Todd Wenker

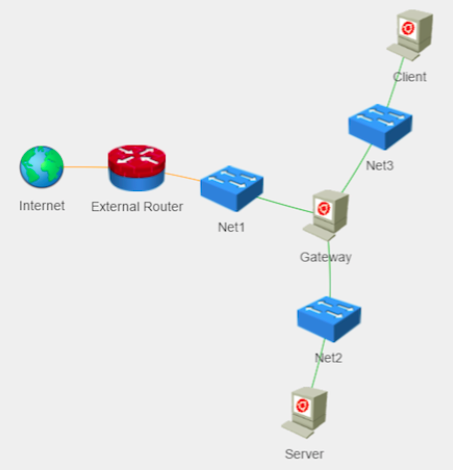
ASU ID: 1206233882

Lab Assignment 6

Intrusion Detection System Lab

**Summary:** The goal of the lab is to use Snort as an intrusion detection system. Snort allows the user to establish rules that log incoming and outgoing traffic through the host.

**Network Setup:**



There are three hosts on the network: Gateway, Server, and Client. Gateway will be the host that will download Snort and establish rules. Client will act as the attacker and Server will be the victim.

**Software Packages Used:**

* Snort
* Bind9

**Lab Tasks --- Install Snort, Establish Rules, and View Alert Log**

Before Snort is set up on the Gateway machine, a number of dependencies need to be installed by using the command:

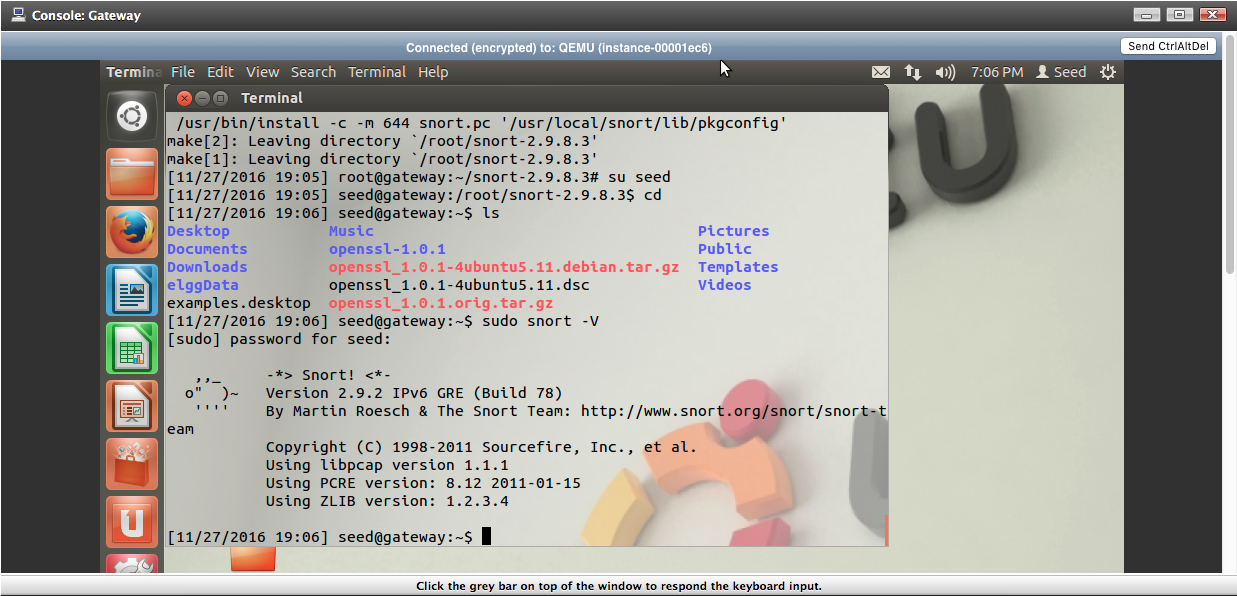
*sudo apt-get install build-essential bison flex libdnet libpcap-dev libpcre3-dev libnet1-dev zlib1g-dev libnetfilter-queue-dev curl libdumbnet1 libdumbnet-dev*

Now, Snort is ready to be installed, which can be done with the commands:

*sudo -i  
cd ̃  
curl --silent --location --output daq-2.0.6.tar.gz \ https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz  
tar xvzf daq-2.0.6.tar.gz  
cd daq-2.0.6  
./configure  
make  
make install  
cd ̃  
curl --silent --location --output snort-2.9.8.3.tar.gz \ https://www.snort.org/downloads/snort/snort-2.9.8.3.tar.gz*

*tar xvzf snort-2.9.8.3.tar.gz  
cd snort-2.9.8.3  
./configure --prefix=/usr/local/snort --enable-sourcefire make  
make install*

The series of commands change the user to root, downloads and decompresses the file *daq-2.0.6.tar.gz* from www.snort.org before configuring and installing it. Then the same is done for the file *snort-2.9.8.3.tar.gz*.



Above is the result of the command *sudo snort –V,* which displays the version of Snort installed, which is version 2.9.2.   
Now that Snort is installed, rules can be established that will track traffic heading to and from the Gateway machine. By using the command *sudo vim /etc/snort/rule/local.rules*, we can edit the local rules. The following three lines are added:

*alert tcp 192.168.3.4 any -> 192.168.2.4 80 (msg:”HTTP connection!”; sid:1000010;)*

*alert tcp 192.168.3.4 any -> 192.168.2.4 22 (msg:”SSH connection!”;sid:1000001;)*

*alert icmp 192.168.3.4 any -> 192.168.2.4 any (itype:8;icmp\_seq:7;msg”Ping \*

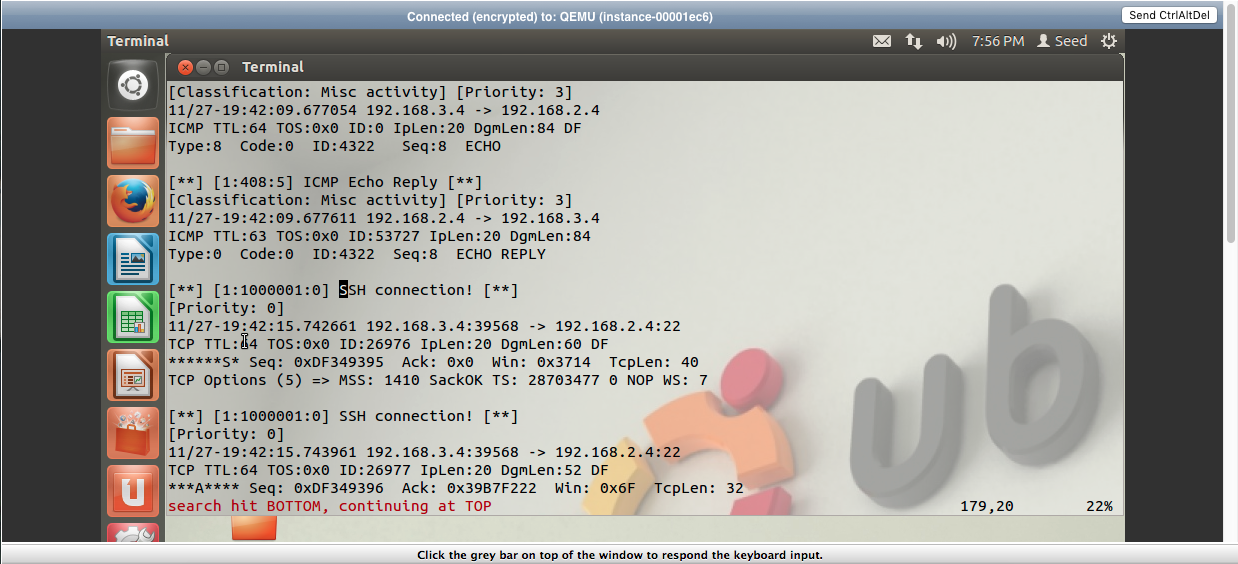
*Request!”sid:1000002;)*

The first command will create an alert if a packet with TCP protocol, source address 192.168.3.4 (the IP address of the Client/attacker), any source port, the destination address 192.168.2.4 (the IP address of the Server/victim), and the destination port being number 80. Because port 80 is the default port for HTTP connections, this alert will log any attempts by the Client machine to access the webpage located on the Server machine. The second alert will catch the Client machine attempting to establish an SSH connection to Server, as the destination port, number 22, correlates to the SSH port. The last alert will catch ICMP messages from Client to Server that have the type number 8, which correlates to an echo request message, and have the sequence number 7, meaning that the message will be the 8th in the sequence.

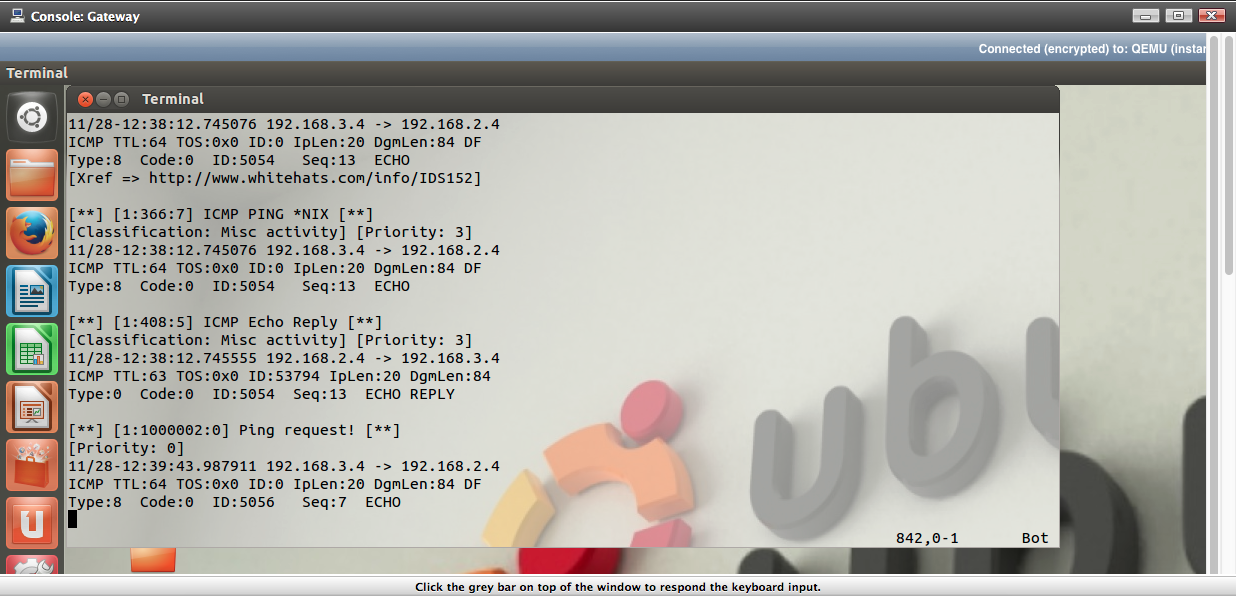
To begin Snort, the command *sudo snort –v –c /etc/snort/snort.conf -i eth2* is used on the Gateway machine. Then, an SSH connection is established from the Client to the server using the command *ssh 192.168.2.4.* Then, Firefox is used to access Server’s webpage by entering *www.toddwenker.test* into the address bar. Then, the command *ping –c 8 192.168.2.*4 is used to send eight ICMP messages to Server. To view the log file where the alerts are written, the command *vim /var/log/snort/alert* is used.



Above is the Snort alert log file showing the first alert’s message, “HTTP connection!” Each message from Client to Server’s HTTP port will activate this alert.



Above is the message generated from the second alert. Each packet from Client to Server’s SSH port will generate this message.



Above is the message generated from the third alert. Because the icmp\_seq is set to 7 in the alert, the alert only fires after the 8th message.

When Snort is being started, if the interface is changed from ‘eth2’ (the interface that connects to Client) to ‘eth1’ (the interface that connects to Server), there is no difference. The alerts will still catch messages. This is because the packets travelling from Client to Server enter the Gateway from the ‘eth2’ interface and leave along the ‘eth1’ interface. Regardless of which of the two interfaces that Snort monitors, it will catch the packets that the alerts were set up to catch. However, if the interface selected is ‘eth0’, the alerts will not catch packets, since they do not enter or leave through ‘eth0’.

**Conclusion:** By using Snort, rules can be set up that will catch any packets that are sent through a gateway. This can allow a user to detect any potential intrusions by an attacker.