Ecole 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[1].

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^{th} second, i.e. 2 min 06 sec.
2. Duration : attack ends up at the 151^{th} 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.

[1] 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 0x0831[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]
17336	126.588000	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 0x5cbd 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

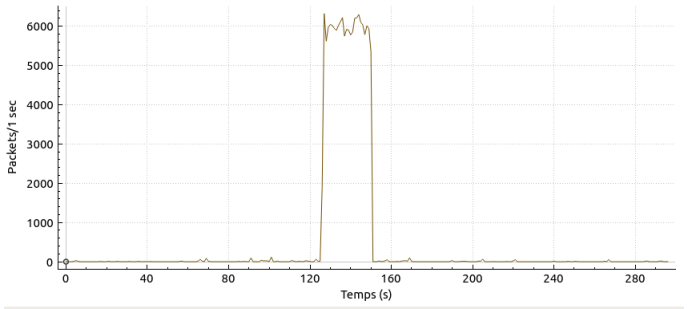

Figure 2: Network activity in terms of DNS packets per second

Question d

1. Start time of attack : attack starts at 144^{th} second, i.e. 2 min 22 seconds.
2. Duration : the end of the attack is observed at the 192^{th} 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*[2], 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.

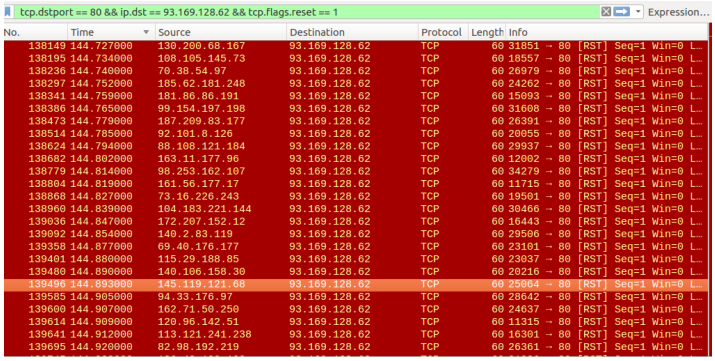

Figure 3: Sample of the reset attack against web server 93.169.128.62

[2]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).

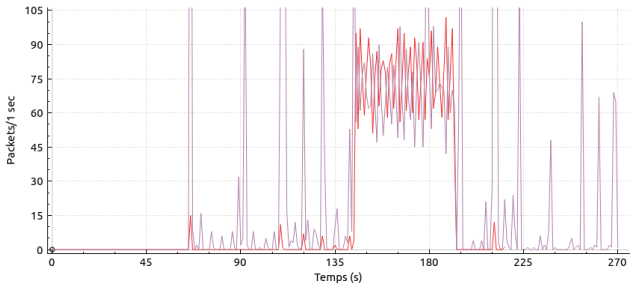

Figure 4: Web server response : Network activity in terms of TCP packets via HTTP application

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…
190560	189.008000	93.169.128.62	67.198.236.163	TCP	58	80 → 12675 [SYN, ACK] Seq=0 Ac…
190577	189.080000	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."[3]

[3]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.

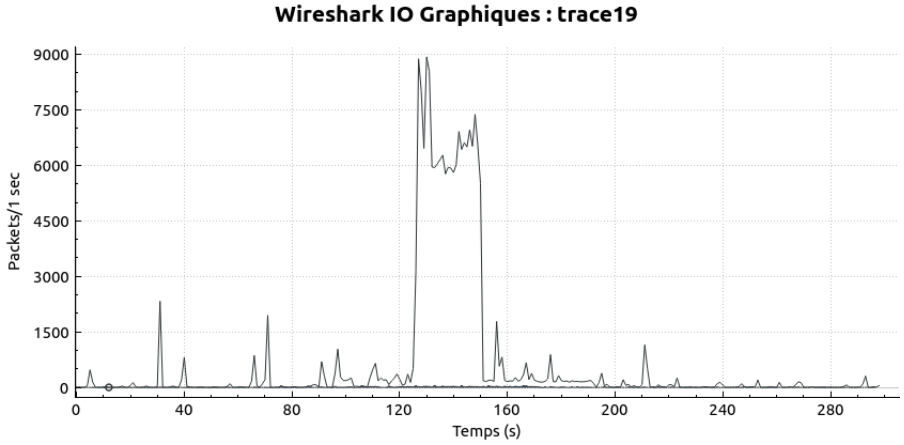

Figure 6: Graphical representation of *pcap* file, showing the network activity in packets per second

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

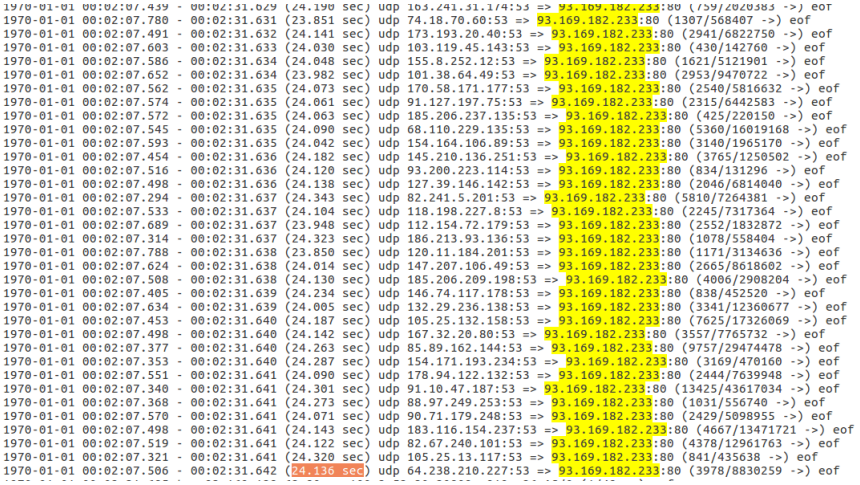

Figure 7: Sample of flow file in *txt* using *yafscii*