Graphical user interface, text, application

Description automatically generated

Hôm nay mk trở lại với 1 bài mới trên Tryhackme, đó là Oh My WebServer. Bắt đầu thôi

1. Dò quét

nmap -p- -v -T4 10.10.202.189 -Pn

A screenshot of a computer

Description automatically generated with low confidence

Tìm được 2 port quen thuộc là 22 và 80

nmap -sC -sV -v -p 22,80 10.10.202.189 -Pn

Text

Description automatically generated

1. Enum

Graphical user interface, text, application

Description automatically generated

Đây là port 80. Mk quyết định tìm hidden files/folders.

gobuster dir -u http://10.10.202.189/ -w /usr/share/wordlists/dirb/big.txt -t 100 -x html,php,txt

Graphical user interface

Description automatically generated

/cgi-bin/ thế này thì khả năng Shell shock là khá cao he.

gobuster dir -u http://10.10.202.189/cgi-bin/ -w /usr/share/wordlists/dirb/big.txt -t 100 -x cgi,sh

A picture containing text

Description automatically generated

Tìm được 2 thư mục nhưng ko giúp ích được gì. Hmm, sử dụng nikto xem có phát hiện được gì ko

A picture containing graphical user interface

Description automatically generated

Đợi cái nikto này lâu quá nên mk xem phiên bản Apache này có lỗi gì ko

Graphical user interface, text, application

Description automatically generated

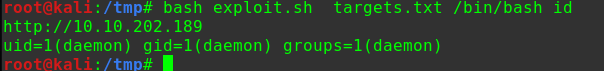
RCE luôn ạ =)). Quá ngon.

1. Khai thác

Graphical user interface, text

Description automatically generated

Test thử cái xem sao



Thành công. Get shell thôi. Mk sửa lại đoạn mã khai thác trước

Text

Description automatically generated

Và đây là kết quả

Text

Description automatically generated

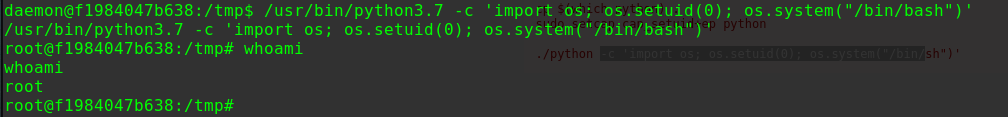
1. Leo thang

Sau 1 hồi vật vã tìm nhưng ko thấy gì nên mk phải dùng đến công cụ linpeas

Graphical user interface, text, chat or text message

Description automatically generated

Hú hú khá là ghê đây. <https://gtfobins.github.io/gtfobins/python/#capabilities> tham khảo đường link này để khai thác



Thành công. Với hướng cap\_chown thì mn có thể tham khảo link này để leo thang: https://player.vimeo.com/video/436702904