Warsztaty z Sieci komputerowych
Lista 6

Podczas tych zajęć topologia sieci w pracowni nie będzie nas interesować.

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.wikipedia.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.wikipedia.pl @198.41.0.4
```

Jakie serwery DNS są odpytywane w tym przypadku? Wykonaj jeszcze raz powyższe polecenie, obserwując przesyłane zapytania i odpowiedzi w Wiresharku.

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
$> dig -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 też działać na innym komputerze.

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

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

Wyśle to jedno zapytanie DNS o adres IP dla nazwy `www.wikipedia.pl` do naszego „serwera". 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:

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

Następnie należy ponowić zapytanie DNS. Obejrzyj przesyłane zapytanie w Wiresharku. Zawartość szesnastkową wysyłanego datagramu można podejrzeć poleceniem

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

powinien tam występować ciąg `www.wikipedia.pl`. Sprawdź również, że szesnastkowa zawartość odpowiada zawartości datagramu, który widać w Wiresharku.

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`. Znak zachęty tego programu będziemy oznaczać ciągiem `LFTP>` Następnie połącz się z jakimś serwerem ftp zawierającym duże pliki, np. `cdimage.debian.org` wpisując w tym programie polecenie

```
LFTP> o cdimage.debian.org
```

Wpisz polecenie

```
LFTP> debug 9
```

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

```
LFTP> cd /cdimage/release/current/amd64/iso-cd
```

W drugim terminalu wyświetl aktualnie nawiązane połączenia poleceniem

```
$> netstat -tapn
```

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

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

i wyświetl listę plików poleceniem

```
LFTP> ls
```

Zacznij pobierać jakiś duży plik, np. wydając polecenie

```
LFTP> mget debian-8.8.0-amd64-CD-1.iso
```

(W razie braku `debian-8.8.0-amd64-CD-1.iso` zastąp go innym dużym plikiem). 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. Czy numer portu ustalił klient czy serwer?

Włącz tryb aktywny protokołu FTP poleceniem

```
LFTP> 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. W tym zadaniu pokażemy jak można wysyłać zapytania HTTP z wiersza poleceń i dodawać w ten sposób nowe wpisy na stronie http://www.ii.uni.wroc.pl/~mbi/hydepark/index.phtml. Przechwytywanie zapytań HTTP można zrealizować również za pomocą rozszerzenia LiveHTTPHeaders, ale w tym zadaniu posłużymy się znowu programem `nc`.

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

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

   tworzące serwer TCP nasłuchujący na porcie 8888.
3. W menu przeglądarki kliknij ikonę *Preferences*, w karcie *Advanced* | *Network* | *Connection* kliknij *Settings*, a następnie wybierz *Manual proxy configuration* i w polu *HTTP proxy* wpisz `localhost` a w sąsiednim polu *Port* wpisz 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. Odpowiednio zmodyfikuj pole `Content-Length`.

8. Ponownie wyślij zapytanie do serwera WWW i sprawdź, czy komunikat został dodany na stronie.

Zadanie 5. Skonfiguruj program pocztowy KMail do korzystania z adresu `ccna`*i*`@example.com`, gdzie *i* jest numerem Twojego komputera. W tym celu w Kmailu wybierz z menu opcję *Settings* | *Configure KMail*. W oknie konfiguracji z menu po lewej stronie wybierz ikonę *Identities*, a następnie zmodyfikuj domyślną tożsamość *Lab 109 Student* wpisując w polu *Email address* napis `ccna`*i*`@example.com`.

W tym samym oknie skonfiguruj serwer poczty przychodzącej. W tym celu z menu wybierz ikonę *Accounts* i w karcie *Receiving* kliknij przycisk *Add*. Wybierz *POP3 E-Mail Server*.[2] W polu *Incoming mail server* wpisz `eagle-server.example.com`, w polu *Username* wpisz `ccna`*i*, zaś w polu *Password* — `cisco`. W tym samym oknie, w karcie *Advanced* wybierz brak szyfrowania i port 110.

W tym samym oknie skonfiguruj również serwer poczty wychodzącej. Wybierz kartę *Sending* i kliknij przycisk *Add*. Wybierz swoją własną nazwę dla tego transportu maili i zaznacz, żeby było on wykorzystywany domyślnie. Następnie w polu *Outgoing mail server* wpisz `eagle-server.example.com` i pozostaw pole uwierzytelnienia puste. W karcie *Advanced* wybierz brak szyfrowania i port 25.

Włącz Wiresharka nasłuchującego na interfejsie `enp3s0`. W Kmailu kliknij przycisk *New*, napisz i wyślij testowy email do samego siebie (tj. do adresu `ccna`*i*`@example.com`). 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 *Check Mail* i pobierz maile z serwera. 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 w Kmailu, czy email dotarł.

Lista i materiały znajdują się pod adresem http://www.ii.uni.wroc.pl/~mbi/dyd/.

Marcin Bieńkowski

[2] Być może w tym momencie konieczne będzie uzyskanie dostępu do *KDE Wallet Service*; w takim przypadku wybierz opcję *Classic, blowfish encrypted file* i ustal własne hasło zabezpieczające *KDE Wallet*.