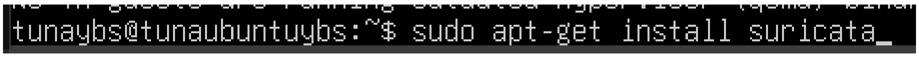
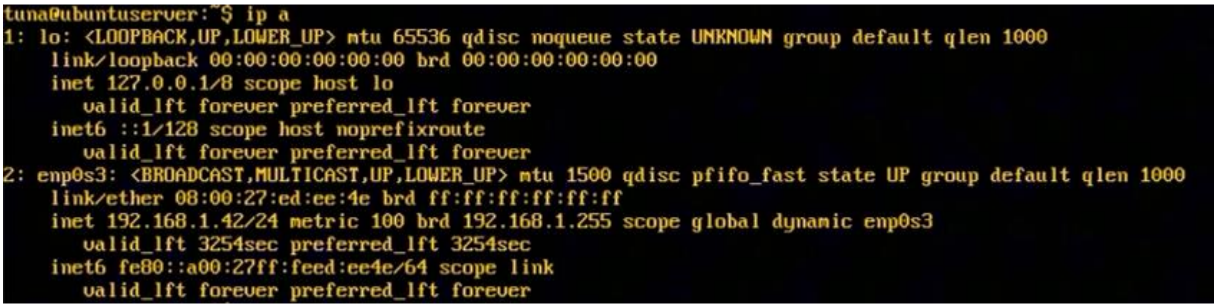
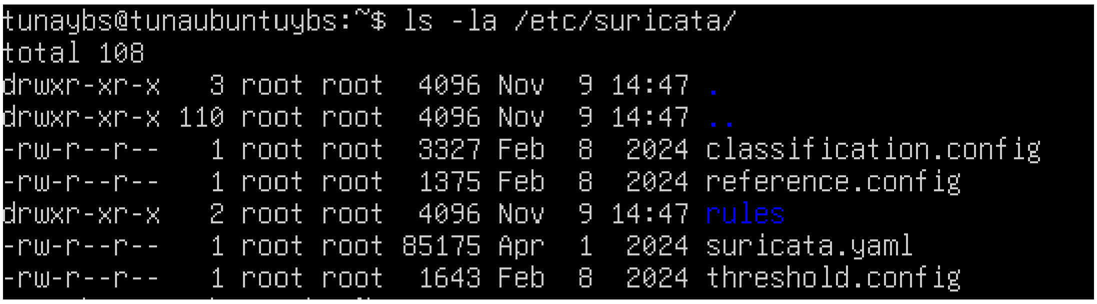


```
tunaybs@tunaubuntuybs:~$ sudo apt-get install suricata_
```

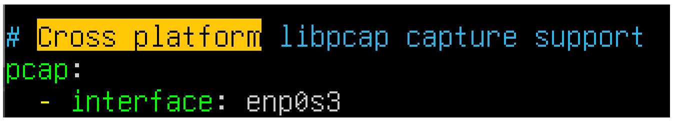


```
tuna@ubuntuserver:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ed:ee:4e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.42/24 metric 100 brd 192.168.1.255 scope global dynamic enp0s3
       valid_lft 3254sec preferred_lft 3254sec
    inet6 fe80::a00:27ff:feed:ee4e/64 scope link
       valid_lft forever preferred_lft forever
```

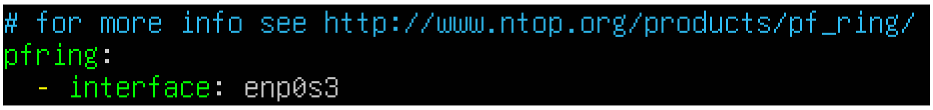
İp adresim 192.168.1.42



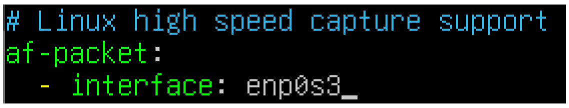
```
tunaybs@tunaubuntuybs:~$ ls -la /etc/suricata/
total 108
drwxr-xr-x   3 root root  4096 Nov  9 14:47 .
drwxr-xr-x 110 root root  4096 Nov  9 14:47 ..
-rw-r--r--   1 root root  3327 Feb  8  2024 classification.config
-rw-r--r--   1 root root  1375 Feb  8  2024 reference.config
drwxr-xr-x   2 root root  4096 Nov  9 14:47 rules
-rw-r--r--   1 root root 85175 Apr  1  2024 suricata.yaml
-rw-r--r--   1 root root  1643 Feb  8  2024 threshold.config
```



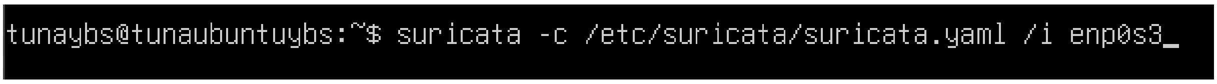
```
# Cross platform libpcap capture support
pcap:
  - interface: enp0s3
```



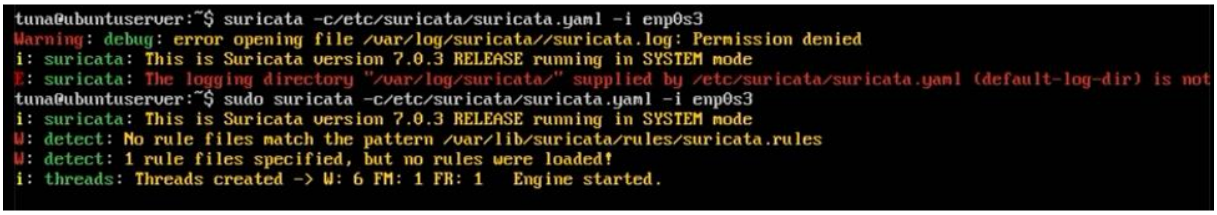
```
# for more info see http://www.ntop.org/products/pf_ring/
pfring:
  - interface: enp0s3
```



```
# Linux high speed capture support
af-packet:
  - interface: enp0s3_
```

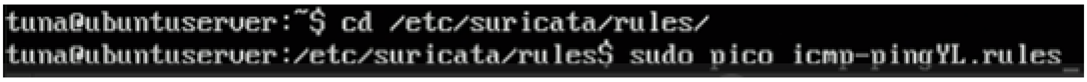


```
tunaybs@tunaubuntuybs:~$ suricata -c /etc/suricata/suricata.yaml /i enp0s3_
```



```
tuna@ubuntuserver:~$ suricata -c/etc/suricata/suricata.yaml -i enp0s3
Warning: debug: error opening file /var/log/suricata//suricata.log: Permission denied
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
E: suricata: The logging directory "/var/log/suricata/" supplied by /etc/suricata/suricata.yaml (default-log-dir) is not
tuna@ubuntuserver:~$ sudo suricata -c/etc/suricata/suricata.yaml -i enp0s3
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
W: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
W: detect: 1 rule files specified, but no rules were loaded!
i: threads: Threads created -> W: 6 FM: 1 FR: 1   Engine started.
```

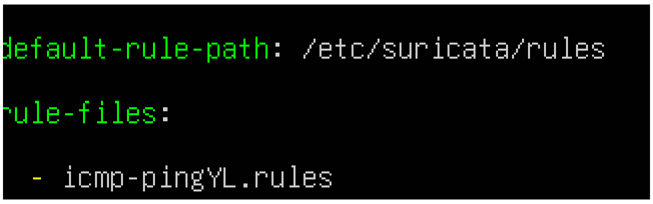
YENİ KURAL DOSYASI OLUŞTURMA



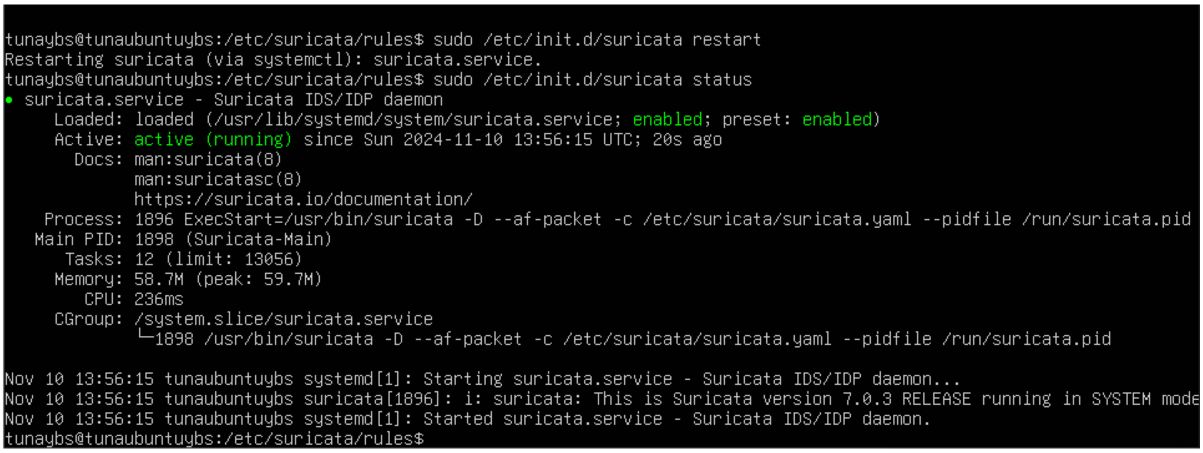
```
tuna@ubuntuserver:~$ cd /etc/suricata/rules/
tuna@ubuntuserver:/etc/suricata/rules$ sudo pico icmp-pingYL.rules_
```

OLUŞTURDUĞUMUZ YENİ KURAL DOSYAMIZIN İÇİNE BUNU YAZIYORUZ alert icmp any any -> any any (msg:"Sn YL Ogrencileri ICMP Echo Request (Ping) detected"; itype:8;sid:1000001; rev:1;)

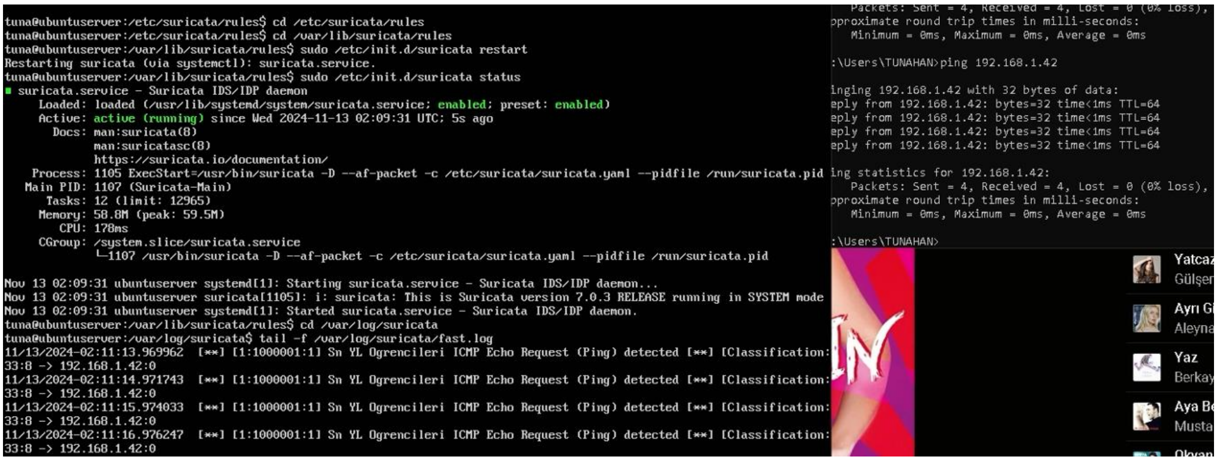
KONFİGRASYON AYARLARIMIZDAN KURAL AYARLARIMIZI DEĞİŞTİRİYORUZ



```
default-rule-path: /etc/suricata/rules

rule-files:

  - icmp-pingYL.rules
```

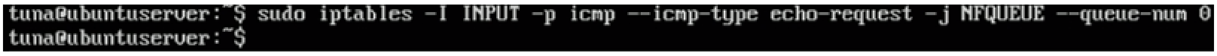


```
tunaybs@tunaubuntuybs:/etc/suricata/rules$ sudo /etc/init.d/suricata restart
Restarting suricata (via systemctl): suricata.service.
tunaybs@tunaubuntuybs:/etc/suricata/rules$ sudo /etc/init.d/suricata status
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Sun 2024-11-10 13:56:15 UTC; 20s ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 1896 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid
   Main PID: 1898 (Suricata-Main)
      Tasks: 12 (limit: 13056)
     Memory: 58.7M (peak: 59.7M)
        CPU: 236ms
     CGroup: /system.slice/suricata.service
             └─1898 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Nov 10 13:56:15 tunaubuntuybs systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Nov 10 13:56:15 tunaubuntuybs suricata[1896]: i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Nov 10 13:56:15 tunaubuntuybs systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
tunaybs@tunaubuntuybs:/etc/suricata/rules$
```

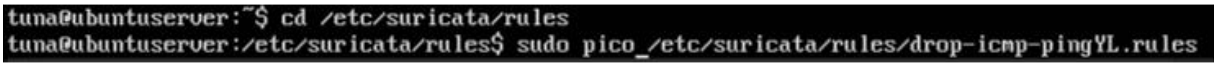


```
tuna@ubuntuserver:/etc/suricata/rules$ cd /etc/suricata/rules
tuna@ubuntuserver:/etc/suricata/rules$ cd /var/lib/suricata/rules
tuna@ubuntuserver:/var/lib/suricata/rules$ sudo /etc/init.d/suricata restart
Restarting suricata (via systemctl): suricata.service.
tuna@ubuntuserver:/var/lib/suricata/rules$ sudo /etc/init.d/suricata status
■ suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Wed 2024-11-13 02:09:31 UTC; 5s ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 1105 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid
   Main PID: 1107 (Suricata-Main)
      Tasks: 12 (limit: 12965)
     Memory: 58.8M (peak: 59.5M)
        CPU: 178ms
     CGroup: /system.slice/suricata.service
             └─1107 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Nov 13 02:09:31 ubuntuserver systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Nov 13 02:09:31 ubuntuserver suricata[1105]: i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Nov 13 02:09:31 ubuntuserver systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
tuna@ubuntuserver:/var/lib/suricata/rules$ cd /var/log/suricata
tuna@ubuntuserver:/var/log/suricata$ tail -f /var/log/suricata/fast.log
11/13/2024-02:11:13.969962  [**] [1:1000001:1] Sn YL Ogrencileri ICMP Echo Request (Ping) detected [**] [Classification:
33:8 -> 192.168.1.42:0
11/13/2024-02:11:14.971743  [**] [1:1000001:1] Sn YL Ogrencileri ICMP Echo Request (Ping) detected [**] [Classification:
33:8 -> 192.168.1.42:0
11/13/2024-02:11:15.974033  [**] [1:1000001:1] Sn YL Ogrencileri ICMP Echo Request (Ping) detected [**] [Classification:
33:8 -> 192.168.1.42:0
11/13/2024-02:11:16.976247  [**] [1:1000001:1] Sn YL Ogrencileri ICMP Echo Request (Ping) detected [**] [Classification:
33:8 -> 192.168.1.42:0
```

```
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms

:\Users\TUNAHAN>ping 192.168.1.42

inging 192.168.1.42 with 32 bytes of data:
eply from 192.168.1.42: bytes=32 time<1ms TTL=64
eply from 192.168.1.42: bytes=32 time<1ms TTL=64
eply from 192.168.1.42: bytes=32 time<1ms TTL=64
eply from 192.168.1.42: bytes=32 time<1ms TTL=64

ing statistics for 192.168.1.42:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms

:\Users\TUNAHAN>
```



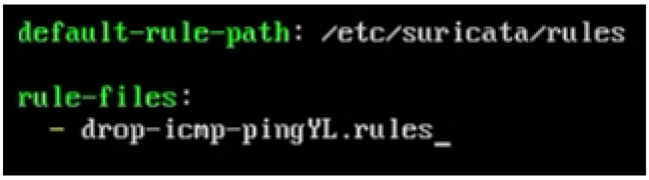
```
tuna@ubuntuserver:~$ sudo iptables -I INPUT -p icmp --icmp-type echo-request -j NFQUEUE --queue-num 0
tuna@ubuntuserver:~$
```



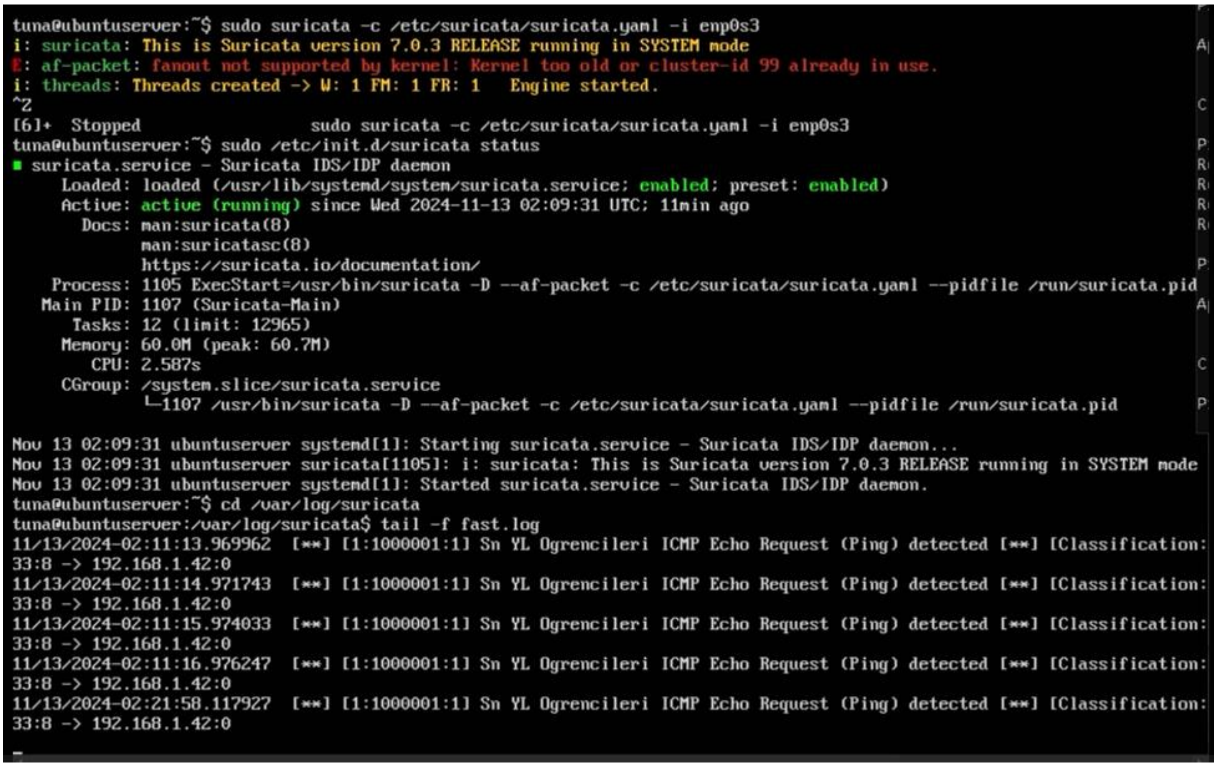
```
tuna@ubuntuserver:~$ cd /etc/suricata/rules
tuna@ubuntuserver:/etc/suricata/rules$ sudo pico_/etc/suricata/rules/drop-icmp-pingYL.rules
```

YENİ OLUŞTURACAĞIMIZ DOSYAYA ALTTAKİ GİBİ YAZIYORUZ

- drop icmp any any -> 192.168.1.137 any (msg:"SnYLOgrencileri Dropped ICMP Echo Request (Ping)"; itype:8;sid:1000002; rev:1;)



```
default-rule-path: /etc/suricata/rules

rule-files:
  - drop-icmp-pingYL.rules_
```



```
tuna@ubuntuserver:~$ sudo suricata -c /etc/suricata/suricata.yaml -i enp0s3
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
E: af-packet: fanout not supported by kernel: Kernel too old or cluster-id 99 already in use.
i: threads: Threads created -> W: 1 FM: 1 FR: 1   Engine started.
^Z
[6]+  Stopped                 sudo suricata -c /etc/suricata/suricata.yaml -i enp0s3
tuna@ubuntuserver:~$ sudo /etc/init.d/suricata status
■ suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Wed 2024-11-13 02:09:31 UTC; 11min ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 1105 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid
   Main PID: 1107 (Suricata-Main)
      Tasks: 12 (limit: 12965)
     Memory: 60.0M (peak: 60.7M)
        CPU: 2.587s
     CGroup: /system.slice/suricata.service
             └─1107 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Nov 13 02:09:31 ubuntuserver systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Nov 13 02:09:31 ubuntuserver suricata[1105]: i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Nov 13 02:09:31 ubuntuserver systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
tuna@ubuntuserver:~$ cd /var/log/suricata
tuna@ubuntuserver:/var/log/suricata$ tail -f fast.log
11/13/2024-02:11:13.969962  [**] [1:1000001:1] Sn YL Ogrencileri ICMP Echo Request (Ping) detected [**] [Classification:
33:8 -> 192.168.1.42:0
11/13/2024-02:11:14.971743  [**] [1:1000001:1] Sn YL Ogrencileri ICMP Echo Request (Ping) detected [**] [Classification:
33:8 -> 192.168.1.42:0
11/13/2024-02:11:15.974033  [**] [1:1000001:1] Sn YL Ogrencileri ICMP Echo Request (Ping) detected [**] [Classification:
33:8 -> 192.168.1.42:0
11/13/2024-02:11:16.976247  [**] [1:1000001:1] Sn YL Ogrencileri ICMP Echo Request (Ping) detected [**] [Classification:
33:8 -> 192.168.1.42:0
11/13/2024-02:21:58.117927  [**] [1:1000001:1] Sn YL Ogrencileri ICMP Echo Request (Ping) detected [**] [Classification:
33:8 -> 192.168.1.42:0

_
```