

Fundamentos de Redes de Computadores

Atividade Extra 01

Depuração de Problemas na Camada de Aplicação

Jonathan Henrique Maia de Moraes - 12/0122553

Universidade de Brasília - Faculdade UnB Gama
15/09/2016

Questões para Estudo

1. Em relação ao serviço de resolução de nomes, há um parâmetro opcional a ser indicado ao comando `nslookup`. Em que contexto é conveniente indicar um valor para esse parâmetro?

R: O parâmetro opcional permite escolher por um servidor DNS alternativo ao padrão estabelecido em suas configurações de rede. Convém indicar um valor para esse parâmetro quando o atual servidor DNS configurado parece não estar funcionando adequadamente e há o desejo de testar a mesma demanda em um servidor DNS alternativo.

2. Qual é o papel do arquivo `/etc/hosts` no processo de resolução de nomes?

R: O arquivo `/etc/hosts` armazena pares de endereço de IP (tanto para IPv4 quanto para IPv6) e **nome do host**, de forma que, ao inserir o **nome do host**, este redirecione para o endereço de IP correspondente quando se tratar de uma transação que exija esse protocolo.

Por exemplo, ao definir os seguintes pares no arquivo `/etc/hosts`:

```
1  # IPv4
2  127.0.0.1 localhost
3  # IPv6
4  ::1 localhost
```

Sempre que realizar uma requisição utilizando o protocolo IP com o **nome de host** `localhost` será redirecionado o valor `127.0.0.1` (IPv4) ou o valor `::1` (IPv6).

3. Em relação às interações com o protocolo HTTP, foi possível identificar o cabeçalho de uma requisição típica? Em relação às respostas do servidor, identifique os campos típicos da resposta incluindo descrições sobre as linhas de cabeçalho e o campo de *payload*.

R: Sim, foi possível identificar o cabeçalho de uma requisição típica HTTP. Diferentes *browsers* possuem ferramentas que registra as requisições e respostas de protocolo HTTP. Como forma de exemplificar e identificar os campos típicos de respostas do servidor, é descrito abaixo duas requisições HTTP de método GET e tipo HTML, o primeiro da página do roteiro desta atividade prática (http://aprender.ead.unb.br/pluginfile.php/238246/mod_resource/content/6/01_pratica_

aplicacao.pdf) e o segundo de uma página do StackExchange (<http://ell.stackexchange.com/questions/103371>). Foi utilizado o navegador Mozilla Iceweasel, versão 38.7.1:

```
1  Accept-Ranges: bytes
2  Age: 0
3  Cache-Control: private
4  Connection: keep-alive
5  Content-Encoding: gzip
6  Content-Length: 22147
7  Content-Type: text/html; charset=utf-8
8  Date: Tue, 13 Sep 2016 13:37:24 GMT
9  Vary: Accept-Encoding
10 Via: 1.1 varnish
11 X-Cache: MISS
12 X-Cache-Hits: 0
13 X-Frame-Options: SAMEORIGIN
14 X-Request-Guid: 73304d1a-6887-44fc-af37-17a34a22125a
15 X-Served-By: cache-gru7122-GRU
16 X-Timer: S1473773844.840175,VS0,VE140
17 x-dns-prefetch-control: off
```

O *payload* para esta requisição foi um arquivo HTML de 2131 linhas. O código de resposta foi 200 e significa OK.

```
1  Accept-Ranges: bytes
2  Cache-Control: private, max-age=21600, no-transform
3  Connection: Keep-Alive
4  Content-Disposition: inline; filename="01
   _pratica_aplicacao.pdf"
5  Content-Length: 205956
6  Content-Type: application/pdf
7  Date: Tue, 13 Sep 2016 13:39:56 GMT
8  Etag: "aa926467c375676a0690dfff6176baaf345aeffb"
9  Expires: Tue, 13 Sep 2016 19:39:56 GMT
10 Keep-Alive: timeout=5, max=100
11 Last-Modified: Wed, 07 Sep 2016 02:35:06 GMT
12 Server: Apache/2.2.22 (Debian)
13 X-Powered-By: PHP/5.6.21-1~dotdeb+7.1
```

O *payload* para esta requisição foi um arquivo PDF de 1894 linhas. O código de resposta foi 200 e significa OK.

Os campos em comum de cabeçalho foram:

(a) **Accept-Ranges**: Permite ao servidor indicar a aceitação de al-

cance de requisições para um recurso. No exemplo, ambos utilizaram o termo **bytes**, que estabelece a aceitação do servidor de origem para o alcance em *bytes*.

- (b) **Cache-Control:** Campo também presente em requisições, é utilizado para especificar diretrizes que serão obedecidos por todos os mecanismos de *caching* na cadeia de requisições e respostas. O termo **private** indica que toda ou parte da mensagem de resposta é intencionada para um usuário único e não deve ser armazenado em *cache* compartilhado.
 - (c) **Connection:** Campo também presente em requisições, permite ao emissor especificar opções que são desejados para uma particular conexão e que não devem ser comunicados por *proxies* ao longo de futuras conexões. O termo *keep-alive* descreve que a conexão será mantida ao fim da emissão.
 - (d) **Content-Length:** Campo que está presente no cabeçalho sempre que houver *payload*, é utilizado para informar o tamanho do *payload*, e deve conter um número maior ou igual a 0.
 - (e) **Content-Type:** Campo também presente em requisições, indica o tipo de arquivo contido no *payload*. O primeiro exemplo possui no *payload* um arquivo de texto **HTML**, e o segundo exemplo um arquivo de aplicação do tipo **PDF**.
 - (f) **Date:** Campo também presente em requisições, representa a data e hora que a mensagem foi gerada. Possui a mesma semântica de **orig-date** descrita na norma **RFC 822**. O valor do campo é um **HTTP-date** com formato de data descrito na norma **RFC 1123**.
4. Em vários dos protocolos ora estudados, foi presenciada uma etapa de autorização que preparava uma sessão para a recepção de comandos de determinado cliente. O **SMTP** demonstrou-se um protocolo que não demanda uma etapa de autorização. Em que momento isso acontece? O fato de essa etapa ser suprimida resulta em algum risco para um serviço de *e-mail*?

R: Não há autenticação de emissor durante a definição do mesmo. Isto significa que, ao ter acesso interno em um servidor que possui interface de comunicação através do protocolo **SMTP**, é possível enviar mensagens de qualquer usuário identificado neste servidor para qualquer outro

servidor **SMTP** válido. O *spamming* é a principal consequência dessa limitação de segurança no protocolo **SMTP**.