Warsztaty z Sieci komputerowych
Lista 6

Tutorial 1 (0 pkt.)

W tej części przyjrzymy się bliżej protokołowi DNS.

- Utwórz maszynę *Virbian0* z domyślną konfiguracją sieciową (jedna wirtualna karta sieciowa podłączona przez NAT z kartą fizyczną komputera). Po uruchomieniu maszyny poleceniem `ip` zmień nazwę interfejsu sieciowego na `enp0` i pobierz konfigurację sieciową poleceniem `dhclient`.

- Odpytując iteracyjnie kolejne serwery DNS poleceniem `dig`, dowiedz się jaki jest adres IP związany z nazwą `www.cs.uni.wroc.pl`. W tym celu zacznij od jednego z serwerów głównych, np. od `198.41.0.4`. Pierwszym poleceniem będzie zatem:

  ```
  V0$> dig www.cs.uni.wroc.pl @198.41.0.4
  ```

  Ten serwer powinien odpowiedzieć adresami serwerów DNS odpowiedzialnych za strefę `pl`. Wykonaj powyższe zapytanie, tym razem kierując je do jednego z serwerów odpowiedzialnych za strefę `pl`. Kolejne polecenia kieruj do serwerów DNS, które są odpowiedzialne za strefy `wroc.pl`, `uni.wroc.pl` i `cs.uni.wroc.pl`.

- Pozwól teraz wykonać całą pracę z poprzedniego akapitu programowi `dig`, wykonując polecenie

  ```
  V0$> dig +trace www.cs.uni.wroc.pl @198.41.0.4
  ```

  Porównaj wyjście programu z wynikami z poprzedniego punktu. 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 `@`, to 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:

  ```
  V0$> dig -t a ii.uni.wroc.pl
  V0$> dig -t ns ii.uni.wroc.pl
  V0$> dig -t mx ii.uni.wroc.pl
  ```

- Poleceniem

  ```
  V0$> dig -t ptr 11.4.17.156.in-addr.arpa
  ```

  sprawdź, jaka jest nazwa domeny związana z adresem `156.17.4.11`.

Tutorial 2 (0 pkt.)

Zobaczymy teraz jak zapisać dane wysyłane przez program `dig` i wykorzystać je w trybie wsadowym.

- Uruchom program `nc` w trybie serwera UDP nasłuchującego na porcie 10053 poleceniem

  ```
  V0$> nc -u -l -p 10053
  ```

  W drugiej konsoli wykonaj polecenie

  ```
  V0$> 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” (oczywiście nie należy oczekiwać na odpowiedź). Zapytanie to (w binarnej i nieczytelnej postaci) zostanie wypisane na ekranie.

- Ze względu na binarne dane, nie należy kopiować ich myszką, lecz przerwać wykonanie serwera UDP i uruchomić go, tak aby wynik był również zapisywany do pliku `dns_request`:

  ```
  V0$> nc -u -l -p 10053 | tee dns_request
  ```

  Ponów zapytanie DNS i obejrzyj przesyłane dane w Wiresharku. Wyłącz program `nc`, a szesnastkową zawartość wysyłanego datagramu podejrzyj poleceniem

  ```
  V0$> hexdump -C dns_request
  ```

  Powinien tam występować ciąg `www.wikipedia.pl`. Sprawdź również, że wyświetlana zawartość odpowiada datagramowi przechwyconemu przez Wiresharka.

- Zapisane zapytanie możemy wysłać dowolnemu serwerowi DNS (np. serwerowi `8.8.8.8` firmy Google). W tym celu wykonaj polecenie

  ```
  V0$> nc -q 1 -u 8.8.8.8 53 < dns_request
  ```

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

Zadanie do zaprezentowania (2 pkt.)

Celem tego zadania jest dodanie nowego wpisu na stronie http://sieci.ii.uni.wroc.pl/ za pomocą programu `nc`.

- Ponieważ domena `sieci.ii.uni.wroc.pl` nie jest rozpoznawana przez publiczne serwery DNS, dodaj wiersz

  ```
  156.17.4.30    sieci.ii.uni.wroc.pl
  ```

  do pliku `/etc/hosts`.

- Wejdź przeglądarką na stronę http://sieci.ii.uni.wroc.pl/ i wykorzystując rozszerzenie przeglądarki *Live HTTP Header* sprawdź, co dzieje się, kiedy dodajesz jakiś wpis.[1]

- Uruchom program `nc` w trybie serwera TCP nasłuchującego na porcie 8888 poleceniem

  ```
  V0$> nc -l -p 8888 | tee http_request
  ```

- Z menu przeglądarki wybierz pozycję *Edit* | *Preferences*, wyszukaj w opcjach *Network settings* i w okienku *Connection Settings* wybierz *Manual proxy configuration*. Następnie w polu *HTTP proxy* wpisz `localhost`, a w sąsiednim polu *Port* wpisz 8888.

- Na stronie http://sieci.ii.uni.wroc.pl/ wpisz jakąś treść w polu „Dodaj uwagę" i kliknij przycisk „Wyślij". Dlaczego przeglądarka wyświetla w pasku stanu komunikat *Waiting for sieci.ii.uni.wroc.pl* a odpowiedni wpis nie został dodany?

- Przerwij działanie programu `nc`. Co zapisał ten program do pliku `http_request`? Wyłącz ustawienia serwera proxy w przeglądarce.

- Wyślij zapisane zapytanie do serwera WWW poleceniem

  ```
  V0$> nc -q 3 sieci.ii.uni.wroc.pl 80 < http_request
  ```

  i sprawdź przeglądarką, czy odpowiedni komunikat został dodany na stronie WWW

- Zmień zawartość pliku `http_request`, wpisując inny komunikat do umieszczenia na stronie. Odpowiednio zmodyfikuj pole `Content-Length`. Ponownie wyślij zapytanie do serwera WWW i upewnij się, że komunikat został dodany na stronie.

Zadanie do zaprezentowania (3 pkt.)

Celem tej części jest prześledzenie zmian stanów protokołu TCP i przesyłanych segmentów.

- Poleceniem `dig` sprawdź, jakie adresy IP są przypisane do domeny `www.debian.org`. Wybierz jeden z nich; będziemy go nazywać ***adres_IP***.

- W jednej konsoli uruchom w polecenie

  ```
  V0$> (while true; do netstat -tan | grep adres_IP; done) | tee tcp_log
  ```

  zaś w drugiej pobierz stronę główną `www.debian.org` za pomocą polecenia

[1] Uwaga: jeśli wejdziemy na stronę https://sieci.ii.uni.wroc.pl/ to przeglądarka będzie później zawsze chciała nas łączyć za pomocą szyfrowanego protokołu HTTPS, którego nie uda się podsłuchać. W takim przypadku pomaga skasowanie katalogu `.mozilla`.

```
V0$> wget http://adres_IP/
```

(Podaliśmy bezpośrednio adres IP, a nie nazwę domeny, żeby mieć pewność, że będziemy łączyć się z konkretnym adresem IP).

Sprawdź, czy w pliku `tcp_log` zostały zaobserwowane stany TCP gniazda `SYN SENT`, `ESTABLISHED` i niektóre ze stanów zamykania połączenia. Jeśli Twoje łącze jest za szybkie i stanów nie udaje się zaobserwować, zmniejsz prędkość pobierania wykorzystując polecenie

```
V0$> trickle -d 10 wget http://adres_IP/
```

- W Wiresharku obejrzyj pakiety IP i zawarte w nich segmenty TCP związane z wykonanym powyżej zapytaniem i odpowiedzią HTTP. Jakie gniazda tworzone są do pobierania pliku przez HTTP? Jaki jest port źródłowy a jaki docelowy połączenia? Dla każdego przesyłanego segmentu TCP określ:
  - Jakie z flag `SYN` / `ACK` / `FIN` są włączone dla danego segmentu?
  - Które bajty (strumienia danych protokołu HTTP) są przesyłane w segmencie?
  - Które bajty strumienia danych są potwierdzane danym segmentem?
  - Na podstawie diagramu stanów TCP (https://en.wikipedia.org/wiki/File:Tcp_state_diagram.png), sprawdź jak zmienia się stan połączenia TCP (po stronie klienta i po stronie serwera) w momencie wysłania i odebrania danego segmentu. Które z tych stanów są widoczne w pliku `tcp_log`?

  Która strona wykonuje otwarcie aktywne, a która zamknięcie aktywne?

- Dezaktywuj kartę `enp0s3` poleceniem `ip link` i wyłącz maszynę wirtualną.

Tutorial 3 (0 pkt.)

W tej części przyjrzymy się działaniu protokołów pocztowych SMTP i POP3. Uruchom trzy maszyny wirtualne *Virbian1*, *Virbian2* i *Virbian3*, każda z jedną kartą sieciową wpiętą do wirtualnej sieci `local0`.

- Zmień nazwę wirtualnego interfejsu na wszystkich maszynach na `enp0`. W maszynie *Virbian*i (dla $i \in \{1, 2, 3\}$) przypisz mu adres `10.0.0.`i`/8`. Na wszystkich maszynach dodaj wpis

  ```
  10.0.0.1    mail.example.com
  ```

  do pliku `/etc/hosts`.

- Na maszynie *Virbian1* uruchom serwery SMTP i POP3 poleceniami

  ```
  V1#> systemctl start postfix
  V1#> systemctl start dovecot
  ```

- Na maszynie *Virbian2* skonfiguruj program *Thunderbird* do korzystania z adresu `student2@mail.example.com`. W tym celu w Thunderbirdzie (w kreatorze tworzenia konta pocztowego) wpisz swoje imię i nazwisko w polu *Your name*, w polu *Email address* wpisz `student2@mail.example.com`, zaś w polu *Password* wpisz `student2`. Po kliknięciu przycisku *Continue* część ustawień zostanie wykryta automatycznie; należy je sprawdzić i poprawić klikając przycisk *Manual config*.
  - W części *Incoming* powinien być wybrany protokół POP3, użytkownik `student2`, serwer `mail.example.com`, port 110, wyłączone szyfrowanie SSL, a w polu *Authentication* wybrana opcja *Normal password*.
  - W części *Outgoing* powinien być wybrany protokół SMTP, użytkownik `student2`, serwer `mail.example.com`, port 25, wyłączone szyfrowanie SSL, a w polu *Authentication* wybrana opcja *No authentication*

  Po kliknięciu przycisku *Done* należy przeczytać i następnie zignorować ostrzeżenie o używaniu nieszyfrowanych protokołów. Jeśli pojawi się okno konfiguracji modułu Enigmail, to należy je zamknąć przyciskiem *Cancel*.

- Wykonaj powyższy punkt z odpowiednimi zmianami, tak żeby skonfigurować program *Thunderbird* na maszynie *Virbian3* do korzystania z adresu `student3@mail.example.com`. (Jego hasło to `student3`, pozostałe opcje należy wybrać identycznie lub analogicznie).

- Włącz Wiresharka na maszynie *Virbian2*. W Thunderbirdzie na maszynie *Virbian2* kliknij przycisk *Write*, napisz i wyślij testowy email do adresu `student3@mail.example.com`). Odbierz ten mail w Thunderbirdzie uruchomionym na maszynie `Virbian3`.

- Wyślij maila z maszyny *Virbian2*, ale tym razem obejrzyj przesyłane pakiety 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 uruchomionym na maszynie *Virbian1*.

- Poleceniem

  ```
  V2$> telnet mail.example.com 25
  ```

  połącz się z portem SMTP i wykorzystaj dane zdobyte w Wiresharku do wysłania wiadomości do adresu `student3@mail.example.com`. Możesz pominąć pola nagłówka lub wpisać tylko niektóre. Na maszynie *Virbian3* sprawdź w Thunderbirdzie, czy mail dotarł.

- Wyłącz serwer SMTP i POP3 poleceniami

  ```
  V1#> systemctl stop postfix
  V1#> systemctl stop dovecot
  ```

  Dezaktywuj karty sieciowe i wyłącz maszyny wirtualne.

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

Marcin Bieńkowski