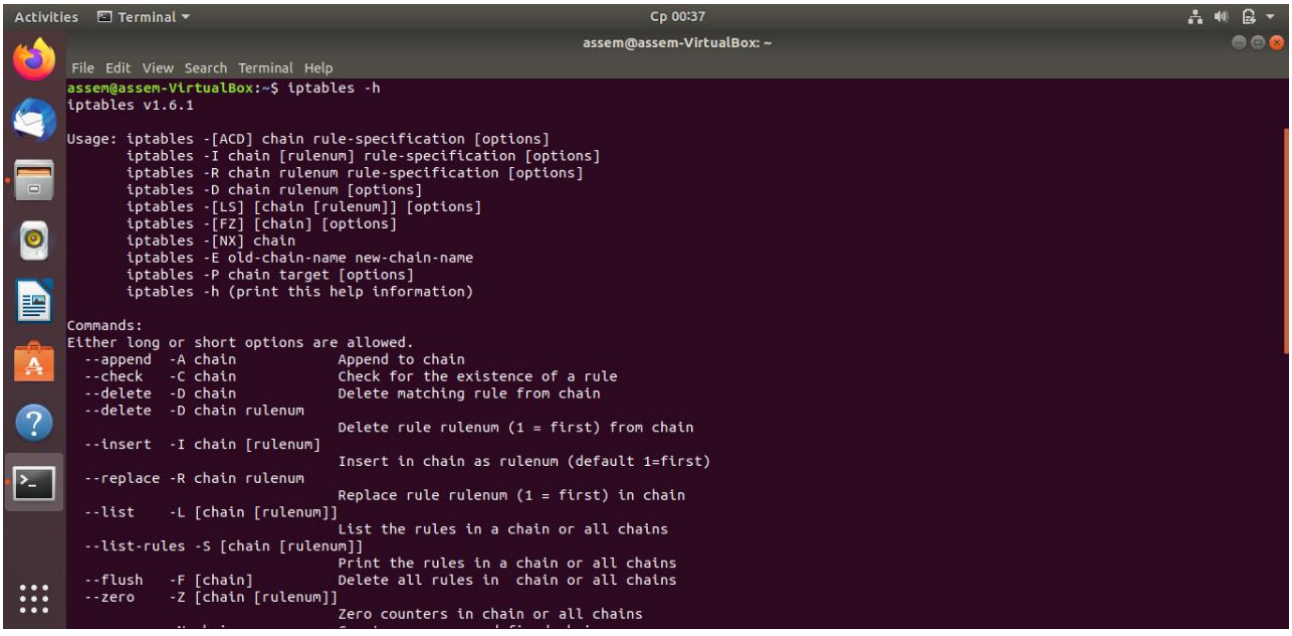
Практикалық сабақ №13: ICMP хаттамасын қолдана отырып жасалған шабуылдар

ОЖ-де жауаптарды блоктау ICMP пакеттерінің flood шабуылдарының алдын алады, бірақ көптеген жүйелер бұл қызметті онлайн бақылау (жүйелік бақылау) үшін пайдаланады. *"UNIX/Linux-та ping (ICMP) жауаптарын бұғаттау"* тақырыбында мен оны қалай өшіруге болатындығын айтамын.

Егер сервер үнемі Ping функциясы арқылы DoS шабуылына тап болса, серверге ping құлпы пайдалы. **IPTables** пайдалану кезінде біз жай ғана серверге ICMP пакеттерінің өтуіне тыйым салуды тоқтата аламыз (іс жүзінде PING-ге тыйым салу керек). Мұны бастамас бұрын Linux-та **Iptables** деген не екендігі туралы түсінік болуы керек. Iptables бұл кіріс және шығыс пакеттерді басқаратын ережелер жиынтығы бар брандмауэр жүйесі. Әдепкі бойынша, Iptables ешқандай ережесіз жұмыс істейді, *сіз ережелерді жасай, қоса аласыз және өңдей аласыз*.

Iptables көмегімен Ping-ті өшіру

ICMP пакеттерін басқару ережелерін жасау үшін қажет iptables - тегі кейбір параметрлерді түсіндіру:



- A: ережелерді қосады.

- D: кестеден ережені жояды.

- p : параметр протоколды көрсету (мұнда 'icmp').

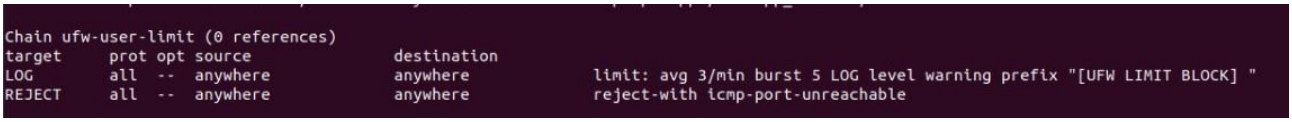
- icmp-түрі: түрін көрсету опциясы.

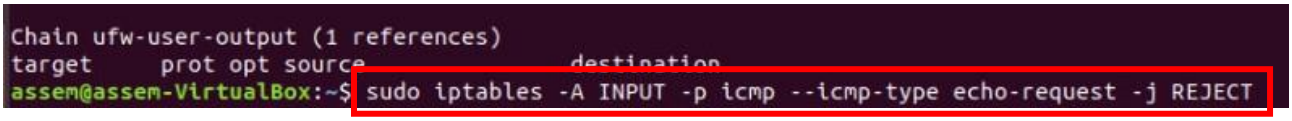
- J: тізбекке өтіңіз.

Төменде мен көрнекі мысалдар келтіремін.

Қате туралы хабарлама шығарумен серверде PING-ті қалай бұғаттауға болады?

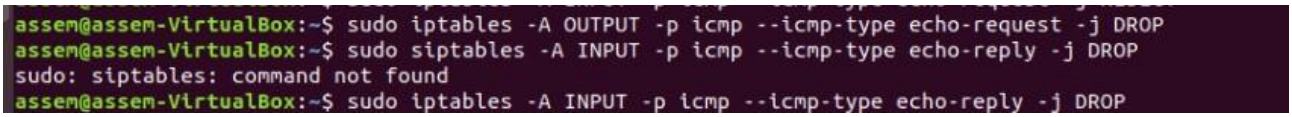
Сіз "*Destination Port Unreachable*" қате туралы хабарлама шығарумен PING-ті ішінара бұғаттай аласыз. Iptables қате туралы хабарлама шығарумен PING-ті бұғаттау үшін келесі ережелерді қосыңыз:





Қате туралы хабарламаларсыз серверде PING-ті блоктау.

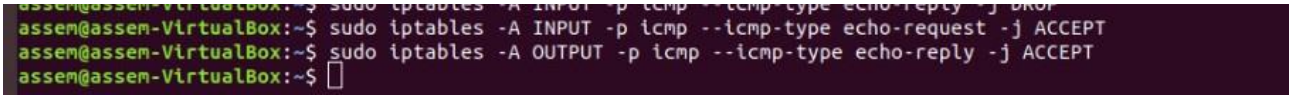
Бұл үшін біз мына команданы қолданамыз:



Сервердегі барлық кіріс және шығыс ICMP пакеттерін бұғаттайды.

Iptables көмегімен пингке рұқсат етіңіз

Егер сіз серверде ping бұғаттаған болсаңыз және оны қалай қайтару керектігін білмесеңіз. Енді мен мұны қалай жасау керектігін айтамын. Бұл келесі ережені IPtables-ке қосу арқылы жасалады:



Бұл ережелер серверден және одан ICMP пакеттерінің өтуіне мүмкіндік береді.

Kernel параметрлерімен ping-ті блоктау

Сондай-ақ, пинг жауаптарын ядро параметрлерімен тікелей бұғаттай аламыз. Сіз пингке жауаптарды уақытша немесе тұрақты түрде бұғаттай аласыз және төменде мұны қалай жасау керектігі көрсетілген.

Ping-ті уақытша құлыптау

Сіз келесі пәрменді қолдана отырып, пингке уақытша жауаптарды бұғаттай аласыз:

```
root@assem-VirtualBox:/home/assem# echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all
root@assem-VirtualBox:/home/assem#
```

Бұл пәрменді ашу үшін келесі әрекеттерді орындаңыз:

```
root@assem-VirtualBox:/home/assem# echo 0 >/proc/sys/net/ipv4/icmp_echo_ignore_all
root@assem-VirtualBox:/home/assem#
```

Pingке мүлдем тыйым салу

Сіз пинг жауаптарын конфигурация файлына келесі параметрді қосу арқылы бұғаттай аласыз:

```
assem@assem-VirtualBox:~$ sudo su
[sudo] password for assem:
root@assem-VirtualBox:/home/assem# vim /etc/sysctl.conf
```

Және былай жазасыз:

```
[...]

net.ipv4.icmp_echo_ignore_all = 1

[...]
```

```
root@assem-VirtualBox: /home/assem
File  Edit  View  Search  Terminal  Help
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

###################################################################3
# Functions previously found in netbase
#net.ipv4.icmp_echo_ignore_all = 1
#
#
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
-- INSERT --                                                    16,2          Top
```

sysctl жұмыс уақытында ядро параметрлерін өзгерту үшін қолданылады, осы параметрлердің бірі "ping daemon" (пинг демоны) болуы мүмкін, егер сіз пингті өшіргіңіз келсе, онда сіз жай ғана төмендегідей жасауыңызға болады:

```
assem@assem-VirtualBox:~$ sudo su
[sudo] password for assem:
root@assem-VirtualBox:/home/assem# sysctl -w net.ipv4.icmp_echo_ignore_all=1
net.ipv4.icmp_echo_ignore_all = 1
root@assem-VirtualBox:/home/assem#
```

Енді сұраныс жасап көріңіз, оған жауап жоқ, солай ма? Пингті қайта қосу үшін мына команданы қолданыңыз:

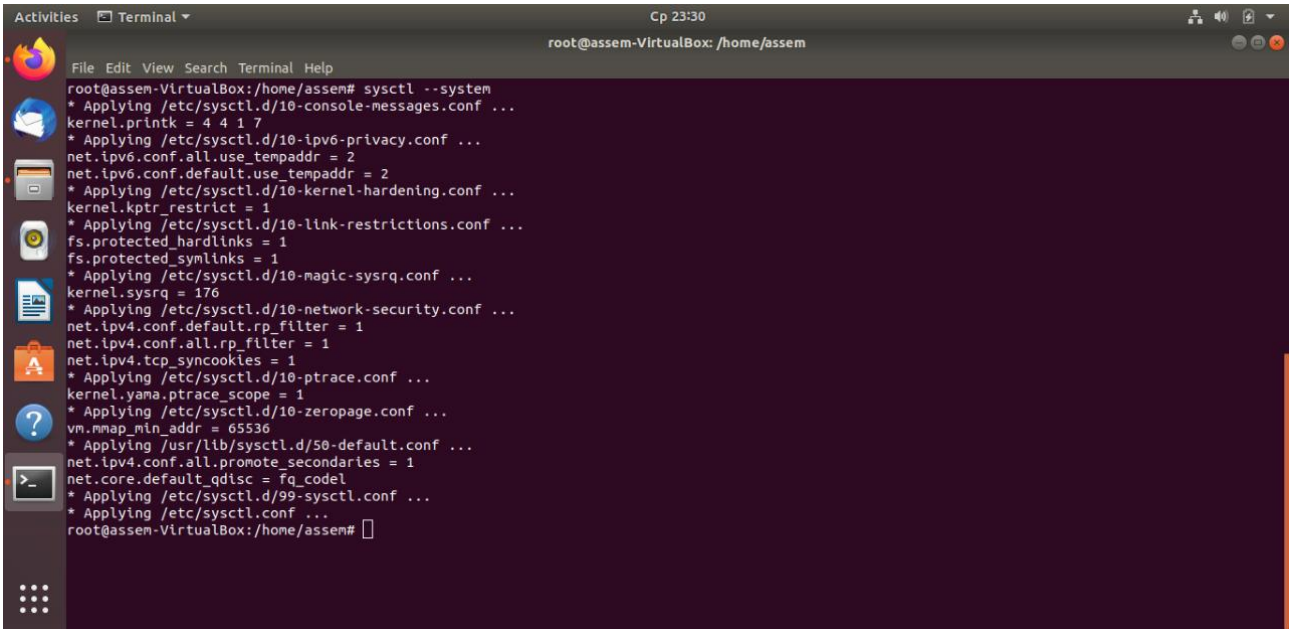
```
root@assem-VirtualBox:/home/assem# sysctl -w net.ipv4.icmp_echo_ignore_all=0
net.ipv4.icmp_echo_ignore_all = 0
root@assem-VirtualBox:/home/assem#
```

- W жалауы кейбір параметрлерді өзгерткіңіз келсе қолданылады.

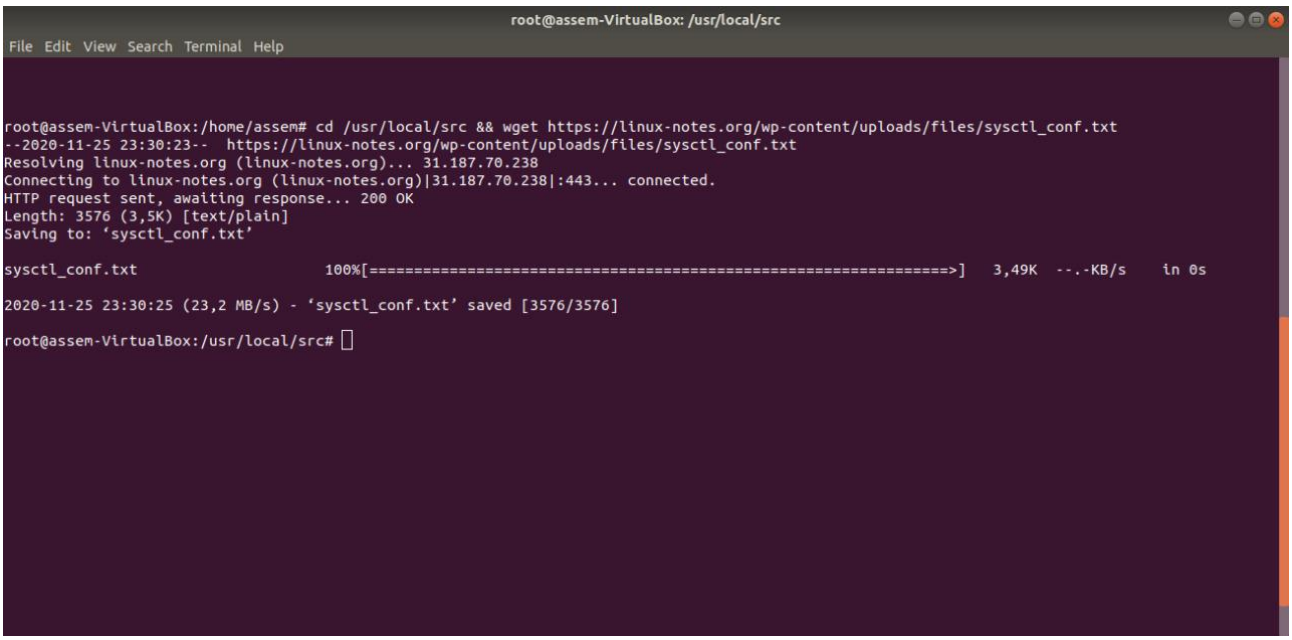
Енді жүйені қайта жүктеместен параметрлерді дереу қолдану үшін келесі пәрменді іске қосыңыз:

```
root@assem-VirtualBox:/home/assem# sysctl -p
root@assem-VirtualBox:/home/assem#
```

Немесе



Міне, менің толық конфигурациям:



содан кейін сіз былай жасай аласыз:

Сіз бұл туралы осы жерден толығырақ оқи аласыз:

https://linux-notes.org/wp-content/uploads/files/sysctl_conf.txt