Chapter 05 – Port Scanning

Notes

Overview

This chapter presents an overview of port scanning and its different types. You will learn about various tools used for port scanning. The purpose of ping sweeps is also explained. Finally, you will learn about scripting and its role in automating security tasks.

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to:

- Describe port scanning and types of port scans
- Describe port-scanning tools
- Explain what ping sweeps are used for
- Explain how shell scripting is used to automate security tasks

Tips

Introduction to Port Scanning

1. Port scanning is a technique that allows you to find out what services a network host offers. Every service is related to a port. Port scanning programs are automated tools that ping each port on a network computer. If the port answers back, the port scanning program knows that port is alive (open). Open ports represent an invitation for an attack. Attackers can use the list of open ports and what services are related to them and search on the Internet for well-known vulnerabilities associated with those services.

Tip	SuperScan is a powerful free port scanning tool available at: http://www.sofotex.com/SuperScan-download_L14815.html.

2. Information port scanning programs report includes:
   a. Open ports
   b. Closed ports
   c. Filtered ports
   d. Best-guess running OS

Types of Port Scans

1. The main characteristics of various types of port scans, include:
   a. SYN scan: Stealthy scan
   b. Connect scan: Completes the three-way handshake
   c. NULL scan: Packet flags are turned off
   d. XMAS scan: FIN, PSH and URG flags are set
   e. ACK scan: Used to get past a firewall
   f. FIN scan: Closed port responds with an RST packet
   g. UDP scan: Closed port responds with ICMP “Port Unreachable” message

Using Port Scanning Tools

Nmap

1. Originally written for *Phrack* magazine in 1997, Nmap has evolved to become one of the most popular port scanning tools. Nmap is an open source tool; therefore, it is common to encounter new features that have been suggested by users. Although you should become proficient using the Nmap command, there is also a GUI front end called Zenmap for those who prefer GUI tools.

2. Activities 5-1 and 5-2 provide guidelines for using the Nmap command. Figure 5-2 shows the Nmap help screen.

Tip	Find the Nmap main pages at: http://www.insecure.org/nmap/data/nmap_manpage.html.

Nessus and OpenVAS (or Greenbone Security Assistant)

1. Security testers should also investigate Nessus, a tool first released in 1998. Although Nessus is no longer under the GPL license, as most open-source software is, it is still available for download.

2. OpenVAS is an open-source fork of Nessus. OpenVAS is now branded as Greenbone Security Assistant. OpenVAS functions much like a database server, performing complex queries while the client interfaces with the server to simplify reporting and configuration.. An OpenVAS plug-in is a security test program (script) that can be selected from the client interface.

Tip	Download Nessus plug-ins from http://cgi.nessus.org/plugins/.

Conducting Ping Sweeps

1. Port scanners can be used to conduct ping sweeps of a large network to identify which IP addresses belong to active hosts. Ping sweeps sends ICMP Echo Requests messages to all IP addresses within the range. An active host normally responds to this request with an ICMP Echo Reply, indicating that it is alive. Several problems are associated with this technique. For example, a computer might be shut down at the time of the sweep and unable to respond to any request. Another problem is that many network administrators configure network nodes not to respond ICMP Echo Requests. Finally, firewalls that filter ICMP traffic can affect ping sweeps.

Fping

1. See Figures 5-5 and 5-6 for the use of Fping, a command-line tool that allows you to ping multiple IP addresses simultaneously. Fping can accept a range of IP addresses entered at a command prompt, or you can create a file containing multiple IP addresses and use it as input for the Fping command.

Hping

1. Hping for ping sweeping. It is important to note that Hping allows users to bypass filtering devices. This characteristic makes Hping a powerful tool; therefore, every security professional should know how to use this tool.

2. Security professionals should spend some time learning and understanding the different parameters offered by Hping.

Crafting IP Packets

1. Understand the advantages of crafting packets when trying to find out information about a network host and its running services. Packets contain fields for source IP addresses, destination IP addresses, and flags. You can craft any type of packet you like using tools like Fping and Hping.

Understanding Scripting

1. A script is a customized computer program that automates otherwise time consuming tasks. This section will explore some basics about scripting.

Scripting Basics

1. Scripting is similar to DOS batch programming. A script or batch file is a text file containing a multiple commands that can be executed by just providing the name of the script (or batch) file. Good candidates for scripting are repetitive tasks involving several commands.

Tip	Check out http://www.freeos.com/guides/lsst/ for a Linux shell scripting tutorial.

Additional Resources

1. Understanding the ICMP Protocol (Part I):
   http://www.windowsnetworking.com/articles_tutorials/Understanding-ICMP-Protocol-Part1.html

2. Understanding the ICMP Protocol (Part II):
   http://www.windowsnetworking.com/articles_tutorials/Understanding-ICMP-Protocol-Part2.html

3. Nessus Official Site:
   https://www.tenable.com/products/nessus-vulnerability-scanner

4. Security Analysis Tool for Analyzing Networks (SATAN):
   http://www.porcupine.org/satan/

5. Mastering the VI Editor:
   http://www.cs.uofs.edu/~contest/mastering_vi_editor.htm

Key Terms

- **closed ports**
- **filtered ports**
- **Fping**
- **Hping**
- **Nessus**
- **Nmap**
- **open ports**
- **OpenVAS**
- **ping sweep**
- **port scanning**