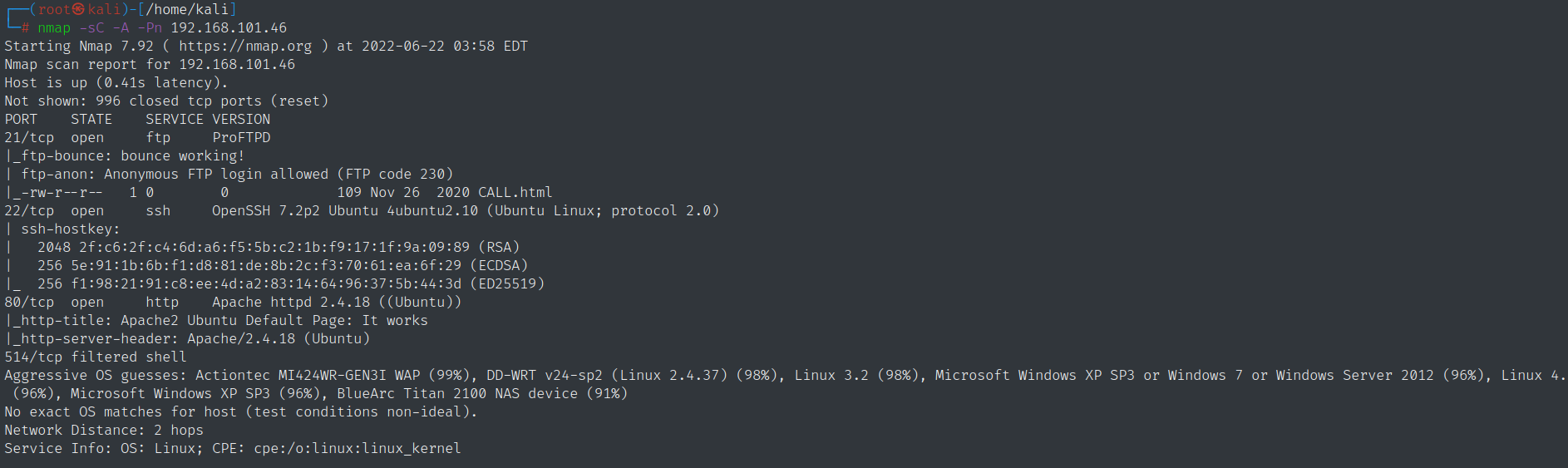
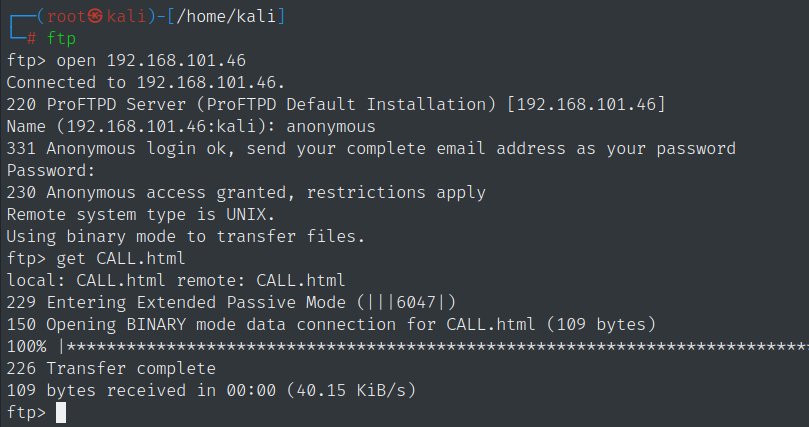
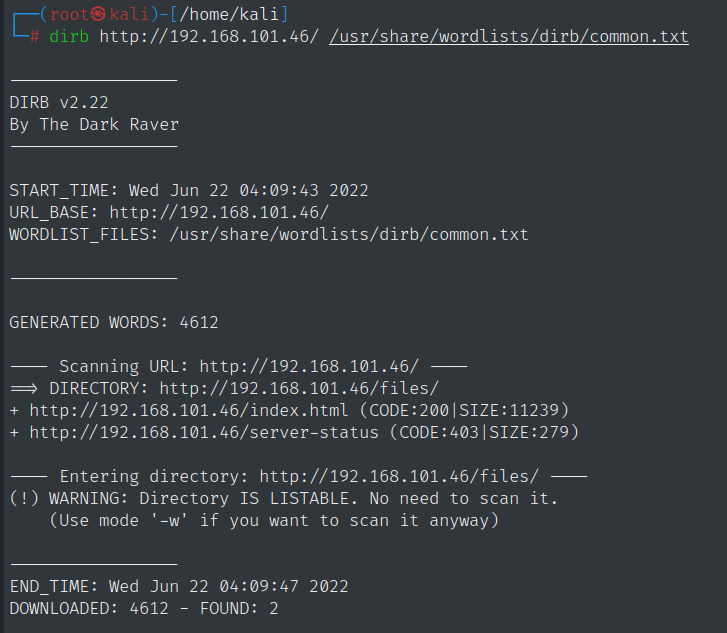
Step1: nmap



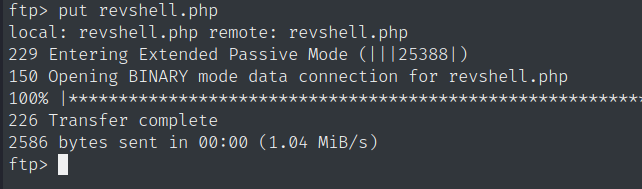
Nhận thấy có file CALL.html

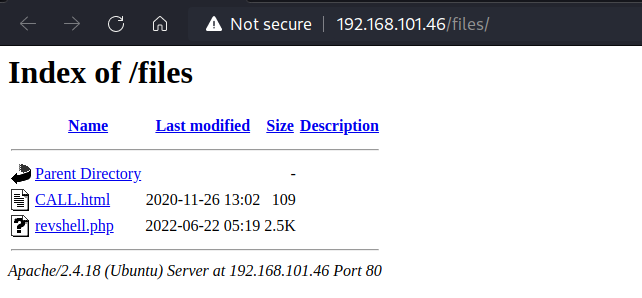


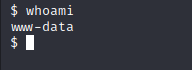
Step2: enumration web

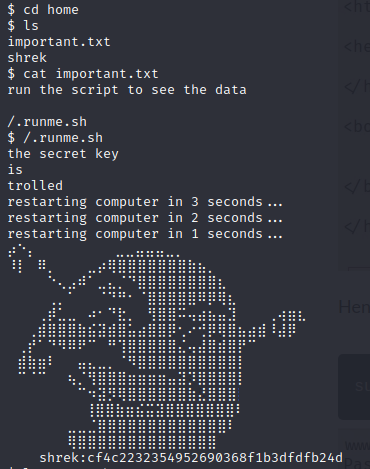


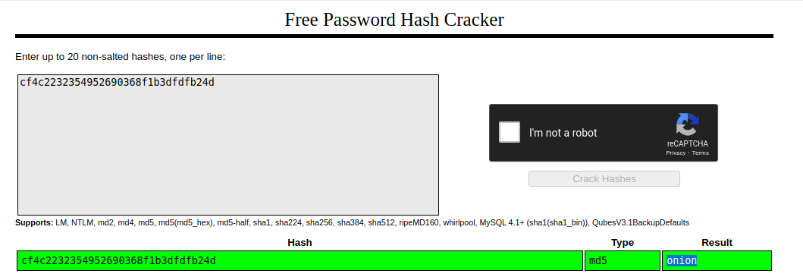
Vao <http://192.168.101.46/files/> thu xem . thay co file CALL.html co lien quan toi ftp chang? Gio tai 1 doan reverseshell up len ftp xem thu < shell nay minh lay tren revshell>

sau khi put, vao link xem lai ta da thay co file revshell.php

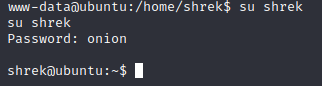


Sau do tai terminal: go nc -lvnp 9001 , o web click vao file revshell.php. Da dang nhap thanh cong . Tiep tuc

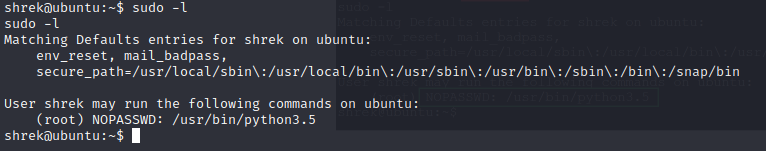
shrek:cf4c2232354952690368f1b3dfdfb24d

Crack mat khau cua shrek ta duoc onion 

Sau do locate python, thay trong may co python3, tiep tuc

python3 -c 'import pty;pty.spawn("/bin/bash")' ,

sudo –l thay

.

Bay gio se dung python de leo len root

sudo python3.5 -c 'import os; os.system("/bin/sh")'. Yah, da len duoc root