Politechnika Wrocławska

SPRAWOZDANIE Z ZAJĘĆ LABORATORYJNYCH
CYBERBEZPIECZEŃSTWO

Lab 11
Rekonesans sieciowy

Tomasz Mroczko, 266604

January 2, 2024

1 Zadania

Zadanie I

> *Uruchom wszystkie maszyny wirtualne, które zainstalowałeś w VirtualBOX, Wykonaj następujące polecenie: nmap 172.16.96.0/24 (CO TO ZA ADRES I CZYM RÓŻNI SIĘ OD ADRESÓW PONIŻEJ?)*

Uruchomiono następujące maszyny wirtualne o danych adresach:

- Kali: 172.16.96.2
- Ubuntu: 172.16.96.3
- Metasploitable: 172.16.96.4

Następnie wykonano polecenie nmap.

```
└─$ sudo nmap 172.16.96.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-01 13:16 CET
Nmap scan report for 172.16.96.1
Host is up (0.00025s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.96.2
Host is up (0.0013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.96.4
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:64:C0:F9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.96.3
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (4 hosts up) scanned in 14.69 seconds
```

Polecenie nmap wykryło 4 hosty, z czego 3 to maszyny o adresach podanych powyżej. Dodatkowy adres: 172.16.96.1, posiada otwarty tylko jeden port - "53/tcp". Prawdopodobnie jest to adres bramy domyślnej w sieci NAT, która pełni rolę serwera DNS.
Jeśli chodzi o adres 172.16.96.0/24, to oznacza on sieć oraz maskę podsieci. 24 oznacza że pierwsze 24 bity przeznaczone są na adres sieci, a pozostałe 8 na adres hosta w danej sieci. Warto zauważyć że maszyna Metasploitable posiada bardzo dużo otwartych portów, z wieloma działającymi usługami.

Zadanie II

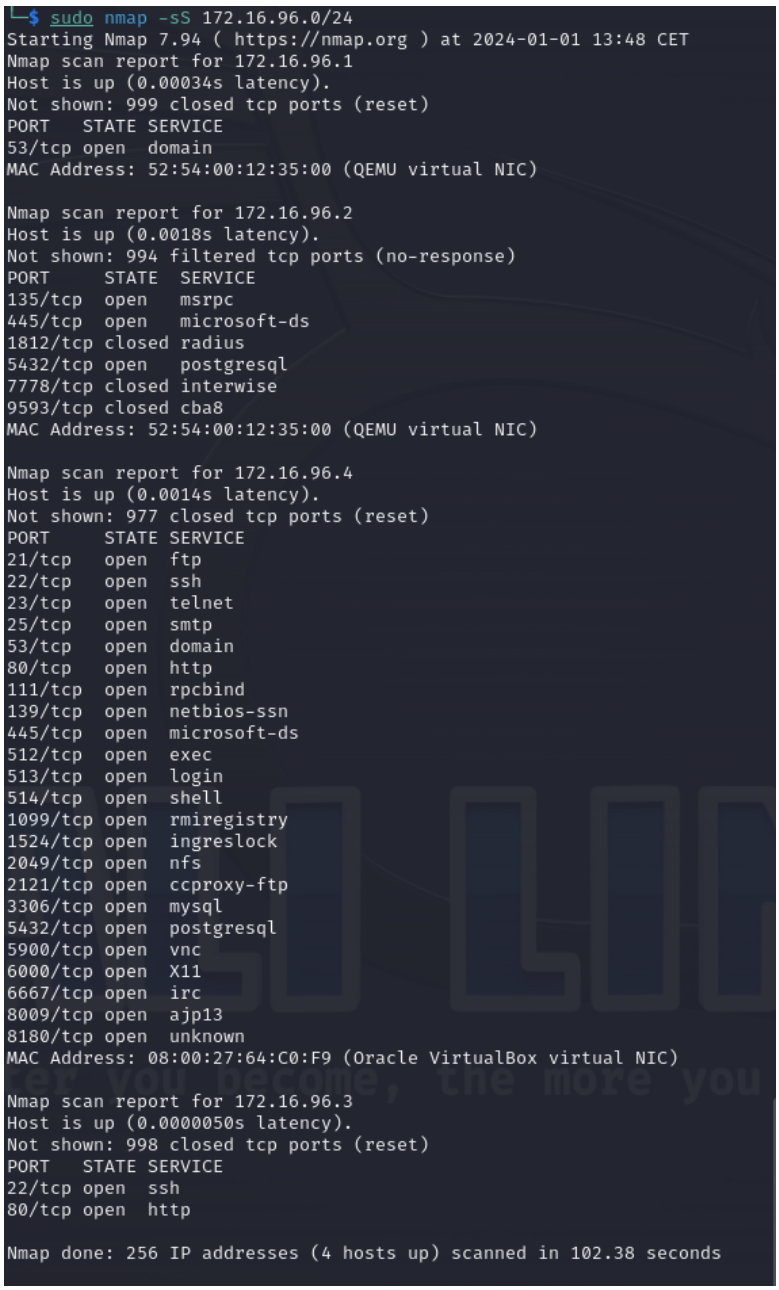
Wykonuj różne typy skanów TCP i porównaj wyniki:
a. opcje –sT, -sS –sN, -sM, -sA, -sW, -sI
b. opisz różnice między skanowaniem z wyżej wymienionymi opcjami

Zrzuty ekrany wyników

- **nmap -sT**

```
└─$ sudo nmap -sT 172.16.96.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-01 13:47 CET
Nmap scan report for 172.16.96.1
Host is up (0.0063s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.96.2
Host is up (0.0026s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.96.4
Host is up (0.0042s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:64:C0:F9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.96.3
Host is up (0.00012s 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 13.29 seconds
```

- **nmap -sS**



```
└─$ sudo nmap -sS 172.16.96.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-01 13:48 CET
Nmap scan report for 172.16.96.1
Host is up (0.00034s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.96.2
Host is up (0.0018s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE
135/tcp  open   msrpc
445/tcp  open   microsoft-ds
1812/tcp closed radius
5432/tcp open   postgresql
7778/tcp closed interwise
9593/tcp closed cba8
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.96.4
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:64:C0:F9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.96.3
Host is up (0.0000050s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (4 hosts up) scanned in 102.38 seconds
```

- **nmap -sN**

```
└─$ sudo nmap -sN 172.16.96.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-01 13:51 CET
Nmap scan report for 172.16.96.1
Host is up (0.00023s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
53/tcp open|filtered domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.96.2
Host is up (0.00026s latency).
All 1000 scanned ports on 172.16.96.2 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.96.4
Host is up (0.00068s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:64:C0:F9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.96.3
Host is up (0.0000040s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE         SERVICE
22/tcp open|filtered ssh
80/tcp open|filtered http

Nmap done: 256 IP addresses (4 hosts up) scanned in 7.40 seconds
```

- **nmap -sM**

```
└─$ sudo nmap -sM 172.16.96.0/24
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-01 17:57 CET
Nmap scan report for 172.16.96.1
Host is up (0.00025s latency).
All 1000 scanned ports on 172.16.96.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.96.2
Host is up (0.00024s latency).
All 1000 scanned ports on 172.16.96.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.96.4
Host is up (0.00056s latency).
All 1000 scanned ports on 172.16.96.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:64:C0:F9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.96.3
Host is up (0.0000040s latency).
All 1000 scanned ports on 172.16.96.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 3.63 seconds
```

- **nmap -sA**

```
└─$ sudo nmap -sA 172.16.96.0/24
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-01 18:26 CET
Nmap scan report for 172.16.96.1
Host is up (0.00028s latency).
All 1000 scanned ports on 172.16.96.1 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.96.2
Host is up (0.00024s latency).
All 1000 scanned ports on 172.16.96.2 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.96.4
Host is up (0.00057s latency).
All 1000 scanned ports on 172.16.96.4 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:64:C0:F9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.96.3
Host is up (0.0000050s latency).
All 1000 scanned ports on 172.16.96.3 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 3.14 seconds
```

- **nmap -sW**

Opisy działania / wyników

- **nmap-sT TCP connect()**
  Skanowanie -sT dało takie same wyniki jak dla skanu nmap bez żadnych opcji (z uprawnieniami root). Tryb ten jest wybierany domyślnie jeśli -sS (Skanowanie TCP SYN) nie jest dostępne. Różni się ono tym, że zamiast wysyłać pakiety raw na niższym poziomie, metoda ta używa do nawiązania połączenia wywołania systemowego connect(). Preferowana jest skanowanie metodą -sS. Powinno być mniej czasochłonne oraz lepiej zoptymalizowane jeśli chodzi o ilość przesłanych danych.
- **nmap-sS (TCP SYN)**
  Skanowanie -sS również dało taki sam efekt jak dla nmap bez opcji. Tryb ten jest domyślną metodą skanowania. Może on być przeprowadzony relatywnie szybko oraz jest dyskretny. Podczas tego tryby nie jest ustanawiane pełne połączenie. Wysyłany jest pakiet SYN (pierwsza część *three-way handshake*), a następnie na podstawie odpowiedzi, nmap identyfikuje port danego hosta.
- **nmap-sN (TCP NULL Scan)**

Skanowanie -sN wysyła pakiet do hosta, nie ustawiając żadnych flag w polu nagłówku TCP. Jeśli port jest zamknięty, otrzymamy pakiet RST. Jeśli jest on otwarty, to nie otrzymamy odpowiedzi. Stosunkowo niska wykrywalność skanowania oraz duża szansa na ominięcie zapór sieciowych i filtrowań to główne zalety tego typu skanowań.

- **nmap -sM (TCP Maimon Scan)**
  Skanowanie tą metodą dało wyniki inne niż poprzednie. Uzyskane wyniki pokazują wszystkie porty na każdym z 4 hostów jako zamknięte. Przesyłane są flagi FIN/ACK. Niektóre systemy pomijają odpowiedzi jeśli port jest otwarty. Może to prowadzić do sytuacji kiedy odpowiedz nie jest generowane, nawet gdy port jest otwarty co powoduje nieoznaczenie otwartych portów.
- **nmap -sA (TCP ACK)**
  Wyniki tego skanowania oznaczyły wszystkie porty jako *niefiltrowane*. Metoda ta wysyła flagi ACK(ostatni etap three-way handshake). Skanowanie to nie wykrywa portów otwarty, zamiast tego wykorzystywane jest do analizy reguł filtrowania. W przypadku skanowania systemów nie posiadających filtrowania, porty otwarte i zamknięte zwrócą pakiet RST, a skan oznaczy je jako niefiltrowane.
- **nmap -sW (Skanowanie TCP Window)**
  Wyniki uzyskane pokazują stan otwarcia portów oraz usługę działającą na nich (nawet na tych z usługą unknown). Skanowanie podobne do -sA. Również wysyła flagi ACK, w celu badania filtrowania portów. Metoda ta skupia się na polu TCP Window Size w nagłówkach. Potrafi ono jednak odróżnić porty otwarte od zamkniętych, zamiast podawać niefiltrowany. Niestety tryb ten polega na implementacji stosu TCP rzadko spotykanej w systemach. Systemy z inną implementacją, oznaczą porty jako zamknięte.
- **nmap -sI (Skanowanie Idl)**
  Bardzo poufna metoda. Pozwala na przeprowadzenie skanowania w sposób poufny, nieśledzony. Operacja wysyłania pakietów TCP, nie przebiega z rzeczywistego adresu hosta. Wykorzystywany jest tzw. *host zombie*. Pozwala na przeprowadzenie dokładnej analizy, dzięki podaniu numerów portu aby dotrzeć do konkretnych portów.

  Źródło: https://nmap.org/man/pl/man-port-scanning-techniques.html

Zadanie III

Wykonaj skanowanie UDP

Skanowanie UDP

```
└─$ sudo nmap -sU 172.16.96.4
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 11:52 CET
Nmap scan report for 172.16.96.4
Host is up (0.00083s latency).
Not shown: 994 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 08:00:27:64:C0:F9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1071.50 seconds

┌──(kali㉿kali)-[~]
└─$
```

Skanowanie UDP, w przeciwieństwie do poprzednich skanowań, używa pakietów UDP, zamiast TCP. Do każdego portu wysyłane są pakiety UDP, jeśli zwrócony zostanie pakiet UDP, to port jest otwarty. Jeśli odpowiedź nie dotrze, to port klasyfikowany jest jako otarty|filtrowany. Skanowanie UDP jset znacznie wolniejsze niż używanie pakietów TCP. Nawet jeśli port jest otwarty to rzadko wysyła jakąkolwiek odpowiedź, co wymusza oczekiwanie i ponawianie próby.

Zadanie IV

> *Wypróbuj różne opcje opóźnienia nmap (-T) z zestawu wartości 0,1,2,3,4,5. Jaka jest różnica w wynikach i wydajności?*

Opcja	Czas trwania
-T 0 (Paranoid)	>1000s
-T 1 (Sneaky)	>1000s
-T 2 (Polite)	>1000s
-T 3 (Normal)	1071s
-T 4 (Aggressive)	400s
-T 5 (Insane)	11s

Table 1: Czas skanowania UDP w zależności od opcji -T

Czas skanowania rósł znacząco wraz ze spadkiem wartości -T. Poziom -T0 to najwolniejsze, najdokładniejsze skanowania. Jest łagodne i minimalizuje ślad skanowania oraz obciążenie sieci. -T1 jest nieco szybsze, ale dalej relatywnie łagodne i dokładne. Opcja -T3 jest opcją domyślną. Dobry kompromis pomiędzy szybkością a agresywnością stanowania. Jeśli nie podamy flagi -T, to właśnie te opcja zostanie przyjęta. -T5 (Insane) to bardzo agresywne skanowanie. Niestety użycie tej opcji zwiększa podatność na błędy oraz zmniejsza dokładność.

Zadanie V

> *Dla wybranego systemu i wybranego serwisu użyj usługi wykrywania wersji (-sV) np. nmap -sV 172.16.96.x -p 22*

Wybrano system Metasploitable(172.16.96.4) oraz serwis mysql, działający na porcie 3306.

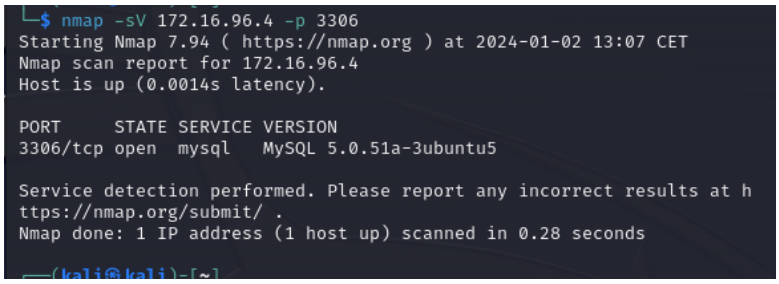


Figure 1: Wyniki wykrywania wersji

Jak widać na powyższym zrzucie ekranu, udało się pomyślnie wykryć wersję działającego na porcie serwisu.

Zadanie VI

Spróbuj znaleźć wersję systemu operacyjnego zainstalowaną na maszynach wirtualnych (opcja –O)

- 172.16.96.1 (brama domyślna)
- 172.16.96.2 (Kali)

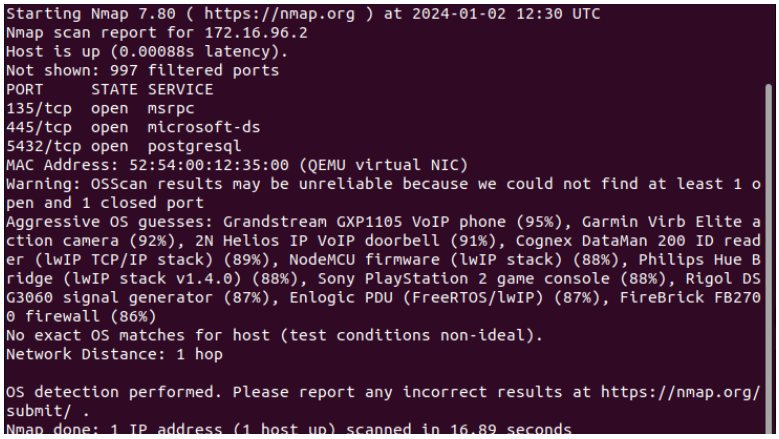


Figure 2: Wyniki wykrywania wersji

Jak widać na zrzucie ekranu, dla systemu Kali nie udało się wykryć systemu operacyjnego. Wyniki dają tylko przewidywane (najbardziej prawdopodobne) możliwości.

- 172.16.96.3 (Ubuntu)

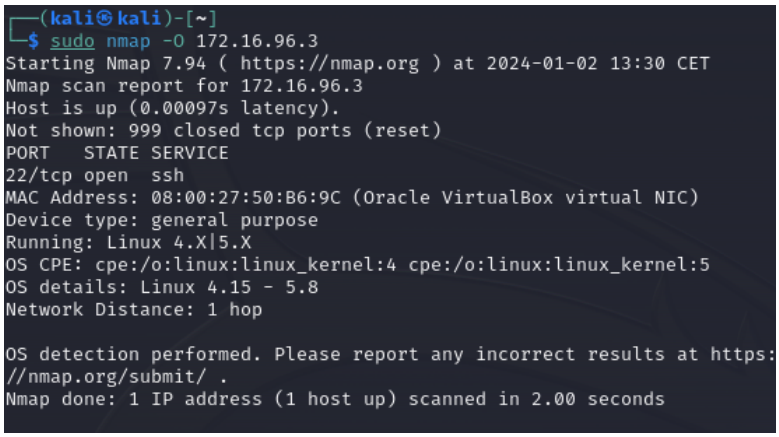


Figure 3: Wyniki wykrywania wersji

Udało się pomyślnie wykryć system operacyjny na maszynie Ubuntu.

- 172.16.96.4 (Metasploitable)

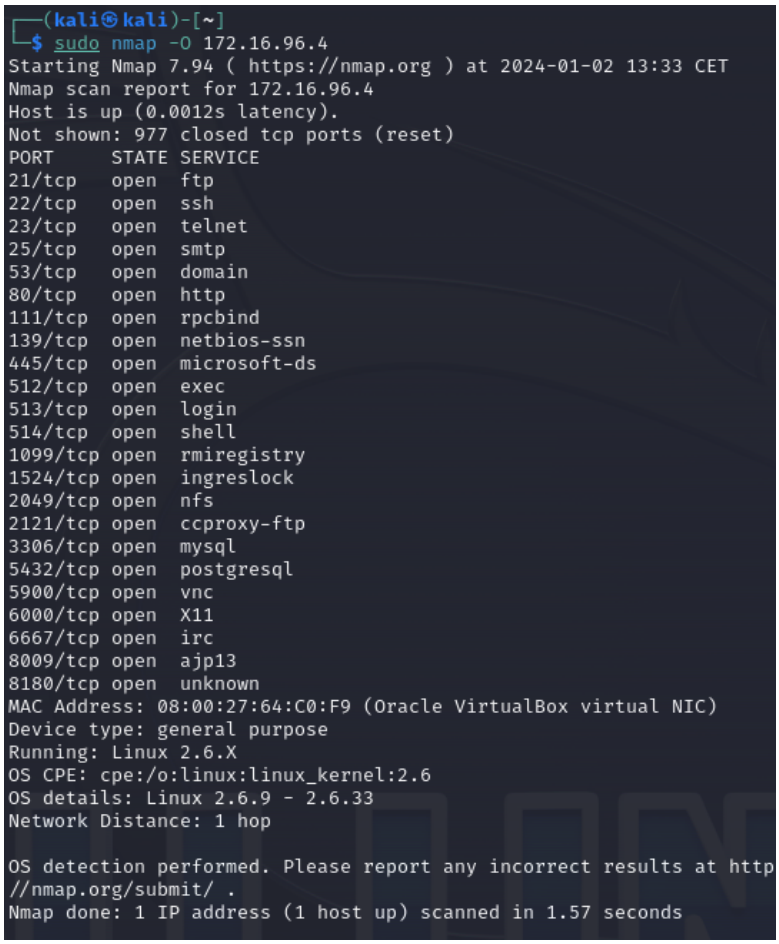


Figure 4: Wyniki wykrywania wersji

Wykrycie systemu na niebezpiecznym systemie (Metasploitable) nie przysporzyło problemów.

Zadanie VII

Sprawdź katalog /usr/share/nmap/scripts i znajdź kilka różnych skryptów nmap i opisz ich aplikację

- **http-grep.nse**
  Ten skrypt jest odpowiednikiem unixowego *grep*. Za jego pomocą można przeszukać podaną stronę internetową. Domyślne zachowanie zwraca adresy email oraz adresy ip zawarte w pliku strony. Istnieje kilka argumentów, najbardziej ogólnym jest http-grep.match, kóry pozwala wyszukać dane wyrażenie regularne.
- **dns-brute.nse**
  Za pomocą tego skryptu można przeszukać badanego hosta pod kątem subdomen.
- **mysql-empty-password.nse**
  Ten skrypt pozwala sprawdzić czy na danym serwerze mysql da się zalogować używając pustego hasła
- **http-headers.nse**
  Zwraca nagłówki HTTP w katalogu root i wyświetla je.

- **http-methods.nse**
  Służy do analizy opcji wspieranych przez serwer HTTP na hoście docelowym.
- **http-enum.nse**
  Służy do skanowania serwerów HTTP w celu pozyskania informacji o zasobach i usługach. Przeszukuje server pod kątem plików o znanych nazwach w celu rozpoznania popularnych aplikacji.

Wykonaj nmap -sC

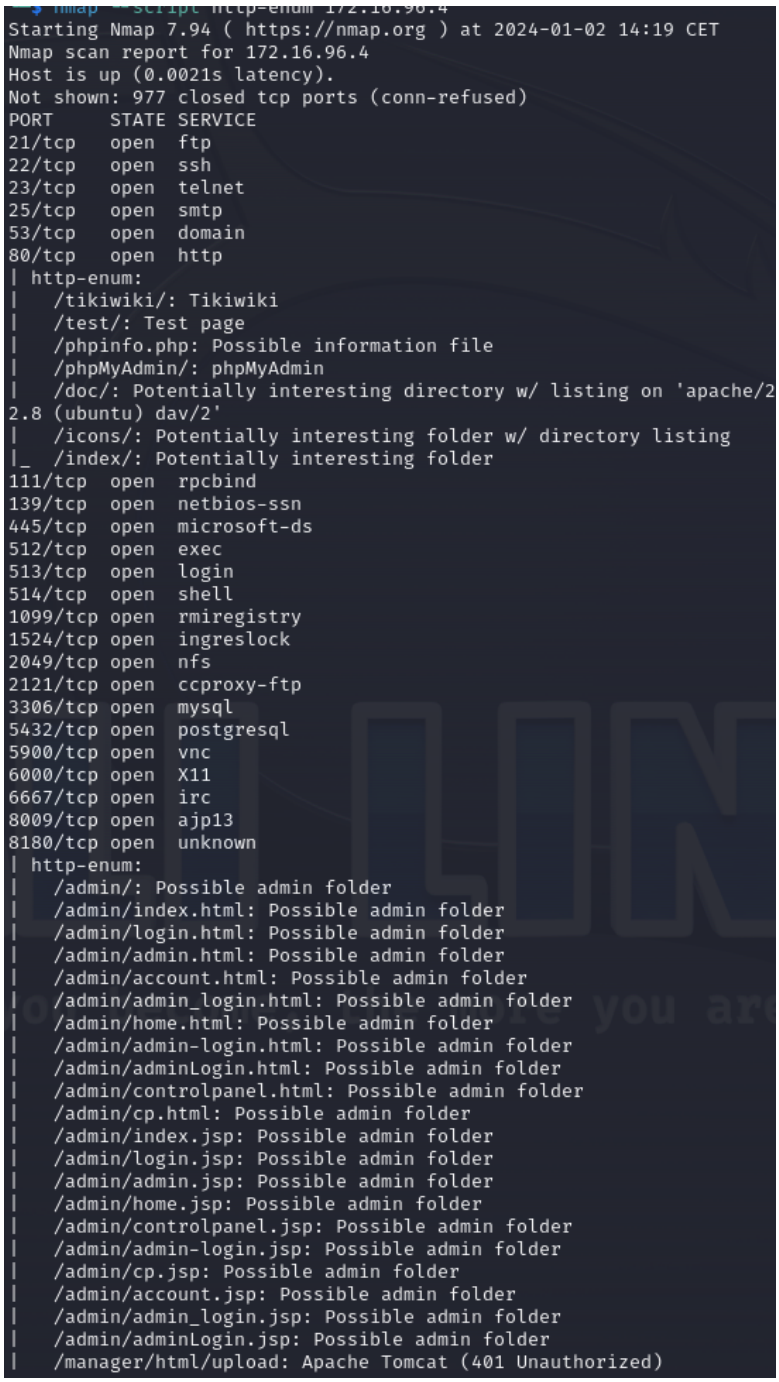
```
└─$ nmap -sC 172.16.96.4
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 13:51 CET
Nmap scan report for 172.16.96.4
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.16.96.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet
25/tcp   open  smtp
|_ssl-date: 2024-01-02T12:52:46+00:00; -1s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 1024000
0, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizati
onName=OCOSA/stateOrProvinceName=There is no such thing outside US/co
untryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      33051/tcp   mountd
|   100005  1,2,3      47034/udp   mountd
|   100021  1,3,4      37584/udp   nlockmgr
|   100021  1,3,4      45160/tcp   nlockmgr
|   100024  1          45942/tcp   status
|_  100024  1          55678/udp   status
139/tcp  open  netbios-ssn
```

```
|   100005  1,2,3      33051/tcp   mountd
|   100005  1,2,3      47034/udp   mountd
|   100021  1,3,4      37584/udp   nlockmgr
|   100021  1,3,4      45160/tcp   nlockmgr
|   100024  1          45942/tcp   status
|_  100024  1          55678/udp   status
139/tcp  open  netbios-ssn
445/tcp  open  X-Powere0
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: SwitchToSSLAfterHandshake, LongColumnFlag, Spe
aks41ProtocolNew, Support41Auth, SupportsTransactions, SupportsCompre
ssion, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: LERMjP2HSGJ{P[Y.w2.2
5432/tcp open  postgresql
|_ssl-date: 2024-01-02T12:52:46+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizati
onName=OCOSA/stateOrProvinceName=There is no such thing outside US/co
untryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11
6667/tcp open  irc
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:00:19
|   source ident: nmap
|   source host: BE1B162D.70F3DAAE.168799A3.IP
|_  error: Closing Link: setpwgmux[172.16.96.2] (Quit: setpwgmux)
8009/tcp open  ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetB
IOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h14m58s, deviation: 2h30m00s, median: -1s
| smb-security-mode:
|   account_used: <blank>
```

```
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-01-02T07:51:49-05:00

Nmap done: 1 IP address (1 host up) scanned in 71.64 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

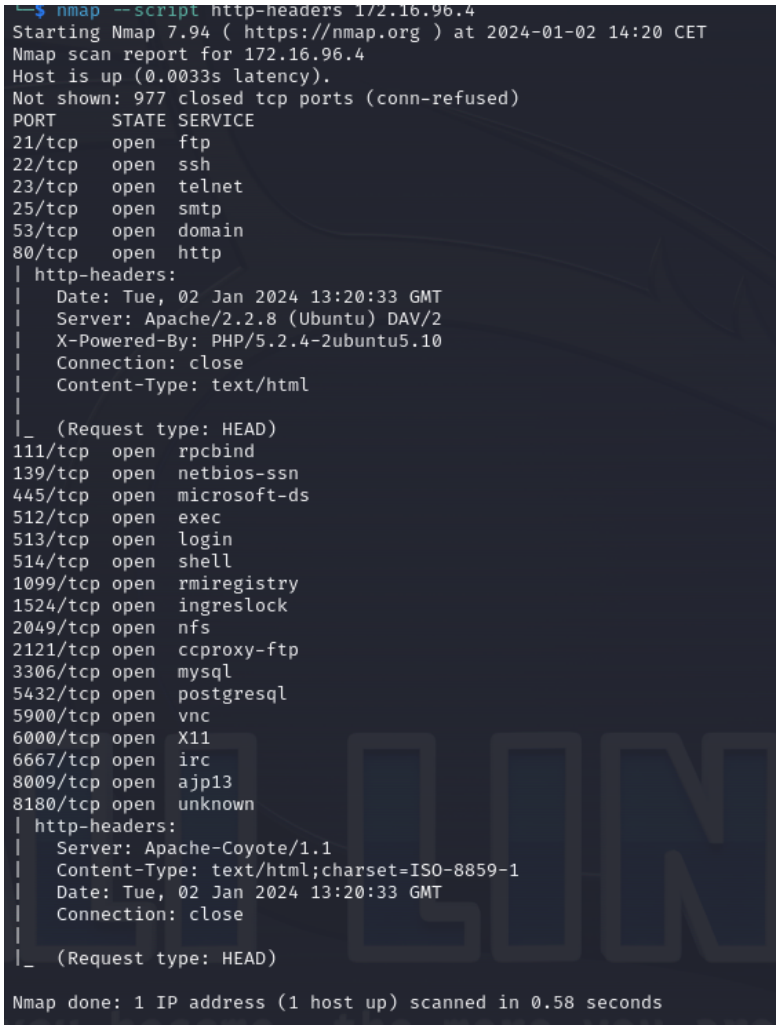
Wykonaj nmap –script http-enum,http-headers,http-methods,http-phpversion

- **http-enum**



```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 14:19 CET
Nmap scan report for 172.16.96.4
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2
2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
|   /admin/home.jsp: Possible admin folder
|   /admin/controlpanel.jsp: Possible admin folder
|   /admin/admin-login.jsp: Possible admin folder
|   /admin/cp.jsp: Possible admin folder
|   /admin/account.jsp: Possible admin folder
|   /admin/admin_login.jsp: Possible admin folder
|   /admin/adminLogin.jsp: Possible admin folder
|   /manager/html/upload: Apache Tomcat (401 Unauthorized)
```

- **http-headers**



- **http-methods**

```
└─$ nmap --script http-methods 172.16.96.4
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 14:21 CET
Nmap scan report for 172.16.96.4
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

- **http-phpversion**

```
└─$ nmap --script http-php-version 172.16.96.4
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 14:22 CET
Nmap scan report for 172.16.96.4
Host is up (0.0034s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
| http-php-version: Versions from logo query (less accurate): 5.1.3 -
 5.1.6, 5.2.0 - 5.2.17
| Versions from credits query (more accurate): 5.2.3 - 5.2.5, 5.2.6RC
3
|_Version from header x-powered-by: PHP/5.2.4-2ubuntu5.10
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

Zadanie IX

IX. Użyj narzędzia amap na wybranej maszynie wirtualnej i porównaj

wyniki z wynikami uzyskanymi podczas skanowania nmap amap -bq 172.16.96.x 80 3306

Wyniki uzyskane przez *amap* dotyczą konkretnych usług działających na danych portach. Są one precyzyjniejsze niż wyniki uzyskane przez nmap, jednak mniej wszechstronne. *Amap* skupia się głównie na usługach i ich wersjach. Amap może być szybkie i wygodne jeśli zależy nam na szybkim i Stosunkowo dokładnym przeanalizowaniu charakterystyki konkretnych portów i usług na nich działających.

2 Pytania

Pytanie I

Czy wyniki uzyskane przez nmap są wiarygodne?

Wyniki uzyskane przez nmap raczej powinny być wiarygone, jeśli użytkownik wie z jakimi sytemami ma do czynienia i rozumie działanie protokołów oraz poszczególne opcje. Jednak zależą one od wielu zmiennych i niedoświadczony użytkownik może uzyskać wyniki nieprawdziwe. Na wyniki może wpłynąć na przykład konfiguracja stosu TCP w danym systemie. Może to prowadzić to nieprawidłowych wyników dla danych metod skanowania. Specyfikacja sieci także może wpłynąć na wyniki. Konfiguracja firewalla lub inne zabezpieczenia mogą utrudnić / uniemożliwić skanowanie.

Pytanie II

Czy uzyskane informacje o hoście docelowym zależą od opcji skanowania?

Zazwyczaj różne opcje mają wpływ na uzyskane informacje. Opcje te wpływają na sposób komunikacji z hostem oraz na informacje które chcemy uzyskać podczas skanowania. Skanowania -sS wykrywa otwarte porty, z kolei skanowanie -sV skupia się bardziej na usługach na konkretnych portach. Opcja -O próbuje zidentyfikować system operacyjny działający na hoście. Dodatkowo różne skrypty pozwalają na uzyskiwanie precyzyjnych informacji na konkretniejsze tematy z wąskich dziedzin. Ustawienia czasu -T wpływają na agresywność skanowania. Szybsze skanowanie kompromisuje dokładność i może zgubić częśc informacji. Dodatkowo, konfiguracja hosta ma również znaczenie. Różne opcje skanowania wykorzystują różne flagi TCP, co może prowadzić do zależności od konfiguracji hosta.

Pytanie III

Czy można używać nmap do skanowania hostów bez pozwolenia?

Odpowiedź na to pytanie nie jest jednoznaczna i zależy od praw w danej lokalzacji geograficznej. Samo narzędzie nmap raczej nie jest wprost nielegalne. Przeprowadzenie skanowania bez pozwolenia może jednak być traktowane jako naruszenie prywatności i może prowadzić do konsekwencji prawnych. Często jest także wątpliwe etycznie. Zawsze powinniśmy uzyskać zgodę przed skanowaniem cudzej sieci.