

# Bezpieczeństwo sieci komputerowych

## Sprawozdanie z laboratorium

Data	Tytuł zajęć	Uczestnicy
26.10.2018 10:15	Zagrożenia i podatności sieci komputerowych	Iwo Bujkiewicz (226203) Bartosz Rodziewicz (226105)

### Budowa sieci

Sieć połączono zgodnie z rysunkiem.

Tabela adresacji w sieci:

Urządzenie	Adres IPv4
Router	10.0.0.1/16
PC (Linux)	10.0.0.2/16
PC (Windows)	10.0.0.3/16

Sieć została niepotrzebnie zaadresowana z maską **255.255.0.0**, co utrudniło nam kolejne zadania.

Umożliwiono łączenie się z CLI routera poprzez Telnet. Na komputerze z Linuxem uruchomiony został serwer WWW Apache 2.

# Netstat

Z komputera z Windowsem połączono się przez Telnet z routerem, oraz, przez przeglądarkę internetową, z serwerem WWW na komputerze z Linuxem. Rezultaty, a także wynik polecenia `netstat`, widoczne są poniżej.

The screenshot shows a Windows desktop environment with several open windows:

- A PuTTY terminal window titled "10.0.0.1 - PuTTY" showing a user access verification session.
- A Microsoft Edge browser window titled "Apache2 Ubuntu Default Page" showing the Apache2 configuration overview page.
- A Command Prompt window titled "C:\Windows\system32\cmd.exe" showing a list of active network connections.

The Command Prompt output (Active Connections) is as follows:

Proto	Local Address	Foreign Address	State
TCP	10.0.0.3:65132	10.0.0.1:telnet	ESTABLISHED
TCP	10.0.0.3:65134	KSSK4:http	ESTABLISHED
TCP	127.0.0.1:49190	KSSK:49191	ESTABLISHED
TCP	127.0.0.1:49191	KSSK:49190	ESTABLISHED
TCP	127.0.0.1:49194	KSSK:49195	ESTABLISHED
TCP	127.0.0.1:49195	KSSK:49194	ESTABLISHED
TCP	127.0.0.1:49215	KSSK:49216	ESTABLISHED
TCP	127.0.0.1:49216	KSSK:49226	ESTABLISHED
TCP	127.0.0.1:49226	KSSK:49225	ESTABLISHED
TCP	127.0.0.1:49538	KSSK:65039	ESTABLISHED
TCP	127.0.0.1:49539	KSSK:65038	ESTABLISHED
TCP	127.0.0.1:65071	KSSK:65072	ESTABLISHED
TCP	127.0.0.1:65072	KSSK:65071	ESTABLISHED
TCP	127.0.0.1:65130	KSSK:65130	ESTABLISHED

Analizując wybrane wpisy:

TCP	10.0.0.3:65132	10.0.0.1:telnet	ESTABLISHED
-----	----------------	-----------------	-------------

Otwarte zostało połączenie TCP z lokalnego portu 65132 do portu Telnet (23) routera.

TCP	10.0.0.3:65134	KSSK4:http	ESTABLISHED
-----	----------------	------------	-------------

Otwarte zostało połączenie TCP z lokalnego portu 65134 do portu HTTP (80) komputera z serwerem WWW.

## Skanowanie sieci za pomocą Nmap

SYN scan podsieci - `nmap -sS 10.0.0.0/16`

Najpierw wykonano *SYN scan* całej ustanowionej podsieci. Skanowanie rozpoczęło się od uzyskania adresów MAC wszystkich hostów w sieci za pomocą pakietów ARP.

Apply a display filter: <Ctrl>/

No.	Time	Source	Destination	Protocol	Length	Info
8493	125.328495	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.8.65? Tell 10.0.0.3
8494	125.328647	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.14.65? Tell 10.0.0.3
8495	125.328651	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.15.65? Tell 10.0.0.3
8496	125.328688	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.16.65? Tell 10.0.0.3
8497	125.329168	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.17.79? Tell 10.0.0.3
8498	125.329361	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.5.78? Tell 10.0.0.3
8499	125.329572	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.7.78? Tell 10.0.0.3
8500	125.329768	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.15.139? Tell 10.0.0.3
8501	125.329801	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.11.139? Tell 10.0.0.3
8502	125.330024	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.11.163? Tell 10.0.0.3
8503	125.330398	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.12.171? Tell 10.0.0.3
8504	125.330536	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.3.175? Tell 10.0.0.3
8505	125.330662	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.10.175? Tell 10.0.0.3
8506	125.330894	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.12.175? Tell 10.0.0.3
8507	125.331024	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.13.175? Tell 10.0.0.3
8508	125.331122	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.14.175? Tell 10.0.0.3
8509	125.331208	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.3.176? Tell 10.0.0.3
8510	125.331307	PcsCompu_94:47:a7	Broadcast	ARP	42	iwho has 10.0.4.176? Tell 10.0.0.3

Frame 8624: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: PcsCompu\_1c:1a:28 (08:00:27:1c:1a:28), Dst: PcsCompu\_94:47:a7 (08:00:27:94:47:a7)

Internet Protocol Version 4, Src Port: 80, Dst Port: 5845, Seq: 0, Ack: 1, Len: 0

Transmission Control Protocol, Src Port: 80, Dst Port: 5845, Seq: 0, Ack: 1, Len: 0

Source Port: 80  
Destination Port: 5845  
[Stream index: 50]  
[TCP Sequence Length: 0]  
Sequence number: 0 (relative sequence number)  
[Next sequence number: 0 (relative sequence number)]  
Acknowledgment number: 1 (relative ack number)  
0110 .... = Header Length: 24 bytes (6)  
+ Flags: 0x012 (SYN, ACK)  
000 ....., = Reserved: Not set  
..0 ....., = Reserve: Not set  
...0 ....., = Congestion Window Reduced (CWR): Not set  
....0..... = ECN-Echo: Not set  
....0..... = Urgent: Not set  
....1..... = Acknowledgment: Set  
....0..... = Push: Not set  
....0..... = Reset: Not set  
....1..... = Syn: Set  
....0..... = Fin: Not set  
[TCP Flags: ....A-S-]   
Window size scale factor: 256  
[Calculated window size: 29200]  
Checksum: 0xa045 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0

0000 08 00 27 94 47 a7 00 00 27 1c 14 28 00 00 45 00 ...G... .(.-E.  
0010 00 2c 00 00 46 00 00 49 05 26 c8 00 00 00 02 00 00 ...@ @ S.....  
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...P...PX-hx'.  
0030 72 10 da 45 00 00 02 00 00 00 00 00 00 00 00 00 00 00 ...E.....

Packets: 25650 · Displayed: 25650 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

Po uzyskaniu adresów MAC dostępnych hostów w sieci, komputer wykonujący skanowanie zaczął wysyłać pakiety SYN na każdy port znalezionego urządzenia.

The screenshot shows a Wireshark interface with several network captures. The main pane displays a list of captured frames, mostly showing TCP SYN and ACK packets between two hosts. A detailed view of frame 8756 is shown, with its bytes and hex dump. A terminal window titled 'C:\Windows\system32\cmd.exe' is open, running the command 'nmap -v -R 192.0.0.1-6'. The output shows the Nmap version (5.80), the target IP (192.0.0.1), and various service discovery results, including 'Service: tftp' on port 69 and 'Service: Oracle VM VirtualBox' on port 2271C.

Dla każdego zamkniętego portu urządzenie zwróciło odpowiedź **RST ACK**.

The figure shows a screenshot of the Wireshark application interface. The main pane displays a list of network frames captured on interface 'notwp'. The columns include No., Time, Source, Destination, Protocol, Length, and Info. Several frames are selected, with their details expanded in the bottom pane. The selected frames are from the 'Frame 8767' section, showing TCP segments between two hosts. The expanded details show fields like Sequence Number, Acknowledgment Number, and Flags (e.g., SYN, ACK). A yellow highlight covers the 'Flags' field of the selected frame.

The right side of the screen features a terminal window titled 'C:\Windows\system32\cmd.exe'. It displays the command 'nmap -v -R 10.0.0.1-16' and its output, which includes:

- SEE THE MAN PAGE (<https://nmap.org/book/man.html>) FOR MORE OPTIONS AND EXAMPLES
- C:\Users\Student>nmap -sS 10.0.0.0/16
- Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 11:37 Central European Daylight Time
- Scanning 10.0.0.0 - 10.0.0.255 (16 hosts)
- Host is up (0.00022s latency).
- Not shown: 999 closed ports
- PORT STATE SERVICE
- 2/tcp open telnet
- telnet (Cisco Systems)
- Nmap scan report for 10.0.0.2
- Host is up (0.00022s latency).
- Not shown: 999 closed ports
- PORT STATE SERVICE
- tcpmux (Oracle VM VirtualBox virtual NIC)

At the bottom of the terminal window, the prompt shows 'PC C:\Users\Student>'. The bottom status bar of the Wireshark window indicates 'Packets: 25650 - Displayed: 4875 (19.0%) - Dropped: 0 (0.0%)'.

Dla każdego otwartego portu otrzymano pakiet z flagami **SYN ACK**. Komputer inicjujący połączenie wysyłał następnie odpowiedź **RST**.

Rozmowa w przypadku zamkniętego portu:

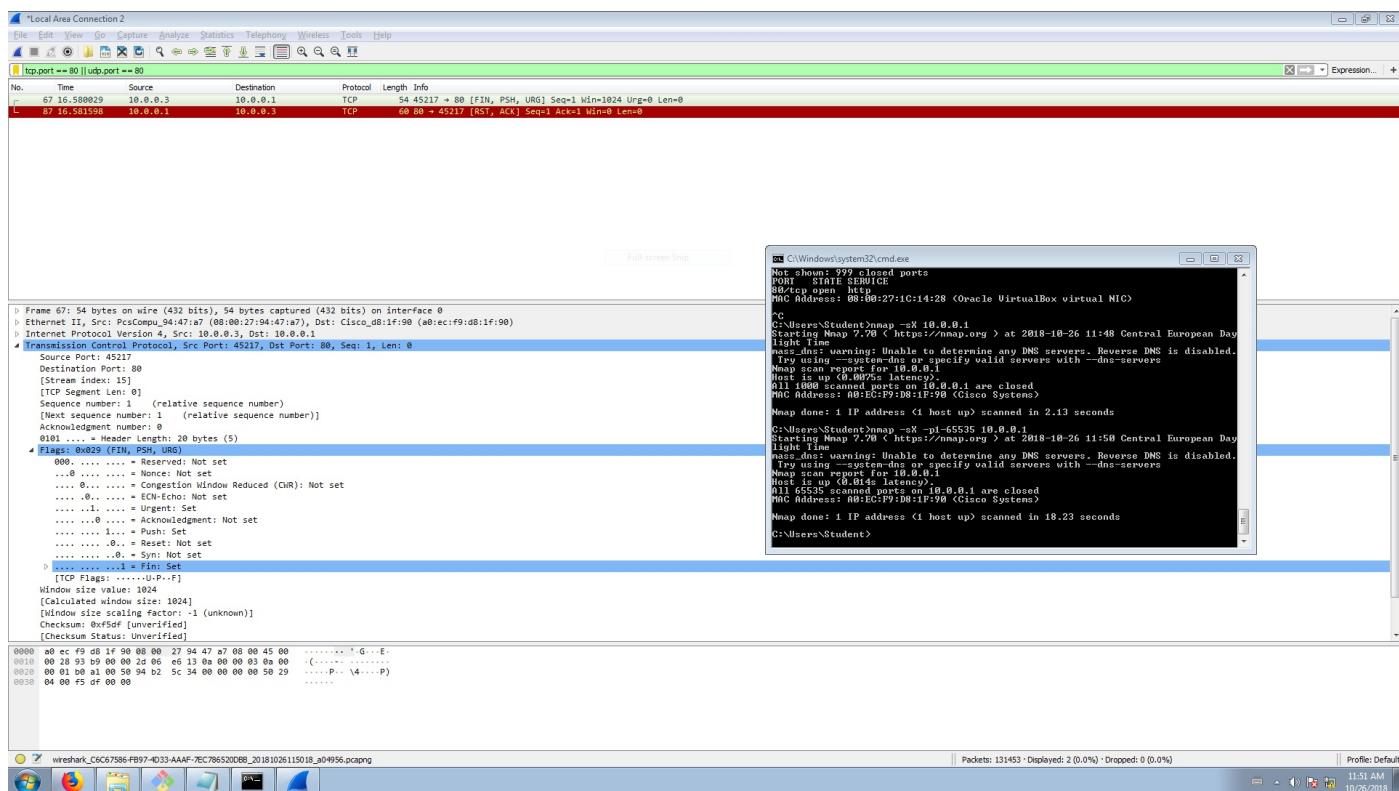
- A: **SYN** - rozpoczynam próbę połączenia
- B: **RST ACK** - otrzymałem, odmawiam połączenia

Rozmowa w przypadku otwartego portu:

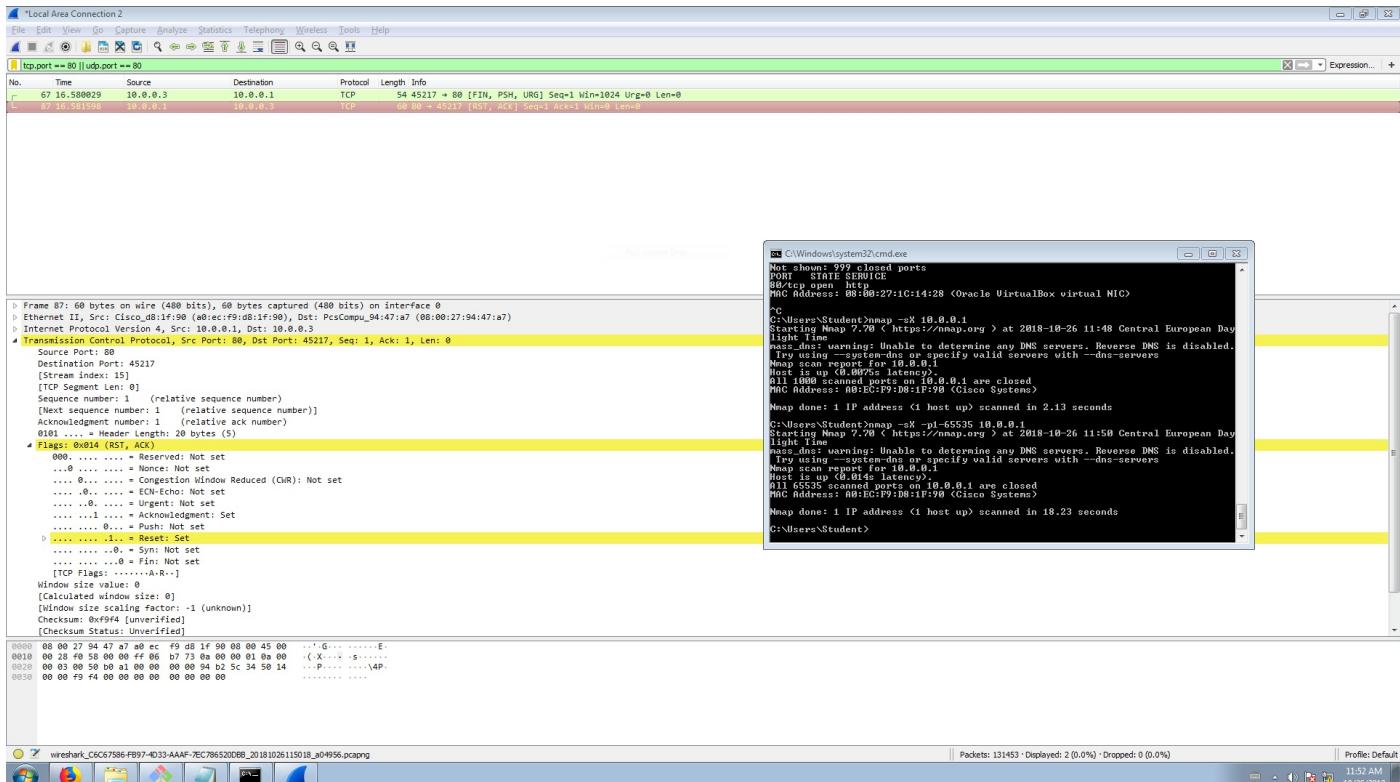
- A: **SYN** - rozpoczynam próbę połączenia
- B: **SYN ACK** - otrzymałem, gotów do połączenia
- A: **RST** - zamykam połączenie

Xmas tree scan routera - **nmap -sX -p1-65535 10.0.0.1**

Kolejnym skanowaniem było skanowanie sieci za pomocą metody choinkowej. Wysłano pakiet **FIN PSH URG** na każdy port routera (port 80 na zrzutach ekranu został wybrany przykładowo, by pokazać rozmowę).



Dla każdego zamkniętego portu otrzymano standardową odpowiedź **RST ACK**.



Dla otwartego portu pakiet powinien zostać zignorowany, jednak **nmap** zwrócił informację, że każdy port na routerze był zamknięty (mimo faktu, że serwer **telnet** został skonfigurowany i port 23 był otwarty).

**SYN scan komputera z Linuxem** - **nmap -sS -p T:21-25,80,443,2137,8080,27015 10.0.0.2**

Ostatnim skanowaniem był *SYN scan* komputera z uruchomionym serwerem HTTP, ograniczony do wybranej grupy portów.

Zasada działania była identyczna, jak w przypadku pierwszego *SYN scana*.

**nmap** zwrócił poniższe podsumowanie skanowania.

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 11:55 Central European Day
light Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.2
Host is up (0.00s latency).

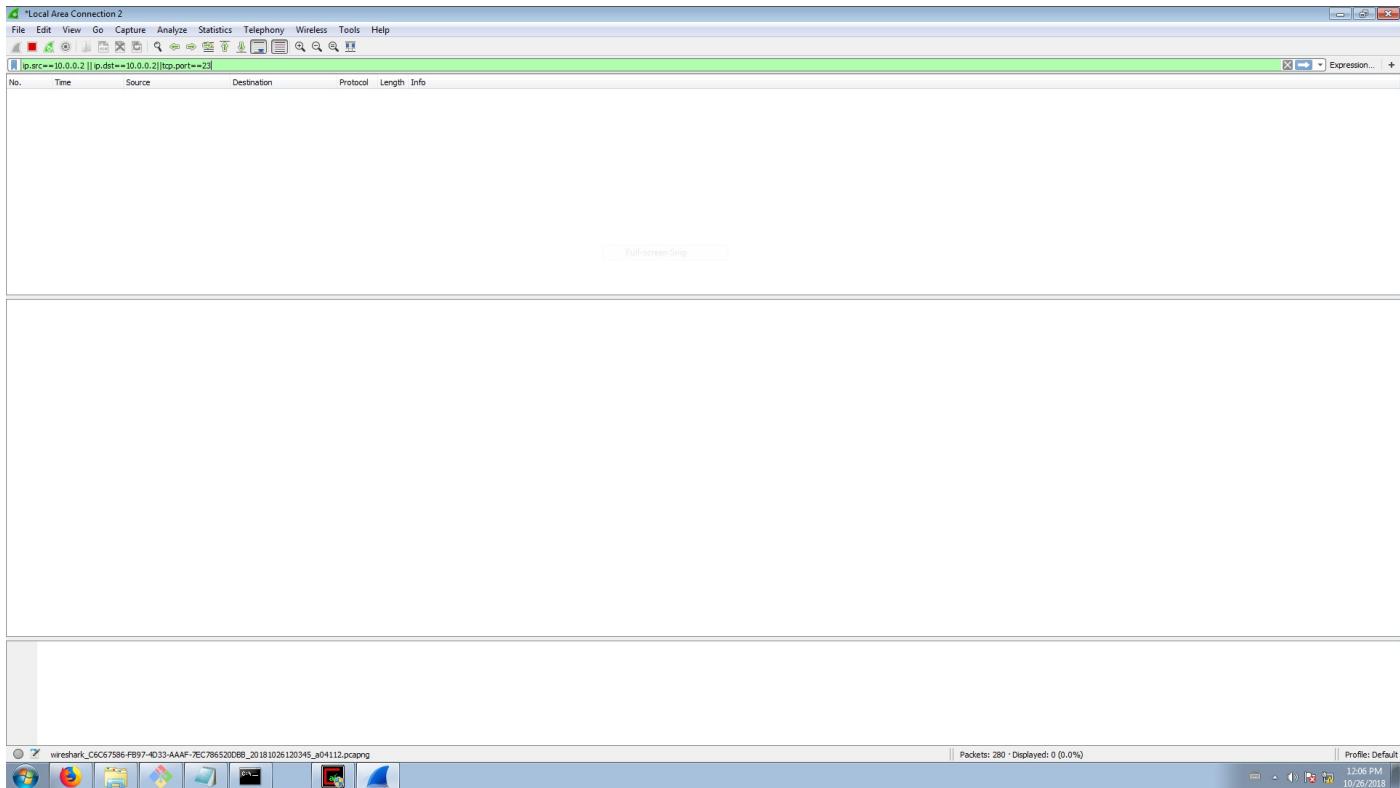
PORT      STATE SERVICE
21/tcp    closed  ftp
22/tcp    closed  ssh
23/tcp    closed  telnet
24/tcp    closed  priv-mail
25/tcp    closed  smtp
80/tcp    open   http
443/tcp   closed https
2137/tcp  closed connect
8080/tcp  closed http-proxy
27015/tcp closed unknown
MAC Address: 08:00:27:1C:14:28 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.00 seconds
```

# ARP poisoning

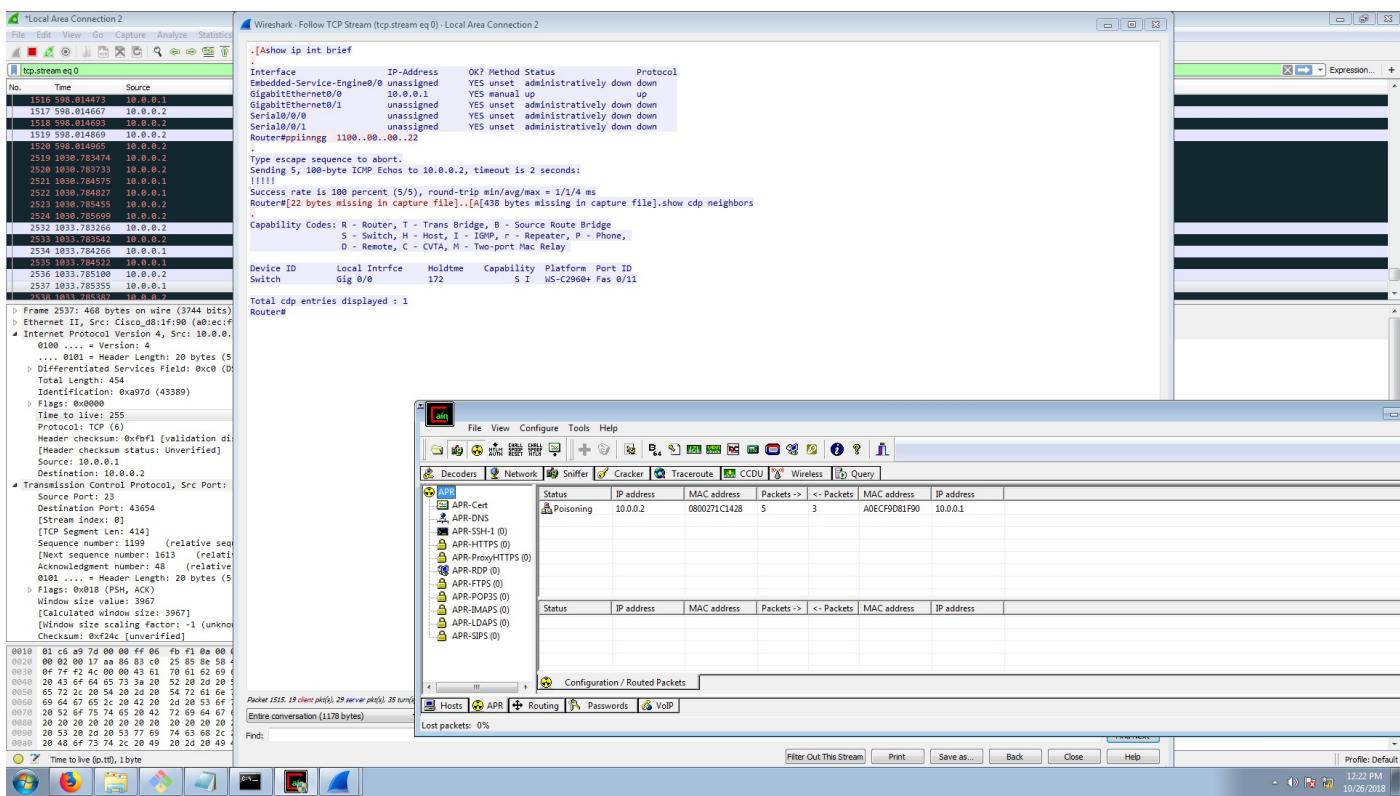
Kolejnym zadaniem było wykonanie skutecznego ataku typu *ARP poisoning* w celu przechwycenia komunikacji Telnet drugiego komputera z routera.

Przed przystąpieniem do ataku zweryfikowano, że switch nie przekazuje ramek przeznaczonych dla konkretnego, znanego urządzenia do innych urządzeń.



Do ataku wykorzystany został program Cain & Abel.

Wynik ataku wraz z przechwyconą treścią rozmowy udokumentowany został poniżej.



Udany atak

Screenshot of Wireshark showing a captured TCP session between two hosts. The session details pane shows the source port as 43654 and destination port as 23. The packet list pane shows several Telnet sessions. The bytes pane displays the raw data of the captured packets.

### Przykładowy przechwycony pakiet

Dodatkowo przechwycono pakiety **ping** wysłane z routera na adres komputera.

Screenshot of Wireshark showing a captured ICMP session between a router and a host. The session details pane shows the source port as 0 and destination port as 0. The packet list pane shows multiple ICMP echo requests and replies. The bytes pane displays the raw data of the captured packets.

Aby dokonać analizy pakietów użytych do 'zatrucia' tabeli ARP, należy spojrzeć na adresy MAC kart sieciowych:

Urządzenie	Adres MAC
Router	A0:EC:F9:D8:1F:90
PC (Linux)	08:00:27:1C:14:28
PC (Windows)	08:00:27:94:47:A7

Atak polegał na przechwyceniu komunikacji pomiędzy komputerem z Linuxem i routerem. Ataku dokonywał komputer z Windowsem.

Pierwszy pakiet był wysyłany na adres komputera z Linuxem z zapytaniem, kto zna adres MAC dla jego adresu IP, oraz prośbą o informację zwrotną na adres MAC komputera z Windowsem, ale podpisany adresem IP routera.

Wireshark - Local Area Connection 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
1033	460.846713	PcsCompu_94:47:a7	IPv4mcast_00	ARP	42	Who has 10.0.0.2? Tell 10.0.0.0
1034	460.862358	PcsCompu_94:47:a7	IPv4mcast_00	ARP	42	Who has 10.0.0.3? Tell 10.0.0.0
1038	461.893645	PcsCompu_94:47:a7	IPv4mcast_01	ARP	42	Who has 10.0.0.1? Tell 10.0.0.0
1039	461.909244	PcsCompu_94:47:a7	IPv4mcast_01	ARP	42	Who has 10.0.0.2? Tell 10.0.0.0
1040	461.924843	PcsCompu_94:47:a7	IPv4mcast_01	ARP	42	Who has 10.0.0.3? Tell 10.0.0.0
1043	461.935875	PcsCompu_94:47:a7	IPv4mcast_01	ARP	42	Who has 10.0.0.1? Tell 10.0.0.0
1046	462.956237	PcsCompu_94:47:a7	IPv4mcast_03	ARP	42	Who has 10.0.0.17? Tell 10.0.0.0
1047	462.974678	PcsCompu_94:47:a7	IPv4mcast_03	ARP	42	Who has 10.0.0.18? Tell 10.0.0.0
1048	462.986880	PcsCompu_94:47:a7	IPv4mcast_03	ARP	42	Who has 10.0.0.19? Tell 10.0.0.0
1265	564.157816	PcsCompu_94:47:a7	PcsCompu_1c:14:28	ARP	42	Who has 10.0.0.2? Tell 10.0.0.0 (duplicate use of 10.0.0.1 detected)
1266	564.157817	PcsCompu_94:47:a7	IPv4mcast_01	ARP	42	Who has 10.0.0.2? Tell 10.0.0.0 (duplicate use of 10.0.0.2 detected)
1267	564.157820	PcsCompu_1c:14:28	PcsCompu_94:47:a7	ARP	42	Who has 10.0.0.1? Tell 10.0.0.0 (duplicate use of 10.0.0.1 detected)
1268	564.157887	PcsCompu_94:47:a7	PcsCompu_1c:14:28	ARP	42	10.0.0.1 is at 08:00:27:94:47:a7
1269	564.157888	Cisco_08:1f:90	PcsCompu_94:47:a7	ARP	68	10.0.0.1 is at a0:ec:f9:d8:1f:90 (duplicate use of 10.0.0.2 detected)
1270	564.158081	PcsCompu_94:47:a7	Cisco_08:1f:90	ARP	42	10.0.0.2 is at 08:00:27:94:47:a7
1376	594.145226	PcsCompu_94:47:a7	PcsCompu_1c:14:28	ARP	42	10.0.0.1 is at 08:00:27:94:47:a7
1377	594.145227	PcsCompu_94:47:a7	IPv4mcast_01	ARP	42	10.0.0.1 is at 08:00:27:94:47:a7
1567	610.828576	PcsCompu_94:47:a7	PcsCompu_1c:14:28	ARP	42	Who has 10.0.0.2? Tell 10.0.0.1

[Frame 1265: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
Ethernet II, Src: PcsCompu\_94:47:a7 (08:00:27:94:47:a7), Dst: PcsCompu\_1c:14:28 (08:00:27:1c:14:28)  
[Duplicate IP address detected for 10.0.0.1 (08:00:27:94:47:a7) - also in use by a0:ec:f9:d8:1f:90 (frame 1011)]  
▲ Address Resolution Protocol (request)  
    Request on interface Ethernet 1  
    Protocol type: IPv4 (0x0800)  
    Hardware size: 6  
    Protocol size: 4  
    Opcode : request (1)  
    Sender MAC address: PcsCompu\_94:47:a7 (08:00:27:94:47:a7)  
    Sender IP address: 10.0.0.1  
    Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)  
    Target IP address: 10.0.0.2

0009 00 00 27 1c 14 28 08 00 27 94 47 a7 00 00 00 01 ...(... 6 ...) 0010 08 00 06 04 00 01 00 00 27 94 47 a7 00 00 00 01 ..... 0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 .....

wireshark\_C6C67586-FB97-4D33-AAAF-7EC786520DB8\_20181026120345\_p04112.pcapng

Packets: 2784 · Displayed: 53 (1.9%) · Dropped: 0 (0.0%)

Profile: Default

12:24 PM 10/25/2018

Zgodnie z planem, odpowiedź na to zapytanie wysyłana była na adres MAC komputera z Windowsem. Ufając danym o źródle zapytania, komputer z Linuxem zapisywał w swojej tabeli ARP, że adres IP routera ( **10.0.0.1** ) dostępny jest również pod adresem MAC komputera z Windowsem.

The screenshot shows a Wireshark session titled "arp" with the following details:

- File Edit View Capture Analyze Statistics Telephone Wireless Tools Help**
- arp** - The current active capture.
- Expression... +** - A search bar for filtering traffic.
- No. Time Source Destination Protocol Length Info** - The column headers for the packet list.
- 1033 469.846713 PcsCompu\_94:47:a7 IPv4mcast\_00 ARP 42 Who has 10.0.0.2? Tell 0.0.0.0**
- 1034 469.862558 PcsCompu\_94:47:a7 IPv4mcast\_00 ARP 42 Who has 10.0.0.3? Tell 0.0.0.0**
- 1038 461.893645 PcsCompu\_94:47:a7 IPv4mcast\_01 ARP 42 Who has 10.0.0.1? Tell 0.0.0.0**
- 1039 461.992244 PcsCompu\_94:47:a7 IPv4mcast\_01 ARP 42 Who has 10.0.0.2? Tell 0.0.0.0**
- 1040 461.992244 PcsCompu\_94:47:a7 IPv4mcast\_01 ARP 68 10.0.1.1 is at 08:00:27:1c:14:28**
- 1041 461.992244 PcsCompu\_94:47:a7 IPv4mcast\_01 ARP 42 Who has 10.0.0.3? Tell 0.0.0.0**
- 1046 461.996237 PcsCompu\_94:47:a7 IPv4mcast\_03 ARP 42 Who has 10.0.0.1? Tell 0.0.0.0**
- 1047 462.974678 PcsCompu\_94:47:a7 IPv4mcast\_03 ARP 42 Who has 10.0.0.2? Tell 0.0.0.0**
- 1048 462.968684 PcsCompu\_94:47:a7 IPv4mcast\_03 ARP 42 Who has 10.0.0.3? Tell 0.0.0.0**
- 1265 564.157016 PcsCompu\_94:47:a7 PcsCompu\_1c:14:28 ARP 42 Who has 10.0.0.1? (duplicate use of 10.0.0.1 detected!)**
- 1266 564.157301 PcsCompu\_94:47:a7 Cisco\_08:1f:90 ARP 42 Who has 10.0.0.1? Tell 10.0.0.2 (duplicate use of 10.0.0.2 detected!)**
- 1267 564.157301 PcsCompu\_94:47:a7 Cisco\_08:1f:90 ARP 68 10.0.1.1 is at 08:ec:f9:d8:1f:90 (duplicate use of 10.0.0.1 detected!)**
- 1268 564.157887 PcsCompu\_94:47:a7 PcsCompu\_1c:14:28 ARP 42 10.0.0.1 is at 08:00:27:94:47:a7**
- 1269 564.157888 Cisco\_08:1f:90 PcsCompu\_94:47:a7 ARP 68 10.0.0.1 is at 08:ec:f9:d8:1f:90 (duplicate use of 10.0.0.2 detected!)**
- 1270 564.158801 PcsCompu\_94:47:a7 Cisco\_08:1f:90 ARP 42 10.0.0.2 is at 08:00:27:94:47:a7**
- 1370 594.144926 PcsCompu\_94:47:a7 PcsCompu\_1c:14:28 ARP 42 10.0.0.1 is at 08:00:27:94:47:a7**
- 1371 594.145255 PcsCompu\_94:47:a7 Cisco\_08:1f:90 ARP 42 10.0.0.2 is at 08:00:27:94:47:a7**
- 1372 594.145255 PcsCompu\_94:47:a7 Cisco\_08:1f:90 ARP 42 10.0.0.3 is at 08:00:27:94:47:a7**
- 1373 594.145255 PcsCompu\_94:47:a7 Cisco\_08:1f:90 ARP 42 10.0.0.1 is at 08:ec:f9:d8:1f:90 (Frame 1011)**
- Frame 1267: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0**
- Ethernet II, Src: PcsCompu\_1c:14:28 (08:00:27:1c:14:28), Dst: PcsCompu\_94:47:a7 (08:00:27:94:47:a7)**
- [Duplicate IP address detected for 10.0.0.1 (08:00:27:94:47:a7). Also in use by 08:ec:f9:d8:1f:90 (Frame 1011)]**
- # Address Resolution Protocol (reply)**
- Hardware type: Ethernet (1)**
- Protocol type: IPv4 (0x0800)**
- Hardware size: 6**
- Protocol size: 4**
- Opcodes: reply (2)**
- Sender MAC address: PcsCompu\_1c:14:28 (08:00:27:1c:14:28)**
- Sender IP address: 10.0.0.2**
- Target MAC address: PcsCompu\_94:47:a7 (08:00:27:94:47:a7)**
- Target IP address: 10.0.0.1**

Hex and ASCII panes showing the raw data for frame 1267, which is a Duplicate IP address detection message.

Bottom status bar: Packets: 2784 • Displayed: 53 (1.9%) • Dropped: 0 (0.0%) | Profile: Default

Następnie na adres routera wysyłane było zapytanie ARP o adres MAC dla jego adresu IP, z prośbą o odpowiedź na adres MAC komputera z Windowsem, ale podpisany adresem IP komputera z Linuxem.

The screenshot shows a network capture from a Windows machine's interface "Local Area Connection 2". It displays several ARP requests and responses. Key entries include:

- ARP request from PcsCompu\_94:47:a7 (Windows) to 10.0.0.2 (Cisco\_d8:1f:90) for the IP 10.0.0.2.
- ARP response from Cisco\_d8:1f:90 (Cisco router) to PcsCompu\_94:47:a7 (Windows) confirming the MAC address 00:ec:f9:d8:1f:90.
- Multiple ARP requests from PcsCompu\_94:47:a7 (Windows) to 10.0.0.1 (PcsCompu\_1c:14:28) for the IP 10.0.0.1.
- ARP responses from PcsCompu\_1c:14:28 (Linux) to PcsCompu\_94:47:a7 (Windows) confirming the MAC address 00:08:27:94:47:a7.
- Duplicate IP detection messages indicating that both 10.0.0.1 and 10.0.0.2 are in use by the same interface (frame 1040).

Router zapisywał w swojej tabeli ARP, że adres IP komputera z Linuxem ( **10.0.0.2** ) dostępny jest również pod adresem MAC komputera z Windowsem.

The screenshot shows a network capture from a Cisco router's interface "Local Area Connection 2". It displays ARP requests and responses. Key entries include:

- ARP request from Cisco\_d8:1f:90 (Cisco router) to PcsCompu\_94:47:a7 (Windows) for the IP 10.0.0.2.
- ARP response from PcsCompu\_94:47:a7 (Windows) to Cisco\_d8:1f:90 (Cisco router) confirming the MAC address 00:ec:f9:d8:1f:90.
- ARP request from PcsCompu\_94:47:a7 (Windows) to 10.0.0.1 (PcsCompu\_1c:14:28) for the IP 10.0.0.1.
- ARP response from PcsCompu\_1c:14:28 (Linux) to PcsCompu\_94:47:a7 (Windows) confirming the MAC address 00:08:27:94:47:a7.
- Duplicate IP detection messages indicating that both 10.0.0.1 and 10.0.0.2 are in use by the same interface (frame 1268).