Lab 4
Gunnar Yonker

Part 1: Installing Zeek on your SEED VM

SeedUbuntu B: 10.0.2.4

Zeek installed

Part 2: Run Zeek

No issues getting zeek up and running, ethernet interface changed to enp0s3

networks.cfg file was not modified

ZeekControl configuration completed

logs will be located in /home/seed/zeek-3.0.11/logs

Part 3: Modify the local script

traceroute and scan scripts were enabled in the local.zeek file and saved

I found it interesting what scripts were included in the local.zeek file and the various scripts that could be run, along with the commented warnings about how performance could be affected. For example, on the traceroute script, there was a warning commented in that if many traceroutes were being run on the network that the performance could suffer and slow down due to that traffic. I would be interested in what kind of other scripts that could be added, or if they can be added using the Zeek program.

Part 4: Attack or scan the VM with Zeek Installed

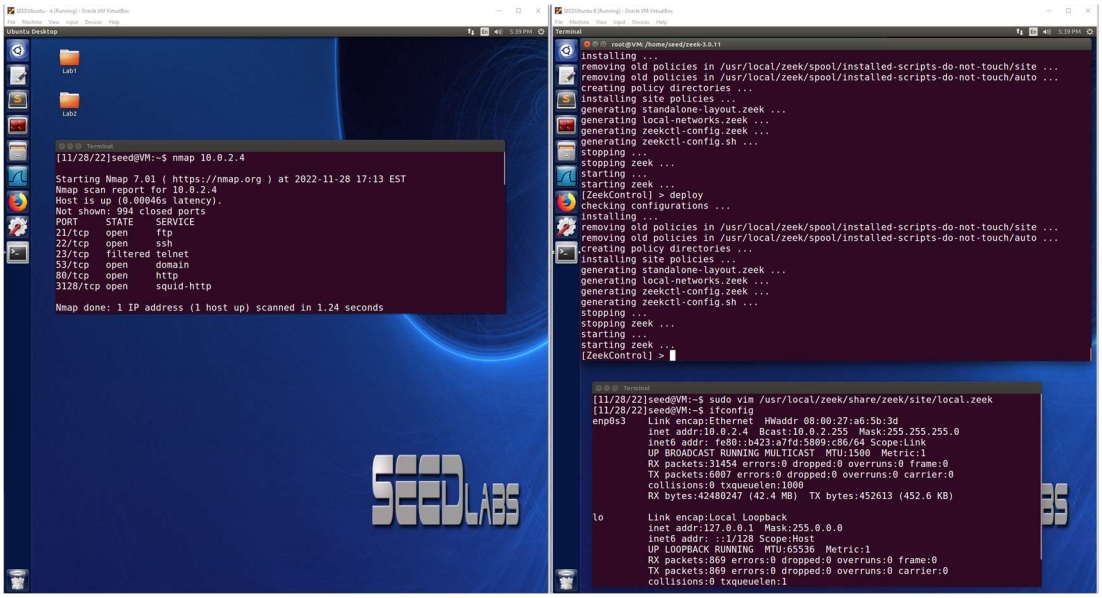
A is the attacker and B is the Zeek VM

Zeek VM: 10.0.2.4

(1) Port Scanning using nmap:

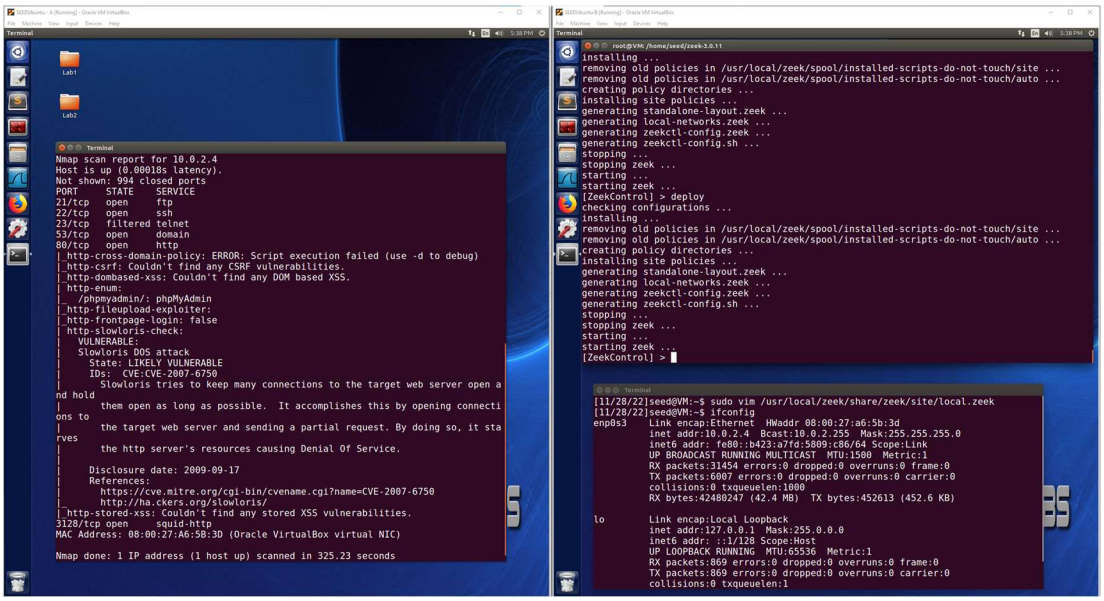
My goal with this scan is to use nmap to see what ports are open on the Zeek VM using:

nmap 10.0.2.4 -v



I also wanted to run a vulnerability scan so I used the nmap command with –script and vuln to see if there were any vulnerabilities on the Zeek VM:

sudo nmap --script vuln 10.0.2.4

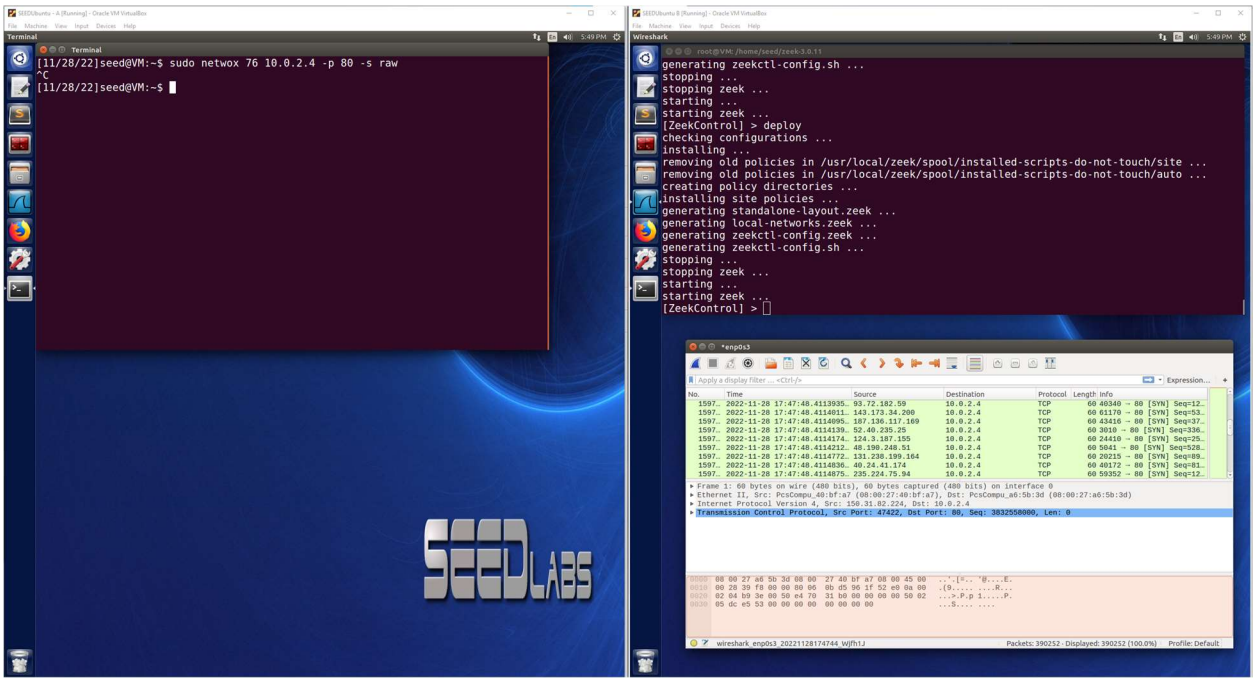


SYN Flooding Attack:

For the SYN Flooding Attack test on the Zeek VM, I am going to use netwox and target port 80 using this command:

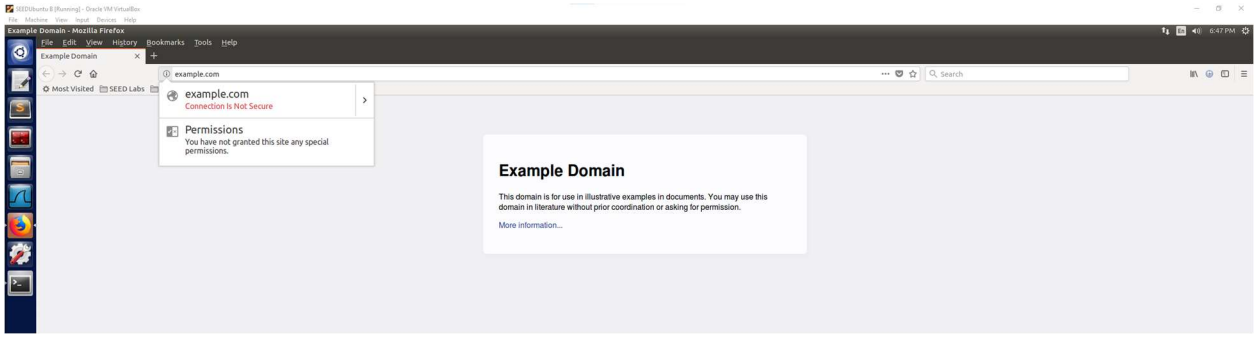
sudo netwox 76 -i 10.0.2.4 -p 80 -s raw

The SYN Flood Attack is successful as seen below through Wireshark on the Zeek VM where a very large number of SYN packets are being received and left open from spoofed IP Addresses.

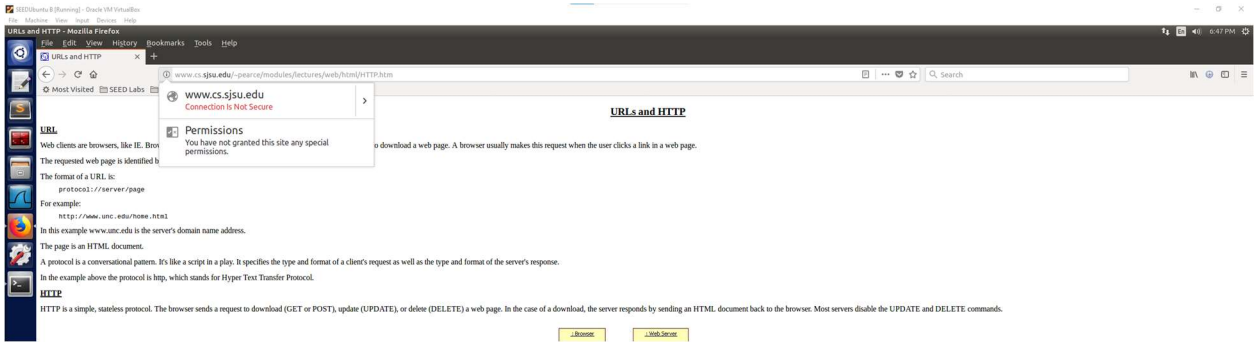


(2) Websites browsed to

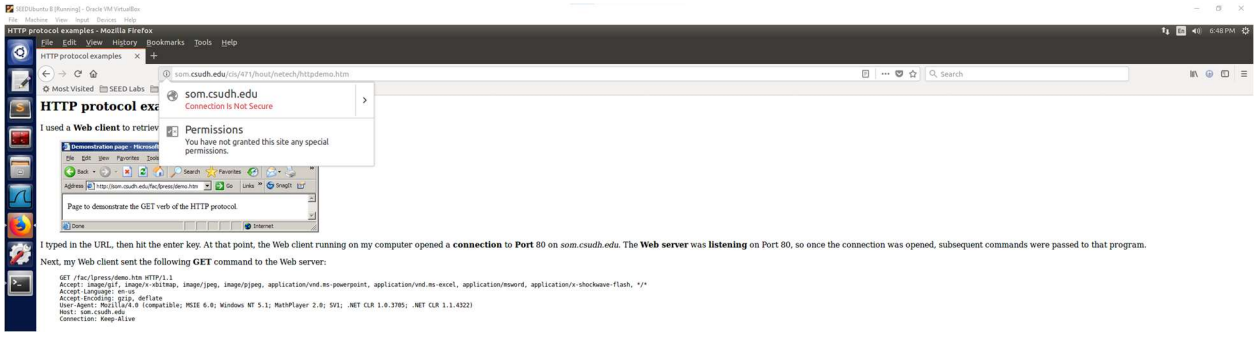
http://example.com/



http://www.cs.sjsu.edu/~pearce/modules/lectures/web/html/HTTP.htm



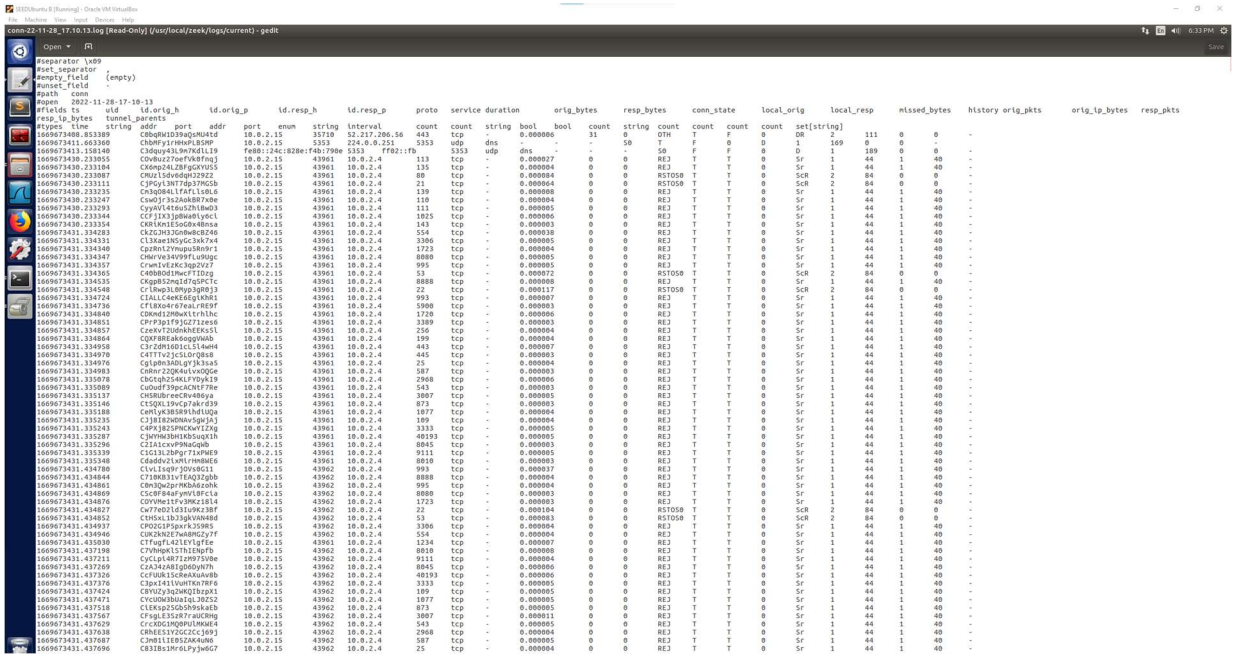
http://som.csudh.edu/cis/471/DDhout/netech/httpdemo.htm



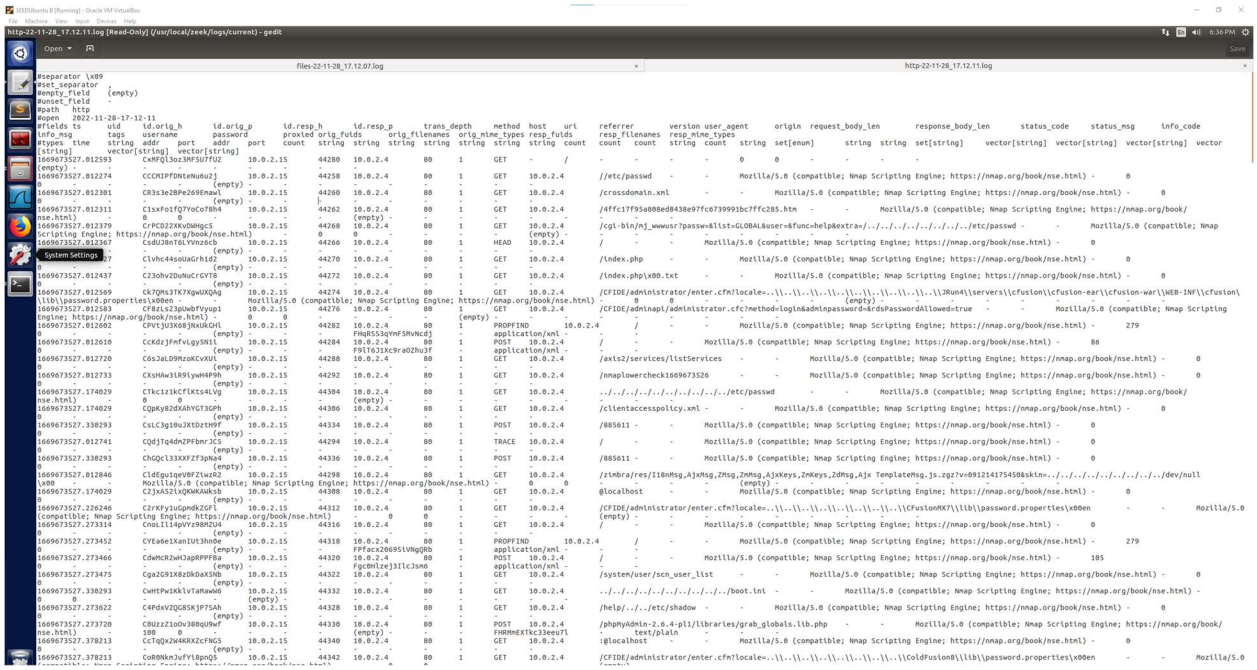
Part 5:

Nmap scan:

It looks like the conn log file contains some information that could be from the nmap scan looking for open ports on the Zeek VM. The source IP listed is that of the attacker carrying out the nmap scan and shows the response such as REJ when the port was found to be closed.

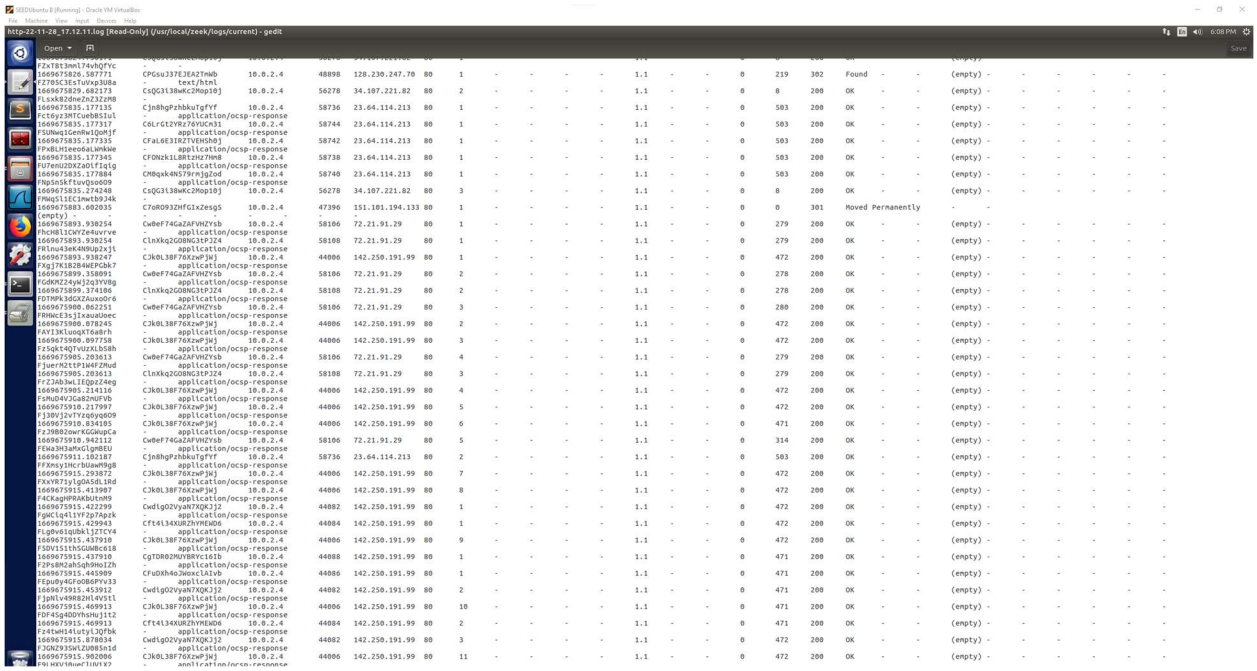


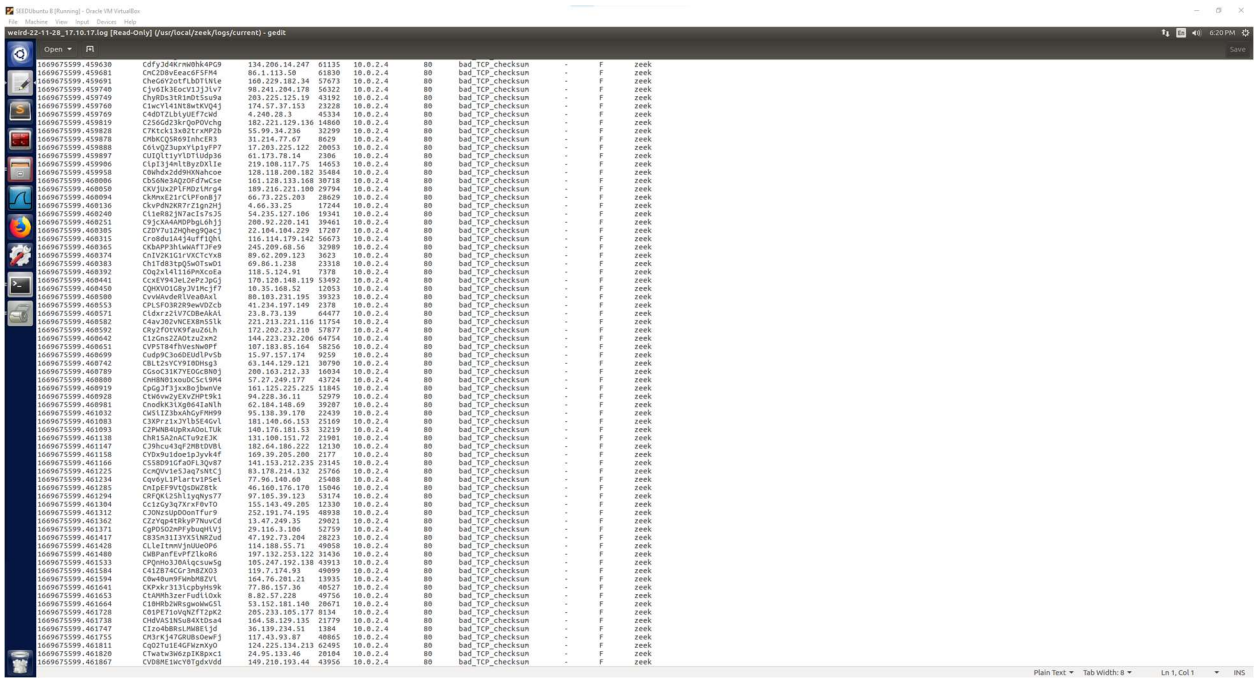
The http log file also shows some interesting information about the nmap scan coming from the attacking machine which shows the attacker's IP address and the contents on the right side of the log file show that the nmap scripting engine was being used.



SYN Flooding Attack:

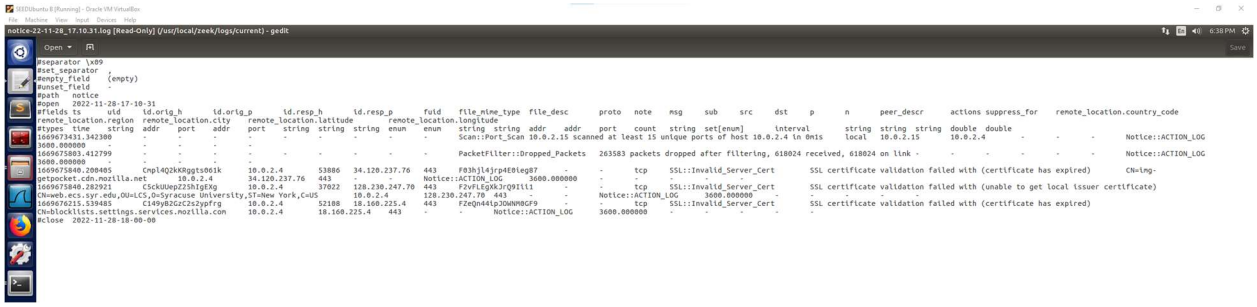
When looking through the logs I was able to find a log titled http-22-11-28_17.12.11.log and when opening it and inspecting the contents, I was able to see the SYN Flooding Attack logged in this file. It shows the SYN packets coming through to port 80, the second screenshot from the weird log also shows that the SYN packets were being detected from the spoofed IPs and was also reporting with inappropriate_FIN. These log files contain interesting data about where the packets were coming from and what happened with them showing that a SYN Flood Attack took place.



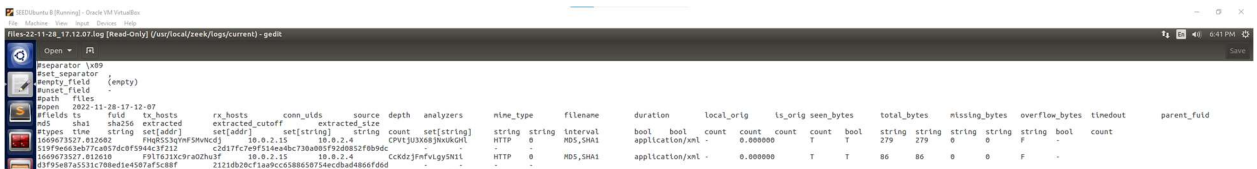


Browsing http Websites:

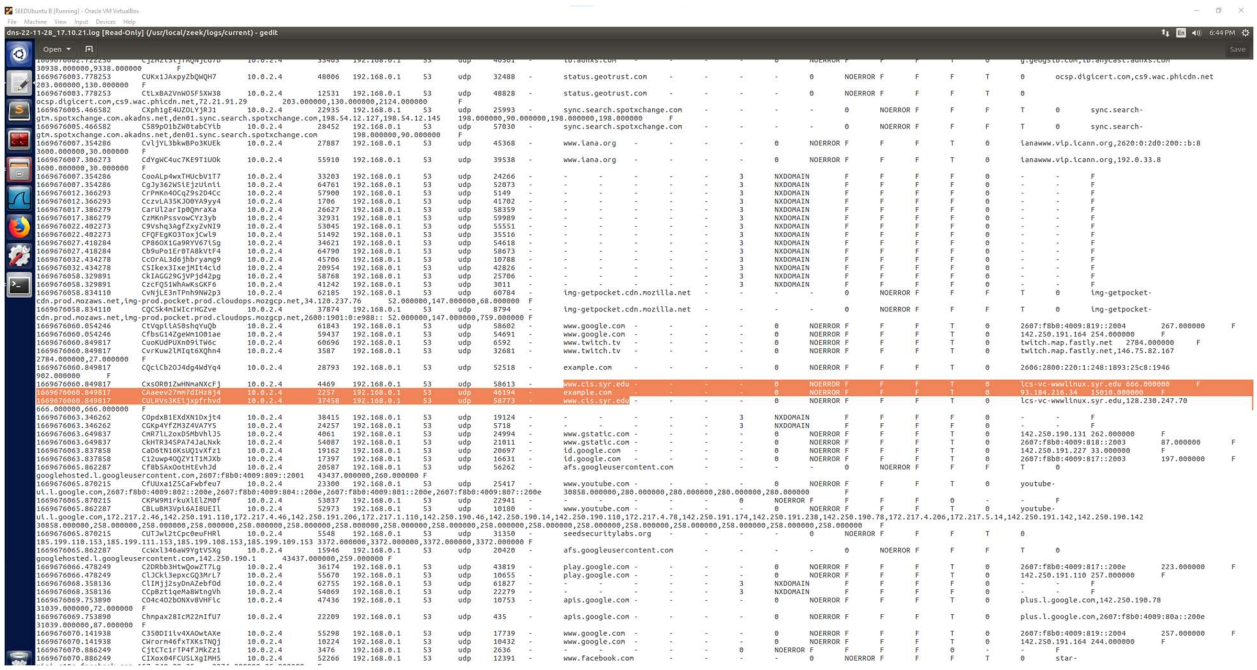
When looking through the logs for any information about browsing to http websites on the Zeek VM, in the notice log I saw one of the web addresses that I had navigated to, and that the SSL certification validation failed. This is interesting information because the log shows that the http webserver reported as being unable to get the local issuer certificate for that web address.



In one of the log files, it also showed some HTTP and SSL reports that could be attributed to the browsing, I am unsure as if this is the case but from a first look it is possible that it could be related to those connections to http webservers instead of https.



I also saw some of the website addresses listed in the dns log as seen below.



I think that the Zeek VM logs were able to provide some interesting information about the attacks. With the SYN Flood Attack, even though the IP addresses were spoofed and random, they were reported, and the log indicated that a SYN Flood Attack was taking place on port 80 and the packets were being left open. By looking through the logs and gathering this information, a user could defend against that attack by changing their firewall ruleset to block outside IP addresses other than the IP addresses that should be allowed through(whitelist). The nmap scan was also logged by the Zeek VM and with this one I am unsure of what kind of information was reported other than being able to tell that the nmap command was run from the attacker VM's IP address and that they were scanning the ports. To combat this, the user could block the attacker's IP address on the firewall. However, that will only be successful if the attacker's IP address is true. It could also prompt the user to ensure that the ports that are open are necessary and properly protected. I think that the notice log provided some interesting information about the web browsing because it logged what website was failing validation and why it was missing that certificate validation (expired or unable to find). I was really surprised with just the sheer amount of information that was collected by Zeek and I am sure that there is information that would be valuable in ways that I haven't learned yet. I think that the logs created by Zeek are a powerful tool to gather information on the traffic between the Zeek VM and outside machines/systems. It can also be used in this case to identify the target port of a SYN Flood Attack, that an attack is occurring, and possibly identify where it is coming from. The logs were also able to provide insight if a website had a valid certificate, so the user could check the logs to see what connections they may have had when browsing the web that resulted in browsing a website that was not secure.