Projekt 2: Omijanie zabezpieczeń - Andrzej, Dawid, Jacek, Jakub, Jan

Projekt 2: Omijanie zabezpieczeń - Andrzej, Dawid, Jacek, Jakub, Jan

Zadanie 1 - Łamanie haseł: Dla podanych hashy określ typ wykorzystanego algorytmu hashującego, a następnie złam hasło metodą brute-force.

- [x] 1.1:

```
Cd workspace/

Touch hash.txt

Nano hash.txt copy hash

└─$ hashcat -m0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
```

```
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

81dc9bdb52d04dc20036dbd8313ed055:1234

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 81dc9bdb52d04dc20036dbd8313ed055
Time.Started.....: Sun Feb 19 03:26:49 2023 (0 secs)
Time.Estimated...: Sun Feb 19 03:26:49 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   917.1 kH/s (0.23ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2048/14344385 (0.01%)
Rejected.........: 0/2048 (0.00%)
Restore.Point....: 1024/14344385 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: kucing → lovers1
Hardware.Mon.#1..: Util: 24%

Started: Sun Feb 19 03:26:47 2023
Stopped: Sun Feb 19 03:26:51 2023
```

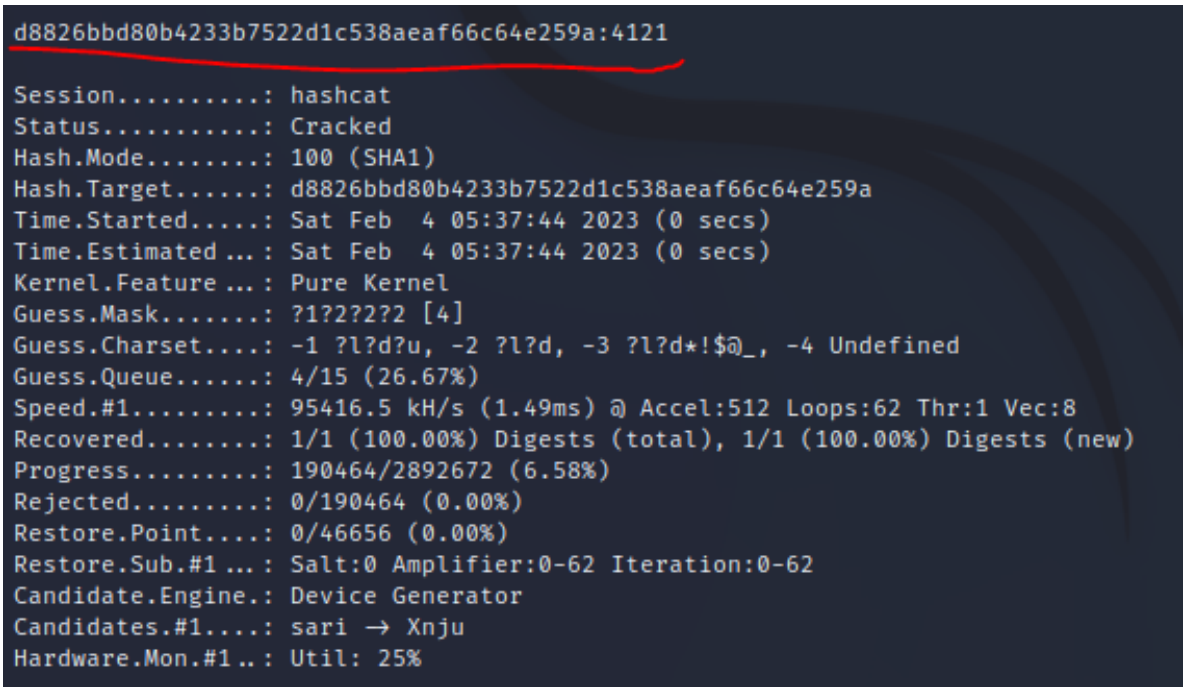
- [x] 1.2:

Hash

`hash-identifier`

d8826bbd80b4233b7522d1c538aeaf66c64e259a

rezulatat

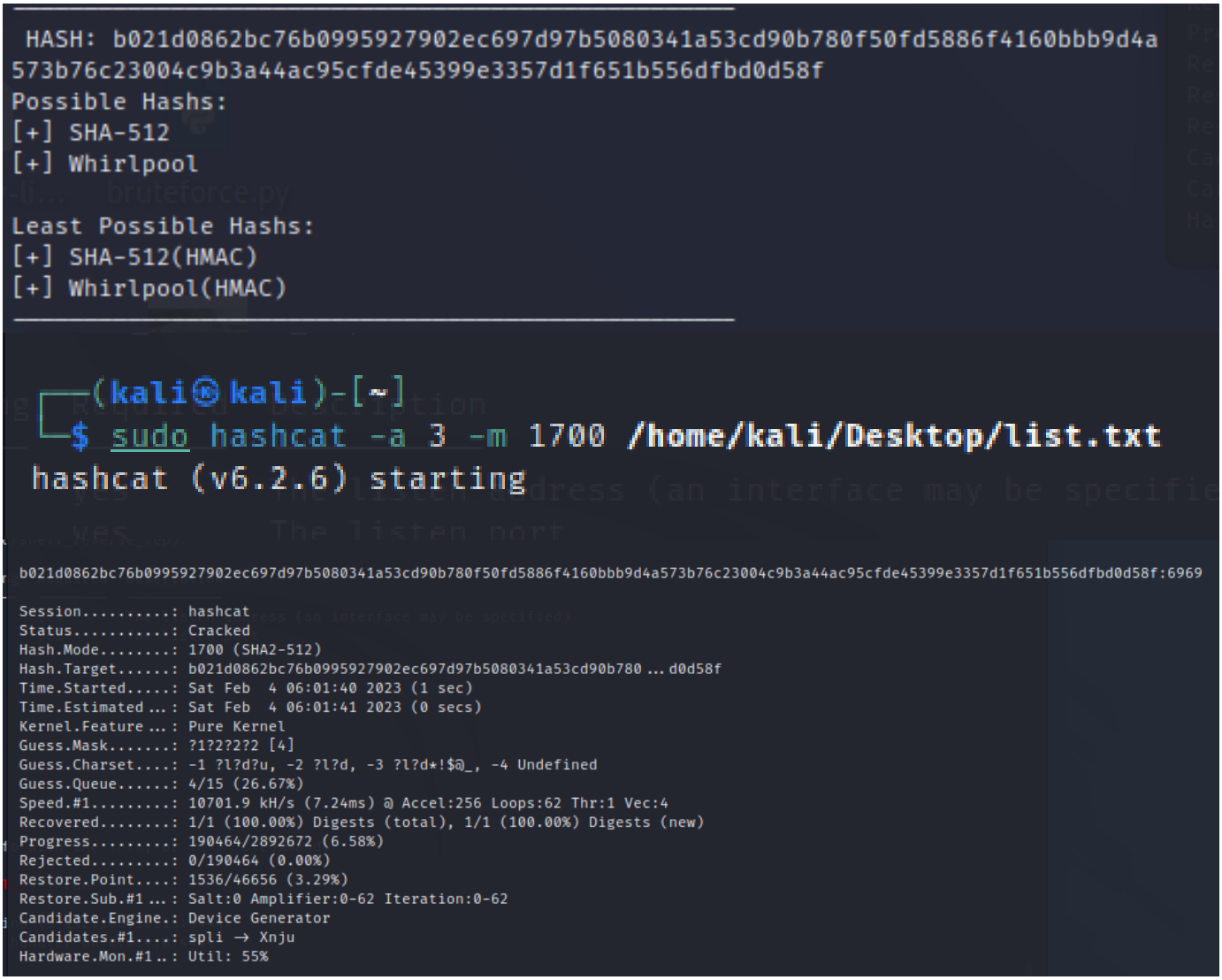


- [x] 1.3:

Hash

b021d0862bc76b0995927902ec697d97b5080341a53cd90b780f50fd5886f4160bbb9d4a573b76c23004c9b3a44ac95cfde45399e3357d1f651b556dfbd0d58f

`hash-identifier`



- [x] 1.4:

Hash

`hash-identifier`

31bca02094eb78126a517b206a88c73cfa9ec6f704c7030d18212cace820f025f00bf0ea68dbf3f3a5436ca63b53bf7bf80ad8d5de7d8359d0b7fed9dbc3ab99

Rezultat:

`hashcat -m 1700 -a 0 hash.txt /usr/share/wordlists/rockyou.txt`

Rezulatat

```
31bca02094eb78126a517b206a88c73cfa9ec6f704c7030d18212cace820f025f00bf0ea68dbf3f3a5436ca63b53bf7bf80ad8d5de7d8359d0b7fed9dbc3ab99:0

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1700 (SHA2-512)
Hash.Target......: 31bca02094eb78126a517b206a88c73cfa9ec6f704c7030d182 ... c3ab99
Time.Started.....: Sat Feb  4 06:13:26 2023 (0 secs)
Time.Estimated ...: Sat Feb  4 06:13:26 2023 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Mask.......: ?1 [1]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 1/15 (6.67%)
Speed.#1.........:   194.7 kH/s (0.03ms) @ Accel:256 Loops:62 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 62/62 (100.00%)
Rejected.........: 0/62 (0.00%)
Restore.Point....: 0/1 (0.00%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-62 Iteration:0-62
Candidate.Engine.: Device Generator
Candidates.#1....: s → X
Hardware.Mon.#1..: Util: 19%

Started: Sat Feb  4 06:13:25 2023
Stopped: Sat Feb  4 06:13:28 2023
```

- [x] **Zadanie 2/3** : Dla podanych hashy określ typ wykorzystanego algorytmu hashującego, a następnie złam hasło metodą brute-force.

`hash-identifier`

9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f51721e2042d9067dcb120accc5741
05b43139b6c9c887dda8202eff20cc4b98bad7b3be1e471b3aa5

```
 HASH: 9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f51721e2042d9067dcb120accc574105b43139b6c9c887dda8202eff20cc4b98bad7b3be1e471b3aa5

Possible Hashs:
[+] SHA-512
[+] Whirlpool

Least Possible Hashs:
[+] SHA-512(HMAC)
[+] Whirlpool(HMAC)

 HASH:
```

Rezulatat :

```
9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f51721e2042d9067dcb120accc574105b43139b6c9c887dda8202eff20cc4b98bad7b3be1e471b3aa5:sda

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1700 (SHA2-512)
Hash.Target......: 9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f5172 ... 1b3aa5
Time.Started.....: Sat Feb  4 06:24:37 2023 (0 secs)
Time.Estimated ...: Sat Feb  4 06:24:37 2023 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Mask.......: ?1?2?2 [3]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 3/15 (20.00%)
Speed.#1.........: 13895.5 kH/s (5.41ms) @ Accel:256 Loops:62 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 80352/80352 (100.00%)
Rejected.........: 0/80352 (0.00%)
Restore.Point....: 0/1296 (0.00%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-62 Iteration:0-62
Candidate.Engine.: Device Generator
Candidates.#1....: sar → Xqx
Hardware.Mon.#1..: Util: 51%
```

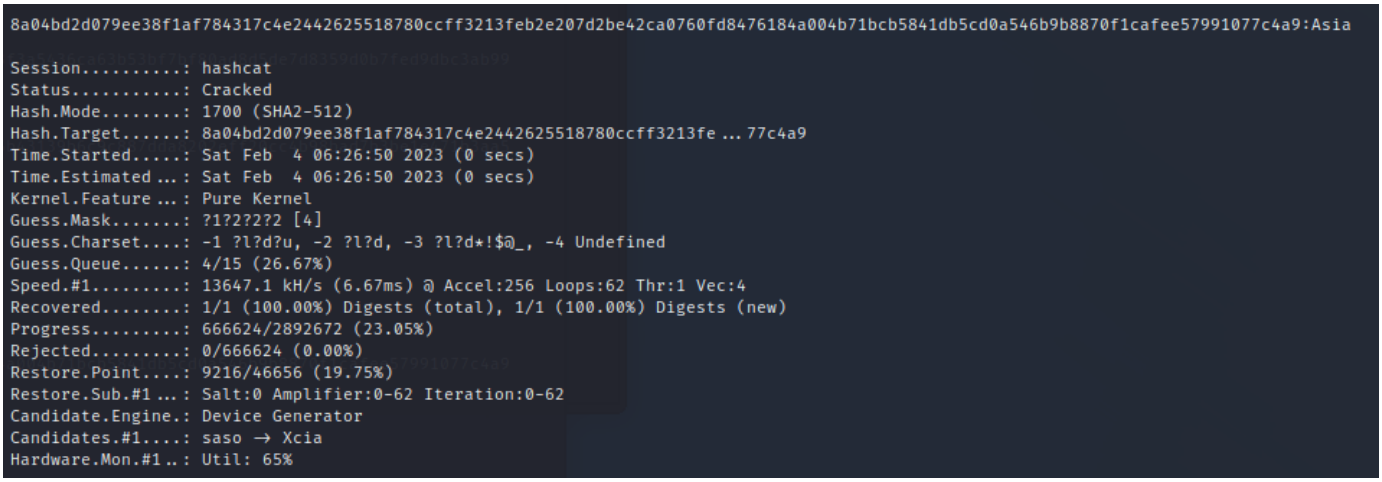
`Hash-identifier`

8a04bd2d079ee38f1af784317c4e2442625518780ccff3213feb2e207d2be42ca0760fd847618

4a004b71bcb5841db5cd0a546b9b8870f1cafee57991077c4a9

Rezultat:

Rezultat:



- [x] **Zadanie 1 3/3**: Dla podanych hashy określ typ wykorzystanego algorytmu hashującego, a następnie złam hasło metodą brute-force.

`Hash-identifier`

44d9886c0a57ddbfdb31aa936bd498bf2ab70f741ee47047851e768db953fc4e43f92be953
e205a3d1b3ab752ed90379444b651b582b0bc209a739a624e109da

Rezulatat:

```
 HASH: 44d9886c0a57ddbfdb31aa936bd498bf2ab70f741ee47047851e768db953fc4e43f92be953
e205a3d1b3ab752ed90379444b651b582b0bc209a739a624e109da
Possible Hashs:
[+] SHA-512
[+] Whirlpool

Least Possible Hashs:
[+] SHA-512(HMAC)
[+] Whirlpool(HMAC)
--------------------------------------------------
 HASH:
```

```
┌──(kali㉿kali)-[~/workspace]
└─$ hashcat -m 1700 -a 0 -d 2 hash2.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

- [x] **Zadanie 2**: Dla podanych hashy określ typ wykorzystanego algorytmu hashującego, a następnie złam hasło metodą słownikową.

`Hash-identifier:`

9fd8301ac24fb88e65d9d7cd1dd1b1ec

7f9a6871b86f40c330132c4fc42cda59

6104df369888589d6dbea304b59a32d4

276f8db0b86edaa7fc805516c852c889

04dac8afe0ca501587bad66f6b5ce5ad

Rezultat:

```
--------------------------------------------------
 HASH: 9fd8301ac24fb88e65d9d7cd1dd1b1ec

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
```

Wszystkie hashe MD5

`hashcat -m0 -a 0 hash.txt /usr/share/wordlists/rockyou-50.txt`

Rezultat:

```
04dac8afe0ca501587bad66f6b5ce5ad:hellokitty
9fd8301ac24fb88e65d9d7cd1dd1b1ec:butterfly
7f9a6871b86f40c330132c4fc42cda59:tinkerbell
6104df369888589d6dbea304b59a32d4:blink182
276f8db0b86edaa7fc805516c852c889:baseball

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: /home/kali/Desktop/list.txt
Time.Started.....: Sat Feb  4 08:01:31 2023 (0 secs)
Time.Estimated...: Sat Feb  4 08:01:31 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/kali/Desktop/wordlist.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    79514 H/s (0.15ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 5/5 (100.00%) Digests (total), 5/5 (100.00%) Digests (new)
Progress.........: 3072/9437 (32.55%)
Rejected.........: 0/3072 (0.00%)
Restore.Point....: 0/9437 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> ANTHONY
Hardware.Mon.#1..: Util: 10%
```

- [x] **Zadanie 2/2 - Łamanie haseł** : Dla podanych hashy określ typ wykorzystanego algorytmu hashującego, a następnie złam hasło metodą słownikową.

Hash:

`Hash-identifier`

7ab68889355673863760 37e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4 e70f6df0e04d1a69d8e7101d881379cf1966c992100389da7f3e9a

470c62e301c771f12d91a242efbd41c5e467cba7419c664f784dbc8a20820abaf6ed43e09b0c da994824f14425 db3e6d525a7aafa5d093a6a5f6bf7e3ec25dfa

```
 HASH: 7ab68889355673863760 37e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0e04d1a69d8e7101d881379cf1966c992100389
da7f3e9a

Possible Hashs:
[+] SHA-512
[+] Whirlpool

Least Possible Hashs:
[+] SHA-512(HMAC)
```

`hashcat -m 1700 -a 0 hash.txt /usr/share/wordlists/rockyou-50.txt`

```
7ab688893556738637 6e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0e04d1a69d8e7101d881379cf1966c992100389da7f3e9a:spiderma
n
470c62e301c771f12d91a242efbd41c5e467cba7419c664f784dbc8a20820abaf6ed43e09b0cda994824f14425db3e6d525a7aafa5d093a6a5f6bf7e3ec25dfa:rockstar

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1700 (SHA2-512)
Hash.Target......: /home/kali/Desktop/list.txt
Time.Started.....: Sat Feb  4 08:04:18 2023 (0 secs)
Time.Estimated...: Sat Feb  4 08:04:18 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/kali/Desktop/wordlist.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  3174.1 kH/s (0.38ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 2/2 (100.00%) Digests (total), 2/2 (100.00%) Digests (new)
Progress.........: 3072/9437 (32.55%)
Rejected.........: 0/3072 (0.00%)
Restore.Point....: 0/9437 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 → ANTHONY
Hardware.Mon.#1..: Util: 12%
```

☑ Zadanie 3 - Analiza ruchu HTTP

1. Rozpocznij monitorowanie ruchu sieciowego (narzędziem Wireshark).
2. W przeglądarce nawiąż połączenie z http://testphp.vulnweb.com/login.php
3. Wykonaj próbę logowania (dowolne dane).
4. Odszukaj w zapisanym ruchu swoje dane logowania.

Zadanie 4: - Analiza ruchu SSH

1. Rozpocznij monitorowanie ruchu sieciowego (narzędziem Wireshark).
2. Nawiąż połączenie pomiędzy Kalim a SDA po SSH.
3. Stwórz pliki sekret1.txt i sekret2.txt z tajnymi hasłami.
4. Edytuj konfigurację vsFTPd, żeby umożliwić wgrywanie plików po FTP.

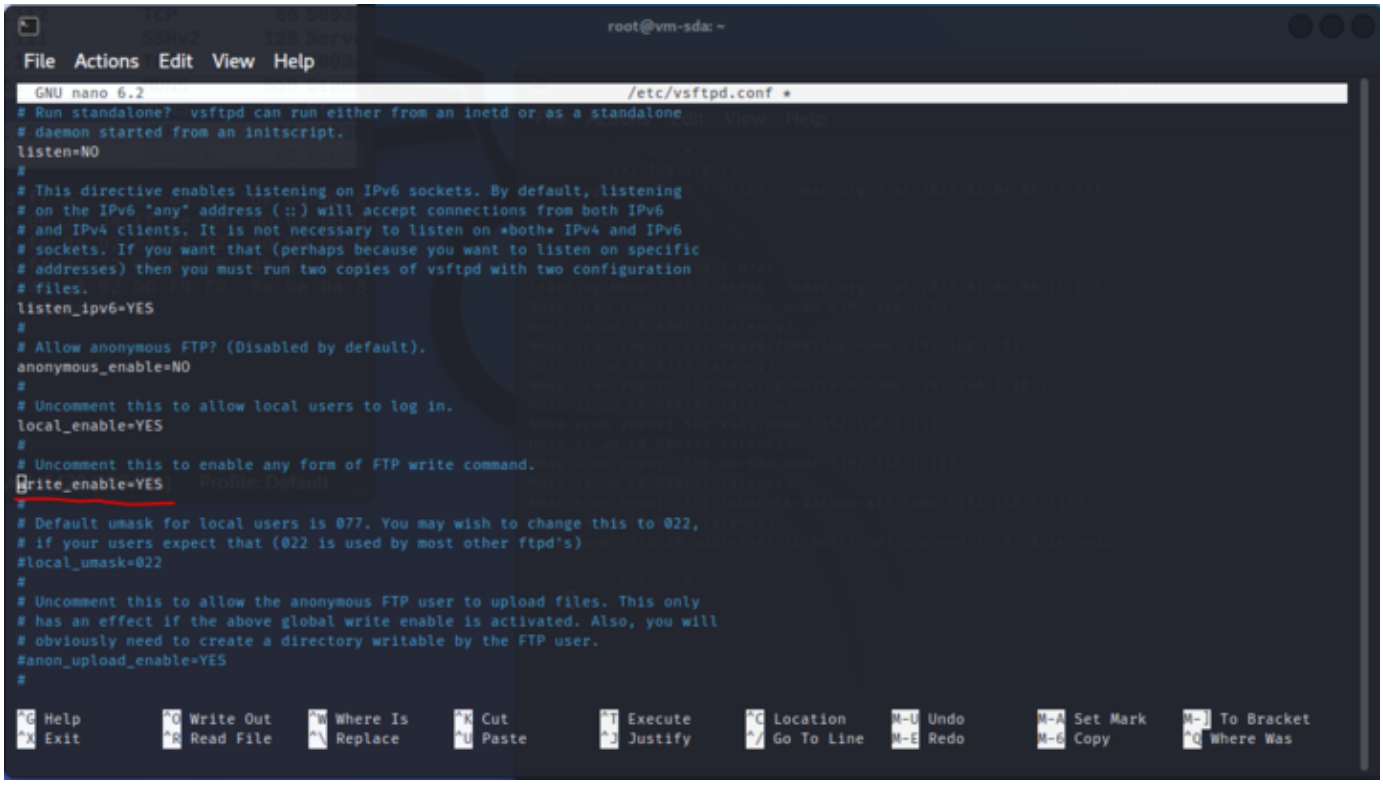
5. Zakończ połączenie po SSH.
6. Spróbuj poszukać w zapisanym ruchu sieciowym zawartość plików sekret1.txt i sekret2.txt

Terminal:

```
ssh root@$IP

touch sekret1.txt

echo ‘tajnehaslo ‘ > sekret1.txt

touch sekret2.txt

echo ‘tajnehaslo2’ > sekret2.txt
```

```
Last login: Tue Dec 20 21:27:20 2022
root@vm-sda:~# ls
root.txt  snap
root@vm-sda:~# touch sekret1.txt
root@vm-sda:~# echo 'tajne1' > sekret1.txt
root@vm-sda:~# touch sekret2.txt
root@vm-sda:~# echo 'tajne2' > sekret2.txt
root@vm-sda:~# ls
root.txt  sekret1.txt  sekret2.txt  snap
root@vm-sda:~# sudo nano /etc/vsftpd.conf
root@vm-sda:~#
```

`Sudo nano /etc/vsftpd.conf`



Zapisujemy

Gotowe

Spróbuj poszukać w zapisanym ruchu sieciowym zawartość plików sekret1.txt i sekret2.

☑ Zadanie 5 - Analiza ruchu FTP.

```
[ftp://root:666@$IP](ftp://root:666@$IP)

mget dowolnyplik.txt

get sekret1.txt
```

```
get sekret2.txt
```