

# 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.

✓ 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
```

✓ 1.2:

Hash

hash-identifier

d8826bbd80b4233b7522d1c538aeaf66c64e259a

```
(kali@kali)-[~]  
$ sudo hashcat -a 3 -m 100 /home/kali/Desktop/list.txt  
hashcat (v6.2.6) starting
```

rezultat

```
d8826bbd80b4233b7522d1c538aeaf66c64e259a:4121  
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode.....: 100 (SHA1)  
Hash.Target.....: d8826bbd80b4233b7522d1c538aeaf66c64e259a  
Time.Started.....: Sat Feb  4 05:37:44 2023 (0 secs)  
Time.Estimated...: Sat Feb  4 05:37:44 2023 (0 secs)  
Kernel.Feature...: Pure Kernel  
Guess.Mask.....: ?1?2?2?2 [4]  
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined  
Guess.Queue.....: 4/15 (26.67%)  
Speed.#1.....: 95416.5 kH/s (1.49ms) @ Accel:512 Loops:62 Thr:1 Vec:8  
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)  
Progress.....: 190464/2892672 (6.58%)  
Rejected.....: 0/190464 (0.00%)  
Restore.Point....: 0/46656 (0.00%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-62 Iteration:0-62  
Candidate.Engine.: Device Generator  
Candidates.#1....: sari → Xnju  
Hardware.Mon.#1..: Util: 25%
```

✓ 1.3:

Hash

b021d0862bc76b0995927902ec697d97b5080341a53cd90b780f50fd5886f4160bbb9d4a573b76c23004  
c9b3a44ac95cfde45399e3357d1f651b556dfbd0d58f

hash-identifier

```
HASH: b021d0862bc76b0995927902ec697d97b5080341a53cd90b780f50fd5886f4160bbb9d4a573b76c23004c9b3a44ac95cfde45399e3357d1f651b556dfbd0d58f
```

Possible Hashs:

[+] SHA-512

[+] Whirlpool

Least Possible Hashs:

[+] SHA-512(HMAC)

[+] Whirlpool(HMAC)

```
(kali@kali)-[~]
```

```
$ sudo hashcat -a 3 -m 1700 /home/kali/Desktop/list.txt
```

```
hashcat (v6.2.6) starting
```

```
b021d0862bc76b0995927902ec697d97b5080341a53cd90b780f50fd5886f4160bbb9d4a573b76c23004c9b3a44ac95cfde45399e3357d1f651b556dfbd0d58f:6969
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1700 (SHA2-512)
Hash.Target.....: b021d0862bc76b0995927902ec697d97b5080341a53cd90b780 ... d0d58f
Time.Started.....: Sat Feb  4 06:01:40 2023 (1 sec)
Time.Estimated...: Sat Feb  4 06:01:41 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?1?2?2?2 [4]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 4/15 (26.67%)
Speed.#1.....: 10701.9 kH/s (7.24ms) @ Accel:256 Loops:62 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 190464/2892672 (6.58%)
Rejected.....: 0/190464 (0.00%)
Restore.Point....: 1536/46656 (3.29%)
Restore.Sub.#1...: Salt:0 Amplifier:0-62 Iteration:0-62
Candidate.Engine.: Device Generator
Candidates.#1....: spli -> Xnju
Hardware.Mon.#1..: Util: 55%
```

✓ 1.4:

Hash

```
hash-identifier
```

```
31bca02094eb78126a517b206a88c73cfa9ec6f704c7030d18212cace820f025f00bf0ea68dbf3f3a5436c
a63b53bf7bf80ad8d5de7d8359d0b7fed9dbc3ab99
```

Rezultat:

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

Rezultat

```

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

```

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

hash-identifier

9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f51721e2042d9067dcb120accc574105b43139b6c9c887dda8202eff20cc4b98bad7b3be1e471b3aa5

```

HASH: 9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f51721e2042d9067dcb120accc574105b43139b6c9c887dda8202eff20cc4b98bad7b3be1e471b3aa5

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

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

HASH: 

```

Rezultat :

```

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:

```
HASH: 8a04bd2d079ee38f1af784317c4e2442625518780ccff3213feb2e207d2be42ca0760fd8476184a004b71bcb5841db5cd0a546b9b8870f1cafee57991077c4a9
Possible Hashs:
[+] SHA-512
[+] Whirlpool

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

(kali@kali)-[~]
$ sudo hashcat -a 3 -m 1700 /home/kali/Desktop/list.txt
hashcat (v6.2.6) starting
```

Rezultat:

```
8a04bd2d079ee38f1af784317c4e2442625518780ccff3213feb2e207d2be42ca0760fd8476184a004b71bcb5841db5cd0a546b9b8870f1cafee57991077c4a9:Asia
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1700 (SHA2-512)
Hash.Target.....: 8a04bd2d079ee38f1af784317c4e2442625518780ccff3213fe ... 77c4a9
Time.Started.....: Sat Feb  4 06:26:50 2023 (0 secs)
Time.Estimated...: Sat Feb  4 06:26:50 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?1?2?2?2 [4]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 4/15 (26.67%)
Speed.#1.....: 13647.1 kH/s (6.67ms) @ Accel:256 Loops:62 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 666624/2892672 (23.05%)
Rejected.....: 0/666624 (0.00%)
Restore.Point....: 9216/46656 (19.75%)
Restore.Sub.#1...: Salt:0 Amplifier:0-62 Iteration:0-62
Candidate.Engine.: Device Generator
Candidates.#1....: saso -> Xcia
Hardware.Mon.#1..: Util: 65%
```

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

Hash-identyfier

44d9886c0a57ddbdfdb31aa936bd498bf2ab70f741ee47047851e768db953fc4e43f92be953  
e205a3d1b3ab752ed90379444b651b582b0bc209a739a624e109da

Rezultat:

```
HASH: 44d9886c0a57ddbdfdb31aa936bd498bf2ab70f741ee47047851e768db953fc4e43f92be953
e205a3d1b3ab752ed90379444b651b582b0bc209a739a624e109da
Possible Hashs:
[+] SHA-512
[+] Whirlpool

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

```
HASH: █
```

```
(kali@kali)~$ hashcat -m 1700 -a 0 -d 2 hash2.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

- ☒ **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:tinkerbelle
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%
```

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

Hash:

```
Hash-identifier
```

```
7ab6888935567386376037e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0e04d1a69d8e7101d881379cf1966c992100389da7f3e9a
```

```
470c62e301c771f12d91a242efbd41c5e467cba7419c664f784dbc8a20820abaf6ed43e09b0cda994824f14425 db3e6d525a7aafa5d093a6a5f6bf7e3ec25dfa
```

```
HASH: 7ab6888935567386376037e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0e04d1a69d8e7101d881379cf1966c992100389da7f3e9a
* If you are connected but behind a firewall, check that Firefox has permission to access the Web.
Possible Hashs:
[+] SHA-512
[+] Whirlpool
Least Possible Hashs:
[+] SHA-512(HMAC)
```

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



```
7ab6888935567386376037e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0e04d1a69d8e7101d881379cf1966c992100389da7f3e9a: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.



Wireshark - Follow TCP Stream (tcp.stream eq 0) - eth0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.111	44.228.249.3	HTTP	418	GET /login.php HTTP/1.1
2	0.184437880	44.228.249.3	192.168.1.111	TCP	66	80 → 33962 [ACK] Seq=1 Ack=353 Win=483 Len=0 TSval=2638607497 TSecr=1361293286
3	0.185217190	44.228.249.3	192.168.1.111	TCP	1444	80 → 33962 [ACK] Seq=1 Ack=353 Win=483 Len=1378 TSval=2638607498 TSecr=1361293286 [TCP segment of a reassembled PDU]
4	0.185231587	192.168.1.111	44.228.249.3	TCP	66	33962 → 80 [ACK] Seq=353 Ack=1379 Win=501 Len=0 TSval=1361293471 TSecr=2638607498
5	0.185297169	44.228.249.3	192.168.1.111	HTTP	1430	HTTP/1.1 200 OK (text/html)
6	0.185403543	192.168.1.111	44.228.249.3	TCP	66	33962 → 80 [ACK] Seq=353 Ack=2749 Win=581 Len=0 TSval=1361293471 TSecr=2638607498
23	9.572529172	192.168.1.111	44.228.249.3	HTTP	600	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
24	9.758297894	44.228.249.3	192.168.1.111	TCP	66	80 → 33962 [ACK] Seq=2749 Ack=887 Win=479 Len=0 TSval=2638617065 TSecr=1361392858
25	9.758298194	44.228.249.3	192.168.1.111	HTTP	342	HTTP/1.1 302 Found (text/html)
26	9.758339940	192.168.1.111	44.228.249.3	TCP	66	33962 → 80 [ACK] Seq=807 Ack=3025 Win=501 Len=0 TSval=1361303044 TSecr=2638617066
27	9.760466113	192.168.1.111	44.228.249.3	HTTP	465	GET /login.php HTTP/1.1
28	9.946131888	44.228.249.3	192.168.1.111	TCP	1444	80 → 33962 [ACK] Seq=3025 Ack=1286 Win=476 Len=1378 TSval=2638617254 TSecr=1361303046 [TCP segment of a reassembled PDU]
29	9.94628694	44.228.249.3	192.168.1.111	HTTP	1436	HTTP/1.1 200 OK (text/html)
30	9.946338867	192.168.1.111	44.228.249.3	TCP	66	33962 → 80 [ACK] Seq=1286 Ack=5773 Win=501 Len=0 TSval=1361303232 TSecr=2638617254

Frame 23: 600 bytes on wire (4800 bits), 600 bytes captured (4800 bits) on interface eth0, id 0  
 Ethernet II, Src: PcsCompu\_b1:9d:67 (08:00:27:b1:9d:67), Dst: Sagemcom\_8a:b2:ea (84:a0:6e:8a:b2:ea)  
 Internet Protocol Version 4, Src: 192.168.1.111, Dst: 44.228.249.3  
 Transmission Control Protocol, Src Port: 33962, Dst Port: 80, Seq: 353, Ack: 2749, Len: 534  
 Hypertext Transfer Protocol  
 POST /userinfo.php HTTP/1.1  
 Host: testphp.vulnweb.com  
 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
 Accept-Language: en-US,en;q=0.5  
 Accept-Encoding: gzip, deflate  
 Content-Type: application/x-www-form-urlencoded  
 Content-Length: 26  
 Origin: http://testphp.vulnweb.com  
 Connection: keep-alive  
 Referer: http://testphp.vulnweb.com/login.php  
 Upgrade-Insecure-Requests: 1  
 [Full request URI: http://testphp.vulnweb.com/userinfo.php]  
 [HTTP request 2/3]  
 [Prev request in frame: 1]  
 [Decompress in frame: 26]

Wireshark - Follow TCP Stream (tcp.stream eq 0) - eth0

```

3D2..).t..l.....<|v....Q...
.79A.....x.4.j!..C/|.....l.[.*')..z.<..q..6/..t.t....B.....;..h..(x6...o..7Z..a.Lo;S.....1^3....l.q.4.4.'..~N$T...u.....e\
{[.Ah.....<...>3.a.....?34Z.x...../..B2.vI1.VV.....v.9..@.l?.U.:=:..F..'.k.6...
..F..?2?..j."vhc..U.....
1&.....a.Q.....).hx.....yD...Y.....o;...l.mf..\....I6...R...je.....K<r|7..
N/2..e).nK.....
1.&L...&a.-l.....<..x...@.....>:7..FC..s^J|.P)9+..V.Z+m.L...OS9k..<.+V...j.....&.CiI4'....X.
%.V....F>..J...<H...([U...lf.#...a.o.....P..3v..1p+...X.l....g.../..H.....9...W.3;.>.l....C...{..3.....
0
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

uname=test123&pass=test123HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Sun, 19 Feb 2023 08:44:22 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php

e
you must login

GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php

```

3 client pkts, 5 server pkts, 5 turns.

Entire conversation (7,057 bytes) Show data as ASCII Stream 0

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

#### ☑ 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 wgrzywanie 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

```
root@vm-sda: ~  
File Actions Edit View Help  
GNU nano 6.2 /etc/vsftpd.conf *  
# Run standalone? vsftpd can run either from an inetd or as a standalone  
# daemon started from an initscript.  
listen=NO  
#  
# 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 ftpd'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  
#  
G Help W Write Out W Where Is R Cut T Execute C Location M-U Undo M-A Set Mark M-J To Bracket  
X Exit R Read File N Replace U Paste J Justify / Go To Line M-E Redo M-C Copy M-Q Where Was
```

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

```
ftp> mget sekret1.txt sekret2.txt
mget sekret1.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||13897|)
150 Opening BINARY mode data connection for sekret1.txt (7 bytes).
100% |*****| 131 21.488855353 192.168.1.85 224.0.0.250 273.43 KiB/s 00:00 ETA
226 Transfer complete.
7 bytes received in 00:00 (23.90 KiB/s)
mget sekret2.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||151315|)
150 Opening BINARY mode data connection for sekret2.txt (7 bytes).
100% |*****| 7 55.12 KiB/s 00:00 ETA
226 Transfer complete.
7 bytes received in 00:00 (16.63 KiB/s)
ftp> put users.txt
local: users.txt remote: users.txt
229 Entering Extended Passive Mode (|||23262|)
150 Ok to send data.
100% |*****| 55 28.16 KiB/s 00:00 ETA
226 Transfer complete.
55 bytes sent in 00:00 (23.28 KiB/s)
ftp>
```

The image shows a Wireshark packet capture of an FTP session. The interface includes a menu bar, a toolbar, and a packet list pane on the left. The main pane displays the details of the selected packet (No. 21, Seq=117, Ack=421, Len=0). The packet list shows the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.117	192.168.1.131	FTP	72	Request: EPSV
2	0.000000	192.168.1.131	192.168.1.117	FTP	114	Response: 229 Entering Extended Passive Mode (   13897 )
3	0.000000	192.168.1.117	192.168.1.131	FTP	84	Request: RETR sekret1.txt
4	0.000000	192.168.1.131	192.168.1.117	FTP	134	Response: 150 Opening BINARY mode data connection for sekret1.txt (7 bytes).
5	0.000000	192.168.1.117	192.168.1.131	FTP	90	Response: 226 Transfer complete.
6	0.000000	192.168.1.117	192.168.1.131	TCP	66	37804 -> 21 [ACK] Seq=99 Ack=401 Win=16384 Len=0 TSval=2271884554 TSecr=3344356542
7	0.000000	192.168.1.117	192.168.1.131	FTP	84	Request: MDTM sekret1.txt
8	0.000000	192.168.1.131	192.168.1.117	FTP	86	Response: 213 20230204155706
9	0.000000	192.168.1.117	192.168.1.131	TCP	66	37804 -> 21 [ACK] Seq=117 Ack=421 Win=16384 Len=0 TSval=2271884598 TSecr=3344356542
10	0.000000	192.168.1.117	192.168.1.131	FTP	84	Request: SIZE sekret2.txt
11	0.000000	192.168.1.131	192.168.1.117	FTP	73	Response: 213 7
12	0.000000	192.168.1.117	192.168.1.131	TCP	66	37804 -> 21 [ACK] Seq=135 Ack=428 Win=16384 Len=0 TSval=2271885489 TSecr=3344357477
13	0.000000	192.168.1.117	192.168.1.131	FTP	72	Request: EPSV
14	0.000000	192.168.1.131	192.168.1.117	FTP	114	Response: 229 Entering Extended Passive Mode (   151315 )
15	0.000000	192.168.1.117	192.168.1.131	FTP	84	Request: RETR sekret2.txt
16	0.000000	192.168.1.131	192.168.1.117	FTP	134	Response: 150 Opening BINARY mode data connection for sekret2.txt (7 bytes).
17	0.000000	192.168.1.117	192.168.1.131	FTP	90	Response: 226 Transfer complete.
18	0.000000	192.168.1.117	192.168.1.131	TCP	66	37804 -> 21 [ACK] Seq=159 Ack=568 Win=16384 Len=0 TSval=2271885490 TSecr=3344357477
19	0.000000	192.168.1.117	192.168.1.131	FTP	84	Request: MDTM sekret2.txt
20	0.000000	192.168.1.131	192.168.1.117	FTP	86	Response: 213 20230204155714

The packet details pane shows the following information for the selected packet (No. 21):

- Destination: 192.168.1.117
- Protocol: FTP
- Length: 0
- Info: Seq=117, Ack=421, Win=16384, Len=0, TSval=2271884598, TSecr=3344356542

The packet bytes pane shows the raw data of the packet, which is a TCP ACK segment.