Exercise 2
ICMP Enumeration Techniques

Software Installation Instructions.

Windows 2000 Machines.

To install ethereal.

1) Copy WinPCap_3.0.exe to a temporary directory.
2) Install WinPCap 3.0
3) Copy ethereal-setup-0.10.0.exe to a temporary directory.
4) Install ethereal
5) Clean the temporary directory.
6) The install directory places an icon on the desktop.

Linux

To install ethereal

1. Copy the following to a temporary directory
   a) ethereal-base-0.9.9-1.7.2.i386.rpm
   b) ethereal-gtk+-0.9.9-1.7.2.i386.rpm
   c) ethereal-usermode-0.9.9-1.7.2.i386.rpm
   d) ethereal-kde-0.9.9-1.7.2.i386.rpm
2. Become root, and execute the following, in the given order. [Yes, the order is required.]
   a) rpm -ivh ethereal-base-0.9.9-1.7.2.i386.rpm
   b) rpm -ivh ethereal-gtk+-0.9.9-1.7.2.i386.rpm
   c) rpm -ivh ethereal-usermode-0.9.9-1.7.2.i386.rpm
   d) rpm -ivh ethereal-kde-0.9.9-1.7.2.i386.rpm
3. Drop root privileges.
4. To run ethereal, you must be in a graphical environment. Start a shell, and become root. Then execute the command ethereal &.

To install fping

1. Copy fping.tar.gz to a temporary directory.
2. Execute the following as root.
   a) tar -xzvf fping.tar.gz
   b) cd fping-2.4b2_to
   c) ./configure
d) make
e) make install
3. Clean the temporary directory.
4. Drop root privileges.
5. The program can be run as a regular use, but some options are unavailable. See the man page for details.
To install icmpenum

1. Copy the following files to a temporary directory.
   a) libpcap.tar.Z
   b) libnet-1.0.2a.tar.gz.tar
   c) icmpenum-1.1.1.tgz.gz

2. To install libpcap, execute the following as root.
   a) tar -xZvf libpcap.tar.Z
   b) cd libpcap-0.4
   c) ./configure
   d) make
   e) make install

3. To install libnet, execute the following as root.
   a) tar -xzvf libnet-1.0.2a.tar.gz.tar
   b) cd Libnet-1.0.2a
   c) ./configure
   d) make
   e) make install

4. Fix the libpcap install, by executing the following as root.
   a) cp /usr/include/pcap/pcap.h /usr/include/pcap.h
   b) cp /usr/include/pcap/net/bpf.h /usr/include/net/bpf.h

5. To install icmpenum, execute the following as root.
   a) tar -xzvf icmpenum-1.1.1.tar.gz
   b) cd icmpenum-1.1.1
      c) gcc `libnet-config --defines` -o icmpenum icmpenum.c -Iinet-lpcap

6. The temporary directories, save for the file /icmpenum-1.1.1/icmpenum can be removed.

7. To execute the program, go to the icmpenum-1.1.1 directory, and run
   ./icmpenum

To install icmpquery

1. Copy icmpquery.c to a temporary directory.

2. Compile the program by executing the command
   gcc icmpquery.c -o icmpquery

3. To run the program, go to the temporary directory, and run
   ./icmpquery
Instructions for Team 1

• Start as many copies of as many machines as you wish.
• You will have some time to configure these machines as you see fit.
• Create a log of all of the machines that you have started. Record each machine's IP address, MAC address, and operating system.

Offense (1/3 Credit)
• When the exercise begins, try to determine what machines in the laboratory are active. You may use any technique you wish.
• Your scans should be as stealthy as possible.
• Log all of your activities.
  • For each action you take, your log should indicate
    • What command you used
    • The host used to issue the command
    • The time the command was executed
    • The target(s) of the command.
• There is a limit on the time available for offensive scans.

Defense (2/3 Credit)
• Determine who scanned your machines.
• Can you determine any information about your attackers?
  • What system scanned you?
  • What operating system were they using?
  • What tools did they use?
Instructions for Team 2

• Start as many copies of as many machines as you wish.
• You will have some time to configure these machines as you see fit.
• Create a log of all of the machines that you have started. Record each machine's IP address, MAC address, and operating system.

Offense (1/3 Credit)
• When the exercise begins, try to determine what machines in the laboratory are active. You may use any technique you wish.
• Your scans should be as stealthy as possible.
• Log all of your activities.
  • For each action you take, your log should indicate
    • What command you used
    • The host used to issue the command
    • The time the command was executed
    • The target(s) of the command.
• There is a limit on the time available for offensive scans.

Defense (2/3 Credit)
• Determine who scanned your machines.
• Can you determine any information about your attackers?
  • What system scanned you?
  • What operating system were they using?
  • What tools did they use?
Instructions for Team 3

- Start as many copies of as many machines as you wish.
- You will have some time to configure these machines as you see fit.
- Create a log of all of the machines that you have started. Record each machine's IP address, MAC address, and operating system.

Offense (1/3 Credit)
- When the exercise begins, try to determine what machines in the laboratory are active. You may use any technique you wish.
- Your scans should be as stealthy as possible.
- Log all of your activities.
  - For each action you take, your log should indicate
    - What command you used
    - The host used to issue the command
    - The time the command was executed
    - The target(s) of the command.
- There is a limit on the time available for offensive scans.

Defense (2/3 Credit)
- Determine who scanned your machines.
- Can you determine any information about your attackers?
  - What system scanned you?
  - What operating system were they using?
  - What tools did they use?
Instructions for Team 4

• Start as many copies of as many machines as you wish.
• You will have some time to configure these machines as you see fit.
• Create a log of all of the machines that you have started. Record each machine's IP address, MAC address, and operating system.

Offense (1/3 Credit)
• When the exercise begins, try to determine what machines in the laboratory are active. You may use any technique you wish.
• Your scans should be as stealthy as possible.
• Log all of your activities.
  • For each action you take, your log should indicate
    • What command you used
    • The host used to issue the command
    • The time the command was executed
    • The target(s) of the command.
• There is a limit on the time available for offensive scans.

Defense (2/3 Credit)
• Determine who scanned your machines.
• Can you determine any information about your attackers?
  • What system scanned you?
  • What operating system were they using?
  • What tools did they use?