Network Security
389.159 - SS 2018
Lab Exercise 1 & Lab Exercise 2

TEAM 02
Corentin Bergès (11741629) (xxxx)
Christoph Echtinger-Sieghart (00304130) (066 938)

May 17, 2018

1 Lab Exercise 1

1.1 rep-1

We obtained our IPv4 address using the following command:

```
team02@pc01:~$ ip address show dev em1
```

Our IPv4 address is **192.168.83.20**.

1.2 rep-2

We sent TCP SYN packets to IPv4 address **192.168.83.33** on ports 113 (ident), 445 (microsoft-ds), 7210 and 9920 using the following command:

```
team02@pc01:~$ for port in 113 445 7210 9920; do \
        tgn "ip(dst = 192.168.83.33) /tcp(dst = $port,syn)"; \
    done
```

We now present our findings for each port. We performed the analysis using `wireshark`, but for brevity include only a textual representation of the communication. Note that the textual representation was obtained using `tcpdump` and has been truncated to show only important data.

Port 113

```
IP 192.168.83.20.1073 > 192.168.83.33.113: Flags [S], seq 0, win 8192, length 0
IP 192.168.83.33.113 > 192.168.83.20.1073: Flags [R.], seq 0, ack 1, win 0, length 0
```

This communication corresponds to **case B**. Port 113 is closed on the target machine.

Port 445

```
IP 192.168.83.20.1073 > 192.168.83.33.445: Flags [S], seq 0, win 8192, length 0
IP 192.168.83.33.445 > 192.168.83.20.1073: Flags [S.], seq 4122740187, ack 1, win 29200
IP 192.168.83.20.1073 > 192.168.83.33.445: Flags [R], seq 1, win 0, length 0
```

This communication corresponds to **case A**. Port 445 is open on the target machine. This is the case with the different behaviour. The difference is due to our TCP/IP stack responding with a RST packet because there is no longer a connection associated with the initial packet.

Port 7210

```
IP 192.168.83.20.1073 > 192.168.83.33.7210: Flags [S], seq 0, win 8192, length 0
```

This communication corresponds to **case C**. The packet to port 7210 was silently dropped.

Port 9920

```
IP 192.168.83.20.1073 > 192.168.83.33.9920: Flags [S], seq 0, win 8192, length 0
IP 192.168.83.33 > 192.168.83.20: ICMP 192.168.83.33 tcp port 9920 unreachable, length 48
```

This communication corresponds to **case D**. We got an ICMP message back, telling us that port 9920 is blocked.

1.3 rep-3

Depending on the amount of traffic passing through the routing device it would be hard to detect any kind of scanning activity on a busy router. Wireshark is not a suitable tool for analyzing large amounts of network traffic data, because ...

- the traffic dump would quickly get quite large, because the packet payload is captured as well.
- Wireshark does not provide suitable binning or aggregation functions.
- we often need statistical/data mining methods to extract useful information from the traffic dump.

2 Lab Exercise 2

2.1 rep-4

Figure 1 shows the commandline and the first three rows from our **synscan.pcap** file. Note that the `tcpdump` output is truncated on the right side.

```
team02@pc01:~$ cat synscan.pcap | tcpdump -t -nr - | head -n 3
IP 192.168.83.20.850 > 192.168.83.1.2049: Flags [P.], seq 4210818527:4210818687, ack 463369472, win 4229, options
IP 192.168.83.1.2049 > 192.168.83.20.850: Flags [P.], seq 1:129, ack 160, win 6365, options [nop,nop,TS val 108011
IP 192.168.83.20.850 > 192.168.83.1.2049: Flags [.], ack 129, win 4229, options [nop,nop,TS val 148271 ecr 1080118
```

Figure 1: First three rows of our synscan.pcap file

2.2 rep-5

We converted our synscan.pcap file to a flow record using the following command:

```
team02@pc01:~$ rwptoflow --flow-output=synscan.rw synscan.pcap --compression-method=zlib
```

Figure 2 shows the commandline and the first five rows from our **synscan.rw** flow record file.

```
team02@pc01:~$ rwcut --fields sTime,sIp,dIP,sPort,dPort,ttl,flags synscan.rw | head -n 6
                 sTime|             sIP|             dIP|sPort|dPort|ttl|   flags|
2018/05/15T11:09:44.616|   192.168.83.20|   192.168.83.1|  850| 2049| 64|   PA   |
2018/05/15T11:09:44.616|    192.168.83.1|  192.168.83.20| 2049|  850| 64|   PA   |
2018/05/15T11:09:44.616|   192.168.83.20|   192.168.83.1|  850| 2049| 64|    A   |
2018/05/15T11:09:44.616|   192.168.83.20|   192.168.83.1|  850| 2049| 64|   PA   |
2018/05/15T11:09:44.616|    192.168.83.1|  192.168.83.20| 2049|  850| 64|   PA   |
```

Figure 2: First five rows of our synscan.rw file

2.3 rep-6

The start time of our team02.flowrecord.rw file is **2012/04/26T20:00:00,38257**. This corresponds to a unix epoch of **1335470400,38257**. The end time is **2012/04/26T20:59:59,34414**. This corresponds to a unix epoch of **1335473999,34414**.

2.4 rep-7

Figure 3 shows the commandline and the number of packets per hour in our team02.flowrecord.rw file. The are 135358046 packets per hour in our file. This number is in the same order of magnitude as the number in the exercise sheet ($\approx 10^8$ to 10^9 packets/hour).

```
team02@pc01:~$ rwuniq --sort-output --bin-time=3600 --fields=stime \
    --values=packet --timestamp-format=epoch --no-titles \
    --no-final-delimiter --delimited=, workfiles/team02.flowrecord.rw
1335470400,135358046
```

Figure 3: Number of packets per hour in team02.flowrecord.rw

2.5 rep-8

Figure 4 shows the commandline and the number of unique IP addresses per hour in our team02.flowrecord.rw file. The are 447148 unique IP addresses per hour in our file. This number is in the same order of magnitude as the number in the exercise sheet ($\approx 10^5$ to 10^6 unique IPs/hour).

```
team02@pc01:~$ rwuniq --sort-output --bin-time=3600 --fields=stime \
    --values=sIP --timestamp-format=epoch --no-titles \
    --no-final-delimiter --delimited=, workfiles/team02.flowrecord.rw
1335470400,447148
```

Figure 4: Unique IP addresses per hour in team02.flowrecord.rw

2.6 rep-9

Since the darkspace is a /8 network it is approximately $\frac{1}{256}^{\text{th}}$ of the whole internet. To be more accurate all publicly unusable address ranges would have to be taken into account.

Undesired packets/hour Using this information we arrive at

$$135358046 * 256 = 34651659776 \approx 34e9$$

undesired packets per hour for the whole internet. The real values are probably smaller, because the publicly unusable address ranges have not been taken into account.

Unique source IPs The number of unique source IPs will roughly be the same for the whole internet as for the darkspace ($\approx 4e5$ unique IPs per hour). The real values are probably bigger, because attackers might avoid the darkspace or target only specific ranges of the address space.

Pollution To give a reliable answer, we would need actual data on the average packet count per hour for the whole internet. We checked caida.org, but could not find suitable data. The traffic statistics at DE-CIX or AMS-IX only give bandwith and not packet count. Since an IP packet might range from 64 bytes to 1500 bytes transported over ethernet deriving a packet count from bandwidth stats is not reliable.
One major effect of the unwanted packets is that the unwanted traffic uses up valuable bandwidth and resources. The unwanted traffic also results in increased power consumption.