Міністерство освіти та науки України
Національний технічний університет України
«Київський політехнічний інститут ім. Ігоря Сікорського»
Факультет прикладної математики
Кафедра системного програмування і спеціалізованих комп’ютерних систем

Лабораторна робота №6

з дисципліни
«Комп`ютерні мережі»
«Мониторинг сети с помощью tcpdump»

Виконали студенти четвертого курсу
групи КВ-32
Гудіков Владислав
Непокритий Микола
Коваль Андріян

м. Київ
2016

Робота програми tcpdump:

vlad@vlad-HP-ProBook-4430s:~$ sudo tcpdump

```
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
19:07:42.385977 IP vlad-HP-ProBook-4430s.48288 > lo-in-f27.1e100.net.smtp: Flags [S], seq 4065421447, win
29200, options [mss 1460,sackOK,TS val 3251292 ecr 0,nop,wscale 7], length 0
19:07:42.410792 IP vlad-HP-ProBook-4430s.56582 > GoodGuys.domain: 14333+ PTR?
27.222.194.173.in-addr.arpa. (45)
19:07:42.438019 IP vlad-HP-ProBook-4430s.57836 > h2web53.infomaniak.ch.https: Flags [.], ack 1509028172,
win 936, length 0
19:07:42.447580 IP GoodGuys.domain > vlad-HP-ProBook-4430s.56582: 14333 1/4/4 PTR
lo-in-f27.1e100.net. (224)
19:07:42.448211 IP vlad-HP-ProBook-4430s.45828 > GoodGuys.domain: 29778+ PTR?
106.1.168.192.in-addr.arpa. (44)
19:07:42.451589 IP GoodGuys.domain > vlad-HP-ProBook-4430s.45828: 29778* 1/0/0 PTR
vlad-HP-ProBook-4430s. (79)
19:07:42.452046 IP vlad-HP-ProBook-4430s.47376 > GoodGuys.domain: 58975+ PTR?
1.1.168.192.in-addr.arpa. (42)
19:07:42.456007 IP GoodGuys.domain > vlad-HP-ProBook-4430s.47376: 58975* 1/0/0 PTR GoodGuys. (64)
19:07:42.456675 IP vlad-HP-ProBook-4430s.17011 > GoodGuys.domain: 46173+ PTR?
129.195.65.128.in-addr.arpa. (45)
19:07:42.529958 IP vlad-HP-ProBook-4430s.38132 > li-in-f94.1e100.net.https: Flags [.], ack 3864643886, win
1918, options [nop,nop,TS val 3251328 ecr 1698000941], length 0
19:07:42.530308 IP vlad-HP-ProBook-4430s.17198 > GoodGuys.domain: 60504+ PTR?
94.162.233.64.in-addr.arpa. (44)
19:07:42.554030 IP GoodGuys.domain > vlad-HP-ProBook-4430s.17198: 60504 1/4/4 PTR li-in-f94.1e100.net.
(223)
19:07:42.564645 IP li-in-f94.1e100.net.https > vlad-HP-ProBook-4430s.38132: Flags [.], ack 1, win 756,
options [nop,nop,TS val 1698046034 ecr 3240044], length 0
```

vlad@vlad-HP-ProBook-4430s:~$ sudo tcpdump -n

```
19:09:21.005954 IP 192.168.1.106.36014 > 149.154.167.51.443: Flags [.], ack 3196355074, win 229, options
[nop,nop,TS val 3275947 ecr 8295101], length 0
19:09:21.230151 IP 192.168.1.106.55838 > 216.58.209.99.443: Flags [P.], seq 2880832172:2880832284, ack
4270413228, win 245, options [nop,nop,TS val 3276003 ecr 1138716610], length 112
19:09:21.230430 IP 192.168.1.106.55838 > 216.58.209.99.443: Flags [P.], seq 112:150, ack 1, win 245, options
[nop,nop,TS val 3276003 ecr 1138716610], length 38
19:09:21.280392 IP 216.58.209.99.443 > 192.168.1.106.55838: Flags [.], ack 112, win 868, options
[nop,nop,TS val 1138745491 ecr 3276003], length 0
19:09:21.280458 IP 216.58.209.99.443 > 192.168.1.106.55838: Flags [.], ack 150, win 868, options
[nop,nop,TS val 1138745491 ecr 3276003], length 0
19:09:21.281962 IP 216.58.209.99.443 > 192.168.1.106.55838: Flags [P.], seq 1:39, ack 150, win 868, options
[nop,nop,TS val 1138745491 ecr 3276003], length 38
19:09:21.290945 IP 216.58.209.99.443 > 192.168.1.106.55838: Flags [P.], seq 39:103, ack 150, win 868,
options [nop,nop,TS val 1138745501 ecr 3276003], length 64
19:09:21.291035 IP 216.58.209.99.443 > 192.168.1.106.55838: Flags [P.], seq 103:133, ack 150, win 868,
options [nop,nop,TS val 1138745502 ecr 3276003], length 30
19:09:21.291097 IP 192.168.1.106.55838 > 216.58.209.99.443: Flags [.], ack 133, win 245, options
[nop,nop,TS val 3276018 ecr 1138745491], length 0
19:09:21.292337 IP 216.58.209.99.443 > 192.168.1.106.55838: Flags [P.], seq 133:171, ack 150, win 868,
options [nop,nop,TS val 1138745502 ecr 3276003], length 38
19:09:21.292602 IP 192.168.1.106.55838 > 216.58.209.99.443: Flags [P.], seq 150:188, ack 171, win 245,
options [nop,nop,TS val 3276018 ecr 1138745502], length 38
19:09:21.382622 IP 216.58.209.99.443 > 192.168.1.106.55838: Flags [.], ack 188, win 868, options
[nop,nop,TS val 1138745593 ecr 3276018], length 0
```

vlad@vlad-HP-ProBook-4430s:~$ sudo tcpdump -i wlo1

```
19:10:02.480778 IP dev.44391 > 239.255.255.250.1900: UDP, length 172
19:10:02.481787 IP vlad-HP-ProBook-4430s.34188 > GoodGuys.domain: 23301+ PTR?
250.255.255.239.in-addr.arpa. (46)
19:10:02.484472 IP GoodGuys.domain > vlad-HP-ProBook-4430s.34188: 23301 NXDomain* 0/1/0 (103)
19:10:02.485135 IP vlad-HP-ProBook-4430s.4885 > GoodGuys.domain: 22961+ PTR?
110.1.168.192.in-addr.arpa. (44)
19:10:02.486452 IP GoodGuys.domain > vlad-HP-ProBook-4430s.4885: 22961* 1/0/0 PTR dev. (61)
19:10:02.486899 IP vlad-HP-ProBook-4430s.15857 > GoodGuys.domain: 34601+ PTR?
1.1.168.192.in-addr.arpa. (42)
19:10:02.488230 IP GoodGuys.domain > vlad-HP-ProBook-4430s.15857: 34601* 1/0/0 PTR GoodGuys. (64)
19:10:02.488623 IP vlad-HP-ProBook-4430s.15299 > GoodGuys.domain: 61748+ PTR?
106.1.168.192.in-addr.arpa. (44)
19:10:05.332092 IP c4.52.c0ad.ip4.static.sl-reverse.com.http > vlad-HP-ProBook-4430s.46088: Flags [P.], seq
4000515529:4000515531, ack 822298871, win 127, options [nop,nop,TS val 1397712475 ecr 3284528], length
2: HTTP
19:10:05.332246 IP vlad-HP-ProBook-4430s.46088 > c4.52.c0ad.ip4.static.sl-reverse.com.http: Flags [P.], seq
1:7, ack 2, win 237, options [nop,nop,TS val 3287028 ecr 1397712475], length 6: HTTP
19:10:05.332339 IP vlad-HP-ProBook-4430s.1032 > GoodGuys.domain: 10080+ PTR?
196.82.192.173.in-addr.arpa. (45)
19:10:05.337597 IP GoodGuys.domain > vlad-HP-ProBook-4430s.1032: 10080 1/6/5 PTR
c4.52.c0ad.ip4.static.sl-reverse.com. (295)
19:10:05.486987 IP c4.52.c0ad.ip4.static.sl-reverse.com.http > vlad-HP-ProBook-4430s.46088: Flags [.], ack 7,
win 127, options [nop,nop,TS val 1397712514 ecr 3287028], length 0
19:10:05.793973 IP vlad-HP-ProBook-4430s.35484 > tl-in-f26.1e100.net.smtp: Flags [S], seq 1712157449, win
29200, options [mss 1460,sackOK,TS val 3287144 ecr 0,nop,wscale 7], length 0
19:10:05.794396 IP vlad-HP-ProBook-4430s.25708 > GoodGuys.domain: 30755+ PTR?
26.189.233.64.in-addr.arpa. (44)
19:10:05.834027 IP GoodGuys.domain > vlad-HP-ProBook-4430s.25708: 30755 1/0/0 PTR tl-in-f26.1e100.net.
(77)
```

vlad@vlad-HP-ProBook-4430s:~$ sudo tcpdump -n -i wlo1 port 25

```
19:14:04.481966 IP 192.168.1.106.37438 > 74.125.25.27.25: Flags [S], seq 484697267, win 29200, options
[mss 1460,sackOK,TS val 3346816 ecr 0,nop,wscale 7], length 0
19:14:20.513940 IP 192.168.1.106.37438 > 74.125.25.27.25: Flags [S], seq 484697267, win 29200, options
[mss 1460,sackOK,TS val 3350824 ecr 0,nop,wscale 7], length 0
19:14:52.609976 IP 192.168.1.106.37438 > 74.125.25.27.25: Flags [S], seq 484697267, win 29200, options
[mss 1460,sackOK,TS val 3358848 ecr 0,nop,wscale 7], length 0
```