**BỘ CÔNG THƯƠNG**



**TRƯỜNG ĐẠI HỌC CÔNG THƯƠNG TP. HCM KHOA CÔNG NGHỆ THÔNG TIN**

**---------------**

BÀI TIỂU LUẬN

## MÔN HỌC: PHÂN TÍCH LỖ HỔNG VÀ KIỂM THỬ

**Giảng viên hướng dẫn:** Nguyễn Thị Hồng Thảo

**SYSTEM HACKING**

1

# MỤC LỤC

[MÔN HỌC: PHÂN TÍCH LỖ HỔNG VÀ KIỂM THỬ 1](#_Toc147958808)

[MỤC LỤC 2](#_Toc147958809)

[Cracking Password 3](#_Toc147958810)

[Escalating Privileges (Dùng kỹ thuật Always Install Elevated) 6](#_Toc147958811)

[Executing Applications 9](#_Toc147958812)

[Hiding Files 10](#_Toc147958813)

[Covering Tracks 11](#_Toc147958814)

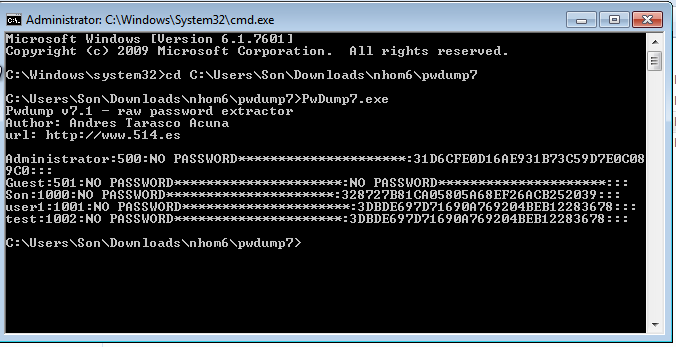
[Penetration Testing 12](#_Toc147958815)

[Tài liệu tham khảo 13](#_Toc147958816)

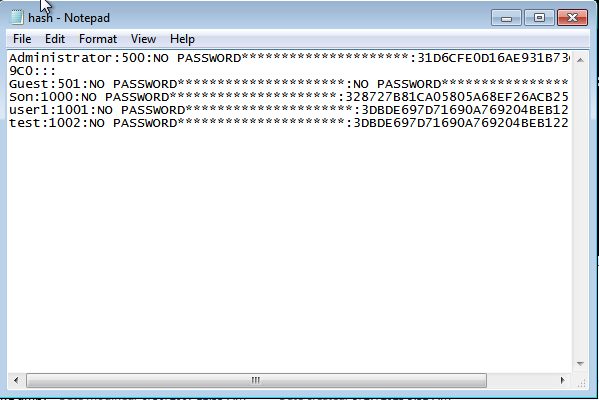
# Cracking Password

**Dùng OHP Crack**

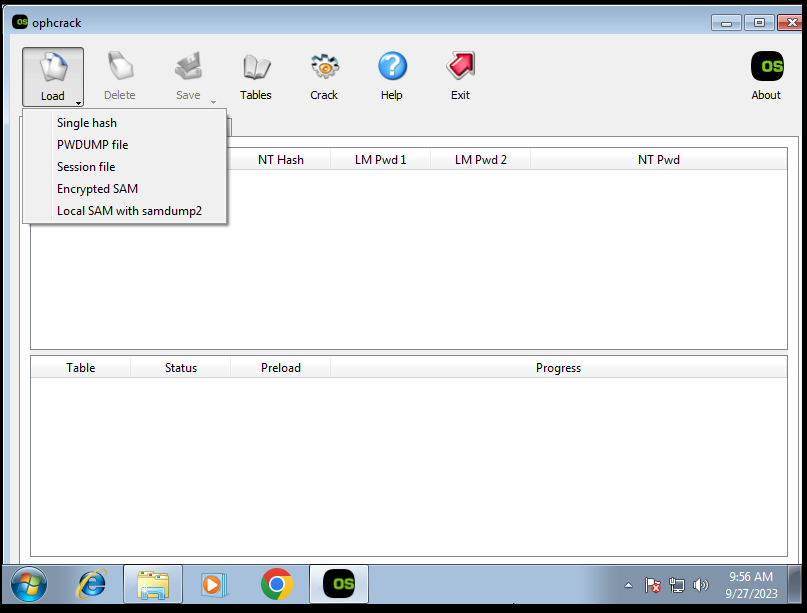
Mở CMD => trỏ đường dẫn tới thư mục pwdump7 => thực thi file PwDump7.exe

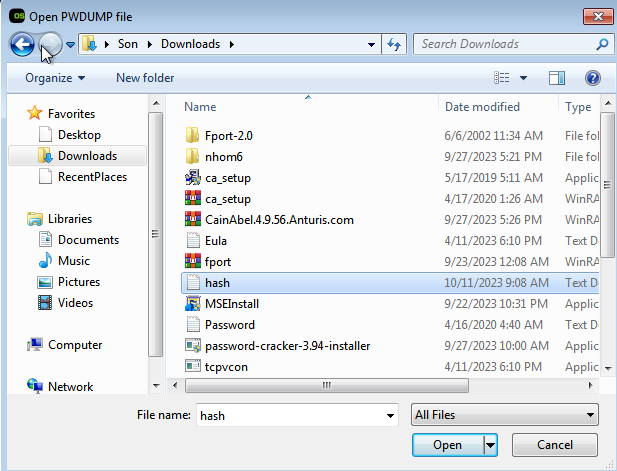


Copy từ Administrator đến 678::: vào 1 file txt và save với tên hash

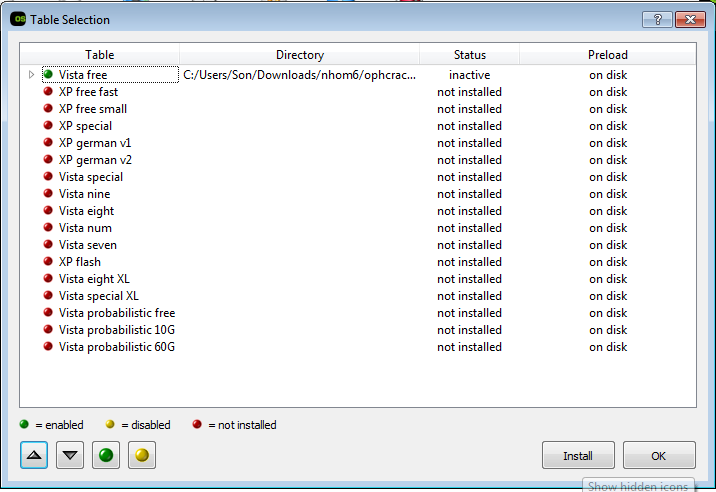


Mở Ohpcrack => chuột phải Load => chọn PWDUMP file => chọn filw Hash vừa lưu

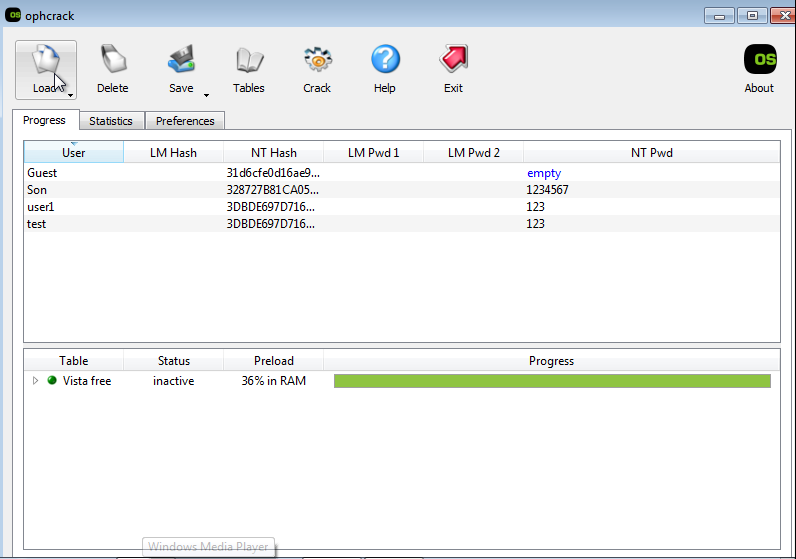




Vào Tables => Chọn Vista free => click install

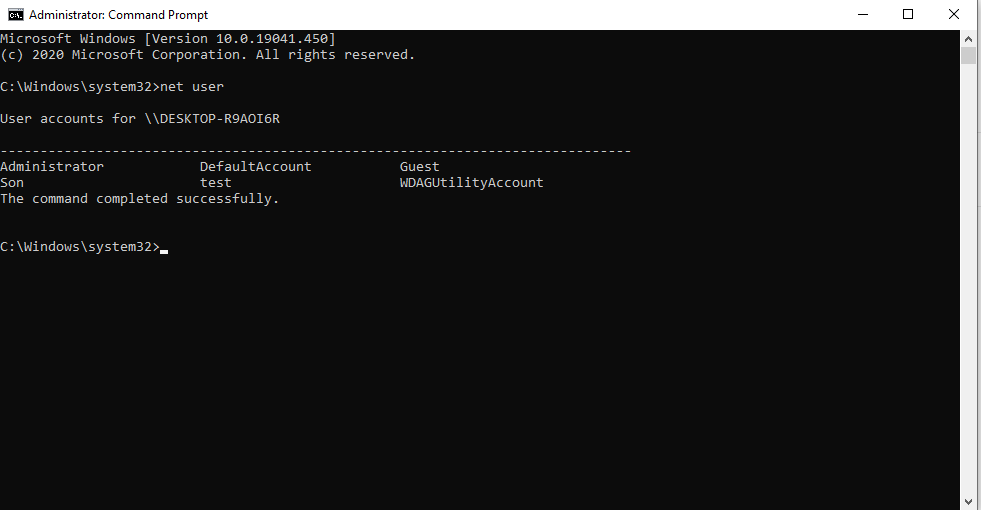


Click Crack => Đã tìm thấy password của user Son là 1234567, user test là 123

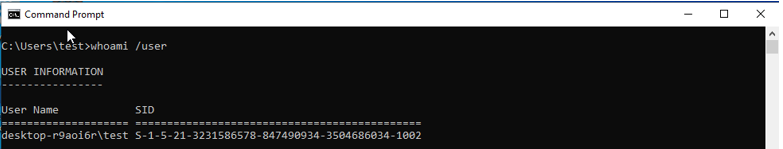


# Escalating Privileges (Dùng kỹ thuật Always Install Elevated)

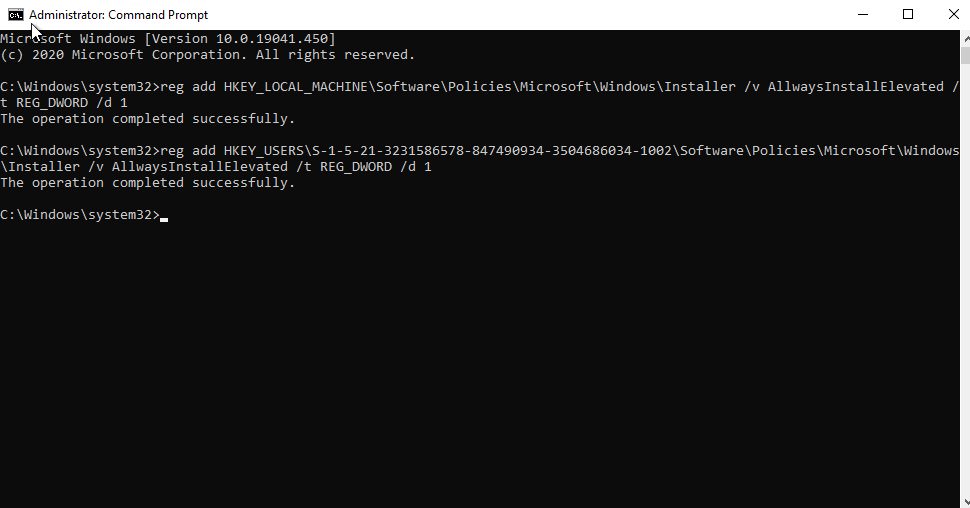
Tại máy win10 đăng nhập vào user test



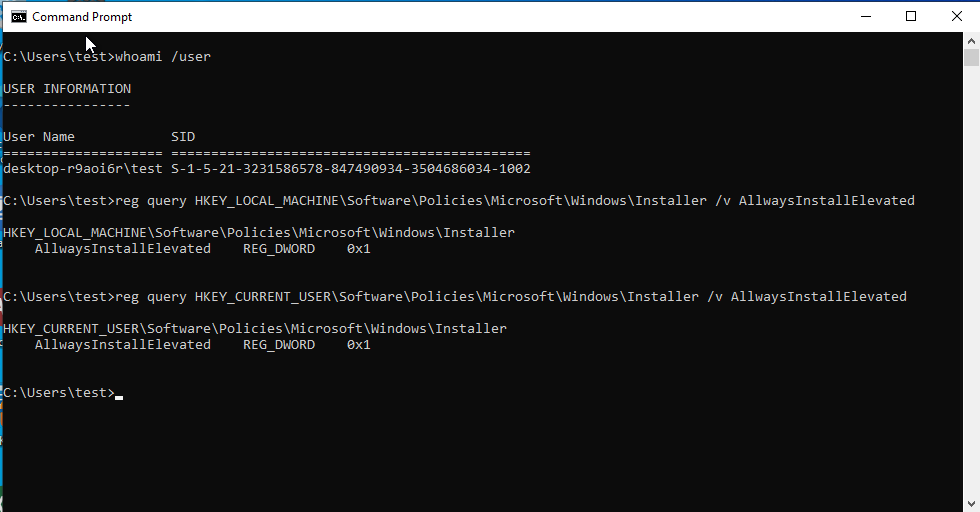
Tại cmd dưới quyền user test => Dùng lệnh whoami /user để hiện SID của user test



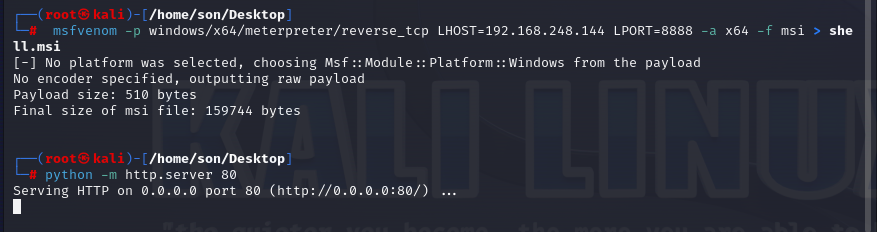
Mở cmd dưới quyền Administrator => tạo ra registry cho Local\_machine và user test



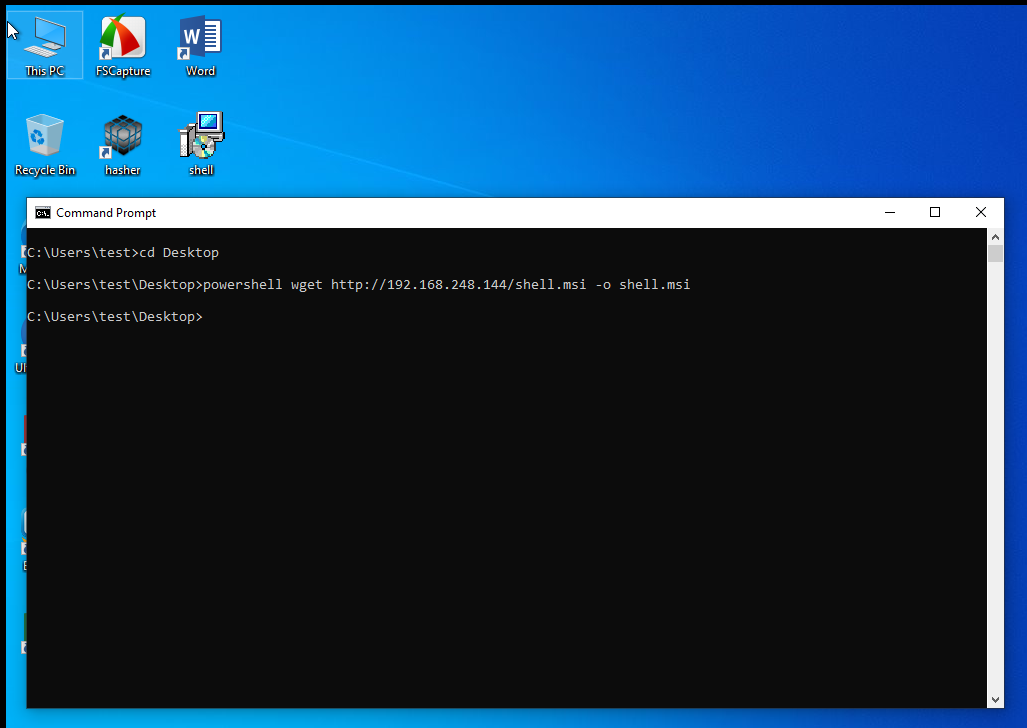
Tại cmd dưới quyền user test dùng 2 lệnh dưới để kiểm tra xem tạo 2 registry thành công chưa



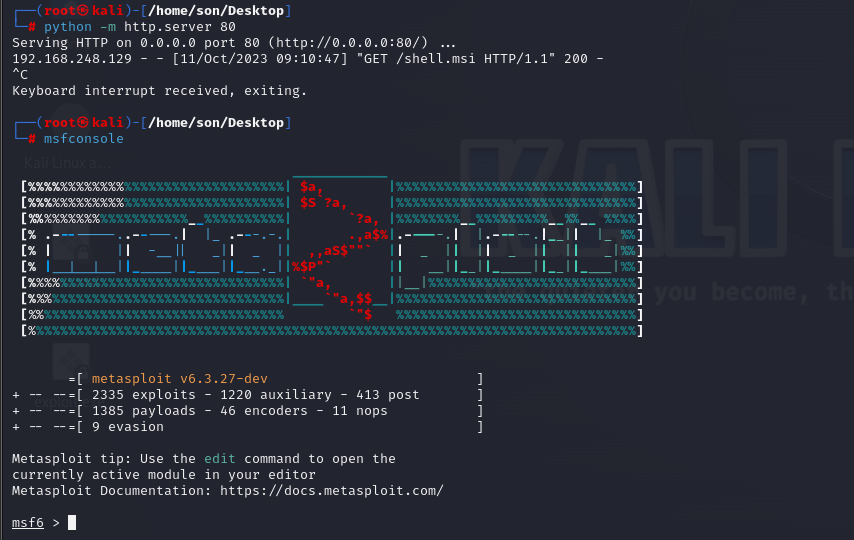
Mở máy Kali dùng lệnh để tạo ra một mã độc có tên là shell định dạng msi



Tại máy win 10 dùng lênh dưới để tải downloaf file shell.msi về



Dùng msfconsole để hứng kết nối => gõ use/exploit/multi/handler => set payload

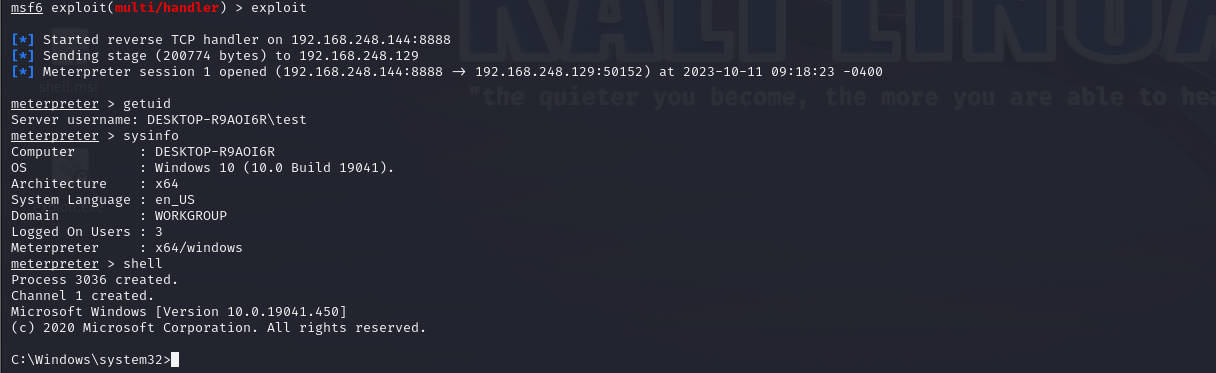




Tại máy win10 gõ lệnh sau để thực thi file shell.msi

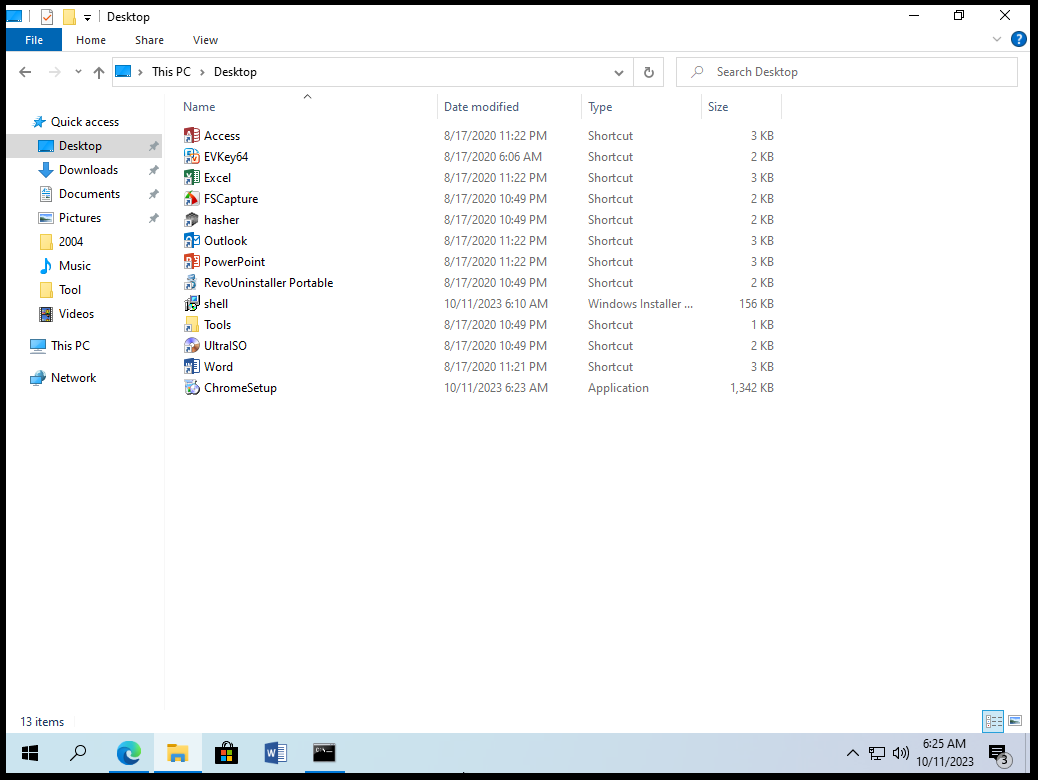


Quay lại Kali => Kết quả thông tin máy win10 đã được trả về. Khi nhấn shell thì giờ đây tại máy kali có thể điều khiển máy win10 với user test bằng quyền hạn cao nhất

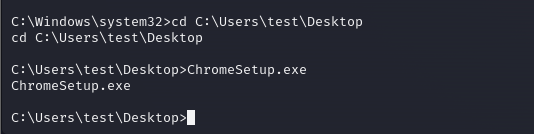


# Executing Applications

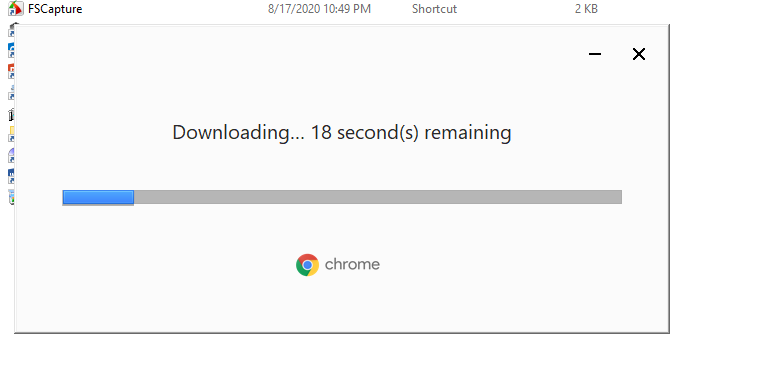
Tại máy win10 ta giả sử file ChromeSetup.exe là file mã độc được cài vào



Quay lại Kali đang ở trạng thái shell ta nhập lệnh như sau để thực hiện file ChromeSetup.exe

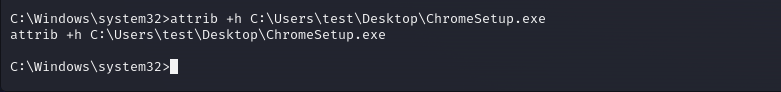


Kết quả tại máy win10 file ChromeSetup.exe đã được thực thi

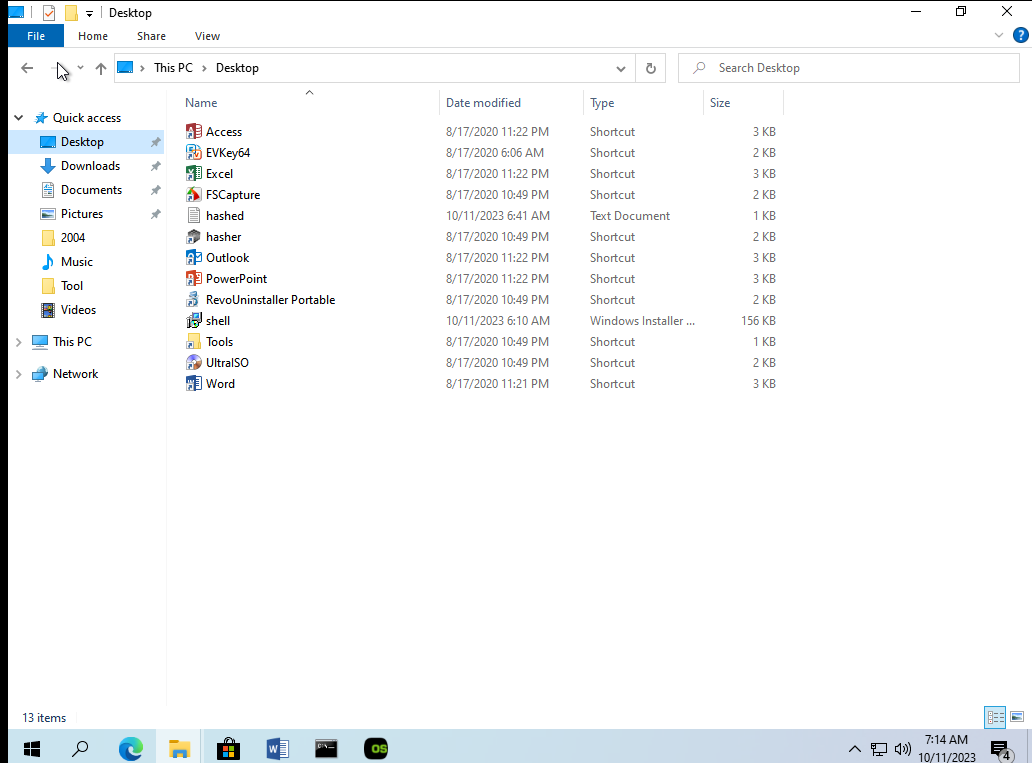


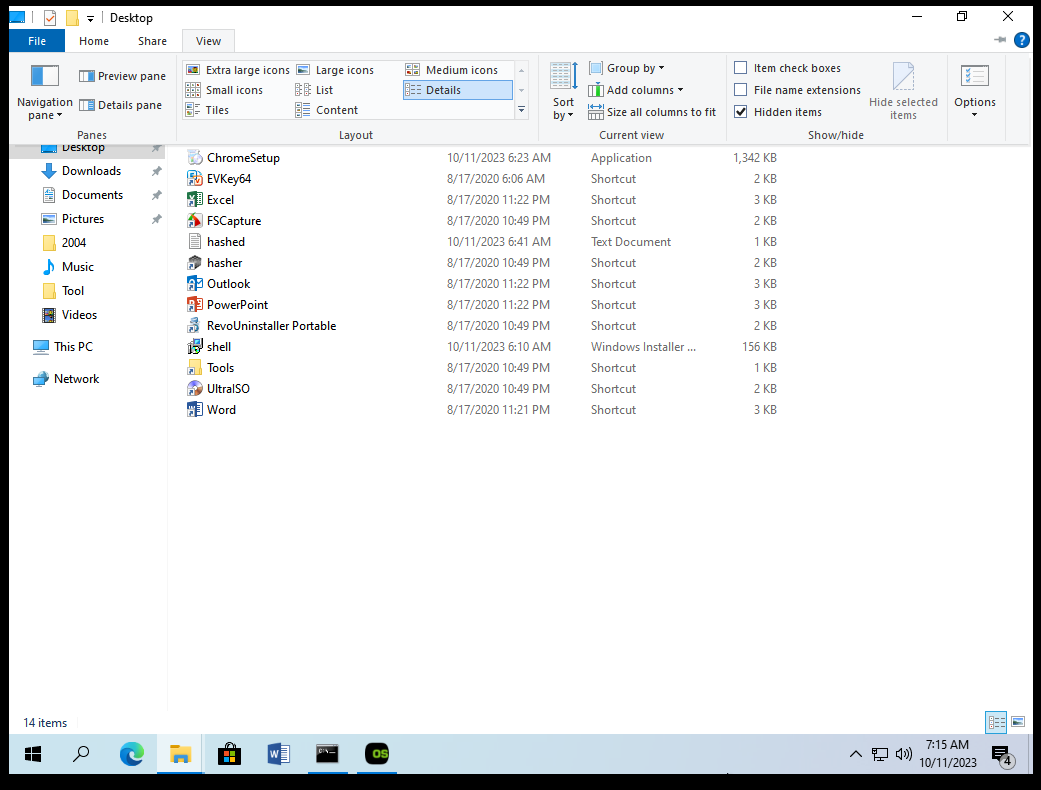
# Hiding Files

Tại kali => Dùng lệnh sau để ẩn file ChromeSetup.exe



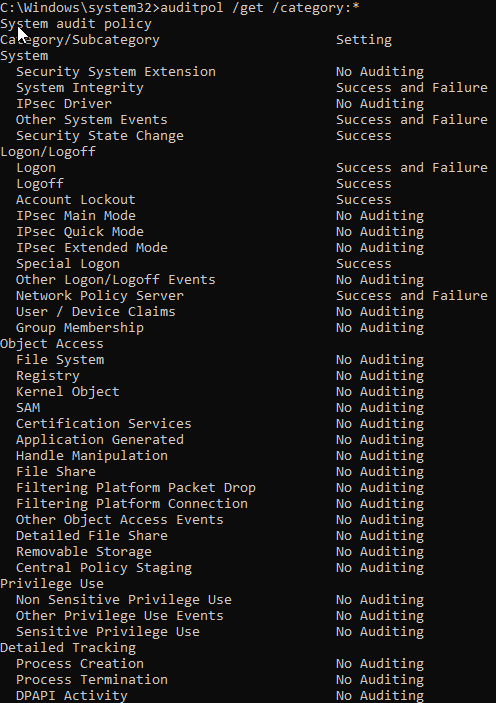
Khi qua máy Win10 => file ChromeSetup.exe đã bị ẩn. Chỉ khi click vào hidden file trong mục views thì nó mới hiện ra



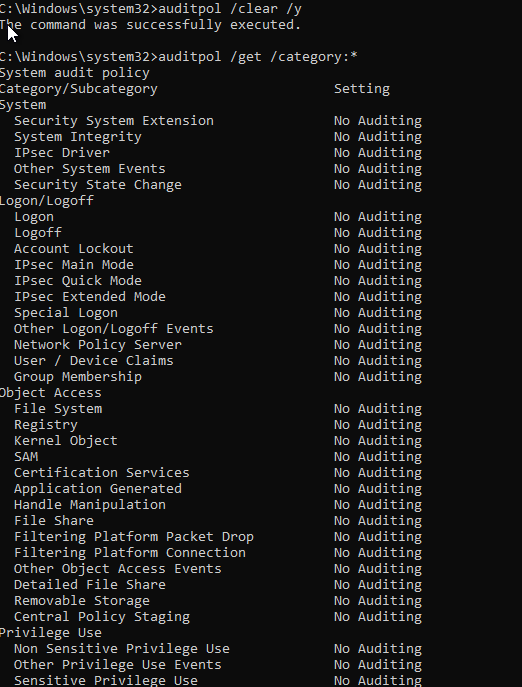


# Covering Tracks

Dùng lệnh Audit /get /category:\* để xem tất cả các tính năng giám sát



Dùng lệnh Audit /clear /y để xem tất cả các tính năng giám sát



# Tài liệu tham khảo

1. CEH v10
2. ChatGPT
3. <https://helpex.vn/article/hieu-sau-hon-ve-cac-cuoc-tan-cong-leo-thang-dac-quyen-608ea6512744c49a00465af3>