Warsztaty z Sieci komputerowych
Lista 6

Podczas tych zajęć topologia sieci nie jest interesująca. Do pierwszej części zadań przyda się połączenie z Internetem. Pamiętaj o rozpoczęciu pracy poleceniem `netmode lab` i skonfigurowaniu interfejsu `eth0` poleceniem `dhclient eth0`.

Zadanie 1. Odpytując iteracyjnie kolejne serwery DNS poleceniem `dig`, dowiedz się jaki jest adres IP związany z nazwą `www.cs.uni.wroc.pl`. Zacznij od jednego z serwerów głównych, np. `198.41.0.4`. Pierwszym poleceniem będzie:

```
$> dig www.cs.uni.wroc.pl @198.41.0.4
```

Kolejne polecenia kieruj do serwerów DNS, które są odpowiedzialne za odpowiednie strefy. Następnie pozwól teraz wykonać pracę z poprzedniego akapitu poleceniu `dig`, uruchamiając polecenie:

```
$> dig +trace www.cs.uni.wroc.pl @198.41.0.4
```

Jakie serwery DNS są odpytywane w tym przypadku?

Jeśli nie podamy serwera DNS po znaku `@` zapytanie będzie wysyłane do domyślnego serwera (zdefiniowanego w pliku `/etc/resolv.conf`), który rozwiązuje dla nas nazwy domen w sposób rekurencyjny. Sprawdź teraz jaki jest adres IP, serwery nazw i serwer obsługujący pocztę dla domeny `ii.uni.wroc.pl` poleceniami:

```
$> dig -t a ii.uni.wroc.pl
$> dig -t ns ii.uni.wroc.pl
$> host -t mx ii.uni.wroc.pl
```

Na końcu poleceniem

```
$> dig -t ptr 1.4.17.156.in-addr.arpa
```

sprawdź, jaka jest nazwa domeny związana z adresem `156.17.4.1`.

Zadanie 2. W tym poleceniu zobaczymy jak zapisać dane wysyłane przez program `dig` i potem wykorzystać je w trybie wsadowym.[1] Poleceniem

```
$> nc -u -l -p 10053
```

[1] W przypadku polecenia `dig` taka operacja nie ma większego sensu, bo polecenie `dig` łatwo wbudować we własny program. Ale ta sama technika umożliwia nagranie i późniejsze powtórzenie poleceń wysyłanych przez przeglądarkę WWW czy też komunikator internetowy; program `nc` może działać nawet na innym komputerze i nie musimy rozumieć, co jest przesyłane!

uruchom program `nc` w trybie serwera UDP nasłuchującego na porcie UDP 10053. Związanie ze standardowym portem 53 wymagałoby uprawnień administratora. Z drugiej konsoli wykonaj polecenie

```
$> dig -p 10053 onet.pl @127.0.0.1 +tries=1
```

Wyśle to jedno zapytanie DNS o adres IP dla nazwy `onet.pl` do naszego „serwera UDP". Zapytanie to (w binarnej i nieczytelnej postaci) zostało wypisane na ekranie. Ze względu na binarne dane, nie należy kopiować ich myszką, lecz przerwać wykonanie serwera UDP i uruchomić go w trybie zapisywania do pliku i na standardowe wyjście:

```
$> nc -u -l -p 10053 > zapytanie_dns
```

Następnie należy ponowić zapytanie DNS. Zawartość szesnastkową wysyłanego datagramu można podejrzeć poleceniem

```
$> hexdump -C zapytanie_dns
```

powinien tam występować ciąg `onet.pl`. Teraz zapisane zapytanie możemy wysłać jakiemuś serwerowi DNS, np. serwerowi `8.8.8.8` firmy Google. W tym celu wykonaj polecenie

```
$> nc -q 1 -u 8.8.8.8 53 < zapytanie_dns
```

Odpowiedź zostanie wyświetlona na ekranie w mało czytelnej postaci binarnej; sprawdź jej interpretację podglądając otrzymany pakiet w Wiresharku.

Zadanie 3. Uruchom klienta ftp poleceniem

```
$> lftp
```

a następnie połącz się z jakimś serwerem ftp zawierającym duże pliki, np. `ftp.kernel.org` wpisując w tym programie polecenie

```
> o ftp.kernel.org
```

Wpisz polecenie

```
> debug 9
```

które spowoduje wyświetlanie poleceń protokołu FTP. (Nie należy mylić poleceń *protokołu* FTP z poleceniami *programu* `lftp`). Polecenia protokołu FTP wyświetlane są po znaku `--->`, zaś odpowiedzi na nie po znaku `<---`. Po strukturze katalogów można się poruszać poleceniami `cd`, zaś listę plików wyświetla się poleceniem `ls`. Wpisz polecenie

```
> cd /pub/linux/kernel/v4.x
```

W drugim terminalu wyświetl aktualnie nawiązane połączenia poleceniem

```
$> netstat -tapn
```

Które z nich odpowiada za połączenie FTP? Włącz tryb pasywny poleceniem

```
> set ftp:passive-mode on
```

i zacznij pobierać jakiś duży plik, np. wydając polecenie

```
> mget linux-4.5.tar.xz
```

Podczas pobierania ponownie wyświetl nawiązane połączenia poleceniem

```
$> netstat -tapn
```

Jakie porty są wykorzystywane do przesyłania danych? Postaraj się odnaleźć ustalanie tych portów w poleceniach protokołu FTP. Kto ustalił numer portu, klient czy serwer?

Włącz tryb aktywny poleceniem

```
> set ftp:passive-mode off
```

Ponownie zacznij pobieranie dużego pliku i wyświetl nawiązane połączenia. Jakie porty wykorzystywane są tym razem? Kto je ustala?

Zadanie 4. Uruchom przeglądarkę Firefox (Iceweasel). Znajdź i zainstaluj rozszerzenie *Live HTTP Headers* (jeśli jeszcze nie jest zainstalowane). Umożliwia ono wyświetlanie w pasku bocznym przeglądarki wysyłanych i odbieranych nagłówków HTTP (w tym celu wybierz z menu pozycję *View* — *Sidebar* — *LiveHTTPHeaders*.

Sprawdź, co jest wysyłane podczas umieszczania komentarza na stronie http://www.ii.uni.wroc.pl/~mbi/hydepark/index.phtml. W tym zadaniu spróbujemy umieścić jakąś treść na tej stronie bez pośrednictwa przeglądarki. Wykorzystamy w tym celu program `nc`.

1. Wejdź przeglądarką na stronę http://www.ii.uni.wroc.pl/~mbi/hydepark/index.phtml.
2. W terminalu uruchom polecenie

   ```
   $> nc -l 8888
   ```

   tworzące serwer TCP nasłuchujący na porcie 8888.
3. Zmień w ustawieniach przeglądarki (*Edit* | *Preferences*, karta *Advanced* | *Network* | *Connection* | *Manual proxy configuration*) serwer proxy na `localhost`, port `8888`.
4. Wpisz jakąś treść w polu „Dodaj uwagę” i kliknij przycisk „Wyślij”. Zauważ, że żądanie HTTP zostało wysłane do nasłuchującego na porcie `8888` serwera TCP i wyświetlone w terminalu. Oczywiście słuchający na tym porcie program `nc` nie jest prawdziwym serwerem proxy i nie przekazał tego żądania HTTP dalej. Dlatego też odpowiedni komunikat nie został wysłany do serwera WWW, a przeglądarka nic nie wyświetliła.
5. Skopiuj wyświetlane żądanie HTTP myszką i zapisz do pliku `zapytanie`.
6. Wyślij to zapytanie do serwera WWW poleceniem

   ```
   $> nc -q 3 www.ii.uni.wroc.pl 80 < zapytanie
   ```

Sprawdź przeglądarką, czy odpowiedni komunikat został dodany na stronie WWW (uprzednio usuń ustawienia serwera proxy w przeglądarce).

7. Zmień zawartość pliku `zapytanie`, wpisując inny komunikat do umieszczenia na stronie. Nie zapomnij odpowiednio zmodyfikować pola `Content-Length`.
8. Ponownie wyślij zapytanie do serwera WWW i sprawdź, czy komunikat został dodany na stronie WWW.

Zadanie 5. Skonfiguruj wybrany program pocztowy (dostępne powinny być KMail i Evolution) do korzystania z adresu pocztowego `ccna`*i*`@example.com`, gdzie *i* jest numerem Twojego komputera. W Evolution możesz skorzystać z uruchamianego na początku programu kreatora ustawień, gdzie jako serwer poczty przychodzącej ustaw `POP` o adresie `eagle-server.example.com`, zaś jako serwer poczty wychodzącej `SMTP` o takim samym adresie. Nie włączaj szyfrowania.

Włącz Wiresharka nasłuchującego na interfejsie `eth0`. W programie Evolution kliknij przycisk *New*, napisz i wyślij testowy email do samego siebie. W Wiresharku znajdź jeden z przesyłanych segmentów TCP i wybierając z kontekstowego menu opcję *Follow TCP Stream* sprawdź, jakie komunikaty zostały wymienione między Twoim komputerem a serwerem SMTP.

Następnie kliknij przycisk *Send/Receive* i pobierz maile z serwera, podając hasło `cisco`. Ponownie obejrzyj w Wiresharku przesyłane komunikaty (tym razem między Twoim komputerem a serwerem POP3). Wyślij email do sąsiada i odbierając pocztę sprawdź, czy sąsiad też Ci taką wysłał.

Posiłkując się danymi zdobytymi przed chwilą w Wiresharku, poleceniem

```
$> telnet eagle-server.example.com 25
```

połącz się z portem SMTP i wyślij email do konta sąsiada. Jako nadawcę wpisz nieistniejący adres email. Możesz pominąć pola nagłówka lub wpisać tylko niektóre. Sprawdź, czy email dotarł.