Graphical user interface, text, application

Description automatically generated

Hôm nay mk sẽ làm bài KoTH Food CTF này. Bắt đầu thôi.

1. Dò quét

rustscan -b 500 -a 10.10.169.66

Text

Description automatically generated

Quét chi tiết hơn để xem cụ thể là dịch vụ gì.

nmap -sC -sV -v -p 22,3306,9999,15065,16109,46969 10.10.169.66 -Pn

Text

Description automatically generated

Text

Description automatically generated

Thì với những port như thế này thì mk triển khai từ port 46969 – Telnet

2. Khai thác

Text

Description automatically generated

Thông tin đăng nhập đây rồi -> tccr:uwjsasqccywsg. Nhìn khá giống rot13. Decode thử xem có gì ko.

Graphical user interface, application

Description automatically generated

Đăng nhập với user/pass này food:givemecookies.

Text

Description automatically generated

Thành công. Sau 1 hồi enum mà ko thấy gì. Mk chuyển qua port chạy http là 15065 xem có gì ko

Graphical user interface, text, application

Description automatically generated

-> Tìm thư mục ẩn

Text

Description automatically generated

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

Description automatically generated

Nhìn khá giống CMD injection. Thế này thì test thử thôi

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

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Ko đc rồi. Ko biết làm sao. Hmm bật thử Burpsuite để test

Graphical user interface, text, application, email

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Với cách này lại thành công. Ko hiểu kiểu gì 😊. Thôi kệ đi =))

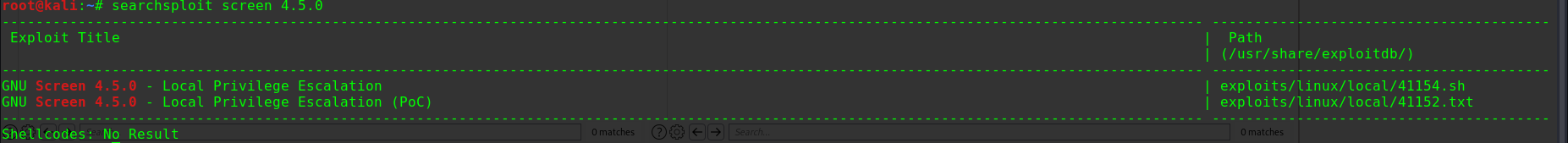
3. Leo thang đặc quyền

Bình thường mk hay bắt đầu bằng việc tìm các tệp SUID

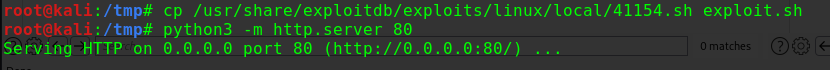
Text

Description automatically generated

/usr/bin/screen-4.5.0 nhìn khá lạ. Mk nhớ là có mã khai thác của cái này. Research thôi.



Transfer file sang máy của target



Tải file về máy victim

Text

Description automatically generated

Chạy mã khai thác: bash exploit.sh

Text

Description automatically generated

Thành công. Nhiệm vụ hoàn thành!!