Graphical user interface, text

Description automatically generated

Lâu lắm rồi thì hôm nay mk mới trở lại với 1 bài trên Tryhackme có tên là Flatline. Bắt đầu thôi.

1. Dò quét

rustscan -b 500 -a 10.10.18.114

Graphical user interface, application

Description automatically generated

2 port đang được mở là 3389 và 8021. Với port 3389 thì chúng ta dễ dàng đoán ra OS là Windows. Mk thấy có port 8021 này khá lạ => Dò quét chi tiết hơn xem nó là cái gì

nmap -p 3389,8021 -sC -sV -v 10.10.18.114 -T4 -Pn

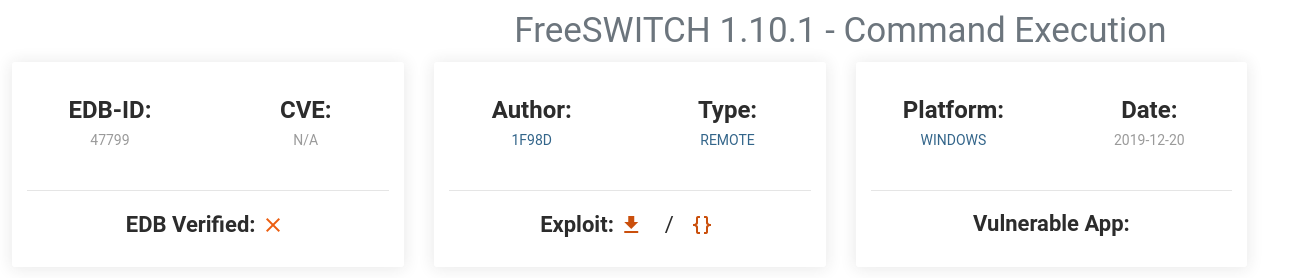
Graphical user interface, text, application

Description automatically generated

“freeswitch-event” khá lạ. Port 8021 này lúc mới đầu mk nhớ nhầm, tưởng nó là vnc =))

1. Enum

Theo quán tính thì phải search ngay xem freeswitch-event có lỗi gì ko và kết quả như mong đợi



1. Exploit

Text

Description automatically generated

Mới đầu mk dùng Metasploit để khai thác nhưng bị lỗi ko nên đành phải chuyển qua dùng đoạn script trên exploitdb vậy.

Do code trên exploitdb chưa đc tối ưu lắm nên mk edit lại chút

Text

Description automatically generated

Sau đó thì chạy thôi.

Text

Description automatically generated

User hiện tại là “nekrotic”

Text

Description automatically generated

Điều đặc biệt là user này lại thuộc group Administrators. Về PrivEsc trên Windows thì có 2 room trên Tryhackme là “Windows PrivEsc” và “Windows PrivEsc Arena”, các bạn có thể tham khảo để rèn luyện thêm. Các lab liên quan đến OS Windows thường sẽ phải trả phí nên mk cũng ko đc luyện tập nhiều như các lab bên Linux (do nghèo ấy mà =)))

Graphical user interface

Description automatically generated

“SeImpersonatePrivilege” đang ở trạng thái Enabled. Tận dụng quyền này để leo thang thì ở đây mk dùng cách dễ nhất ấy là sd module “incognito” trên Metasploit. Tham khảo https://www.offensive-security.com/metasploit-unleashed/fun-incognito/

Bước 1: Tạo mã độc với msfvenom

Bước 2: Chạy mã độc trên máy victim

Bước 3: Lắng nghe kết nối đến

A screenshot of a computer

Description automatically generated

Text

Description automatically generated



Đợi 1 lúc thì kết nối đến

Text, chat or text message

Description automatically generated

Thành công. Nhiệm vụ hoàn thành