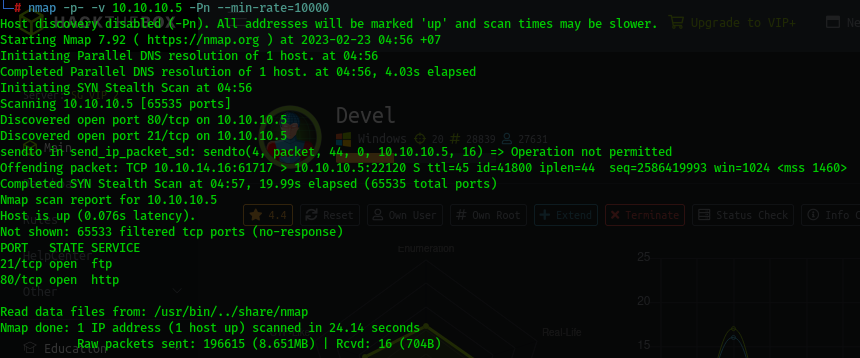
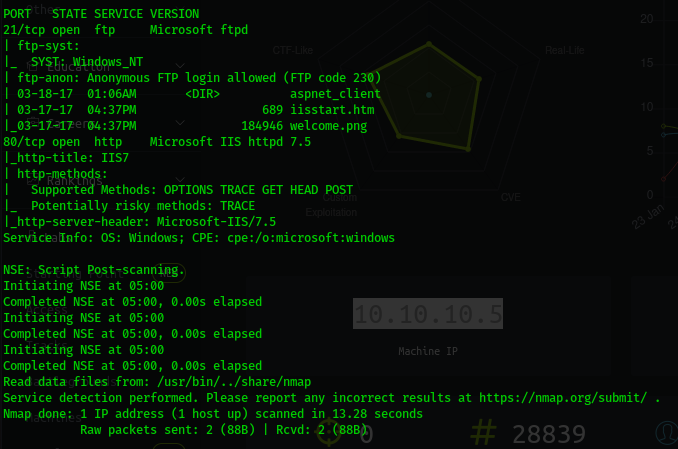


Cũng đã lâu lắm rồi mk ko viết writeup, thì ngày hôm nay mk sẽ trở lại với 1 chuỗi các bài trên Hackthebox và bài lần này có tên là “Devel”.

1. **Dò quét**



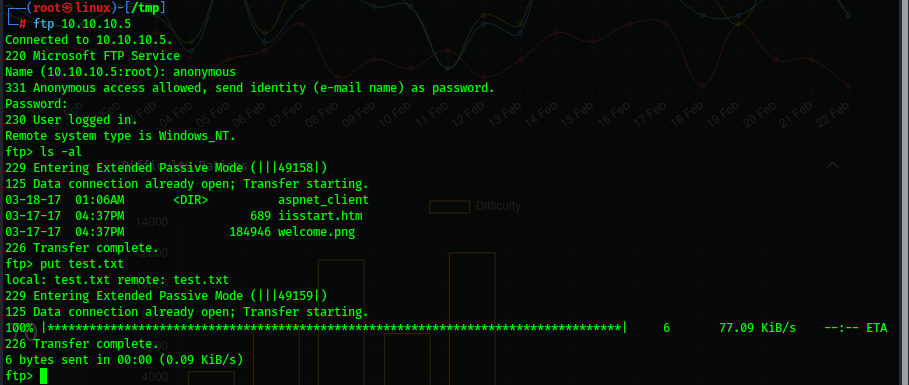
Có 2 port đang mở là ftp – 21 và http – 80.



Như mn thấy đây là máy sử OS Windows và một điều quan trọng khi cta nhìn kết quả dò quét là ở dv ftp thì nó đang share các file thuộc dịch vụ web và nó cho phép chúng ta login mà ko cần mật khẩu (anonymous login). Điều này có nghĩa là nếu chúng ta có quyền write trên folder này thì có thể upload một con webshell. Một điều nữa cần lưu tâm là Web Server của nó là IIS Server => nếu upload thì cần phải lựa chọn ngôn ngữ cho phù hợp (.asp hoặc .aspx)

Khi research thì mk biết được thư mục mặc định của dịch vụ web trên Windows đặt ở vị trí “ C:\inetpub\wwwroot”

1. **Enum**



Mk có upload thử 1 file có tên là “test.txt” và kết quả thật bất ngờ. Dịch vụ ftp này cho phép chúng ta upload file lên server mà ko cần xác thực gì cả.

Thế thì hướng mk nhận định ở trên là khá chuẩn =)).

1. **Exploitation**

Graphical user interface, text, application, email

Description automatically generated

Mk sẽ dùng con web shell này. Lưu ý: cần thay đổi host và port.

Graphical user interface

Description automatically generated with low confidence

A picture containing text, dark, clock

Description automatically generated

Thực hiện upload shell.aspx và lắng nghe kết nối đến cổng 4444.

A picture containing graphical user interface

Description automatically generated

Text

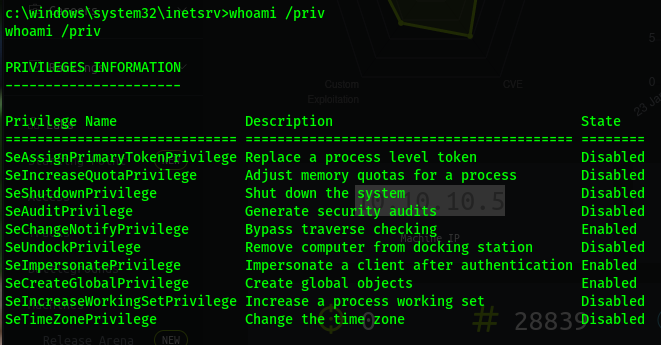
Description automatically generated

Đến đây là thành công được 1 nửa rồi.

1. **Leo thang**

Graphical user interface, text, chat or text message

Description automatically generated



Graphical user interface, text, application, chat or text message

Description automatically generated

Một số lệnh mk thường dùng để enum trên máy local Windows. Với “systeminfo” để ta biết được Name/Version của OS, “whoami /priv” để xem user này có những permission nào, “net user” để liệt kê các user hiện có.

Một số hướng khi leo thang: check version => xem có phiên bản đó có xuất hiện lỗi nào ko; permission của user hiện tại (như kết quả ở trên thì “SeImpersonatePrivilege” đang được Enable => có thể tận dụng); tìm password mà user đó lưu trên máy; user hiện tại đang thuộc group nào và nếu thuộc group đặc biệt => có thể tận dụng quyền của group đó; check xem những phần mềm mà target cài đặt có cái nào bị dính lỗi ko;………….

A screenshot of a computer

Description automatically generated with medium confidence



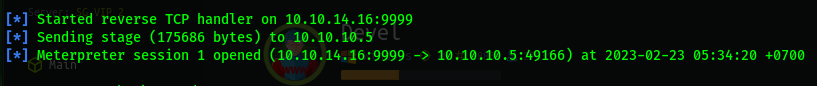
Text

Description automatically generated

Graphical user interface, text, chat or text message

Description automatically generated

Sau khi chạy file privesc.exe thì ngay lập tức 1 session đã được open trên meterpreter =)).

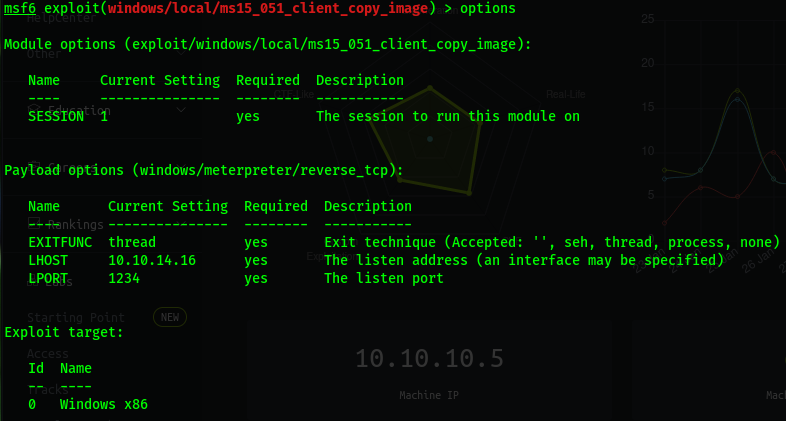


Tiếp đó, sử dụng module local\_exploit\_suggester để check xem trên version này có những lỗi gì chưa được fix.

Graphical user interface, text, application, chat or text message

Description automatically generated

Khi xem kết quả thì thấy rằng, target dính khá nhiều lỗi và nó cũng chưa được fix. Mk quyết định thử với lỗi “windows/local/ms15\_051\_client\_copy\_image”.



Sau khi set có tham số rồi thì tiến hành chạy mã khai thác. Và đây là kết quả:

Graphical user interface, text, application, chat or text message

Description automatically generated