Warsztaty nr 6 z Sieci komputerowych

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 `dhcpcd` lub `dhclient`.
- Uruchom Wiresharka nasłuchującego na wszystkich interfejsach.

Tutorial 1

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

- Poleceniem `dig example.org A` sprawdź, jakie adresy IP są przypisane do domeny `example.org`. Wybierz jeden z nich; będziemy go nazywać *`adres_IP`*.
- W jednym terminalu uruchom polecenie

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

  zaś w drugiej pobierz stronę główną `example.org` za pomocą polecenia[1]

  ```
  curl -4 --connect-to example.org:adres_IP http://example.org/
  ```

  Opcja `--connect-to` wyłącza rozpoznawanie nazw domen; dzięki niej mamy pewność, że łączymy się z wybranym adresem IP.

  Sprawdź, czy w pliku `tcp_log` zostały zaobserwowane stany gniazda TCP takie jak `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 1 curl -4 --connect-to example.org:adres_IP http://example.org/
  ```

  Zignoruj komunikat o niedostępności serwera `trickled`.
- W Wiresharku obejrzyj pakiety IP i zawarte w nich segmenty TCP związane z wykonanym powyżej zapytaniem i odpowiedzią HTTP.
  - Jakie są nagłówki zapytania i odpowiedzi HTTP?
  - Jaki jest port źródłowy a jaki docelowy połączenia?

  Dla każdego przesyłanego segmentu TCP określ:
  - Które z flag `SYN` / `ACK` / `FIN` są włączone dla danego segmentu?
  - Które bajty (strumienia danych protokołu HTTP) są przesyłane w danym segmencie?
  - Które bajty strumienia danych są potwierdzane danym segmentem?

[1] Jeśli masz starszą wersję Virbiana i polecenie `curl` nie jest dostępne, możesz wykorzystać polecenie `wget` lub zainstalować pakiet `curl` za pomocą `apt`.

- 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?
- Wykonaj powyższą analizę flag oraz numerowania przesyłanych i potwierdzanych bajtów pobierając inną, większą stronę WWW. Przykładowo możesz wykonać polecenie

  ```
  curl -4 https://www.debian.org/
  ```

  Ile danych przesyłanych jest w ramach pojedynczego połączenia TCP? Czy liczba segmentów z potwierdzeniami jest równa liczbie segmentów z danymi?

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.ii.uni.wroc.pl`. W tym celu zacznij od jednego z serwerów głównych, np. od `198.41.0.4`. Ponieważ pytamy o rekord `A`, pierwszym poleceniem będzie

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

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

  ```
  V0$> dig -4 +trace @198.41.0.4 www.ii.uni.wroc.pl A
  ```

  Porównaj wyjście programu z wynikami z poprzedniego punktu. Jakie serwery DNS są odpytywane w tym przypadku?
- 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$> dig ii.uni.wroc.pl A
  V0$> dig ii.uni.wroc.pl NS
  V0$> dig ii.uni.wroc.pl MX
  ```

  Zaobserwuj przesyłane zapytania i odpowiedzi DNS w Wiresharku.

  - Jakie są warstwy tych komunikatów? Jaki protokół warstwy transportowej jest wykorzystywany przez DNS? Jaki port wykorzystuje?
  - Porównaj adres IP wpisany w pliku `/etc/resolv.conf` z adresem IP, do którego kierowane są zapytania DNS.
  - Porównaj pola z liczbą pytań i odpowiedzi w zapytaniu i odpowiedzi DNS. Dlaczego odpowiedź zawiera kopię zapytania?

- Poleceniem

```
V0$> dig 11.4.17.156.in-addr.arpa PTR
```

sprawdź, jaka jest nazwa domeny związana z adresem `156.17.4.11`. Spróbuj uzyskać tę samą informację wykonując iteracyjne przechodzenie przez drzewo DNS, ponownie zaczynając od serwera DNS o adresie `198.41.0.4`.

Tutorial 3

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

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

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

W drugim terminalu wykonaj polecenie

```
V0$> dig -p 10053 +tries=1 @127.0.0.1 www.wikipedia.pl A
```

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 resolverowi DNS (np. `8.8.8.8`). W tym celu wykonaj polecenie

```
V0$> nc -w 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

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

- Wykonaj polecenie

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

Uruchomi ono usługę serwera WWW nasłuchującego na porcie 8080 i wyświetlającego prostą stronę służącą do dodawania wpisów.

- Włącz przeglądarkę i otwórz w niej narzędzia deweloperskie (naciskając klawisz F12 lub wybierając z menu *More Tools* | *Web Developer Tools*); wybierz w nich kartę *Network*. Następnie otwórz w przeglądarce 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? Czy wykorzystywana jest metoda `GET` czy `POST` protokołu HTTP?
- 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. Zatwierdź zmiany przyciskiem *OK*.
- Na stronie http://virbian:8080/ wpisz jakąś treść w okienku tekstowym i kliknij przycisk wysyłania. Dlaczego przeglądarka zachowuje się jakby oczekiwała na odpowiedź, a odpowiedni wpis nie zostaje dodany?
- Przerwij działanie programu `nc`. Co zostało zapisane do pliku `http_request`? Wyłącz ustawienia serwera proxy w przeglądarce.
- Wyślij zapisane zapytanie do serwera WWW poleceniem

  ```
  V0$> nc -w 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 przeglądarką, że komunikat został dodany na stronie.

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

Marcin Bieńkowski