Mục Lục

I.Mô hình.....2

II.Cài đặt Graylog.....2

III.Gửi log từ CentOS9 đến Graylog.....3

IV.Cấu hình input Graylog.....3

V. Tấn công từ Kali.....4

VI.Kết quả SIEM.....5

Mô phỏng tấn công và giám sát bằng Kali Linux và SIEM

I.Mô hình

Máy	Hệ điều hành	Vai trò	IP
Kali Linux	Kali	Attacker	192.168.88.145
CentOS	CentOS Stream 9	Target	192.168.88.160
Ubuntu	Ubuntu 20.04	Graylog SIEM	192.168.88.162

II.Cài đặt Graylog

Cập nhật hệ thống

```
sudo apt update && sudo apt upgrade -y
```

Cài đặt Java OpenJDK

```
sudo apt install openjdk-17-jre-headless -y
```

Cài đặt MongoDB

```
wget -qO - https://pgp.mongodb.com/server-6.0.asc | sudo gpg --dearmor -o /usr/share/keyrings/mongodb-server-6.0.gpg
echo "deb [ signed-by=/usr/share/keyrings/mongodb-server-6.0.gpg ] https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/6.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-6.0.list

sudo apt update
sudo apt install mongodb-org -y
sudo systemctl enable --now mongod
```

Cài Elasticsearch

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list

sudo apt update
sudo apt install elasticsearch -y
```

```
sudo nano /etc/elasticsearch/jvm.options.d/heap.options
Sửa:
-Xms512m
-Xmx512m
```

```
sudo systemctl enable --now elasticsearch
```

Cài Graylog

```
wget https://packages.graylog2.org/repo/packages/graylog-5.1-repository_latest.deb
sudo dpkg -i graylog-5.1-repository_latest.deb
sudo apt update
sudo apt install graylog-server -y
```

Cấu hình Graylog

```
pwgen -N 1 -s 96
echo -n "adminpassword" | sha256sum
```

```
sudo nano /etc/graylog/server/server.conf
Sửa:
password_secret = <output pwgen>
root_password_sha2 = <output hash>
http_bind_address = 0.0.0.0:9000
http_publish_uri = http://192.168.88.162:9000/
```

Khởi động Graylog

```
sudo systemctl daemon-reexec
sudo systemctl enable --now graylog-server
```

III.Gửi log từ CentOS9 đến Graylog

Cài rsyslog

```
sudo dnf install rsyslog -y
```

Cấu hình gửi log

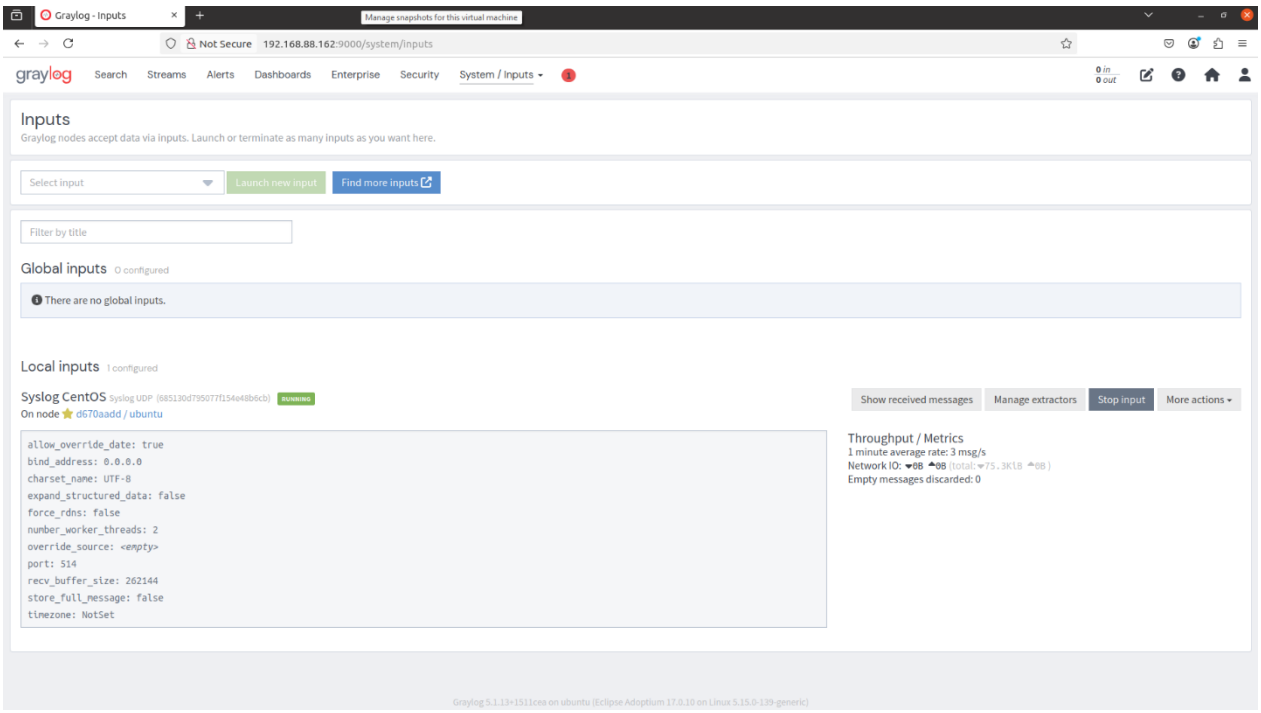
```
sudo nano /etc/rsyslog.conf
Thêm:
*.* @192.168.88.162:1514  (UDP)
Hoặc
*.* @@192.168.88.162:1514  (TCP)
```

```
sudo systemctl restart rsyslog
```

IV.Cấu hình input Graylog

- Truy cập : http://192.168.88.162:9000
- Đăng nhập :admin / adminpassword

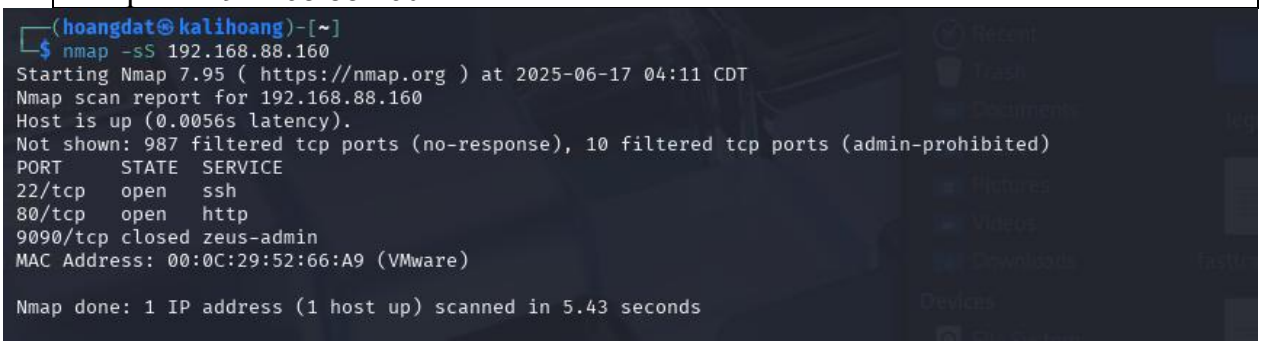
- Chọn System --> inputs
- Chọn Syslog UDP → Launch Input
    - Port :1514
    - Title: Syslog CentOS
    - Bind: 0.0.0.0



V. Tấn công từ Kali

- Port scan :

```
nmap -sS 192.168.88.160
```



- SSH brute-force

```
hydra -l nhd-P /usr/share/wordlists/rockyou.txt ssh:// 192.168.88.160-t 4
```

```
┌──(hoangdat㉿kalihoang)-[~]
└─$ hydra -l nhd -P /usr/share/wordlists/rockyou.txt ssh://192.168.88.160 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-17 05:56:31
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session foun
d, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.88.160:22/
[STATUS] 66.00 tries/min, 66 tries in 00:01h, 14344333 to do in 3622:19h, 4 active
[STATUS] 62.67 tries/min, 188 tries in 00:03h, 14344211 to do in 3814:57h, 4 active
[STATUS] 62.14 tries/min, 435 tries in 00:07h, 14343964 to do in 3847:03h, 4 active
[STATUS] 63.27 tries/min, 949 tries in 00:15h, 14343450 to do in 3778:35h, 4 active
[22][ssh] host: 192.168.88.160   login: nhd   password: mommy
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-17 06:13:06
```

- Scan lỗ hổng web

nikto -h http:// 192.168.88.160

```
┌──(hoangdat㉿kalihoang)-[~]
└─$ nikto -h http://192.168.88.160
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.88.160
+ Target Hostname:    192.168.88.160
+ Target Port:        80
+ Start Time:         2025-06-17 04:53:31 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.62 (CentOS Stream)
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8909 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2025-06-17 04:53:43 (GMT-5) (12 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


      ********************************************************************
      Portions of the server's headers (Apache/2.4.62) are not in
      the Nikto 2.5.0 database or are newer than the known string. Would you like
      to submit this information (*no server specific data*) to CIRT.net
      for a Nikto update (or you may email to sullo@cirt.net) (y/n)? y

+ ERROR:  →
+ ERROR: Update failed, please notify sullo@cirt.net of the previous line.
```

VI.Kết quả SIEM

Timestamp	Node	Message
2025-06-17T03:55:42-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T03:53:32-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T03:45:26-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T03:43:19-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T03:41:29-07:00	d670aadd / ubuntu	Input [Syslog UDP/Syslog CentOS/685130d795077f154e48b6cb] is in state RUNNING
2025-06-17T03:41:29-07:00	d670aadd / ubuntu	Input [Syslog UDP/Syslog CentOS/685130d795077f154e48b6cb] is in state STARTING
2025-06-17T03:41:22-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T03:40:28-07:00	d670aadd / ubuntu	Input [Syslog UDP/Syslog CentOS/685130d795077f154e48b6cb] is in state TERMINATED
2025-06-17T03:40:28-07:00	d670aadd / ubuntu	Input [Syslog UDP/Syslog CentOS/685130d795077f154e48b6cb] is in state STOPPED
2025-06-17T03:40:27-07:00	d670aadd / ubuntu	Input [Syslog UDP/Syslog CentOS/685130d795077f154e48b6cb] is in state STOPPING
2025-06-17T03:38:36-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T03:38:27-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T03:35:05-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T03:26:58-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T03:15:40-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T02:48:08-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T02:36:02-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T02:32:01-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T02:27:51-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T02:09:43-07:00	d670aadd / ubuntu	Input [Syslog UDP/Syslog CentOS/685130d795077f154e48b6cb] is in state RUNNING
2025-06-17T02:09:43-07:00	d670aadd / ubuntu	Input [Syslog UDP/Syslog CentOS/685130d795077f154e48b6cb] is in state STARTING
2025-06-17T02:09:36-07:00	d670aadd / ubuntu	Notification condition [NO_LEADER] has been fixed.
2025-06-17T02:02:50-07:00	d670aadd / ubuntu	Cycled index alias <gl-system-events_deflector> from <none> to <gl-system-events_0>.
2025-06-17T02:02:49-07:00	d670aadd / ubuntu	Started up.
2025-06-17T02:02:49-07:00	d670aadd / ubuntu	There is no index target to point to. Creating one now.
2025-06-17T02:02:48-07:00	d670aadd / ubuntu	Cycled index alias <gl-events_deflector> from <none> to <gl-events_0>.
2025-06-17T02:02:47-07:00	d670aadd / ubuntu	There is no index target to point to. Creating one now.

Phân tích:

- Notification condition [NO_LEADER] has been fixed.
    - Thông báo này lặp đi lặp lại rất nhiều lần,cho biết một tình trạng "không có leader" (NO_LEADER) đã được khắc phục.
    - Dấu hiệu cho thấy có sự không ổn định trong việc chọn leader của cụm Graylog. Mặc dù thông báo nói rằng vấn đề đã được "fixed" (khắc phục), nhưng việc nó lặp đi lặp lại với tần suất cao chỉ ra rằng lỗi NO_LEADER đang xảy ra liên tục và sau đó được tự động khắc phục.
    - Nguyên nhân tìm hiểu được:
        - Mất kết nối tạm thời giữa Graylog và các thành phần phụ thuộc (như MongoDB hoặc Elasticsearch).
        - Vấn đề về tài nguyên hệ thống (CPU, RAM, Disk I/O) khiến Graylog khó duy trì trạng thái ổn định (khả năng xảy ra cao vì chạy trên Ubuntu 20.04 với RAM 3GB và bộ nhớ 20GB).
        - Sự cố mạng nội bộ.
- Input [Syslog UDP/Syslog CentOS/685130d795077f154e48b6cb] is in state RUNNING / STARTING / TERMINATED / STOPPED.

- Các thông báo này cho thấy input Syslog UDP (được đặt tên là Syslog CentOS) đang liên tục thay đổi trạng thái.
- Cụ thể, chúng ta thấy các chuỗi trạng thái như:
  - RUNNING (04:33:53) -> (một số thông báo NO_LEADER ở giữa)
  - STARTING (04:31:29)
  - TERMINATED (04:30:28)
  - STOPPED (04:30:27)
  - STOPPING (04:27:53)
- Liên tục giữa các trạng thái STARTING, RUNNING, STOPPED, TERMINATED →input UDP này đang rất không ổn định. Nó không thể duy trì hoạt động liên tục.
- Điều này dẫn đến việc mất dữ liệu nhật ký vì input không hoạt động đủ lâu để thu thập và xử lý các gói Syslog UDP.