**CSCI 530 Lab**

**Intrusion Detection**

General Description:

Virtual Machine IP address assigned: 192.168.1.70

IP address of Windows Host: 192.168.1.75

1. Nothing happened to the values below 800. The alert was triggered at value 801.
2. The Alert file is used to log “alert” messages based on the pre-configured snort rules. It is mainly used to log potential threats/intrusions and any pre-determined malicious behavior.

Snort.log files are the complete log of all the messages intercepted by the Snort IDS. It stores a complete list of all activities. It logs the data into this file.

1. “Xref” is used as a cross reference where a Nessus script resides, that can be used to perform the same kind of attach from the user’s host.
2. The rule explains that an alert is to be raised, by writing to the snort log file if there is a TCP packet having source IP address as $HOME\_NET, with the source port 23. The destination IP address is to the be same as the $EXTERNAL\_NET, with no restrictions on the destination port.

The contents of the packet described above should be “Login incorrect”. When such a packet is encountered the message in the alert file should say

“MSG:”TELNET login incorrect”.”

The action corresponding to the packet’s presence is an entry into the snort ALERT file.

The string “TELNET login incorrect” is a “human readable” string which users can see the title of the alert file entry for such packets.

The content “login incorrect” is the content of a packet which triggers and activates the Snort functionality.