Report_Week_05

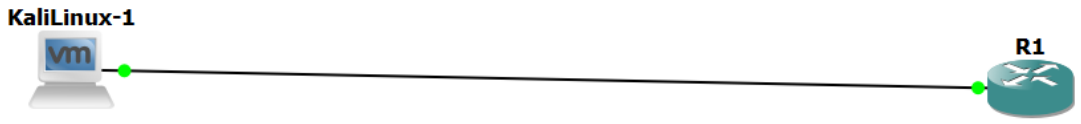
Họ và tên: Trần Hân Nhi

MSSV: 2011770131 Lớp: 20DATA1

Ex_5.3:

Mô hình triển khai:

- Kali Linux
  - VMNET1
  - Cài đặt công cụ Yersinia
- Router

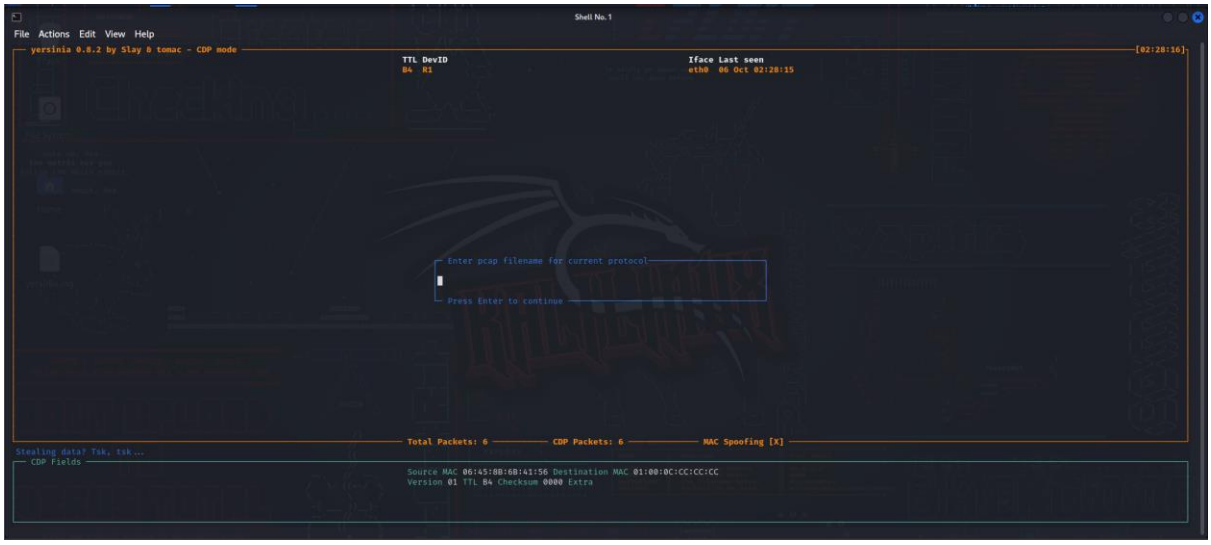


Kiểm tra CDP neighbor, traffic, CPU cho quá trình xử lý gói tin CDP. Kiểm tra hiệu xuất CPU và các tiến trình.

```
R1#sh cdp traffic
CDP counters :
        Total packets output: 4, Input: 0
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 4, Input: 0
R1#sh process cpu sorted | include CPU|PID Runtime| CDP Protocol
CPU utilization for five seconds: 0%/100%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
  59           4        37        108  0.00%  0.00%  0.00%   0 CDP Protocol
```

- R1 đang hoạt động bình thường. Số lượng gói tin CDP nhận được và gửi đi là nhỏ, do đó không gây ảnh hưởng đáng kể đến hiệu suất CPU.

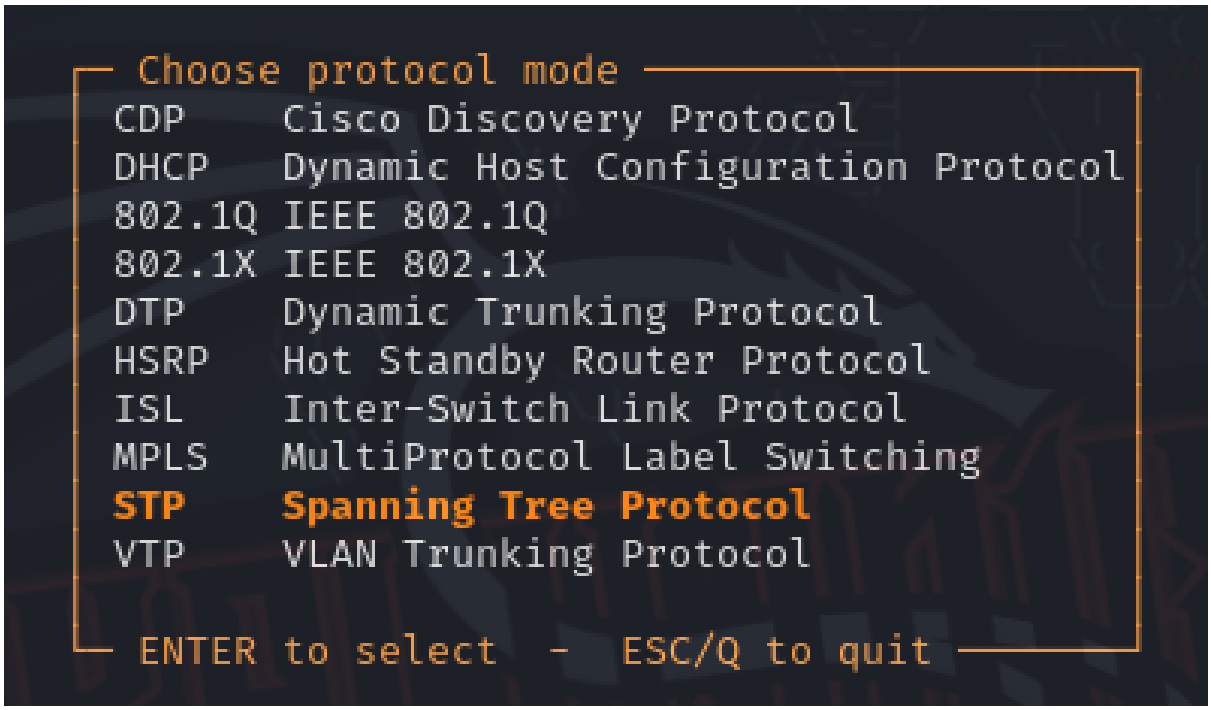
Giao diện công cụ Yersinia



Có nhiều cách tấn công ở công cụ Yersinia:

- Tấn công CDP: Sử dụng CDP để thu thập thông tin về mạng, chẳng hạn như địa chỉ IP, cổng kết nối và phiên bản phần mềm. Thông tin này có thể được sử dụng để thực hiện các cuộc tấn công khác, chẳng hạn như tấn công xâm nhập hoặc tấn công DoS.
- Tấn công DHCP: Sử dụng DHCP để chiếm quyền kiểm soát máy tính. Điều này có thể được thực hiện bằng cách cung cấp cho máy tính một địa chỉ IP và địa chỉ MAC giả.
- Tấn công 802.1Q: Sử dụng 802.1Q để tiêm nhiễm mã độc vào mạng. Điều này có thể được thực hiện bằng cách chèn gói tin chứa mã độc vào lưu lượng mạng được gắn thẻ VLAN.
- Tấn công 802.1X: Sử dụng 802.1X để vượt qua xác thực. Điều này có thể được thực hiện bằng cách cung cấp thông tin đăng nhập giả mạo hoặc giả mạo máy chủ RADIUS.
- Tấn công DTP: Sử dụng DTP để thay đổi cấu hình của thiết bị mạng. Điều này có thể được thực hiện bằng cách gửi gói tin DTP giả mạo.

- Tấn công HSRP: Sử dụng HSRP để đánh lừa người dùng nghĩ rằng một máy chủ không khả dụng. Điều này có thể được thực hiện bằng cách gửi gói tin HSRP giả mạo.
- Tấn công ISL: Sử dụng ISL để tạo một đường hầm giữa hai thiết bị mạng. Đường hầm này có thể được sử dụng để truyền mã độc hoặc dữ liệu nhạy cảm.
- Tấn công MPLS: Sử dụng MPLS để định tuyến lưu lượng mạng đến một điểm đến không mong muốn. Điều này có thể được thực hiện bằng cách thay đổi bảng định tuyến của thiết bị mạng.
- Tấn công STP: Sử dụng STP để ngắt kết nối một thiết bị mạng khỏi mạng. Điều này có thể được thực hiện bằng cách gửi gói tin STP giả mạo.
- Tấn công VTP: Sử dụng VTP để thay đổi cấu hình của nhiều thiết bị mạng cùng một lúc. Điều này có thể được thực hiện bằng cách gửi gói tin VTP giả mạo.



Chọn CDP và thực hiện quá trình tấn công CDP flooding

- CDP flooding là loại tấn công mạng nhằm mục đích làm cho một thiết bị mạng trở nên không khả dụng bằng cách gửi một lượng lớn gói tin CDP đến thiết bị đó.

Yersinia tạo ra hàng nghìn gói tin CDP nhằm mục đích:

- Làm cho thiết bị mạng mục tiêu không khả dụng.
- Giảm hiệu suất của thiết bị mạng mục tiêu.
- Tạo ra một lỗ hổng bảo mật có thể được khai thác bởi các cuộc tấn công khác.

Kiểm tra lại trên Router R1, so với lần kiểm tra ban đầu các thông số đều tăng lên rất nhiều và đồng thời thời gian thao tác cũng rất chậm.

```
R1#sh cdp traffic
CDP counters :
        Total packets output: 24, Input: 12000
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
        CDP version 1 advertisements output: 4, Input: 12000
        CDP version 2 advertisements output: 20, Input: 0
R1#sh process cpu sorted | include CPU|PID Runtime| CDP Protocol
CPU utilization for five seconds: 91%/100%; one minute: 95%; five minutes: 49%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
  59      207892    163383       1272 91.54% 94.01% 49.80%   0 CDP Protocol
```

- Số gói tin nhận được đã tăng lên so với ban đầu, tổng số gói tin CDP nhận được là 24.
- Tỷ lệ sử dụng CPU cho quá trình xử lý gói tin CDP là 91%
- PID 59 là PID của tiến trình CDP Protocol.
- Runtime của tiến trình này là 207892 ms, tức là tiến trình này đã chạy trong 20,7892 giây.
- Invoked uSecs của tiến trình này là 163383, tức là tiến trình này đã được gọi 163383 lần.
- 5Sec của tiến trình này là 91.54%, tức là CPU đã được sử dụng 91,54% trong 5 giây.
- 1Min của tiến trình này là 94.01%, tức là CPU đã được sử dụng 94,01% trong 1 phút.
- 5Min của tiến trình này là 49.80%, tức là CPU đã được sử dụng 49,80% trong 5 phút.

Tất cả các thông tin này cho thấy rằng thiết bị R1 đã bị tấn công CDP flooding. Quá trình xử lý gói tin CDP đang sử dụng CPU đáng kể, điều này có thể dẫn đến hiệu suất mạng chậm hoặc thiết bị không khả dụng.

Hiện thị chi tiết thông tin về các thiết bị lân cận phát hiện sử dụng CDP

```
R1#sh cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
0000000          Fas 0/0            0        R T S I r    yersinia  Eth 0
000NNNN          Fas 0/0            0          R H I      yersinia  Eth 0
0000000          Fas 0/0            0         R T B S     yersinia  Eth 0
0000000          Fas 0/0            0       R T S H I r   yersinia  Eth 0
00000MM          Fas 0/0            0           B S       yersinia  Eth 0
VV00000          Fas 0/0            0          R T I      yersinia  Eth 0
0000000          Fas 0/0            0        R T B H r    yersinia  Eth 0
0000000          Fas 0/0            0         R T B r     yersinia  Eth 0
0000000          Fas 0/0            0        R T S I r    yersinia  Eth 0
0000000          Fas 0/0            0        R T B H r    yersinia  Eth 0
0000000          Fas 0/0            0         R S I r     yersinia  Eth 0
0000000          Fas 0/0            0         R T H I     yersinia  Eth 0
0000000          Fas 0/0            0           H I       yersinia  Eth 0
0000000          Fas 0/0            0          R T I      yersinia  Eth 0
RRRR000          Fas 0/0            0       R T S H I r   yersinia  Eth 0
0000000          Fas 0/0            0          R T I      yersinia  Eth 0
VVVV000          Fas 0/0            0          R T I      yersinia  Eth 0
0000000          Fas 0/0            0       R T S H I r   yersinia  Eth 0
VVVV000          Fas 0/0            0        R T S I r    yersinia  Eth 0
0000000          Fas 0/0            0       R T S H I r   yersinia  Eth 0
```

- Sử dụng Yersinia để thực hiện cuộc tấn công CDP flooding. Các thiết bị này đã được sử dụng để gửi một lượng lớn gói tin CDP đến thiết bị R1, khiến thiết bị bị quá tải và không khả dụng.

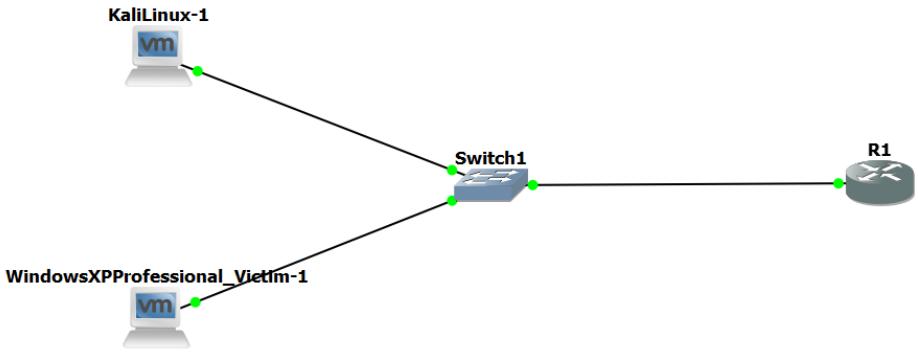
Để bảo vệ thiết bị mạng khỏi các cuộc tấn công CDP flooding, có thể thực hiện các bước sau:

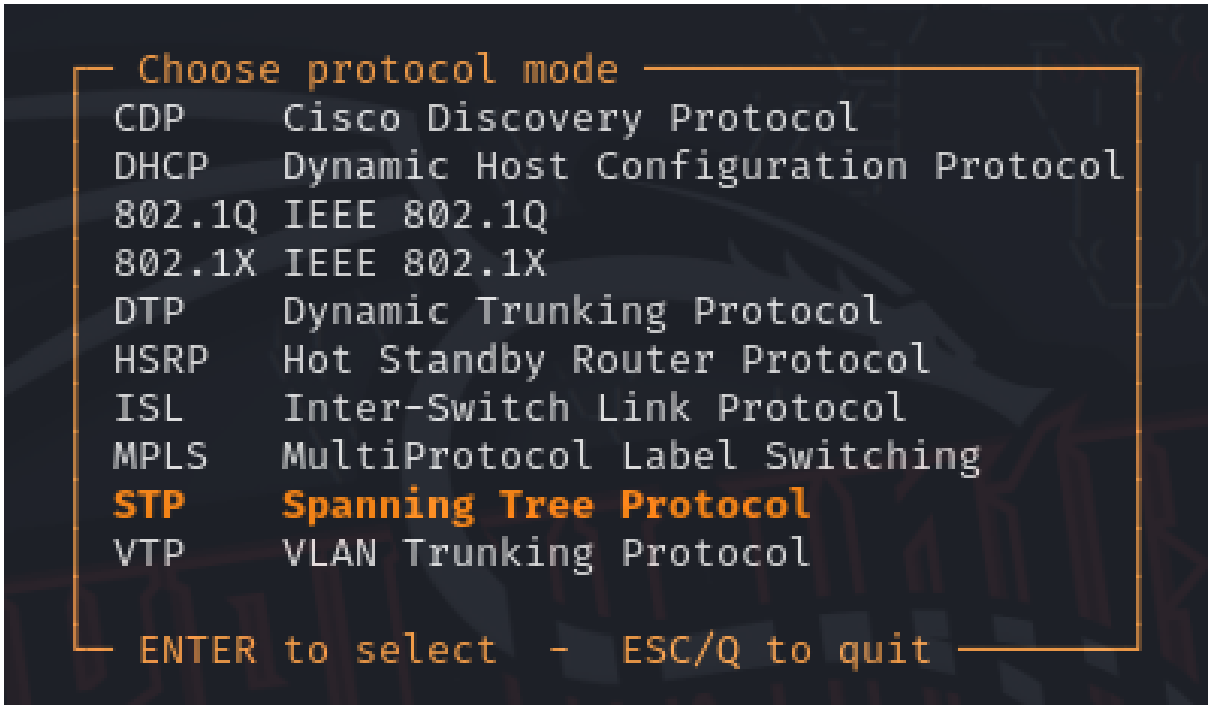
- Tắt CDP trên các thiết bị mạng. Điều này sẽ ngăn chặn kẻ tấn công gửi gói tin CDP đến thiết bị.
- Sử dụng các biện pháp xác thực cho CDP. Điều này sẽ giúp xác thực người gửi gói tin CDP và ngăn chặn kẻ tấn công giả mạo các gói tin CDP.
- Theo dõi lưu lượng mạng để phát hiện bất kỳ hoạt động đáng ngờ nào.

Ex_5.4:

Mô hình thực hiện:

- Kali Linux:
    - Cài đặt công cụ Yersinia
    - Sử dụng card mạng VMNet1
- Switch
- Router
- WinXP: Sử dụng card mạng VMNet1

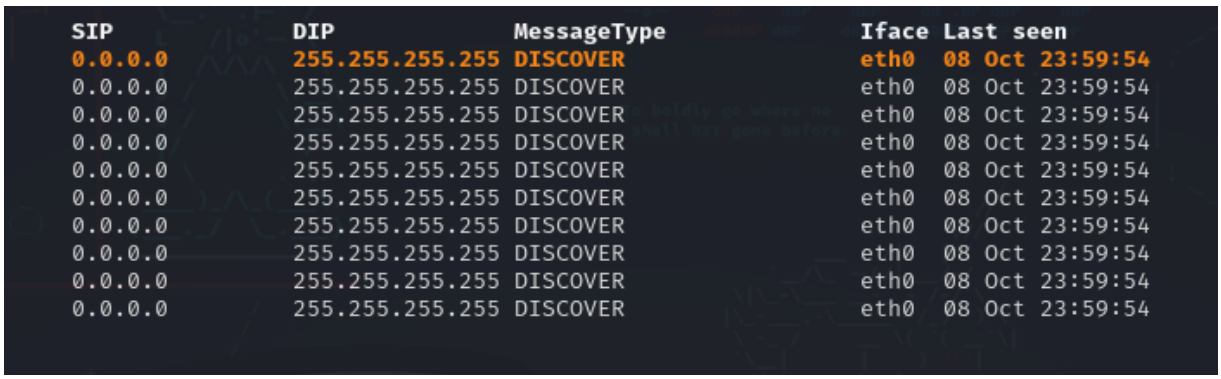




Chọn DHCP và thực hiện quá trình tấn công DHCP Starvation Attack:

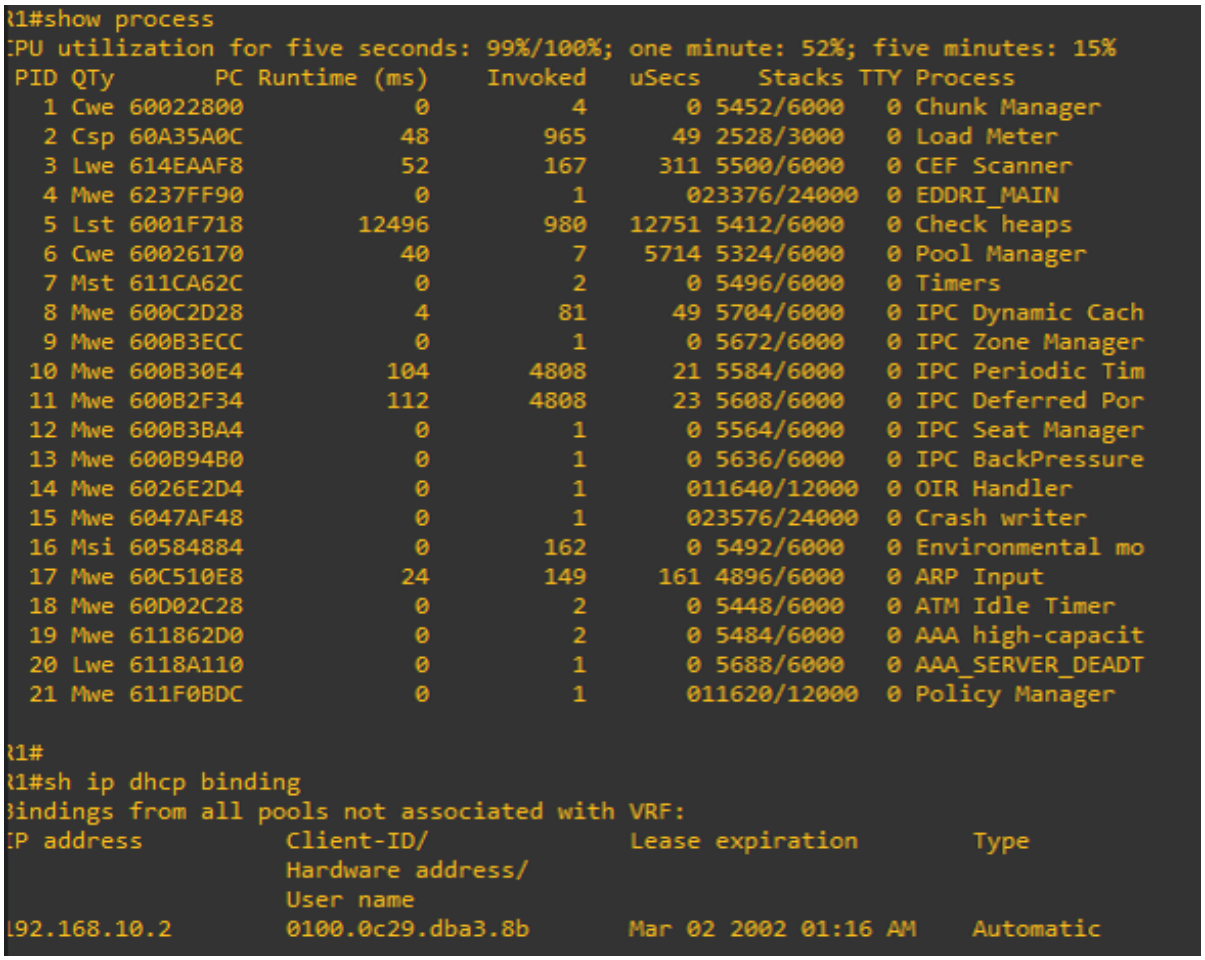
- Sending DISCOVER packet: Gửi các gói tin phát hiện DHCP tới mạng của nạn nhân. Các gói tin này có thể khiến máy chủ DHCP của nạn nhân

cấp địa chỉ IP cho các thiết bị của attacker. Điều này có thể ngăn các thiết bị hợp pháp truy cập vào mạng.



```
SIP             DIP             MessageType              Iface Last seen
0.0.0.0         255.255.255.255 DISCOVER                 eth0  08 Oct 23:59:54
0.0.0.0         255.255.255.255 DISCOVER                 eth0  08 Oct 23:59:54
0.0.0.0         255.255.255.255 DISCOVER                 eth0  08 Oct 23:59:54
0.0.0.0         255.255.255.255 DISCOVER                 eth0  08 Oct 23:59:54
0.0.0.0         255.255.255.255 DISCOVER                 eth0  08 Oct 23:59:54
0.0.0.0         255.255.255.255 DISCOVER                 eth0  08 Oct 23:59:54
0.0.0.0         255.255.255.255 DISCOVER                 eth0  08 Oct 23:59:54
0.0.0.0         255.255.255.255 DISCOVER                 eth0  08 Oct 23:59:54
0.0.0.0         255.255.255.255 DISCOVER                 eth0  08 Oct 23:59:54
0.0.0.0         255.255.255.255 DISCOVER                 eth0  08 Oct 23:59:54
```

Quá trình tấn công DHCP, attacker gửi các gói tin DHCP giả mạo để chiếm đoạt mạng. Trong trường hợp này, có thể đã gửi các gói tin DHCP DISCOVER giả mạo để khiến máy chủ DHCP cấp địa chỉ IP cho thiết bị của kẻ tấn công. Sau đó có thể sử dụng thiết bị của mình để thực hiện các hoạt động độc hại trên mạng.



```
1#show process
PU utilization for five seconds: 99%/100%; one minute: 52%; five minutes: 15%
 PID QTy       PC Runtime (ms)    Invoked    uSecs    Stacks TTY Process
   1 Cwe 60022800          0           4        0 5452/6000   0 Chunk Manager
   2 Csp 60A35A0C         48         965       49 2528/3000   0 Load Meter
   3 Lwe 614EAAF8         52         167      311 5500/6000   0 CEF Scanner
   4 Mwe 6237FF90          0           1       023376/24000   0 EDDRI_MAIN
   5 Lst 6001F718      12496         980    12751 5412/6000   0 Check heaps
   6 Cwe 60026170         40           7     5714 5324/6000   0 Pool Manager
   7 Mst 611CA62C          0           2        0 5496/6000   0 Timers
   8 Mwe 600C2D28          4          81       49 5704/6000   0 IPC Dynamic Cach
   9 Mwe 600B3ECC          0           1        0 5672/6000   0 IPC Zone Manager
  10 Mwe 600B30E4        104        4808       21 5584/6000   0 IPC Periodic Tim
  11 Mwe 600B2F34        112        4808       23 5608/6000   0 IPC Deferred Por
  12 Mwe 600B3BA4          0           1        0 5564/6000   0 IPC Seat Manager
  13 Mwe 600B94B0          0           1        0 5636/6000   0 IPC BackPressure
  14 Mwe 6026E2D4          0           1       011640/12000   0 OIR Handler
  15 Mwe 6047AF48          0           1       023576/24000   0 Crash writer
  16 Msi 60584884          0         162        0 5492/6000   0 Environmental mo
  17 Mwe 60C510E8         24         149      161 4896/6000   0 ARP Input
  18 Mwe 60D02C28          0           2        0 5448/6000   0 ATM Idle Timer
  19 Mwe 611862D0          0           2        0 5484/6000   0 AAA high-capacit
  20 Lwe 6118A110          0           1        0 5688/6000   0 AAA_SERVER_DEADT
  21 Mwe 611F0BDC          0           1       011620/12000   0 Policy Manager

1#
1#sh ip dhcp binding
indings from all pools not associated with VRF:
P address          Client-ID/              Lease expiration        Type
                   Hardware address/
                   User name
92.168.10.2        0100.0c29.dba3.8b       Mar 02 2002 01:16 AM    Automatic
```

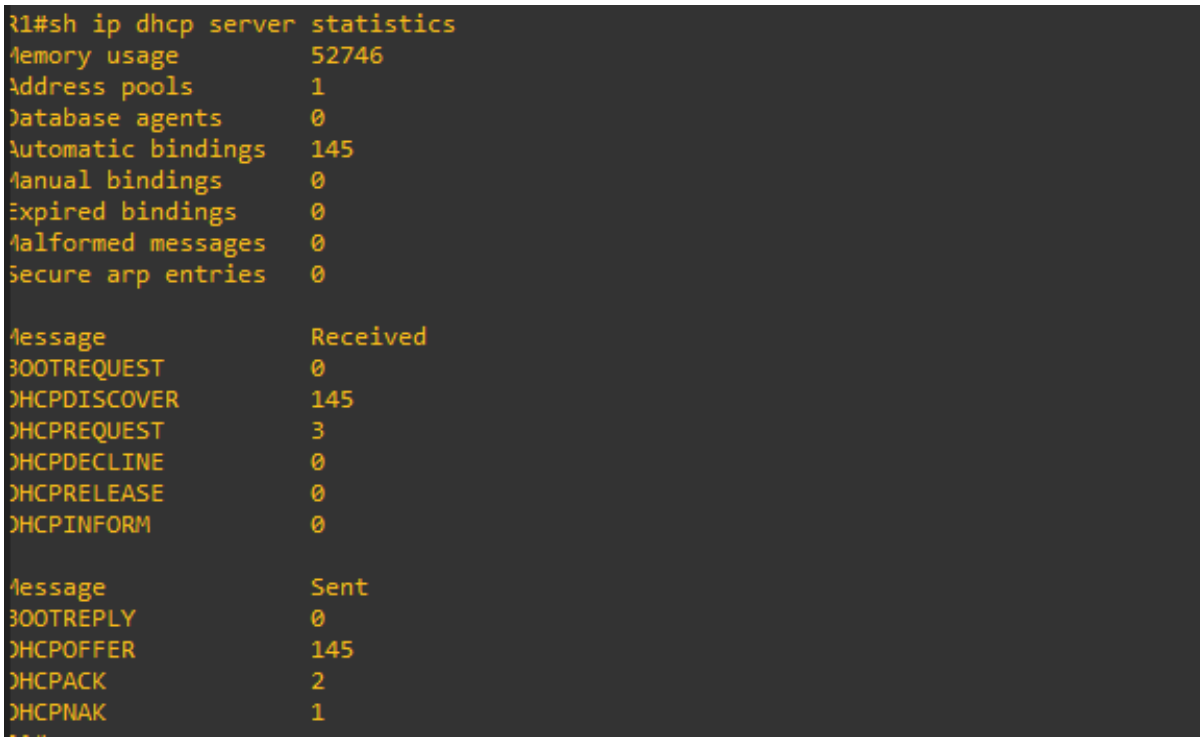
Quy trình đang chiếm dụng tổng cộng 99% CPU, Router lúc này xử lý rất chậm, CPU dành cho việc xử lý gói tin DISCOVER chiếm hầu hết hiệu suất

```
C:\Users\DHTT>ipconfig /renew

Windows IP Configuration

An error occurred while renewing interface Local Area Connection 2 : unable to c
ontact your DHCP server. Request has timed out.
No operation can be performed on VPN - VPN Client while it has its media disconn
ected.
An error occurred while releasing interface Loopback Pseudo-Interface 1 : The sy
stem cannot find the file specified.
```

Máy Client tiến hành xoá IP cũ và xin cấp phát lại địa chỉ IP từ DHCP Server nhưng không thành công. Thông báo lỗi này cho biết rằng máy tính đã cố gắng gia hạn địa chỉ IP cho "Local Area Connection 2", nhưng không thể liên hệ với máy chủ DHCP. Yêu cầu gia hạn đã hết thời gian chờ. Lỗi này có thể do máy chủ DHCP không khả dụng hoặc máy tính không thể kết nối với máy chủ DHCP.

```
R1#
R1#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.10.2        0100.0c29.dba3.8b       Mar 02 2002 01:16 AM    Automatic
192.168.10.3        0100.0c29.fb0d.6b       Mar 02 2002 01:18 AM    Automatic
192.168.10.4        147a.1669.8b5e          Mar 01 2002 01:24 AM    Automatic
192.168.10.5        f1ab.f152.e46e          Mar 01 2002 01:24 AM    Automatic
192.168.10.6        888e.5075.3d11          Mar 01 2002 01:24 AM    Automatic
192.168.10.7        9967.971c.94f7          Mar 01 2002 01:24 AM    Automatic
192.168.10.8        297f.9e21.98b5          Mar 01 2002 01:24 AM    Automatic
192.168.10.9        bfdf.cb5d.dc9a          Mar 01 2002 01:24 AM    Automatic
192.168.10.10       e023.4672.ac4b          Mar 01 2002 01:24 AM    Automatic
192.168.10.11       959a.2b10.3b81          Mar 01 2002 01:24 AM    Automatic
192.168.10.12       8f00.d94a.c297          Mar 01 2002 01:24 AM    Automatic
192.168.10.13       eae1.6330.ba67          Mar 01 2002 01:24 AM    Automatic
192.168.10.14       3904.9d17.d263          Mar 01 2002 01:24 AM    Automatic
192.168.10.15       ac3e.717c.d7ed          Mar 01 2002 01:24 AM    Automatic
192.168.10.16       7b9a.9962.fc58          Mar 01 2002 01:24 AM    Automatic
192.168.10.17       eddc.635a.dc08          Mar 01 2002 01:24 AM    Automatic
192.168.10.18       0e45.c919.d2d1          Mar 01 2002 01:25 AM    Automatic
192.168.10.19       067f.6378.01c2          Mar 01 2002 01:25 AM    Automatic
192.168.10.20       68f9.f636.4d76          Mar 01 2002 01:25 AM    Automatic
192.168.10.21       7c15.6b1b.37b4          Mar 01 2002 01:25 AM    Automatic
```

Có nhiều địa chỉ IP mà DHCP đã cấp do quá trình tấn công DHCP Starvation đã gửi nhiều gói tin Discover liên tục tới Router. Nếu gửi đủ số lượng gói tin Discover, máy chủ DHCP sẽ hết sạch các địa chỉ IP có sẵn. Điều này sẽ khiến các thiết bị người dùng sử dụng không thể nhận được địa chỉ IP từ máy chủ DHCP. Do đó máy Client đã không được cấp địa chỉ IP



Giá trị của thông số Automatic bindings tăng đột ngột do đang thực hiện một cuộc tấn công DHCP Starvation.

Một số biện pháp phòng chống tấn công DHCP Starvation:

- Tắt tính năng DHCP trên máy chủ DHCP khi không cần thiết. Điều này sẽ ngăn chặn gửi yêu cầu thuê địa chỉ IP tới máy chủ DHCP.
- Sử dụng tính năng lọc gói tin để chặn các gói tin Discover giả mạo. Các gói tin Discover giả mạo là các gói tin được gửi bởi kẻ tấn công để yêu cầu thuê địa chỉ IP. Tính năng lọc gói tin có thể được sử dụng để chặn các gói tin này.
- Sử dụng tính năng hạn chế số lượng gói tin Discover mà một máy tính có thể gửi trong một khoảng thời gian nhất định. Tính năng này có thể được

sử dụng để ngăn chặn attacker gửi quá nhiều yêu cầu thuê địa chỉ IP trong một khoảng thời gian nhất định.

- Cấu hình máy chủ DHCP để xóa các địa chỉ IP đã được Offer mà không nhận được gói tin DHCP Request sau một khoảng thời gian nhất định. Điều này sẽ giúp máy chủ DHCP giải phóng các địa chỉ IP đã được cấp nhưng không được sử dụng.