Ping sweeps and port scans

Technology, Development

PING SWEEPS AND PORT SCANS Affiliation Computer systems have become an important component in organizations, businesses and homes. Unfortunately, computer systems are usually targeted by hackers who want to take advantage of such systems for their own gain or to cause malice. Electronic attacks have become common and pose a major threat to individuals and organizations. Port scanning and ping sweeping are two popular techniques used by hackers to exploit systems. All systems that are connected to the internet are prone to these forms of attack. Although ping sweeping and port scanning are dangerous can lead to data and information loss, they can easily be detected and defended against.

The ping is an important utility of the Internet Control Message Protocol (ICMP) that helps in verifying that a given host is operational (Chen & Davis, 2006). Ping sweeps are used to detect the IP addresses that are being used by live hosts. Ping messages are made up of a pair of ICMP messages referred to as Echo Request and Echo Reply (Chen & Davis, 2006). Unfortunately, ping is usually taken advantage of by attackers to scan a block of IP addresses for a set of active hosts. There are many tools that can perform a ping sweep, and this further makes it easy for attackers to exploit. The major advantage is that ping sweeps can easily be noticed. In addition, it possible for ICMP messages to be blocked, and therefore some organizations might opt to block these messages as a safety precaution. When the administrator wants to carry out a ping sweep, he may enable the ICMP messages temporarily and block them after the ping sweep (Chen & Davis, 2006). Generally, ping sweeps are an old and slower technology, and are rarely used today.

A port scan refers to a series of messages sent by an individual with the intent of breaking into a computer system (Christopher, 2014). The messages are sent to each port one by one. Once the attacker breaks into the computer, he will be able to learn about the computer network services each associated with a port number provided by that computer (Christopher, 2014). The attacker can also learn about the owners of these services and understand whether or not anonymous logins are supported on that computer. A server that is publicly accessible is highly susceptible to port scans. Luckily, port scans are easy to detect. In addition, using the proper tools, the amount of information relating to open services can be limited. One way of limiting this information is the use of TCP Wrappers which allow the administrator greater levels of flexibility either to permit or deny access to the services (Christopher, 2014). Furthermore, PortSentry is another tool offered by Psionic which is capable of detecting requests on selected ports (Christopher, 2014).

Based on the analysis above, it is clear that ping sweeps and port scans are a threat to the security of an organization. However, it is easy for an organization to detect and deal with ping sweeps and port scans. Therefore, these activities are not something to worry about if the right defense strategies and policies are in place. If the organization deploys the necessary tools, dealing with these threats is easy.

In conclusion, port scans and ping sweeps are dangerous processes that can expose an organization to great risk. However, both processes can easily be detected and their threat neutralized. It is important that an organization puts the right policies and defense mechanisms in place to deal with such

threats.

References

Chen, T. M & Davis, C (2006). An Overview of Electronic Attacks. In P. Kannellis, E. Kiountouzis & N. Kolokotronis (Eds.), Digital Crime and Forensic Science in Cyberspace (pp. 1-21). Idea Group Inc.

Christopher, R (2014). Port Scanning Techniques and the Defense Against Them. SANS Institute. Retrieved from http://www. sans. org/reading-room/whitepapers/auditing/port-scanning-techniques-defense-70