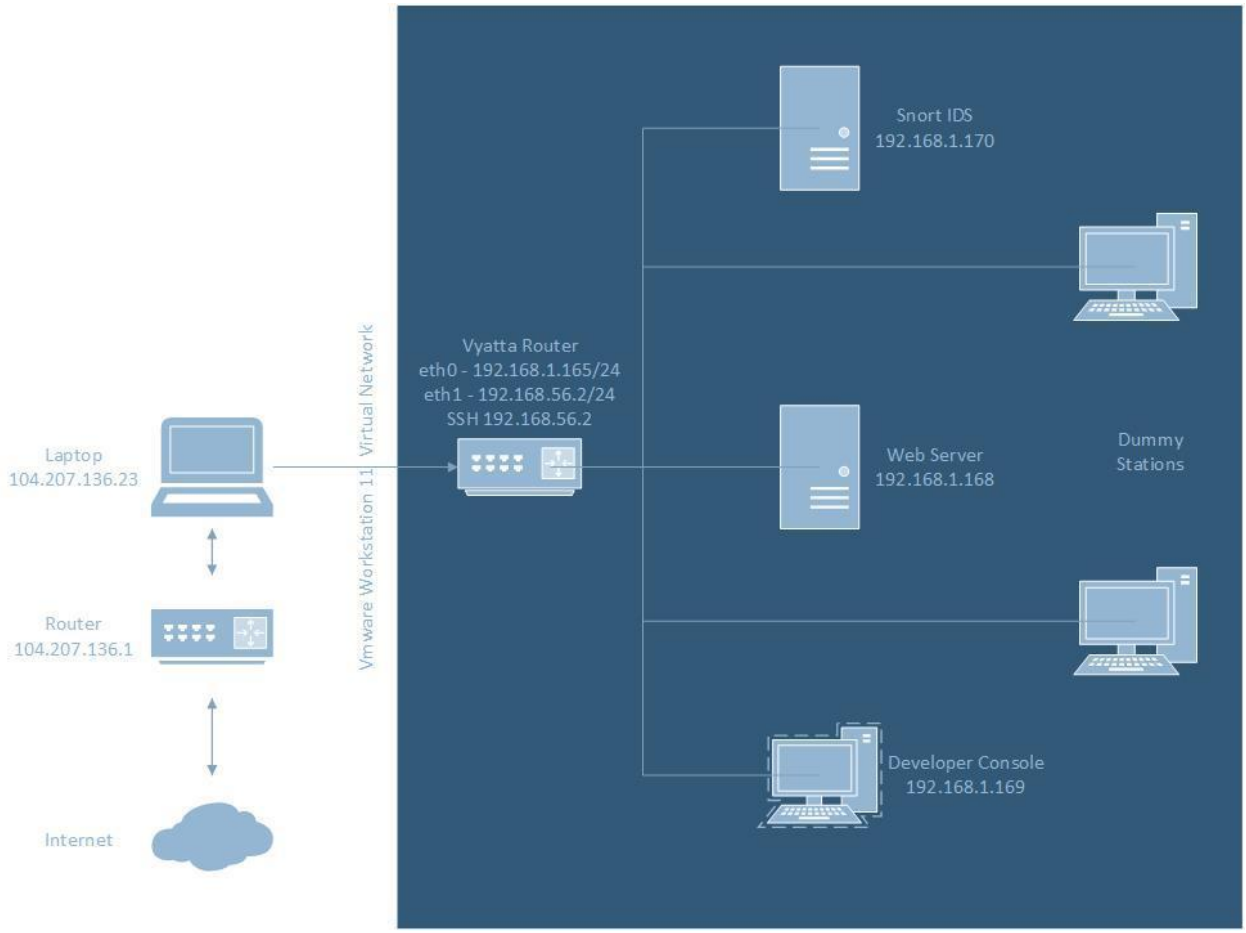
Lab Memorandum

Professor: **Barrett**
Course: **NTW415, Network Defense & Countermeasures**
Student: **SSH[ghost]**
Date: **15-Feb-15**
Lab / Activity: **Final Project**

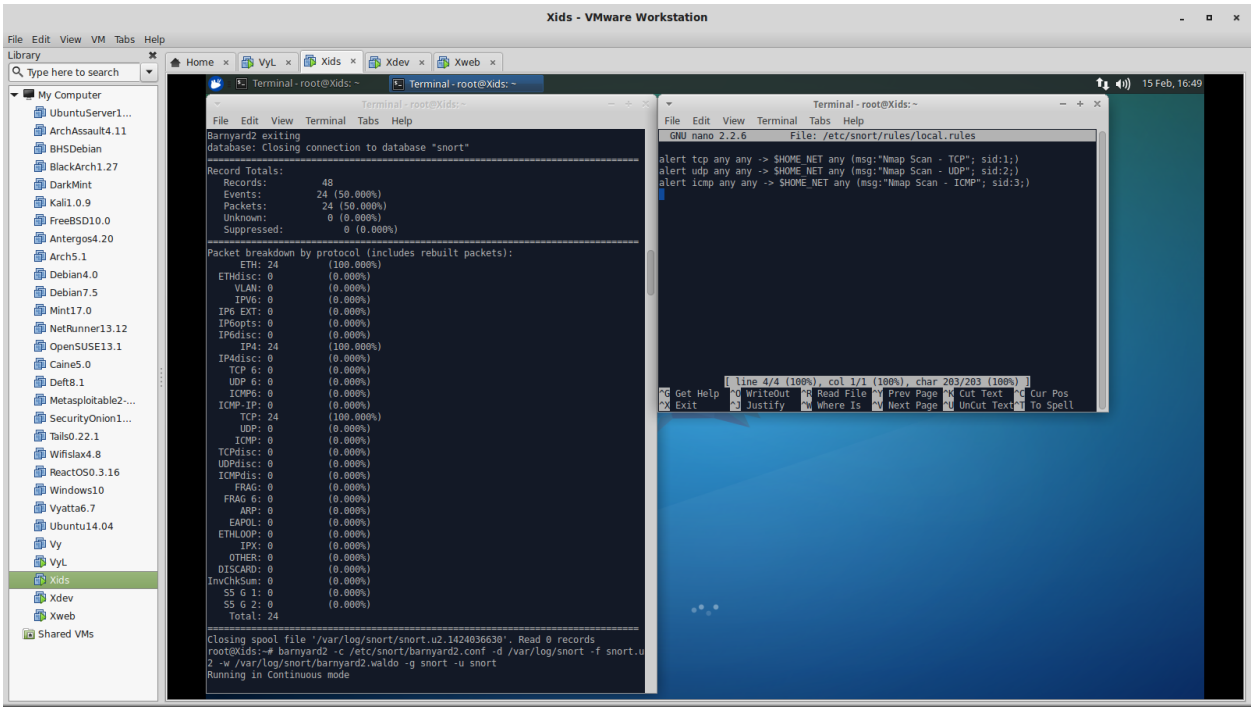
1) Brief description with network diagram.



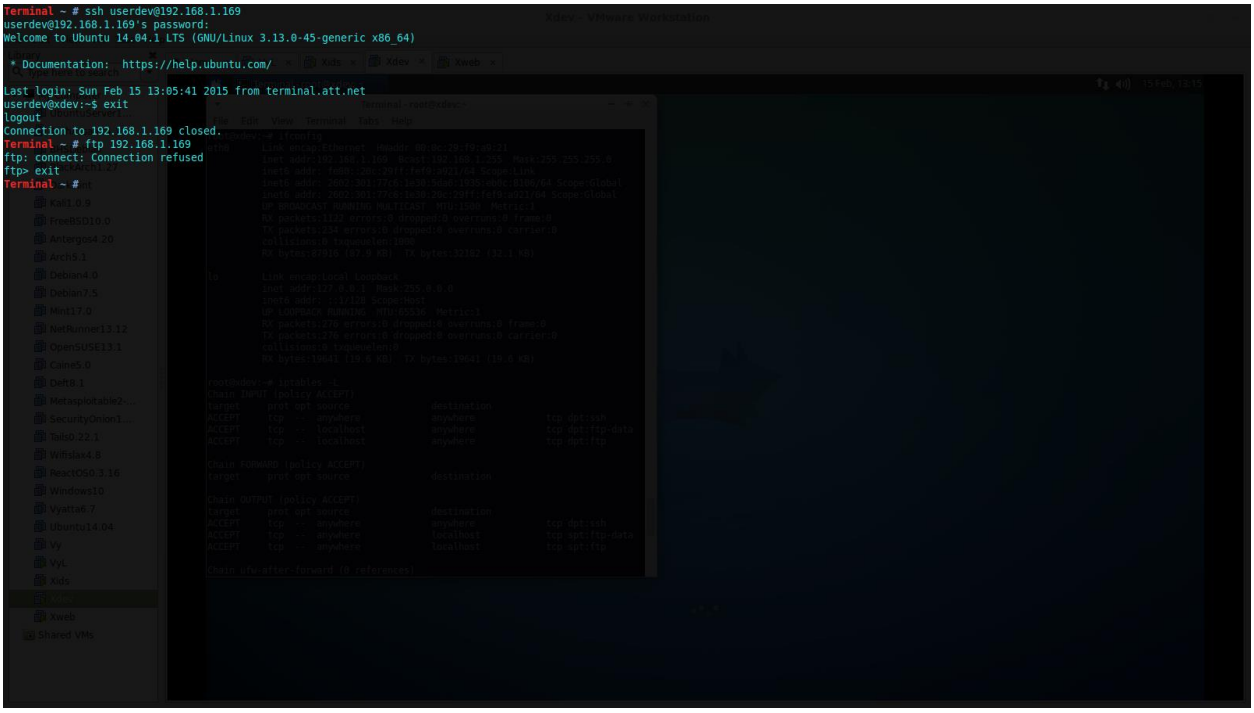
This is my virtual network running off my laptop with Linux Mint complete with configured AT&T Motorola router on class A network. The Vyatta firewall / router VM is run ahead of the other VMs to ensure that they connect to Vyatta. Vyatta has inbound Internet connection on eth1 host-only adapter while outbound for the other VMs with NAT on eth0 NAT adapter. It's also configured to use DHCP on outbound, listen for SSH connections on 192.168.56.2, and allow said SSH and HTTPS for other VMs connected (thwarting HTTP?). The Snort IDS server is configured with Snort to log, in my virtual network, ALL traffic in order to learn general from unusual. It's set to recognize any and all TCP, ICMP, and UDP connections on the Vyatta

network with a constant connection since Snort and Barnyard2 start up on boot. The web server, which doesn't actually act as a web server since we never installed apache2 for the virtual network, is supposed to act as the web server for the virtual network. Any guest, dubbed dummy stations on the diagram below, are able to make an FTP connection into the web server, but users outside the network cannot. The only station permitted to create a SSH connection is the developer console and all outbound FTP and SSH is blocked. The developer console can accept SSH connections from any computer on any network inbound and outbound. It can accept FTP connections from any computer inbound or outbound as long as it is on the Vyatta network.

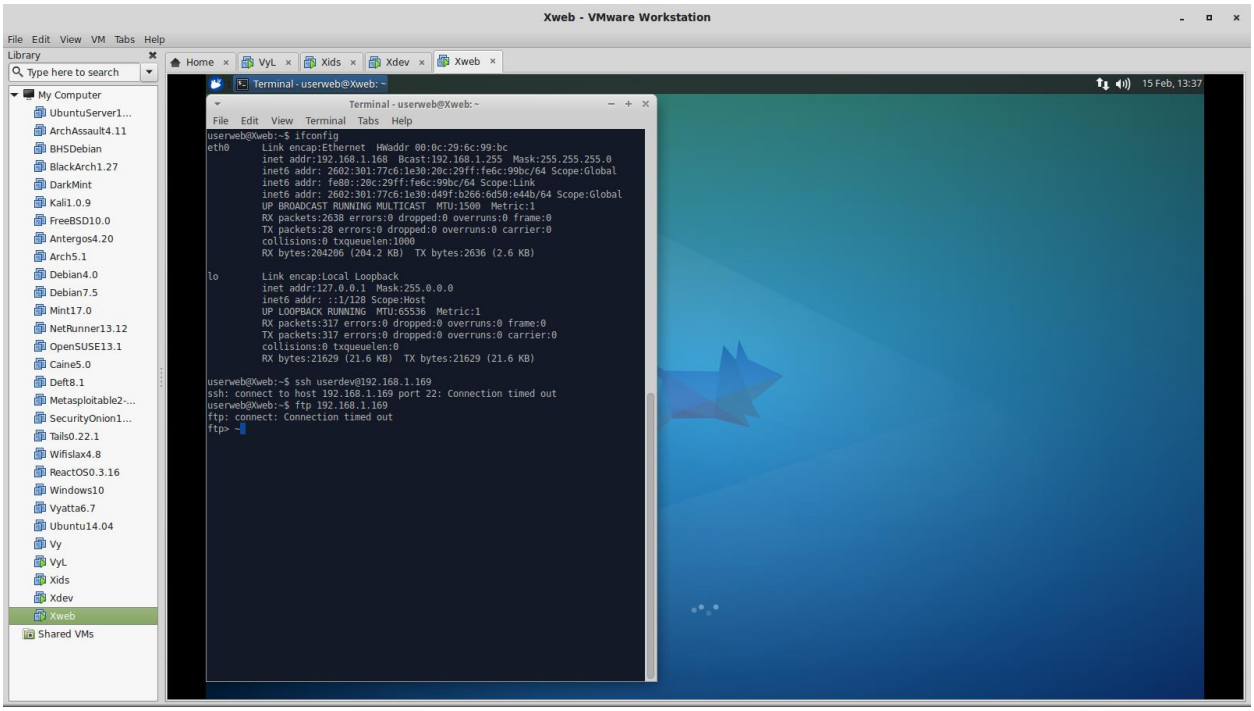
2) Perform Nmap scan with IDS detection.



3) SSH into dev from host. Connected - Success. FTP into dev from host. Rejected – Failure/Success. As per week 4 assignment, the dev console blocks FTP connections that are not from the local network. Due to a time crunch, no guest was added, installed, and additionally configured to see FTP connection to act as "host," but FTP blocking was verified. Thus, blocking FTP from host was success.



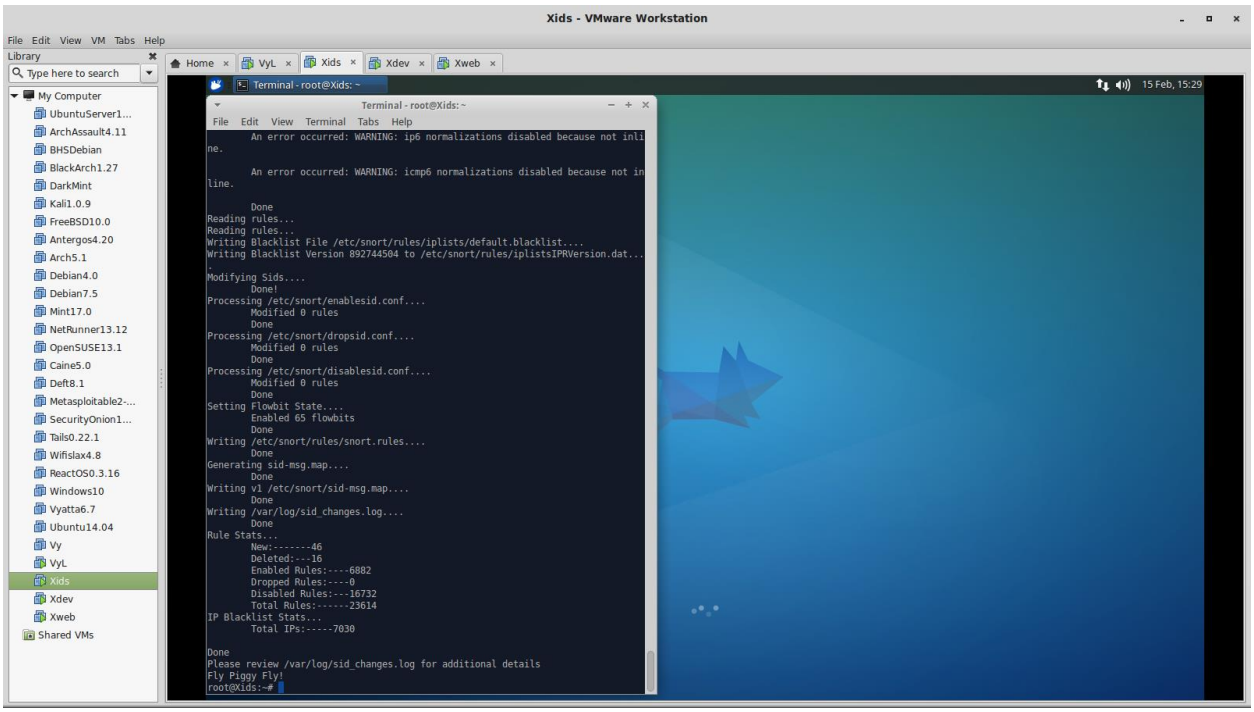
4) SSH into dev from web server. Blocked - Success. FTP into dev from host. Blocked - Success.



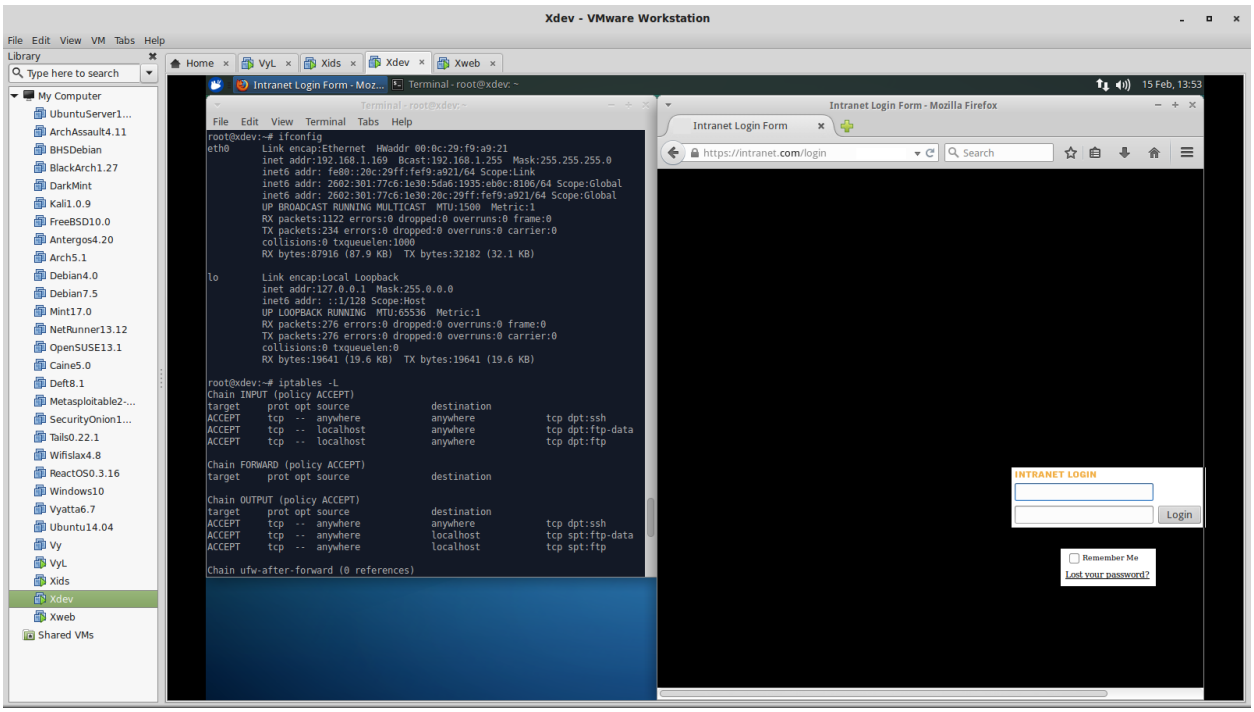
5) See #3

6) See #4

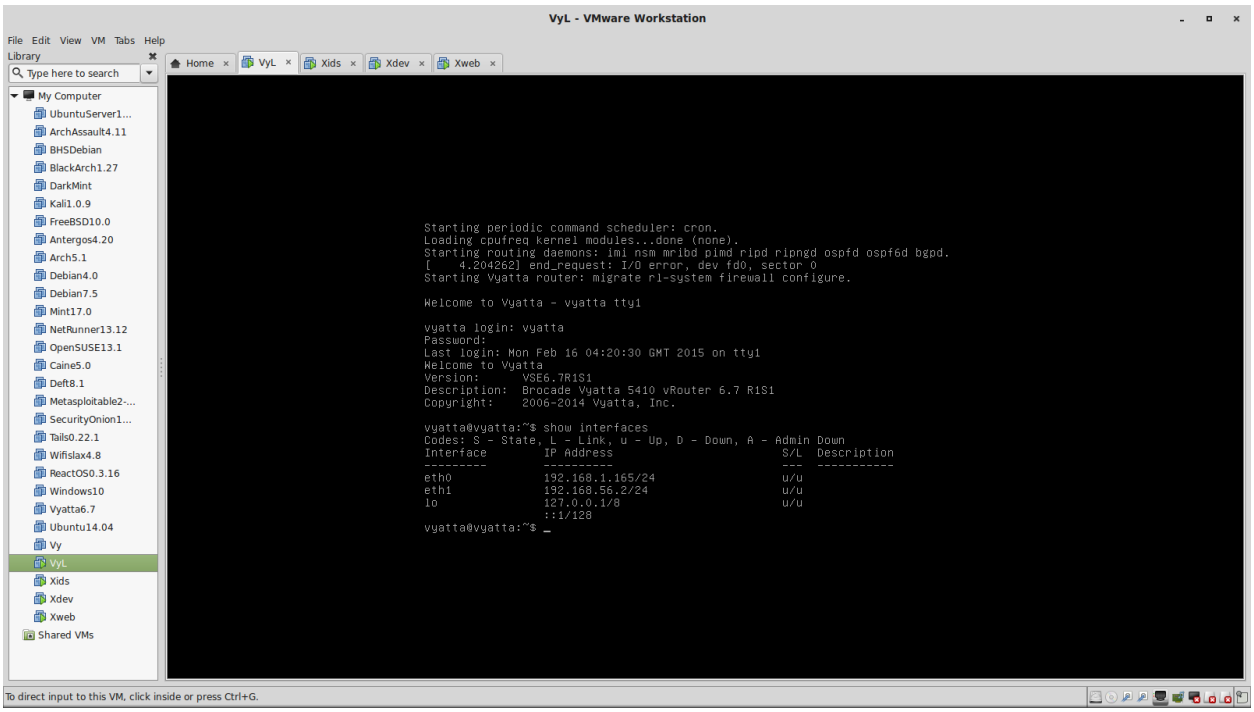
7) Snort rules updated via Pulled Pork. See screenshot after #8 for Vyatta connection.



8) Browsed to Intranet login page from dev console. See screenshot after #8 for Vyatta connection.



Vyatta connection screenshot



Lab/Activity Summary:

This was a fairly challenging and hard assignment that needed the assignments from week 1, 3, and 4 done correctly in order to succeed. Good thing week 1 and 4 were done correctly, but that means 3 days was spent on week 3's Snort IDS. I finally managed to get it to work with a few jury rigged commands here and there. Thus, we have a live, fully functional virtual network! I really hope to have more assignments this challenging in the future!