Graphical user interface, text

Description automatically generated

Hôm nay mk trở lại với bài “Gaming Server”. Bài này cũng khá đơn giản. Bắt đầu thôi!

1. Dò quét

rustscan -b 500 -a 10.10.43.101

A screenshot of a computer

Description automatically generated with low confidence

Vẫn là 2 cổng quen thuộc là 22 và 80. Xem chi tiết hơn

nmap -p 22,80 -sC -sV -v 10.10.43.101 -Pn -T4

Graphical user interface, text

Description automatically generated

2. Enum

A picture containing text, book

Description automatically generated

Giao diện khá đẹp. View page source xem có gì ko. 

Ngoài thông tin về user “john” chúng ta tìm được 1 vài page khác như: about.html, myths.html, archives.html. Ở page “about.html” mk tìm được chỗ khá thú vị

A black screen with white text

Description automatically generated with low confidence

Khi bấm vào nó sẽ dẫn chúng ta tới thư mục “uploads”.

Graphical user interface, text, application, email

Description automatically generated

Table

Description automatically generated

File “dict.lst” giống như là 1 list các password. Mk nhớ lại user “john” ở trên, nên tiến hành brute force ssh.

A screenshot of a map

Description automatically generated with medium confidence

Ko thành công rồi. Khả năng là dùng cho login trên web. Mk tìm xem có file/folder ẩn ko.

Text

Description automatically generated

Text

Description automatically generated“secret” chính là nó. Trong thư mục này chúng ta sẽ tìm được id\_rsa và khả năng nó là của user “john”.

A screenshot of a computer

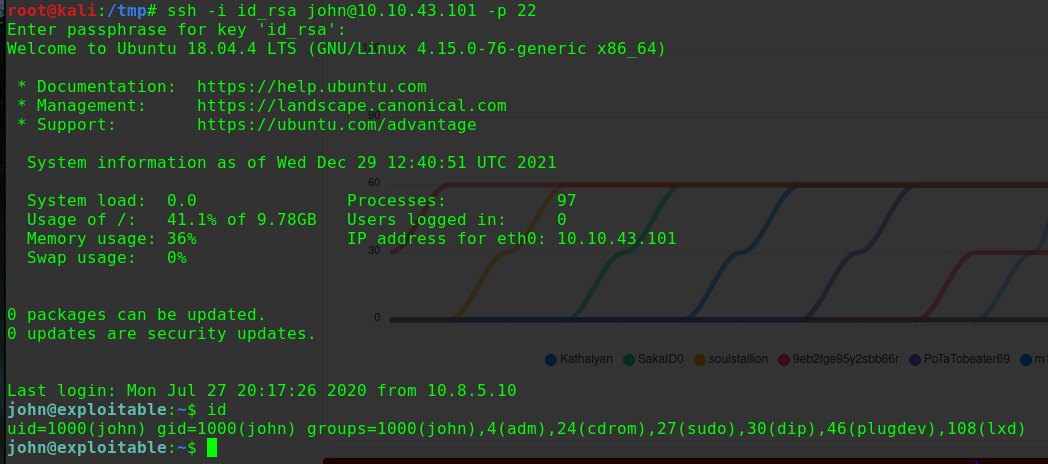
Description automatically generated with medium confidence

Ở đây nó yêu cầu passphrase nên phải crack rồi.

Text

Description automatically generated

“letmein” là passphrase chúng ta tìm được.



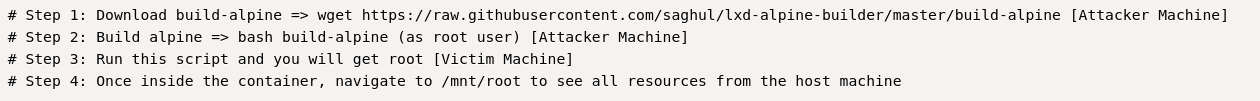
3. Leo thang đặc quyền

Lxd group chúng ta sẽ tìm được lỗi cho phép chúng ta chiếm được quyền root

Graphical user interface, text, application

Description automatically generated

Trong đoạn mã, thì tác giả có hướng dẫn cụ thể các bước, đơn giản là làm theo thôi!



Text

Description automatically generated

Thành công, chúng ta đã có được quyền root trên hệ thống.