

## Lab 6 – Part 1

Gunnar Yonker

### Part 1:

VM A: 10.0.2.6

VM B(Zeek): 10.0.2.4

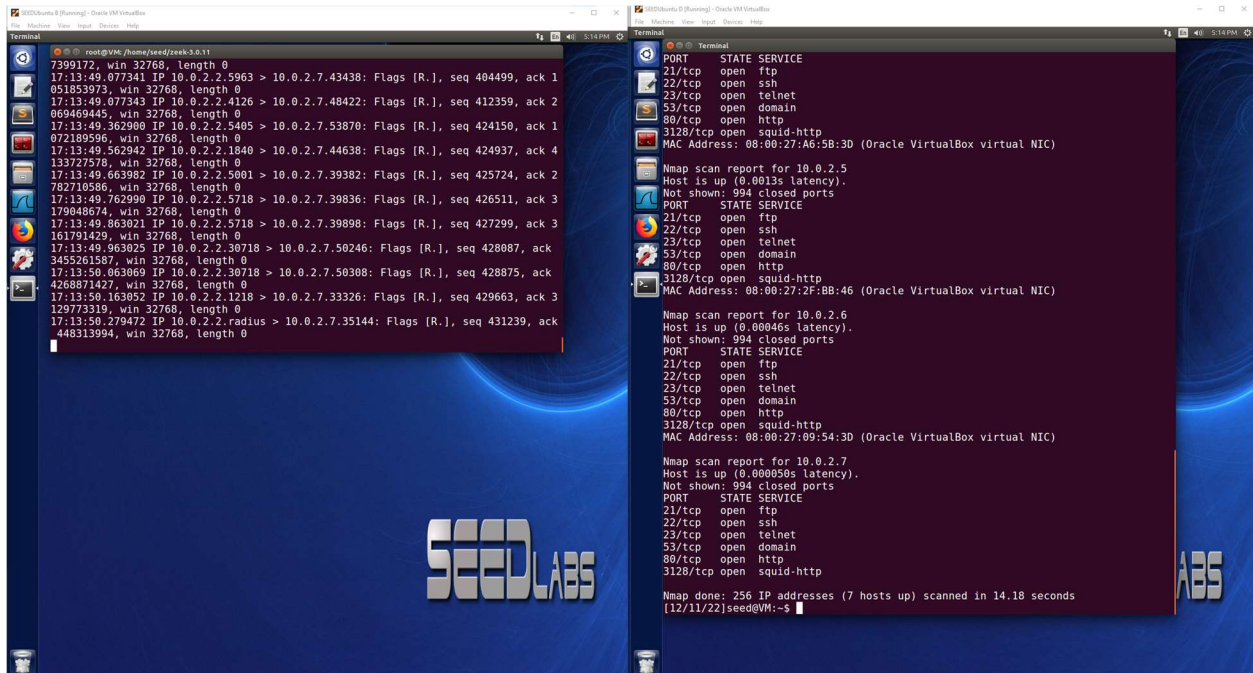
VM C: 10.0.2.5

VM D(being treated as outside attacker): 10.0.2.7

I couldn't seem to get my personal pc to detect hosts being up on the subnet of my VMs, so to show the steps of the lab out outlined in the lab introduction I will be simulating this outside attacker as VM D but still located on the same subnet.

Outside VM: 192.168.56.1

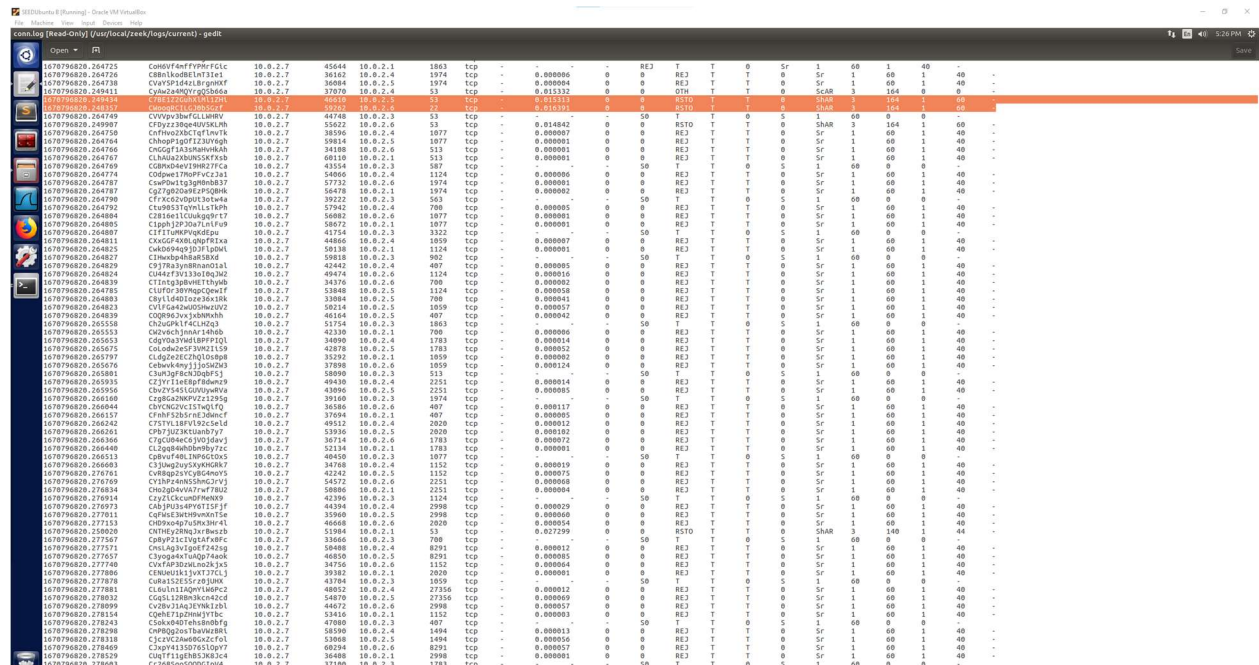
nmap -sT 10.0.2.0/24 and Zeek VM running tcpdump



Command for SYN Flood Attack on 10.0.2.6 using port 80 which is open according to the nmap scan

sudo netwox 76 -i 10.0.2.6 -p 80 -s raw

The conn.log file provides some really good information about the nmap scan on the subnet, in the image below it shows that the nmap scan was coming from VM D(10.0.2.7) and checking the ports on the 10.0.2.0/24 subnet so each connection attempt is shown in this log for each of the port scans. The highlighted rows show that on 10.0.2.5 port 53 that the response logged is RSTO which means that tcp port is open. Also 10.0.2.6 port 22 has the RSTO response instead of being rejected(REJ) which also shows in the log what ports were found to be open that the attacker now knows about.



10.0.2.7	10.0.2.7	45644	10.0.2.1	1863	tcp	-	0.000000	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	36162	10.0.2.4	1974	tcp	-	0.000000	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	36084	10.0.2.5	1974	tcp	-	0.000004	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	37070	10.0.2.4	53	tcp	-	0.01332	0	0	OTF	T	T	0	Sr	3	164	0	-	-
10.0.2.7	10.0.2.7	40176	10.0.2.5	53	tcp	-	0.01332	0	0	OTF	T	T	0	Sr	3	164	0	-	-
10.0.2.7	10.0.2.7	44748	10.0.2.3	53	tcp	-	0.01332	0	0	OTF	T	T	0	Sr	3	164	0	-	-
10.0.2.7	10.0.2.7	53622	10.0.2.6	53	tcp	-	0.014842	0	0	RSTO	T	T	0	Sr	3	164	1	60	-
10.0.2.7	10.0.2.7	38396	10.0.2.4	1077	tcp	-	0.000007	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	59814	10.0.2.5	1077	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	34188	10.0.2.6	513	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	48110	10.0.2.1	513	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	43354	10.0.2.3	187	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	54866	10.0.2.4	1124	tcp	-	0.000000	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	57732	10.0.2.6	1974	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	56478	10.0.2.1	1974	tcp	-	0.000002	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	39222	10.0.2.3	1077	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	57942	10.0.2.4	708	tcp	-	0.000005	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	56882	10.0.2.6	1077	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	58572	10.0.2.1	1077	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	41754	10.0.2.3	1077	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	44866	10.0.2.4	1059	tcp	-	0.000007	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	43442	10.0.2.3	1077	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	59818	10.0.2.3	902	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	42442	10.0.2.4	407	tcp	-	0.000005	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	49474	10.0.2.6	1124	tcp	-	0.000010	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	3874	10.0.2.4	1124	tcp	-	0.000002	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	53840	10.0.2.5	1124	tcp	-	0.000050	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	33084	10.0.2.5	708	tcp	-	0.000041	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	58214	10.0.2.5	1059	tcp	-	0.000057	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	51754	10.0.2.3	1863	tcp	-	0.000042	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	42330	10.0.2.1	708	tcp	-	0.000004	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	34990	10.0.2.4	1703	tcp	-	0.000004	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	42878	10.0.2.5	1703	tcp	-	0.000052	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	31392	10.0.2.1	1059	tcp	-	0.000002	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	37898	10.0.2.6	1059	tcp	-	0.000124	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	58990	10.0.2.3	513	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	49430	10.0.2.4	2251	tcp	-	0.000014	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	43096	10.0.2.5	2251	tcp	-	0.000005	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	39160	10.0.2.3	1974	tcp	-	0.000117	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	36386	10.0.2.6	407	tcp	-	0.000005	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	37694	10.0.2.1	2251	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	49312	10.0.2.4	2020	tcp	-	0.000012	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	53936	10.0.2.5	2020	tcp	-	0.000102	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	36714	10.0.2.6	1703	tcp	-	0.000072	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	52134	10.0.2.1	1703	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	48450	10.0.2.3	1077	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	34760	10.0.2.4	1152	tcp	-	0.000019	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	42142	10.0.2.5	1152	tcp	-	0.000075	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	54572	10.0.2.6	2251	tcp	-	0.000060	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	35960	10.0.2.5	2251	tcp	-	0.000004	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	42390	10.0.2.3	1124	tcp	-	0.000029	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	40394	10.0.2.4	2998	tcp	-	0.000000	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	35960	10.0.2.5	2998	tcp	-	0.000000	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	46868	10.0.2.6	2020	tcp	-	0.000004	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	51984	10.0.2.1	53	tcp	-	0.027299	0	0	RSTO	T	T	0	Sr	3	140	1	44	-
10.0.2.7	10.0.2.7	33666	10.0.2.3	708	tcp	-	0.000012	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	58400	10.0.2.4	8291	tcp	-	0.000012	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	44850	10.0.2.5	8291	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	34756	10.0.2.6	1152	tcp	-	0.000004	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	39382	10.0.2.1	2020	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	43784	10.0.2.3	1059	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	48032	10.0.2.4	27356	tcp	-	0.000012	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	54878	10.0.2.5	27356	tcp	-	0.000009	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	44672	10.0.2.6	2998	tcp	-	0.000007	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	53416	10.0.2.1	1152	tcp	-	0.000003	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	47800	10.0.2.3	407	tcp	-	0.000013	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	58390	10.0.2.5	1494	tcp	-	0.000013	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	53068	10.0.2.5	1494	tcp	-	0.000056	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	60284	10.0.2.6	8291	tcp	-	0.000057	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	36400	10.0.2.1	2998	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-
10.0.2.7	10.0.2.7	37180	10.0.2.3	1703	tcp	-	0.000001	0	0	REJ	T	T	0	Sr	1	60	1	40	-

The image below is important regarding the nmap scan in relation to the following SYN Flood attack. This is because the scan information logged shows that the attack was able to find on 10.0.2.6 that port 80 was open and potentially vulnerable to a SYN Flood attack on that machine. This is the information that an attack could use to carry out that attack on port 80 or any of the other open tcp ports that the nmap scan found, which the conn.log file shows what IP address the scans were originating from and what machines were found with open ports.

[illegible]

Looking through the other logs created by Zeek there is not anything additional that stands out in terms of indicating that there was an attack other than in the conn.log. The weird.log, image below, shows that the attacking VM 10.0.2.7 accessed port 80 and the message of bad\_tcp\_checksum could show that there was a potential attack taking place in relation to the attack on port 80, but there is no additional information in terms of the machine that was suffering from the attack.



My thoughts on how effectively Zeek was able to detect any unusual activity is that it did not explicitly point out any information in the logs that I saw. I would've expected some information on the SYN Flood Attack to be located in the weird.log file but did not find much in that log file, the other log files also did not contain any information that clearly pointed out an attack from 10.0.2.7 on 10.0.2.6 through port 80 other than the conn.log file. It was very evident with the nmap and the SYN Flood attack in the conn.log file what was happening, but it also required the user to scroll through large amounts of data since every piece of information was logged into that file. A human reader could clearly look at the conn.log file to see that there was an attack taking place on the 10.0.2.6 VM, but I did not see any information automatically separated in the log files by Zeek detecting any anomalies on it's own. Zeek is very useful in it's default script that all of the information is logged and a human user could analyze that to see patterns or indications of an attack. However, it was not apparent that Zeek on it's own was able to differentiate using the default script that an attack was taking place or even that there was anything abnormal taking place that could be considered an anomaly. From this part of the lab my current takeaway is that the default script that Zeek runs when logging all of the information is really useful when it will be sorted through by a human user, but that Zeek on its own as a detection method for anomalous activity did not show that it would log something like a SYN Flood attack as a separate detection from normal traffic.

The only information that I think could also be attributed to the attack is in the capture\_loss.log where the line highlighted shows that there was a high number of acks and gaps at a certain timestamp, but this does not directly associate any other information with an attack.

