Graduate Program in Information Science and Telecommunications and Networking
School of Information Sciences
University of Pittsburgh

TEL2821/IS2150: INTRODUCTION TO SECURITY
Lab 2: Forensics & Port Re-direction

Version 1.2, Last Edited: September 24, 2007
contact: Saubhagya Joshi {srjoshi at mail.sis.pitt.edu}

Group Members: _____

_____

_____

_____

Date of Experiment: _____

Graduate Program in Information Science and Telecommunications and Networking
School of Information Sciences
University of Pittsburgh

Part I: Objective

The objective of this laboratory exercise is twofold:

1. Introduce you to some of the tools and techniques used for forensic analysis.
2. Demonstrate some of the mechanisms used by malicious attackers as well as forensic experts to disrupt computer networks and manipulate information access.

This lab session will cover data storage and access, bypassing filtered [blocked] ports, reviewing Internet activity, and the use of steganography. Open-source forensic tools will be introduced and demonstrated for each exercise.

The lab has been setup for all of the exercises and the required executables are available in the lab machines. Instructions are available throughout the lab handout.

Part II: Equipment/Software

Most of the tools used for this lab exercise is freely available for non-commercial testing purposes and open-source software, either freeware or shareware. All the executables required for the lab is available in the lab or as temporary download as a zip-compressed file at: http://www.sis.pitt.edu/~srjoshi/public/d/lab2.zip

The zip-compressed file contains three folders: (1) Data, which contains all the original data you need for the lab exercises, (2) Exercises, which contains all of the four exercises in this lab, and, (3) Installers, which contains all the executables you will need for completing the exercises (Please make sure your system has a text editor like Notepad. Also you need to be able to access the command prompt).

Note that Exercise 1 has parts that use different executables for hex editor and hash function, and hence, different folders. Also, any data that needs to be manipulated are available within the respective exercise folders. If at any point, you corrupt the working data, or you need to re-do the exercises, you can copy fresh copies of the data files from the "Data" folder.

Windows Vista PCs are provided for the purposes of the lab. The access accounts and passwords are given on the screen. Some of the exercises use GUI, but some use the command line interface. When the command line is required, a shortcut to the command prompt is given in the exercise folder.

The executables that are used in this lab exercise are as follows:

Hidden Files:

- XVI32 hex editor (Shareware renamed to hex.exe for the lab purposes)
- "fciv.exe" is a ***File Checksum Integrity Verifier*** from Microsoft.
- Text editor (Notepad is good enough)
- Data files: "sol.exe" and "sol.modified.exe"

Graduate Program in Information Science and Telecommunications and Networking
School of Information Sciences
University of Pittsburgh

Port Redirection:

- Quick 'n Easy FTP Server (Freeware download from http://www.pablovandermeer.nl)
- FPIPE (Freeware download from http://www.foundstone.com)
- Batch executable file: "checkPort.bat" used to display relevant port information.
- User database file for the FTP server: "users.xml"

IE Activity analysis:

- Pasco (Freeware download from http://www.foundstone.com)
- Galleta (Freeware download from http://www.foundstone.com)
- Internet Explorer cache file (index.dat)
- Internet Explorer cookie files

Steganography:

- JPHS (Jpeg Hide and Seek) v0.5 (Freeware download from www.stegoarchive.com)
- Text editor (i.e. Notepad)
- Image file in *jpeg* format: "KaalBhairava.jpg"

Part III: Exercises

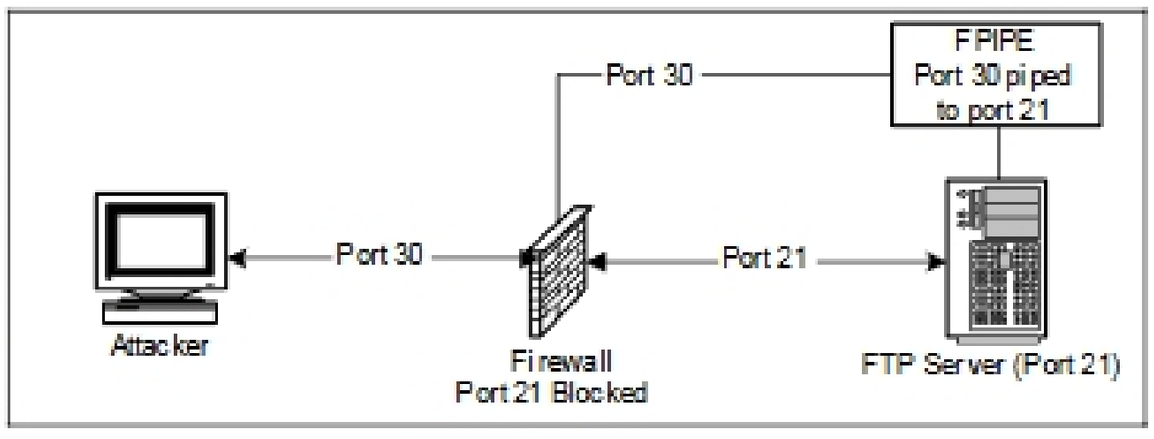
You can do the following exercises either in laboratory in the Windows Vista machines, or re-create the exercise environment in any other Windows 2000 (or later) environment of your choice. Instructions are provided in Part IV: Appendix A. After you complete all the exercises, make sure you roll back to the original state. Refer Part IV: Appendix B.

Exercise 1: ***Port Redirection***

Objective

The purpose of this lab is to demonstrate how an attacker could exploit a machine and obtain access to a server with a filtered port by piping another unfiltered port. Because of sophisticated Trojans, it could be hard for a virus detection program to detect the problem. Because of that, a port scanner/listener must be used to determine if/what ports are actively carrying traffic.

Scenario



Imagine that an IT department has an FTP server on an IBM server that they use to share source code between other departments within the organization in various locations throughout the US on the same LAN/WAN. By default, the information security department blocks certain known ports from being exposed to the internet through a firewall. Some of these ports include the well known 21, 23, 80, 8080, etc.