?: trang 37: Sử dụng smbdomain và ko dung khác nhau gì, làm sao để biết được các host đang lắng nghe port445. Làm thêm sau khi chiếm được FILE01, thu thập hash password trên máy đó và crack mật khẩu Draco Malfoy

Psexec là công cụ cho phép thực thi lệnh từ xa trên hệ thống. Sử dụng SMB để kết nối đến máy đích, sao chép 1 dịch vụ tạm thời lên máy đó và thực thi lệnh, rồi xóa dịch vụ sau khi hoàn tất.

Mục đích của bài này là từ máy linux ta sẽ lấy được password hashes ở máy window, và sẽ sử dụng hashes đó để truy cập vào các hệ thống khác. Nên nhớ ta sẽ lấy các LM,NT hashes để sử dụng chúng truy cập vào máy mục tiêu mà ko bẻ khóa chúng.

1. Obtaining hashes

Sử dụng psexec trong Metasploit

A close up of a message

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

Thành công chiếm được shell với quyền system



Thực hiện thu thập passwords hashes của các user

A screenshot of a computer

AI-generated content may be incorrect.

Thu thập được vài hash ở đây. Ta sẽ khai thác hash của user antivirus vì đây có thể là tài khoản dung chung

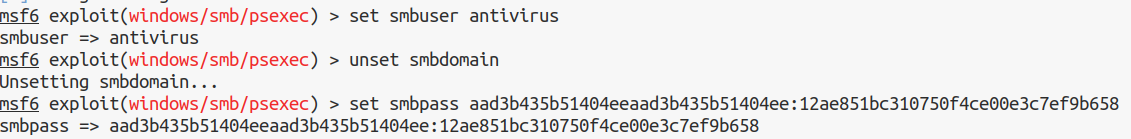
1. Using the Hashes

Tiếp tục chạy nền sessions hiện tại

Background và set các options để khai thác user antivirus với các hệ thống khác



Pass là đoạn hash vừa thu được phía trên



Host là những host đang mở. Ta sẽ xem những host nào đang lắng nghe trên port 445 để khai thác. Sử dụng nmap để quét

A screenshot of a computer

AI-generated content may be incorrect.

Có 3 host nhưng loại bỏ .10 vì đó là máy ta đang truy cập



1. Exploit

A screenshot of a computer code

AI-generated content may be incorrect.

Thành công truy cập được máy 10.130.10.45.

A close-up of a computer screen

AI-generated content may be incorrect.

1. Meterpreter shell

Tương tác với shell vừa khai thác được

A screenshot of a computer code

AI-generated content may be incorrect.

Thành công với quyền System

Xem thông tin máy mục tiêu

A screenshot of a computer

AI-generated content may be incorrect.

Tạo 1 shell và thực hiện tạo 1 tài khoản trên đây

A screenshot of a computer error

AI-generated content may be incorrect.