

FERRAMENTA NSLOOKUP

Introdução

Será abordado alguns assuntos introdutórios a respeito da internet, bem como alguns aplicativos, autores e curiosidade a respeito do tema. Assim, antes de conceituar a respeito da ferramenta NSLOOKUP, faz-se necessário apresentação de outros assuntos para a melhor compreensão do tema abordado.

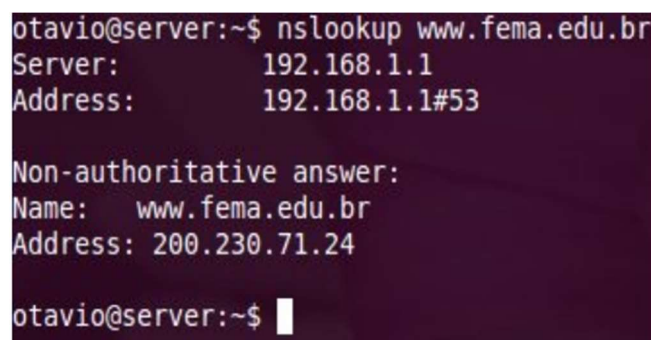
DNS - Domain Name System (Sistema de Nomes de Domínio)

O DNS é um banco de dados distribuído implementado em uma hierarquia de servidores de nome e um protocolo de camada de aplicação que permite que hospedeiros consultem o banco de dados distribuído com a finalidade de traduzir nomes de hospedeiro para endereços IP.

NSLOOKUP

GIAVAROTO et al. (2013) informa que a ferramenta Nslookup não é caracterizada por ser uma ferramenta, e sim um comando que está presente não só no Backtrack 5 R3 Linux, mas em várias outras distribuições Linux e também no ambiente Windows. Este comando pode ser executado em modo simples de usuário, não precisando estar em modo root, e sua função é descobrir informações simples a respeito de um determinado domínio DNS. É importante destacá-lo justamente por sua simplicidade.

No exemplo seguinte da Figura 8 é exibido um exemplo onde é retornado o endereço IP da página WEB da Fundação Educacional do Município de Assis.



```
otavio@server:~$ nslookup www.fema.edu.br
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
Name:   www.fema.edu.br
Address: 200.230.71.24

otavio@server:~$
```

Figura 1 - Exemplo de utilização do comando Nslookup.

Outras informações a serem levadas em consideração é algumas especificações de tal ferramenta. Como serão citadas abaixo:

O protocolo DNS utiliza UDP e usa a porta 53, no entanto pode, em casos específicos, utilizar TCP na mesma porta (53);

Comumente empregado por outras entidades da camada de aplicação:

HTTP, FTP e SMTP

Exemplo de Aplicação Web

Cenário: O usuário Pedro deseja acessar `www.someschool.edu/index.html` através do seu navegador (browser).

Como funciona:

1. A própria máquina do usuário executa um lado cliente da aplicação DNS;
2. O browser extrai o nome do hospedeiro, `www.someschool.edu`, do URL e passa o nome para o lado cliente da aplicação;
3. O cliente DNS envia uma consulta contendo o nome do hospedeiro para um servidor DNS;
4. O cliente DNS finalmente recebe uma resposta, que inclui o endereço IP correspondente ao nome de hospedeiro;
5. Tão logo o browser receba o endereço do DNS, pode abrir uma conexão TCP com o processo servidor HTTP localizado naquele endereço IP

Outras aplicações fornecidas pelo DNS

Distribuição de carga

Realiza a distribuição de carga entre servidores replicados, tais como servidores Web, à exemplo do Google;

Cada servidor roda em um sistema final diferente e tem um endereço IP diferente;

No caso dos servidores Web, um conjunto de endereços IP fica associado a um único nome canônico e contido no banco de dados do DNS;

Quando clientes consultam um nome mapeado para um conjunto de endereços, o DNS responde com o conjunto inteiro de endereços IP, mas faz um rodízio da ordem dos endereços dentro de cada resposta;

Normalmente, o cliente envia sua mensagem de requisição HTTP ao endereço IP que ocupa o primeiro lugar do conjunto, o rodízio de DNS distribui o tráfego entre os servidores replicados.

Conclusão

Este trabalho introdutório ao tema DNS e NSLOOKUP, demonstrou que há ainda muitos conceitos, trabalhos e pesquisas dentro do mundo de redes, demonstrando a imensidão de ambos os temas. Apesar do grande avanço da ciência nesta área, é notório

que possui muitas lacunas a serem preenchidas, mantendo-se assim um ciclo infinito de descobertas e aprendizados.

Referências Bibliográficas

GIAVAROTO, Sílvio César Roxo; SANTOS, Gerson Raimundo dos. “Backtrack Linux – Auditoria e Teste de Invasão em Redes de Computadores”. Rio de Janeiro: Editora Ciência Moderna Ltda., 2013

KUROSE, James F.; ROSS, Keith W. Redes de computadores e a Internet: uma abordagem top-down. 5 ed. São Paulo: Addison Wesley, 2010.

TANENBAUM, Andrew S. Redes de computadores. 4. ed. Rio de Janeiro: Elsevier, 2003.

FROSSARD, Vera. Arquitetura e protocolos de rede TCP/IP. Rio de Janeiro: Rede Nacional de Ensino e Pesquisa, 2005.