

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут»
Факультет прикладної математики
Кафедра спеціалізованих комп'ютерних систем

Лабораторна робота №2
З дисципліни
«Комп'ютерні мережі»

Виконав:
Студент групи KB-92
Михайлик Михайло
Перевірів:

Оцінка_____

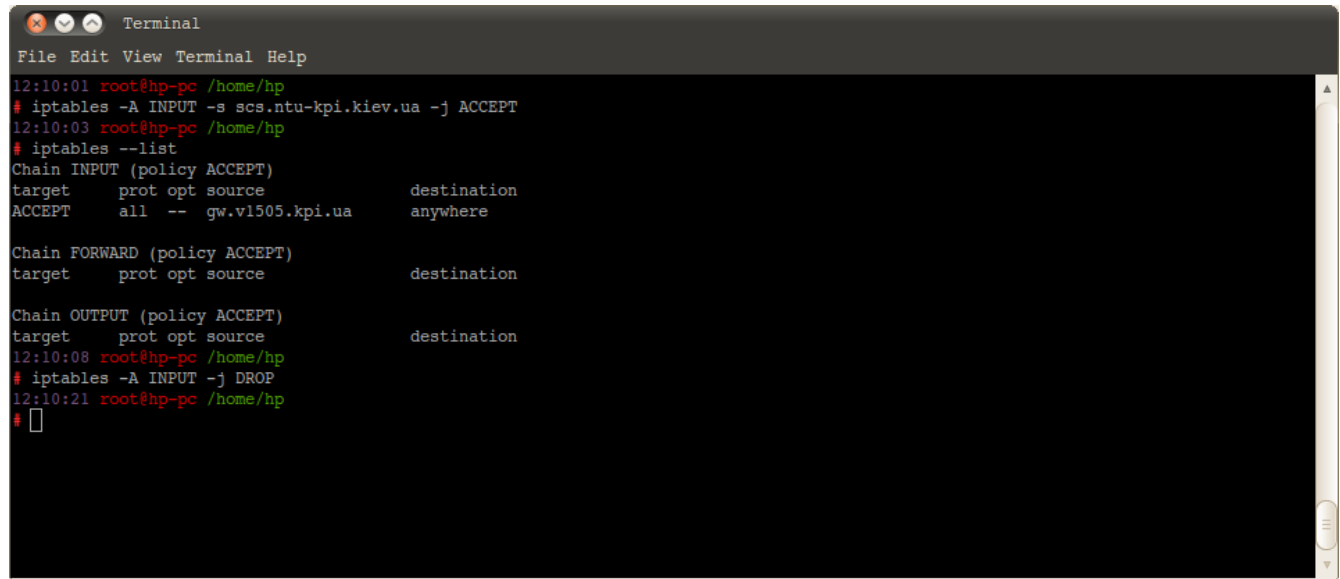
Київ 2012

Мережа 192.168.11.0/24

PC1 (192.168.11.252)

PC2 (192.168.11.253)

Завдання 1. Дозволити приймати пакети лише з хоста scs.ntu-kpi.kiev.ua.



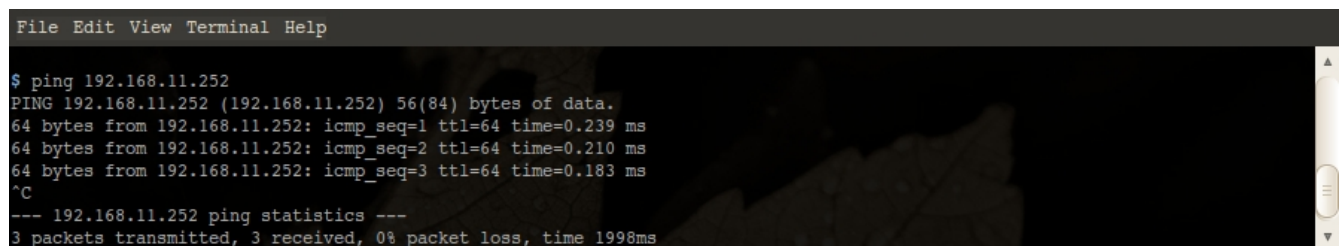
```
Terminal
File Edit View Terminal Help
12:10:01 root@hp-pc /home/hp
# iptables -A INPUT -s scs.ntu-kpi.kiev.ua -j ACCEPT
12:10:03 root@hp-pc /home/hp
# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  gw.v1505.kpi.ua       anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
12:10:08 root@hp-pc /home/hp
# iptables -A INPUT -j DROP
12:10:21 root@hp-pc /home/hp
#
```

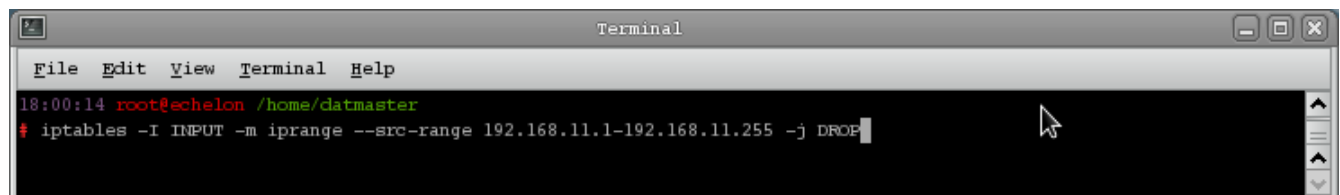
Завдання 2. Заборонити з'єднання з вашою машиною з комп'ютерів в локальній мережі.

PC2



```
File Edit View Terminal Help
$ ping 192.168.11.252
PING 192.168.11.252 (192.168.11.252) 56(84) bytes of data:
64 bytes from 192.168.11.252: icmp_seq=1 ttl=64 time=0.239 ms
64 bytes from 192.168.11.252: icmp_seq=2 ttl=64 time=0.210 ms
64 bytes from 192.168.11.252: icmp_seq=3 ttl=64 time=0.183 ms
^C
--- 192.168.11.252 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
```

PC1



```
Terminal
File Edit View Terminal Help
18:00:14 root@echelon /home/datmaster
# iptables -I INPUT -m iprange --src-range 192.168.11.1-192.168.11.255 -j DROP
```

```
Terminal
File Edit View Terminal Help
18:02:27 root@echelon /home/datmaster
# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      all  --  anywhere              anywhere           source IP range 192.168.11.1-192.168.11.255

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
18:02:33 root@echelon /home/datmaster
#
```

PC2

```
File Edit View Terminal Help
22:00:49 hp@hp-pc /home/hp
$ ping 192.168.11.252
PING 192.168.11.252 (192.168.11.252) 56(84) bytes of data.
#
```

Завдання 3. Відключити відклик на ICMP запити на вашій машині.

PC2

```
File Edit View Terminal Help
$ ping 192.168.11.252
PING 192.168.11.252 (192.168.11.252) 56(84) bytes of data.
64 bytes from 192.168.11.252: icmp_seq=1 ttl=64 time=0.239 ms
64 bytes from 192.168.11.252: icmp_seq=2 ttl=64 time=0.210 ms
64 bytes from 192.168.11.252: icmp_seq=3 ttl=64 time=0.183 ms
^C
--- 192.168.11.252 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
```

PC1

```
Terminal
File Edit View Terminal Help
18:53:46 root@echelon /home/datmaster
# iptables -A INPUT -p icmp --icmp-type 8 -j DROP
```

```
Terminal
File Edit View Terminal Help
18:54:10 root@echelon /home/datmaster
# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP       icmp -- anywhere         anywhere          icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
18:54:16 root@echelon /home/datmaster
#
```

PC2

```
File Edit View Terminal Help
22:00:49 hp@hp-pc /home/hp
$ ping 192.168.11.252
PING 192.168.11.252 (192.168.11.252) 56(84) bytes of data.
#
```

Завдання 4. Закрити всі порти, крім SMTP. Для перевірки закриємо всі порти крім SSH (22 порт)

PC2

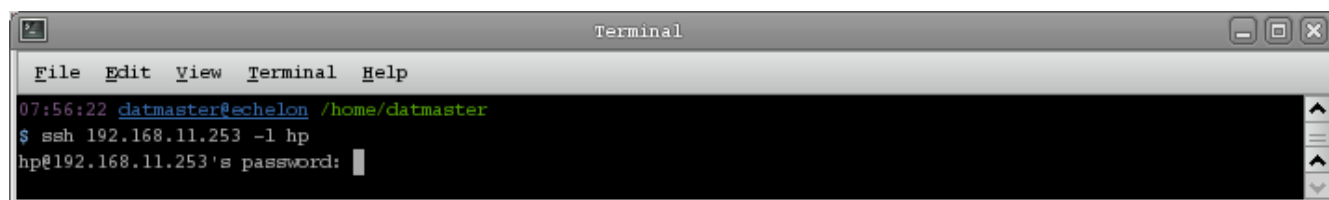
```
Terminal
File Edit View Terminal Help
11:47:08 root@hp-pc /home/hp
# iptables -A INPUT -p udp -m multiport --ports ssh -j ACCEPT
11:47:16 root@hp-pc /home/hp
# iptables -A INPUT -p tcp -j DROP
11:47:23 root@hp-pc /home/hp
# iptables -A INPUT -p udp -j DROP
11:47:28 root@hp-pc /home/hp
#
```

```
Terminal
File Edit View Terminal Help
# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     tcp  -- anywhere             anywhere          multiport ports ssh
ACCEPT     udp  -- anywhere             anywhere          multiport ports ssh
DROP       tcp  -- anywhere             anywhere
DROP       udp  -- anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
11:48:02 root@hp-pc /home/hp
#
```

PC1



A screenshot of a terminal window titled "Terminal". The window has a menu bar with "File", "Edit", "View", "Terminal", and "Help". The terminal content shows a timestamp "07:56:22" followed by the prompt "datmaster@echelon /home/datmaster". Below this, the command "\$ ssh 192.168.11.253 -l hp" is entered. The next line shows the prompt "hp@192.168.11.253's password:" followed by a cursor. The terminal has a scrollbar on the right side.

```
07:56:22 datmaster@echelon /home/datmaster
$ ssh 192.168.11.253 -l hp
hp@192.168.11.253's password: 
```