Warsztaty 6 Sieci Komputerowe

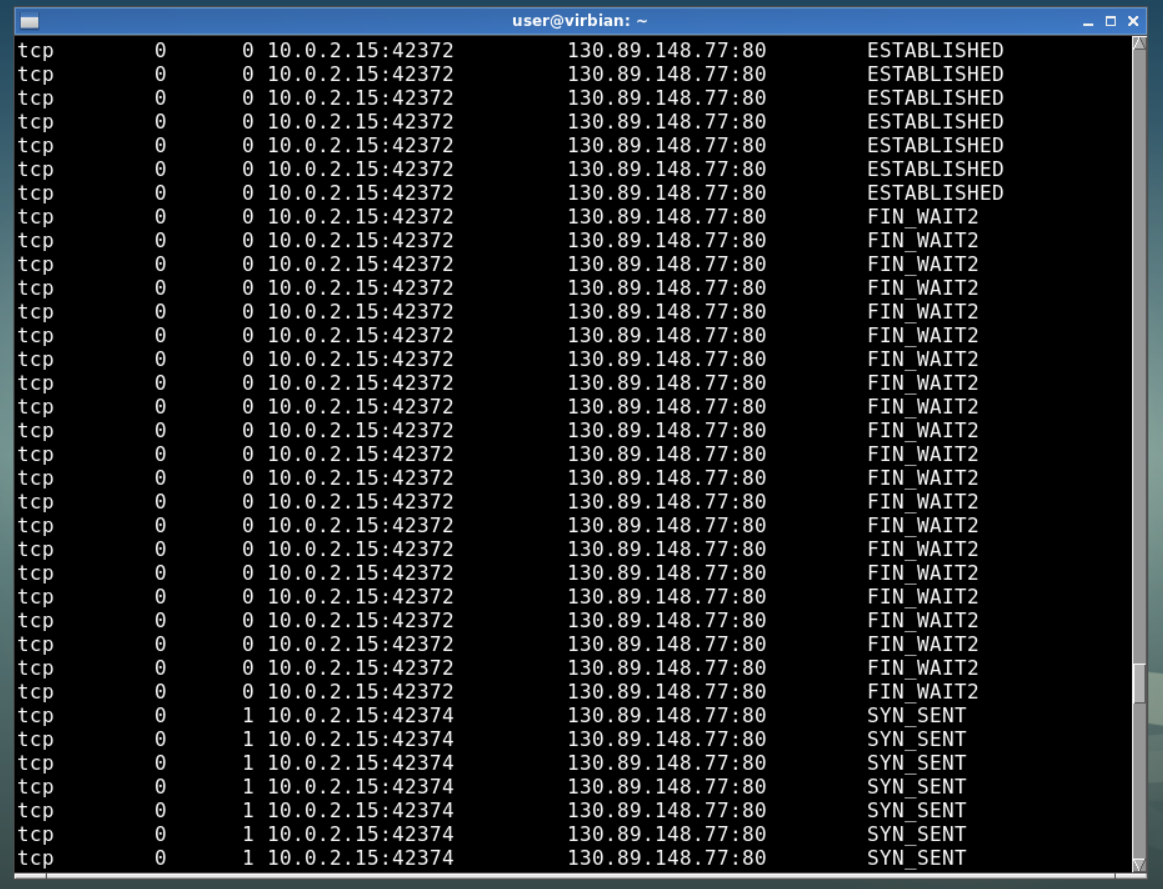
Konrad Kasprzyk

Zadanie do zaprezentowania (2 pkt.)

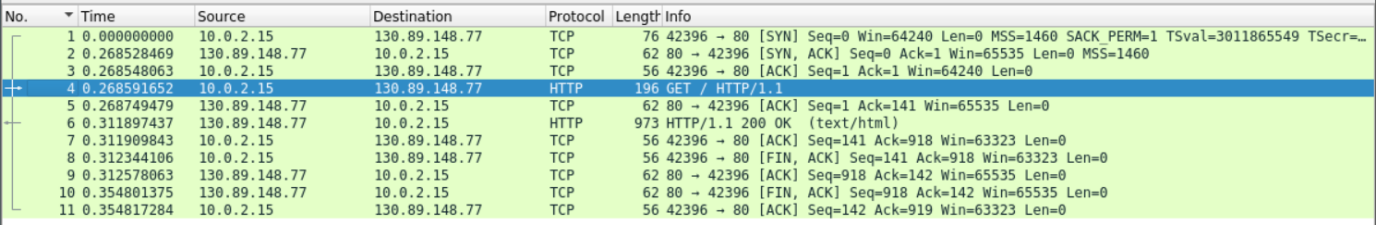
* Wejdź przeglądarką na stronę http://sieci.ii.uni.wroc.pl/ i wykorzystując rozszerzenie przeglądarki Live HTTP Header sprawdź, co dzieje się, kiedy dodajesz jakiś wpis.  
    
  Wysyłamy zapytanie do pliku (adresu) akcept.php z treścią naszego wpisu. Potem Zostajemy przekierowani do pliku index.php. Na końcu odwołujemy się do pliku favion.ico, który nie zostaje odnaleziony.
* 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?  
    
  Przeglądarce ustawiliśmy nasz lokalny serwer na porcie 8888 jako serwer Proxy. Na terminalu widzimy, że nasz lokalny serwer przechwycił żądanie. Jednak nasz lokalny serwer nie odpowiada przeglądarce.
* Przerwij działanie programu nc. Co zapisał ten program do pliku http request?  
    
  Zapisał przechwycone żądanie w czytelnej formie (nie binarnej). Po wyłączeniu ustawień Proxy i wpisaniu nc -q 3 sieci.ii.uni.wroc.pl 80 < http request, komunikat z tego żądania został dodany na stronie. Po zmianie zawartości w http request i ponownym wysłaniu, zmiany są widoczne na stronie.

Zadanie do zaprezentowania (3 pkt.)

* 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  
    
  wklejam wynik grep –v TIME\_WAIT tcp\_log



* 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?



* Jakie gniazda tworzone są do pobierania pliku przez HTTP?  
    
  Gniazda połączone. Są opisane między innymi przez lokalny IP, lokalny port, zdalny IP, zdalny port.
* Jaki jest port źródłowy a jaki docelowy połączenia?  
    
  Port serwera to 80, jest dobrze znany. U mnie system przydzielił port 42496, został losowo przydzielony, nie jest dobrze znany.
* Dla każdego przesyłanego segmentu TCP określ:  
    
  Pierwsze 3 segmenty to trójfazowe nawiązywanie połączenia. Na diagramie TCP z linku są to stany nad ESTABLISHED. Klient wysyła [SYN], dostaje [SYN, ACK] i odpowiada [ACK]. Nie ma tu wymiany danych przez HTTP.  
    
  Teraz połączenie jest nawiązane. Na diagramie stanów TCP z linku jest to stan ESTABLISHED na zielonym tle.  
    
  Kolejne segmenty to pobranie strony, po kolei:  
  4. Wysłanie żądanie GET pod wskazany adres IP, by pobrać stronę. Komunikacja HTTP.  
  5. Odpowiedź serwera [ACK], że otrzymał żądanie GET.  
  6. Otrzymanie strony w HTML od serwera. Komunikacja HTTP.  
  7. Wysłanie serwerowi potwierdzenia otrzymania strony [ACK].  
    
  Teraz następuje czterofazowe kończenie połączenia. Na diagramie TCP z linku są to stany pod ESTABLISHED w ramkach Active Close i Passive Close.  
    
  Klient wysyła [FIN, ACK], Serwer odpowiada [ACK] oraz w drugim segmencie [ACK, FIN]. Klient teraz przechodzi w stan TIME WAIT. Wysyła serwerowi [ACK] otrzymania poprzednich flag.
* Które z tych stanów są widoczne w pliku tcp log?  
    
  W pliku tcp\_log są widoczne stany z diagramu TCP: TIME\_WAIT, SYN\_SENT, ESTABILISHED, FIN\_WAIT2.
* Która strona wykonuje otwarcie aktywne, a która zamknięcie aktywne?  
    
  Klient wykonuje otwarcie aktywne i zamknięcie aktywne. To on pierwszy wysyła segmenty do serwera.