TASK-2 : WAZUH x FIREWALL

Syed Muhammad Shah

TEAM ~ OMEGA

1) installing Firewall in Kali Linux (Agent)

Sudo apt install ufw

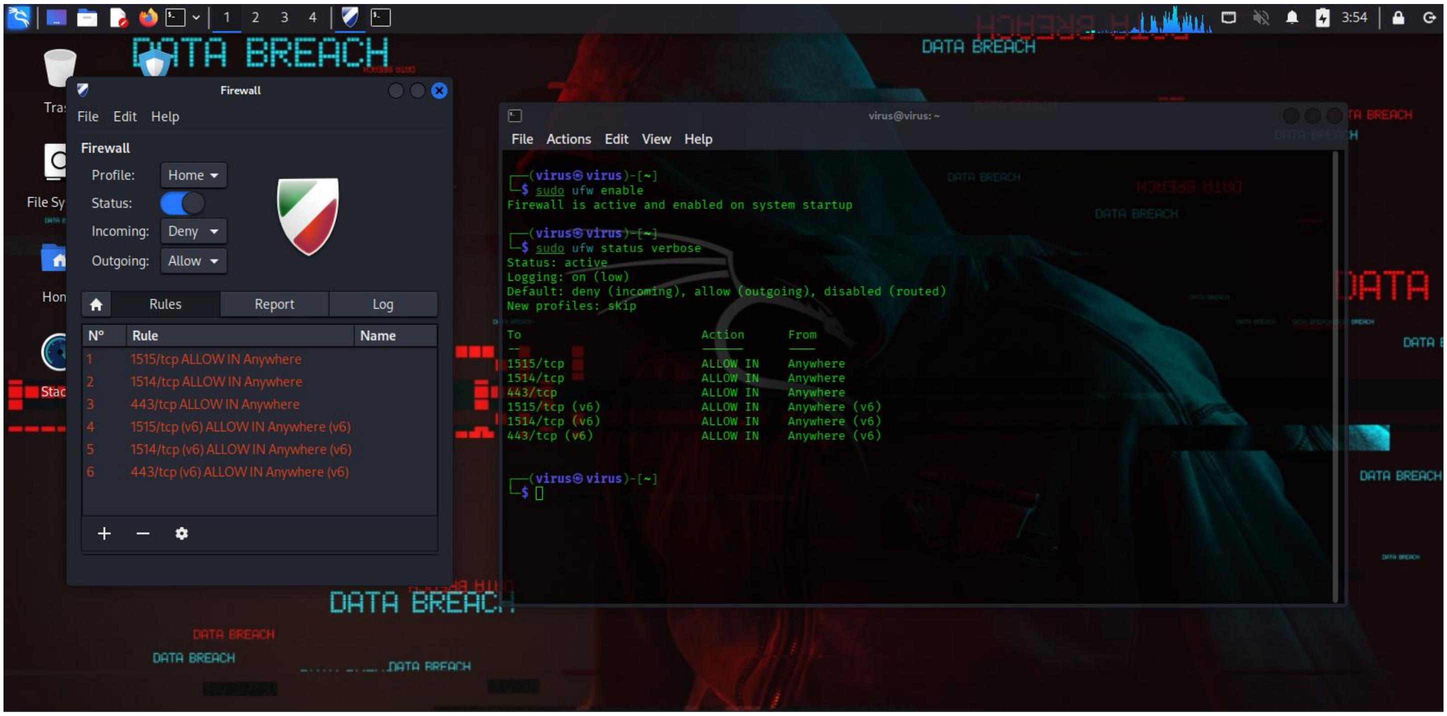
Sudo apt install gufw

sudo ufw enable

sudo ufw status verbose

Sudo apt update

Sudo apt upgrade



Firewall

Profile: Home

Status: ●

Incoming: Deny

Outgoing: Allow

N°	Rule	Name
1	1515/tcp ALLOW IN Anywhere	
2	1514/tcp ALLOW IN Anywhere	
3	443/tcp ALLOW IN Anywhere	
4	1515/tcp (v6) ALLOW IN Anywhere (v6)	
5	1514/tcp (v6) ALLOW IN Anywhere (v6)	
6	443/tcp (v6) ALLOW IN Anywhere (v6)	

```
┌──(virus㉿virus)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

┌──(virus㉿virus)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
1515/tcp                   ALLOW IN    Anywhere
1514/tcp                   ALLOW IN    Anywhere
443/tcp                    ALLOW IN    Anywhere
1515/tcp (v6)              ALLOW IN    Anywhere (v6)
1514/tcp (v6)              ALLOW IN    Anywhere (v6)
443/tcp (v6)               ALLOW IN    Anywhere (v6)


┌──(virus㉿virus)-[~]
└─$ 
```

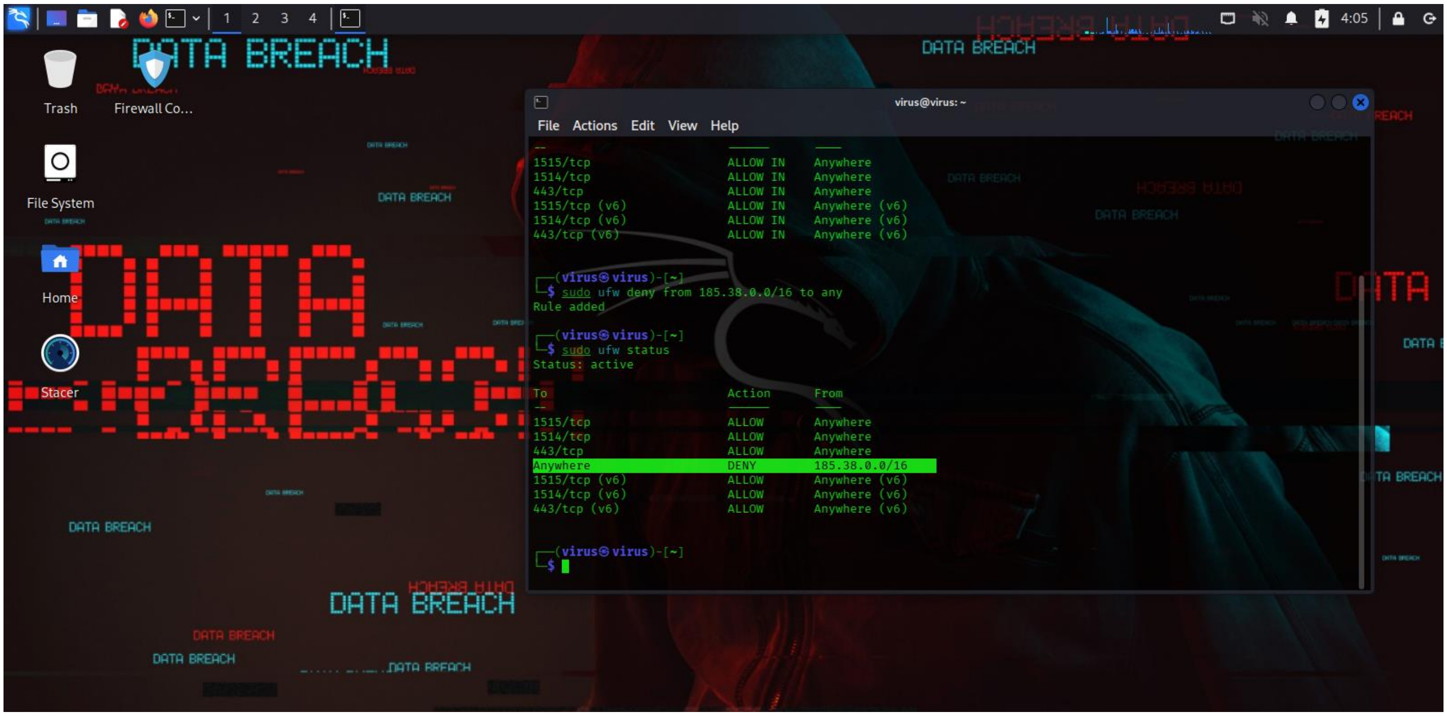
2) Configurations & Rules (FireWall)

UFW logs go to **/var/log/ufw.log** or **/var/log/syslog**

A) Block Country Traffic (Russia)

Since UFW doesn’t support GeoIP , So i used Russian ip Ranges To Stimulate Our Task . (https://www.ip2location.com/free/visitor-blocker) using this website to get ip CIDRs .

sudo ufw deny from 185.38.0.0/16 to any



```
--                         ------      ----
1515/tcp                   ALLOW IN    Anywhere
1514/tcp                   ALLOW IN    Anywhere
443/tcp                    ALLOW IN    Anywhere
1515/tcp (v6)              ALLOW IN    Anywhere (v6)
1514/tcp (v6)              ALLOW IN    Anywhere (v6)
443/tcp (v6)               ALLOW IN    Anywhere (v6)


┌──(virus㉿virus)-[~]
└─$ sudo ufw deny from 185.38.0.0/16 to any
Rule added

┌──(virus㉿virus)-[~]
└─$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
1515/tcp                   ALLOW       Anywhere
1514/tcp                   ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
Anywhere                   DENY        185.38.0.0/16
1515/tcp (v6)              ALLOW       Anywhere (v6)
1514/tcp (v6)              ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)


┌──(virus㉿virus)-[~]
└─$ 
```

B) Block Access to Specific Websites (Youtube,Facebook)

nslookup facebook.com

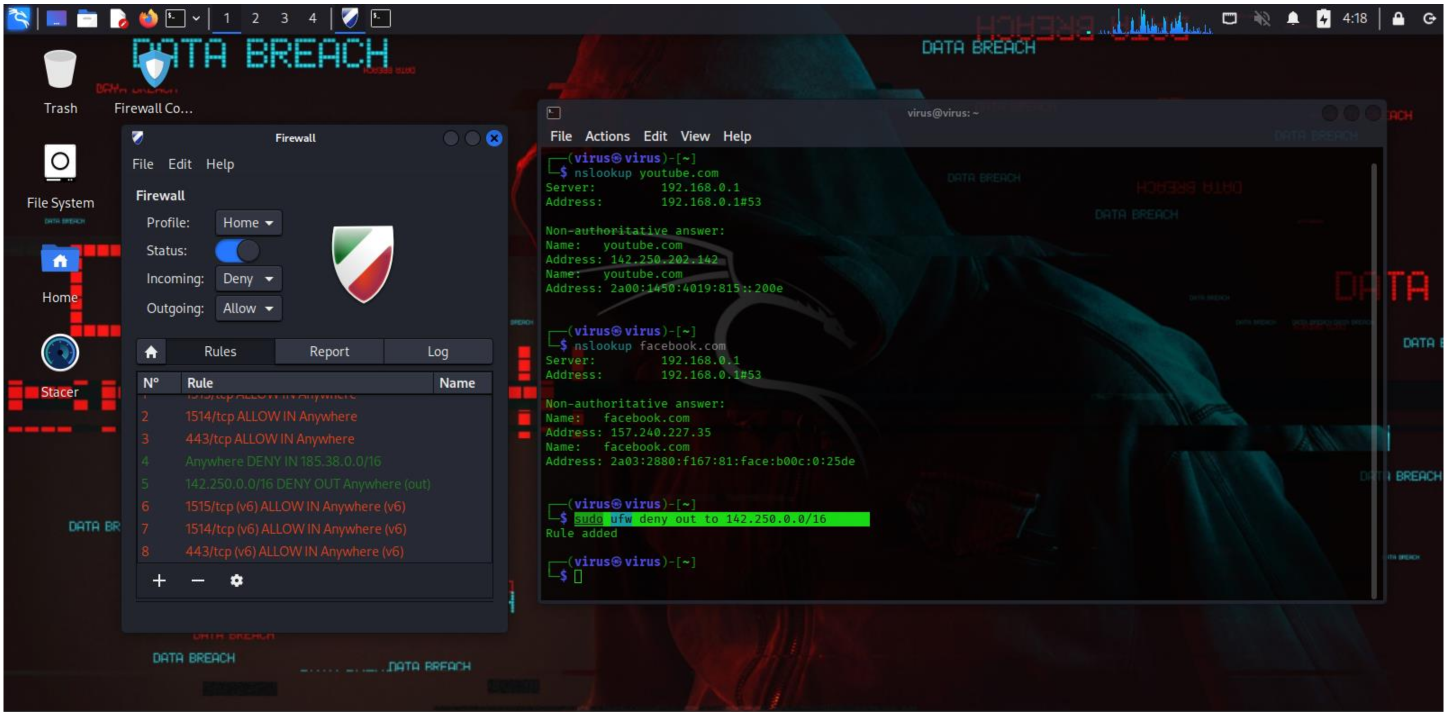
nslookup youtube.com

After Getting their ips ,

we block them using their whole range as CIDR (ip Class B)

sudo ufw deny out to 157.240.0.0/16

sudo ufw deny out to 142.250.0.0/16



Firewall

Profile: Home

Status: on

Incoming: Deny

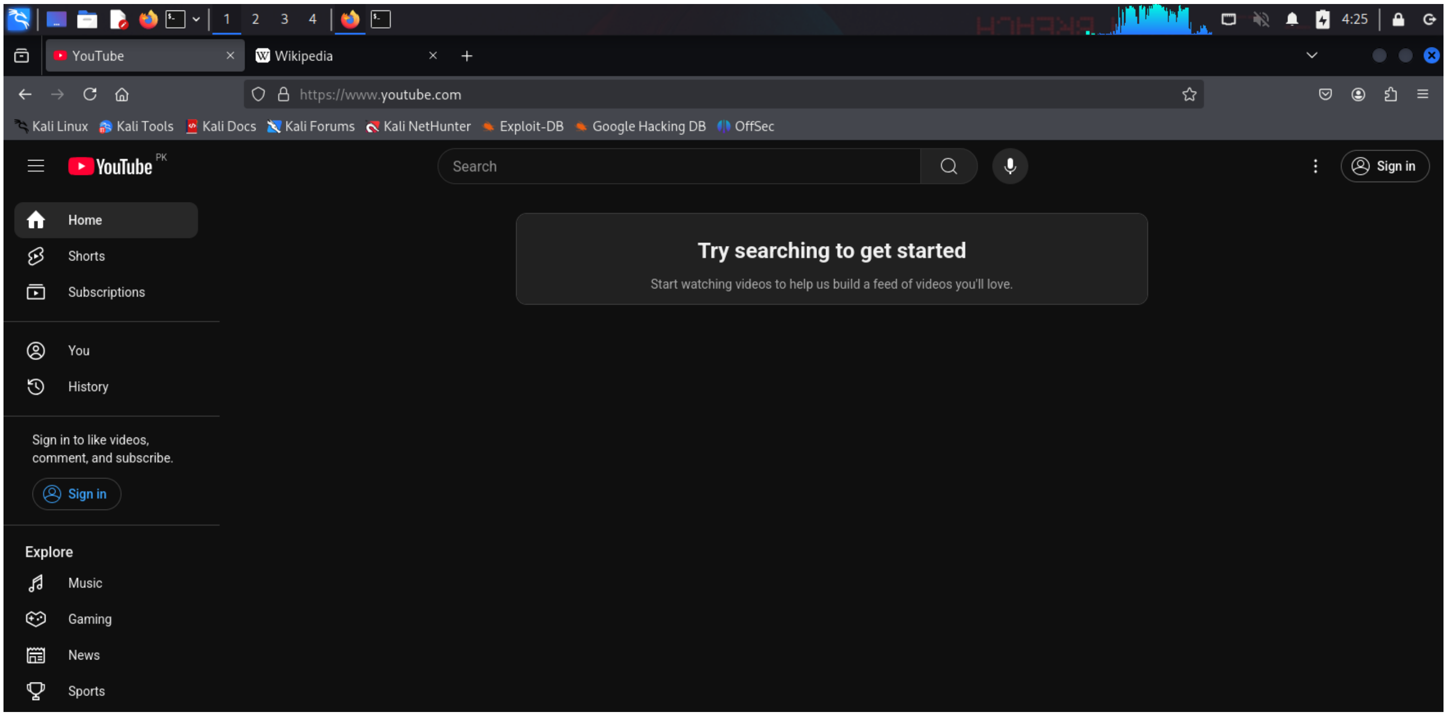
Outgoing: Allow

Nº	Rule	Name
1	1515/tcp ALLOW IN Anywhere	
2	1514/tcp ALLOW IN Anywhere	
3	443/tcp ALLOW IN Anywhere	
4	Anywhere DENY IN 185.38.0.0/16	
5	142.250.0.0/16 DENY OUT Anywhere (out)	
6	1515/tcp (v6) ALLOW IN Anywhere (v6)	
7	1514/tcp (v6) ALLOW IN Anywhere (v6)	
8	443/tcp (v6) ALLOW IN Anywhere (v6)	

```
┌──(virus㉿virus)-[~]
└─$ nslookup youtube.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   youtube.com
Address: 142.250.202.142
Name:   youtube.com
Address: 2a00:1450:4019:815::200e


┌──(virus㉿virus)-[~]
└─$ nslookup facebook.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   facebook.com
Address: 157.240.227.35
Name:   facebook.com
Address: 2a03:2880:f167:81:face:b00c:0:25de


┌──(virus㉿virus)-[~]
└─$ sudo ufw deny out to 142.250.0.0/16
Rule added

┌──(virus㉿virus)-[~]
└─$ 
```

Verification : Firewall Working (100%)

Before:



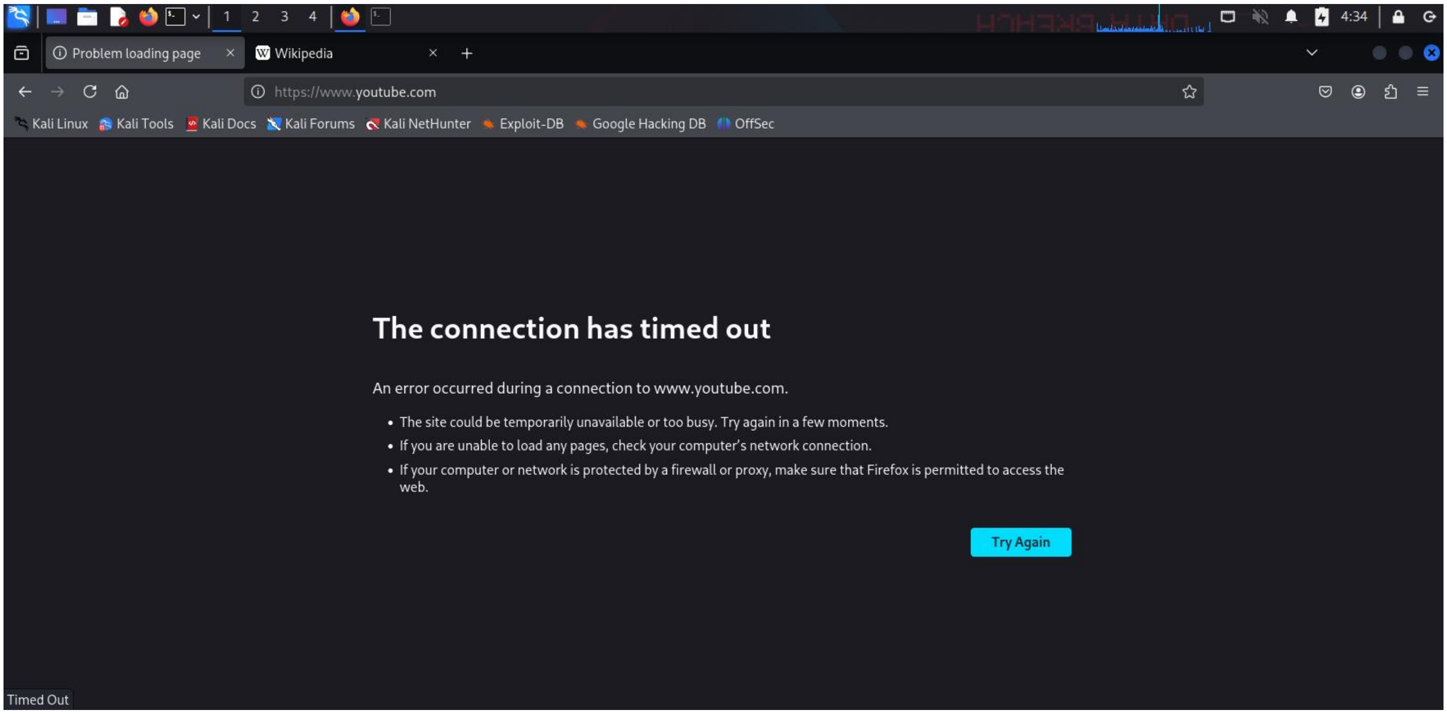
https://www.youtube.com

Try searching to get started

Start watching videos to help us build a feed of videos you'll love.

After:

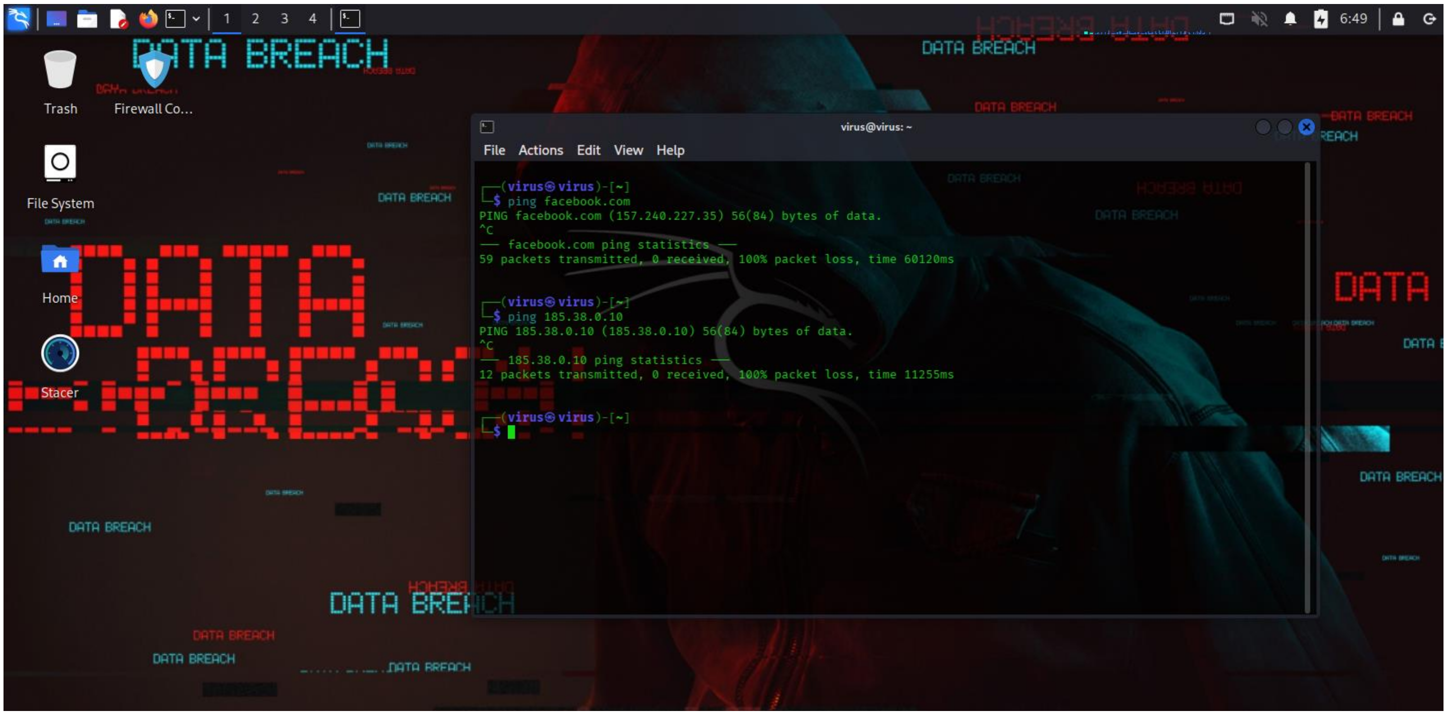
Sudo ufw reload



The connection has timed out

An error occurred during a connection to www.youtube.com.

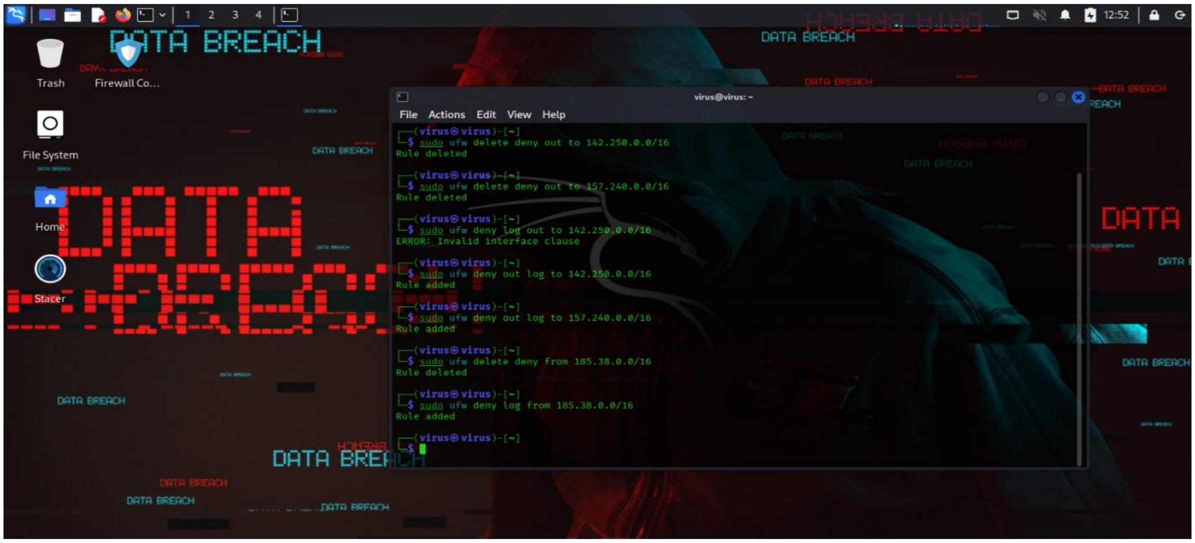
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.



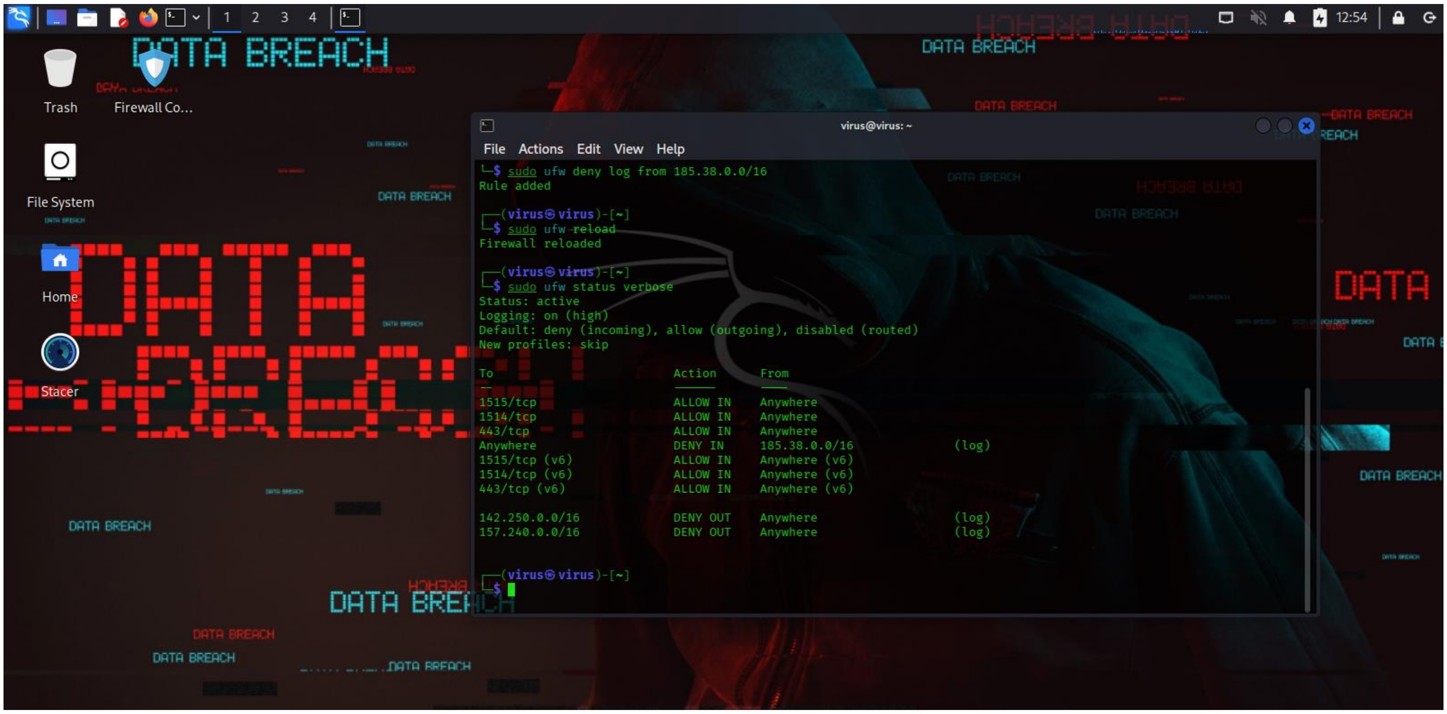
```
┌──(virus㉿virus)-[~]
└─$ ping facebook.com
PING facebook.com (157.240.227.35) 56(84) bytes of data.
^C
--- facebook.com ping statistics ---
59 packets transmitted, 0 received, 100% packet loss, time 60120ms


┌──(virus㉿virus)-[~]
└─$ ping 185.38.0.10
PING 185.38.0.10 (185.38.0.10) 56(84) bytes of data.
^C
--- 185.38.0.10 ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 11255ms


┌──(virus㉿virus)-[~]
└─$ 
```

ISSUE: Here we got an issue , the firewall blocks the traffic but did not store logs on high stream . which wazuh cant detect by local rules . to fix this , so we delete the rules and create again on high logout to their syslog & ufw log files .

```
sudo ufw delete deny out to 142.250.0.0/16

sudo ufw delete deny out to 157.240.0.0/16

sudo ufw delete deny from 185.38.0.0/16

sudo ufw logging high

sudo ufw deny out log to 142.250.0.0/16

sudo ufw deny out log to 157.240.0.0/16

sudo ufw deny log from 185.38.0.0/16

sudo ufw reload

sudo ufw status verbose
```



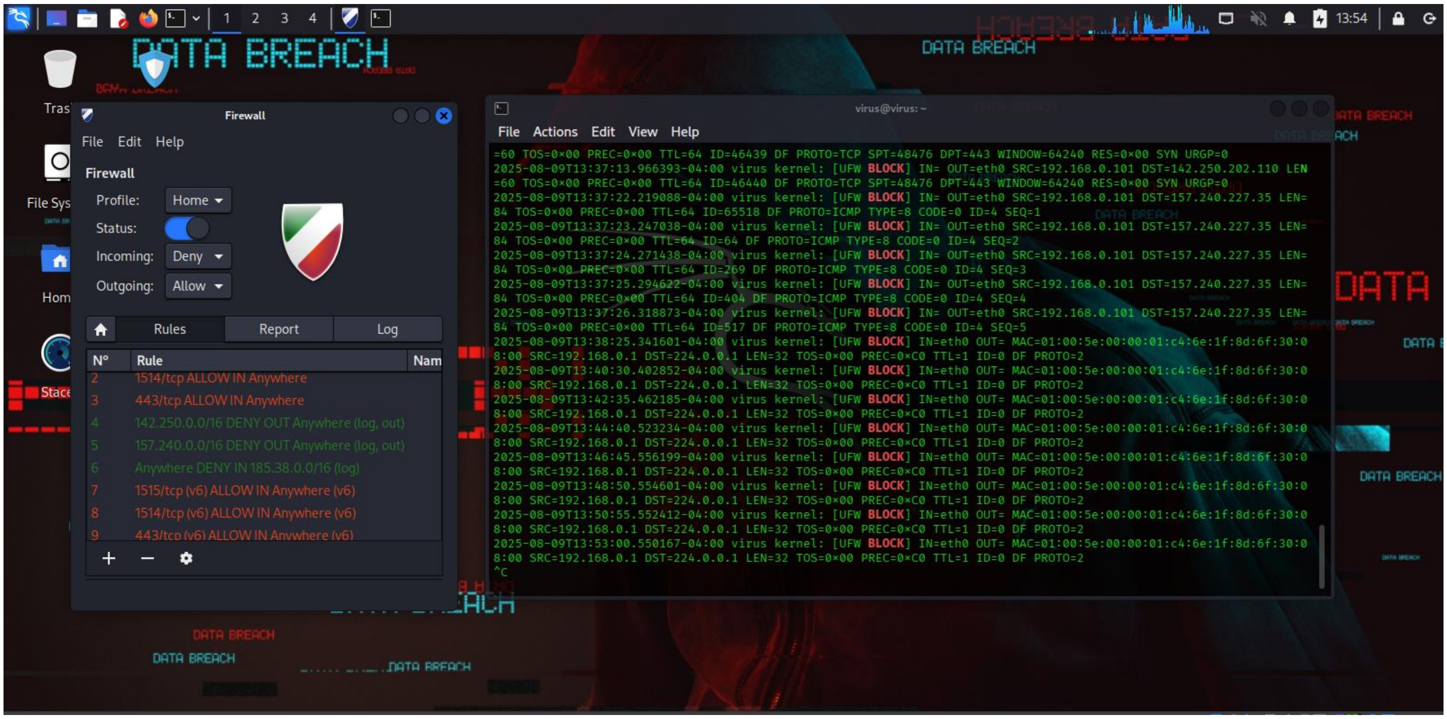
```
┌──(virus㉿virus)-[~]
└─$ sudo ufw delete deny out to 142.250.0.0/16
Rule deleted

┌──(virus㉿virus)-[~]
└─$ sudo ufw delete deny out to 157.240.0.0/16
Rule deleted

┌──(virus㉿virus)-[~]
└─$ sudo ufw deny log out to 142.250.0.0/16
ERROR: Invalid interface clause

┌──(virus㉿virus)-[~]
└─$ sudo ufw deny out log to 142.250.0.0/16
Rule added

┌──(virus㉿virus)-[~]
└─$ sudo ufw deny out log to 157.240.0.0/16
Rule added

┌──(virus㉿virus)-[~]
└─$ sudo ufw delete deny from 185.38.0.0/16
Rule deleted

┌──(virus㉿virus)-[~]
└─$ sudo ufw deny log from 185.38.0.0/16
Rule added

┌──(virus㉿virus)-[~]
└─$ 
```



```
└─$ sudo ufw deny log from 185.38.0.0/16
Rule added

┌──(virus㉿virus)-[~]
└─$ sudo ufw reload
Firewall reloaded

┌──(virus㉿virus)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (high)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
1515/tcp                   ALLOW IN    Anywhere
1514/tcp                   ALLOW IN    Anywhere
443/tcp                    ALLOW IN    Anywhere
Anywhere                   DENY IN     185.38.0.0/16              (log)
1515/tcp (v6)              ALLOW IN    Anywhere (v6)
1514/tcp (v6)              ALLOW IN    Anywhere (v6)
443/tcp (v6)               ALLOW IN    Anywhere (v6)

142.250.0.0/16             DENY OUT    Anywhere                   (log)
157.240.0.0/16             DENY OUT    Anywhere                   (log)


┌──(virus㉿virus)-[~]
└─$ 
```

Confirming Logs Traffic :

sudo tail -f /var/log/ufw.log | grep BLOCK



Firewall

Profile: Home

Status: ●

Incoming: Deny

Outgoing: Allow

N°	Rule	Nam
2	1514/tcp ALLOW IN Anywhere	
3	443/tcp ALLOW IN Anywhere	
4	142.250.0.0/16 DENY OUT Anywhere (log, out)	
5	157.240.0.0/16 DENY OUT Anywhere (log, out)	
6	Anywhere DENY IN 185.38.0.0/16 (log)	
7	1515/tcp (v6) ALLOW IN Anywhere (v6)	
8	1514/tcp (v6) ALLOW IN Anywhere (v6)	
9	443/tcp (v6) ALLOW IN Anywhere (v6)	

```
=60 TOS=0×00 PREC=0×00 TTL=64 ID=46439 DF PROTO=TCP SPT=48476 DPT=443 WINDOW=64240 RES=0×00 SYN URGP=0
2025-08-09T13:37:13.966393-04:00 virus kernel: [UFW BLOCK] IN= OUT=eth0 SRC=192.168.0.101 DST=142.250.202.110 LEN
=60 TOS=0×00 PREC=0×00 TTL=64 ID=46440 DF PROTO=TCP SPT=48476 DPT=443 WINDOW=64240 RES=0×00 SYN URGP=0
2025-08-09T13:37:22.219088-04:00 virus kernel: [UFW BLOCK] IN= OUT=eth0 SRC=192.168.0.101 DST=157.240.227.35 LEN=
84 TOS=0×00 PREC=0×00 TTL=64 ID=65518 DF PROTO=ICMP TYPE=8 CODE=0 ID=4 SEQ=1
2025-08-09T13:37:23.247038-04:00 virus kernel: [UFW BLOCK] IN= OUT=eth0 SRC=192.168.0.101 DST=157.240.227.35 LEN=
84 TOS=0×00 PREC=0×00 TTL=64 ID=64 DF PROTO=ICMP TYPE=8 CODE=0 ID=4 SEQ=2
2025-08-09T13:37:24.271438-04:00 virus kernel: [UFW BLOCK] IN= OUT=eth0 SRC=192.168.0.101 DST=157.240.227.35 LEN=
84 TOS=0×00 PREC=0×00 TTL=64 ID=269 DF PROTO=ICMP TYPE=8 CODE=0 ID=4 SEQ=3
2025-08-09T13:37:25.294622-04:00 virus kernel: [UFW BLOCK] IN= OUT=eth0 SRC=192.168.0.101 DST=157.240.227.35 LEN=
84 TOS=0×00 PREC=0×00 TTL=64 ID=404 DF PROTO=ICMP TYPE=8 CODE=0 ID=4 SEQ=4
2025-08-09T13:37:26.318873-04:00 virus kernel: [UFW BLOCK] IN= OUT=eth0 SRC=192.168.0.101 DST=157.240.227.35 LEN=
84 TOS=0×00 PREC=0×00 TTL=64 ID=517 DF PROTO=ICMP TYPE=8 CODE=0 ID=4 SEQ=5
2025-08-09T13:38:25.341601-04:00 virus kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:c4:6e:1f:8d:6f:30:0
8:00 SRC=192.168.0.1 DST=224.0.0.1 LEN=32 TOS=0×00 PREC=0×C0 TTL=1 ID=0 DF PROTO=2
2025-08-09T13:40:30.402852-04:00 virus kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:c4:6e:1f:8d:6f:30:0
8:00 SRC=192.168.0.1 DST=224.0.0.1 LEN=32 TOS=0×00 PREC=0×C0 TTL=1 ID=0 DF PROTO=2
2025-08-09T13:42:35.462185-04:00 virus kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:c4:6e:1f:8d:6f:30:0
8:00 SRC=192.168.0.1 DST=224.0.0.1 LEN=32 TOS=0×00 PREC=0×C0 TTL=1 ID=0 DF PROTO=2
2025-08-09T13:44:40.523234-04:00 virus kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:c4:6e:1f:8d:6f:30:0
8:00 SRC=192.168.0.1 DST=224.0.0.1 LEN=32 TOS=0×00 PREC=0×C0 TTL=1 ID=0 DF PROTO=2
2025-08-09T13:46:45.556199-04:00 virus kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:c4:6e:1f:8d:6f:30:0
8:00 SRC=192.168.0.1 DST=224.0.0.1 LEN=32 TOS=0×00 PREC=0×C0 TTL=1 ID=0 DF PROTO=2
2025-08-09T13:48:50.554601-04:00 virus kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:c4:6e:1f:8d:6f:30:0
8:00 SRC=192.168.0.1 DST=224.0.0.1 LEN=32 TOS=0×00 PREC=0×C0 TTL=1 ID=0 DF PROTO=2
2025-08-09T13:50:55.552412-04:00 virus kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:c4:6e:1f:8d:6f:30:0
8:00 SRC=192.168.0.1 DST=224.0.0.1 LEN=32 TOS=0×00 PREC=0×C0 TTL=1 ID=0 DF PROTO=2
2025-08-09T13:53:00.550167-04:00 virus kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:c4:6e:1f:8d:6f:30:0
8:00 SRC=192.168.0.1 DST=224.0.0.1 LEN=32 TOS=0×00 PREC=0×C0 TTL=1 ID=0 DF PROTO=2
^C
```

Also confirm other side if :

Check the agent log: sudo tail -n 50 /var/ossec/logs/ossec.log

Wazuh Manager (OVA) Logs : sudo tail -n 100 /var/ossec/logs/alerts/alerts.json | grep test_fim

C) Monitor Administrator Privileges

sudo ls /root or sudo su or any sudo related command

These actions are **automatically logged by Linux and detected by Wazuh**, as long as the agent is monitoring **/var/log/auth.log**.

To Stimulate SSH Blockage By UFW ,

sudo ufw allow from 192.168.0.105 to any port 22 then sudo ufw deny 22 to restrict others.

Or

sudo ufw insert 1 allow from 192.168.0.105 to any port 22

sudo ufw deny log 22

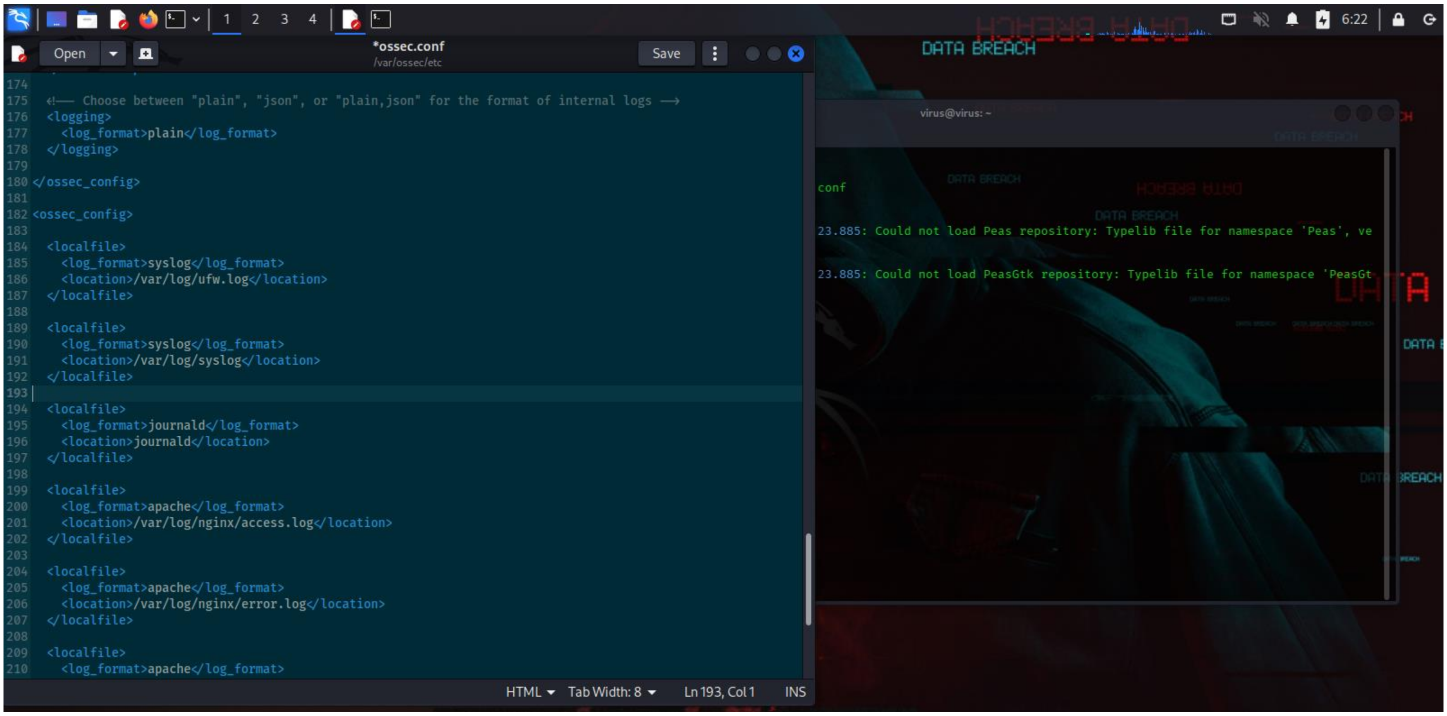
After This The Logs Will be Monitored By Wazuh .

3) Connecting Wazuh With FireWall

In the agent config , sudo gedit /var/ossec/etc/ossec.conf

Add ,

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/ufw.log</location>
</localfile>
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/syslog</location>
</localfile>
```



```
  <!-- Choose between "plain", "json", or "plain,json" for the format of internal logs -->
  <logging>
    <log_format>plain</log_format>
  </logging>

</ossec_config>

<ossec_config>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/ufw.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/syslog</location>
  </localfile>

  <localfile>
    <log_format>journald</log_format>
    <location>journald</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/nginx/access.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/nginx/error.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
```

```
conf

23.885: Could not load Peas repository: Typelib file for namespace 'Peas', ve

23.885: Could not load PeasGtk repository: Typelib file for namespace 'PeasGt
```

sudo systemctl restart wazuh-agent

On Wazuh server VM,

```
sudo nano /var/ossec/etc/rules/local_rules.xml
```

Add,

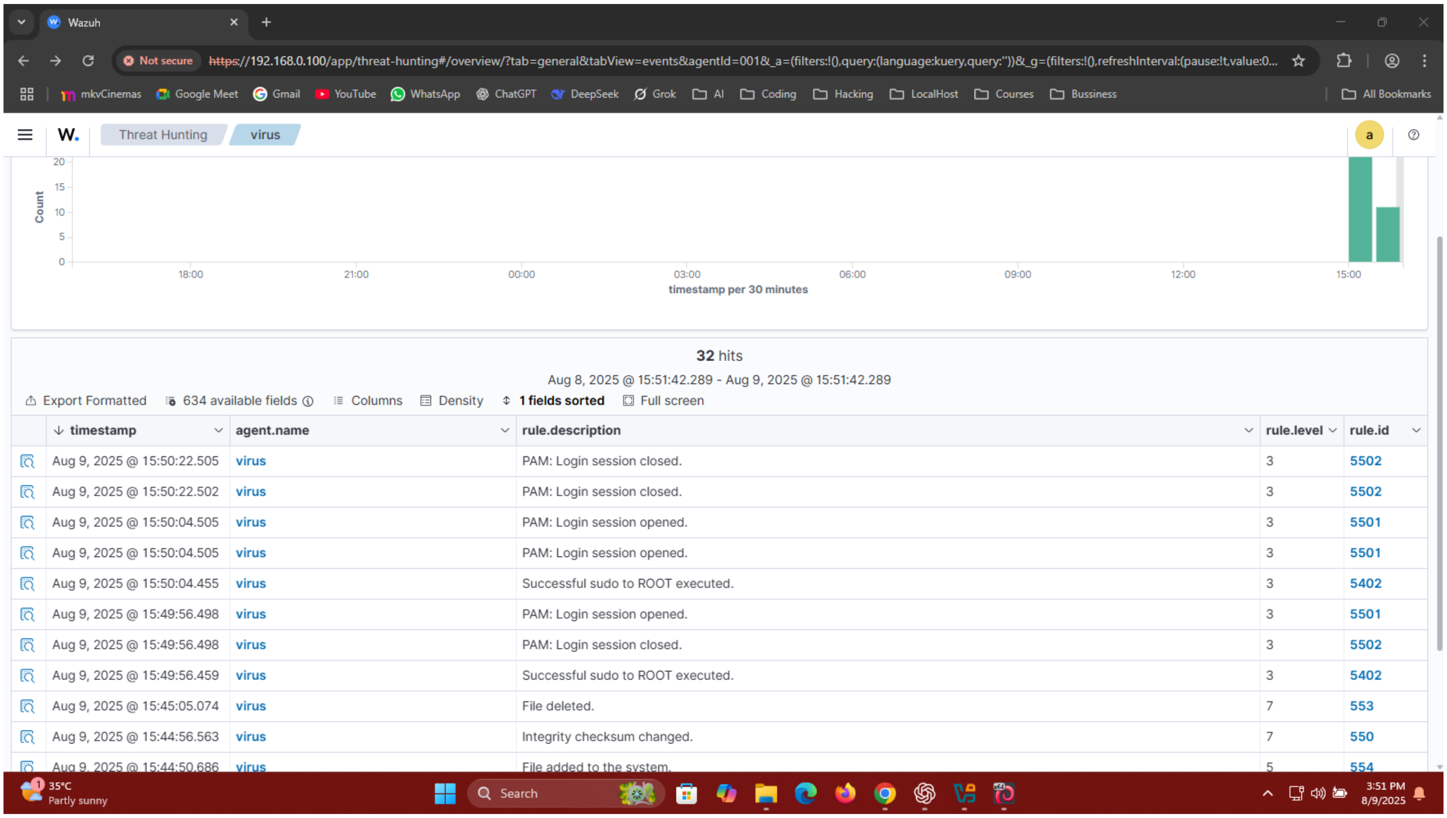
```
<group name="ufw,">
  <rule id="100050" level="7">
    <match>UFW BLOCK</match>
    <description>Traffic Blocked By FireWall UFW</description>
  </rule>
</group>
```

Then , sudo systemctl restart wazuh-manager

4) Monitoring Logs and All Process/Working Check

In Kali agent,

```
ping 185.38.0.10
curl facebook.com
ping facebook.com
curl youtube.com
```

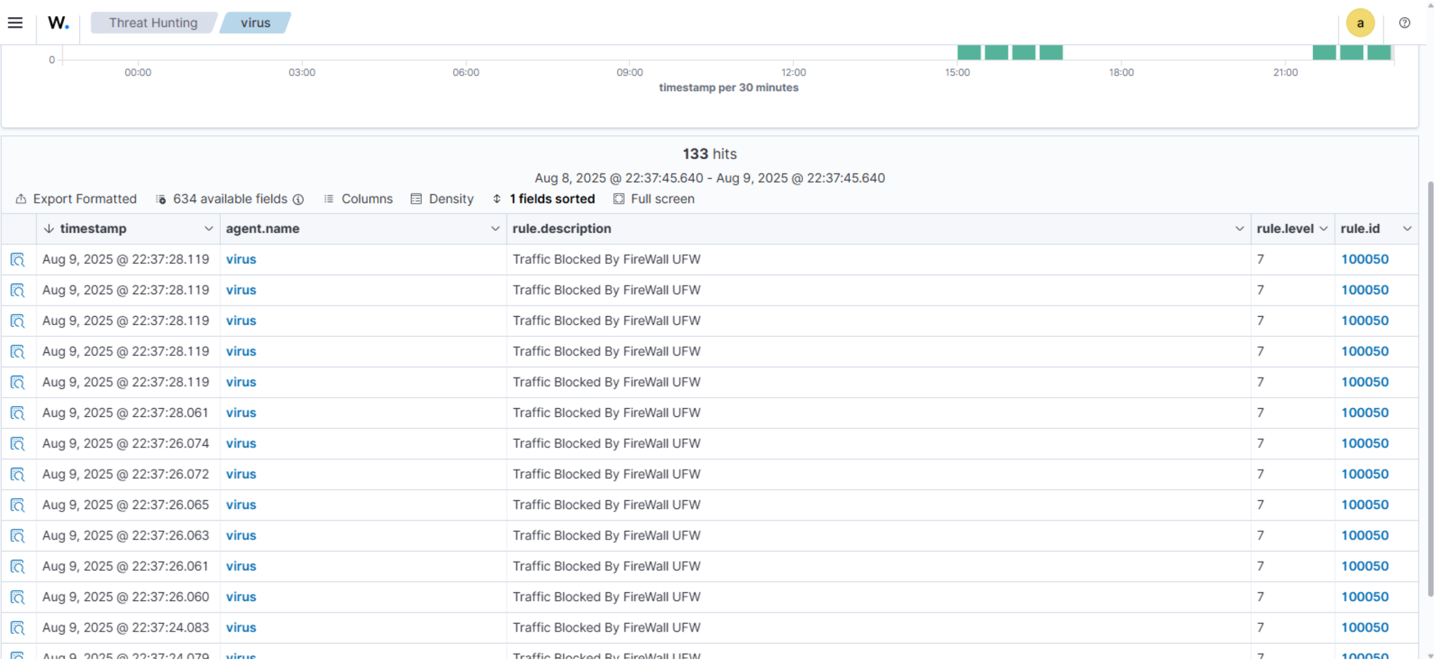

Wazuh
Not secure
https://192.168.0.100/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=001&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,value:0...
mkvCinemas Google Meet Gmail YouTube WhatsApp ChatGPT DeepSeek Grok AI Coding Hacking LocalHost Courses Bussiness All Bookmarks
Threat Hunting
virus
a
Count
20
15
10
5
0
18:00
21:00
00:00
03:00
06:00
09:00
12:00
15:00
timestamp per 30 minutes
35°C
Partly sunny
Search
3:51 PM
8/9/2025

32 hits

Aug 8, 2025 @ 15:51:42.289 - Aug 9, 2025 @ 15:51:42.289

Export Formatted | 634 available fields | Columns | Density | **1 fields sorted** | Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Aug 9, 2025 @ 15:50:22.505	virus	PAM: Login session closed.	3	5502
Aug 9, 2025 @ 15:50:22.502	virus	PAM: Login session closed.	3	5502
Aug 9, 2025 @ 15:50:04.505	virus	PAM: Login session opened.	3	5501
Aug 9, 2025 @ 15:50:04.505	virus	PAM: Login session opened.	3	5501
Aug 9, 2025 @ 15:50:04.455	virus	Successful sudo to ROOT executed.	3	5402
Aug 9, 2025 @ 15:49:56.498	virus	PAM: Login session opened.	3	5501
Aug 9, 2025 @ 15:49:56.498	virus	PAM: Login session closed.	3	5502
Aug 9, 2025 @ 15:49:56.459	virus	Successful sudo to ROOT executed.	3	5402
Aug 9, 2025 @ 15:45:05.074	virus	File deleted.	7	553
Aug 9, 2025 @ 15:44:56.563	virus	Integrity checksum changed.	7	550
Aug 9, 2025 @ 15:44:50.686	virus	File added to the system.	5	554



133 hits

Aug 8, 2025 @ 22:37:45.640 - Aug 9, 2025 @ 22:37:45.640

Export Formatted | 634 available fields | Columns | Density | **1 fields sorted** | Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Aug 9, 2025 @ 22:37:28.119	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:28.119	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:28.119	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:28.119	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:28.119	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:28.061	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:26.074	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:26.072	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:26.065	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:26.063	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:26.061	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:26.060	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:24.083	virus	Traffic Blocked By FireWall UFW	7	100050
Aug 9, 2025 @ 22:37:24.079	virus	Traffic Blocked By FireWall UFW	7	100050

THE END