Warsztaty z Sieci komputerowych
Lista 6

Konfiguracja początkowa

- 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`.

Tutorial #1

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

- Poleceniem `host -a www.debian.org` 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

  `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?

Tutorial #2

W tej części przyjrzymy się bliżej protokołowi DNS.

- 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 -4 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 #3

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.

Wyzwanie #1

Celem tego zadania jest dodanie nowego wpisu na stronie WWW za pomocą programu `nc`.

- Uruchom usługę serwera WWW wyświetlającego prostą stronę służącą do dodawania wpisów uruchamiając polecenie

  ```
  V0#> systemctl start hydepark
  ```

- Włącz przeglądarkę[1] i otwórz w niej narzędzia deweloperskie (naciskając klawisz F12 lub wybierając z menu *More Tools* | *Web Developer Tools*); wybierz w nich kartę *Network*. Następnie wejdź przeglądarką na stronę `http://virbian:8080/`. W narzędziach deweloperskich sprawdź komunikację między przeglądarką i serwerem WWW: po kliknięciu zapytania można zobaczyć nagłówki i treść zapytania i odpowiedzi. Zaznaczając opcję *Raw* możesz wyświetlić te dane w postaci „surowej" bez interpretacji.

- W narzędziach deweloperskich przeglądarki Firefox sprawdź, co dzieje się, kiedy dodajesz jakiś wpis w formularzu. Spróbuj dodać wielowierszowy wpis zawierający polskie znaki. Co jest przesyłane jako treść zapytania?

- 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 *Settings*, 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://virbian:8080/` wpisz jakąś treść w polu „Dodaj jakiś komunikat" i kliknij przycisk „Wyślij". Dlaczego przeglądarka zachowuje się jakby oczekiwała na odpowiedź, a odpowiedni wpis nie zostaje 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 virbian 8080 < 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.

- Zakończ działanie serwera WWW poleceniem

  ```
  V0#> systemctl stop hydepark
  ```

  Dezaktywuj kartę `enp0` poleceniem `ip link` i wyłącz maszynę wirtualną.

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

Marcin Bieńkowski

[1] Rozszerzenie *HTTP Header Live* dodane w Virbianie do Firefoksa stało się przestarzałe i jeśli Firefox uzyska dostęp do internetu, to po jakimś czasie je wyłączy ze stosownym komunikatem.