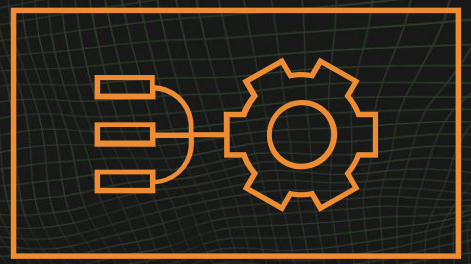
Enumeracja sieci

Pentest

Zajęcia nr 2

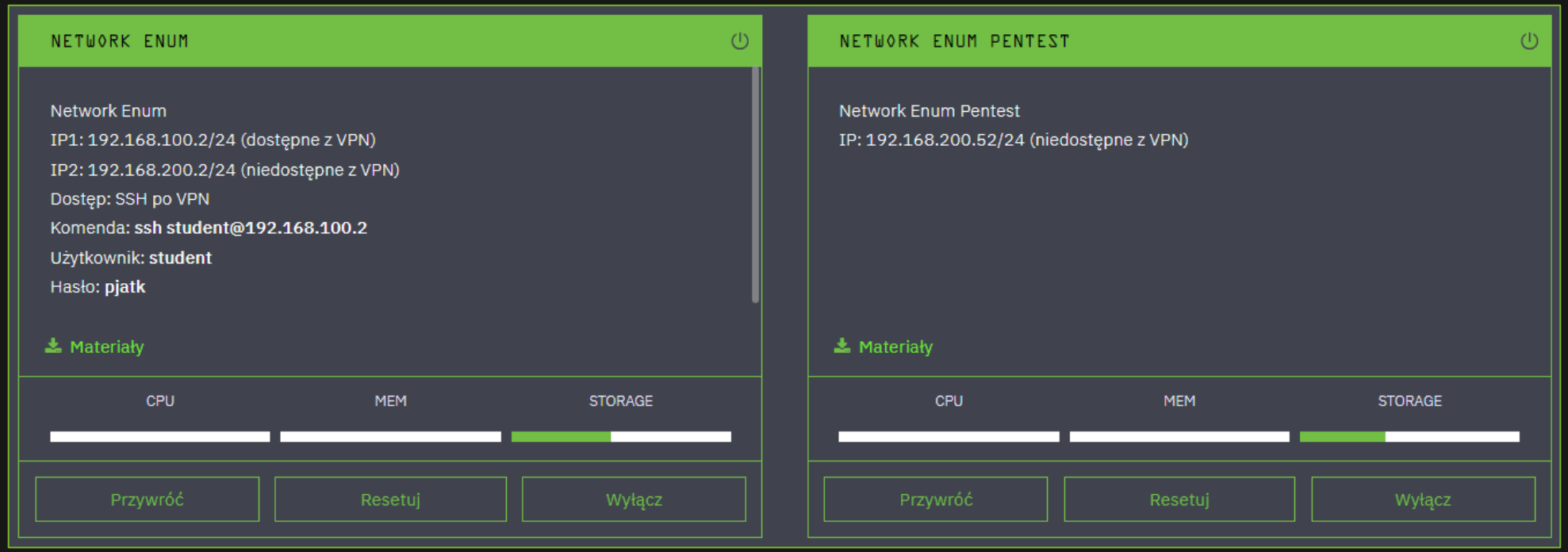


Spis treści

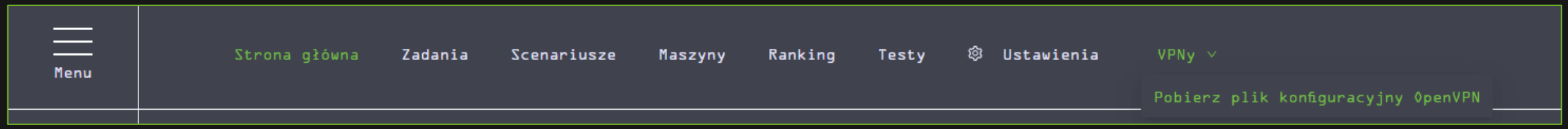
Przygotowanie środowiska

Uruchamianie maszyn

Przed rozpoczęciem upewnij się, że maszyny *Network Enum* oraz *Network Enum PENTEST* są włączone.
Jeżeli coś się zepsuje, w każdej chwili możesz je przywrócić do stanu początkowego.



Połączenie OpenVPN



Połączenie OpenVPN jest niezbędne do rozwiązania zadań.
Aby połączyć się z siecią VPN, należy pobrać plik konfiguracyjny OpenVPN z rozwijanego menu „VPNy” na stronie głównej.
Następnie należy wykonać komendę:

```
sudo openvpn /sciezka/do/pliku.ovpn
```

Legenda

cat /etc/passwd - komendę należy wykonać na maszynie Kali
cat /etc/passwd - komendę należy wykonać na maszynie Ćwiczenia
cat /etc/passwd - komendę należy wykonać na maszynie Pentest

Zadania

Zadanie 2.1p: Nmap - podsumowanie

Celem zadania jest przeskanowanie maszyny 192.168.200.52
Nmap powinien zostać uruchomiony w połączeniu z przełącznikami, których nauczyliśmy się do tej pory.

Większość opcji Nmapa możemy ze sobą **łączyć**:

```
nmap -sT -sV -sC -O --osscan-guess 192.168.200.52
```

Zadanie zostanie rozwiązane po uruchomieniu tej komendy.
Skan wykonujemy z „wnętrza” sieci! Najpierw `ssh student@192.168.100.2 -p 23`

```
student@network-enum:~$ nmap -sT -sV -sC -O --osscan-guess -p- -vv 192.168.200.52
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-01 12:46 UTC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:46
Completed NSE at 12:46, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:46
Completed NSE at 12:46, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 12:46
Completed NSE at 12:46, 0.00s elapsed
Initiating ARP Ping Scan at 12:46
Scanning 192.168.200.52 [1 port]
Completed ARP Ping Scan at 12:46, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:46
```

Zadanie 2.2p: Serwer HTTP

Celem zadania jest odczytanie flagi z pliku flag2.2p.txt na serwerze HTTP i wklejenie do formularza na stronie.

```
curl http://192.168.200.52/
curl http://192.168.200.52/flag2.2p.txt
```

alternatywnie:

```
wget http://192.168.200.52/flag2.2p.txt
cat flag2.2p.txt
```

pobieranie wszystkich plików:

```
wget -r --no-parent http://192.168.200.52/
```

```
student@network-enum:~$ wget http://192.168.200.52/flag2.2p.txt
--2024-08-01 12:50:20--  http://192.168.200.52/flag2.2p.txt
Connecting to 192.168.200.52:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 25 [text/plain]
Saving to: 'flag2.2p.txt'

flag2.2p.txt              100%[===================>]      25  --.-KB/s    in 0s

2024-08-01 12:50:20 (5.74 MB/s) - 'flag2.2p.txt' saved [25/25]

student@network-enum:~$ cat flag2.2p.txt
```

Zadanie 2.3p: Serwer FTP

Celem zadania jest odczytanie flagi z pliku flag2.3p.txt na serwerze FTP i wklejenie do formularza na stronie.

```
ftp 192.168.200.52
Name: anonymous
Password: dowolne
dir
get  flag2.3p.txt
```

```
student@network-enum:~$ ftp 192.168.200.52
Connected to 192.168.200.52.
220 pyftpdlib 1.5.7 ready.
Name (192.168.200.52:student): anonymous
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering extended passive mode (|||58169|).
125 Data connection already open. Transfer starting.
-rw-r--r--    1 root     root           21 Aug 01 12:36 flag2.3p.txt
226 Transfer complete.
ftp> get flag2.3p.txt
local: flag2.3p.txt remote: flag2.3p.txt
229 Entering extended passive mode (|||60757|).
125 Data connection already open. Transfer starting.
100% |***********************************************************|    21       42.72 KiB/s    00:00 ETA
226 Transfer complete.
21 bytes received in 00:00 (31.84 KiB/s)
ftp> quit
221 Goodbye.
student@network-enum:~$ cat flag2.3p.txt
```

Zadanie 2.4p: Serwer SMB

Celem zadania jest odczytanie flagi z pliku flag2.4p.txt na serwerze SMB i wklejenie do formularza na stronie.

```
smbclient -N -L //192.168.200.52/ #wylistuje nazwy zasobów, w tym FLAG
smbclient -N //192.168.200.52/FLAG #połączy się z zasobem FLAG
ls
get flag2.4p.txt
```

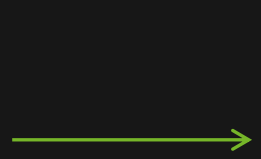
W narzędziu smbclient, **przełączniki -L i -N** pełnią następujące funkcje:
-L: Wyświetla listę dostępnych zasobów (udostępnionych folderów) na serwerze SMB. Używa się go, aby zobaczyć, jakie udostępnione foldery są dostępne na serwerze.
-N: Pomija uwierzytelnienie hasłem, co oznacza, że smbclient łączy się z serwerem SMB bez wymagania podania hasła. Jest użyteczne, gdy dostęp do zasobów wymaga tylko identyfikacji użytkownika.

Zadanie 2.4p: Serwer SMB

```
student@network-enum:~$ smbclient -N -L //192.168.200.52/

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            Disk
        FLAG            Disk
SMB1 disabled -- no workgroup available
student@network-enum:~$ smbclient -N //192.168.200.52/FLAG
Try "help" to get a list of possible commands.
smb: \> ls
  flag2.4p.txt                        AN       29  Thu Aug  1 12:36:50 2024

                148529400 blocks of size 1024. 14851044 blocks available
smb: \> get flag2.4p.txt
getting file \flag2.4p.txt of size 29 as flag2.4p.txt (3.5 KiloBytes/sec) (average 3.5 KiloBytes/sec)
smb: \> quit
student@network-enum:~$ cat flag2.4p.txt
```



Koniec ćwiczeń