Project

Goal

The goal of this project is to give you some experience in analyzing the security of a system. For this, you will play the role of a security analyst.

You work for a corporation that keeps its data on a system protected by a firewall. The system runs a web server that displays sanitized data. It should not display any sensitive data. Your bosses have asked you to determine the following two things:

1. Does the firewall correctly pass the traffic that it is supposed to pass, and block all other traffic?
2. Can outsiders (those without accounts on the system) get access to any data beyond that displayed on pages marked *authorized*?

The following outlines what you are to do to answer these questions

First Step: Firewall

Your first step is to look at the firewall. It should allow the following types of messages through: *ssh* (port 22) and *http* (port 80), using TCP and UDP. Checking this requires a program known as a *port scanner*. You can find several; we've set up one for you. This program, *nmap*, is very powerful but must be run as *root*. You can look on the class home page for the manual page. As most of you don't have *root* access to any systems, we've set up a special login that will run *nmap* against the target system, which has IP address 169.237.7.61.

To use this login, *telnet* to *nob.cs.ucdavis.edu* and log in as *nmap*. No password is required. You will see a greeting, and then you will be asked for options. The standard TCP scan requires the option –sT; the standard UDP scan, –sU. The *nmap* manual page describes other options. Once you enter them, you will see a line like:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
```

It will then sit for a while (how long depends upon the options) and print out the list of what it believes are open ports. Good options are –p, which allows you to specify port ranges, and various -s options such as –sX. You should also look at –O.

To Turn In: You are to turn in 3 files. The first, *tcpudp*, is to contain the results of a standard TCP and UDP port scan. List ports for both the TCP and UCP protocols. You can use *nmap*, as described above, or your own favorite port scanner. The second file, *oddpacket*, is to contain the results of any of the following port scans: TCP SYN scan, Stealth FIN scan, Christmas Tree scan, or Null scan. The third, *log.txt*, is to contain your notes on the scanning. In particular, please explain why we asked you to run the scans in *oddpacket*. Did you get different results? Does the manual page suggest why?

Extra Credit: Determine if the firewall is stateful (that is, a proxy firewall) or not (a filtering firewall).

Second Step: System

Now you are to look at the host behind the firewall. The first step is to figure out what servers the remote host is running. A good way to start is to look for the most common servers: telnet, smtp (mail server), www, ftp, rlogin, rsh, the portmapper, and X11. To get other ideas, look at the servers that CSIF machines are running.

Step 1: What servers is the CSIF running?

To find this, run *netstat -a* on any CSIF system. Look at the fourth column (Local Address). You will see either an IP address, a host name, or an asterisk (*) followed by a colon and a name or a number. The name following the colon is the name of a server. To figure out which port the server is running on, look for the server name in the first column of the file */etc/services*. The second field in that line contains the port number followed by the protocol (tcp or udp).

Step 2: Look at the target system.

What servers is the target running? You might look at the results of the first step to see which ports are open, and tie them back to the names of the servers. Here are a few questions to get you going.

1. Is a web server running? If so, can you think of any security-related problems that may arise from running a web server?

2. Does the system behind the firewall allow you to *rlogin* into it?
3. Does the system behind the firewall run an X window server (look for open TCP and UDP ports in the range 6000 on up)?

To Turn In: You are to turn in 3 files. The first file, *csif-servers*, is to list the servers running on a CSIF system (please name the system, of course …). The second, *target-servers*, is to list the servers running on the target system behind the firewall. In both files, please *name* the server as well as the port number (unless there is no server associated with that port in */etc/services*). The third file, *log2.txt*, is to contain a record of how you obtained the data in the other two files.

Turning In Results

Please submit them to the directory *proj1* using the *handin* program. This is due on November 30.