Project 3: Snort and Syslog

CSE 468 Computer Network Security

Due Date: Apr 9, 2014 11:59PM

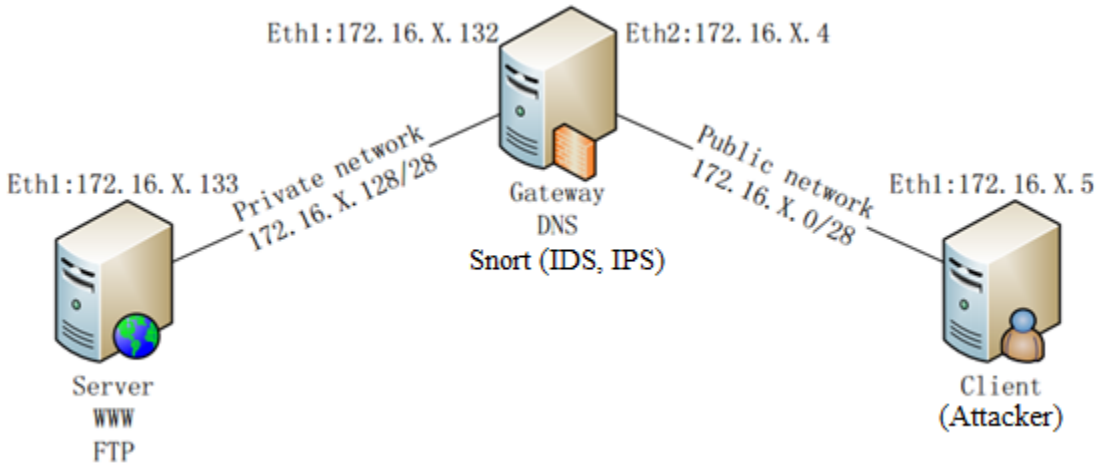
1 Objective

The learning objective of this project for students is to gain hands-on experiences with the usage and functionality of Snort and Syslog. After the project, students should know how to set up a network based intrusion detection system using snort to detect and prevent network intrusions, and how to set up a remote syslog server to accept the alert messages generated by Snort.

2 Project Description and Tasks

2.1 Environment Setup

The network consists of three VMs: Gateway, Client, and Server. They simulate a typical network application scenario: the Server resides in a private network; the Client resides in a public network; the Gateway protects the Server from public access by using IDS and iptables. The network topology as illustrated in the following figure.



Install Snort package on your gateway and run another internal computer accessing the external network through the gateway. Configure iptables properly on the gateway to allow traffic from vnet 1 to vnet 2 and vice versa.. Please follow the steps below to install Snort in your Gateway:

1. In order to install Snort with both IDS and IPS mode, you need to install it from the source. You have two options:
   a. Download Snort source file from www.snort.org and other necessary dependency packages. The latest version of Snort is **snort-2.9.6.0.tar.gz**. Follow instructions in the http://hacktracking.blogspot.com/2013/10/snort-ips-inline-mode-installation.html page to compile and install Snort. Please change the version number in the script to 2960.
   b. Download the shell script "buildSnort.sh" using "wget" command in the terminal from http://cse468.mobicloud.asu.edu/projects/buildSnort.sh. Run the shell script to download, compile and install the snort. Please also change the version number in the script to 2960.
2. Download and install the rule sets "**snortrules-snapshot-2960.tar.gz**" from www.snort.org according to your installation method in Step 1. Before downloading the rule sets, you must register at snort.org to obtain this file.
   a. Follow the instructions in Step 1.(a) to update our rule sets.
   b. Download the shell script "rules.sh" using "wget" command in the terminal from http://cse468.mobicloud.asu.edu/projects/rules.sh. Change the version number and corresponding folder in the script to 2.9.6.0.
3. Make sure you have installed the required module to perform IPS with NFQ in Snort by issuing the following command:

   ```
   sudo snort --daq-dir=<your daq folder> --daq-list
   ```
4. Make sure you have Web Server, ssh and syslog (rsyslog) running on the server

2.2 Project Tasks

Students need to write rules in the snort and setup iptables properly on the Gateway to satisfy the following requirements:

1 Write simple rules in the local.rules to check the traffic originated from the attacker to the server.

   a. Any HTTP connection request from attacker to the server.

   b. Any ssh connection request from attacker to the server.

c. ICMP echo request message with sequence number = 7 (using ping command from the attacker to the server).

2 Configure Snort in the IPS mode with DAQ type afpacket and block the ping traffic from the attacker to the server. (Note that your iptables should initially allow ping without using Snort; once the Snort starts, detected ping traffic should be blocked.)

3 Configure Snort in the IPS mode with DAQ type NFQ, and block HTTP request from the attacker to the server.

4 The snort log should be handled by the rsyslog. The rsyslog server is running at the server. The gateway should generate log and store them at the server side (you can decide using what file at the server side to store the logs).

3 Project Report

You should submit a report to record detailed project process as required on Blackboard. In addition to the general requirements, you also need to answer the following questions:

1 Which approach you're using to install Snort, what's the purpose of each step in the installation script, and where is the Snort binary file located after installation? (Refer to the step 1 and 2 in section 2.1)

2 What's the result you get after performing the command in the step 3 of section 2.1?

3 Describe the detailed steps of how to set up a remote syslog server to accept the log from Snort.

4 For each task in section 2.2, please describe the detailed steps and the result after the configuration. Please include some major screenshots to proof your configurations are working and satisfy the requirement for each task.