

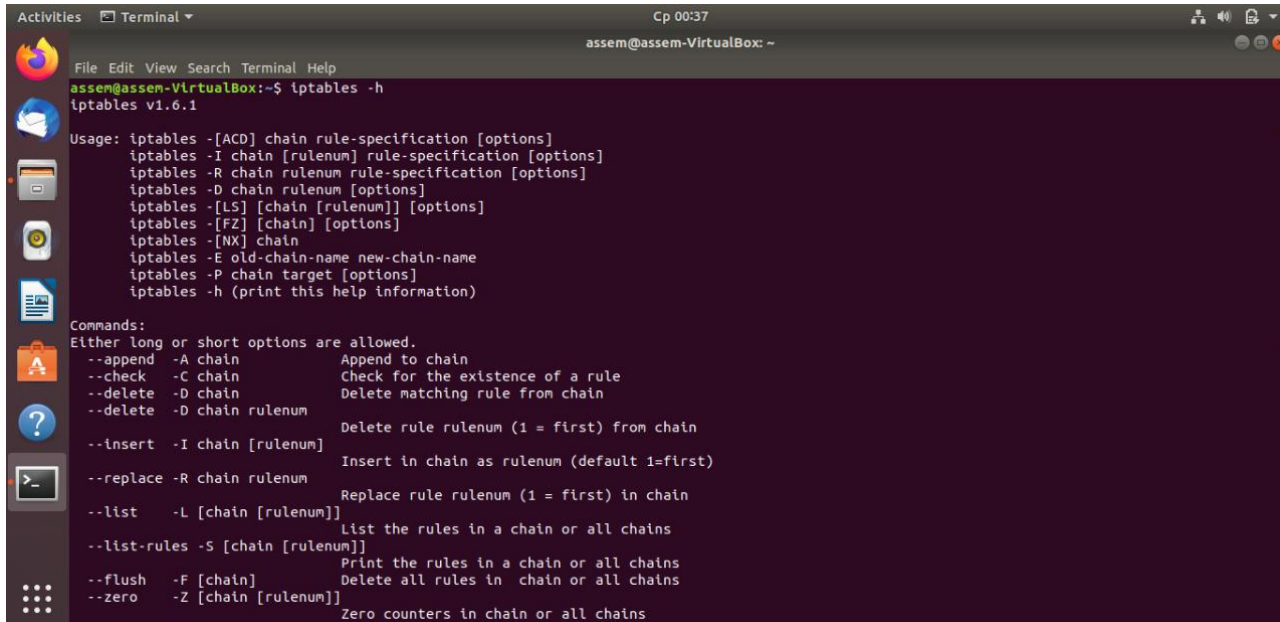
## Практикалық сабақ №13: ICMP хаттамасын қолдана отырып жасалған шабуылдар

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 бұзатмау"* 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:



```
assem@assem-VirtualBox:~$ iptables -h
iptables v1.6.1

Usage: iptables [-ACD] chain rule-specification [options]
iptables -I chain [rulenum] rule-specification [options]
iptables -R chain rulenum rule-specification [options]
iptables -D chain rulenum [options]
iptables -[LS] [chain [rulenum]] [options]
iptables -[FZ] [chain] [options]
iptables -[NX] chain
iptables -E old-chain-name new-chain-name
iptables -P chain target [options]
iptables -h (print this help information)

Commands:
Either long or short options are allowed.
--append -A chain          Append to chain
--check  -C chain          Check for the existence of a rule
--delete -D chain          Delete matching rule from chain
--delete -D chain rulenum Delete rule rulenum (1 = first) from chain
--insert -I chain [rulenum] Insert in chain as rulenum (default 1=first)
--replace -R chain rulenum Replace rule rulenum (1 = first) in chain
--list   -L [chain [rulenum]] List the rules in a chain or all chains
--list-rules -S [chain [rulenum]] Print the rules in a chain or all chains
--flush  -F [chain]        Delete all rules in chain or all chains
--zero   -Z [chain [rulenum]] Zero counters in chain or all chains
```

- 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:

```
Chain ufw-user-limit (0 references)
target     prot opt source                destination            limit: avg 3/min burst 5 LOG level warning prefix "[UFW LIMIT BLOCK] "
LOG        all  -- anywhere             anywhere
REJECT     all  -- anywhere             anywhere                reject-with icmp-port-unreachable
```

```
Chain ufw-user-output (1 references)
target     prot opt source                destination
assem@assem-VirtualBox:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT
```

Қате туралы хабарламаларсыз серверде PING-ті блоктау.

Бұл үшін біз мына команданы қолданамыз:

```
assem@assem-VirtualBox:~$ sudo iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP
assem@assem-VirtualBox:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-reply -j DROP
sudo: iptables: command not found
assem@assem-VirtualBox:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-reply -j DROP
```

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:

```
assem@assem-VirtualBox:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-reply -j DROP
assem@assem-VirtualBox:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
assem@assem-VirtualBox:~$ sudo iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
assem@assem-VirtualBox:~$
```

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# █
```

## Пингке 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 Spoof protection (reverse-path filter)
# 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:

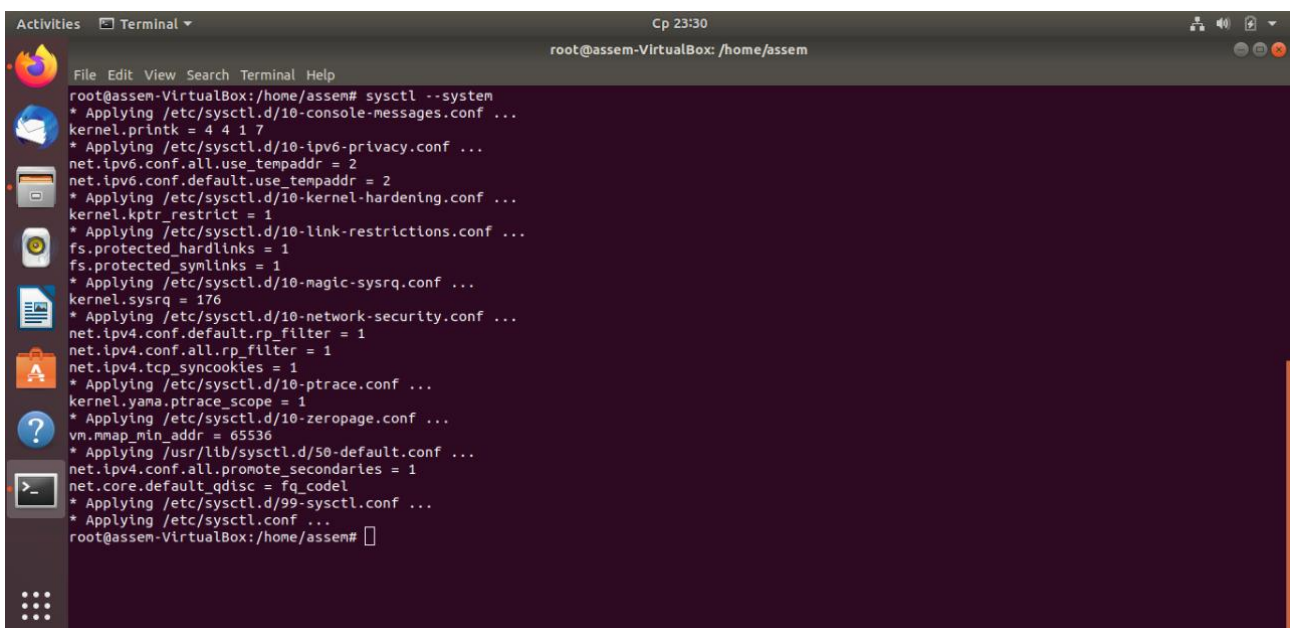
```
root@assem-VirtualBox:/home/assem# sysctl -w net.ipv4.icmp_echo_ignore_all=0
net.ipv4.icmp_echo_ignore_all = 0
root@assem-VirtualBox:/home/assem#
```

- **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



```
Activities Terminal Cp 23:30
root@assem-VirtualBox: /home/assem
File Edit View Search Terminal Help
root@assem-VirtualBox:/home/assem# sysctl --system
* Applying /etc/sysctl.d/10-console-messages.conf ...
kernel.printk = 4 4 1 7
* Applying /etc/sysctl.d/10-ipv6-privacy.conf ...
net.ipv6.conf.all.use_tempaddr = 2
net.ipv6.conf.default.use_tempaddr = 2
* Applying /etc/sysctl.d/10-kernel-hardening.conf ...
kernel.kptr_restrict = 1
* Applying /etc/sysctl.d/10-link-restrictions.conf ...
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
* Applying /etc/sysctl.d/10-magic-sysrq.conf ...
kernel.sysrq = 176
* Applying /etc/sysctl.d/10-network-security.conf ...
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.tcp_syncookies = 1
* Applying /etc/sysctl.d/10-pttrace.conf ...
kernel.yama.pttrace_scope = 1
* Applying /etc/sysctl.d/10-zero-page.conf ...
vm.mmap_min_addr = 65536
* Applying /usr/lib/sysctl.d/50-default.conf ...
net.ipv4.conf.all.promote_secondaries = 1
net.core.default_qdisc = fq_codel
* Applying /etc/sysctl.d/99-sysctl.conf ...
* Applying /etc/sysctl.conf ...
root@assem-VirtualBox:/home/assem#
```

**Міне, менің толық конфигурациям:**

```
root@assem-VirtualBox: /usr/local/src
File Edit View Search Terminal Help

root@assem-VirtualBox:/home/assem# cd /usr/local/src && wget https://linux-notes.org/wp-content/uploads/files/sysctl_conf.txt
--2020-11-25 23:30:23-- https://linux-notes.org/wp-content/uploads/files/sysctl_conf.txt
Resolving linux-notes.org (linux-notes.org)... 31.187.70.238
Connecting to linux-notes.org (linux-notes.org)[31.187.70.238]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3576 (3,5K) [text/plain]
Saving to: 'sysctl_conf.txt'

sysctl_conf.txt          100%[=====] 3,49K  --.-KB/s   in 0s
2020-11-25 23:30:25 (23,2 MB/s) - 'sysctl_conf.txt' saved [3576/3576]

root@assem-VirtualBox:/usr/local/src#
```

**содан кейін сіз былай жасай аласыз:**

```
root@assem-VirtualBox:/usr/local/src# cp /usr/local/src/sysctl_conf.txt /etc/sysctl.conf
root@assem-VirtualBox:/usr/local/src#
```

**Сіз бұл туралы осы жерден толығырақ оқи аласыз:**

[https://linux-notes.org/wp-content/uploads/files/sysctl\\_conf.txt](https://linux-notes.org/wp-content/uploads/files/sysctl_conf.txt)