

Ping sweeps and port scans case studies examples

[Law](#), [Security](#)



\n[[toc title="Table of Contents"](#)]\n

\n \t

1. [Introduction](#) \n \t
2. [Network Probes – Ping Sweeps and Port Scans](#) \n \t
3. [Protection from Ping Sweeps and Port Scans](#) \n \t
4. [Other Side to Ping Sweeps and Port Scans](#) \n \t
5. [Conclusion](#) \n \t
6. [References](#) \n

\n[/toc]\n \n

Introduction

Technology, though has made it convenient to run better businesses and commercial ventures, it has brought along numerous threats with it. These threats are dangerous and malicious – they could steal data or bring down a network, and mostly occur from external sources. Some notable and common ones of these are the two network probes called Ping Sweeps and Port Scans.

Network Probes – Ping Sweeps and Port Scans

Network probes by themselves cannot be called as intrusions, but they can be used in a malicious manner that could affect a business by stealing or even bring a whole network down thus incapacitating a business. The common probes used for such intentions are Ping Sweeps and Port Scans.

Ping Sweep; is where an intruder sends across a set of ICMP ECHO packets to a set of machines in a network (usually this set is defined by a range of IP

addresses) and tries to see if any one of those systems responds. Usually, the request is sent to one of these IP addresses, one after another, till a response is received. This in turn will intimate the hacker on which machines are active, providing him with a point to focus on while hacking the network. If this machine that has responded happens to be a mail/application server or a database server, then he could through this machine, gain control on the whole network. Thus he could manipulate, delete, steal data or crash the whole setup thus bringing the business to a halt.

Port Scans; are dangerous where the hacker will discover an open port through which he can figure out the list of services running on the machine and hence understand what of those services are vulnerable enough to attack by studying the kind of services and the versions. If this kind of intrusion happened in a retail network then access to the customer passwords, account numbers or credit card information can be stolen and misused. This might cause the organization to lose its value and trust with the market, also customers might end up suffering losses due to their data being misused.

Protection from Ping Sweeps and Port Scans

Protecting one's network from these network probes is not difficult. It is imperative to never expose any important security related information on any machine. Such information comprising of passwords, encryption keys, password hints, SSN and financial information should be stored on encrypted flash drives. The IP addresses in the URLs displayed on websites should be masked. It is important to set up a firewall to protect the network, this way

the intruder will be blocked at the firewall level itself. It is also required to keep the monitoring software updated and hire ethical hackers to observe the network. If these steps are observed one could very well protect the network to a large extent.

Other Side to Ping Sweeps and Port Scans

However, these network probes - Ping Sweeps and Port Scans are not all about intrusion or hacking. These network probes also aid the network security administrators in checking whether the network is secure enough. To achieve this, the administrators should use these probes to scan the network for active machines or open ports that may be accessible from an external source, there are tools available that assist in executing these vulnerability and penetration checks. If these prove to be a risk then precautions must be taken immediately to secure the network.

Conclusion

The best approach here could be that, one should always assume that their network could be vulnerable in some way or the other and regularly work at protecting it. It is highly required for organizations to secure themselves from these attacks for better business continuity management. These measures are very important for the brand value and integrity of the business.

References

Teo, Lawrence. (2000). Network Probes Explained: Understanding Port Scans and Ping Sweeps. Security. Linux Journal, 4234. Retrieved from <http://www.>

<https://assignbuster.com/ping-sweeps-and-port-scans-case-studies-examples/>

linuxjournal.com/article/4234

Branch, Solomon. (2015). What is a Ping Sweep?, wiseGeek. Retrieved from <http://www.wisegeek.com/what-is-a-ping-sweep.htm>

(2014). What is a Port Scan?. Facts About Port Scanning. (n. d.). Retrieved from <http://whatismyipaddress.com/port-scan>