1. Setup Metasploit

A close-up of a text

AI-generated content may be incorrect.

A screenshot of a computer code

AI-generated content may be incorrect.

Set ExitOnSession. Handler sẽ tự động dừng nếu như nhận được 1 session. Khi ta set False, handler sẽ vẫn tiếp tục chờ thêm kết nối mới

1. VBS

Msfvenom là công cụ tạo payload trong metasploit

Sử dụng msfvenom để tạo payload vbscript

A screenshot of a computer program

AI-generated content may be incorrect.

Msfvenom: công cụ

-p windows/meterpreter/reverse\_http: chỉ định payload.

Lhost, lport: địa chỉ ip và port lắng nghe

-f vbs: đầu ra payload dưới dạng vbscript

Tee /tmp/payload.vbs: ghi nội dung vào file và hiển thị trên terminal

A screenshot of a computer program

AI-generated content may be incorrect.

Chạy máy chủ http để chia sẻ file



Tải file ở máy window

A blue screen with white text

AI-generated content may be incorrect.

Chạy file vbs



Thành công nhận được meterpreter session và thử khai thác thông tin về máy window

A computer screen with text

AI-generated content may be incorrect.

1. MSI payload in an ISO file

Sử dụng msfvenom tạo payload msi

A computer screen shot of a computer code

AI-generated content may be incorrect.

Tạo file iso bằng cách sử dụng genisoimage

A screen shot of a computer

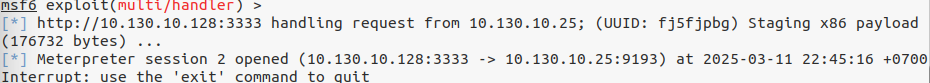
AI-generated content may be incorrect.

Tải file iso về máy window và khởi động( ta sử dụng file iso thay vì msi vì nó giúp vượt qua các cơ chế bảo mật)

A screen shot of a computer

AI-generated content may be incorrect.

Thành công nhận 1 session



1. Sử dụng Sliver

Khởi động sliver server và sử dụng https

A screenshot of a computer

AI-generated content may be incorrect.

Tạo payload dll -> thành công xuất ra file MUSHY\_BLIND.dll

A screenshot of a computer

AI-generated content may be incorrect.

Gửi file sang máy window.

* Xem quyền của file dll vừa tạo



* Chỉ root mới có quyền rwx. Chuyển quyền đó về tài khoản sec560 ta đang sử dụng



* Thành công
* Sử dụng smbclient.py để copy file đến máy chủ(sử dụng tài khoàn bgreen:Password1 đã khai thác ở bài trước)

A screenshot of a computer

AI-generated content may be incorrect.

* Sử dụng wmiexec.py để thực thi file

A computer screen shot of a computer code

AI-generated content may be incorrect.

Nhận được 1 session trên silver server

A close-up of a computer screen

AI-generated content may be incorrect.

Session có id là bd61836d. Sử dụng session bằng 2 chữ cái đầu

A screenshot of a computer program

AI-generated content may be incorrect.