SMB là giao thức chia sẻ file và tài nguyên trên Windows

* Chia sẻ file giữa các máy
* Truy cập từ xa
* Thực hiện lệnh từ xa nếu có quyền admin
* Chạy trên port 445 hoặc 139

Cách thức hoạt động

* Khi client muốn truy cập file trên server, nó gửi yêu cầu qua SMB
* SMB hỗ trợ xác thực bằng tk windows

1. Khởi động Metasploit

A screenshot of a computer

AI-generated content may be incorrect.



1. Thực hiện tấn công

A screen shot of a computer code

AI-generated content may be incorrect.

A computer screen shot of a program

AI-generated content may be incorrect.

Meterpreter dung reverse handler để lắng nghe kết nối từ target. Target thực hti payload, nó kết nối ngược lại, xác thực và thực thi Meterpreter -> thành công tạo 1 Meterpreter session

1. Meterpreter



Thành công có được quyền System của target

Sử dụng session này để lấy những giá trị băm của mục tiêu. Sử dụng **smart\_hashdump** module để trích xuất mật khẩu băm của mục tiêu từ xa ( đôi khi còn có những mật khẩu được gợi ý)A screenshot of a computer

AI-generated content may be incorrect.

Smart\_hashdump sẽ lấy mật khẩu từ gợi ý từ hệ thống nếu bất ký người dung nào cấu hình tài khoản của họ với mật khẩu gợi ý. Tuy nhiên để ý thấy rằng phần thứ 2 của các giá trị băm là null NT hash -> module này không hoạt động tại đây, nhưng sẽ có lợi nếu hoạt đọng trên Domain Controller

Ta sử dụng module hashdump

A screenshot of a computer

AI-generated content may be incorrect.

Thành công lấy được cái giá trị băm từ máy mục tiêu. Cta có thể crack và sử dụng chúng trong pass-the-hash attack

1. Mimikatz setup

Sử dụng mimikatz hay mimikatz kiwi để pass-the-hash

Sử dụng notepad dưới quyền của nguiowf dung bgreen bằng runas

A screenshot of a computer

AI-generated content may be incorrect.

1. Khởi chạy Mimikatz

Thực hiện trên hệ thống Window cục bộ của mình để ko làm sập hệ thống. Mimikatz rất an toàn nhưng ta cần dy chuyển vào 1 quá trình của hệ thống để làm việc này. Nếu nhiều nguiowf cùng di chuyển vào 1 quy trình nhạy cảm cùng lúc sẽ ảnh hướng đến tính ổn định server.

Thoát meterpreter session hiện tại và chuyển sang 1 session khác với người dung là sec560

A screenshot of a computer program

AI-generated content may be incorrect.

Có thể thấy kiến trúc của target là 64bit nhưng với phiên của session lại là 86. Cần phải vào trong quá trình 64bit của hệ thống để thực hiện pass-the-hash

Hãy tìm những quá trình 64bit

A screenshot of a computer

AI-generated content may be incorrect.

Có 1 số quá trình 64bit ở đây. Ta cần xác định các quá trình này để có thể di chuyển vào.

Lưu ý: không nên di chuyển vào quá trình svchost.exe vì có thể gây sập hệ thống và bị bảo vệ chặt chẽ. Nên di chuyển vào spoolsv vì nó ít cần thiết nhất trên hệ thống

A close up of a message

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

Thành công

Load kiwi và creds\_all để lấy các thông tin xác thực

A computer screen shot of a computer

AI-generated content may be incorrect.

Thành công. Thấy được những thông tin như máy hiện tại đang đăng nhập bằng user sec560.

Sử dụng psexec để tạo 1 meterpreter với thông tin xác thực là tài khoản bgreen và Password1. Sau đó sử dụng smart\_dump để thu thập những thông tin hash của các tài khoản cục bộ trong SAM Database(ngoài ra nếu có mật khẩu gợi ý nó cũng sẽ dump ra). Sau đó sử dụng mimikatz để thu thập thông tin những hash này