this is determined, the intruder can then determine which machines to focus their attacks on. In this two probe process, ping sweeps can be thought of as finding the end-points on a particular network.

Port scans are the second part in this process in which an intruder tries to find an “open-door” among these end-points (detected by the ping sweep). A port scan is conducted on the addresses that the ping sweep received responses from in order to identify any open ports, which then enables the intruder to focus their attacks even more. Ultimately, through use of these two probes an intruder aims to find a way into your network so that they may conduct any number and form of malicious behaviors. Because ping sweeps are commonplace in IT troubleshooting and the fact that port scan programs can be extremely easy to construct and run, it is of the utmost importance that proper security be put in place to secure the network and its assets.

By using even basic forms of network security, such as a firewall, you can help greatly reduce the number of successful intrusions. It’s a bit unreasonable to try and prevent ping sweeps or try only to use ping sweeps as the early warning signs for potential attacks. This is because ping sweeps are not always used maliciously and also because nowadays not all port scanning software performs ping sweeps by default. Therefore the real key in securing the network is doing your best to prevent against easy port detection and access. Let’s discuss some forms of port scans and why knowing how they function can help you secure your own network.

TCP connect is a basic form of port scanning in which the scanner tries to open a TCP connection on every port. If a port is open, then the scanner will be successful in its task. TCP SYN, TCP FIN, and UDP ICMP are other forms of basic port scans that use slightly more specialized attempts at determining which ports are open. Most of these can be prevented by use of a properly configured firewall and use of a Network Intrusion Detection System (NIDS). NIDS is an intrusion detection system that analyzes network traffic for signs of malicious activity and helps determine unauthorized access to a network. When these forms of basic port scans fail, there are always more advanced methods such as OS and version detection and idlescanning. In order to prepare for these types of access attempts, a network administrator can simply implement more stringent firewall rules and even conduct practices such as IP spoofing in order to try and confuse external attackers.

On a final note, being “worried” about malicious attacks that may come from ping sweeps and port scans should not be a concern if you (or your network administrator) simply practice some, or all, of the security practices listed here. Just knowing is half the battle. The other half is implementation and taking action and precaution in the first place. In addition to basic firewall and use of a NIDS, a network can be configured to only enable traffic to access hosts that are needed and automatically deny all other traffic. Most firewalls, and ISPs, can detect unusual activity and thus thresholds can be set to cut off activity when these thresholds are reached (such as many ping requests or port scans in a short period of time). Preparation is the best form of defense, and it is important for any company to have these set in place before a breach can occur.

References

Conklin, A., White, G. B., Cothren, C., Williams, D., & Davis, R. L. (2004). *Principles of Computer Security.* Burr Ridge, Illinois: McGraw-Hill Companies Inc.

McKeag, L. (2010, April 14). Defending yourself against port scanners. Retrieved October 31, 2014, from <http://features.techworld.com/security/490/defending-yourself-against-port-scanners/>

Teo, L. (2000, December 1). Network Probes Explained: Understanding Port Scans and Ping Sweeps. Retrieved October 31, 2014, from <http://www.linuxjournal.com/article/4234?page=0,0>