Laboratório 02 – Wireshark e DNS
24 ou 26/Agosto/2011

Tarefa:
Neste laboratório você irá estudar o funcionamento do protocolo DNS, assim como uma ferramenta para captura e análise de pacotes: o Wireshark.

Parte 1: Ambientação com o Wireshark

O aplicativo Wireshark é um software livre disponível para sistemas Linux e Windows. Nesta parte você deve verificar se o mesmo está funcionando corretamente e se ambientar com o aplicativo. Realize os seguintes passos:

1 – Inicialize o aplicativo Wireshark (no menu Internet).
2 – No Wireshark, inicialize a captura de pacotes para isso escolhendo a interface apropriada (Capture->Interfaces).
3 – Na janela de captura, aplique um filtro para que apenas pacotes originados ou com destino ao seu sistema seja exibido. Ex: **ip.src == 172.16.2.85 || ip.dst == 172.16.2.85**
4 – Navegue na internet e verifique os pacotes no Wireshark.
5 – Interrompa a captura de pacotes e análise os protocolos utilizados. Você conhece todos eles?

Parte 2: Baixando uma página HTML

Agora vamos analisar quais mensagens são trocadas entre dois sistemas ao fazer download de um arquivo de um servidor http. Realize os seguintes passos:

1 - Feche todos os browsers em sua máquina. Note que algumas páginas pode enviar mensagens com frequência dificultando a análise no Wireshark.

2 – Inicialize a captura de pacotes no Wireshark.

3 – Execute o seguinte comando em um console do Linux: **wget www.each.usp.br**

4 – Analise as mensagens geradas e tente justificar cada uma delas.

5 – Acesse agora uma página utilizando um browser (é interessante acessar uma página simples, por exemplo a página de um professor) e verifique as mensagens enviadas entre os sistemas. Quantas conexões TCPs foram abertas com o servidor http?

Parte 3: Utilizando o DNS

Um aplicativo linux que pode ser utilizado a partir da linha de comando para fazer consultas DNS é o **dig**. Ele permite que você escolha o servidor de DNS ao qual será feita a consulta e escolher o tipo de consulta (MX, A, CNAME, SOA, NS). Lembre-se que você pode continuar utilizando o Wireshark para visualizar as trocas de mensagens. Realize os seguintes passos:

1 – Execute o comando: **dig www.each.usp.br**. Você consegue interpretar a resposta obtida? Para qual servidor de DNS foi enviada a consulta?

2 – A opção **@** permite escolher um servidor de DNS em particular. Execute o comando: **dig @199.7.83.42 www.each.usp.br**. Você consegue interpretar a resposta obtida? Você conseguiu obter o IP do servidor responsável por www.each.usp.br? Em qual nível da hierarquia de servidores DNS encontra-se o servidor 199.7.83.42?

3 – Repita o passo 2 recursivamente mudando o servidor de DNS até encontrar o IP do servidor responsável por www.each.usp.br.

4 – Utilize o que você viu nos passos anteriores para descobrir o IP do servidor de e-mail da USP. Utilize o help do comando dig (**man dig**) para verificar como fazer uma consulta MX.

5 – Outro comando interessante no Linux é o comando whois. Este comando acessa um servidor whois e trás informações sobre um domínio. Execute o comando: **whois www.each.usp.br**. Quais informações interessantes são exibidas?