

CS393/682 Lab 3: Introduction to Intrusion Detection Systems

Introduction

Intrusion Detection Systems (IDS) are used in a network to monitor traffic or in a host to monitor events to detect malicious activities. As you have seen in class there are different types of IDS's each having its own advantages and disadvantages. In this assignment you will (i) learn to use Snort, an open source network IDS and (ii) create an application specific IDS that will detect malicious traffic going to a telnet server using the telnet password sniffer you've developed in lab 1. Part II has to be done individually and Part I can be done in groups.

What you are recommended to read before starting the assignment:

- For part 1 read about Snort <http://www.snort.org> and find more information about it from <http://www.google.com>
- Telnet RFC: <http://www.faqs.org/rfcs/rfc854.html> (for part 2)
- Understand minisniff from: <http://vip.poly.edu/kulesh/skunk/src> (for part 2)

Part I: Snort (Group work)

Download the current release of snort from snort.org, configure it and install it in your node that has two NIC cards, make sure that you are using the latest rules.

Now do the following experiment:

- 1) Install the vulnerable rootecho from MyPoly into the node that has one NIC card.
To install rootecho:
 - 1) Log on as root
 - 2) Compile the code using gcc
 - 3) Move the a.out file to /sbin and rename a.out to rootecho
 - 4) Type "chmod 4755 rootecho" to set UID.Now telnet to the host where you installed rootecho, from your windows desktop, as guest and exploit rootecho to get a root shell. Observe if this rootecho attach is detected and identified by snort that is running in your router (the machine with two NIC cards).
- 2) The Linux boxes have Nessus already installed. An introduction to Nessus is http://www.linuxsecurity.com/feature_stories/nessusintro-printer.html. Use Nessus to launch attacks towards your node that has two NIC cards. Observe if any of these attacks are detected and identified by snort.
- 3) Explain the observations you made in 1 and 2. In your explanation you must clearly indicate the differences between the attacks and why snort was able to detect some but not all. You could give references to other material such as class slides, research papers and web sites.
Please remember: we are not expecting you to write a book out of this experiment, so this explanation should not be more than one double-sided page with single spaced lines and font size 12 without screenshots.

Part II: (Telnet IDS) (Individual Work)

Create an IDS system based on minisniff to catch attacks such as "rootecho" that escalate normal user privileges to root in a telnet session. You should be running your IDS in the node that has two NIC cards and must detect attacks performed in the internal node. Write a one-page description on the design of your IDS and a justification for the design. Clearly state your assumptions and the limitations of your IDS. Also submit all source code and screenshots.