FACULDADES SPEI

Curso: **Bacharel em Sistemas de Informação**
Professor: **Paulo Cezar de Oliveira**
Disciplina: **Rede de Computadores** Turma:_____
Aluno(a): Data: 17/03/2016

Observações:

- LEIA ATENTAMENTE AS INSTRUÇÕES E O ENUNCIADO ANTES DE INICIAR O EXERCÍCIO.
- Deve ser entregue por email (paulocezar@spei.br) e em dupla até o término da aula de hoje.
    - No **assunto do email** coloque a **turma e o período**.
- Não se esqueça de identificar a atividade com nome e turma.
    - No **nome do arquivo** coloque o **primeiro nome de cada envolvido**
- As respostas copiadas não serão consideradas, tanto de quem copiou quanto de quem forneceu o original.
- Não será aceito atraso na entrega do trabalho.

3ª Lista de Exercícios

Exercício extraído de Wireshark Lab: DNS - J.F. Kurose, K.W. Ross.

TRABALHANDO COM DNS NSLOOKUP e WIRESHARK

NSLOOKUP

- Funciona tanto no prompt do Windows como no Linux.
- Permite obter informações sobre registros de DNS sobre um determinado domínio, host ou IP.
- Se não é fornecido o nome do servidor, a busca é feita no servidor local.
- Trabalha em 2 modos:
    - **Direto** - É digitado o comando e mais alguns parâmetros.
    - **Interativo** – Permite fazer várias pesquisas. Basta digitar nslookup e pressionar enter.

Comandos

nslookup www.spei.br

Resultado

C:\ >nslookup www.spei.br
Servidor: resolver1.xxx.xxx.br
Address: 201.195.51.110
Não é resposta de autorização:
Nome: spei.br
Address: 187.45.193.151
Aliases: www.spei.br

Em uma busca *nslookup* padrão, o servidor DNS do provedor de acesso é consultado, e retorna as informações sobre o domínio ou host pesquisado.
A mensagem **Não é resposta de autorização** informa que o servidor DNS do provedor de acesso não responde por este domínio, ou seja, o servidor não é responsável pelo domínio consultado.

Uma consulta externa foi realizada, aos servidores DNS do domínio pesquisado (neste caso, spei.br).

nslookup -type=NS spei.br

Resultado

C:\Users\paulo>nslookup -type=NS spei.br
Servidor: resolver1.XXX.XXX.br
Address: 201.195.51.110

Não é resposta de autorização:
spei.br nameserver = ns3.locaweb.com.br
spei.br nameserver = ns2.locaweb.com.br
spei.br nameserver = ns1.locaweb.com.br
ns2.locaweb.com.br internet address = 201.76.40.2
ns1.locaweb.com.br internet address = 189.126.108.2
ns3.locaweb.com.br internet address = 187.45.246.2

A opção **-type=NS** e o domínio **spei.br** faz com que o *nslookup* envie uma requisição para um registro **type-NS** para o servidor padrão local DNS solicitando o envio dos nomes do host do servidor de autoridade para **spei.br**.
A resposta dada indica o servidor DNS que está providenciando a resposta (que é o servidor local padrão DNS) e com três servidores de nomes **spei.br**. Cada um destes servidores é um servidor de autoridade DNS para os hosts SPEI.
O *nslookup* também indica que a resposta veio do cache de algum servidor ao invés de um servidor DNS da SPEI. A resposta também inclui os endereços IP dos servidores de autoridade DNS.

nslookup spei.br ns1.locaweb.com.br

Resultado

C:\Users\paulo>nslookup spei.br ns1.locaweb.com.br
Servidor: ns1.locaweb.com.br
Address: 189.126.108.2

Nome: spei.br
Address: 187.45.193.151

Neste exemplo a requisição foi enviada para o servidor DNS **ns1.locaweb.com.br** ao invés do servidor padrão DNS (resolver1.xxx.xxx.br). Assim, a transação de requisição e resposta toma lugar diretamente entre o host que solicita e o servidor **ns1.locaweb.com.br**.

IPCONFIG

- Pode ser usado para mostrar a informação atual de endereçamento IP, incluindo seu endereço IP, endereço de servidor DNS, tipo de adaptador e etc.
  - Ipconfig /all.
- Também é útil para gerenciar a informação DNS armazenada no host.
  - **IPCONFIG/DISPLAYDNS** - Lista o cache do DNS local.
  - **IPCONFIG/FLUSHDNS** - Limpa o cache do DNS local.

Teste várias possibilidades com a ferramenta Nslookup.

EXPERIMENTO 1 - DNS e Wireshark

Consulte e faça um print do cache DNS de sua máquina.
Esvazie o cache DNS em sua máquina.
Compare e descreva o print com a tela atual.

Inicie o browser e esvazie o cache do navegador.
Execute Wireshark e desmarque a opção “promiscuous mode” ou digite “ip.addr == endereço_IP da máquina” no campo de filtro.
Este filtro remove todos os pacotes que não foram originados ou destinados para seu host.
Inicie a captura de pacotes no Wireshark.
Acesse o site **http://www.ietf.org**
Finalize a captura de pacotes.
Responda:

1. Localize as mensagens de requisição e resposta DNS. Elas são enviadas sobre o UDP ou TCP?
2. Qual é a porta destino para a mensagem de requisição DNS? Qual é a porta de origem da mensagem DNS?
3. Examine a mensagem de requisição DNS. Qual o tipo de requisição DNS?
4. Examine a mensagem DNS response. Quantas “respostas” são providas? O que cada resposta contém?

EXPERIMENTO 2 – NSLOOKUP e Wireshark
Inicie o nslookup.

• Inicie captura de pacotes no wireshark.
• Digite **nslookup www.mit.edu**
• Finalize a captura de pacotes.

Responda:

5. Qual a porta destino para a mensagem de requisição DNS? Qual é porta de origem da mensagem DNS response?
6. Para qual endereço IP a mensagem de requisição DNS é enviada? Este é o endereço IP de seu servidor padrão local DNS?
7. Examine a mensagem de requisição DNS. Qual é o tipo mensagem de requisição DNS? A mensagem de requisição contém quais “respostas”?
8. Examine a mensagem DNS response. Quantas “respostas” são providas? O que cada uma dessas mensagens contém?

EXPERIMENTO 3
Repita o experimento 2 com o comando **nslookup –type=NS mit.edu**

Responda:

9. Examine a mensagem de requisição DNS. Qual é o tipo da mensagem de requisição DNS? A mensagem de requisição contém quais "respostas"?
10. Examine a mensagem DNS response. Quantos nomes de servidores MIT a mensagem response provê?

EXPERIMENTO 4
Repita o experimento 2 executando o comando **nslookup www.aiit.or.kr bitsy.mit.edu**

Responda:

11. Examine a mensagem de requisição DNS. Qual o tipo de requisição de DNS? A mensagem de requisição contém alguma "resposta"?
12. Examine a mensagem response DNS. Quantas "respostas" são dadas? O que cada resposta contém?

Aponte o NSLOOKUP para internetsociety.org

13. Quais os endereços IP deste servidor?
14. Existe algum valor separado por "**:**" e outro por "**.**"? Caso exista, explique a diferença entre eles.

Visite esses sites

http://ipv6.br/

http://test-ipv6.com/

http://www.internetsociety.org/deploy360/blog/2012/05/the-top-4-websites-are-permanently-enabling-ipv6-are-you/