



ÉCOLE POLYTECHNIQUE DE LOUVAIN

LINGI2347 - COMPUTER SYSTEM SECURITY

## Project 1 - Group 19

*Berton Thomas 7260-14-00*  
*Delaunoy Valentin 5254-14-00*

Professor : Sadre Ramin

April 21, 2018

## Question 0

We are the group 19.

## Question a

The company network has the address 93.169.1.0/16 and the company is called Saudi. After some researches on the Internet, we learned that in 2015, twelve percent of Saudi companies were targeted with distributed denial of service (DDoS) attacks, says a study conducted by Kaspersky Lab<sup>1</sup>.

## Question b

After analyzing the pcap file with *Wireshark*, we conclude that it contains no more than 196 415 different addresses. Here are the following 7 hosts in the company network, with their respective number of occurrences and their function .

	Host	Number of occurrences	function
1	93.169.182.233	148 511 (75.61%)	DNS Server
2	93.169.112.145	21 228 (10.81 %)	Web Server
3	93.169.128.62	14 225 (7.24 %)	Web Server
4	93.169.160.153	11 856 (6.04 %)	Web Server
5	93.169.49.97	4221 (2.15 %)	End Host
6	93.169.156.76	1340 (0.68 %)	End Host
7	93.169.59.9	613 (0.31 %)	End Host

We concluded that 3 hosts are Web server since they are only used via the port 80 for HTTP. We also have a DNS server which is the target of the first attack we found. And there are three remaining end hosts which are probably employee workstations.

## Question c

1. Start time of attack : the first peak appears at the 126<sup>th</sup> second, i.e. 2 min 06 sec.
2. Duration : attack ends up at the 151<sup>th</sup> second (i.e. 2min 31sec.), so it lasted 24 seconds.
3. Number of attacking IP addresses : 87 different addresses.
4. Average number of attack packets per second : 6050 packets/second.
5. Short attack description : as we can clearly observe it in the figure 1, there is a massive number of DNS packets that were transmitted to the server of the network company. We are facing here a DNS Amplification DDoS Attack using ANY query for the amplification. Indeed ANY queries ask the DNS server to return all information it knows about a domain. This is a very popular method to amplify attacks because of the high amplification factor. By analyzing the destination of those DNS packets, we remarked that 99.81 % of them were directed to the 93.169.182.233 IP address which is the DNS server of the company.

---

<sup>1</sup><http://www.arabnews.com/node/932371/saudi-arabia>

17320 126.581000	82.241.5.201	93.169.182.233	DNS	3231 Standard query response 0x280d[Packet size limited during capture]
17321 126.581000	82.241.5.201	93.169.182.233	DNS	3231 Standard query response 0x6831[Packet size limited during capture]
17327 126.582000	82.241.5.201	93.169.182.233	DNS	3231 Standard query response 0x14c6[Packet size limited during capture]
17330 126.586000	77.168.206.54	93.169.182.233	DNS	122 Standard query response 0x7e2c ANY isc.org[Packet size limited during capture]
17339 126.590000	186.213.93.136	93.169.182.233	DNS	532 Standard query response 0x696c ANY isc.org[Packet size limited during capture]
17340 126.591000	186.213.93.136	93.169.182.233	DNS	532 Standard query response 0x5c5d ANY isc.org[Packet size limited during capture]
17341 126.591000	77.168.206.54	93.169.182.233	DNS	122 Standard query response 0x7e2c ANY isc.org[Packet size limited during capture]

Figure 1: Observe here the DNS ANY queries in the beginning of the attack

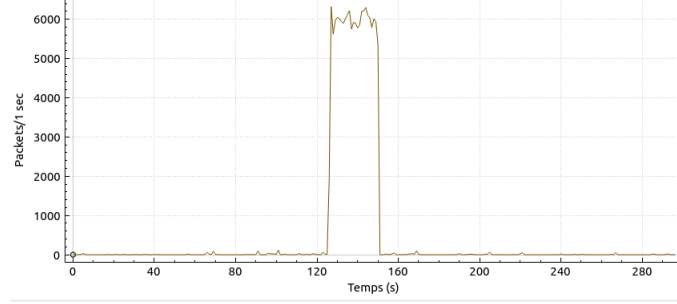


Figure 2: Network activity in terms of DNS packets per second

## Question d

1. Start time of attack : attack starts at 144<sup>th</sup> second, i.e. 2 min 22 seconds.
2. Duration : the end of the attack is observed at the 192<sup>th</sup> second, i.e. 3 min 12 seconds. So it lasted 48 seconds
3. Number of attacking IP addresses : 3204 different attacks
4. Average number of attack packets per second : 67 packets/second
5. Short attack description : for this second attack, we observe that someone is attempting a TCP reset attack. According to Wikipedia, a *TCP Reset Attack*, also known as *Forged TCP Resets*<sup>2</sup>, is a way to tamper and terminate the Internet connection between two hosts by sending forged TCP reset packet. In other terms, the attacker hijack a TCP session and sends packets with RST Flag *ON* to both hosts or any one of them. Since they ignored that there is an abnormal intruder they treat these packets normally. But they are reset packets so connection between A and B is terminated.

No.	Time	Source	Destination	Protocol	Length	Info
138149	144.727000	130.209.68.167	93.169.128.62	TCP	60	31851 → 80 [RST] Seq=1 Win=0 L.
138195	144.734000	100.105.145.73	93.169.128.62	TCP	60	16557 → 80 [RST] Seq=1 Win=0 L.
138236	144.740000	70.30.54.97	93.169.128.62	TCP	60	20979 → 80 [RST] Seq=1 Win=0 L.
138297	144.752000	105.62.181.248	93.169.128.62	TCP	60	24262 → 80 [RST] Seq=1 Win=0 L.
138341	144.759000	181.86.86.191	93.169.128.62	TCP	60	15093 → 80 [RST] Seq=1 Win=0 L.
138386	144.765000	99.154.197.198	93.169.128.62	TCP	60	31688 → 80 [RST] Seq=1 Win=0 L.
138473	144.779000	107.209.93.177	93.169.128.62	TCP	60	26391 → 80 [RST] Seq=1 Win=0 L.
138514	144.785000	92.161.8.126	93.169.128.62	TCP	60	20955 → 80 [RST] Seq=1 Win=0 L.
138624	144.794000	88.108.121.184	93.169.128.62	TCP	60	29937 → 80 [RST] Seq=1 Win=0 L.
138682	144.802000	163.11.177.96	93.169.128.62	TCP	60	12082 → 80 [RST] Seq=1 Win=0 L.
138779	144.814000	98.253.162.107	93.169.128.62	TCP	60	34279 → 80 [RST] Seq=1 Win=0 L.
138804	144.819000	161.96.177.17	93.169.128.62	TCP	60	11715 → 80 [RST] Seq=1 Win=0 L.
138868	144.827000	73.16.226.243	93.169.128.62	TCP	60	19501 → 80 [RST] Seq=1 Win=0 L.
138960	144.839000	104.183.221.144	93.169.128.62	TCP	60	30466 → 80 [RST] Seq=1 Win=0 L.
139036	144.847000	172.207.152.12	93.169.128.62	TCP	60	16443 → 80 [RST] Seq=1 Win=0 L.
139092	144.854000	140.2.83.115	93.169.128.62	TCP	60	29506 → 80 [RST] Seq=1 Win=0 L.
139358	144.877000	69.40.176.177	93.169.128.62	TCP	60	23181 → 80 [RST] Seq=1 Win=0 L.
139401	144.880000	115.29.188.85	93.169.128.62	TCP	60	23037 → 80 [RST] Seq=1 Win=0 L.
139480	144.890000	140.106.158.30	93.169.128.62	TCP	60	20216 → 80 [RST] Seq=1 Win=0 L.
139496	144.893000	145.119.121.68	93.169.128.62	TCP	60	25064 → 80 [RST] Seq=1 Win=0 L.
139555	144.905000	93.33.176.97	93.169.128.62	TCP	60	20642 → 80 [RST] Seq=1 Win=0 L.
139600	144.907000	162.71.58.250	93.169.128.62	TCP	60	24637 → 80 [RST] Seq=1 Win=0 L.
139614	144.909000	120.96.142.51	93.169.128.62	TCP	60	11315 → 80 [RST] Seq=1 Win=0 L.
139641	144.912000	113.121.241.238	93.169.128.62	TCP	60	16301 → 80 [RST] Seq=1 Win=0 L.
139695	144.920000	82.98.192.219	93.169.128.62	TCP	60	26361 → 80 [RST] Seq=1 Win=0 L.

Figure 3: Sample of the reset attack against web server 93.169.128.62

<sup>2</sup>or still *Spoofed TCP reset packets*

As we can see in the Figure 4, the 93.169.128.62 server has to deal with a lot of received *tcp* packets (blue peaks) but returns a small number of sent packets (red peaks). This explains why we thought about a *SYN flood* attack at a first sight. But section between 2 min 22 seconds and 3 min 12 seconds couldn't be explained in that way. After analyzing packets through *Wireshark* (Figure 3) and doing some researches on the Internet, we opted for a *TCP Reset Attack* : number of packets is increasing due to closing connections (4 packets needed to end up the connexion).

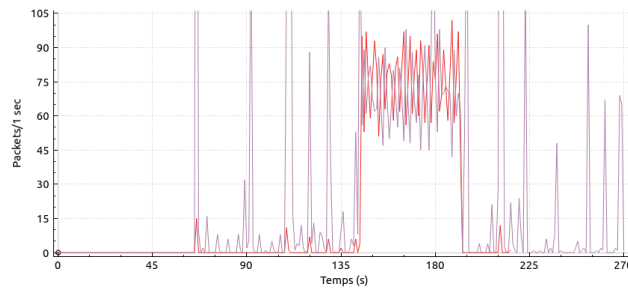


Figure 4: Web server response : Network activity in terms of TCP packets via HTTP application

No.	Time	Source	Destination	Protocol	Length	Info
190541	188.887000	93.169.128.62	96.201.174.221	TCP	74	80 → 12420 [SYN, ACK] Seq=0 Ac...
190542	188.895000	93.169.128.62	89.76.127.184	TCP	74	80 → 33126 [SYN, ACK] Seq=0 Ac...
190543	188.902000	93.169.128.62	186.138.206.6	TCP	58	80 → 12204 [SYN, ACK] Seq=0 Ac...
190544	188.913000	93.169.128.62	160.230.137.178	TCP	74	80 → 25665 [SYN, ACK] Seq=0 Ac...
190545	188.917000	93.169.128.62	116.199.180.104	TCP	74	80 → 32636 [SYN, ACK] Seq=0 Ac...
190546	188.919000	93.169.128.62	174.130.155.255	TCP	58	80 → 33906 [SYN, ACK] Seq=0 Ac...
190547	188.921000	93.169.128.62	182.217.100.254	TCP	74	80 → 24120 [SYN, ACK] Seq=0 Ac...
190548	188.926000	93.169.128.62	157.161.4.16	TCP	74	80 → 17365 [SYN, ACK] Seq=0 Ac...
190549	188.930000	93.169.128.62	140.8.243.225	TCP	74	80 → 32640 [SYN, ACK] Seq=0 Ac...
190550	188.942000	93.169.128.62	98.124.222.156	TCP	74	80 → 10115 [SYN, ACK] Seq=0 Ac...
190551	188.947000	93.169.128.62	73.114.164.50	TCP	74	80 → 31530 [SYN, ACK] Seq=0 Ac...
190552	188.954000	93.169.128.62	89.202.62.229	TCP	74	80 → 13979 [SYN, ACK] Seq=0 Ac...
190553	188.959000	93.169.128.62	108.213.13.67	TCP	58	80 → 26644 [SYN, ACK] Seq=0 Ac...
190554	188.970000	93.169.128.62	104.183.214.144	TCP	74	80 → 10523 [SYN, ACK] Seq=0 Ac...
190555	188.972000	93.169.128.62	108.185.222.74	TCP	74	80 → 32521 [SYN, ACK] Seq=0 Ac...
190556	188.984000	93.169.128.62	124.49.186.173	TCP	58	80 → 25373 [SYN, ACK] Seq=0 Ac...
190557	188.996000	93.169.128.62	115.239.178.110	TCP	74	80 → 21229 [SYN, ACK] Seq=0 Ac...
190558	188.998000	93.169.128.62	140.0.21.86	TCP	58	80 → 28635 [SYN, ACK] Seq=0 Ac...
190559	189.000000	93.169.128.62	67.198.236.163	TCP	58	80 → 12675 [SYN, ACK] Seq=0 Ac...
190577	189.000000	93.169.128.62	153.65.19.182	TCP	58	80 → 10577 [SYN, ACK] Seq=0 Ac...
190585	189.140000	93.169.128.62	78.237.43.168	TCP	74	80 → 27005 [SYN, ACK] Seq=0 Ac...
190588	189.165000	93.169.128.62	136.154.14.146	TCP	58	80 → 13637 [SYN, ACK] Seq=0 Ac...
190603	189.269000	93.169.128.62	72.232.176.146	TCP	74	80 → 34640 [SYN, ACK] Seq=0 Ac...
190614	189.342000	93.169.128.62	78.222.86.129	TCP	58	80 → 24338 [SYN, ACK] Seq=0 Ac...
190624	189.422000	93.169.128.62	159.159.125.221	TCP	74	80 → 18003 [SYN, ACK] Seq=0 Ac...

Figure 5: Responses of the same web server to different addresses on different ports

## Question e

Doing some analysis with the flow records generated through *Yaf*, we couldn't understand what was the APF flag in the *txt* file containing the flow records. We thus checked on the web to discover that it was the way we will resolve *Question e*.

Indeed every hosts that access the company's servers in a legitimate way (i.e. no attack) must have this flag while he's communicating with the company's network services. According to the IBM's article we found : "The authorized program facility (APF) allows your installation to identify system or user programs that can use sensitive system functions."<sup>3</sup>

<sup>3</sup>[https://www.ibm.com/support/knowledgecenter/en/SSLTBW\\_2.1.0/com.ibm.zos.v2r1.bpxb200/hfsapf.html](https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.bpxb200/hfsapf.html)

Here are the legal hosts we found using APF flag:

1. 85.235.98.126
2. 139.83.107.81
3. 119.2.247.82
4. 83.54.13.172
5. 102.173.200.69
6. 107.25.174.237
7. 156.236.113.119
8. 149.179.18.51
9. 177.124.25.121
10. ...

They are many more addresses but for the sake of space, we just put a sample of them.

## Analysis

We analyzed the packet with *Snort* but the results were disappointing. Indeed 86 % of the packets were discarded due to the lack of the payload. Another portions of the packets were discarded due to a bad checksum error. So the IDS Snort was useless.

In consequence, we analyze the packet through *Wireshark* and we were able to find meaningful information. Indeed the statistics panel shows that the intensity of the network had increased significantly near the second minute after the launch of the network measurement. This was the first clue for the two attacks we had to find.

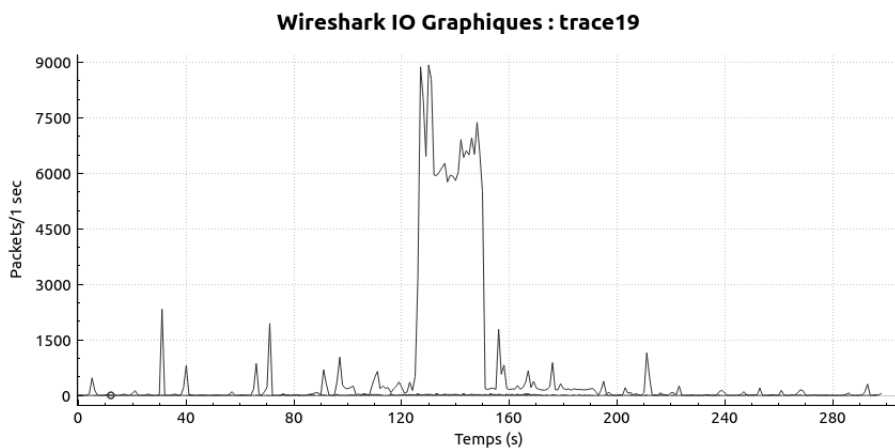


Figure 6: Graphical representation of *pcap* file, showing the network activity in packets per second

To gather more information about the hosts and their activity/exchanges, we also used *Yaf* to generate flow records of the *pcap* file.

```

1970-01-01 00:02:07.439 - 00:02:31.629 (24.190 sec) udp 105.241.51.174:53 => 93.169.182.233:80 (1307/568407 ->) eof
1970-01-01 00:02:07.780 - 00:02:31.631 (23.851 sec) udp 74.18.70.60:53 => 93.169.182.233:80 (1307/568407 ->) eof
1970-01-01 00:02:07.491 - 00:02:31.632 (24.141 sec) udp 173.193.20.40:53 => 93.169.182.233:80 (2941/6822750 ->) eof
1970-01-01 00:02:07.603 - 00:02:31.633 (24.030 sec) udp 103.119.45.143:53 => 93.169.182.233:80 (430/142760 ->) eof
1970-01-01 00:02:07.506 - 00:02:31.634 (24.048 sec) udp 155.8.252.12:53 => 93.169.182.233:80 (1621/5121901 ->) eof
1970-01-01 00:02:07.652 - 00:02:31.634 (23.982 sec) udp 101.38.64.49:53 => 93.169.182.233:80 (2953/9470722 ->) eof
1970-01-01 00:02:07.562 - 00:02:31.635 (24.073 sec) udp 170.58.171.177:53 => 93.169.182.233:80 (2540/5816632 ->) eof
1970-01-01 00:02:07.574 - 00:02:31.635 (24.061 sec) udp 91.127.197.75:53 => 93.169.182.233:80 (2315/6442583 ->) eof
1970-01-01 00:02:07.572 - 00:02:31.635 (24.063 sec) udp 185.206.237.135:53 => 93.169.182.233:80 (425/220150 ->) eof
1970-01-01 00:02:07.545 - 00:02:31.635 (24.090 sec) udp 68.110.229.135:53 => 93.169.182.233:80 (5360/16019168 ->) eof
1970-01-01 00:02:07.593 - 00:02:31.635 (24.042 sec) udp 154.104.106.89:53 => 93.169.182.233:80 (3140/1965170 ->) eof
1970-01-01 00:02:07.454 - 00:02:31.636 (24.182 sec) udp 145.210.136.251:53 => 93.169.182.233:80 (3765/1250502 ->) eof
1970-01-01 00:02:07.516 - 00:02:31.636 (24.120 sec) udp 93.200.223.114:53 => 93.169.182.233:80 (834/131296 ->) eof
1970-01-01 00:02:07.498 - 00:02:31.636 (24.138 sec) udp 127.39.146.142:53 => 93.169.182.233:80 (2046/6814040 ->) eof
1970-01-01 00:02:07.294 - 00:02:31.637 (24.343 sec) udp 82.241.5.201:53 => 93.169.182.233:80 (5810/7264381 ->) eof
1970-01-01 00:02:07.533 - 00:02:31.637 (24.104 sec) udp 118.198.227.8:53 => 93.169.182.233:80 (2245/7317364 ->) eof
1970-01-01 00:02:07.689 - 00:02:31.637 (23.948 sec) udp 112.154.72.179:53 => 93.169.182.233:80 (2552/1832872 ->) eof
1970-01-01 00:02:07.314 - 00:02:31.637 (24.323 sec) udp 186.213.93.136:53 => 93.169.182.233:80 (1078/558404 ->) eof
1970-01-01 00:02:07.708 - 00:02:31.638 (23.850 sec) udp 120.11.184.201:53 => 93.169.182.233:80 (1171/3134636 ->) eof
1970-01-01 00:02:07.624 - 00:02:31.638 (24.014 sec) udp 147.207.106.49:53 => 93.169.182.233:80 (2665/8618602 ->) eof
1970-01-01 00:02:07.508 - 00:02:31.638 (24.130 sec) udp 185.206.209.198:53 => 93.169.182.233:80 (4006/2908204 ->) eof
1970-01-01 00:02:07.405 - 00:02:31.639 (24.234 sec) udp 146.74.117.178:53 => 93.169.182.233:80 (838/452520 ->) eof
1970-01-01 00:02:07.634 - 00:02:31.639 (24.005 sec) udp 132.29.236.138:53 => 93.169.182.233:80 (3341/12360677 ->) eof
1970-01-01 00:02:07.453 - 00:02:31.640 (24.187 sec) udp 105.25.132.158:53 => 93.169.182.233:80 (7625/17326069 ->) eof
1970-01-01 00:02:07.498 - 00:02:31.640 (24.142 sec) udp 167.32.20.80:53 => 93.169.182.233:80 (3557/7765732 ->) eof
1970-01-01 00:02:07.377 - 00:02:31.640 (24.263 sec) udp 85.89.162.144:53 => 93.169.182.233:80 (9757/29474478 ->) eof
1970-01-01 00:02:07.353 - 00:02:31.640 (24.287 sec) udp 154.171.193.234:53 => 93.169.182.233:80 (3169/470160 ->) eof
1970-01-01 00:02:07.551 - 00:02:31.641 (24.090 sec) udp 178.94.122.132:53 => 93.169.182.233:80 (2444/7639948 ->) eof
1970-01-01 00:02:07.340 - 00:02:31.641 (24.301 sec) udp 91.10.47.187:53 => 93.169.182.233:80 (13425/43617034 ->) eof
1970-01-01 00:02:07.368 - 00:02:31.641 (24.273 sec) udp 88.97.249.253:53 => 93.169.182.233:80 (1031/556740 ->) eof
1970-01-01 00:02:07.570 - 00:02:31.641 (24.071 sec) udp 90.71.179.248:53 => 93.169.182.233:80 (2429/5098955 ->) eof
1970-01-01 00:02:07.498 - 00:02:31.641 (24.143 sec) udp 183.116.154.237:53 => 93.169.182.233:80 (4667/13471721 ->) eof
1970-01-01 00:02:07.519 - 00:02:31.641 (24.122 sec) udp 82.67.240.101:53 => 93.169.182.233:80 (4378/12961763 ->) eof
1970-01-01 00:02:07.321 - 00:02:31.641 (24.320 sec) udp 105.25.13.117:53 => 93.169.182.233:80 (841/435638 ->) eof
1970-01-01 00:02:07.506 - 00:02:31.642 (24.136 sec) udp 64.238.210.227:53 => 93.169.182.233:80 (3978/8830259 ->) eof

```

Figure 7: Sample of flow file in *txt* using *yafscii*