Exercícios Wireshark – DNS

Parte 1: usando o comando nslookup, faça os exercícios de 1 a 3:

1. Execute nslookup para obter o endereço IP de um servidor Web na Ásia. Qual é o endereço IP desse servidor?

2. Execute nslookup para determinar os servidores DNS autorizados para uma universidade na Europa.

3. Execute nslookup para que um dos servidores DNS obtidos na Questão 2 seja consultado para os servidores de correio do Yahoo! correspondência. Qual é o endereço IP dele?

Parte 2: O comando ipconfig (windows) ou ifconfig (linux/unix) são comandos muito úteis quando queremos fazer uma depuração (debug) na rede. Desta forma, nesta parte vamos utilizar os comandos nslookup e ifconfig para responder às perguntas de 4 a 10.

Primeiramente, vamos preparar o ambiente:

1. limpe a cache do seu navegador;
2. abra o wireshark e digite no campo filtro (filter) **“ip.addr == seu_endereço_IP”**. Este filtro removerá todos os pacotes que não se originam ou se destinam à sua máquina.
3. Inicialize a captura de pacotes pelo wireshark.
4. Utilizando seu navegador acesse o endereço: http://www.ietf.org
5. Pare a captura de pacotes.

Após as etapas de 1 a 5, responda às perguntas de 4 a 10:

4. Localize as mensagens de consulta e resposta do DNS. Tais mensagens são enviadas por UDP ou TCP?

5. Qual é a porta de destino para a mensagem de consulta DNS? Qual é a porta de origem da mensagem de resposta do DNS?

6. Para qual endereço IP a mensagem de consulta DNS é enviada? Use ifconfig para determinar o endereço IP do seu servidor DNS local. Esses dois endereços IP são iguais?

7. Examine a mensagem de consulta DNS. Qual é o “tipo” de consulta de DNS? A mensagem de consulta contém alguma “resposta”?

8. Examine a mensagem de resposta do DNS. Quantas “respostas” são fornecidas? O que cada uma dessas respostas contém?

9. Considere o pacote TCP SYN subsequente enviado por sua máquina. O endereço IP de destino do pacote SYN corresponde a algum dos endereços IP fornecidos na mensagem de resposta do DNS?

10. Esta página web contém imagens. Antes de recuperar cada imagem, sua máquina emite novas consultas de DNS?

Após as etapas de 4 a 10, responda às perguntas de 11 a 15:

Preparação:

- Inicialize a captura de pacotes;
- Execute: nslookup www.mit.edu
- Pare a captura de pacotes;

11. Qual é a porta de destino para a mensagem de consulta DNS? Qual é a porta de origem da mensagem de resposta do DNS?

12. Para qual endereço IP a mensagem de consulta DNS é enviada? Este é o endereço IP do seu servidor DNS local padrão?

13. Examine a mensagem de consulta DNS. Qual é o “tipo” de consulta de DNS? A mensagem de consulta contém alguma “resposta”?

14. Examine a mensagem de resposta do DNS. Quantas “respostas” são fornecidas? O que cada uma dessas respostas contém?

15. Forneça uma captura de tela.

Para as questões de 16 a 19:

Preparação:

- Inicialize a captura de pacotes;
- Execute: nslookup -type=NS mit.edu
- Pare a captura de pacotes;

16. Para qual endereço IP a mensagem de consulta DNS é enviada? Este é o endereço IP do seu servidor DNS local padrão?

17. Examine a mensagem de consulta DNS. Qual é o “tipo” de consulta de DNS? A mensagem de consulta contém alguma “resposta”?

18. Examine a mensagem de resposta do DNS. Quais servidores de nomes do MIT a mensagem de resposta fornece? Essa mensagem de resposta também fornece os endereços IP dos nomes do MIT?

19. Forneça uma captura de tela.

Para as questões de 20 a 23:

Preparação:

- Inicialize a captura de pacotes;
- Execute: nslookup www.aiit.or.kr
- Pare a captura de pacotes;

20. Para qual endereço IP a mensagem de consulta DNS é enviada? Este é o endereço IP do seu servidor DNS local padrão? Se não, a que corresponde o endereço IP?

21. Examine a mensagem de consulta DNS. Qual é o “tipo” de consulta de DNS? A mensagem de consulta contém alguma “resposta”?

22. Examine a mensagem de resposta do DNS. Quantas “respostas” são fornecidas? O que cada uma dessas respostas contém?

23. Forneça uma captura de tela.