**Sieci komputerowe**

**Laboratorium nr 5**

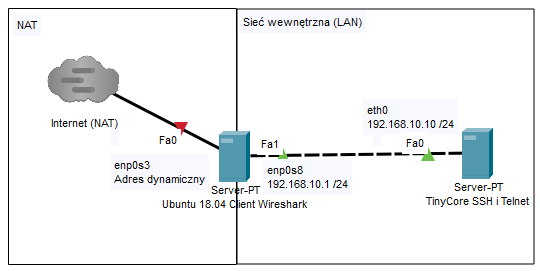
Przechwytywanie i analiza ruchu sieciowego

|  |  |  |  |
| --- | --- | --- | --- |
| **Grupa** | **Nazwisko** | **Imię** | **Nr studenta (X)** |
| WCY20IY4S1 | Relidzyński | Radosław | 9 |

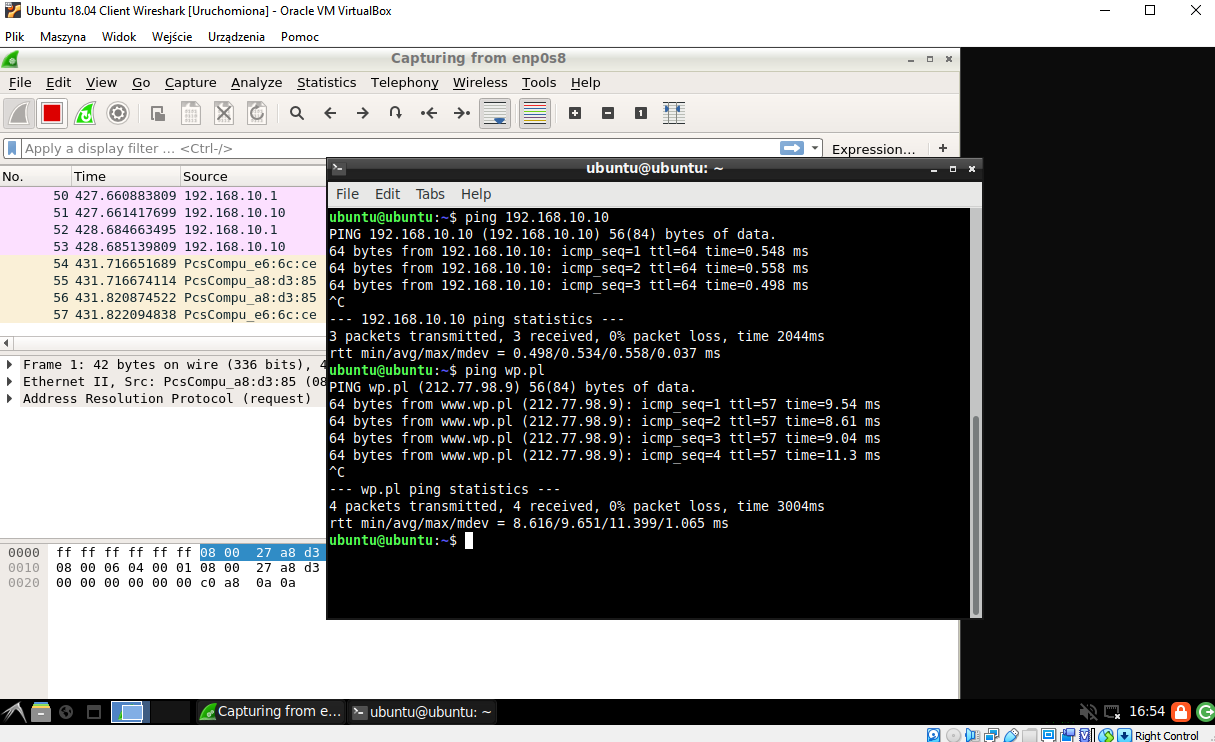
**Sprawozdanie:**

1. **Sprawozdanie należy wykonywać na zajęciach laboratoryjnych (zrzuty ekranu należy wykonywać za pomocą kombinacji ALT+PrntScr).**
2. **Sprawozdanie należy zapisać w formacie z rozszerzeniem .docx i nadać mu nazwę „Grupa Nazwisko Imię NrStudenta – Lab Y Temat zadania”, np. WCYIX19S1 Rabiak Adam 1 – Lab 1 Podłączenie komputera do sieci.docx”.**
3. **Sprawozdanie wraz z plikiem projektowym (jeśli dotyczy zadania) należy przesłać na e-mail prowadzącego z odpowiednim tytułem wiadomości: „Grupa Nazwisko Imię – Sprawozdanie Lab Y”, gdzie Y jest numerem laboratorium (najważniejsze jest podanie pełnej grupy studenckiej i nazwiska).**

**Zadanie nr 1.**

****

1. Uruchomić obydwie maszyny (serwer + klient). Zalogować się na maszynę kliencką i sprawdzić możliwość komunikacji z maszyną serwerową oraz siecią Internet np. z serwerem strony wp.pl (*ping*). **Jeżeli występuje problem z komunikacją z którąś z sieci, to należy zgłosić to prowadzącemu i wprowadzić poprawną konfigurację sieci**.



(Wkleić tutaj zrzuty ekranu przedstawiające poprawną komunikację z maszyną serwerową oraz siecią Internet)

1. Sprawdzić konfigurację interfejsów sieciowych na maszynie klienckiej (*ifconfig*).

Obraz zawierający tekst

Opis wygenerowany automatycznie

(Wkleić tutaj zrzut ekranu przedstawiający poprawną konfigurację interfejsów sieciowych maszyny klienckiej)

1. Uruchomić program Wireshark i przechwycić pakiety związane ze sprawdzaniem osiągalności węzła sieci. Należy włączyć przechwytywanie komunikacji sieciowej w programie Wireshark, następnie w terminalu uruchomić polecenie *ping <adres maszyny serwerowej w sieci LAN>*, odczekać na wysłanie co najmniej dwóch pakietów żądających potwierdzenia komunikacji, wyłączyć przechwytywanie komunikacji sieciowej i uzupełnić poniższą tabelę.r

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | IP | | | | | ICMP | |
| Adres IP | | Identyfikator pakietu | TTL | Protokół warstwy wyższej | Typ | Kod |
| nadawcy | odbiorcy |
| Pakiet zapytania nr 1 | 192.168.10.1 | 192.168.10.10 | 0x075a | 64 | ICMP | 8 | 0 |
| Pakiet odpowiedzi nr 1 | 192.168.10.10 | 192.168.10.1 | 0x075a | 64 | ICMP | 0 | 0 |
| Pakiet zapytania nr 2 | 192.168.10.1 | 192.168.10.10 | 0x075a | 64 | ICMP | 8 | 0 |
| Pakiet odpowiedzi nr 2 | 192.168.10.10 | 192.168.10.1 | 0x075a | 64 | ICMP | 0 | 0 |

1. Na podstawie jakich wartości z nagłówków protokołów można wskazać który pakiet odpowiedzi jest odpowiedzią na dany pakiet zapytania? **Kolejność pakietów wysyłanych zapytań i otrzymywanych odpowiedzi nie jest poprawną odpowiedzią.**

**Odp.: Numer sekwencji (sequence number)**

1. W programie Wireshark przechwycić pakiety związane z logowaniem na serwer SSH. Do zalogowania się za pomocą usługi Telnet i SSH z poziomu terminala na maszynie klienckiej wykorzystać dane z tabeli. Po zalogowaniu się i przechwyceniu pakietów zakończyć połączenie telnet/ssh za pomocą polecenia (*exit*). Odpowiedzieć na poniższe pytania.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rodzaj połączenia** | **Adres serwera** | **Użytkownik** | **Hasło** | **Gotowe polecenie** |
| Telnet | 192.168.10.10 | TelnetUser | telnet | *telnet 192.168.10.10 -l TelnetUser* |
| SSH | 192.168.10.10 | SSHUser | sshssh | *ssh SSHUser@192.168.10.10* |

1. Jak wygląda przesyłane hasło z wykorzystaniem protokołu Telnet?

**Odp.: Przekazywane jest literka po literce, gdzie każdy pakiet to jedna litera.**

Obraz zawierający tekst

Opis wygenerowany automatycznie

(Wkleić tutaj zrzut ekranu przedstawiający przechwycony pakiet z hasłem lub jego fragmentem)

1. Jak wygląda przesyłane hasło z wykorzystaniem protokołu SSH?

**Odp.: Przekazywane pakiety są zaszyfrowane i dopiero wtedy przekazywane, rozmiary pakietów są nierównomierne.**

Obraz zawierający tekst

Opis wygenerowany automatycznie

(Wkleić tutaj zrzut ekranu przedstawiający przechwycony pakiet z hasłem lub jego fragmentem)

1. Jaki protokół warstwy czwartej wykorzystuje protokół Telnet i SSH do zestawienia połączenia i na których portach?

**Odp.: TCP, port 22 dla SSH i 23 dla Telnet**

1. W jakim celu wykorzystuje się połączenie z użyciem protokołów Telnet lub SSH? Jaka jest między nimi podstawowa różnica w działaniu oraz którego lepiej używać w dzisiejszych czasach?

**Odp.: Są to protokoły służące do łączenia się z poziomu konsoli ze zdalnym komputerem.**

1. W programie Wireshark przechwycić komunikację sieciową podczas wysłania zapytania do serwera DNS w celu uzyskania adresu IP serwera WWW podanego przez prowadzącego (*nslookup*). Uzupełnić tabelę i wkleić odpowiednie zrzuty ekranu.

|  |  |  |
| --- | --- | --- |
| **Nazwa strony internetowej** | **Adres IP serwera WWW** | **Adres serwera DNS** |
| http://bielsko.pl | 212.106.184.5 | 127.0.0.53 |

Obraz zawierający tekst

Opis wygenerowany automatycznie

(Wkleić tutaj zrzuty ekranu przedstawiające wpisane polecenie wraz z uzyskaną odpowiedzią od serwera DNS oraz przechwycone pakiety w programie Wireshark)

1. Na którym domyślnie porcie działa usługa DNS oraz z którego protokołu warstwy czwartej korzystają zapytania DNS z polecenia *nslookup*?

**Odp.: UDP 53**

1. Uruchomić przeglądarkę internetową na maszynie klienckiej (Firefox); przejść do trybu prywatnego/incognito (*CTRL + SHIFT + P*); zamknąć okno przeglądarki, które nie jest w trybie prywatnym/incognito; w oknie prywatnym/incognito wejść pod wskazany adres z wykorzystaniem przedrostka „http://”. W programie Wireshark przechwycić wszystkie pakiety do czasu wczytania strony w przeglądarce.
2. W przechwyconej komunikacji odszukać segmenty odpowiedzialne za inicjowanie połączenia sesji TCP. Uzupełnić dane w tabeli (3 segmenty).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Inicjowanie połączenia** | | | | | |
| **Nadawca** | | **Odbiorca** | | **Nadawca** | |
| Identyfikator ramki IP  0x75cb (30155) | | Identyfikator ramki IP  0x0413 (1043) | | Identyfikator ramki IP  0x75cc (30156) | |
| IP nadawcy  10.0.2.15 | IP odbiorcy  212.106.184.5 | IP nadawcy  212.106.184.5 | IP odbiorcy  10.0.2.15 | IP nadawcy  10.0.2.15 | IP odbiorcy  212.106.184.5 |
| port nadawcy  43858 | port odbiorcy  443 | port nadawcy  443 | port odbiorcy  43858 | port nadawcy  43858 | port odbiorcy  443 |
| nr sekwencyjny  0 | | nr sekwencyjny  0 | | nr sekwencyjny  1 | |
| nr potwierdzenia  0 | | nr potwierdzenia  1 | | nr potwierdzenia  1 | |
| flagi  SYN | wielkość okna  64240 | flagi  SYN, ACK | wielkość okna  65535 | flagi  ACK | wielkość okna  64240 |

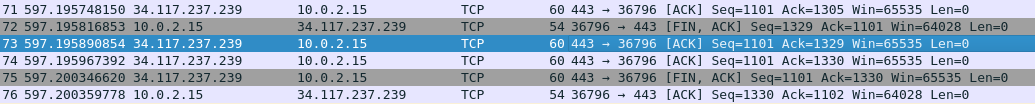
1. W przechwyconej komunikacji odszukać segmenty odpowiedzialne za transfer danych (np. grafiki strony internetowej lub kodu HTML). Uzupełnić dane w tabeli (maksymalnie 6 segmentów). **Podpowiedź: Szukać segmentów z flagą PSH.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Transfer danych** | | | | | |
| **Nadawca** | | **Odbiorca** | |  | |
| Identyfikator ramki IP  0x2bfe (11262) | | Identyfikator ramki IP  0x0426 (1062) | | Identyfikator ramki IP | |
| IP nadawcy  10.0.2.15 | IP odbiorcy  212.106.184.5 | IP nadawcy  212.106.184.5 | IP odbiorcy  10.0.2.15 | IP nadawcy | IP odbiorcy |
| port nadawcy  45607 | port odbiorcy  80 | port nadawcy  80 | port odbiorcy  45606 | port nadawcy | port odbiorcy |
| nr sekwencyjny  1 | | nr sekwencyjny  3528 | | nr sekwencyjny | |
| nr potwierdzenia  1 | | nr potwierdzenia  345 | | nr potwierdzenia | |
| flagi  PSH, ACK | wielkość okna  64240 | flagi  PSH, ACK | wielkość okna  65535 | flagi | wielkość okna |
|  | |  | |  | |
| Identyfikator ramki IP | | Identyfikator ramki IP | | Identyfikator ramki IP | |
| IP nadawcy | IP odbiorcy | IP nadawcy | IP odbiorcy | IP nadawcy | IP odbiorcy |
| port nadawcy | port odbiorcy | port nadawcy | port odbiorcy | port nadawcy | port odbiorcy |
| nr sekwencyjny | | nr sekwencyjny | | nr sekwencyjny | |
| nr potwierdzenia | | nr potwierdzenia | | nr potwierdzenia | |
| flagi | wielkość okna | flagi | wielkość okna | flagi | wielkość okna |

1. W przechwyconej komunikacji odszukać segmenty odpowiedzialne za kończenie połączenia sesji TCP. Uzupełnić dane w tabeli (3 segmenty).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Zamykanie połączenia** | | | | | |
| **Nadawca** | | **Odbiorca** | | **Nadawca** | |
| Identyfikator ramki IP  0x04bf (1215) | | Identyfikator ramki IP  0x7752 (30546) | | Identyfikator ramki IP  0xe983 (59779) | |
| IP nadawcy  10.0.2.15 | IP odbiorcy  212.106.184.5 | IP nadawcy  10.0.2.15 | IP odbiorcy  34.117.237.239 | IP nadawcy  34.117.237.239 | IP odbiorcy  10.0.2.15 |
| port nadawcy  443 | port odbiorcy  36796 | port nadawcy  36796 | port odbiorcy  443 | port nadawcy  443 | port odbiorcy  36796 |
| nr sekwencyjny  1101 | | nr sekwencyjny  1329 | | nr sekwencyjny  1101 | |
| nr potwierdzenia  1305 | | nr potwierdzenia  1101 | | nr potwierdzenia  1329 | |
| flagi  ACK | wielkość okna  65535 | flagi  FIN, ACK | wielkość okna  64028 | flagi  ACK | wielkość okna  65535 |

W tym przypadku wystąpiły 2 zestawy segmentów spełniających to zadanie, widoczne na poniższym zrzucie ekranu. Do opisu wybrałem pierwszy zestaw.



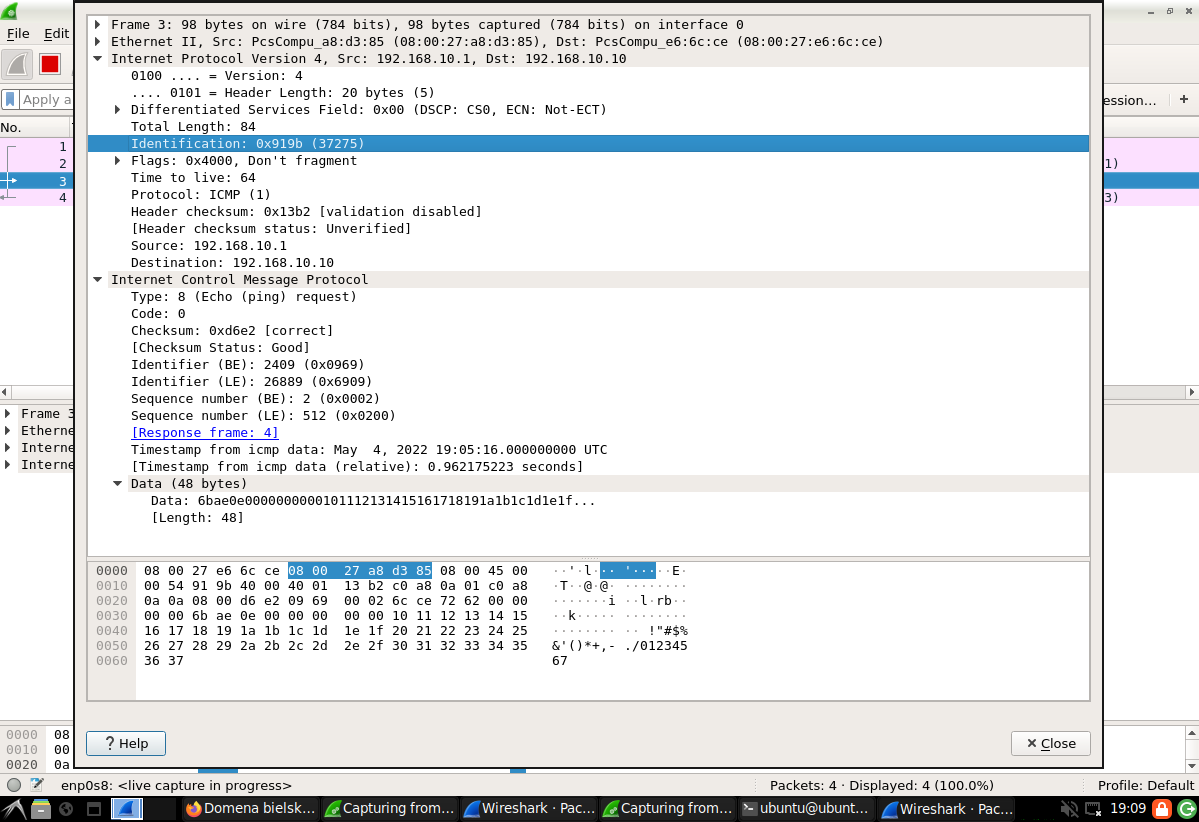
1. Jaka powinna być prawidłowa (podręcznikowa) sekwencja flag inicjowania i zamykania połączenia sesji TCP? **Flagi podać w formie nazw, a nie wartości liczbowych!**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Nadawca** | **Odbiorca** | | **Nadawca** |
| Inicjowanie połączenia (*three-way handshake*) | SYN | SYN, ACK | | ACK |
| Zamykanie połączenia (*four-way handshake*) | FIN | ACK | FIN | ACK |

1. Na podstawie literatury lub Internetu (np. *IPv4 header*) zapoznać się z wyglądem poszczególnych nagłówków protokołów sieciowych: Ethernet, IPv4, ARP, ICMP, UDP, TCP.
2. Uruchomić program Wireshark, włączyć nasłuchiwanie na interfejsie w sieci lokalnej, z maszyny klienckiej wysłać zapytania ICMP Echo Request do maszyny serwerowej, przechwycić komunikaty ICMP, odszukać jeden z pakietów IP ICMP Echo Reply. Wkleić zrzut ekranu przedstawiający wspomniany pakiet wraz z rozwiniętymi zakładkami dot. protokołów IP oraz ICMP, a także widocznymi wartościami heksadecymalnymi. Wypisać wszystkie pola nagłówków wraz danymi z przechwyconego pakietu (po polsku!) w następującej formie:

<Nazwa pola>: <Wartość>

np.: Adres IP źródłowy: 192.168.10.10



(Wkleić tutaj zrzut ekranu przedstawiający w odpowiedni sposób przechwycony pakiet IP ICMP Echo Reply)

1. Protokół IP:

**Odp.:**

* **Wersja: 4**
* **Rozmiar nagłówka: 20 bytes**
* **Usługi zróżnicowane: 0x00 (DSCP: CSO, ECN: Not-ECT)**
* **Całkowity rozmiar: 84**
* **Identyfikator: 0x919b (37275)**
* **Flagi: 0x4000 (Don’t fragment)**
* **Czas życia: 64**
* **Protokół: ICMP**
* **Suma kontrolna: 0x13b2 (bez walidacji)**
* **Adres IP źródła: 192.168.10.1**
* **Adres IP docelowy: 192.168.10.10**

1. Protokół ICMP:

**Odp.:**

* **Typ: 0**
* **Kod: 0**
* **Suma kontrolna: 0xd6e2**
* **Nagłówki:** 
  + **Identyfikator (zapisany w Big Endian): 2308 (0x0904)**
  + **Numer sekwencyjny (zapisany w Big Endian): 1 (0x0001)**
  + **Czas otrzymywania wiadomości: May 4, 2022 18:41:28.000000000 UTC**
* **Data: 6b:ae:0e:00:00:00:00:00:10:11:12:13:14:15:16:17:18:19:1a:1b:1c:1d:1e:1f:20:21:22:23:24:25:26:27:28:29:2a:2b:2c:2d:2e:2f:30:31:32:33:34:35:36:37**

**Zadania dodatkowe (niepodlegające ocenie)**

1. W której warstwie modelu ISO/OSI przesyłane są:
2. Segmenty,
3. Bity,
4. Ramki,
5. Datagramy,
6. Pakiety,
7. Dane (zależne już od konkretnego protokołu)?
8. Na których portach działają poniższe usługi i z którego protokołu warstwy czwartej korzystają?

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa usługi** | **Nr portu/ów** | **TCP (tak/nie)** | **UDP (tak/nie)** |
| FTP |  |  |  |
| SSH |  |  |  |
| Telnet |  |  |  |
| SMTP |  |  |  |
| DNS |  |  |  |
| TFTP |  |  |  |
| HTTP |  |  |  |
| HTTPS |  |  |  |
| SFTP |  |  |  |
| NTP |  |  |  |
| IMAP |  |  |  |
| LDAP |  |  |  |
| LDAPS |  |  |  |
| SNMP |  |  |  |
| SMB |  |  |  |
| IMAPS |  |  |  |
| Doom 😉 |  |  |  |

1. Na czym polegają ataki ARP Spoofing oraz IP Spoofing?
2. Obejrzeć Star Wars Episode IV przez Telnet (*telnet towel.blinkenlights.nl*) 😉