Chapter 06 – Enumeration

Notes

Overview

This chapter describes the process of enumeration. Enumeration involves connecting to a system and obtaining information about users, passwords, and shared resources. You will learn what tools can be used to enumerate Windows systems. Finally, this chapter presents tools to enumerate *nix OS targets.

Chapter Objectives

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

- Describe the enumeration step of security testing
- Enumerate Windows OS targets
- Enumerate *nix OS targets

Tips

Introduction to Enumeration

1. Enumeration is the next step after port scanning. It involves connecting to a system, not just identifying that a system is present on the network. Enumeration attempts to recover information about the following:
   a. Resources or shares on the network
   b. Network topology and architecture
   c. User names or groups assigned on the network
   d. Information about users and recent logon times

2. The process of enumeration. You start by port scanning and footprinting a system to determine what type of OS it is using. Then you start a more intrusive process (enumeration) in which you try to exploit your knowledge of the system's OS to gain access to it.

3. Several enumeration tools are available for any OS. Usually security testers are proficient in installing and working with tools on Windows and Linux environments. Learn how to install applications on Linux systems. See Activity 6-1 for an example of how to install and use NBTscan on a Linux machine.

Tip	Almost all Linux distributions have a GUI tool that allows users to install applications graphically.

Enumerating Windows Operating Systems

1. When enumerating an OS, it is important to know its history because attacks for older versions of the OS may still apply to newer versions. See Table 6-1 for the history of the Windows OSs.

NetBIOS Basics

1. The Network Basic Input Output System (NetBIOS) is a Windows programming interface that allows computers to communicate over a LAN. It is commonly used to share files and printers.

2. NetBIOS names: When you assign a name to a Windows system, you are assigning it a NetBIOS name. NetBIOS names consist of 16 characters, where the last character is reserved for a hexadecimal number (00 to FF) that identifies the type of service running on that computer. NetBIOS names must be unique on a network. See Table 6-2 for the NetBIOS names and suffixes associated with the last character of a NetBIOS name.

Tip	Read http://www.microsoft.com/technet/security/bulletin/MS03-034.mspx for an example of a NetBIOS vulnerability.

NetBIOS Null Sessions

1. One of the biggest vulnerabilities of NetBIOS systems is a null session, which is an unauthenticated connection to a Windows computer that uses no logon and password values. This vulnerability has been around for more than a decade and is still present in Windows XP.

NetBIOS Enumeration Tools

1. The Nbtstat command is a powerful enumeration tool included with Windows. This command displays the NetBIOS table associated with a network host.

2. The Net view command is also included with Windows. The Net view command shows whether there are any shared resources on a computer or server on a network.

3. See Activity 6-2 for the use of these enumeration tools and also the Net use command, which allows a user to connect to a computer with shared folders or files.

Additional Enumeration Tools

1. Additional enumeration tools such as DumpSec, Hyena, Nessus, and OpenVAS (Greenbone Security Assistant).

2. See Activity 6-3 for Windows enumeration tools included with Kali Linux.

DumpSec

1. DumpSec is another powerful enumeration tool for Windows systems. DumpSec is produced by Foundstone, Inc. and allows you to connect to a server and download (or “dump”) information such as:
    a. Permissions for shares
    b. Permissions for printers
    c. Permissions for the Registry
    d. Users in column or table format
    e. Policies
    f. Rights
    g. Services

Hyena

1. Hyena is an excellent GUI product for managing and securing Windows OSs. With this tool you can easily see shares and logon names for Windows servers and domain controllers. In addition, Hyena display a graphical representation of the following areas:
    a. Microsoft Terminal Services
    b. Microsoft Windows Network
    c. Web Client Network
    d. Find User/Group

Nessus and OpenVAS (aka Greenbone Security Assistant)

1. OpenVAS is an open-source descendent of Nessus. It is a popular tool for identifying vulnerabilities.

2. The latest version of Nessus Server and Client can run on Windows, Mac OS X, FreeBSD, and most Linux distributions. It is a handy tool when enumerating different OSs on a large network.

Tip	Visit http://www.nessus.org, the official Nessus Web site.

Enumerating the *nix Operating System

1. This section covers enumeration tools for UNIX systems and a few of the more popular variations of the UNIX OS.

*NIX Enumeration

1. The Simple Network Management Protocol (SNMP) network management service enables remote administration and can run on both Windows and *nix, but we focus on *nix.

2. SNMPWalk is a tool useful in enumerating hosts running SNMP with default configuration.

3. Nessus is another important *nix enumeration tool. See Figure 6-15 for its ability to assess vulnerabilities.

4. The Finger utility is a useful enumeration tool for security testers and hackers to find out who's logged in to a *nix system. The Finger daemon (fingerd) listens on TCP port 79.

Tip	See http://www.computerhope.com/unix/ufinger.htm for more information on the Finger command.

Additional Resources

1. Nessus Client: http://www.nessus.org/download/?product=NessusClient
2. NetBIOS Enumeration Tools: http://www.cotse.com/tools/netbios.htm
3. Top 100 Network Security Tools: http://www.insecure.org/tools.html
4. An Overview of NetBIOS: https://technet.microsoft.com/en-us/library/cc940063.aspx
5. Oscanner: An Oracle Enumeration tool: http://www.securityfocus.com/tools/3588

Key Terms

- **enum4linux**
- **enumeration**
- **Network Basic Input/Output System (NetBIOS)**
- **null session**
- **Simple Network Management Protocol (SNMP)**