4.6.1

Microsoft Port Reporter

Port Reporter (PortRptr.exe)

Windows

June 2008

Laboratory Overview

Objective

At the end of this lab students will be able to use Microsoft Port Reporter and understand what TCP and UDP ports are in use

as well as what processes on the OS are using them and also which user account has them in use.

Information for Laboratory

A. Students will install Microsoft Port Reporter
B. Students will test and see what ports are in use on a host
C. Students will use the Port Reporter to see what vulnerabilities, if any, exist on a system.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Instructor Preparation

Before class, the instructor or a lab assistant will ensure that the computers have internet access and have Microsoft IE. An instructor may wish to have some services running on the host prior to this lab such as a TFTP service.

Estimated Completion Time

30 Minutes

TCP/UDP Ports

TCP and UDP ports are logical doors used on computers to send and receive information. Various application programs and services use these doors to pass information back and forth as needed. The status of a port can be in one of several different states such as closed, listening or established.

Ports that are open, or listening, can pose a security threat on a host system. If a system is hijacked, it may have sereptiously opened up some ports that are unknown to the user. These can then be exploited to load illegitimate programs to hijack the host.

Microsoft Port Reporter

The Port Reporter tool logs TCP and UDP port activity. The tool is a small program that runs as a service on a computer that is running Windows Server 2003, Windows XP, or Windows 2000.

On Windows Server 2003 and on Windows XP-based computers, the service can log the following information:

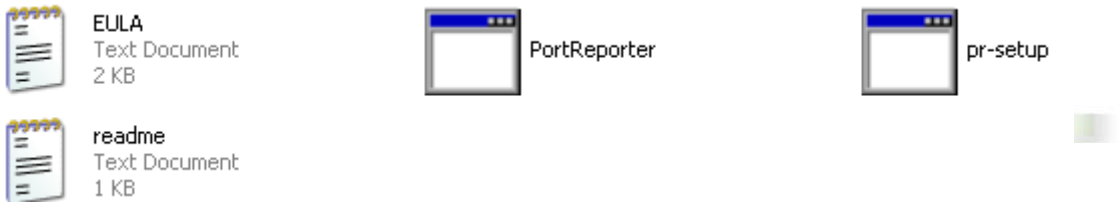
- The ports that are used
- The processes that use the port
- Whether a process is a service
- The modules that a process loaded
- The user accounts that run a process

Step I:
Download and install the Microsoft Port Reporter tool. NOTE: Your instructor may have already installed this tool on the host system. The tool can be downloaded from Microsoft at:

http://www.microsoft.com/downloads/details.aspx?familyid=69ba779b-bae9-4243-b9d6-63e62b4bcd2e&displaylang=en

If you need to install it, unzip the PortRptr windows Cabinet file to a directory that your instructor has specified.

Navigate to that directory and you should see 4 files. A screen shot is shown below:



Click on the readme text file and you will see a link to the support page of Microsoft explaining about PortReporter and how to setup on the host. Instructions from this link are shown below:

Install the Port Reporter service

When you run the Setup program (Pr-Setup.exe) to install Port Reporter, the Setup program performs the following operations:

- Adds the following registry subkey to the Windows registry:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\PortReporter

  The Port Reporter service requires this registry key to log entries to the application event log on the computer.

- Installs the Port Reporter service.

  The Setup program creates a service object for the Port Reporter tool and then adds the object to the Service Control Manager database.

Step 2: Install the Port Reporter service to the default location

By default, the Port Reporter service is installed to the following folder on the hard disk:
drive:\Program Files\PortReporter

To install the Port Reporter service to the default location:

1. Log on to the computer as a member of the local administrators group.

2. Quit all programs that are running on the computer, including the Services tool and Event Viewer in Administrative Tools.

3. Double-click **Pr-Setup.exe** to run the Setup program.

4. When you are prompted to install the Port Reporter tool to the Program Files folder, press Y.

   After you press Y, the Setup program creates a subfolder named PortReporter in the Program Files folder. Portreporter.exe is copied to the subfolder and is registered as a service in Service Control Manager.

After installing you will see the following screen shown below:

PR-Setup will install Port Reporter in the following location on this system:

C:\Program Files\PortReporter

Do you want to install Port Reporter? (Y/N)y

Creating PortReporter directory...completed successfully

Copying PortReporter.exe to target directory...completed successfully

Creating service...completed successfully

Creating registry key and values...completed successfully

PR-Setup has successfully installed the Port Reporter service
The service is currently stopped and set to manual startup type

Please use the services applet (Administrative Tools) in the control panel to configure and start the Port Reporter service

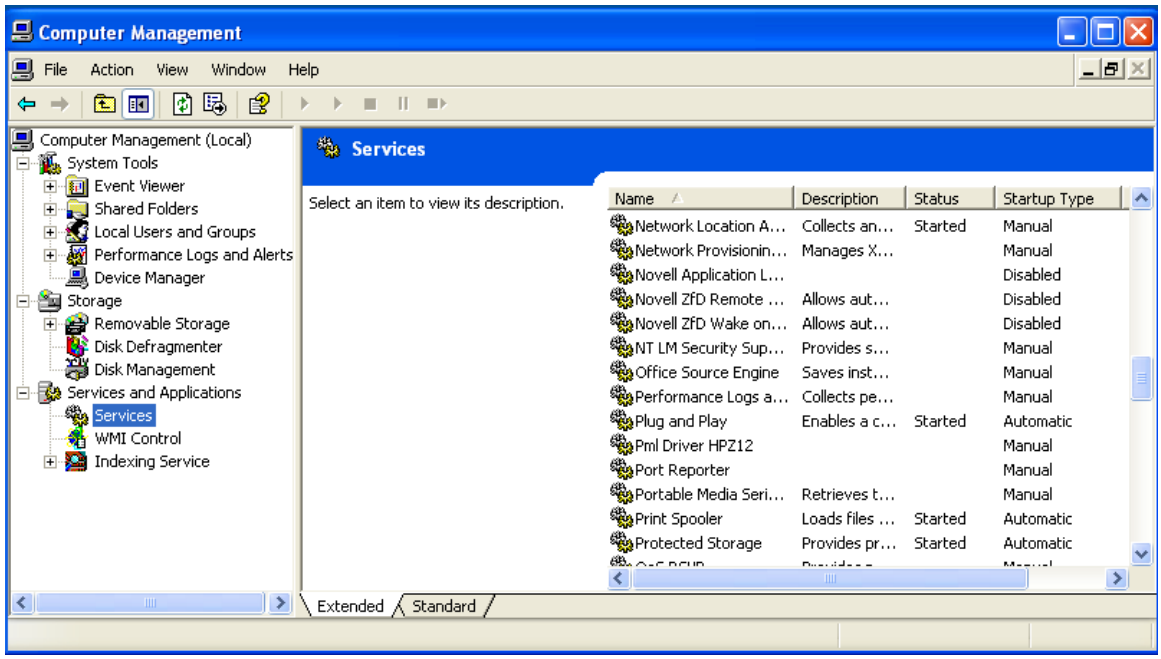
press any key to exit setup

Step 3:
You now have to start up the service. To configure and start the PortReporter service you must do the following steps:

To verify that the Port Reporter service installed successfully and to start the service, follow these steps:

1. Click **Start**, right-click **My Computer**, and then click **Manage**.
2. Expand **Services and Applications**, and then expand **Services**.
3. In the right pane, verify that the Port Reporter service is listed.

   A screen shot of this is shown below:



4. To start the service, double-click the service name, and then click to select the **Start** button. Click **OK**.

   The Port Reporter service will create a log entry in the application log

that indicates that it is started.

By default, the startup type for the Port Reporter service is set to use the **Manual** setting. If you want the service to start automatically when Windows starts, set the startup type to use the **Automatic** setting.

By default, the Port Reporter service uses the Local System account to log on to the computer. By using the Local System account, the Port Reporter service can gather details about processes that the administrator account or other user accounts do not have access to. Because of this, Microsoft recommends that you do not modify this setting.

PortReporter is now logging TCP/UDP port activity to its log files. Information on location and information contained within the log files is shown below.

Location of log files

By default, the Port Reporter tool tries to create the log files in the following folder: %systemroot%\System32\LogFiles\PortReporter
If this folder does not already exist, the folder is created for you. -ld

Size of log files

By default, the Port Reporter service continues to write to the log files until the log files reach 5 megabytes (MB). After the log files reach 5 MB, a new log file is created.

Interpret Port Reporter log files

When the Port Reporter service starts, the following log files are created:

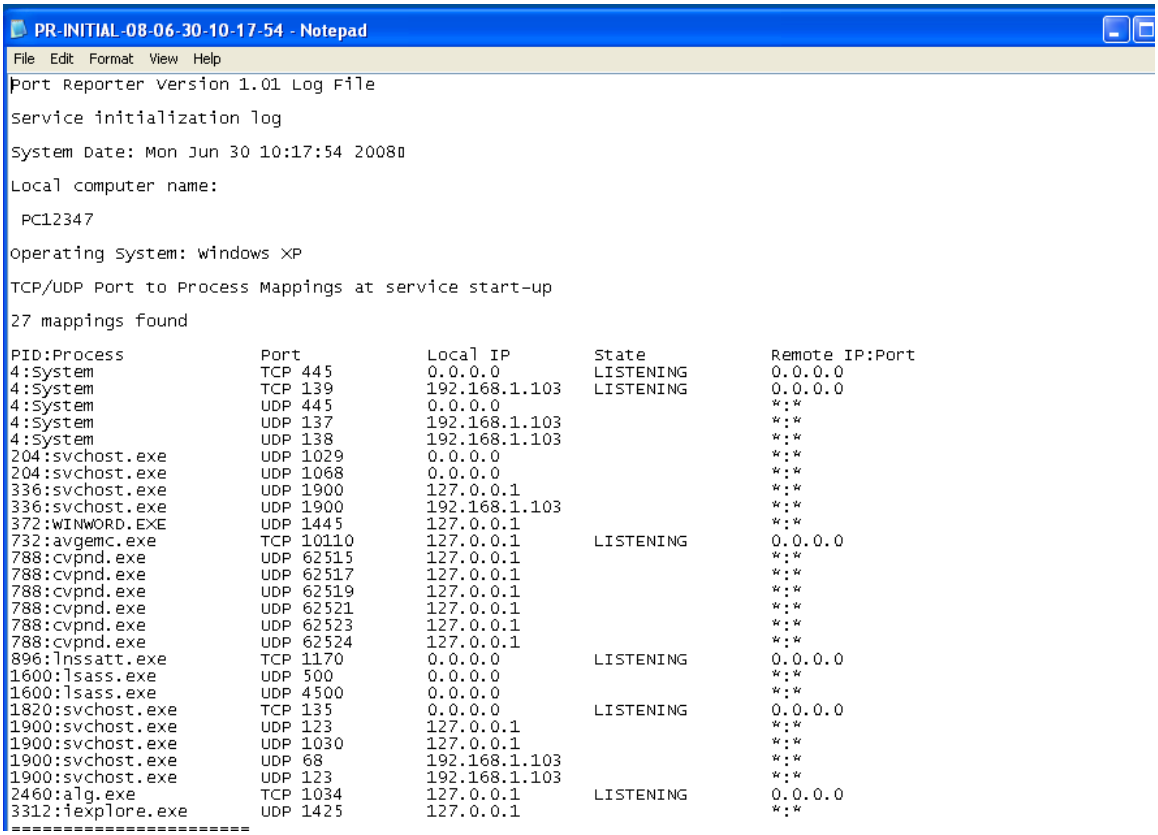
- PR-INITIAL-*.log
- PR-PORTS-*.log
- PR-PIDS-*.log

The name of each log file uses the date and the time (in 24-hour format) when the file was created. The format of the date and time stamp is year-month-day-hour-minute-second. For example, the following three files were created January 24, 2004, at 8:49:30 A.M.:

- PR-INITIAL-04-01-24-8-49-30.log
- PR-PORTS-04-01-24-8-49-30.log
- PR-PIDS-04-01-24-8-49-30.log

The PR-INITIAL log file

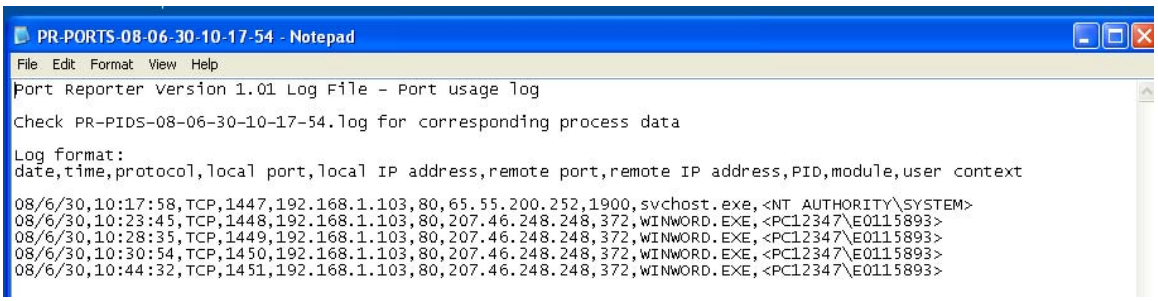
The PR-INITIAL log file contains data that the Port Reporter service collects about the ports, processes, and modules that run on the computer when the Port Reporter service is started. The user context that each process is running under is also logged. The following screen shots are a partial example of the contents of a PR-INITIAL log file on a Windows XP-based computer that was created when the Port Reporter service started:



```
=====================================================

Process ID: 4 (System)

System Process

PID     Port            Local IP        State           Remote IP:Port
4       TCP 445         0.0.0.0         LISTENING       0.0.0.0
4       TCP 139         192.168.1.103   LISTENING       0.0.0.0
4       UDP 445         0.0.0.0                         *:*
4       UDP 137         192.168.1.103                   *:*
4       UDP 138         192.168.1.103                   *:*

Port Statistics

TCP mappings: 2
UDP mappings: 3

TCP ports in a LISTENING state:         2 = 100.00%


Could not access module information for this process

=====================================================

Process ID: 1308 (smss.exe)

User context: NT AUTHORITY\SYSTEM

Process doesn't appear to be a service


Port Statistics

TCP mappings: 0
UDP mappings: 0


Loaded modules:
\SystemRoot\System32\smss.exe (0x48580000)

C:\WINDOWS\system32\ntdll.dll (0x7C900000)
```

The PR-PORTS log file

The PR-PORTS log file contains summary data about TCP and UDP port activity on the computer. The data is listed by using a comma-separated value (csv) format as follows: date,time,protocol,local port,local IP address,remote port,remote IP address,PID,module,user context. A sample is shown below from an XP system



The PR-PIDS log file
The PR-PIDS log file contains detailed information about ports, processes, related modules, and the user account the process uses to run.

Step 4:
Locate your log files, open them up and take a screen shot of each one and save to a Word file. Make sure you put your name within the document. Print this off for your instructor.

Step 5: Experimentation
Stop the PortReporter service on your PC. Startup a service such as TinyWeb server and/or a TFTP service. Startup the PortReporter service again and analyze the results.

Analysis

1) In what context can you see using the Microsoft PortReporter tool?
2) What value could this tool be in a business/IT security setting? How would you utilize this tool?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

Appendix

This lab was performed using Microsoft PortReporter Version 1.01

The host operating system was Microsoft Windows XP Professional SP2.