

Wrocław, 20.10.2020

# Bezpieczeństwo sieci komputerowych

## Laboratorium 1

### Zagrożenia i podatności sieci komputerowych

Prowadzący: dr inż. Marcin Markowski

Autorka: Agnieszka Płoszaj 218353

Zadanie zostało wykonane przy wykorzystaniu 2 komputerów:

- 1 komputer to macOS z windows 7 professional w postaci maszyny wirtualnej (VirtualBox) — pełniący rolę serwera.
- 2 komputer z systemem windows 8.1 — pełniący rolę stacji roboczej.

#### Zadanie 1

Na serwerze zostały uruchomione 4 usługi:

- HTTP oraz FTP — przy pomocy Menedżera Internetowych Usług Informacyjnych,
- TFTP — przy pomocy programu tftpd32,
- TELNET — przy pomocy programu hk-telnet-server.

#### Zadanie 2

Na stacji roboczej zostały także uruchomione wszystkie 4 usługi:

- HTTP — przeglądarka internetowa
- FTP — Filezilla
- TELNET — Putty
- TFTP — Tftpd64.

Na ilustracji 1 widać efekt wywołania komendy *netstat* na stacji roboczej. Jednak polecenie to bez użycia dodatkowych opcji pokazuje jedynie listę otwartych gniazd. Żeby zobaczyć gniazda nasłuchujące potrzebne jest użycie opcji *-a*, efekty tego polecenia można zobaczyć na ilustracji 2.

```
C:\Users\Agnieszka>netstat
Active Connections

Proto Local Address          Foreign Address         State
TCP   127.0.0.1:1030          Coquette:5354           ESTABLISHED
TCP   127.0.0.1:1031          Coquette:5354           ESTABLISHED
TCP   127.0.0.1:1392          Coquette:2994           ESTABLISHED
TCP   127.0.0.1:2994          Coquette:1392           ESTABLISHED
TCP   127.0.0.1:5354          Coquette:1030           ESTABLISHED
TCP   127.0.0.1:5354          Coquette:1031           ESTABLISHED
TCP   192.168.0.129:1161      51.103.5.159:https      ESTABLISHED
TCP   192.168.0.129:1163      lo-in-f 188:5228        ESTABLISHED
TCP   192.168.0.129:1184      13.68.168.63:https      ESTABLISHED
TCP   192.168.0.129:1297      AGA:telnet              ESTABLISHED
TCP   192.168.0.129:1420      13.88.181.35:https      ESTABLISHED
TCP   192.168.0.129:1426      AGA:ftp                 ESTABLISHED
TCP   192.168.0.129:1428      AGA:http                ESTABLISHED
TCP   192.168.0.129:1429      AGA:http                ESTABLISHED
```

Ilustracja 1 Polecenie *netstat*.

```

C:\Users\Agnieszka>netstat -a
Active Connections

```

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	Coquette:0	LISTENING
TCP	0.0.0.0:445	Coquette:0	LISTENING
TCP	0.0.0.0:554	Coquette:0	LISTENING
TCP	0.0.0.0:1025	Coquette:0	LISTENING
TCP	0.0.0.0:1026	Coquette:0	LISTENING
TCP	0.0.0.0:1027	Coquette:0	LISTENING
TCP	0.0.0.0:1028	Coquette:0	LISTENING
TCP	0.0.0.0:1029	Coquette:0	LISTENING
TCP	0.0.0.0:1032	Coquette:0	LISTENING
TCP	0.0.0.0:1060	Coquette:0	LISTENING
TCP	0.0.0.0:1061	Coquette:0	LISTENING
TCP	0.0.0.0:2869	Coquette:0	LISTENING
TCP	0.0.0.0:10243	Coquette:0	LISTENING
TCP	127.0.0.1:1030	Coquette:5354	ESTABLISHED
TCP	127.0.0.1:1031	Coquette:5354	ESTABLISHED
TCP	127.0.0.1:1392	Coquette:2994	ESTABLISHED
TCP	127.0.0.1:2994	Coquette:1392	ESTABLISHED
TCP	127.0.0.1:5354	Coquette:0	LISTENING
TCP	127.0.0.1:5354	Coquette:1030	ESTABLISHED
TCP	127.0.0.1:5354	Coquette:1031	ESTABLISHED
TCP	127.0.0.1:27015	Coquette:0	LISTENING
TCP	192.168.0.129:139	Coquette:0	LISTENING
TCP	192.168.0.129:1161	51.103.5.159:https	ESTABLISHED
TCP	192.168.0.129:1163	lo-in-f188:5228	ESTABLISHED
TCP	192.168.0.129:1184	13.68.168.63:https	ESTABLISHED
TCP	192.168.0.129:1297	AGA:telnet	ESTABLISHED
TCP	192.168.0.129:1420	13.88.181.35:https	ESTABLISHED
TCP	192.168.0.129:1426	AGA:ftp	ESTABLISHED
TCP	192.168.0.129:1428	AGA:http	ESTABLISHED
TCP	192.168.0.129:1429	AGA:http	ESTABLISHED
TCP	[::]:135	Coquette:0	LISTENING
TCP	[::]:445	Coquette:0	LISTENING
TCP	[::]:554	Coquette:0	LISTENING
TCP	[::]:1025	Coquette:0	LISTENING
TCP	[::]:1026	Coquette:0	LISTENING
TCP	[::]:1027	Coquette:0	LISTENING
TCP	[::]:1028	Coquette:0	LISTENING
TCP	[::]:1029	Coquette:0	LISTENING
TCP	[::]:1032	Coquette:0	LISTENING
TCP	[::]:1061	Coquette:0	LISTENING
TCP	[::]:2869	Coquette:0	LISTENING
TCP	[::]:10243	Coquette:0	LISTENING

Ilustracja 2 Polecenie *netstat -a*.

Na podstawie wyników powyższych poleceń można zobaczyć, że stacja robocza nawiązała sesje z usługami hostowanymi przez serwer (AGA:telnet, AGA:ftp, AGA:http). (Usługa TFTP była widoczna tylko z poziomu programu *Wireshark*).

Widoczne są tu również porty o 2 stanach:

- LISTENING - gniazdo nasłuchuje nadchodzących połączeń,
- ESTABLISHED - gniazdo zestawilo połączenie.

Jednak, żeby opisać otwarte porty na stacji roboczej potrzebne było wykorzystanie opcji *-b*, która u dołu każdego portu/ połączenia [w nawiasie], wypisuje nazwę pliku wykonywalnego, który jest zaangażowany w jego tworzenie. W moim przypadku są to aplikacje potrzebne do wykonania laboratorium, antywirus, eksplorator windows oraz aplikacje firmy Apple, co można zobaczyć na ilustracji 3.

```
C:\Windows\system32>netstat -b

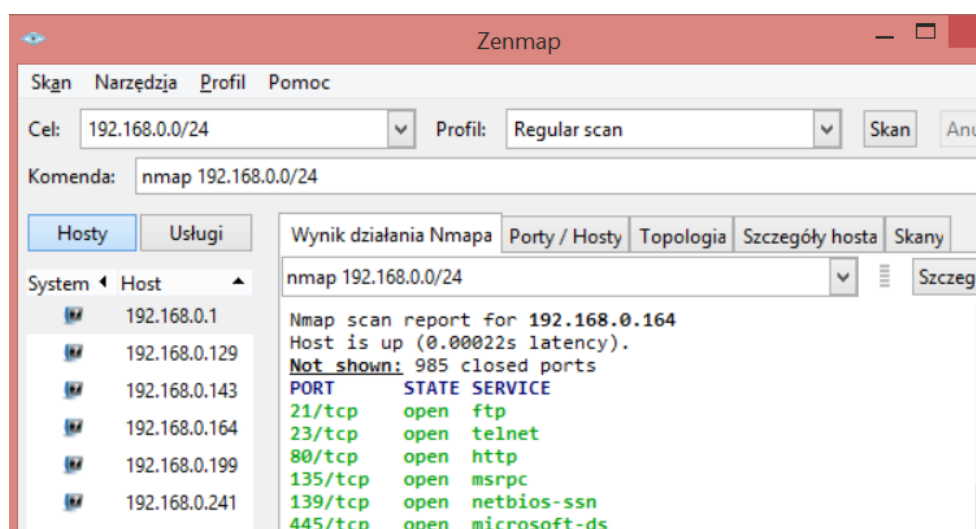
Active Connections

    Proto Local Address          Foreign Address        State
    TCP    127.0.0.1:1030         Coquette:5354         ESTABLISHED
    [AppleMobileDeviceService.exe]
    TCP    127.0.0.1:1031         Coquette:5354         ESTABLISHED
    [AppleMobileDeviceService.exe]
    TCP    127.0.0.1:2222         Coquette:2994         ESTABLISHED
    [tftpd64.exe]
    TCP    127.0.0.1:2994         Coquette:2222         ESTABLISHED
    [tftpd64.exe]
    TCP    127.0.0.1:5354         Coquette:1030         ESTABLISHED
    [mDNSResponder.exe]
    TCP    127.0.0.1:5354         Coquette:1031         ESTABLISHED
    [mDNSResponder.exe]
    TCP    192.168.0.129:1033     51.103.5.159:https    ESTABLISHED
    [Explorer.EXE]
    TCP    192.168.0.129:2205     13.68.168.63:https    ESTABLISHED
    [NortonSecurity.exe]
    TCP    192.168.0.129:2259     AGA:telnet            ESTABLISHED
    [putty.exe]
    TCP    192.168.0.129:2463     lr-in-f188:5228       ESTABLISHED
    [opera.exe]
    TCP    192.168.0.129:2601     13.88.181.35:https    ESTABLISHED
    [NortonSecurity.exe]
    TCP    192.168.0.129:2602     AGA:ftp               ESTABLISHED
    [filezilla.exe]
    TCP    192.168.0.129:2605     AGA:http              ESTABLISHED
    [opera.exe]
    TCP    192.168.0.129:2606     AGA:http              ESTABLISHED
    [opera.exe]
    TCP    192.168.0.129:2607     n30-03-09-vip:https   ESTABLISHED
    [opera.exe]
```

Ilustracja 3 Polecenie *netstat -b*.

### Zadanie 3

Następnie został uruchomiony program *nmap* i uruchomione zostało na nim skanowanie całej sieci (ilustracja 4). Wśród wyszukanych hostów znalazł się serwer (192.168.0.164) oraz 5 innych hostów.



Ilustracja 4 Program *nmap*.

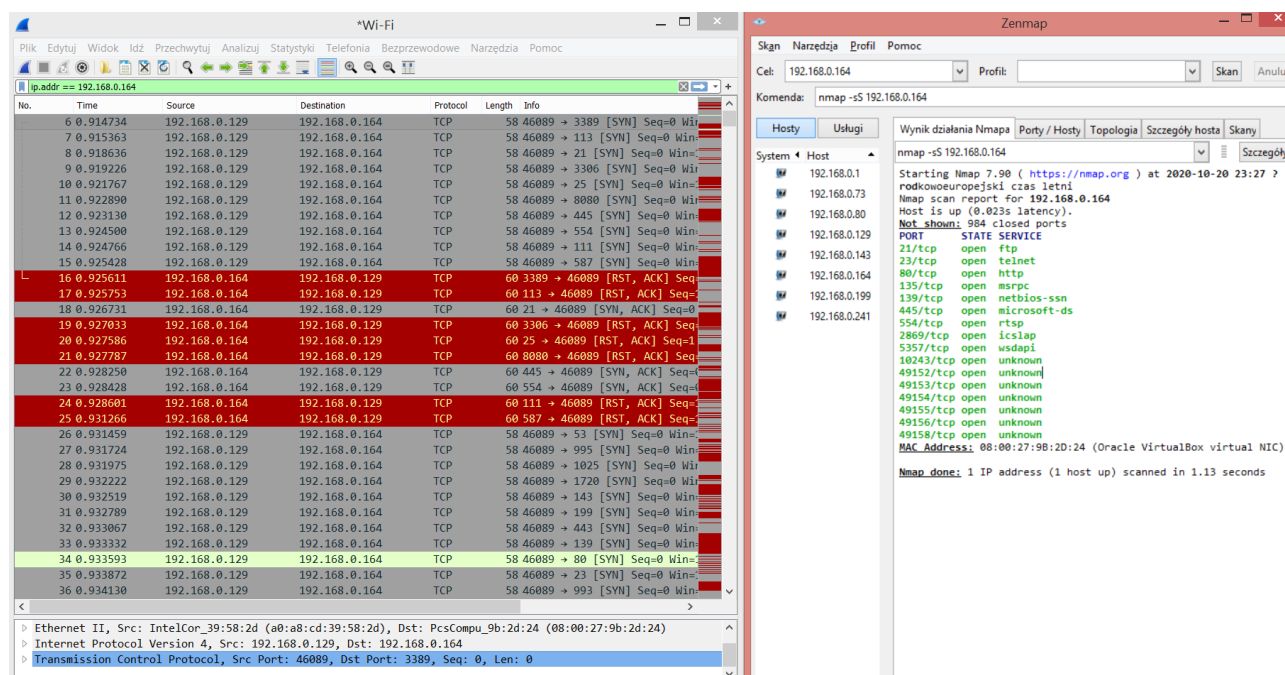
W następnej kolejności program nmap przeskanował porty od 0-1000 na serwerze (komenda `-p 0-1000`, jednakże jest to również ustawienie domyślne).

Żeby lepiej było widać wyniki dla połączeń z serwerem w *Wireshark* został użyty następujący filtr przechwytywania: `ip.addr == 192.168.0.164`.

Za pierwszym razem (ilustracja 5) użyłam opcji **-sS** (skanowanie SYN), która to jest domyślną metodą skanowania. Polega ona na połowicznym otwarciu połączenia.

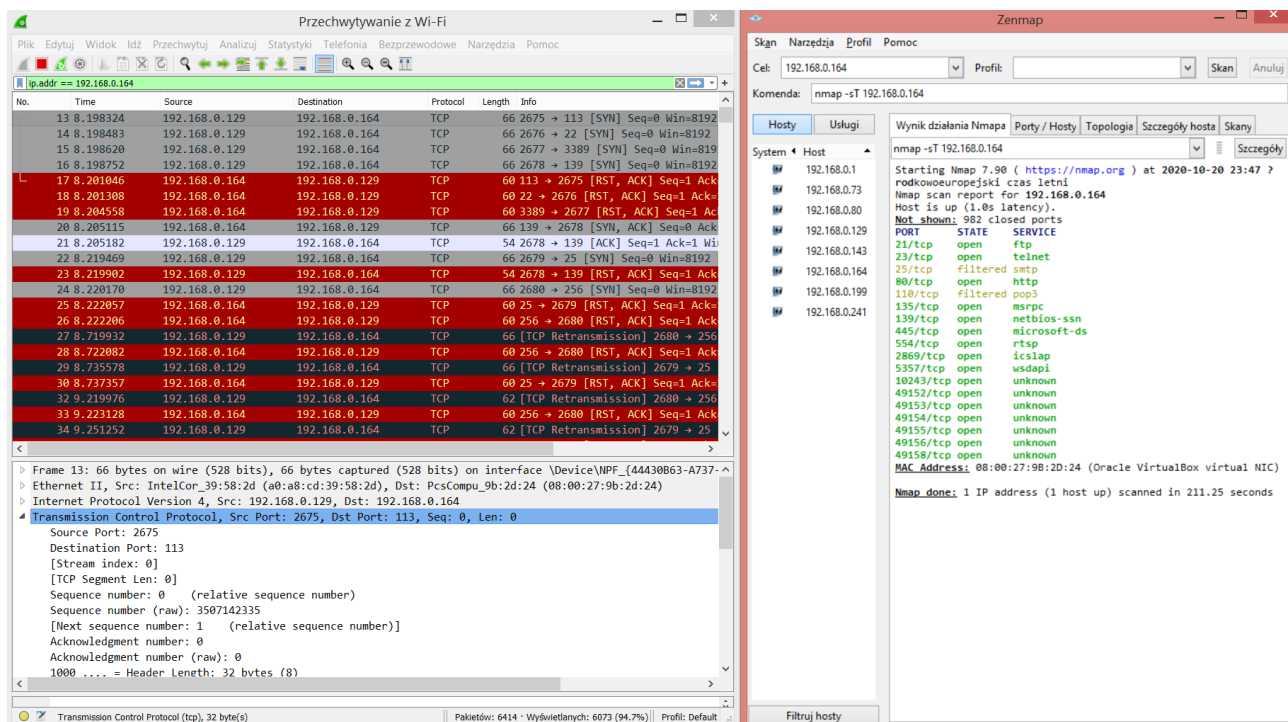
Wysyła **[SYN]** (czyli ustawioną flagę TCP Syn) natomiast w ramach odpowiedzi może otrzymać:

- **[SYN/ACK]** (ustawione 2 flagi TCP: Syn oraz Acknowledgment) — port jest otwarty,
- **[RST/ACK]** (ustawione 2 flagi TCP: Reset oraz Acknowledgment) — port jest zamknięty.



Ilustracja 5 Skanowanie SYN.

Za drugim razem (ilustracja 6) użyłam opcji **-sT** (skanowanie TCP connect), która polega na wywoływaniu funkcji systemowej `connect()` i otwarciu pełnego połączenia.



Ilustracja 6 Skanowanie TCP connect.

Pierwszą zauważalną różnicą pomiędzy wymienionymi powyżej opcjami jest czas potrzebny na uzyskanie wyników skanowania. Dla opcji **-sS** jest on bardzo krótki. Najprawdopodobniej wynika to z tego, że w przypadku tej opcji połączenie otwierane jest tylko połowicznie.

Różnią się też one możliwymi odpowiedziami flagi TCP, gdyż w przypadku drugiej opcji po uzyskaniu odpowiedzi **[SYN/ACK]** można również uzyskać:

- **[ACK]** (ustawiona flaga TCP: Acknowledgment) — czyli wysłanie potwierdzenia, które powoduje ustawienie stanu ESTABLISHED.

Różnica ta również wynika z typu połączenia.

Możliwe sekwencje w przypadku opcji **-sT**:

- **SYN** (Seq=0) → **SYN/ACK** (Seq=0, Ack=1) → **ACK** (Seq=1, Ack=1)
- **SYN** (Seq=0) → **RST/ACK** (Seq=1, Ack=1)

Możliwe sekwencje w przypadku opcji **-sS**:

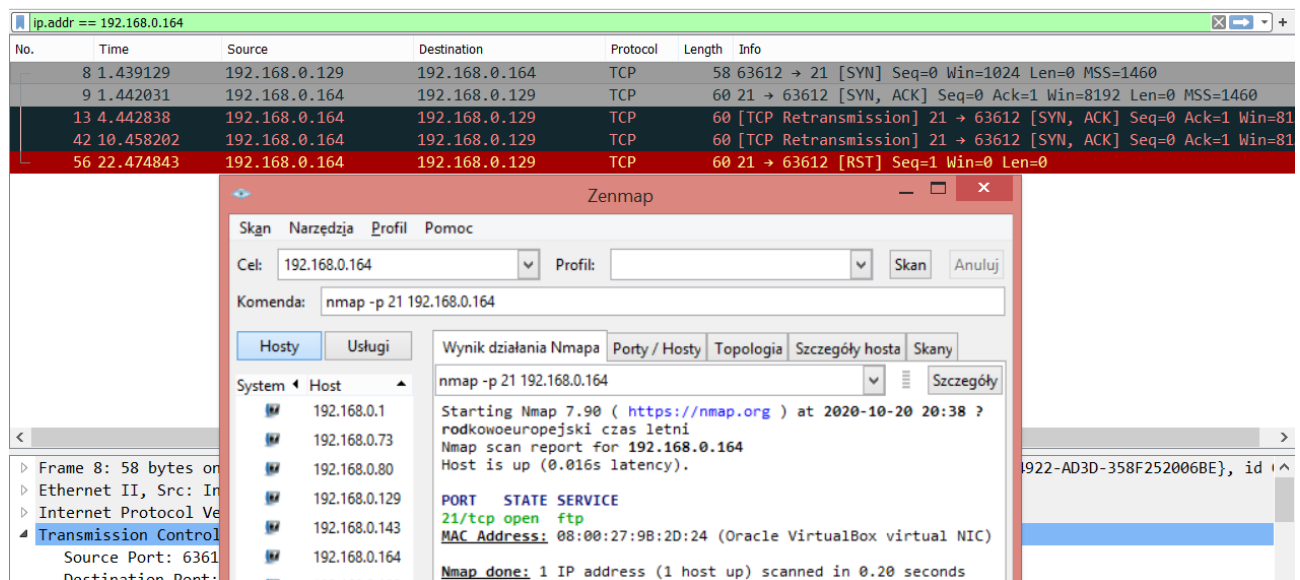
- **SYN** (Seq=0) → **SYN/ACK** (Seq=0, Ack=1)
- **SYN** (Seq=0) → **RST/ACK** (Seq=1, Ack=1)

Pakiety skanujące charakteryzują się wyżej opisanymi możliwymi sekwencjami ich występowania (oczywiście możliwa jest jeszcze sekwencja uwzględniająca retransmisję), które różnią się pomiędzy sobą w zależności od użytych opcji skanowania w programie *nmap*. Łatwo jest je więc rozpoznać. Jednak, żeby lepiej zobrazować różnice, wykonałam dwa dodatkowe skanowania tym razem dla konkretnego portu. Wybrałam port 21 (FTP).

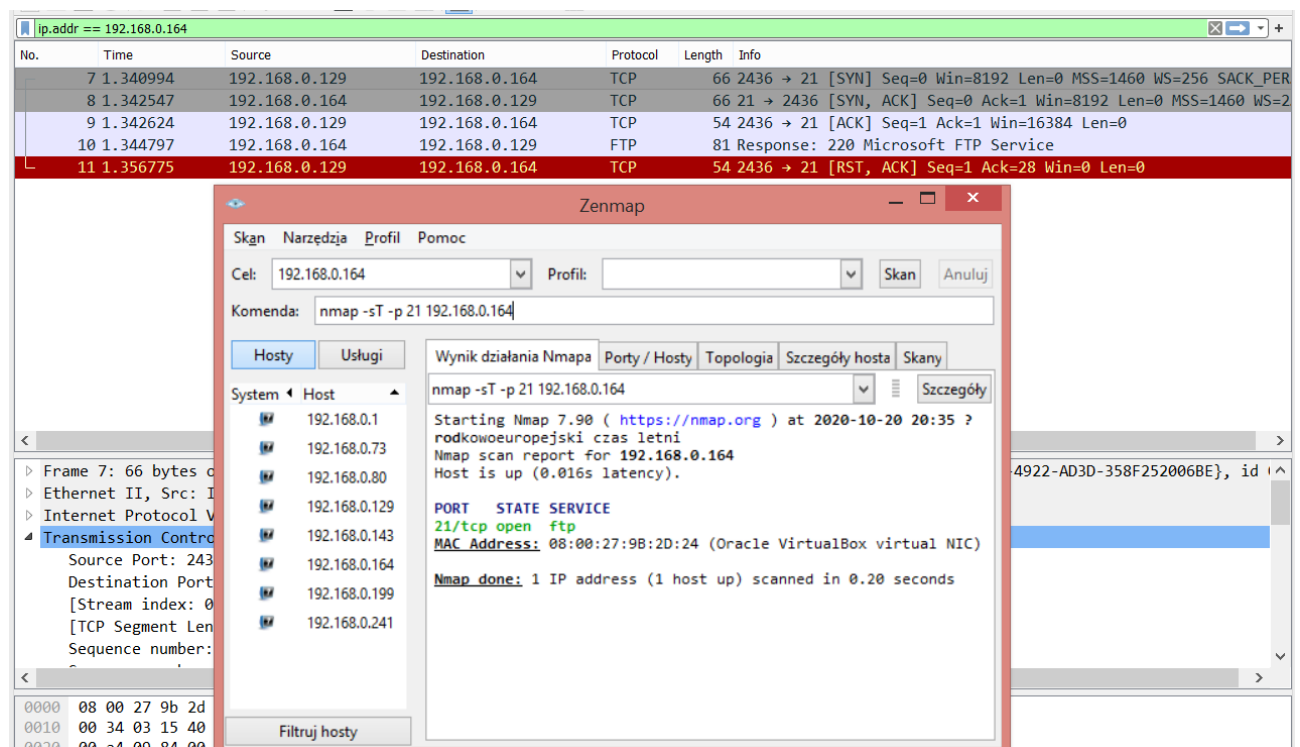
Pierwsze skanowanie: *nmap -p 21 192.168.0.164* — ilustracja 7.

Drugie skanowanie: *nmap -sT -p 21 192.168.0.164* — ilustracja 8.

Jak widać na poniższych ilustracjach tylko w przypadku skanowania TCP connect, możemy uruchomić protokół FTP, właśnie przez wzgląd na różnicę pomiędzy otwieraniem pełnego połączenia, a połowicznego.

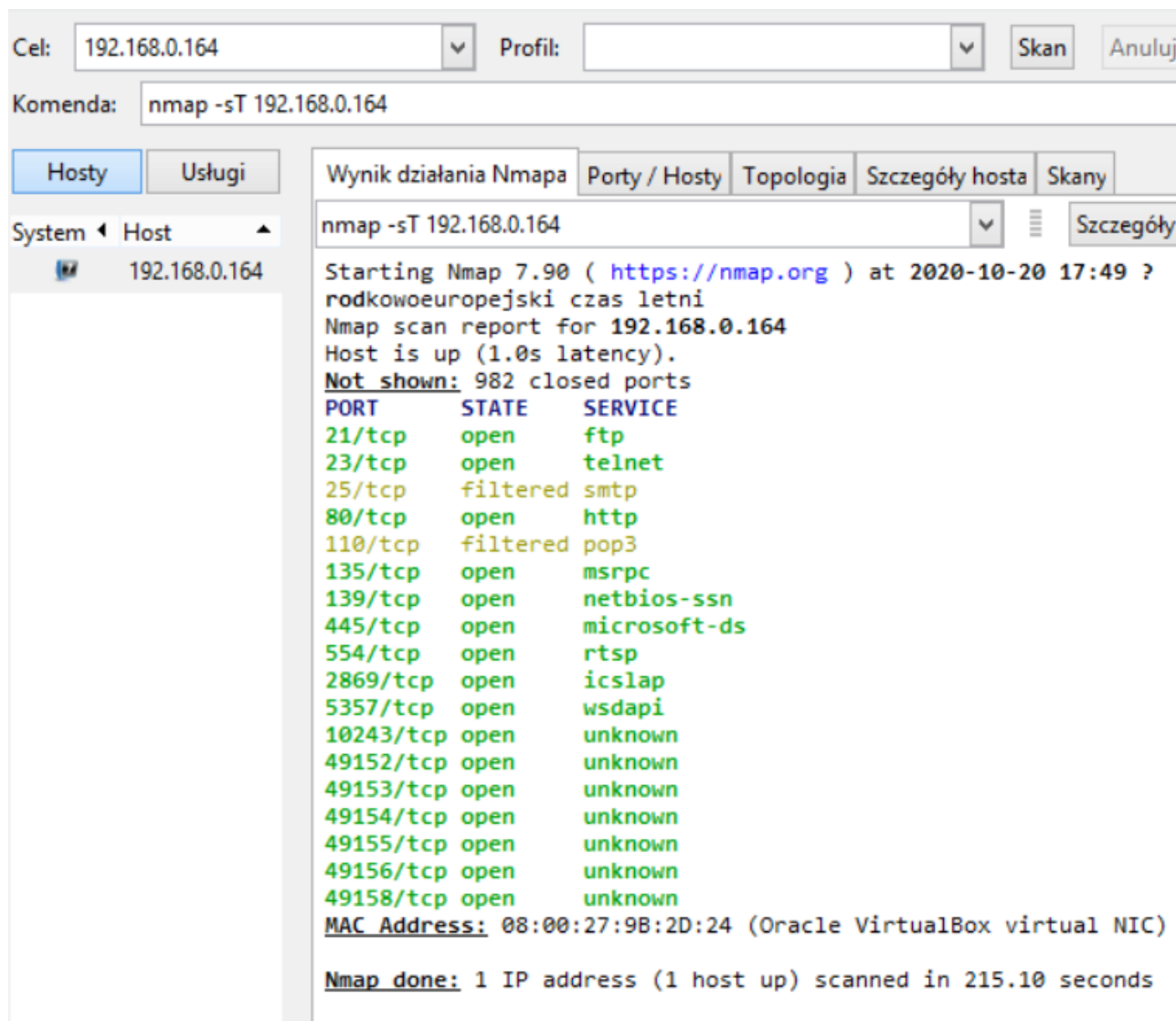


Ilustracja 7 Skanowanie SYN dla portu 21.



Ilustracja 8 Skanowanie TCP connect dla portu 21.

Skanowanie TCP connect może dodatkowo wyświetlać w *nmap* porty, które mają stan: *filtrowany*, co oznacza, że *nmap* nie może określić czy port jest otwarty z powodu filtrowania komunikacji (ilustracja 9).



Cel: 192.168.0.164 Profil: Skan Anuluj

Komenda: nmap -sT 192.168.0.164

Hosty Usługi Wynik działania Nmapa Porty / Hosty Topologia Szczegóły hosta Skany

System Host 192.168.0.164

nmap -sT 192.168.0.164 Szczegóły

Starting Nmap 7.90 ( <https://nmap.org> ) at 2020-10-20 17:49 ?  
rodkowoeuropejski czas letni  
Nmap scan report for 192.168.0.164  
Host is up (1.0s latency).  
Not shown: 982 closed ports

PORT	STATE	SERVICE
21/tcp	open	ftp
23/tcp	open	telnet
25/tcp	filtered	smtp
80/tcp	open	http
110/tcp	filtered	pop3
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
554/tcp	open	rtsp
2869/tcp	open	icslap
5357/tcp	open	wsdapi
10243/tcp	open	unknown
49152/tcp	open	unknown
49153/tcp	open	unknown
49154/tcp	open	unknown
49155/tcp	open	unknown
49156/tcp	open	unknown
49158/tcp	open	unknown

MAC Address: 08:00:27:9B:2D:24 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 215.10 seconds

Ilustracja 9 Skanowanie TCP connect — nmap.



Na stacji roboczej wywołane zostało polecenie *arp -a*, którego wynik widać na ilustracji 10. Jednym z adresów ip przydzielonych dynamicznie jest adres **192.168.0.143**, który reprezentuje inny komputer, podłączony do tej samej sieci LAN, z którym stacja robocza się aktualnie kontaktuje.

W poniższej tabeli arp figurują również adresy przydzielane statycznie jak np.: **255.255.255.255**, który jest specjalnym adresem bramy domyślnej. Jest przydatny w sytuacji, kiedy chce się wysłać coś w określonej sieci, bez konieczności zastanawiania się nad konkretnym adresem ip. Jako więc, że jest to brama domyślna, to adres MAC jest spójny z adresem MAC bramy domyślnej podsieci (**192.168.0.0/24**).

```
C:\Windows\system32>arp -a
```

```
Interface: 192.168.0.129 --- 0x3
```

Internet Address	Physical Address	Type
192.168.0.1	90-5c-44-dd-1f-08	dynamic
192.168.0.143	98-de-d0-04-a1-81	dynamic
192.168.0.164	08-00-27-9b-2d-24	dynamic
192.168.0.206	a8-db-03-22-3f-73	dynamic
192.168.0.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Ilustracja 10 Tabela arp.

Na stacji roboczej wywołane zostało polecenie *route print*, którego wynik widać na ilustracji 11. Zgodnie z tabelą routingu stacja robocza korzysta z trasy 1: network destination: 0.0.0.0 wysyłając pakiety do internetu. Trasa ta jako „miejsce docelowe w sieci” ma podany adres **0.0.0.0** - który oznacza wszystkie adresy w sieci, tak samo z maską sieci.

Miejscem docelowym w sieci tras od 2 do 4 jest localhost, który służy do wymiany informacji wewnątrz hosta.

Miejscem docelowym w sieci tras od 5 do 7 jest obecna podsieć, z czego adres 192.168.0.255 jest adresem broadcast tej podsieci.

Miejscem docelowym w sieci tras od 8 do 9 są adresy multicast.

Miejscem docelowym w sieci tras od 10 do 11 jest specjalny adres bramy domyślnej.

```
C:\Windows\system32>route print
=====
Interface List
 5...a0 a8 cd 39 58 2e .....Karta Microsoft Wi-Fi Direct Virtual Adapter
 4...28 d2 44 a3 d6 ba .....Kontroler Realtek PCIe GBE Family Controller
 3...a0 a8 cd 39 58 2d .....Intel(R) Wireless-N 7260
 1.....Software Loopback Interface 1
 6...00 00 00 00 00 00 00 e0 Karta Microsoft ISATAP #2
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
 0.0.0.0                    0.0.0.0          192.168.0.1      192.168.0.129    25
 127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
 127.0.0.1                  255.255.255.255  On-link          127.0.0.1        306
 127.255.255.255            255.255.255.255  On-link          127.0.0.1        306
 192.168.0.0                255.255.255.0    On-link          192.168.0.129    281
 192.168.0.129              255.255.255.255  On-link          192.168.0.129    281
 192.168.0.255              255.255.255.255  On-link          192.168.0.129    281
 224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
 224.0.0.0                  240.0.0.0        On-link          192.168.0.129    281
 255.255.255.255            255.255.255.255  On-link          127.0.0.1        306
 255.255.255.255            255.255.255.255  On-link          192.168.0.129    281
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
 1      306 ::1/128                      On-link
 3      281 fe80::/64                    On-link
 3      281 fe80::3831:e5b9:d6ad:c5fe/128
                                      On-link
 1      306 ff00::/8                      On-link
 3      281 ff00::/8                      On-link
=====
Persistent Routes:
None
```

Ilustracja 11 Tabela routingu.