Lab 6: Firewalls, IDS, and Antivirus

CS 460 Spring 2015: Security Lab

Due 11:59 PM Thursday 03/12/15

Overview

ipTables is a basic firewall installed by default in the Linux kernel since 2.6. With it, you can do basic things like deny packets from an IP, or create more sophisticated rulesets like a stateful firewall. Snort is a free and open source software that provides IDS functionality. And lastly, ClamAV provides antivirus software. You will be implementing all three of these software packages, as well as some WinBlows equivalents.

Note: This lab is going to be taxing on the VM infrastructure. Because the VM Infrastructure is not really all that great, if you are not actively working on the lab, please turn off your VM. Please. Course Staff will turn on the VMs, before they grade them. Do your work but understand that your VM may get shut down at any time. If your VMs run out of memory, Course Staff recommends stopping CUPS, the bluetooth service, and if you feel comfortable working without a GUI, X11/lightDM.

Ubuntu

ipTables

Your task for this section is to set up a firewall using iptables that blocks all connections except connections on port 80. There is a good write-up for setting up ipTables here.

In order to test that you properly set up your firewall, the grading script will make an http request to your VM's IP on port 80. You will want to install Apache web server using apt-get, in order to make sure that http request does not fail. It doesn't matter what the html on the page is, as long as the HTTP request does not fail.

Snort

Read this introduction to Snort, and snort rules here. You can install snort using apt-get. Write a snort rule to alert you when someone connects to your apache webserver over port 80. If you write your snort rule correctly, you can have it log/capture any offending requests, which will get you the flag Course Staff will be sending you. Submit the flag in flag1.txt.

ClamAV

Attached in your SVN directory is a file called malicious. Install clamav using apt-get, and then scan malicious. Find out the name of the virus in that file and attach it as flag2.txt.

Windows

Set up the Windows Server Firewall to allow connections on port 31337. You don't have to run any service on it, but just open up inbound connections to that port. Here's a helpful link.

Deliverables

1. Fill out the myIP.txt file with the first line being the IP of your Ubuntu Machine, and the second line being the IP of your Windows Machine.

2. ipTables should be configured so that a machine can make an HTTP request to your Ubuntu server on port 80 but no other port can recieve connections.

3. Put the flags in flag1.txt and flag2.txt.

4. Windows Firewall should be configured to allow connections on port 31337 to your Windows Server 2008 but not anything else.