Xmas tree port scan research research paper example

Business

Introduction

Xmas tree scan is a port scanner software application based technique that is designed and used for detecting open ports for a server or host. Opel (2010) argued that, “ Xmas tree scan exploits a subtle loophole in the TCP RFC to differentiate between open and closed ports.” This is accomplished by manipulating the TCP header bits to invoke a response from a remote server or host. If a port is open, an out of state flag segment sent to the TCP port will be discarded while a closed port will return a RST frame response.

The Xmas tree scan has such advantages as: It has high capability of scanning through stateless ACL filters or firewalls usually configured to block access of ports by SYN packets thus preventing any attempts of connection set-up. These packets also have the ability to conduct DoS attacks by capitalizing on the advantage, that they require more processing time by end-hosts and routers unlike other scan packets. Eventually, they are stealthy than even SYN scans i. e. they send single frames to TCP ports without additional packet transfers.

According to Fyodor (2001), “ There is no certain way to defeat port scans.” However, there are various techniques that can be used to protect systems from port scans. These include: closure of all unnecessary services on target systems. Another way is the use of TCP wrappers which give administrators flexibility to deny or permit access to services e. g. based on domain names or IP addresses. Ultimately, is the use of port sentry that is offered by Psionic which detects requests and connections made on the specific ports of a system?

Conclusion

It is therefore, evident that Xmas tree scan is better technique compared to other port scan techniques. Default OS installations should be avoided and test scans done before online use.

References

Fyodor, O. (1997). The Art of Port Scanning. Retrieved from http://www. insecure. org/nmap/nmap_doc. html.

Opel, A. (2005). Design and implantation of a support tool for attack trees internship thesis. Retrieved from http:// www. toengel. net/internship/data/internship-thesis. pdf.

William, S. (1995). Network and Internet Security: Principles and Practice. IEEE Computer Press, ISBN 0-02-425483-0.