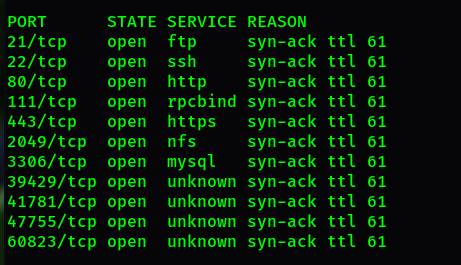
Graphical user interface, text, application, website

Description automatically generated

Lâu lắm rồi, hn mk mới trở lại với 1 bài trên Tryhackme có tên là “Corgi”.

1. Dò quét

rustscan -b 500 -a 10.10.49.27



Rất nhiều port/service được mở.

nmap -p 21,22,80,111,443,2049,3306,39429,41781,47755,60823 -sC -sV -v -T4 10.10.49.27 -Pn

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

Dịch vụ tìm được đó là: FTP, SSH, NFS, HTTP/HTTPS, MYSQL

1. Enum

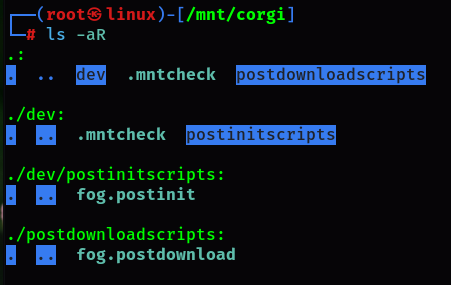
Với ftp mk thử qua anonymous login => ko thành công (từ kết quả Nmap cũng cho biết điều đó)

Với mysql chúng ta thử 1 vài creds mặc định => kết quả tương tự như bên ftp

Vậy bh chỉ còn lại http/https và nfs. Mk thấy nfs sáng cửa hơn nhiều =))

Graphical user interface, text

Description automatically generated



Rất nhiều file/folder được share. Lúc đầu, mk đoán folder được mount này rất có thể là web folder/file hoặc là 1 cronjob nào đó mà mk có thể tận dụng để upload shell. Nhưng chúng ta chỉ có quyền read chứ ko thể write hoặc remove.

Mk có check thử trên web xem có tồn tại những file/folder này

Text

Description automatically generated

Kết quả ko đc như mong đợi.

Cũng ko có .git folder. Công cuộc này xem ra còn căng đây.

Graphical user interface, application, website

Description automatically generated

Sau 1 hồi thư giãn đầu óc mk quyết định research xem những file trong thư mục được mount là gì

Graphical user interface, text, application, email

Description automatically generated

Thì ra nó là FOGProject. Cái này mk chưa nghịch bh =)). Đương nhiên theo quán tính chúng ta phải research ngay với keyword là: fogproject exploit.

Graphical user interface, application, Word

Description automatically generated

1. Exploitation

Theo như PoC trên ExploitDB chúng ta sẽ tìm được tới giao diện của Project trên web. Vấn đề đặt ra ở đây là chúng ta ko có user/pass.

Graphical user interface, application

Description automatically generated

Thử qua 1 số creds như: admin:admin, admin:password, root:root, root:toor,…. đều ko đc. Mk chuyển sang xem default password của nó là gì. Và đã tìm được.

Graphical user interface, text, application

Description automatically generated

Sử dụng user/pass này để login vào admin dashboard.

Giao diện cũng khá đẹp mắt

Graphical user interface, application

Description automatically generated

Dễ thấy version của nó là 1.5.9 trùng với version bị lỗi chúng ta tìm đc trên exploitDB. Chúng ta sẽ tiến hành các bước theo hướng dẫn này:



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

Description automatically generated

Graphical user interface, application

Description automatically generated

Sau khi đã install thành công shell lên thì hãy xem thành quả thôi.

Graphical user interface, text, application

Description automatically generated

Đến bước này thì quen thuộc rồi. Get shell về máy chúng ta thôi.

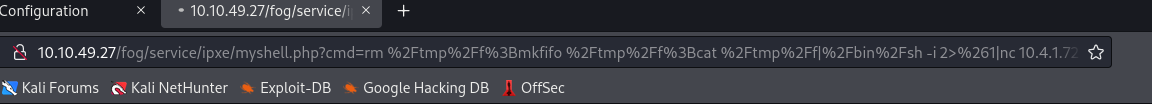
Text

Description automatically generated

Text

Description automatically generated

Lấy đoạn payload đã được url encode và chạy



Kết quả

Text

Description automatically generated

1. Leo thang

Text

Description automatically generated

Tệp cupsfilter nhìn khá đáng ngờ. Mk quyết định tra trên gtfobin.

Graphical user interface, text, application

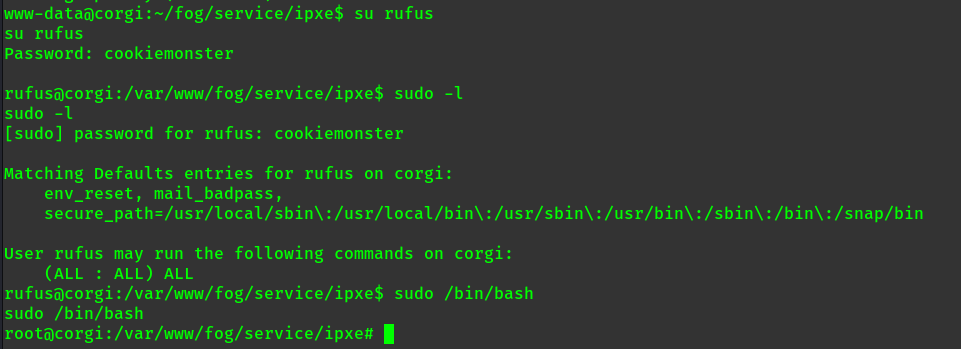
Description automatically generated

Cho phép read file => có thể đọc những file như id\_rsa, /etc/shadow,….hoặc bất kỳ file nào chúng ta thích =)).

Text

Description automatically generated

Thu được 2 hash của user rufus và fogproject. Tiến hành crack 2 hash này. “cookiemonster” là password của user rufus.



Thành công. Nhiệm vụ hoàn thành.