# Mục tiêu:

+ Dùng beRoot.exe và Power up để tìm các vấn đề liên quan đến leo thang đặc quyền

+ Lợi dụng cài đặt trong window để leo thang đặc quyền

# 1. Log on to Windows

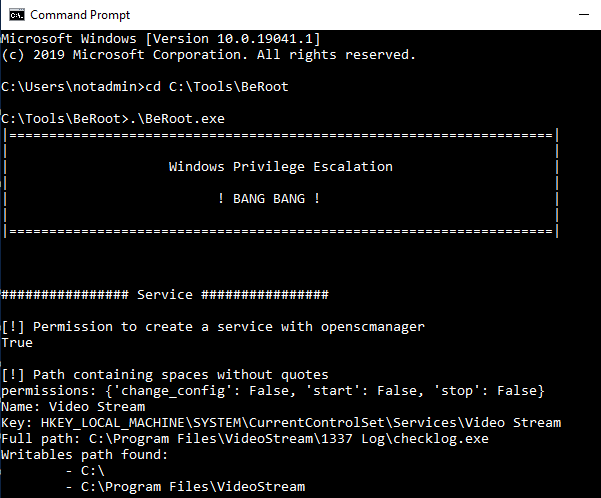
Username: notadmin

Password: notadmin

# 2. Run beRoot.exe (Để leo thang đặc quyền)

# 3. Review beRoot’s results

beRoot.exe cung cấp phản hồi lập tức về các khả năng leo thang đặc quyền. Và nó tìm ra đc 1 khả năng với dịch vụ video stream trên windows



# 4. Run PowerUp.ps1

# 5. Review PowerUp.ps1

PowerUp là 1 trong những cơ chế chính để thực hiện tấn công leo thang đặc quyền

Invoke-allchecks là thực hiện kiểm tra. Kết quả đầu ra số lượng lỗ hổng đến DLL hịjacking ở đường dẫn %PATH%; 1 số lỗ hổng liên quan đến sự cho phép và chạy dịch vụ; dịch vụ video stream ko có đường dẫn %PATH%

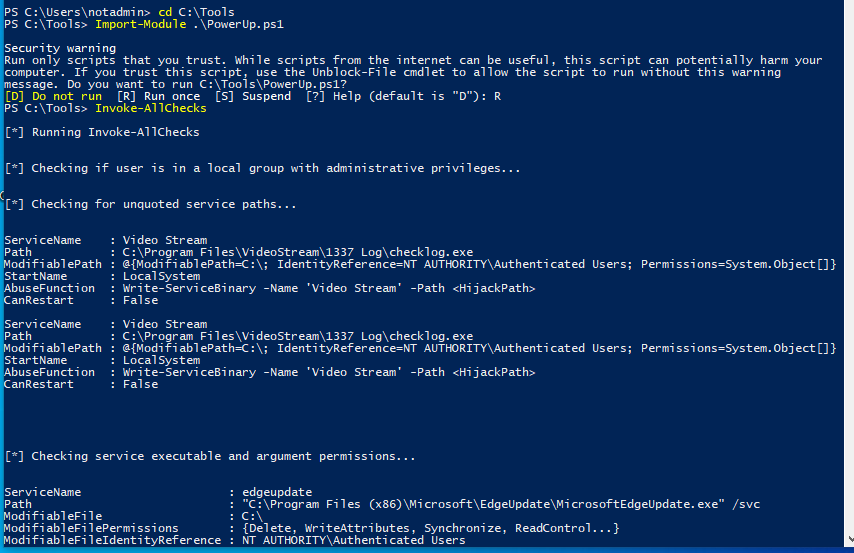
PowerUp nên trả về một số kết quả có thể đáng chú ý:

· Đường dẫn dịch vụ không được trích dẫn cho dịch vụ Video Stream (như được xác định bởi BeRoot.exe)

· Một số lỗ hổng tiềm năng về DLL hijacking trong các thư mục %PATH%

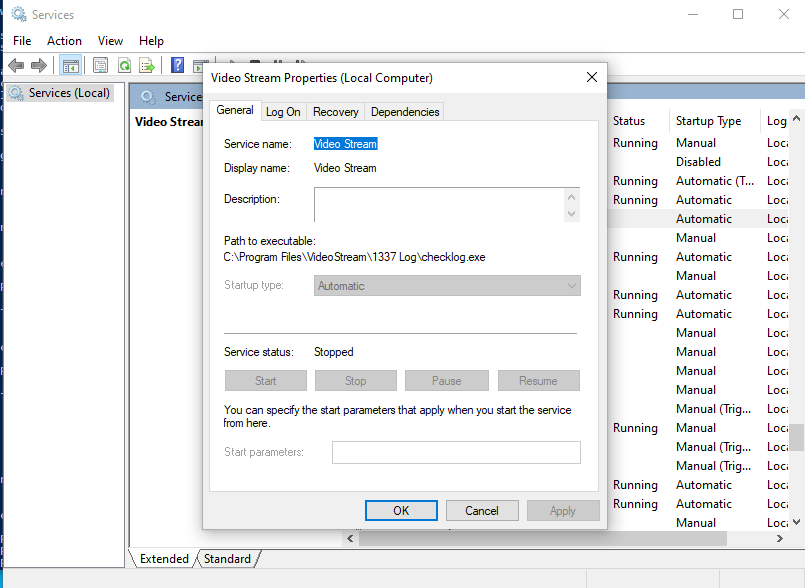
· Một số lỗ hổng liên quan đến các tập tin và quyền thực thi dịch vụ

Kết quả từ cả beRoot.exe và PowerUp luôn cần một số xác minh thủ công, vì đôi khi chúng hiểu sai quyền lồng nhau



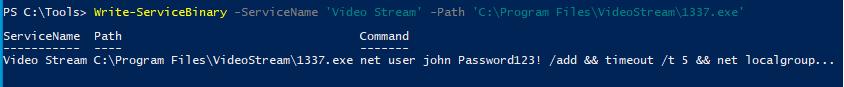
# 6. Review the “Video Stream” service in services view

Services.msc để xem các dịch vụ trên windows



# 7. Exploiting the vulnerability using PowerUp

# 8. Adapt the “HijackPath”



Kết quả là: "Lệnh PowerUp ở trên sẽ viết một tập lệnh độc hại vào vị trí cuối cùng! Kết quả của việc chạy AbuseFunction, bạn sẽ nhận thấy rằng tập lệnh được viết bởi PowerShell sẽ tạo một người dùng có tên john với mật khẩu Password123! Sau đó, người dùng này sẽ được thêm vào nhóm quản trị viên cục bộ."

# 9. Reboot the computer

# 10. Log on to windows

# 11. Confirm user was added

Net users để quản lý người dùng trên hệ thống

