Politechnika Rzeszowska
Katedra Mechaniki Stosowanej i Robotyki

SIECI KOMPUTEROWE I BAZY DANYCH
Laboratorium

Temat 2:

Warstwa Aplikacji
Protokół HTTP, DNS

Autor: dr inż. Paweł Penar

Rzeszów 2024

Instrukcja przygotowana z wykorzystaniem materiałów dodatkowych do książki Computer Networking: A Top-Down Approach, edycja 8 autorstwa J.F. Kurose and K.W. Ross dostępnych pod adresem: https://gaia.cs.umass.edu/kurose_ross/index.php

Liczba laboratoriów z tematu: 2

1. Cel laboratorium

Celem laboratorium jest zapoznanie studentów z dwoma protokołami warstwy aplikacji: HTTP (ang. Hypertext Transfer Protocol) i DNS (ang. Domain Name System).

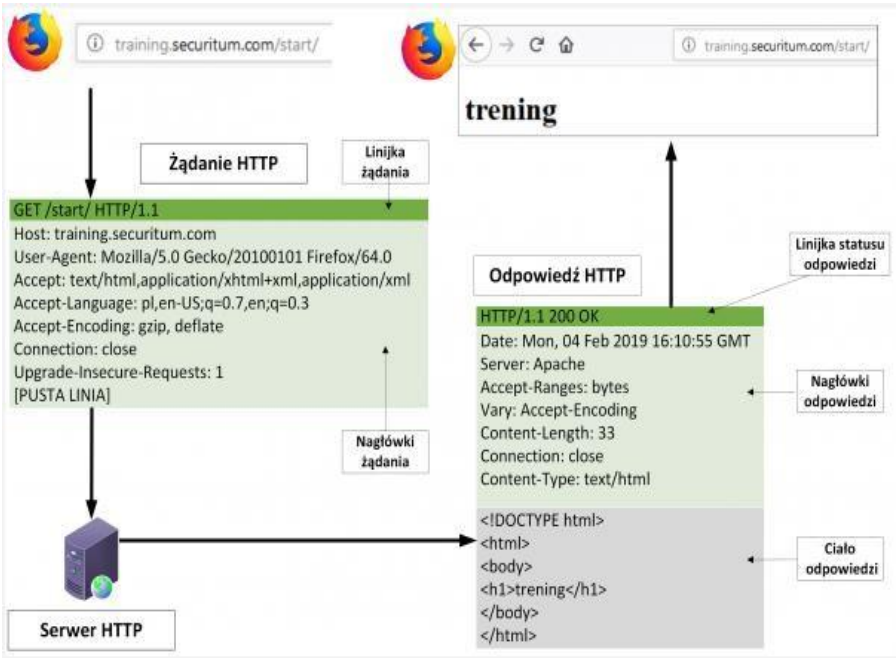
2. Wprowadzenie

2.1. Protokół HTTP

HTTP to protokół do pobierania zasobów serwera, takich jak dokumenty HTML. Jest ważnym protokołem służącym do wymiany danych w sieci działającym w architekturze klient-serwer. Ten typ architektury oznacza, że klient inicjuje komunikacji poprzez wysłanie żądania (*request*) do serwera. Protokół HTTP normalizuje sposób komunikacji, a zatem określa formę żądania i odpowiedzi (*response*) serwera. Jego powszechność jest związana z pobieraniem dokumentów HTML które są przetwarzane przez przeglądarki internetowe. HTTP jest protokołem bezstanowym co oznacza, że nie zachowuje informacji o wcześniejszych żądaniach klienta. Ta cecha stanowi problem w przypadku, gdy użytkownik powinien być identyfikowany, by w sposób intuicyjny wchodzić w interakcje ze stronami np. sklep internetowy. Ten problem rozwiązuje się wykorzystując mechanizm sesji po stronie serwera z wykorzystaniem tzw. ciasteczek.

Domyślny port dla protokołu HTTP, który opisano w dokumencie RFC7230, to port 80.

Najczęściej spotkamy się z komunikacją HTTP odbywającą się z wykorzystaniem protokołu TCP. Komunikacja HTTP realizowana jest poprzez wysłanie żądania do serwera, który następnie generuje odpowiedź. Ten schemat pokazano na rys. 1.



Rysunek 1: Komunikacja HTTP (źródło: LINK)

W rozważanym przypadku żądanie HTTP ma postać

```
GET /start/ HTTP/1.1
Host: training.securitum.com
[pusta-linia]
Accept: text/html,application/xhtml+xml
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cache-Control: max-age=0
Connection: keep-alive
…
```

Pierwsza linia żądania zawiera:

- Metodę (w tym wypadku GET). Inne metody to np. GET, HEAD, POST, PUT, DELETE. Ich opis znajduje się w dokumencie RFC7231
- Adres URL (w rozpatrywanym przypadku /start/)
- Wersje protokołu

Elementy pierwszej linii żądania rozdziela spacja. Dalszą część żądania stanowią niewymagane nagłówki. Ich spis znajduje się m.in. na stronie: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers

Odpowiedz serwera to:

```
HTTP/1.1 200 OK
Date: Mon, 28 Jan 2019 18:15:03 GMT
Server: Apache
Last-Modified: Mon, 28 Jan 2019 18:11:05 GMT
```

```
ETag: „2d2e0-21-5808899aa4c5d”
Accept-Ranges: bytes
Content-Length: 33
Vary: Accept-Encoding
Content-Type: text/html

<body>
<h1>trening</h1>
</body>
```

Odpowiedz serwera zawiera następujące elementy

- Linia statusu odpowiedzi: status 200 oznacza, że zapytanie przetworzono poprawnie. Inne statusy odpowiedzi wynikające z protokołu HTTP podano m.in. na stronie LINK
- Kolejne nagłówki odpowiedzi. Ich lista oraz znaczenie znajduje się m.in. na stronie LINK Pusta linia
- Ciało odpowiedzi (dane)

2.2. Protokół DNS

Protokół DNS tłumaczy nazwy hostów na ich adresy IP, pełniąc kluczową rolę w infrastrukturze internetowej. Z punktu widzenia klienta protokół DNS jest jednak dość prosty – formułowane jest zapytanie (o adres IP domeny) do lokalnego serwera DNS i odbierana jest odpowiedź (adres ID). Niemniej, taki opis protokołu DNS jest uroszczony, gdyż wiele jego mechanizmów jest niewidocznymi dla klienta DNS, ponieważ hierarchiczne serwery DNS komunikują się ze sobą (rekursywnie lub iteracyjnie) w celu rozwiązywania zapytania DNS.

Prócz protokoły sieciowego DNS opisuje sposób definiowania domen w Internecie, które zorganizowano w sposób hierarchiczny a zarządzanie różnymi jej poziomami, powierzono różnym organizacją. Dlatego na DNS można również patrzeć jako na system prawny organizujący sieć w kontekście zarządzania i odpowiedzialności za nazwy domenowe.

nslookup (ang. *name server lookup*)

To polecenie znane z różnych systemów operacyjnych służące wyszukiwaniu informacji odnoszących się do serwerów DNS takich jak adresy IP serwerów DNS, nazwy domen czy aliasy.

Aby uruchomić *nslookup*, wystarczy wpisać polecenie *nslookup* w wierszu poleceń. Jego dokumentacja dla systemów Windows znajduje się TU.

W swojej najbardziej podstawowej funkcjonalności *nslookup* umożliwia hostowi, zapytanie domyślnego lub określonego serwera DNS o rekord DNS. Odpytywany serwer DNS może być głównym serwerem DNS, serwerem DNS domeny najwyższego poziomu (TLD), autorytatywnym serwerem DNS lub pośrednim serwerem DNS. Przykład odpowiedzi lokalnego (lokalnego dla

kampusu Uniwersytetu w Massachusetts (UMass)) na zapytanie dotyczące serwisu www.nyu.edu pokazano na rys. 1.

W tym przykładzie komenda *nslookup* otrzymuje jeden argument, tj. nazwę hosta. Jej działanie w stosunku do serwera DNS, można obrazowo przedstawić jako: *proszę, wyślij mi adres IP hosta www.nyu.edu*. Z rys. 1 wynika, że odpowiedź z tego polecenia zawiera dwie informacje: (1) nazwę i adres IP serwera DNS, który udziela odpowiedzi (w tym przypadku lokalnego serwera DNS w UMass) oraz (2) samą odpowiedź, czyli kanoniczną nazwę hosta i adres IP *www.nyu.edu*. Odpowiedz zawiera dwie pary nazwa-adres. Pierwsza (216.165.47.12) to adres IPv4 a druga (2607:f600:1002:6113::100) to dłuższy i bardziej skomplikowany adres IPv6. Warto zauważyć, że chociaż odpowiedź pochodziła z lokalnego serwera DNS (z adresem IP 128.119.240.1) w UMass, jest całkiem możliwe, że ten lokalny serwer DNS iteracyjnie skontaktował się z kilkoma innymi serwerami DNS, aby uzyskać odpowiedź na postawione żądanie.

```
newworld.cs.umass.edu> nslookup www.nyu.edu
Server:         128.119.240.1
Address:        128.119.240.1#53

Non-authoritative answer:
www.nyu.edu     canonical name = WEB.GSLB.nyu.edu.
Name:   WEB.GSLB.nyu.edu
Address: 216.165.47.12
Name:   WEB.GSLB.nyu.edu
Address: 2607:f600:1002:6113::100
```

Rysunek 1: podstawowe zastosowanie polecenia `nslookup`

Oprócz standardowego działania, czyli zapytań o rekord DNS typu A, możemy również użyć *nslookup* do zapytania o rekord typu NS. W tym wypadku, prócz nazwy hosta i jego adresu IP, zwracane są informacje (nazwa i IP) o autorytatywnych serwerach DNS. W przykładzie pokazanym na rys. 2 *nslookup* został wywołany z opcją *-type=NS* i domeną *nyu.edu*. Powoduje to, że *nslookup* wysyła zapytanie o rekord typu NS do lokalnego (domyślnego) serwera DNS. Takie zapytanie można zobrazować zdaniem: *proszę o przesłanie nazw hostów autorytatywnego DNS dla nyu.edu*. (gdy opcja *–type* nie jest używana, *nslookup* używa wartości domyślnej, czyli zapytania o rekordy typu A.) Odpowiedź, wyświetlona na zrzucie ekranu z rys. 2, najpierw wskazuje serwer DNS, który udziela odpowiedzi (jest to lokalny serwer DNS UMass o adresie 128.119.240.1) wraz z trzema serwerami nazw DNS NYU. Każdy z tych serwerów jest autorytatywnym serwerem DNS dla hostów w kampusie NYU. Jednak *nslookup* wskazuje również, że odpowiedź jest nieautorytatywna, co oznacza, że ta odpowiedź pochodzi z pamięci podręcznej jakiegoś serwera, a nie z autorytatywnego serwera DNS NYU. W drugiej części odpowiedzi podawane są adresy IP autorytatywnych serwerów DNS w NYU. (Uwaga: Napis *Authoritative answers can be found* from może nie występować a serwery autoratywne w odpowiedzi oddziela tylko pusta linia)

```
newworld.cs.umass.edu> nslookup -type=NS nyu.edu
Server:         128.119.240.1
Address:        128.119.240.1#53

Non-authoritative answer:
nyu.edu nameserver = ns2.nyu.org.
nyu.edu nameserver = ns4.nyu.edu.
nyu.edu nameserver = ns1.nyu.net.

Authoritative answers can be found from:
ns2.nyu.org     internet address = 128.122.0.76
ns1.nyu.net     internet address = 128.122.0.8
ns4.nyu.edu     internet address = 216.165.87.102
ns4.nyu.edu     has AAAA address 2607:f600:2001:6100::135
```

Rysunek 2.: Użycie nslookup do znalezienia autorytatywnych serwerów nazw dla domeny nyu.edu

Nslookup ma wiele dodatkowych opcji poza -type=NS, które można użyć. Część z nich przytoczono na stronie https://www.cloudns.net/blog/10-most-used-nslookup-commands/.

3. Zadania

3.1. Protokół HTTP

Wykonaj następujące czynności:
1. Uruchom przeglądarkę internetową i wyczyść pamięć podręczną.
2. Uruchom sniffer pakietów Wireshark i prowadź „http” (tylko litery, bez cudzysłowów i małymi literami) w oknie specyfikacji filtra wyświetlania.
3. Wprowadź w przeglądarce adres strony #1 podany przez prowadzącego.
4. Zatrzymaj przechwytywanie pakietów Wireshark.
5. Zapisz plik z przechwyconymi pakietami który należy dołączyć do sprawozdania.

Analizując informacje zawarte w komunikatach HTTP GET i odpowiedziach, odpowiedz na następujące pytania:

1. Ile komunikatów żądania GET wysyła przeglądarka?
2. Ile pakietów/segmentów było potrzebnych do przesłania strony #1?
3. Z jakiej wersji protokołu http korzysta przeglądarka? Jaka wersja protokołu HTTP działa na serwerze?
4. Jakie języki (jeśli w ogóle) występujące na serwerze akceptuje przeglądarka?
5. Jaki jest adres IP Twojego komputera? Jaki jest adres IP serwera strony #1 podanej przez prowadzącego?
6. Jaki jest kod stanu zwracany z serwera do przeglądarki?
7. Czy można się dowiedzieć, kiedy plik HTML który pobrano, był ostatnio modyfikowany?
8. Ile bajtów (ich suma oraz podział na pakiety) treści jest zwracanych do Twojej przeglądarki?

3.2. Protokół DNS

9. Gdzie można kupić domenę (podaj dwa miejsca w Internecie)? Jakie to koszty? Gdzie sprawdzić, do jakiej organizacji przypisano zarządzanie domenami najwyższego poziomu?

10. Uruchom *nslookup* i uzyskaj adres IP serwera internetowego strony rządu/parlamentu wybranego kraju Ameryki Południowej. Jaka jest jego nazwa i adres IP?

11. Jaki jest adres IP serwera DNS, który dostarczył odpowiedź na polecenie *nslookup* w pytaniu 10?

12. Czy odpowiedź na polecenie *nslookup* w pytaniu 10 pochodzi z autorytatywnego czy nieautorytatywnego serwera?

13. Użyj polecenia *nslookup*, aby określić nazwę autorytatywnego serwera nazw dla domeny instytucji, wybranej w zadaniu 10. Jaka to nazywa? (Jeśli istnieje więcej niż jeden autorytatywny serwer, podaj ich nazwę).

Po wykonaniu zadań 10-13 dotyczących polecenia *nslookup* należy wykonać następujące kroki

- Wyczyść pamięć podręczną DNS na hoście (dla Windows: ipconfig /flushdns)
- Otwórz przeglądarkę internetową i wyczyść pamięć podręczną przeglądarki.
- Otwórz Wireshark i wpisz dns w filtrze wyświetlania
- Rozpocznij przechwytywanie pakietów w Wireshark.
- W przeglądarce odwiedź stronę internetową ustaloną w zadaniu 10
- Po wykonaniu tych czynności należy odpowiedzieć na pytania

14. Zlokalizuj pakiet zapytania DNS odnoszący się do strony ustalonej w zadaniu 10. Jaki jest identyfikator transakcji pakietu zapytania DNS? Czy ten pakiet jest wysyłana przez protokół UDP czy TCP?

15. Zlokalizuj odpowiedź DNS na zapytanie DNS z pkt. 14. Jaki jest jego identyfikator ? Za pośrednictwem jakiego protokołu przesłano ten pakiet? Skomentuj obserwacje.

16. Jaki jest port docelowy dla pakietu zapytania DNS? Jaki jest port źródłowy pakietu odpowiedzi DNS?

17. Na jaki adres IP jest wysyłany pakiet będący zapytaniem DNS?

18. Ile „pytań” zawiera pakiet zapytania DNS? Ile „odpowiedzi” zawiera pakiet odpowiedzi na zapytanie DNS. Czy ich liczba może być różna w zależności od zapytania?

4. Wymagania dotyczące sprawozdania

Sprawozdanie dokumentuje wykonanie zadań z punktu 3 za pomocą opisu, podpisanych screenów, odpowiedzi na pytania kontrolne i komentarzy. Do sprawozdania należy dołączyć pliki Wireshark.

Sprawozdanie należy oddać w formie ustalonej z prowadzącym.