Exercise 3
IP Enumeration Techniques

Windows 2000 Machines.

wiz.exe.
Many programs come in .zip format. Windows 2000 does not have a native unzip utility. The program wiz.exe can be used to uncompress these files. To install it, proceed as follows.

1. Create a directory called wiz.
2. Copy the file wiz502xN.exe to this directory.
3. Run the program, and install the files in the wiz directory.
4. To unzip a file, use the program wiz.exe that now resides in the wiz directory.

SuperScan 4.0

1. Create the directory SuperScan.
2. Copy the file superscan4.zip to this directory.
3. Use wiz.exe (above) to extract the files to this directory.
4. To run the program, use the program SuperScan4.exe in this directory.

Prosolve Winscan 2.0

1. Copy the file winscan2.exe to a temporary directory.
2. Run the program to install the file.
3. To execute the program, click Start / Programs / Prosolve / Winscan2.0 / Winscan2.0.

netcat (for windows)

1. Create the directory netcat.
2. Copy the file nc11nt.zip to this directory.
3. Use wiz.exe (above) to extract the files to this directory.
4. The program is nc.exe and should be run from the command line in the netcat directory.

nmap (for windows)

1. Copy the file nmap-3.50-win32.zip to c:\
2. Use the wiz.exe file to extract this file to its default location (c:\nmap-3.50)
3. The program is nmap.exe, and should be run from the command line.

Snort 2.1

1. Create the directory c:\snort
2. Copy the file snort-2_1_0-1.exe to this directory.
3. Execute the program, taking the default options.
4. The program requires that WinPcap [Exercise 2] already be installed on your machine.
5. The program is a snort.exe and resides in the directory c:\snort\bin
6. The configuration file for snort is c:\snort\etc\snort.conf
7. Read the documentation before running snort. One useful command would be

from the snort/bin directory to run

snort -dev -l ../log -h 10.0.0.0/24 -c ../etc/snort.conf

Linux Machines

nmap

1. nmap version 2.54BETA31 is already installed on both RedHat 7.3 virtual machines.

netcat

There are two different versions of netcat available for linux, unix and variants. The first is nc1.10, which is a product of Avian Research. The second is the GNU netcat project, which is netctat-0.7.1. We will use the GNU version in class.

1. Create a temporary directory.
2. Copy the file netcat-0.7.1.tar.bz2 to the temporary directory.
3. To install the program, execute the following commands
   a) tar -xjvf netcat-0.7.1.tar.bz2.
   b) cd netcat-0.7.1
   c) ./configure
   d) make
   e) make install (As root)
4. The temporary directory can now be removed.
5. The program is called netcat, so to find help on the program, use the command man netcat. A link will be make between nc and netcat in /usr/local/bin so that you can execute nc instead of netcat.

Snort

1. Create a temporary directory.
2. Copy the file snort-2.0.4-1.i386.rpm to this directory.
3. Install the package by running rpm -ivh snort-2.0.4-1.i386.rpm
4. Remove the temporary directory.

Installation Notes

1. By default, the rules for snort are contained in /etc/snort/snort.conf
2. By default, the logs for snort are contained in /var/log/snort
3. The program will be installed and run as a service the next time the machine boots.

Instructions for Team 1

Start as many machines as you wish.
On each machine, you may start or stop as many services (http, telnet, etc.) as you wish.
Determine which services are running on each of your machines.
For each machine, fill out a sheet that describes its properties before the start of the exercise.

Offense (1/3 Credit)

- Determine which machines are active on the network.
- For those machines that are active, determine which services are active.
- Whenever possible, determine the operating system of the target, as well as the version numbers of all available services.
- Summarize your results on the Machine Information Sheets that have been provided.

FOR EACH COMMAND YOU EXECUTE, YOU MUST CREATE A LOG ENTRY BEFORE EXECUTING ANOTHER COMMAND. Please use the log sheets provided.

Defense (2/3 Credit)

- After the exercise is concluded, try to determine who scanned your machine.
- What do your log files tell you about the attacker? Explain.