Date. |
Page. |

other IDS

Intrusion detection system (Snort)

- # Zeek
- # suricata

60.0.0.13

- Consider two machines attacker and victim
  ↳ 60.0.0.14

On victim machine, IDS installed

- sudo apt-get installe snort

Find directory

- which snort

Snort has configuration file

- cd /etc/snort

Snort.lua : snort configuration file

Add the following in configuration file

```
HOME_NET = {'60.0.0.14/24'}
EXTERNAL_NET = '!$HOME_NET'
```

Snort is a rule based system

- cd /usr/ local/ etc/ rules
- ls
  ↳ some rules are already there

create my-~~rule~~rules.rules
↳ add rules here

Format:

Protocol any direction any any

```
alert icmp <source_ip><source_port> → <dip> <dport>
(
msg ("ICMP Attemp"; sid : 1000005;)
```

Action Rule header

Rule option ↳ Rule id

[illegible]

configuration file ↙ Rule file ↙

```
Sudo snort -c /etc/snort/snort.lua -R
/usr/local/etc/rules/my-rules.rules -i eth0
-A alert-fast
```

hping3 : tool in kali to generate high traffic
(by default in kali)

Alerts appear on victim machine

<u>On Attacker machine</u>

```
sudo hping3 --icmp --fast 60.0.0.14
```

--icmp ↓ protocol

--fast ↓ rate of packet
can be fast/flood
(10packets/sec) (1000 packets/s)

<u>ON VICTIM</u>

*

```
sudo systemctl start apache2
```

```
cd /var/www/html
ls
```

index.html changed , <script> to check status of server

run this on victim (open through chrome)

from attacker; hping3 flood on port 80 ⇒ on victim server unresponsive (After long time)

Smurf Attack

takes leaverage of broadcast message

on Attacker

```
                      spoofing ip        broadcast ip
hping3  --icmp  -a 10.10.10.0     60.0.0.14
```

on victim

icmp packets from 10.10.10.0 → 60.0.0.14
using tcp dump

Attacker

↳ sends broadcast message with spoofed ip
(victim ip)

packets sent to all machines.
All machines will send reply packets to spoofed ip
(victim in our case)

```
hping3  --icmp  -a 60.0.0.3    60.0.0.255
```

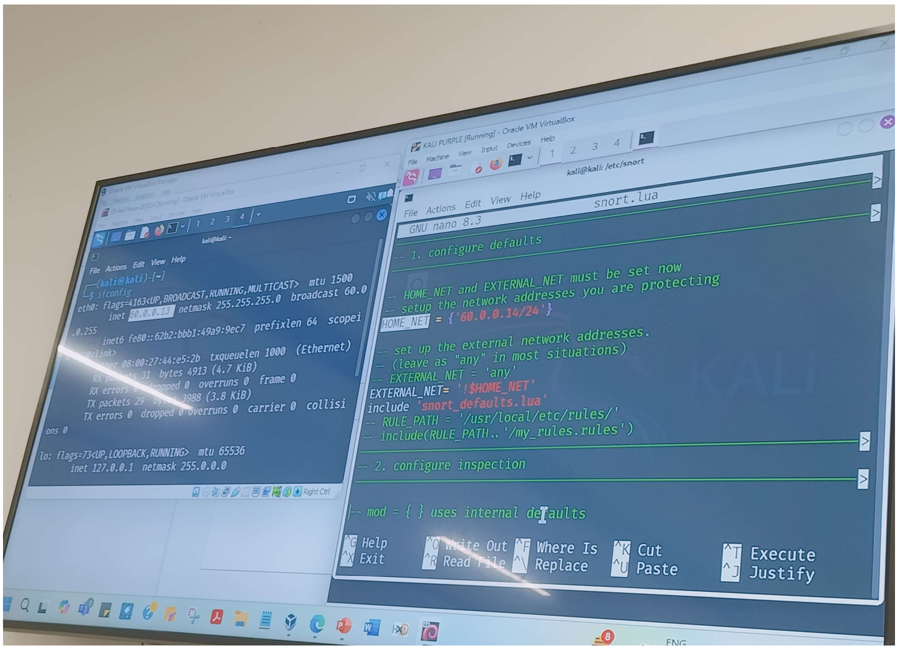
Smurf DDos Attack

from our machine to attack 60.0.0.3

set icmp-echo-ignore broadcast to 0 → using sudo systemctl

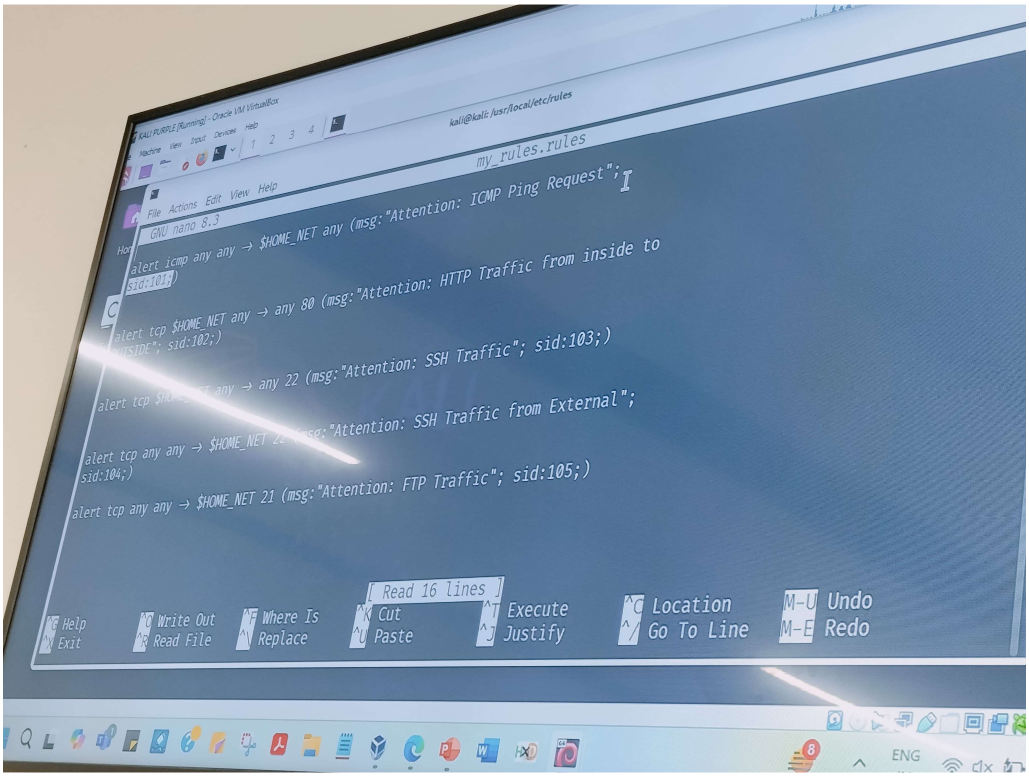
↳ cat /proc/sys/net/ipv4/icmp-echo-ignore-broadcast
to check value

Changes to be done in configuration file



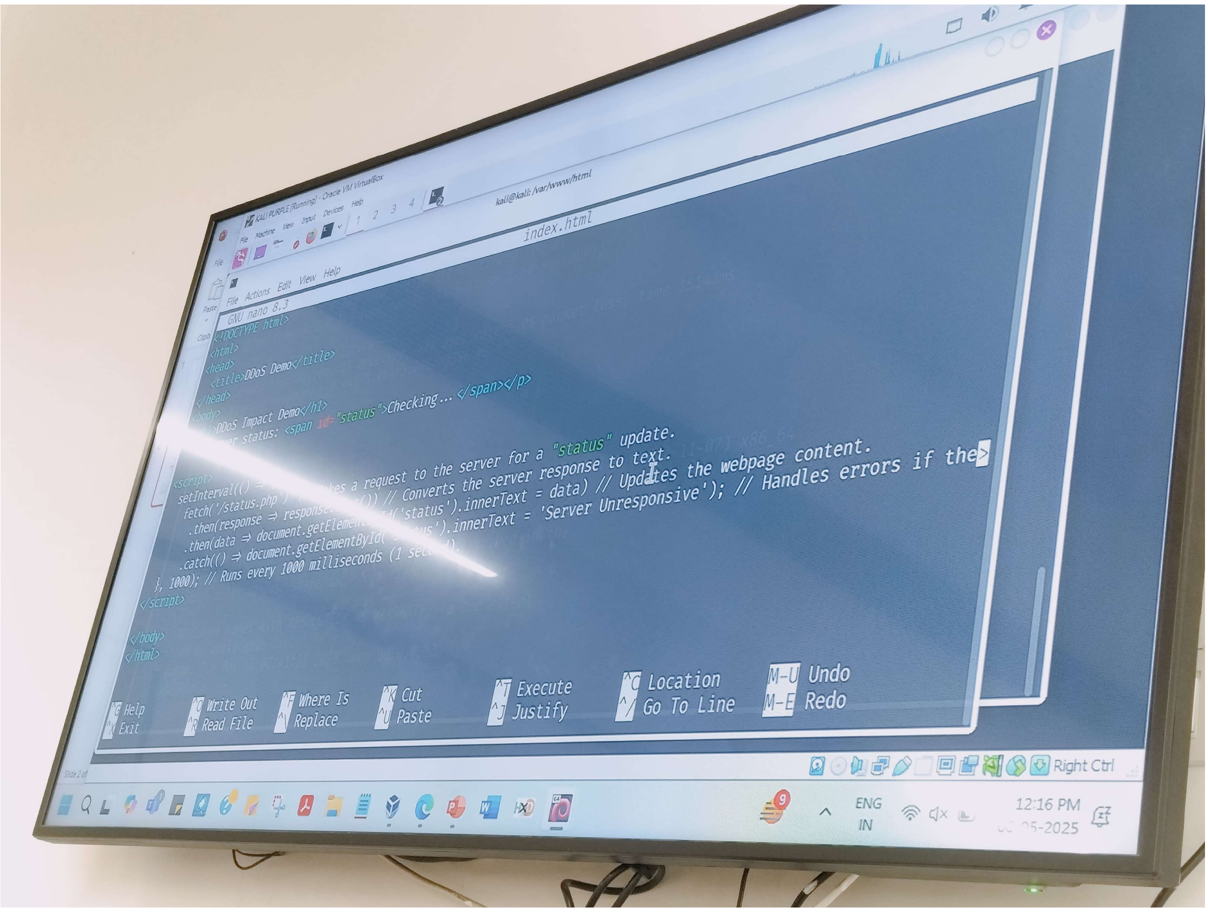
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 60.0.0.13  netmask 255.255.255.0  broadcast 60.0.0.255
        inet6 fe80::62b2:bbb1:49a9:9ec7  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:44:e5:2b  txqueuelen 1000  (Ethernet)
        RX packets 31  bytes 4913 (4.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 3988 (3.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
```

```
GNU nano 8.3                         snort.lua
---------------------------------------------------------------------
-- 1. configure defaults
---------------------------------------------------------------------

-- HOME_NET and EXTERNAL_NET must be set now
-- setup the network addresses you are protecting
HOME_NET = {'60.0.0.14/24'}

-- set up the external network addresses.
-- (leave as "any" in most situations)
-- EXTERNAL_NET = 'any'
EXTERNAL_NET= '!$HOME_NET'
include 'snort_defaults.lua'
-- RULE_PATH = '/usr/local/etc/rules/'
-- include(RULE_PATH..'/my_rules.rules')
---------------------------------------------------------------------
-- 2. configure inspection
---------------------------------------------------------------------

-- mod = { } uses internal defaults
```



```
GNU nano 8.3                         my_rules.rules

alert icmp any any → $HOME_NET any (msg:"Attention: ICMP Ping Request";
sid:101;)

alert tcp $HOME_NET any → any 80 (msg:"Attention: HTTP Traffic from inside to
OUTSIDE"; sid:102;)

alert tcp $HOME_NET any → any 22 (msg:"Attention: SSH Traffic"; sid:103;)

alert tcp any any → $HOME_NET 22 (msg:"Attention: SSH Traffic from External";
sid:104;)

alert tcp any any → $HOME_NET 21 (msg:"Attention: FTP Traffic"; sid:105;)

                              [ Read 16 lines ]
```

Alert rules added in my_rules.rules



```
  GNU nano 8.3                         index.html
<!DOCTYPE html>
<html>
<head>
  <title>DDoS Demo</title>
</head>
<body>
  <h1>DDoS Impact Demo</h1>
  [illegible]er status: <span id="status">Checking... </span></p>

<script>
  setInterval(() => {
    fetch('/status.php') // Makes a request to the server for a "status" update.
      .then(response => response.text()) // Converts the server response to text.
      .then(data => document.getElementById('status').innerText = data) // Updates the webpage content.
      .catch(() => document.getElementById('status').innerText = 'Server Unresponsive'); // Handles errors if the>
  }, 1000); // Runs every 1000 milliseconds (1 second).
</script>

</body>
</html>

^G Help      ^O Write Out   ^F Where Is   ^K Cut     ^T Execute   ^C Location     M-U Undo
^X Exit      ^R Read File   ^\ Replace    ^U Paste   ^J Justify   ^/ Go To Line   M-E Redo
```

Script tag in index.html