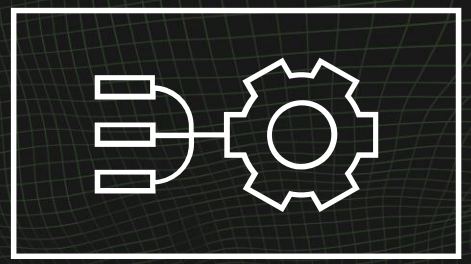
Enumeracja sieci

Zajęcia nr 2



Spis treści

Wstęp

Enumeracja sieci to proces zbierania informacji o sieci komputerowej, jej urządzeniach oraz usługach. W jego ramach identyfikowane są adresy IP, nazwy hostów, otwarte porty, systemy operacyjne, a także wersje zainstalowanego oprogramowania. Jest to kluczowy etap w testowaniu bezpieczeństwa, umożliwiający lepsze zrozumienie struktury i potencjalnych słabości sieci. Techniki enumeracji obejmują skanowanie portów, analizę protokołów oraz wykorzystanie narzędzi takich jak Nmap czy Metasploit. Celem jest zgromadzenie jak najwięcej informacji, które mogą być wykorzystane do dalszych działań, takich jak testy penetracyjne czy ocena podatności.

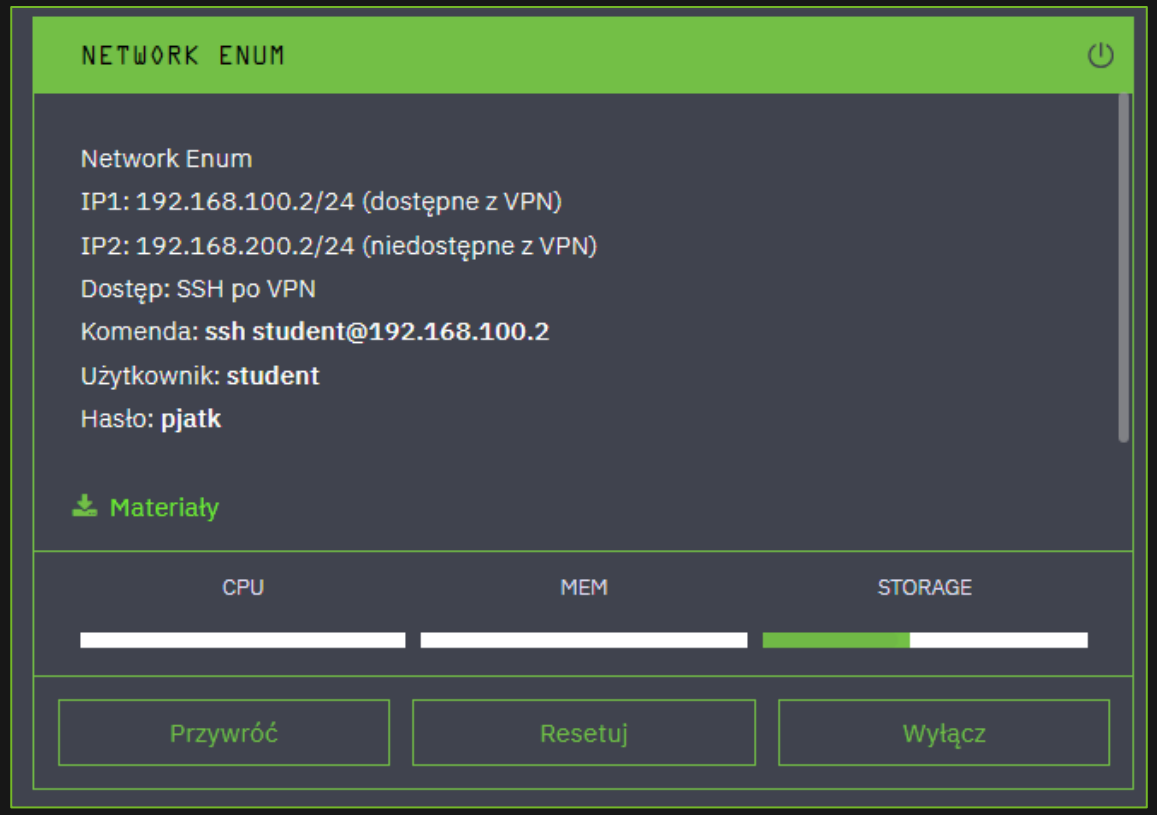
Czym jest Nmap?

Nmap (Network Mapper) to popularne narzędzie open source służące do odkrywania sieci i audytowania jej bezpieczeństwa. Jest używane głównie do skanowania portów, co pozwala na identyfikację aktywnych urządzeń oraz uruchomionych usług w sieci. Nmap może również wykrywać systemy operacyjne oraz szczegóły dotyczące oprogramowania na podstawie tzw. fingerprintingu. Dzięki swojej wszechstronności i dostępności, jest często wykorzystywane przez administratorów sieci, specjalistów ds. bezpieczeństwa oraz entuzjastów IT do diagnozowania problemów i identyfikacji słabości sieci. Nmap jest dostępny na wielu platformach, w tym Linux, Windows i macOS, i ma zarówno interfejs wiersza poleceń, jak i graficzny (Zenmap).

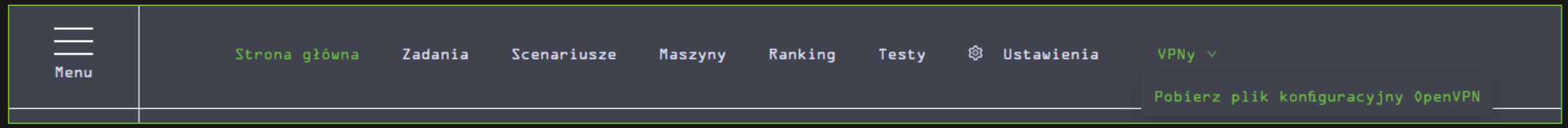
Przygotowanie środowiska

Uruchamianie maszyn

Przed rozpoczęciem upewnij się, że maszyna *Network Enum* jest włączona.
Jeżeli coś się zepsuje, w każdej chwili możesz ją 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

Teoria

Czym jest enumeracja sieci i dlaczego jest kluczowa?

Enumeracja sieci to pierwszy i niezwykle istotny etap testów penetracyjnych, który polega na zbieraniu szczegółowych informacji o infrastrukturze sieciowej danej organizacji lub systemu. Jest to proces aktywnego skanowania, który pozwala na identyfikację aktywnych hostów, otwartych portów, uruchomionych usług oraz potencjalnych podatności. Pentesterzy i badacze zabezpieczeń wykorzystują enumerację, aby uzyskać punkt zaczepienia do dalszych etapów testów, takich jak eskalacja uprawnień czy eksploitacja znalezionych słabości.

Czym jest enumeracja sieci i dlaczego jest kluczowa?

Bez znajomości struktury sieci trudno skutecznie przeprowadzić atak lub symulację rzeczywistego zagrożenia. Dlatego enumeracja jest pierwszym krokiem w pentestingu, a jej skuteczność może przesądzić o dalszym przebiegu testów. Właściwie przeprowadzona enumeracja może dostarczy informacji o:

- Uruchomionych hostach i topologii sieci,
- Otwartych portach i usługach nasłuchujących na tych portach,
- Systemach operacyjnych i ich wersjach,
- Potencjalnych punktach wejścia do systemu,
- Używanych protokołach i ich konfiguracji,
- Możliwych podatnościach na ataki.

Nmap i alternatywy dla skanowania sieci

Jednym z najpopularniejszych narzędzi do enumeracji sieci jest Nmap (Network Mapper), który pozwala na szybkie skanowanie hostów, identyfikację otwartych portów oraz wykrywanie uruchomionych usług. Nmap obsługuje również skrypty NSE (Nmap Scripting Engine), które umożliwiają bardziej zaawansowaną analizę podatności oraz identyfikację słabości systemowych.
Jednak Nmap nie jest jedynym narzędziem do skanowania sieci. Istnieje wiele alternatyw, które pozwalają na przeprowadzenie skutecznej enumeracji:

- Masscan - niezwykle szybki skaner portów,
- Unicornscan - narzędzie stworzone z myślą o szybkim skanowaniu oraz zbieraniu metadanych,
- Zmap - zoptymalizowany do bardzo szybkiego skanowania dużych sieci,
- RustScan - nowoczesny skaner portów, zaprojektowany z myślą o maksymalnej wydajności i integracji z Nmapem.

Enumeracja sieci na Windowsie

Chociaż wiele narzędzi pentestingowych jest tworzonych z myślą o systemach Linux, to Windows również oferuje kilka potężnych rozwiązań do enumeracji sieci:

- PowerShell - wbudowane polecenia, takie jak Test-NetConnection, Get-NetTCPConnection, Get-NetIPAddress, pozwalają na zbieranie informacji o sieci,
- SharpHound - narzędzie do zbierania informacji o strukturze Active Directory,
- Advanced IP Scanner - przyjazne użytkownikowi narzędzie do identyfikacji hostów w sieci.

Zaawansowane aspekty enumeracji sieci

Enumeracja sieci nie ogranicza się tylko do skanowania portów i hostów. Istnieje wiele technik umożliwiających uzyskanie jeszcze dokładniejszych informacji:

- Enumeracja DNS - analiza rekordów DNS może ujawnić subdomeny, struktury organizacyjne oraz potencjalne cele ataku. Narzędzia takie jak dnsrecon, Fierce czy Sublist3r są wykorzystywane do zbierania danych z systemu nazw domenowych.
- Enumeracja SNMP - Simple Network Management Protocol może być używany do zbierania informacji o urządzeniach sieciowych, jeśli nie jest odpowiednio zabezpieczony. Narzędzia takie jak snmpwalk pomagają w analizie SNMP.
- Enumeracja systemów kontroli wersji - analiza publicznych repozytoriów kodu może ujawnić kluczowe informacje na temat architektury aplikacji i potencjalnych podatności. Służą do tego np. aplikacje Gitwalk oraz Gitdump.

Podsumowanie

Enumeracja sieci to fundamentalny krok w testach penetracyjnych, który pozwala pentesterom na zdobycie kluczowych informacji o strukturze sieci, dostępnych hostach oraz potencjalnych podatnościach. Choć Nmap jest najpopularniejszym narzędziem, istnieje wiele alternatyw, które sprawdzają się w różnych scenariuszach. Ponadto, system Windows oferuje własne narzędzia do przeprowadzania enumeracji, co czyni go dość istotnym środowiskiem do testów penetracyjnych. Współczesne techniki enumeracji obejmują nie tylko skanowanie portów, ale także analizę DNS, SMB czy SNMP, co czyni je nieodzownym elementem każdego audytu bezpieczeństwa.

Zadania

Zadanie 2.1: Prosty Nmap

Celem zadania jest przeskanowanie hosta 192.168.100.2 za pomocą narzędzia Nmap i znalezienie portu, na którym nasłuchuje usługa SSH.
Najprostsze użycie Nmap to: *nmap 192.168.100.2*
Uwaga! Pierwsze zadanie wykonujemy z naszej maszyny. Następne już po połączeniu się przez SSH z maszyny 192.168.100.2!

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.100.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 12:57 CEST
Nmap scan report for 192.168.100.2
Host is up (0.015s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

Zadanie 2.1: Prosty Nmap

Nmap domyślnie wykonuje tzw. Stealth Scan (-sS), który nie weryfikuje jakie usługi i w jakich wersjach są uruchomione na znalezionych portach. Np. znaleziona usługa "telnet" została zasugerowana tylko na podstawie numeru domyślnego portu TCP.
Użycie Nmap z bardziej szczegółowym raportem: `nmap -A 192.168.100.2`
W kolejnych zadaniach nauczysz się najważniejszych przełączników do Nmap.
Zadanie zostanie automatycznie zaliczone po znalezieniu usługi SSH na niestandardowym porcie!

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.100.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 12:58 CEST
Nmap scan report for 192.168.100.2
Host is up (0.044s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
23/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 fd:3d:38:36:a9:5d:44:65:3d:7f:a9:c1:13:31:cc:a2 (ECDSA)
|_  256 ef:4f:50:1a:82:0f:1e:8f:31:bc:19:3e:56:c9:d7:4c (ED25519)
80/tcp open  http
|_http-title: Site doesn't have a title (text/html).
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, He
lp, Kerberos, LDAPSearchReq, LPDString, NULL, RPCCheck, RTSPRequest, SMBProgNeg, SSLSessionReq, TLSSessionR
eq, TerminalServerCookie, X11Probe:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/html
|_    Content-Length: 3
1 service unrecognized despite returning data. If you know the service/version, please submit the following
 fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.94SVN%I=7%D=8/1%Time=66AB6A4A%P=x86_64-pc-linux-gnu%r(NU
```

Zadanie 2.2: Połączenie SSH

W ramach tego zadania połącz się poprzez SSH ze znalezionym wcześniej portem: `ssh student@192.168.100.2 -p 23` #hasło: pjatk; port znaleziony w 2.1.

```
┌──(kali㉿kali)-[~]
└─$ ssh student@192.168.100.2 -p 23
student@192.168.100.2's password:
Linux network-enum 6.1.0-23-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Aug  1 14:00:49 2024 from 10.65.0.6
student@network-enum:~$
```

Zadanie 2.3: Lista opcji

nmap -h - polecenie to pokaże nam listę wszystkich opcji i parametrów, z jakimi możemy uruchomić Nmap. Warto się z nimi zapoznać choć pobieżnie. Niektóre będą nam później potrzebne.

```
student@network-enum:~$ nmap -h
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
```

Zadanie 2.4: Odkrywanie hostów

Celem zadania jest przeskanowanie sieci 192.168.100.0/24 pod kątem uruchomionych hostów bez skanowania portów i usług.
`nmap -sn 192.168.100.0/24` [wytłumaczenie: -sn wyłącza skanowanie portów]

```
student@network-enum:~$ nmap -sn 192.168.100.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-01 11:13 UTC
Nmap scan report for 192.168.100.250
Host is up (0.00065s latency).
MAC Address: 00:50:56:BF:6E:77 (VMware)
Nmap scan report for 192.168.100.254
Host is up (0.00083s latency).
MAC Address: 00:50:56:BF:CB:07 (VMware)
Nmap scan report for 192.168.100.2
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 35.74 seconds
```

Zadanie 2.5: Otwarte porty

Celem zadania jest przeskanowanie sieci 192.168.100.0/24 pod kątem uruchomionych hostów oraz otwartych portów TCP bez dokładnego skanowania usług.

`nmap -sT 192.168.100.0/24` [wytłumaczenie: -sT skanuje porty TCP]

```
student@network-enum:~$ nmap -sT 192.168.100.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-01 11:12 UTC
Nmap scan report for 192.168.100.250
Host is up (0.46s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:50:56:BF:6E:77 (VMware)

Nmap scan report for 192.168.100.254
Host is up (0.76s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:50:56:BF:CB:07 (VMware)

Nmap scan report for 192.168.100.2
Host is up (0.00011s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http

Nmap done: 256 IP addresses (3 hosts up) scanned in 36.50 seconds
```

Zadanie 2.6: Detekcja wersji

Celem zadania jest przeskanowanie sieci 192.168.100.0/24 pod kątem uruchomionych hostów oraz otwartych portów TCP z uwzględnieniem wersji usług.

`nmap -sV 192.168.100.0/24` [wytłumaczenie: -sV skanuje porty TCP i pobiera wersje działających usług]

```
student@network-enum:~$ nmap -sV 192.168.100.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-01 11:15 UTC
Nmap scan report for 192.168.100.250
Host is up (0.00015s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
MAC Address: 00:50:56:BF:6E:77 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.100.254
Host is up (0.00010s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
MAC Address: 00:50:56:BF:CB:07 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.100.2
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
23/tcp open     ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp filtered http
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Zadanie 2.7: Skrypty

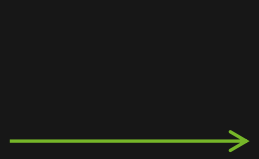
Celem zadania jest przeskanowanie sieci 192.168.100.0/24 pod kątem uruchomionych hostów, otwartych portów TCP oraz uruchomieniem domyślnych skryptów.

`nmap -sC 192.168.100.0/24` [wytłumaczenie: -sC skanuje porty TCP, uruchamia domyślne skrypty]

```
student@network-enum:~$ nmap -sC 192.168.100.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-01 11:18 UTC
Nmap scan report for 192.168.100.250
Host is up (0.00090s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 d0f6da54149c8418243377945ce8b5d3 (RSA)
|   256 1f6c4f83d67b1c7264a71551be7de8f1 (ECDSA)
|_  256 77c6d033ee7ba3b77d27f272a11372bc (ED25519)
MAC Address: 00:50:56:BF:6E:77 (VMware)

Nmap scan report for 192.168.100.254
Host is up (0.00063s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 5d085487da0042dcc99914e8008976e5 (RSA)
|   256 d8082ab82053989957001a84e451957c (ECDSA)
|_  256 6b9805514137841930d45f04a8addbfe (ED25519)
80/tcp open  http
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 00:50:56:BF:CB:07 (VMware)

Nmap scan report for 192.168.100.2
Host is up (0.0000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE    SERVICE
23/tcp open     telnet
80/tcp filtered http
```



Zadanie 2.8: Detekcja OS

Celem zadania jest przeskanowanie sieci 192.168.100.0/24 pod kątem uruchomionych hostów i systemów operacyjnych.
`nmap -O --osscan-guess 192.168.100.0/24` [wytłumaczenie: -O --osscan-guess zgaduje system operacyjny na hostach]

```
student@network-enum:~$ nmap -O --osscan-guess 192.168.100.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-01 11:20 UTC
Nmap scan report for 192.168.100.250
Host is up (0.00077s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:50:56:BF:6E:77 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

Nmap scan report for 192.168.100.254
Host is up (0.00057s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:50:56:BF:CB:07 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

Nmap scan report for 192.168.100.2
Host is up (0.00013s latency).
```

Referencje

https://nmap.org/man/pl/man-briefoptions.html
polski manual dla Nmap

https://nmap.org/docs.html
dokumentacja Nmap

Koniec ćwiczeń