

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

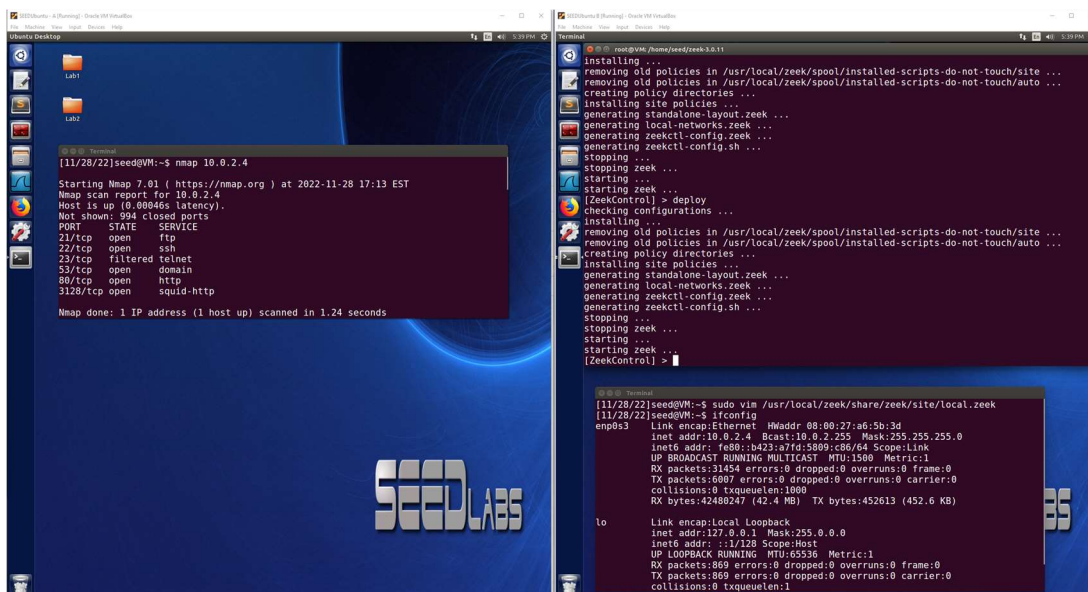
A is the attacker and B is the Zeek VM

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



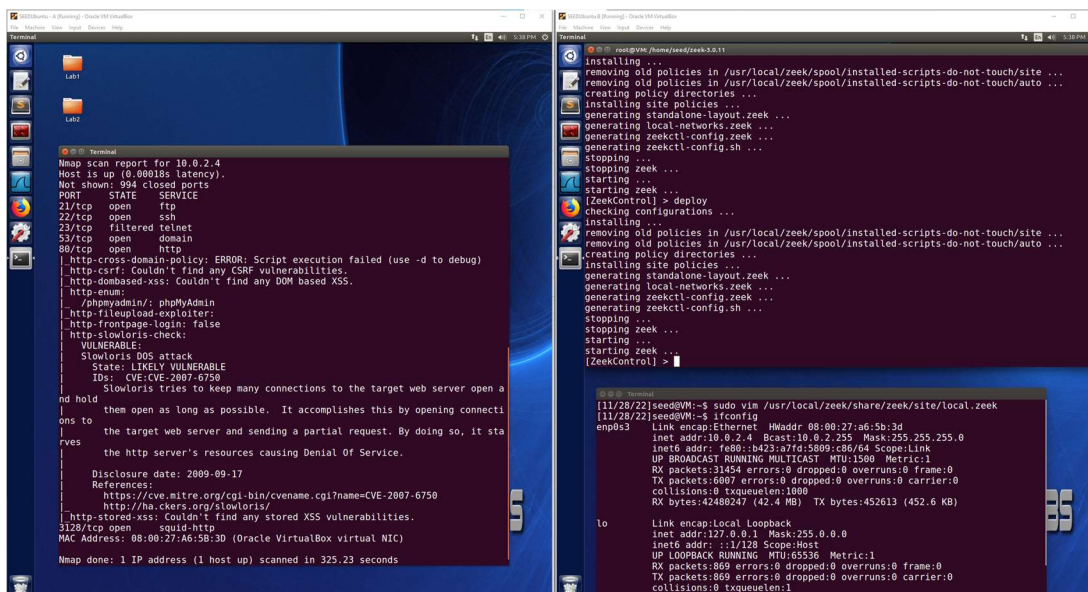
The image shows two terminal windows. The left window displays the output of an nmap scan on 10.0.2.4, showing open ports 21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 53/tcp (domain), 80/tcp (http), and 3128/tcp (squid-http). The right window shows the Zeek installation process, including the removal of old policies, creation of policy directories, and the generation of Zeek configuration files.

```
[11/28/22]seed@VM:~$ nmap 10.0.2.4
Starting Nmap 7.81 ( https://nmap.org ) at 2022-11-28 17:13 EST
Nmap scan report for 10.0.2.4
Host is up (0.00046s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    filtered telnet
53/tcp    open  domain
80/tcp    open  http
3128/tcp  open  squid-http
Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds
```

```
installing ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping zeek ...
starting ...
starting zeek ...
[ZeekControl] > deploy
checking configurations ...
installing ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping zeek ...
starting ...
starting zeek ...
[ZeekControl] >
```

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



The image shows two terminal windows. The left window displays the output of an nmap vulnerability scan on 10.0.2.4, showing open ports 21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 53/tcp (domain), 80/tcp (http), and 3128/tcp (squid-http). The right window shows the Zeek installation process, including the removal of old policies, creation of policy directories, and the generation of Zeek configuration files.

```
Nmap scan report for 10.0.2.4
Host is up (0.00015s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    filtered telnet
53/tcp    open  domain
80/tcp    open  http
3128/tcp  open  squid-http
Nmap done: 1 IP address (1 host up) scanned in 325.23 seconds
```

```
http-cross-domain-policy: ERROR: Script execution failed (use -d to debug)
http-csrf: Couldn't find any CSRF vulnerabilities.
http-dombased-xss: Couldn't find any DOM based XSS.
http-enumer:
  /phpmyadmin/: phpMyAdmin
  http-fileupload-exploiter:
  http-frontpage-login: false
http-slowloris-check:
  VULNERABLE:
    Slowloris DOS attack
    State: LIKELY VULNERABLE
    IDS: CVE:CVE-2007-6750
    Slowloris tries to keep many connections to the target web server open a
nd hold
them open as long as possible. It accomplishes this by opening connecti
ons to
the target web server and sending a partial request. By doing so, it sta
rves
the http server's resources causing Denial Of Service.
Disclosure date: 2009-09-17
References:
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
  http://ha.ckers.org/slowloris/
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
3128/tcp open squid-http
MAC Address: 08:00:27:A6:5B:3D (Oracle VirtualBox virtual NIC)
```

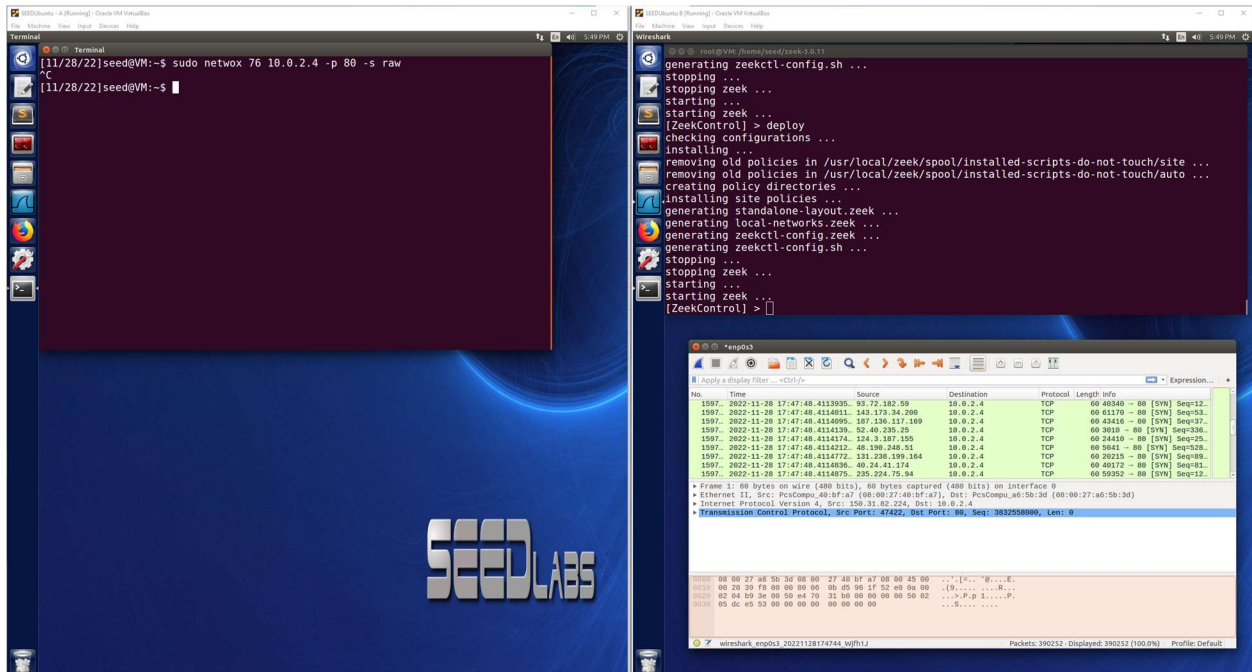
```
installing ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping zeek ...
starting ...
starting zeek ...
[ZeekControl] >
```

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:

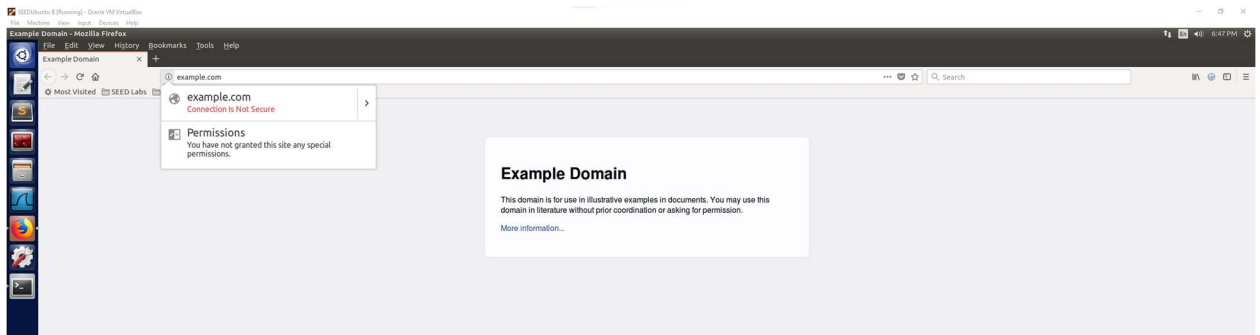
```
sudo netwox 76 -i 10.0.2.4 -p 80 -s raw
```

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.

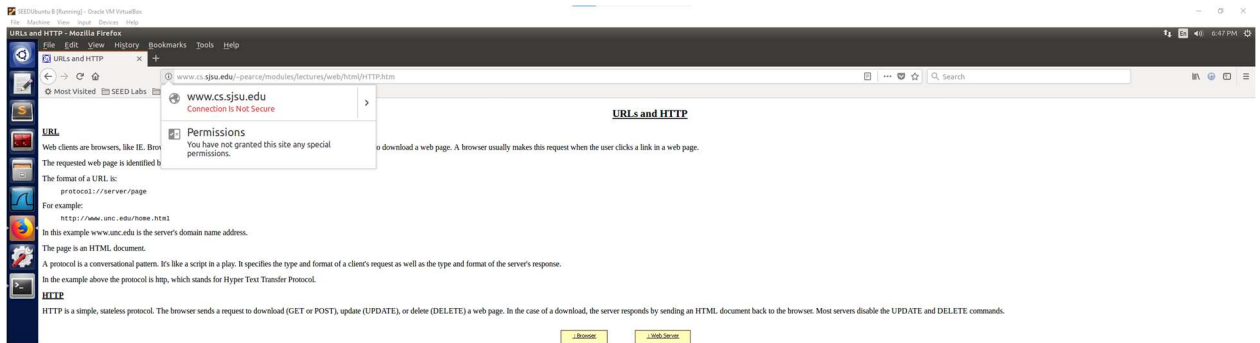


(2) Websites browsed to

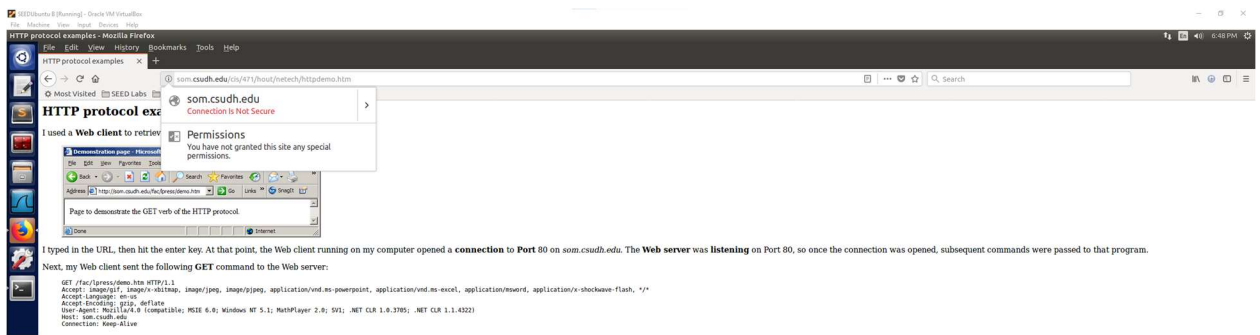
<http://example.com/>



<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.

[illegible]

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.

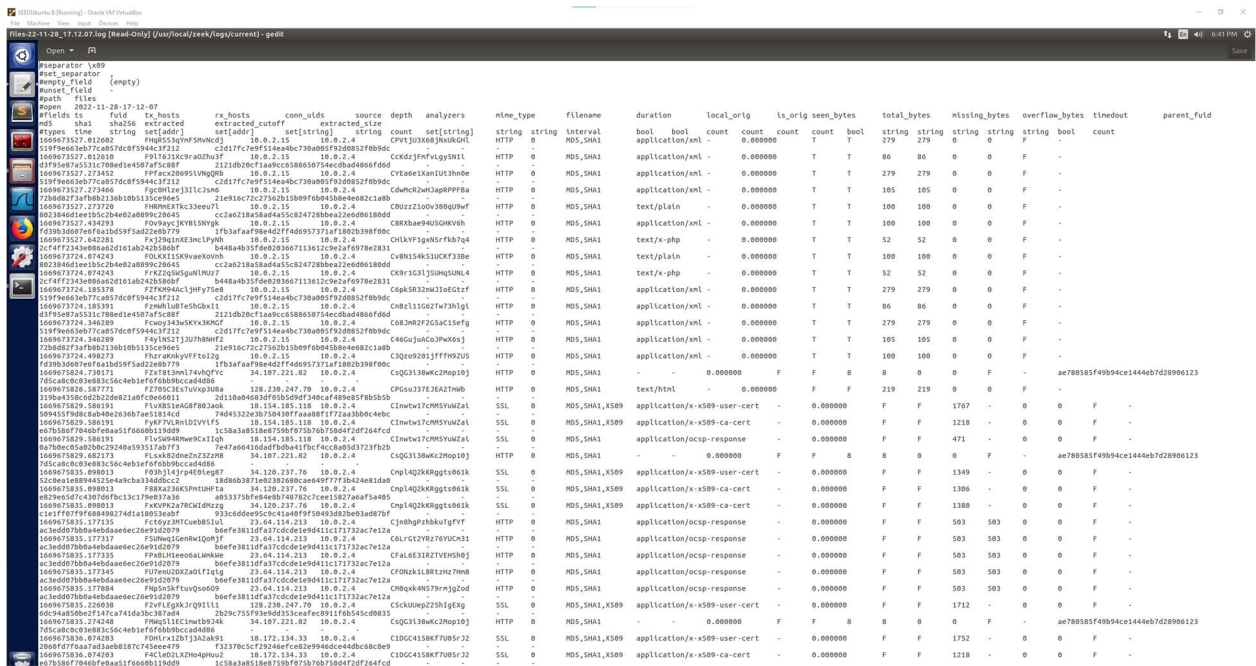
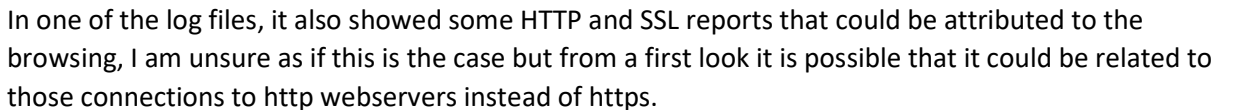
[illegible]

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.

[illegible]

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.



66-22-11-28_17.12.13log (Read-Only) (Vue/col/2ee/foq/current) - edit										6:44 PM Save									
Open																			
19938.00000,139.00000	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	g-gopertnet.com,mykash.com
19938.00000,17825.1	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	ecsp.digicert.com,c9.wa.phicdn.net
19938.00000,138.00000	CLCk2b3p3yqoqH7	19.0-2.4	12531	192.168.0.1	53	udp	48028	-	-	-	0	NOERR	F	F	F	T	0	-	-
19938.00000,17825.1	CLCk2b3p3yqoqH7	19.0-2.4	12531	192.168.0.1	53	udp	48028	-	-	-	0	NOERR	F	F	F	T	0	-	-
19938.00000,139.00000	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,17825.1	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,139.00000	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,17825.1	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,139.00000	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,17825.1	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,139.00000	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,17825.1	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,139.00000	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,17825.1	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,139.00000	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,17825.1	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,139.00000	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,17825.1	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,139.00000	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,17825.1	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-
19938.00000,139.00000	Cgicq3l3p3yqoqH7	19.0-2.4	48006	192.168.0.1	53	udp	32488	-	-	-	0	NOERR	F	F	F	T	0	-	sync-search-</

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.