Credentials Harvesting (Thu thập các thông tin xác thực)

1. Introduction

Chào mừng đến với Credentials Harvesting

Phòng này thảo luận về kiến ​​thức cơ bản dành cho những người trong nhóm đỏ tận dụng thông tin xác thực đã có để thực hiện Di chuyển ngang và truy cập tài nguyên trong môi trường AD.  Chúng tôi sẽ chỉ cho bạn cách lấy, sử dụng lại và mạo danh thông tin xác thực của người dùng.

Thu thập thông tin xác thực bao gồm các kỹ thuật để lấy thông tin xác thực như thông tin đăng nhập, tên tài khoản và mật khẩu. Đây là kỹ thuật trích xuất thông tin xác thực từ hệ thống ở nhiều vị trí khác nhau như tệp văn bản thuần túy, registry, memory dumping, v.v.

Với tư cách là thành viên nhóm đỏ, việc tiếp cận thông tin xác thực hợp lệ có những lợi ích sau:

* Nó có thể cung cấp quyền truy cập vào các hệ thống (Chuyển động ngang).
* Điều này khiến việc phát hiện hành động của chúng ta trở nên khó khăn hơn.
* Nó cung cấp cơ hội tạo và quản lý tài khoản để giúp đạt được mục tiêu cuối cùng của sự tham gia của nhóm đỏ.

Mục tiêu học tập

* Hiểu phương pháp trích xuất thông tin xác thực từ cửa sổ cục bộ (cơ sở dữ liệu SAM)
* Tìm hiểu cách truy cập bộ nhớ Windows và lưu mật khẩu dạng văn bản thuần túy cùng các phiếu xác thực cục bộ và từ xa.
* Giới thiệu về Windows Credentials Manager và cách trích xuất thông tin đăng nhập.
* Tìm hiểu phương pháp trích xuất thông tin xác thực cho Bộ điều khiển miền
* Liệt kê tính năng Giải pháp mật khẩu quản trị viên cục bộ (LAPS).
* Giới thiệu về các cuộc tấn công AD dẫn đến việc lấy được thông tin xác thực.

Điều kiện tiên quyết của phòng

Chúng tôi thực sự khuyên bạn nên hoàn thành các phòng Active Directory sau trước khi tìm hiểu sâu hơn về phòng này:

* [Đường dẫn kiểm tra thâm nhập Jr.](https://tryhackme.com/path-action/jrpenetrationtester/join)
* [Cơ bản về Active Directory](https://tryhackme.com/room/activedirectorybasics)
* [Vi phạm AD](https://tryhackme.com/room/breachingad)
* [Đánh số AD](https://tryhackme.com/room/adenumeration)
* [Chuyển động ngang và xoay](https://tryhackme.com/room/lateralmovementandpivoting)

1. Credentials Harvesting

Credentials Harvesting là thuật ngữ dùng để truy cập vào thông tin xác thực của người dùng và hệ thống.  Đây là kỹ thuật tìm kiếm hoặc đánh cắp thông tin xác thực đã lưu trữ, bao gồm cả việc đánh hơi mạng, trong đó kẻ tấn công sẽ nắm bắt thông tin xác thực đã truyền.

Credentials can be found in a variety of different forms, such as:

* Accounts details (usernames and passwords)
* Hashes that include NTLM hashes, etc.
* Authentication Tickets: Tickets Granting Ticket (TGT), Ticket Granting Server (TGS)
* Any information that helps login into a system (private keys, etc.)

Nhìn chung, có hai loại thu thập thông tin xác thực: bên ngoài và bên trong. Thu thập thông tin xác thực bên ngoài rất có thể liên quan đến email lừa đảo và các kỹ thuật khác để lừa người dùng nhập tên người dùng và mật khẩu của mình. Nếu bạn muốn tìm hiểu thêm về email lừa đảo, chúng tôi khuyên bạn nên thử phòng THM [Phishing](https://tryhackme.com/room/phishingyl). Việc thu thập thông tin xác thực thông qua mạng nội bộ sử dụng các phương pháp khác nhau.

Trong phòng này, trọng tâm sẽ là thu thập thông tin đăng nhập từ góc độ nội bộ, trong đó kẻ tấn công đã xâm nhập vào hệ thống và có được quyền truy cập ban đầu.

Chúng tôi đã cung cấp Windows Server 2019 được cấu hình như một Bộ điều khiển miền. Để theo dõi nội dung được thảo luận trong phòng này, hãy triển khai máy và chuyển sang nhiệm vụ tiếp theo.

Bạn có thể truy cập máy trong trình duyệt hoặc thông qua  RDP  bằng thông tin đăng nhập bên dưới.

Machine IP: 10.10.44.94            Username: thm         Password: Passw0rd!

1. Credential Access (Truy cập thông tin xác thực)

Truy cập thông tin xác thực

Truy cập thông tin xác thực là nơi kẻ tấn công có thể tìm thấy thông tin xác thực trong các hệ thống bị xâm phạm và có được quyền truy cập vào thông tin xác thực của người dùng. Điều này giúp kẻ tấn công sử dụng lại thông tin xác thực hoặc mạo danh danh tính của người dùng. Đây là bước quan trọng để di chuyển ngang và truy cập vào các tài nguyên khác như các ứng dụng hoặc hệ thống khác. Việc có được thông tin xác thực người dùng hợp pháp được ưu tiên hơn là khai thác các hệ thống bằng CVE.

Để biết thêm thông tin, bạn có thể truy cập vào  khuôn khổ MITRE ATT&CK ( [TA0006](https://attack.mitre.org/tactics/TA0006/) ).

Thông tin xác thực được lưu trữ không an toàn ở nhiều vị trí khác nhau trong hệ thống:

* Clear-text files (Các tệp văn bản rõ ràng)
* Database files
* Memory
* Password managers
* Enterprise Vaults (kho lưu trữ của doanh nghiệp)
* Active Directory
* Network Sniffing

Chúng ta hãy thảo luận thêm một chút nhé!

Clear-text files (Các tập tin văn bản rõ ràng)

Kẻ tấn công có thể tìm kiếm thông tin xác thực trong hệ thống tệp cục bộ hoặc từ xa trên máy bị xâm phạm. Tệp văn bản thuần túy có thể bao gồm thông tin nhạy cảm do người dùng tạo, chứa mật khẩu, khóa riêng, v.v.  Khung MITRE ATT&CK định nghĩa thông tin này là  **Unsecured Credentials: Credentials In Files (T1552.001).**

Sau đây là một số loại tệp văn bản thuần túy mà kẻ tấn công có thể quan tâm:

* Lịch sử lệnh
* Tệp cấu hình (Ứng dụng web, tệp FTP , v.v.)
* Các tệp khác liên quan đến Ứng dụng Windows (Trình duyệt Internet, Ứng dụng email, v.v.)
* Các tập tin sao lưu
* Chia sẻ các tập tin và thư mục
* Đăng ký
* Mã nguồn

Là một ví dụ về lệnh lịch sử, PowerShell lưu các lệnh PowerShell đã thực thi trong tệp lịch sử trong hồ sơ người dùng theo đường dẫn sau: **C:\Users\USER\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost\_history.txt**

Có thể đáng để kiểm tra những gì người dùng đang làm hoặc tìm thông tin nhạy cảm. Một ví dụ khác là tìm thông tin thú vị. Ví dụ, lệnh sau là tìm từ khóa "password" trong sổ đăng ký Window.

Tìm kiếm từ khóa "mật khẩu" trong Registry

**c:\Users\user> reg query HKLM /f password /t REG\_SZ /s**

**#OR**

**C:\Users\user> reg query HKCU /f password /t REG\_SZ /s**

Database Files (Tập tin cơ sở dữ liệu)

Các ứng dụng sử dụng các tệp cơ sở dữ liệu để đọc hoặc ghi các thiết lập, cấu hình hoặc thông tin xác thực. Các tệp cơ sở dữ liệu thường được lưu trữ cục bộ trong hệ điều hành Windows.  Các tệp này là mục tiêu tuyệt vời để kiểm tra và săn tìm thông tin xác thực.  Để biết thêm thông tin, chúng tôi đề xuất kiểm tra phòng THM : [Breaching AD](https://tryhackme.com/room/breachingad) . Nó chứa một ví dụ minh họa về cách trích xuất thông tin xác thực từ tệp cơ sở dữ liệu McAfee Endpoint cục bộ.

Password Managers (Trình quản lý mật khẩu)

Trình quản lý mật khẩu là ứng dụng lưu trữ và quản lý thông tin đăng nhập của người dùng cho các trang web và dịch vụ cục bộ và Internet. Vì nó xử lý dữ liệu của người dùng nên phải được lưu trữ an toàn để ngăn chặn truy cập trái phép.

Ví dụ về ứng dụng Quản lý mật khẩu:

* Trình quản lý mật khẩu tích hợp (Windows)
* Bên thứ ba: KeePass, 1Password, LastPass

Tuy nhiên, các ứng dụng này có cấu hình sai và lỗi bảo mật cho phép kẻ tấn công truy cập dữ liệu được lưu trữ. Nhiều công cụ khác nhau có thể được sử dụng trong giai đoạn liệt kê để lấy dữ liệu nhạy cảm trong các ứng dụng quản lý mật khẩu được trình duyệt Internet và ứng dụng máy tính để bàn sử dụng.

Phòng này sẽ thảo luận về cách truy cập trình quản lý Windows Credentials và trích xuất mật khẩu.

Memory Dump

Bộ nhớ của hệ điều hành là nguồn thông tin nhạy cảm phong phú thuộc về hệ điều hành Windows , người dùng và các ứng dụng khác. Dữ liệu được tải vào bộ nhớ khi chạy hoặc trong quá trình thực thi. Do đó, việc truy cập bộ nhớ bị giới hạn đối với người dùng quản trị viên kiểm soát hoàn toàn hệ thống.

Sau đây là các ví dụ về dữ liệu nhạy cảm được lưu trữ trong bộ nhớ, bao gồm:

* Thông tin xác thực dạng văn bản rõ ràng
* Mật khẩu được lưu trong bộ nhớ đệm
* Vé AD

Trong phòng này, chúng ta sẽ thảo luận về cách truy cập vào bộ nhớ và trích xuất mật khẩu dạng văn bản thuần túy cùng các phiếu xác thực.

Active Directory (Thư mục hoạt động)

Active Directory lưu trữ rất nhiều thông tin liên quan đến người dùng, nhóm, máy tính, v.v. Do đó, việc liệt kê môi trường Active Directory là một trong những trọng tâm của các đánh giá của nhóm đỏ. Active Directory có thiết kế vững chắc, nhưng việc cấu hình sai của quản trị viên khiến nó dễ bị tấn công theo nhiều cách khác nhau được trình bày trong phòng này.

Sau đây là một số cấu hình sai của Active Directory có thể làm rò rỉ thông tin đăng nhập của người dùng .

* **Mô tả của người dùng** : Người quản trị đặt mật khẩu trong phần mô tả cho nhân viên mới và giữ nguyên ở đó, khiến tài khoản dễ bị truy cập trái phép.
* **Chính sách nhóm SYSVOL** : Khóa mã hóa bị rò rỉ cho phép kẻ tấn công truy cập vào tài khoản quản trị viên. Kiểm tra Nhiệm vụ 8 để biết thêm thông tin về phiên bản SYSVOL dễ bị tấn công.
* **NTDS:** Chứa thông tin đăng nhập của người dùng AD, khiến nó trở thành mục tiêu của kẻ tấn công.
* **Tấn công AD :** Cấu hình sai khiến AD dễ bị tấn công theo nhiều cách khác nhau, chúng ta sẽ thảo luận về vấn đề này trong Nhiệm vụ 9.

Network Sniffing

Việc có được quyền truy cập ban đầu vào mạng mục tiêu cho phép kẻ tấn công thực hiện nhiều cuộc tấn công mạng khác nhau vào máy tính cục bộ, bao gồm cả môi trường AD . Cuộc tấn công Man-In-the-Middle vào các giao thức mạng cho phép kẻ tấn công tạo ra một tài nguyên đáng tin cậy giả mạo hoặc giả mạo trong mạng để đánh cắp thông tin xác thực như băm NTLM .

Câu 1:

A black background with white text

Description automatically generated

Câu 2

Get-ADUser -Filter \* -Properties \* | select Name,SamAccountName,Description