

SIP – Studia Podyplomowe dla nie-inżynierów

Ćwiczenie laboratoryjne 1 Instrukcja

Instytut Telekomunikacji
Wydział Elektroniki i Technik Informatycznych
Politechnika Warszawska, marzec 2015

Wprowadzenie

Ćwiczenie jest wykonywane na komputerach z systemem operacyjnym Windows XP, które pełnią rolę hostów sieci IP. Komputery te są w rzeczywistości maszynami wirtualnymi, uruchomionymi w infrastrukturze informatycznej Zakładu Sieci i Usług Teleinformatycznych na WEiTI PW. Dostęp do maszyn jest realizowany w sposób zdalny, z dowolnego komputera PC wyposażonego w dostęp do sieci Internet, klienta protokołu ssh (np. PuTTY) oraz klienta usługi Remote Desktop. Dostęp do zasobów laboratorium wymaga ich uprzedniej rezerwacji w Systemie Rezerwacji, który jest dostępny za pośrednictwem publicznej strony internetowej.

Szczegóły dotyczące dostępu oraz korzystania z systemu rezerwacji opisane są w osobnym dokumencie – *ResourceReservation-UsersGuide*. Szczegóły zdalnego dostępu do zasobów laboratorium opisane są w dokumencie *RemoteAccess-UsersGuide*. Obydwa te dokumenty powinny być udostępnione razem z niniejszą instrukcją i stanowią jej integralną część.

Uwaga: przed rozpoczęciem ćwiczenia proszę upewnić się, że połączenia zdalne (Remote Desktop) z maszynami, na których wykonywane są ćwiczenia są skonfigurowane tak, że możliwe jest przesyłanie plików z tych maszyn na dysk lokalny (odpowiednie zasoby lokalne zostały „podłączone” w opcjach połączenia zdalnego przed nawiązaniem sesji). Jest to niezbędne do przesłania plików (np. logów z aplikacji Wireshark), które będą stanowiły załączniki do sprawozdania.

Uwaga: proszę **nie modyfikować ustawień sieciowych maszyn wirtualnych** i nie wykonywać na nich żadnych działań wykraczających poza czynności opisane w niniejszej instrukcji.

Przebieg ćwiczenia

1. Zapoznanie się z podstawami HTML

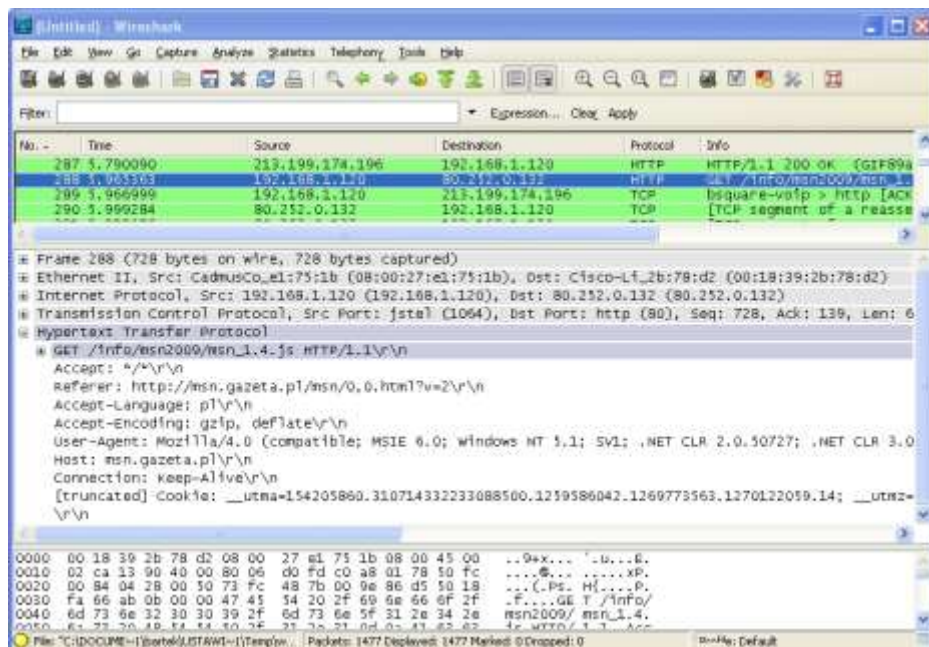
Przed rozpoczęciem ćwiczenia należy się zapoznać się z podstawowymi elementami języka HTML; w czasie laboratorium będzie to niezbędne do modyfikacji kodu źródłowego strony internetowej. W tym celu można skorzystać ze strony <http://www.w3schools.com/html/default.asp>.

2. Zapoznanie się z podstawami protokołu HTTP

Przed rozpoczęciem ćwiczenia należy się zapoznać z podstawami protokołu HTTP. Laboratorium będzie polegało na wysyłaniu i odbieraniu wiadomości tego protokołu. Opis protokołu można znaleźć w dokumencie <http://www.ietf.org/rfc/rfc2616.txt>, który należy jednak traktować tylko jako źródło wiedzy pomocne w laboratorium, nie jest natomiast wymagane zapoznanie się z całym dokumentem.

3. Zapoznanie się z programem **Wireshark**

Wireshark jest analizatorem protokołów, udostępnionym pod licencją GNU. Jest dostępny na większości popularnych systemów operacyjnych (Windows, Unix, Linux, OS X). Pozwala na obserwację i zapisywanie pakietów przesyłanych na interfejsach sieciowych komputera. Warto zapoznać się z jego podstawowymi możliwościami jeszcze przed rozpoczęciem ćwiczenia.



Na stronie <http://www.wireshark.org/> znajduje się dokumentacja do programu, bardzo obszerna, jako że oferuje on bardzo duże możliwości. Poniżej zostaną zaprezentowane podstawowe opcje, które mogą się przydać w trakcie ćwiczenia.

Filtrowanie pokazywanych pakietów wyrażeniami:

```
ip.src==194.29.169.x
ip.dst==194.29.169.x
```

Wyrażenia można łączyć za pomocą logicznych operatorów, dlatego do ćwiczenia wpisujemy jako „src” komputer, na którym pracujemy, a jako „dst” drugą stronę np.

```
ip.src==194.29.169.30 and ip.dst==194.29.169.91
```

Dzięki temu w oknie nie pojawią nam się nieistotne w danej chwili informacje. Należy jednak pamiętać, że taki filtr może powodować, że nie widzimy wszystkich istotnych wiadomości, np. zapytań o adres hosta.

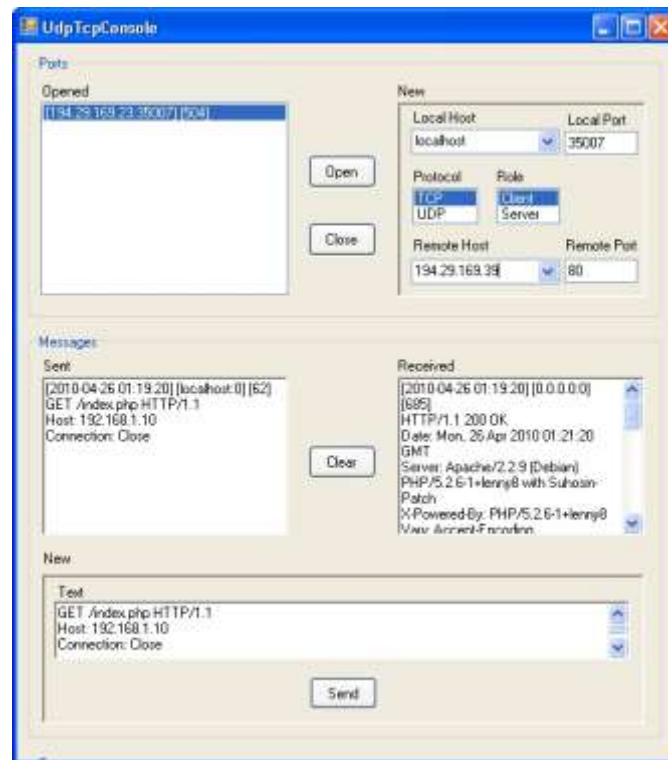
4. Ustalenie konfiguracji sieciowej

Na początku należy ustalić konfigurację swojego komputera (adres fizyczny MAC, adres IP, maska podsieci, itd.) Służy do tego polecenie **ipconfig**. Należy uruchomić program linii poleceń poprzez wybranie „Start -> Run...”, wpisanie **cmd.exe** i naciśnięcie klawisza Enter. Pojawi się konsola systemu Windows. Następnie należy uruchomić pomoc **ipconfig** poprzez wywołanie komendy `ipconfig /all`.

Serwer, na którym znajduje się strona WWW przeznaczona do pobrania ma adres IP **10.0.0.129**.

5. Aplikacja **UdpTcpConsole**

Normalnie, do pobierania stron WWW korzysta się z przeglądarek internetowych, takich jak np. Internet Explorer, Opera czy Firefox. W ramach ćwiczenia zamiast przeglądarki trzeba będzie skorzystać z programu **UdpTcpConsole** w taki sposób, aby zasymulować działanie przeglądarki, tzn. wysłać odpowiednie żądania protokołu HTTP, a z otrzymanych odpowiedzi odtworzyć całą stronę WWW.



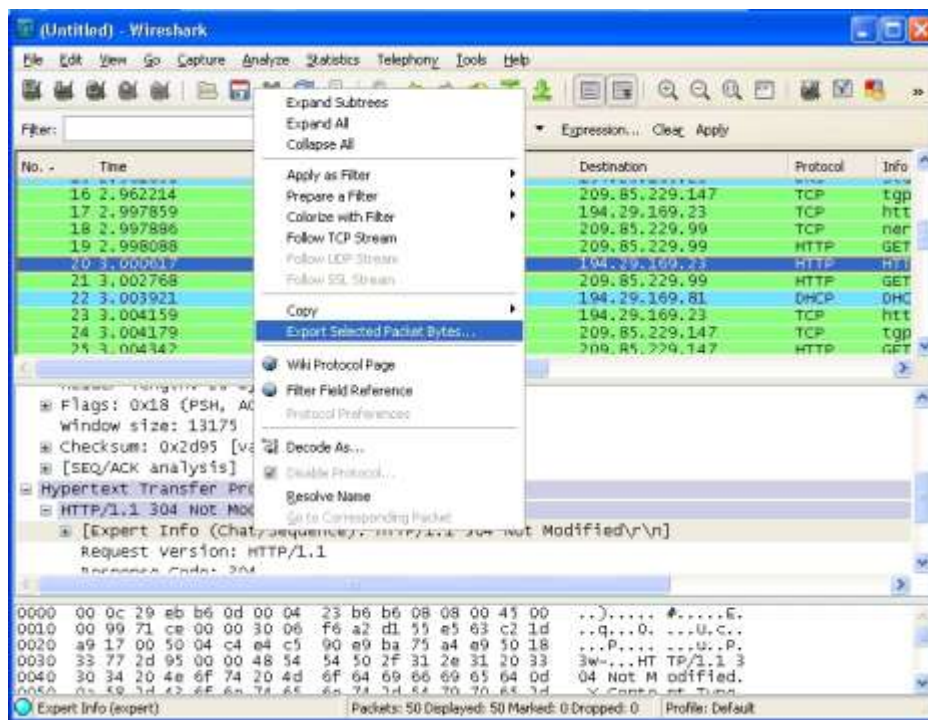
W celu wysłania żądania do serwera, należy w aplikacji **UdpTcpConsole** utworzyć połączenie klienckie: w oknie „New” jako „Protocol” należy wybrać *TCP*, a jako „Role” wybrać *Client*; jako „Remote Host” należy wpisać adres sieciowy serwera WWW, a port zdalny pozostawić w polu „Remote Port” ustawiony na 80; port lokalny w polu „Local Port” należy ustawić na dowolny wolny numer portu, np. 10001; na koniec należy utworzyć port komunikacyjny i połączenie klienckie klikając przycisk „Open”.

Należy uruchomić program **WireShark** i rozpocząć nasłuchiwanie. Można oczywiście ustawić filtrowanie pakietów na podstawie adresów serwera WWW i wykorzystywanego komputera.

Na serwerze znajduje się plik o nazwie *index.php*, którego należy zażądać od serwera. Po wybraniu utworzonego portu z listy otwartych portów, należy przejść do okna „Text”, by wpisać żądanie. Znajduje się tam przykładowe żądanie typu GET, które należy odpowiednio zmodyfikować, na podstawie wiedzy o protokole HTTP (chodzi o odpowiednie uzupełnienie nagłówków). Uwaga: W tym jak i w kolejnych wysyłanych żądaniach musi się znajdować nagłówek `User-Agent: UdpTcpConsole`.

Po wysłaniu żądania i otrzymaniu odpowiedzi zawierającej kod HTML, kod należy przekopiować do pliku tekstowego (warto korzystać z programu **notepad++**, który po wybraniu języka HTML odpowiednio koloruje elementy składni dokumentu HTML). Należy zapisać plik z rozszerzeniem *.html*, po czym otworzyć go w dowolnej przeglądarce internetowej. Jak łatwo zauważyć, na stronie brakuje pewnych elementów. Aby je uzupełnić, należy przejrzeć kod HTML w celu odnalezienia wszelkich zasobów, które są użyte/wskazane na stronie (obrazki, dźwięki, filmy, CSS, itp.). Do pobrania każdego z nich należy użyć osobnego żądania GET, żądając od serwera przesłania odpowiedniego elementu. Część pobranych elementów będzie dostępna bezpośrednio poprzez program UdpTcpConsole w oknie odbiorczym, natomiast niektóre elementy należy zapisać z wykorzystaniem programu **WireShark**. W tym celu należy odnaleźć zapisany przez program **WireShark** pakiet z odpowiedzią 200 OK na wybrane żądanie, w podglądzie pakietu odnaleźć fragment z danymi (PNG, WAV, itd.), i klikając prawym przyciskiem polecenie **Export Selected Packet Bytes...** zapisać dane do pliku z odpowiednim dla nich rozszerzeniem (*.png, .jpg, .wav, itd.*)

Uwaga: w razie problemów z aplikacją UdpTcpConsole („crash” po próbie wysłania wiadomości) proszę wysyłać wiadomości http bez nagłówka *Connection: Close*



Po zapisaniu wszystkich elementów pobranej i zapisanej wcześniej strony, należy umieścić je w folderze razem ze stroną. Następnie trzeba zmodyfikować plik *.html*, podmieniając ścieżki elementów, które zostały pobrane, na odpowiednie ścieżki lokalne. Należy otworzyć plik *.html* z użyciem przeglądarki i zobaczyć, czy strona wyświetla się poprawnie. **Proszę wykonać zrzut ekranu z otrzymaną w ten sposób stroną i dołączyć go do protokołu. Do protokołu należy również dołączyć folder z plikiem *.html* i pobranymi elementami.**

6. Sprawozdanie

Należy przygotować dokument (w formacie PDF) zawierający opis przebiegu ćwiczenia, obserwacje i wnioski na temat rodzajów wiadomości przesyłanych w sieci (tzn. wytłumaczenie, jakie rodzaje wiadomości, kiedy i w jakim celu zostały wysłane). Do protokołu powinny być dołączone zrzuty z programu Wireshark (w formacie *.pcap*) zebrane podczas ćwiczenia, oraz ewentualne pliki wymienione wcześniej w instrukcji.