Graphical user interface, text, application

Description automatically generated

Với màn come back lần này thì hn mk sẽ tiếp tục với 1 bài vừa mới đc “ra mắt” trên Tryhackme là Gallery. Bắt đầu thôi

1. Dò quét

nmap -p- -T4 -v 10.10.133.233 -Pn

A picture containing text, clock, green

Description automatically generated

2 port đang mở là 80 là 8080

1. Enum

Graphical user interface, text, email

Description automatically generated

Graphical user interface, application, chat or text message

Description automatically generated

Đây là nội dung ở 2 port 80 và 8080 khi chúng ta truy cập thông qua browser. Đập vào mắt đương nhiên là dòng chữ “Simple Image Gallery System” và mk đã quyết định research xem cụ thể nó là cái gì với từ khóa mk tra là “Simple Image Gallery System exploit”

Graphical user interface, application

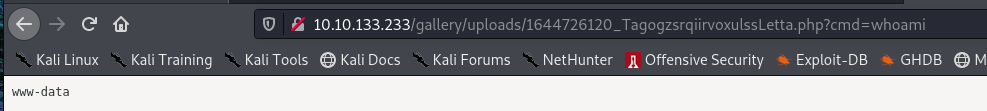
Description automatically generated

RCE cực kỳ ngon =)). Lấy đoạn mã khai thác về để tiến hành xâm nhập

Graphical user interface, text

Description automatically generated

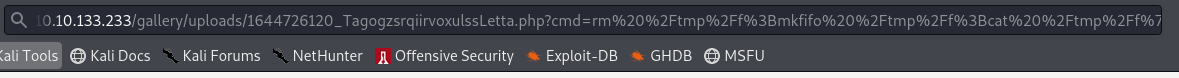
Thành công và chúng ta hãy xem kết quả



Đương nhiên rồi đến đây phải làm nhiệm vụ tiếp theo là lấy shell. Các bước thì vẫn như các bài writeup trc mk viết.

Text

Description automatically generated



Nhớ phải encode đoạn mã. Và đây là kết quả

Text

Description automatically generated

1. Leo thang

Sau 1 hồi lần mò code trong thư mục /var/www/html/gallery thì mk tìm được cả hash và password.

Graphical user interface, text

Description automatically generated

Tưởng sd được ai ngờ hash thì ko crack được còn password thì chỉ dùng để đăng nhập vào mysql. Sau 1 hồi loay hoay đủ các thứ như sudo permission, SUID, cronjob, kernel,…. nhưng đều ko có gì. Cái hay ho mk tìm đc đó là file rootkit.sh ở thư mục /opt nhưng file này với user www-data thì chỉ đọc được thui ko sửa hay run được.

Text

Description automatically generated

Haizz bí quá cuối cùng mk phải dùng đến biện pháp cuối cùng đó là “linpeas.sh” =)).

A picture containing text

Description automatically generated

Với linpeas chúng ta tìm được thư mục rất đáng nghi ngờ là /var/backups/mike\_home\_backup

A screenshot of a computer

Description automatically generated with medium confidence

Rất nhanh chóng mk đã tìm được password của user mike

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

Hóa ra file rootkit.sh tìm được ở trên là dành cho mike. Nd file này mk đã chụp ở trên, trong đó thì có 2 điểm mà chúng ta cần chú ý ở trong code là “rkhunter” và “nano”. Thì với rkhunter thì mk đã tra cứu nhưng ko tìm đc cái nào. Còn với nano thì cũng khá quen thuộc rồi <https://gtfobins.github.io/gtfobins/nano/>

Graphical user interface, text, application

Description automatically generated

Sudo -u root /bin/bash /opt/rootkit.sh

* Nhập “read”



Ở trong giao diện của trình soạn thảo Nano:

* Ctrl + R
* Ctrl + X
* reset; sh 1>&0 2>&0

Graphical user interface, text

Description automatically generated

Thành công. Nhiệm vụ hoàn thành.