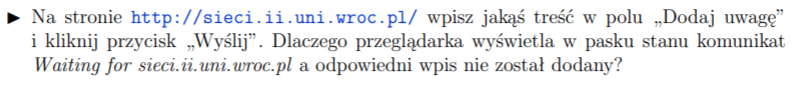
**Warsztaty 6 z Sieci Komputerowych**

**Pierwsze zadanie do zaprezentowania:**



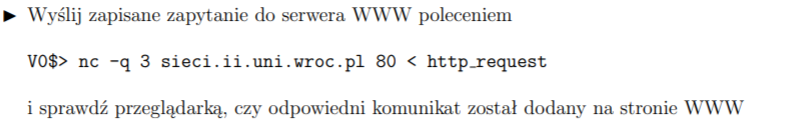
W oknie Live HTTP Header pojawia się nowa pozycja o nagłówku <http://sieci.ii.uni.wroc.pl/accept.php>. Jest tam wiersz: tresc=[tresc wyslanego przez formularz komunikatu]. Oznacza to, że serwer za pomocą accept.php przyjął i przetworzył wysłany napis.



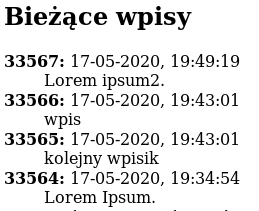
Przeglądarce poleciliśmy, aby łączyła się przez proxy localhost:8888. Na adresie localhost, porcie 8888 nasłuchuje nasz program nc włączony wcześniej w konsoli. Przechwycił on wysłany komunikat http. Możemy to sprawdzić oglądając wysłane pakiety w wiresharku oraz patrząc na konsolę z uruchomionym programem. Zobaczymy tam wysłany komunikat z naszą zawartością, którą chcieliśmy wysłać na stronę.

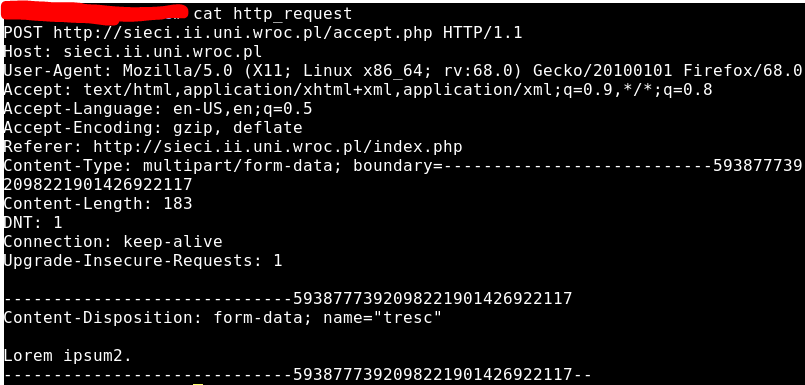


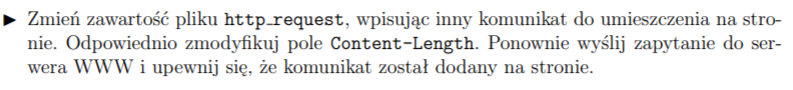
Program zapisał do http\_request komunikat, który chcieliśmy wysłać na stronę sieci.ii.uni.wroc.pl. Taki sam komunikat wyświetlił się po odebraniu komunikatu przez nc z przeglądarki.



Jak widzimy poniżej, został dodany wpis o treści „Lorem ipsum2.”. Poniżej wklejam również zawartość pliku http\_request.







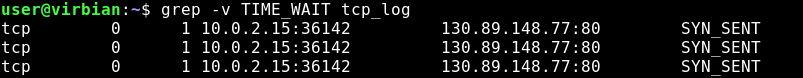
Zmodyfikowałem napis „Lorem ipsum2.” na „Lorem ipsum222.”. Zmieniłem także pole „Content-Length” z 183 na 185 (ponieważ doszły dwie liczby 2, a więc 2 dodatkowe bajty). Poniżej widzimy wynik wysłania zmodyfikowanego komunikatu na stronie.



**Drugie zadanie do zaprezentowania:**

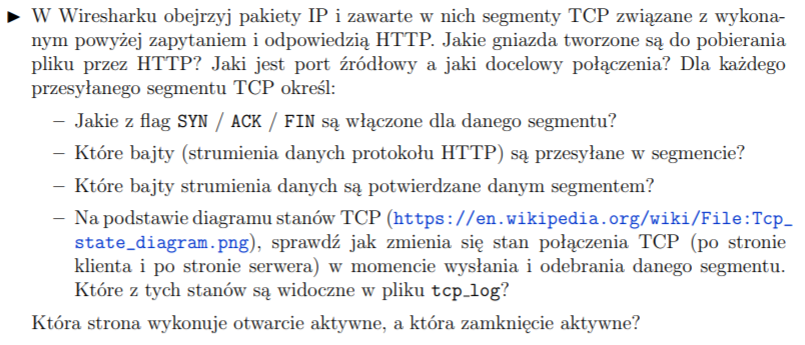




Moim adresem „adres\_IP” będzie 130.89.148.77. Użycie „trickle” nie przyniosło rezultatu (widzę tylko stany TIME\_WAIT), jednak przeszukując plik „tcp\_log” z wyłączeniem linijek „TIME\_WAIT” można zaobserwować jeszcze 3 inne stany połączenia:  




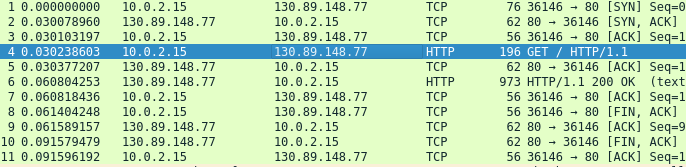




**Jakie gniazda tworzone są do pobierania pliku przez HTTP ?** Są tworzone gniazda połączone. Następuje nawiązanie połączenia między userem a serwerem.

**Jaki jest port źródłowy, a jaki docelowy połączenia?** Host wysyła z portu 36146 na port 80 serwera. W drugą stronę jest odwrotnie (serwer wysyła przez 80, host dostaje na 36146).

**- Jakie z flag SYN / ACK / FIN są włączone dla danego segmentu?**



Przeanalizujmy po kolei pakiety. Możemy tutaj zauważyć tzw. „three way handshake”. Host wysyła pakiet TCP z flagą SYN w celu nawiązania połączenia. Serwer odpowiada pakietem z flagami SYN oraz ACK (również rozpoczyna połączenie i potwierdza otrzymanie pakietu SYN od hosta). Trzeci krok to wysłanie przez hosta pakietu z flagą ACK, czyli potwierdzenie otrzymania pakietu SYN od serwera. Połączenie zostaje nawiązane. Potem mamy wysłania żądania GET do serwera (aby pobrać stronę html). Serwer najpierw potwierdza otrzymanie pakietu za pomocą ACK, potem wysyła przez HTTP żądany zasób z kodem 200 (OK). Host potwierdza flagą ACK, zaraz po tym wysyła pakiet, którym chce zakończyć połączenie (FIN, ACK). Serwer potwierdza otrzymanie wiadomości, zaraz po tym wysyła również pakiet z flagami FIN, ACK do hosta i na końcu host potwierdza otrzymanie flagą ACK.

**- Które bajty (strumienia danych protokołu http) są przesyłane w segmencie?**

Pakiety HTTP możemy zaobserwować w dwóch miejscach. Pierwszy pakiet http to żądanie GET od hosta do serwera w celu pobrania strony, drugi to odpowiedź serwera z żądaną stroną html wysłana do hosta.

Pierwszy pakiet HTTP zawiera m.in:

* Napis „GET” mówiący co zawierają dalsze dane
* Informacje na temat nadawcy wiadomości
* Kodowanie
* Adres ip, na który łączy się nadawca
* Informacje o połączeniu

Drugi pakiet HTTP zawiera m.in:

* Napis „GET” oraz kod mówiący czy wszystko udało się zrobić
* Datę
* Informacje o serwerze
* Kiedy zawartość strony była modyfikowana
* Informacje o połączeniu
* Długość pakietu

**- Które ze stanów TCP są widoczne w pliku tcp\_log?**

TIME\_WAIT, SYN\_SENT, ESTABLISHED oraz FIN\_WAIT2

-Która strona wykonuje otwarcie aktywne, a która zamknięcie aktywne?

Obie czynności wykonuje host.