Hôm nay mk tiếp tục với 1 bài trên Tryhackme là “Cat Pictures”. Bài này thì ra cách đây cũng 1 thời gian dài rồi nhưng mk thấy hay nên quyết định viết writeup. Bắt đầu thôi.

Graphical user interface, text

Description automatically generated with medium confidence

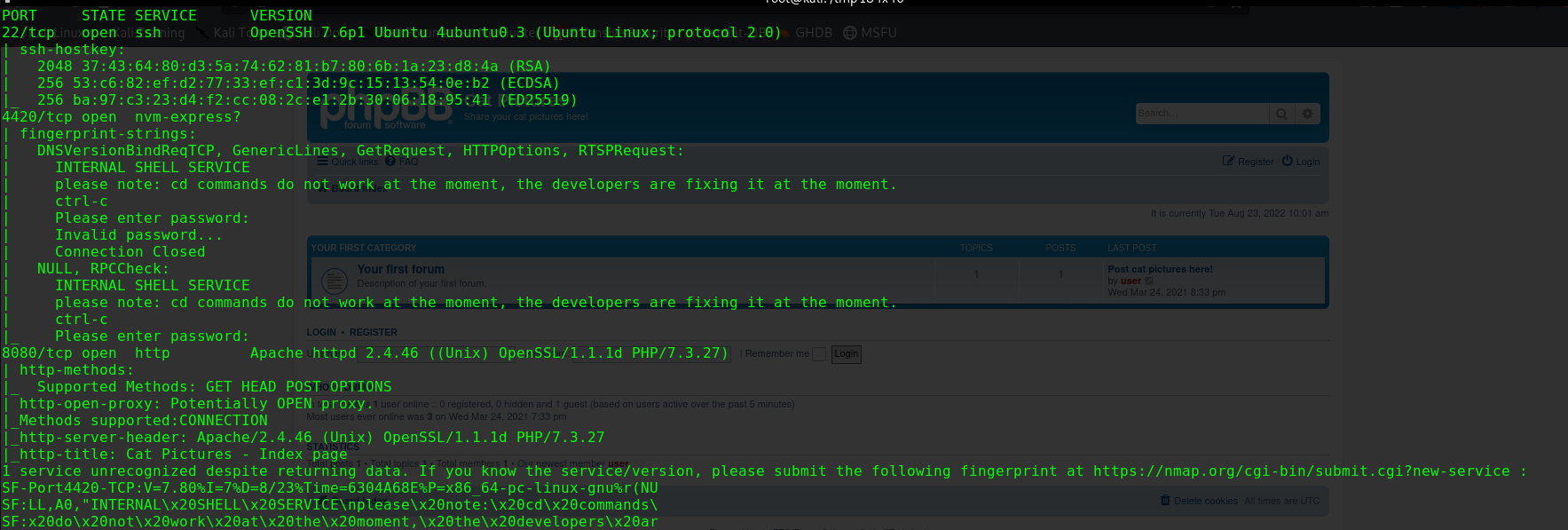
1. Dò quét

rustscan -b 500 -a 10.10.104.30

A picture containing text, clock, green, clock radio

Description automatically generated

Hay rồi đây. Có port 4420 khá là lạ.



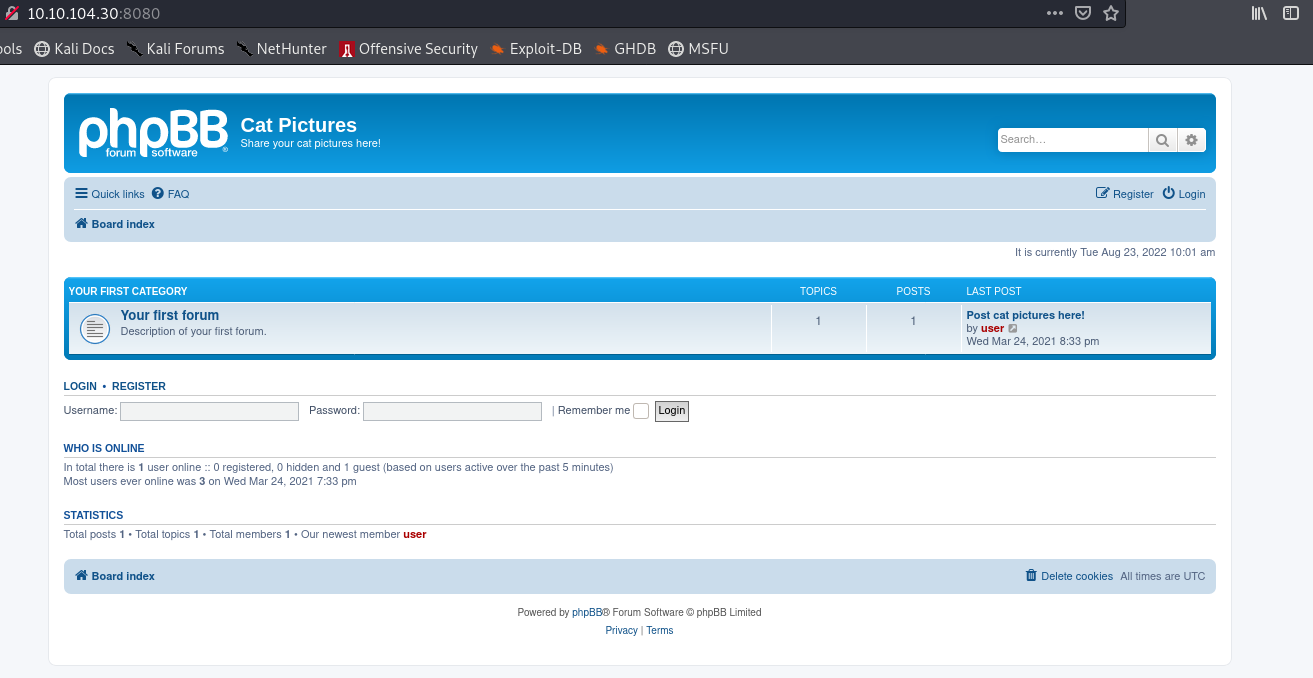
1. Enum

Ở port 4420, hệ thống yêu cầu nhập đúng password, nhìn qua thì khá giống 1 số bài liên quan đến buffer overflow mà trc đây mk đã làm. Thử 1 số password xem có đc ko mà …=))

A screenshot of a computer

Description automatically generated with medium confidence

Ở port 8080 thì họ dùng CMS là phpBB chưa rõ version.



Đến đây thì mk đoán khả năng là ở phpBB này có 1 lỗi nghiêm trọng nào đó mà chúng ta có thể RCE, nên mk research khá là kỹ.

Graphical user interface, application, Word

Description automatically generated

Khá là vui vì phán đoán của mk đã đúng.

Graphical user interface, application

Description automatically generated

Theo hướng dẫn ở trong video thì cần có user/pass để xác thực. Hmm, lại khó rồi đây. Mk thử 1 số creds mặc định mà đều chưa đc. Loay hoay 1 thời gian mà chưa có kết quả => nghỉ ngơi chút để bình tĩnh lại. Sau khi thư giãn 1 chút, mk soát lại xem có bỏ mất điều gì ko thì mới phát hiện ra nó =))

Rectangle

Description automatically generated with low confidence

Port knock mn ạ.

Text

Description automatically generated

1. Exploitation

Sau khi đã “knock” thì port 21 đã xuất hiện. Với ftp thì cứ test “anonymous login” thôi

Text

Description automatically generated

Đã có password cho port 4420 là “sardinethecat”

Graphical user interface, application

Description automatically generated

Sau khi enum chúng ta biết đc user là “catlover”, có 1 file thực thi là “runme” ở folder “/home/catlover” và chúng ta có thể dùng đc 1 số lệnh như: bash, cat, echo, ls, rm,sh, nc. Mk quyết định tải file “runme” về xem nó có nội dung là gì.

Graphical user interface, text, application

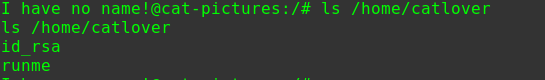
Description automatically generated

Mk sử dụng công cụ ghidra để reverse. Như mn thấy ở đây thì runme sẽ yêu cầu chúng ta nhập password, nếu đúng thì nó sẽ tạo 1 file /tmp/gibmethesshkey (kn là private key ssh cho user catlover). Nhìn đoạn code trên biết đc ngay password chính là “rebecca”. Chạy file để lấy key thôi.

Graphical user interface, text, chat or text message

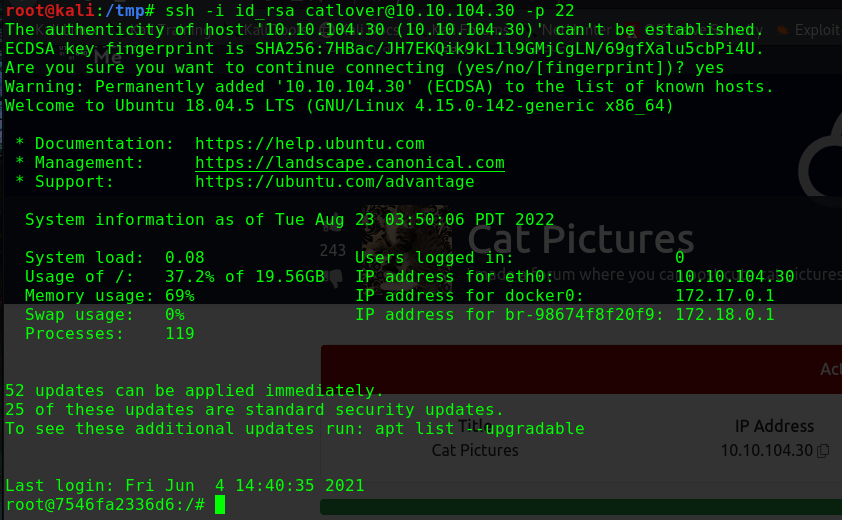
Description automatically generated

Hmm file rỗng, lừa thực sự.



Mà key nó lại nằm ở “/home/catlover”. “Chú giấu kỹ quá, chẳng ai biết gì cả”

1. Leo thang đặc quyền



User root luôn ạ. Lạ thật đấy

Graphical user interface, application

Description automatically generated

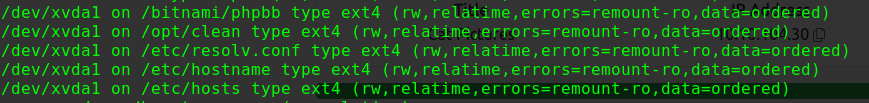
Container rồi mn (.dockerenv là thứ cho chúng ta biết điều đó)

Từ “.bash\_history” chúng ta có thêm manh mối “/opt/clean/clean.sh”

Graphical user interface, application

Description automatically generated

Kết hợp với lệnh “mount” thì chúng ta thấy rằng có file/folder đã được mount tới “/opt/clean” trên container



Và khi đọc file “clean.sh” => Mk kết luận được rằng: đây là 1 file schedule của host được mount tới container.

A screenshot of a computer

Description automatically generated with low confidence

Sửa lại file clean.sh để lấy shell trên host thôi.

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

Đợi 1 lúc thì lấy được shell user root của host.

Đến đây là kết thúc rồi. Xin chào mn.