Warsztaty nr 1 z Sieci komputerowych

Przed zajęciami

Otwórz znajdujący się w materiałach do kursu dokument *Opis maszyny wirtualnej Virbian* i uważnie go przeczytaj.

Konfiguracja początkowa

Pobierz obraz maszyny ze strony wykładu. Utwórz konfigurację dla maszyn *Virbian0* i *Virbian1*. Następnie uruchom maszynę *Virbian0*.

Znak `Vi$>` oznacza wykonanie danego polecenia w konsoli maszyny *Virbiani* z uprawnieniami zwykłego użytkownika. Natomiast znak `Vi#>` oznacza konieczność wykonania polecenia z prawami administratora. W tym celu należy uprzednio zalogować się na konto użytkownika `root` albo poprzedzić takie polecenie napisem `sudo`.

Tutorial 1

Poniższe zadanie należy wykonać w uruchomionej maszynie *Virbian0*. Na początku włącz interfejs graficzny poleceniem `startx`.

- Poleceniem

  ```
  V0$> ip addr
  ```

  wyświetl wszystkie dostępne interfejsy sieciowe. Powinny być dostępne dwa interfejsy: `lo` i `enp0s3`. Jeśli nazwa drugiego interfejsu jest trochę inna, należy odpowiednio zmodyfikować poniższe polecenia.

- Uzyskaj konfigurację sieciową dla maszyny poleceniem[1]

  ```
  dhcpcd enp0s3
  ```

  Ponownie wykonaj polecenie

  ```
  V0$> ip addr
  ```

  i sprawdź, że wyświetlana informacja zmieniła się i interfejs maszyny ma teraz przypisany adres IP równy `10.0.2.15` (lub podobny).

- Uruchom przeglądarkę Firefox. Otwórz narzędzia programistyczne klawiszem `F12` i przejdź do karty *Network*. Wejdź przeglądarką na stronę `http://example.com/` i obejrzyj przesyłane żądania i odpowiedzi protokołu HTTP.
  - Ile żądań HTTP jest wysyłanych? Do jakich serwerów są one skierowane?
  - Jaką wersję protokołu HTTP wykorzystuje przeglądarka?
  - Sprawdź, że otrzymywanym kodem odpowiedzi jest `200 OK` lub `304 Not Modified`.
  - Jaka jest data ostatniej modyfikacji zwracanego dokumentu HTML?

[1] Jeśli masz starszą wersję Virbiana i polecenie `dhcpcd` nie jest dostępne, użyj polecenia `dhclient -v enp0s3`.

- Sprawdź jaki adres IP jest związany z nazwą `example.com` poleceniem

```
V0$> dig example.com
```

Niech *w.x.y.z* będzie tym adresem IP. Być może polecenie zwróci więcej niż jeden adres IP; w takim przypadku wybierz dowolny z nich.

Uruchom program Wireshark i włącz w nim obserwację interfejsu `enp0s3` klikając dwukrotnie na jego nazwie. Aby odfiltrować wyświetlanie zbędnych pakietów w polu *Apply a display filter …* wpisz `ip.addr ==` *w.x.y.z* i kliknij przycisk *Apply* (niebieska strzałka po prawej stronie tego pola). W razie potrzeby możesz również kliknąć ikonę *Restart current capture* (jedna z pierwszych ikon od lewej na górze okna programu).

- Odśwież oglądaną stronę w przeglądarce naciskając `Shift` + `Ctrl` + `R`. W Wiresharku wśród wysyłanych pakietów znajdź ten zawierający żądanie HTTP pobierające stronę HTML. Obejrzyj w tym pakiecie nagłówki warstwy sieciowej (IP) i transportowej (TCP). Klikając poszczególne pola opisu, podświetlisz w widoku szesnastkowym pakietu (na dole okna) odpowiadające im bajty.
  - Jaki jest źródłowy i docelowy adres IP tego pakietu?
  - Jaki jest jego źródłowy i docelowy port?
  - W których nagłówkach znajdują się te informacje?

  Powtórz powyższe operacje dla pakietu zawierającego odpowiedź HTTP (powinien zawierać kod odpowiedzi `200 OK` wraz ze stroną w HTML lub kod odpowiedzi `304 Not Modified`). Czy dane identyfikujące połączenie (źródłowy/docelowy adres/port) zmieniły się czy są takie same? Dlaczego?

- W karcie *Network* narzędzi programistycznych Firefoksa zaznacz żądanie pobierające stronę główną `example.com`. Wybierz kartę *Headers*, przewiń do nagłówków żądania (*Request Headers*) i kliknij przełącznik *Raw*. Skopiuj otrzymane w ten sposób nagłówki do pliku `headers.txt` i dodaj na jego końcu pusty wiersz. Wynikowa zawartość pliku powinna wyglądać mniej więcej tak:

```
GET / HTTP/1.1
Host: example.com
User-Agent: ...
...
<wiersz-odstępu>
```

Wyślij to zapytanie do serwera WWW (tj. do portu `80` komputera `example.com`) poleceniem

```
V0$> nc -w 3 example.com 80 < headers.txt
```

Opcja `-w 3` czeka 3 sekundy przed zamknięciem połączenia. Na ekranie wyświetli się odpowiedź serwera WWW, ale będzie ona nieczytelna dla człowieka. Problematyczny okazuje się wiersz `Accept-Encoding: gzip, deflate` proszący serwer WWW o kompresję przesyłanych danych. Usuń ten wiersz z pliku `headers.txt` i spróbuj ponownie. Obejrzyj przesyłane pakiety w Wiresharku.

- Sprawdź, czy uzyskasz odpowiedź, jeśli w pliku `headers.txt` pozostawisz jedynie dwa pierwsze wiersze (zaczynające się od `GET` i `Host:`) i następujący po nich pusty wiersz. Ponownie obejrzyj pakiety w Wiresharku. Co stanie się, jeśli zostawisz tylko pierwszy wiersz i wiersz odstępu?

- Poleceniem

```
V0$> telnet example.com 80
```

otwórz strumień danych do serwera WWW na komputerze `example.com`. Wpisz tam zapytanie HTTP, czyli wiersze

```
GET / HTTP/1.1
Host: example.com
```

a następnie pusty wiersz. W odpowiedzi otrzymasz kolejny raz powyższą stronę WWW.

- Poleceniami

```
V0$> ss -lntu4
V0$> ss -ltu4
```

wyświetl uruchomione na Twoim komputerze usługi „przypięte” do konkretnych portów warstwy transportowej. Pierwsze polecenie wyświetla wartości numeryczne, drugie zaś stara się je interpretować wykorzystując plik `/etc/services` (obejrzyj ten plik).

Uruchom serwer SSH poleceniem

```
V0#> systemctl start ssh
```

i ponownie wyświetl listę usług poleceniem `ss`.

- Wybierz kilka lokalnych usług wykorzystujących protokół TCP, w tym usługę SSH (port 22), serwer echa (port 7) i serwer czasu (port 13). Połącz się z nimi w interaktywny sposób programem `telnet` i wyślij do nich jakieś dane. Przykładowo z portem 7 połączysz się poleceniem

```
V0$> telnet localhost 7
```

Nazwa `localhost` zostanie zamieniona na adres IP maszyny, w której aktualnie pracujesz, tzn. powyższe polecenie utworzy połączenie z działającą lokalnie usługą (serwerem echa) „przypiętą” do portu 7. Aby rozłączyć się, naciśnij kombinację `Ctrl` + `]` i następnie wpisz polecenie `quit`.

Na końcu zamknij maszynę *Virbian0*.

Tutorial 2

Zmień konfigurację maszyn *Virbian0* i *Virbian1*, tak żeby ich pierwsze (i jedyne) karty sieciowe były podłączone do wirtualnej sieci `local0`. Następnie uruchom obie maszyny.

- Na obu maszynach wyświetl dostępne interfejsy sieciowe poleceniami

```
Vi$> ip link
Vi$> ip addr
```

Aktywne interfejsy oznaczone są napisem `UP`, nieaktywne — `DOWN`. Drugie z tych poleceń wyświetla dodatkowo przypisane do interfejsów adresy IP.

- Interfejsy `enp0s3` obu maszyn są połączone ze sobą wirtualną siecią, ale obecnie nie mają one przypisanych adresów IP. Poleceniem

```
Vi$> ethtool enp0s3
```

sprawdź status warstwy fizycznej interfejsu `enp0s3`. Zwróć uwagę na pola `Speed` i `Duplex`. Deklarowana szybkość połączenia powinna wynosić 1 Gbit/s.[2]

- Aktywuj interfejsy `enp0s3` i nadaj im odpowiednie adresy IP poleceniami:

```
V0#> ip link set up dev enp0s3
V0#> ip addr add 192.168.0.1/24 dev enp0s3
V1#> ip link set up dev enp0s3
V1#> ip addr add 192.168.0.2/24 dev enp0s3
```

  Wartość `/24` jest tzw. maską podsieci i jej znaczenie zostanie wyjaśnione na przyszłych zajęciach. Sprawdź, jak zmieniła się informacja wyświetlana przez polecenia `ip link` i `ip addr`. Jeśli przypadkowo nadasz interfejsowi `enp0s3` błędny adres IP, możesz usunąć wszystkie przypisane do tego interfejsu adresy poleceniem `ip addr flush dev enp0s3`.

- Polecenie `ping` służy do testowania warstwy sieciowej. W polu danych pakietów IP wysyłane są wtedy specjalne komunikaty protokołu ICMP. Wykonaj polecenie

```
V0$> ping 192.168.0.2
```

  Jaki jest wyświetlany RTT (*round trip time*)? Uruchom program Wireshark (na dowolnej z maszyn) i włącz w nim obserwację wszystkich interfejsów (wybierając sztuczny interfejs *any*). Obejrzyj pakiety wysyłane i odbierane przez program `ping`. Czy znaczniki czasowe (pole *timestamp*) w wysyłanym zapytaniu i odpowiedzi różnią się, czy są takie same?

- Na maszynie *Virbian0* zmodyfikuj plik `/etc/hosts`, tak aby zawierał następujący wiersz

```
192.168.0.2 jakaś_nazwa
```

  Sprawdź, że polecenie `ping` działa też z wpisaną tutaj nazwą. Uwaga: takie przypisanie działa tylko lokalnie, na maszynie, na której zostało skonfigurowane.

- Na maszynie *Virbian1* uruchom polecenie

```
V1$> iperf3 -s
```

  zaś na maszynie *Virbian0* polecenie

```
V0$> iperf3 -c 192.168.0.2
```

  Jaką prędkość przesyłania udało Ci się uzyskać?

- Na końcu na obu maszynach usuń adres IP z interfejsu `enp0s3` i dezaktywuj ten interfejs poleceniami

```
Vi#> ip addr flush dev enp0s3
Vi#> ip link set down dev enp0s3
```

Wyłącz obie maszyny.

Wyzwanie

- Utwórz dodatkową maszynę *Virbian2*. Podłącz karty sieciowe *Adapter1* maszyn *Virbian1* i *Virbian2* do wirtualnej sieci `local1` i następnie uruchom obie maszyny.

[2] W przypadku wirtualnych interfejsów informacja o prędkości nie będzie prawdziwa. Dodatkowo pole `Link detected` będzie równe `yes`, jeśli tylko aktywujemy interfejs maszyny.

- Aktywuj interfejsy sieciowe w obu urządzeniach poleceniem `ip` i sprawdź stan warstwy fizycznej interfejsów poleceniem `ethtool`.
- Interfejsowi sieciowemu maszyny *Virbian1* przypisz adres IP równy `192.168.100.1`, zaś interfejsowi maszyny *Virbian2* adres `192.168.100.2`. Pamiętaj o masce podsieci `/24`.
- Poleceniem `ping` sprawdź, czy jedna maszyna jest osiągalna z drugiej. Jaki jest RTT? Obejrzyj przesyłane pakiety Wiresharkiem. Wskaż w pakiecie miejsce w którym przechowywany jest źródłowy i docelowy adres IP.
- Wykorzystaj program `iperf3`, żeby zbadać przepustowość połączenia między maszynami.
- Z maszyny *Virbian1* połącz się z serwerem echa maszyny *Virbian2*. Zaobserwuj przesyłane pakiety w Wiresharkach uruchomionych jednocześnie na obu maszynach.

Materiały do kursu znajdują się w systemie SKOS: `https://skos.ii.uni.wroc.pl/`.

Marcin Bieńkowski