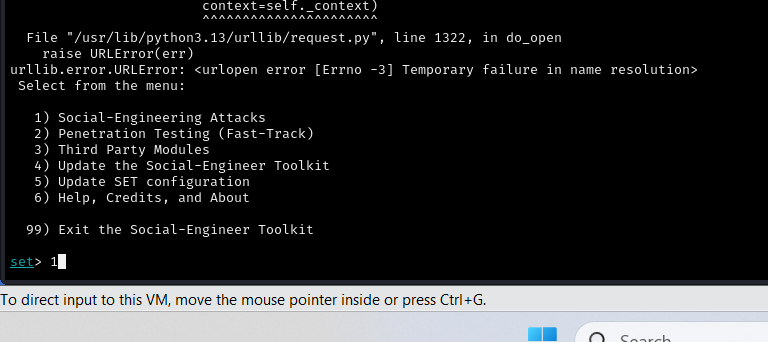
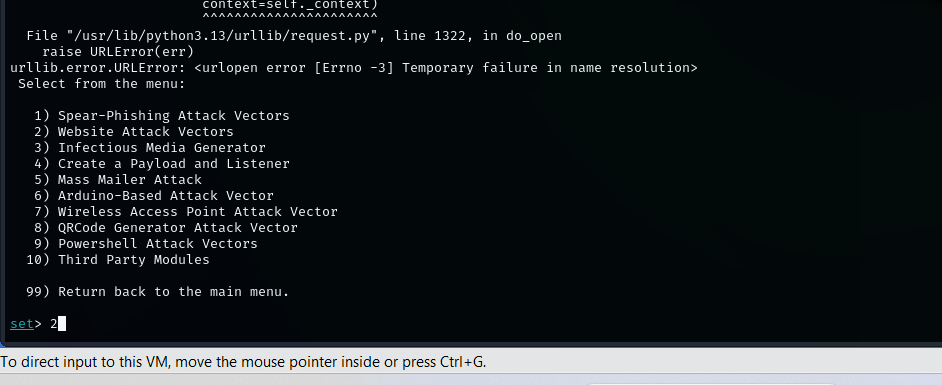
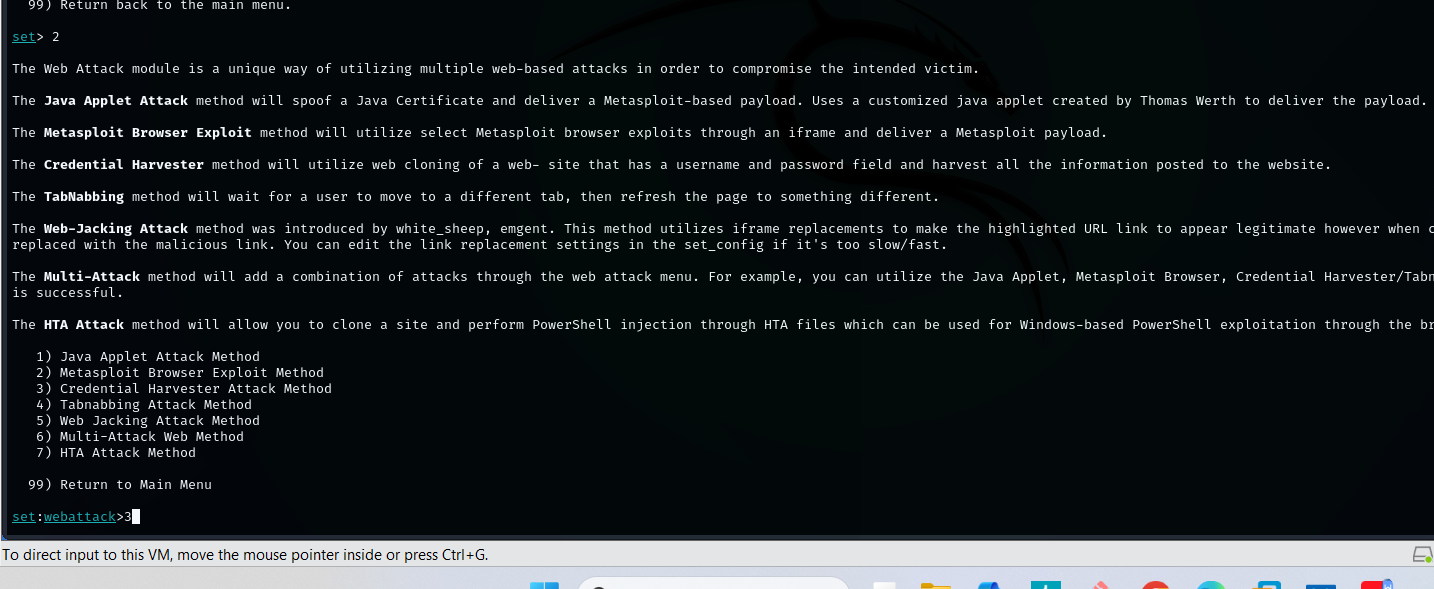
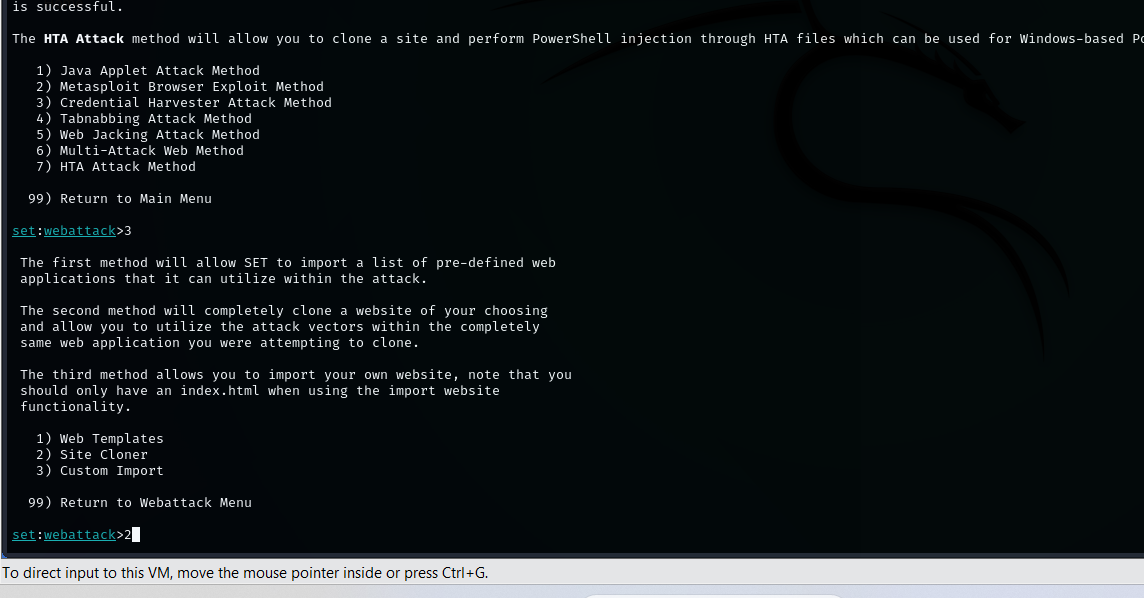
**Tấn công settoolkit**

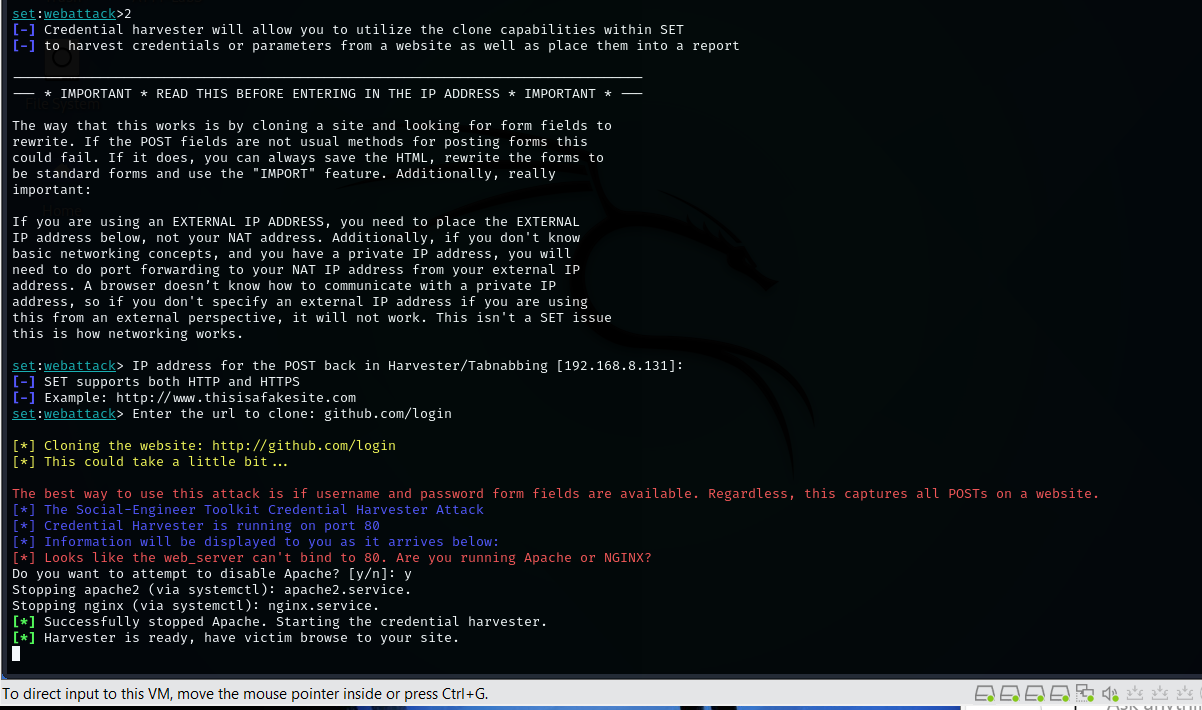
Tấn công



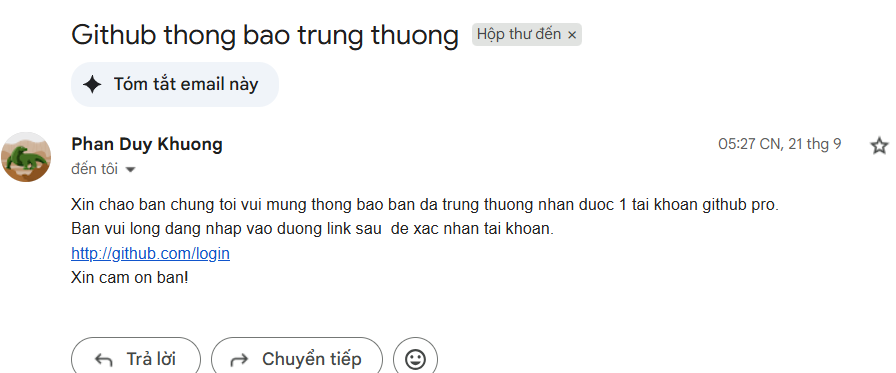


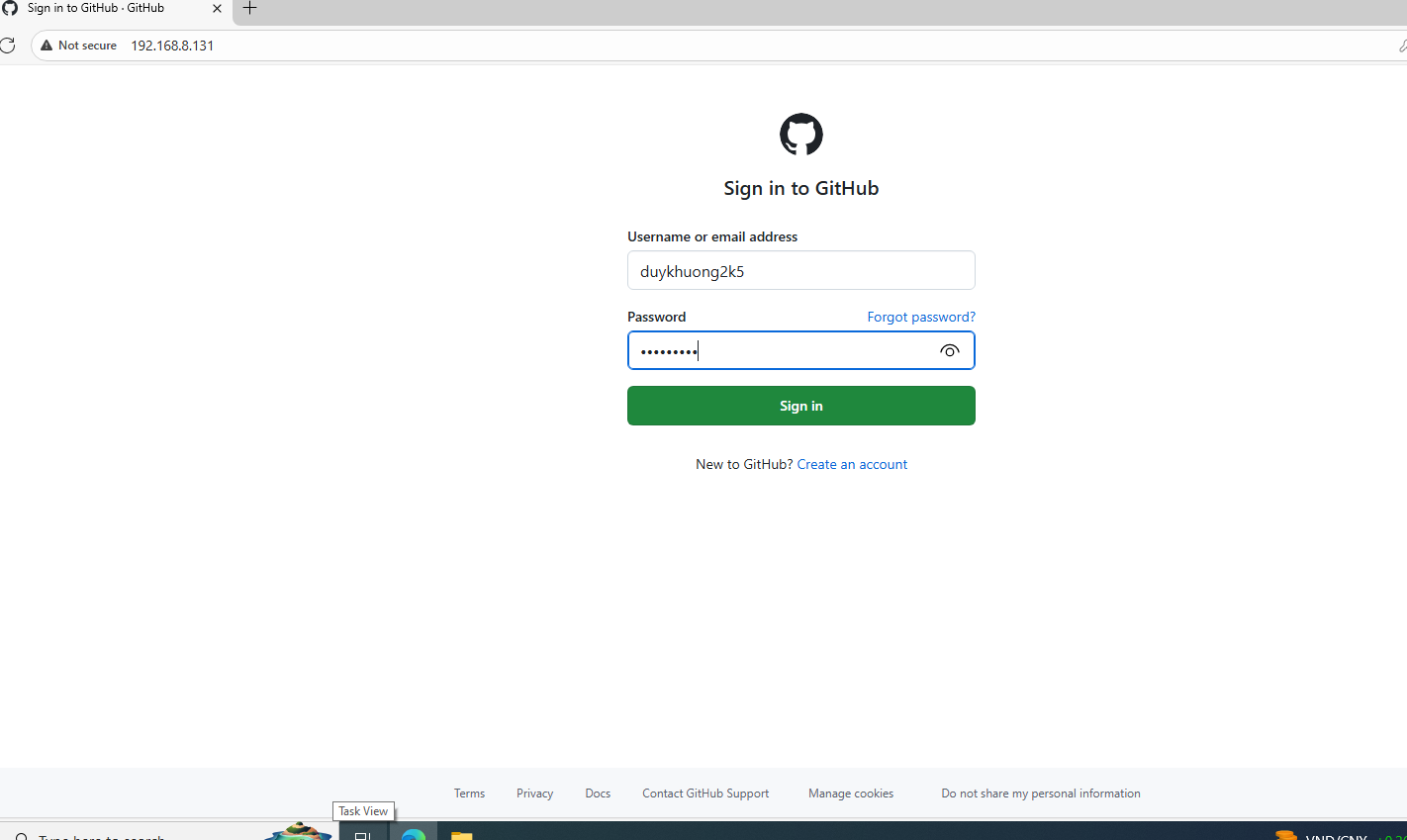




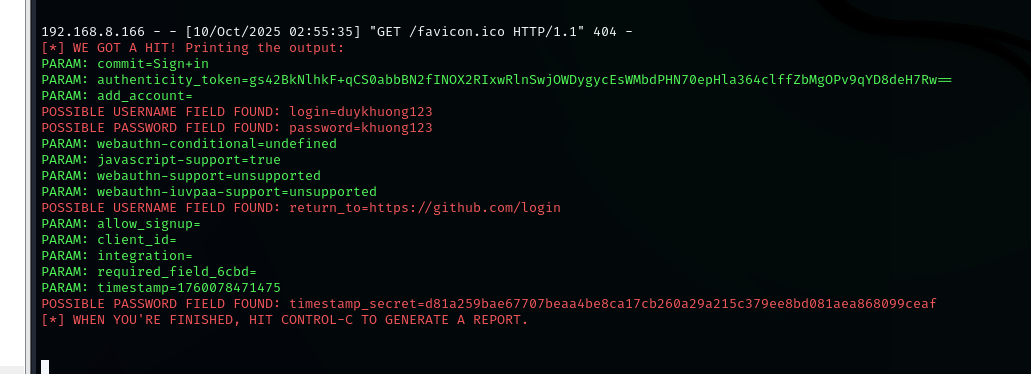


Trên máy nạn nhân sau khi hacker gửi link github.com/login qua mail nạn nhân mở trình duyệt và nhân thông tin

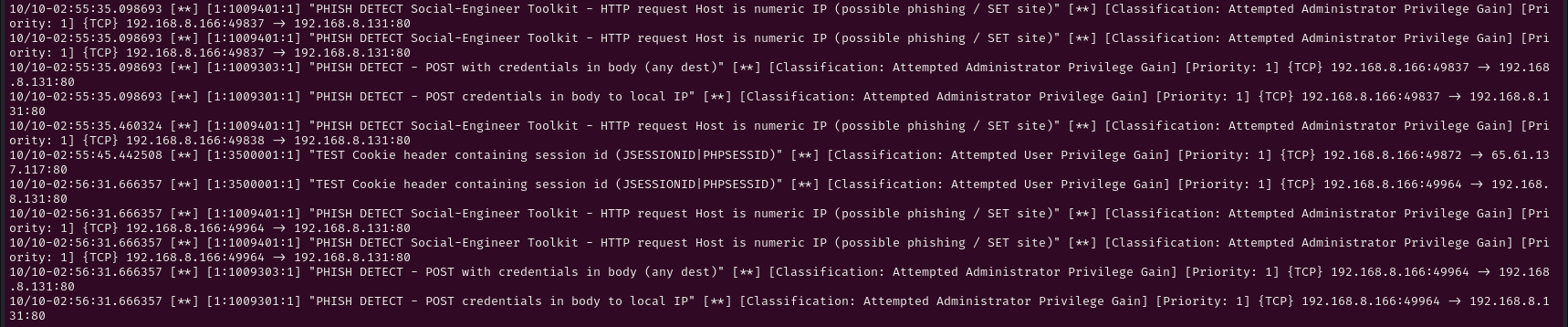




Trên máy tấn công đã có được username passworpassword



Kết quả trên kali snort phát hiện log



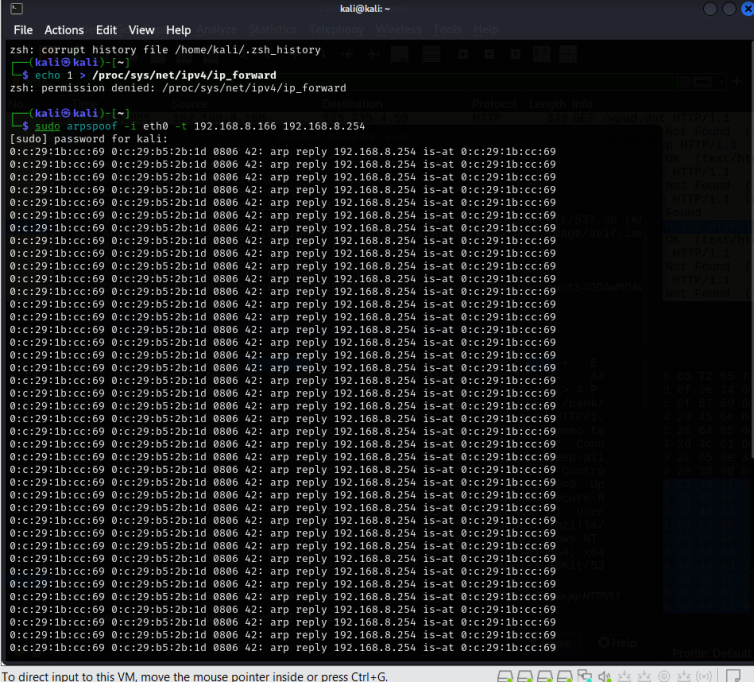
**Tấn công RST**

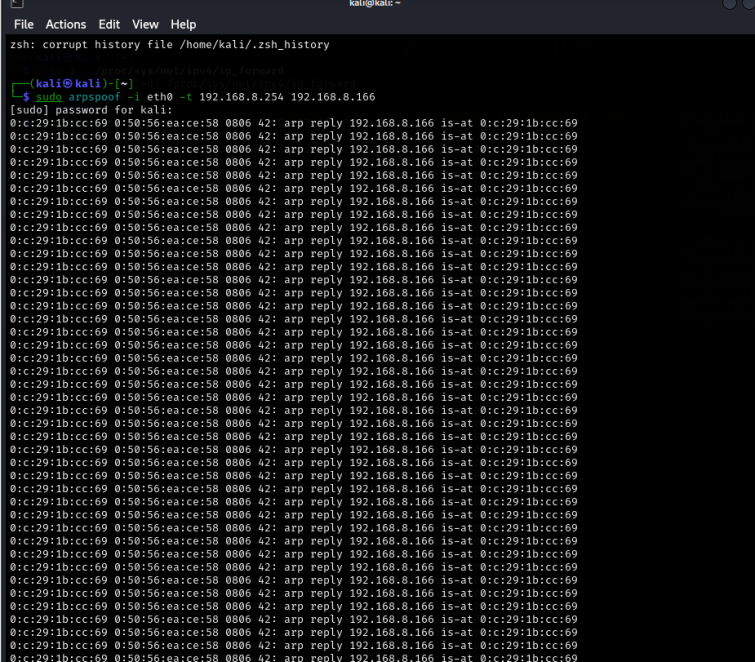
Tấn công

**Kích hoạt IP Forwarding** trên Kali Linux để có thể chuyển tiếp các gói tin:

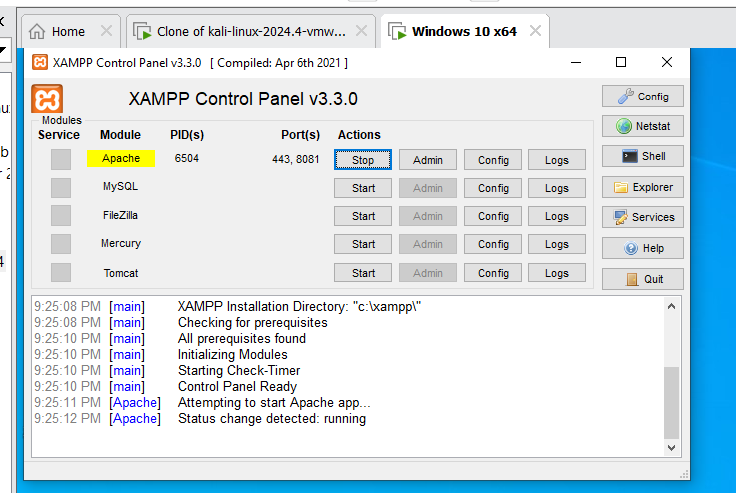
**Sử dụng ARP Spoofing** gửi lưu lượng qua Kali:  
giả mạo ARP từ Kali đến W**indows 10**, làm cho W**indows 10** gửi tất cả lưu lượng đến Kali thay vì **Gateway**:

giả mạo ARP từ Kali đến **Gateway**, làm cho **Gateway** gửi tất cả lưu lượng đến Kali thay vì **Windows 10**





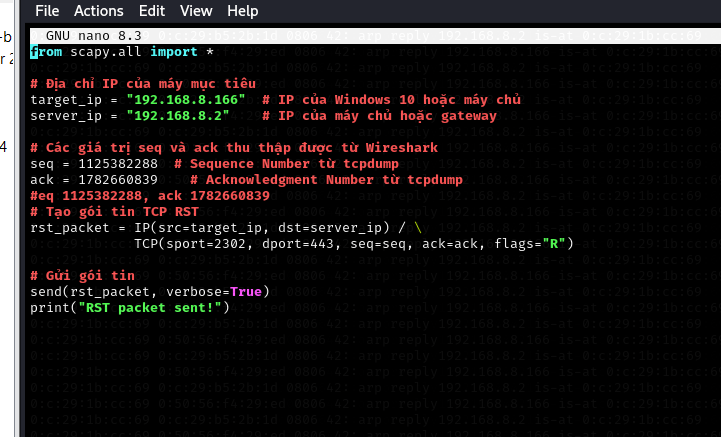
Tren victim chay server XAMPP



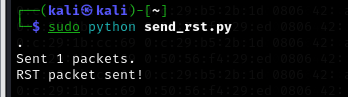
Tren máy tấn công bắt seq và ack bằng lệnh

sudo tcpdump -i eth0 -n 'tcp'

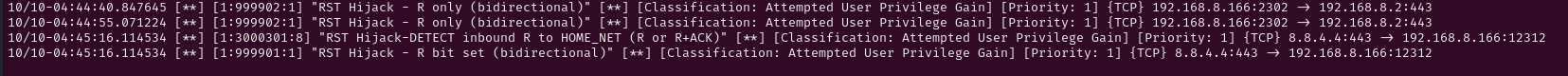
Tạo gói tin RST



Thực hiện gửi gói tin đến server trên máy victivictim



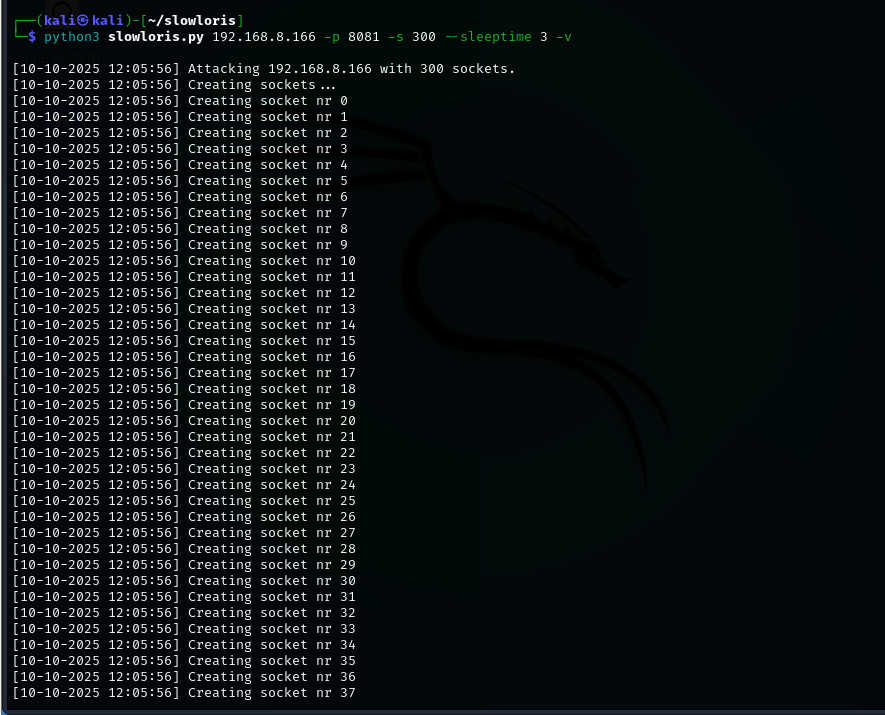
Kết quả trên kali snort

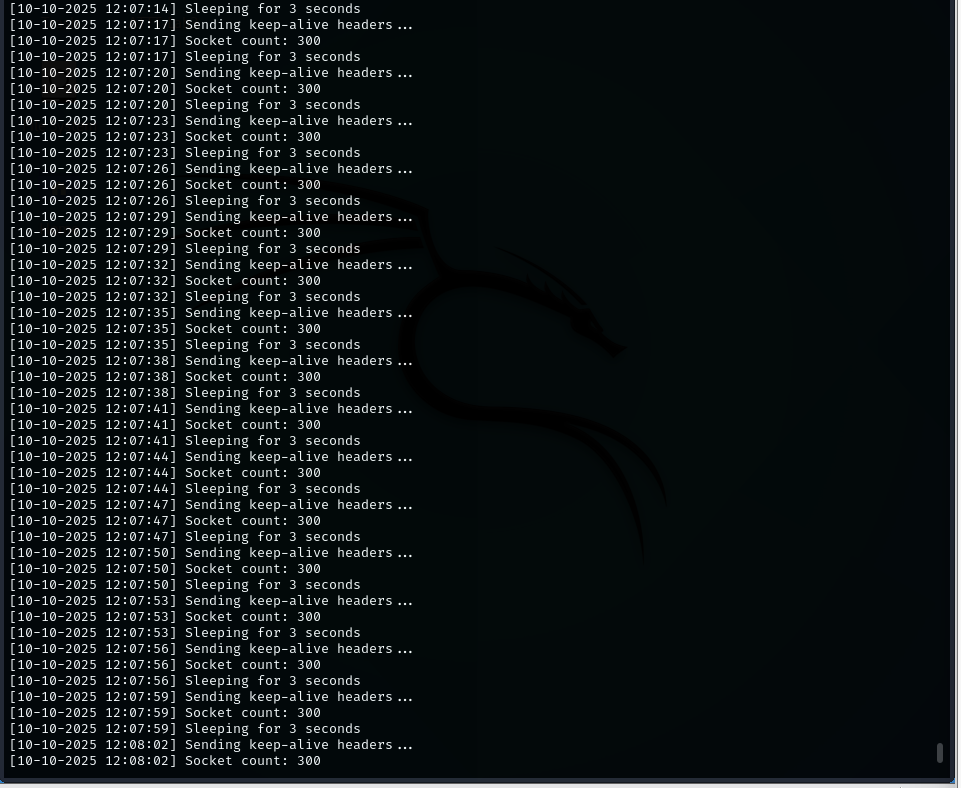


Tan cong dos using http

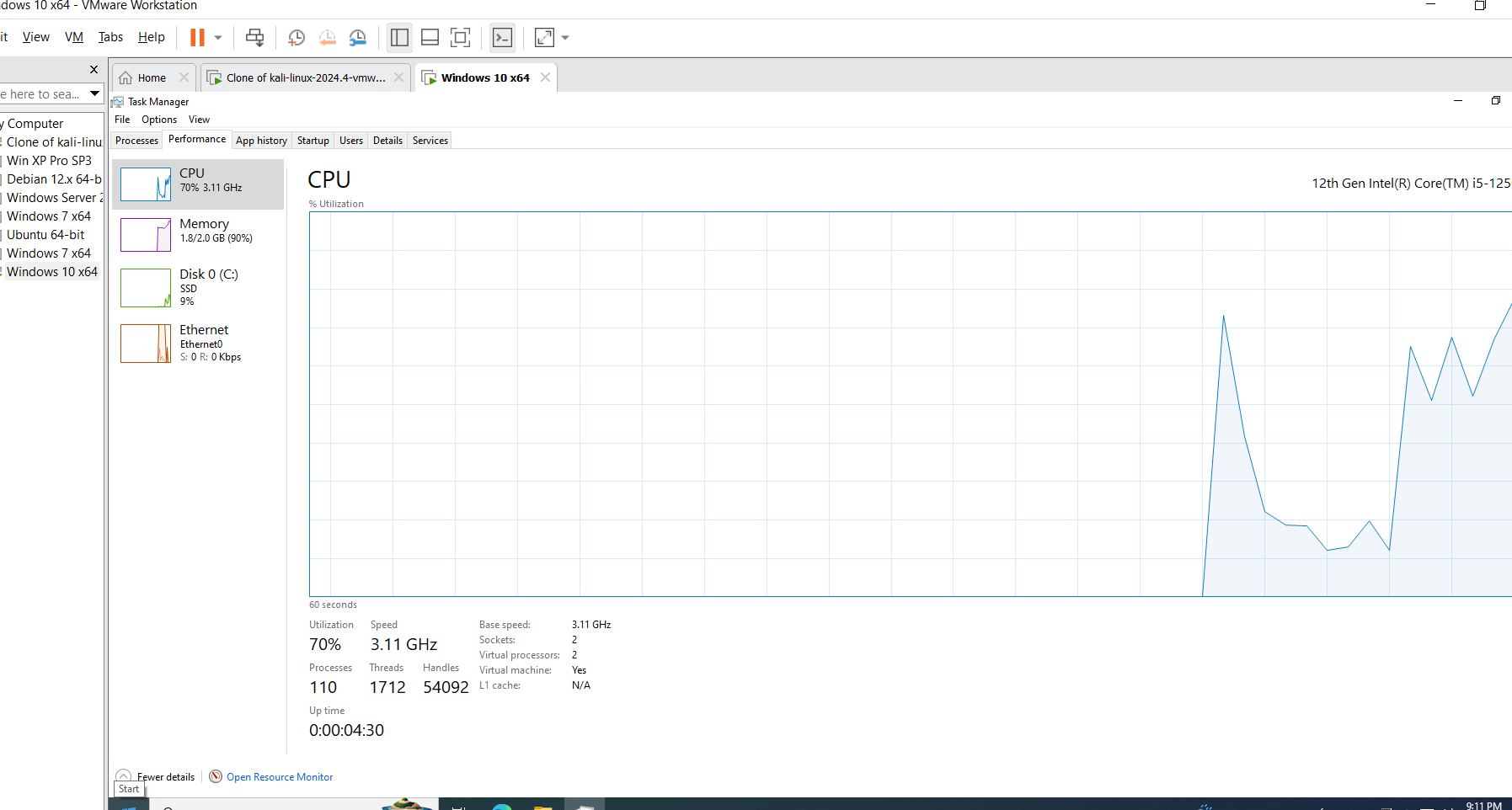
cd ~/slowloris

python3 slowloris.py 192.168.8.166 -p 8081 -s 300 --sleeptime 3 -v

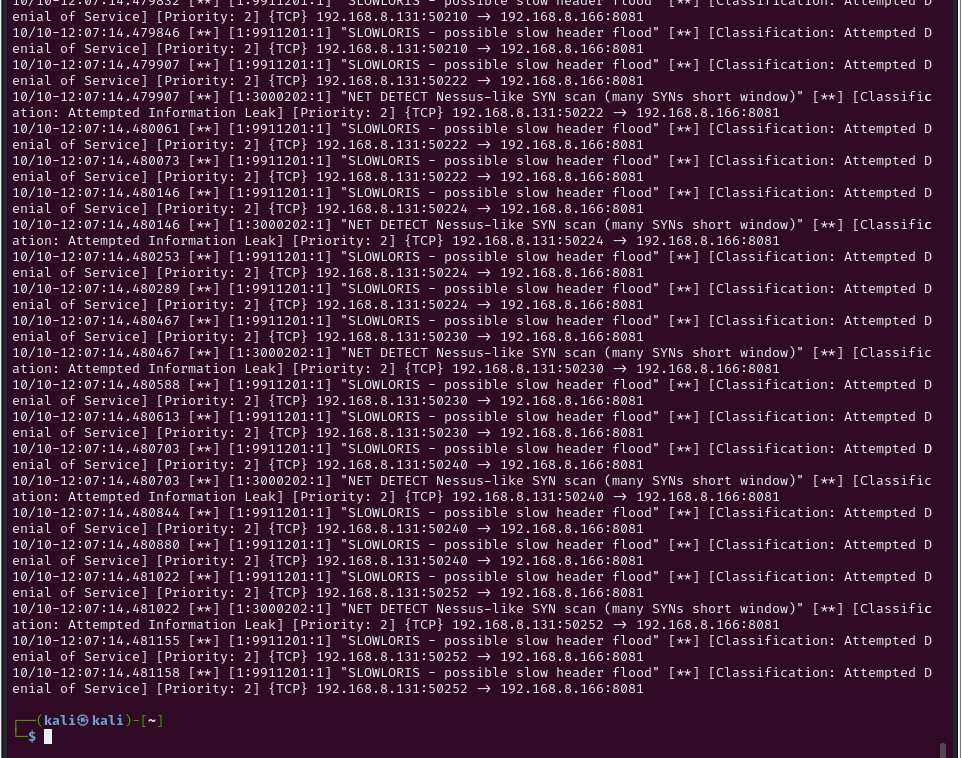




Tren may victim CPU tantang



Trên snort



Tren elk

