Laboratório - Explore o tráfego DNS

# Objetivos

Parte 1: Capturar tráfego DNS

Parte 2: Explore o tráfego de consulta DNS

Parte 3: Explore o tráfego de resposta do DNS

# Histórico/Cenário

O Wireshark é uma ferramenta de captura e análise de pacotes de código aberto. O Wireshark fornece uma análise detalhada da pilha de protocolos de rede. O Wireshark permite filtrar o tráfego para solucionar problemas de rede, investigar problemas de segurança e analisar protocolos de rede. Como o Wireshark permite visualizar os detalhes do pacote, ele pode ser usado como uma ferramenta de reconhecimento para um invasor.

Neste laboratório, você instalará o Wireshark e usará o Wireshark para filtrar pacotes DNS e visualizar os detalhes dos pacotes de consulta e resposta DNS.

# Recursos necessários

=   1 PC com acesso à internet e Wireshark instalado

# Instruções

## Parte 1: Capturar o tráfego de DNS

### Etapa 1: Baixar e instalar o Wireshark.

a.     Baixe a última versão estável do Wireshark em [www.wireshark.org](http://www.wireshark.org). Escolha a versão do software necessária com base na arquitetura e no sistema operacional do PC.

b.     Siga as instruções na tela para instalar o Wireshark. Se você for solicitado a instalar o USBPcap, **NÃO instale** o USBPcap para captura de tráfego normal. O USBPcap é experimental e pode causar problemas USB no seu PC.

### Capture o tráfego DNS

a.   Inicie o Wireshark. Selecione uma interface ativa com tráfego para captura de pacotes.

b.   Limpe o cache DNS.

1)     No Windows, digite **ipconfig /flushdns** no prompt de comando.

2)     Para a maioria das distribuições Linux, um dos seguintes utilitários é usado para cache de DNS: Systemd -Resolved, DNSMasq e NSCD. Se a sua distribuição Linux não usar um dos utilitários listados, faça uma pesquisa na Internet para o utilitário de cache DNS para sua distribuição Linux.

Identifique o utilitário usado na sua distribuição Linux verificando o status:

1.     Systemd-Resolved:**systemctl status systemd-resolved.service**

2.     DnsMaq: **systemctl status dnsmasq.service**

3.   NSCD: **statussystemctl nscd.service**

Se você estiver usando o sistema resolvido, digite **systemd-resolve —flush-caches** para liberar o cache para Systemd-Resolved antes de reiniciar o serviço. Os comandos a seguir reiniciam o serviço associado usando privilégios elevados:

4.     Systemd-Resolved:**sudo systemctl restart systemd-resolved.service**

5.     DNSMasq: **sudo systemctl restart dnsmasq.service**

6.     NSCD: **sudo systemctl restart nscd.service**

3)     Para o macOS, digite **sudo killall -HUP mDNSResponder** para limpar o cache DNS no Terminal. Execute uma pesquisa na Internet para os comandos para limpar o cache DNS de um sistema operacional mais antigo.

c.     Em um prompt de comando ou terminal, digite **nslookup** enter o modo interativo.

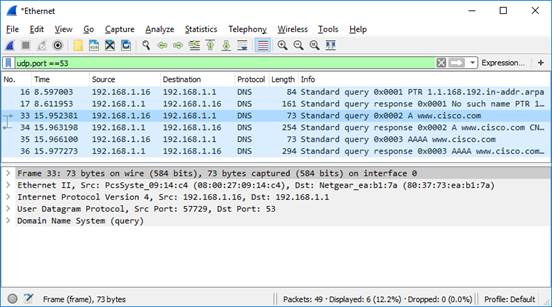
d.     Insira o nome do domínio. O nome do domínio [www.cisco.com](http://www.cisco.com) É usado neste exemplo.

e.     Digite **exit** quando terminar. Feche o prompt de comando.

f.      Clique em **Parar a captura de pacotes** para parar a captura do Wireshark.

## Parte 2: Explore o tráfego de consulta DNS

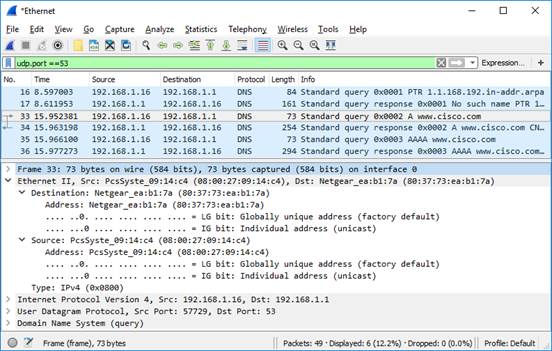
a.     Observe o tráfego capturado no painel Wireshark Packet List. Entre com **udp.port == 53** na caixa de filtro e clique na seta (ou pressione Enter) para exibir apenas pacotes DNS. **Observação**: As capturas de tela fornecidas são apenas exemplos. Sua saída talvez um pouco diferente.



b.     Selecione o pacote DNS contém consulta **padrão** e **A www.cisco.com** na coluna Informações.

c.     No painel Detalhes do Pacote, observe que este pacote possui Ethernet II, Internet Protocol Versão 4, User Datagram Protocol e Domain Name System (consulta).

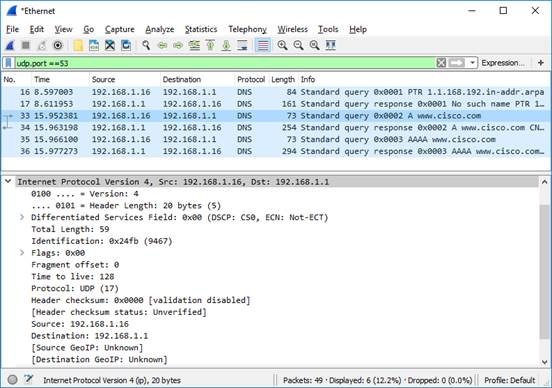
d.     Expanda **Ethernet II** para ver os detalhes. Observe os campos de origem e destino.



Quais são os endereços MAC de origem e destino? A quais interfaces de rede esses endereços MAC estão associados?

Digite suas respostas aqui.

e.     Expanda **Internet Protocol Version 4**. Observe os endereços IPv4 de origem e destino.

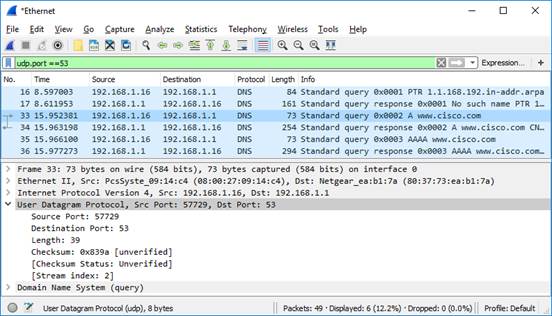


#### Pergunta:

Quais são os endereços IP de origem e destino? A quais interfaces de rede esses endereços IP estão associados?

Digite suas respostas aqui.

f.      Expanda a aba **User Datagram Protocol**. Observe os campos de origem e destino.



#### Pergunta:

Quais são os valores das portas origem e destino? Qual é o número da porta DNS padrão?

Digite suas respostas aqui.

g.     Determine o endereço IP e MAC do PC.

1)    Em um prompt de comando do Windows, digite **arp –a** e **ipconfig /all** para registrar os endereços MAC e IP do PC.

2)    Para Linux e macOS PC, digite **ifconfig** ou **ip address** em um terminal.

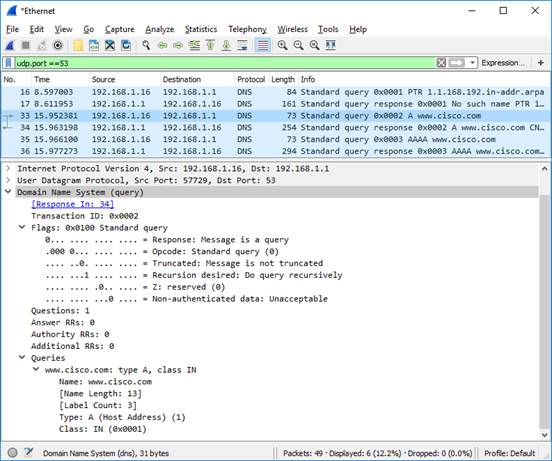
#### Pergunta:

Compare os endereços MAC e IP nos resultados do Wireshark com os endereços IP e MAC. O que você observa?

Digite suas respostas aqui.

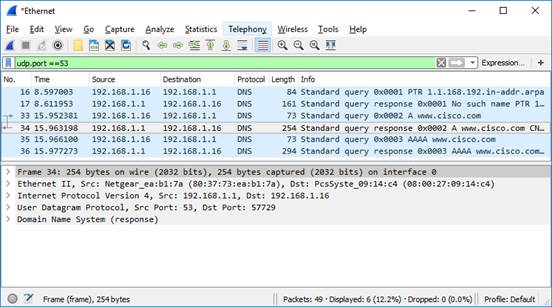
h.     Exanda o **Domain Name System (query**) no painel Detalhes do pacote. Então expanda também **Flags** e **Queries**.

i.      Observe os resultados. O sinalizador está configurado para fazer a consulta recursivamente para procurar o endereço IP em www.cisco.com.



## Parte 3: Explore o tráfego de resposta do DNS

a.     Selecione a resposta correspondente. O pacote DNS tem uma **resposta de consulta padrão** e **A www.cisco.com** na coluna Info.



#### Pergunta:

Quais são os endereços MAC e IP de origem e destino e os números de porta? Como eles se comparam aos endereços nos pacotes de consulta DNS?

Digite suas respostas aqui.

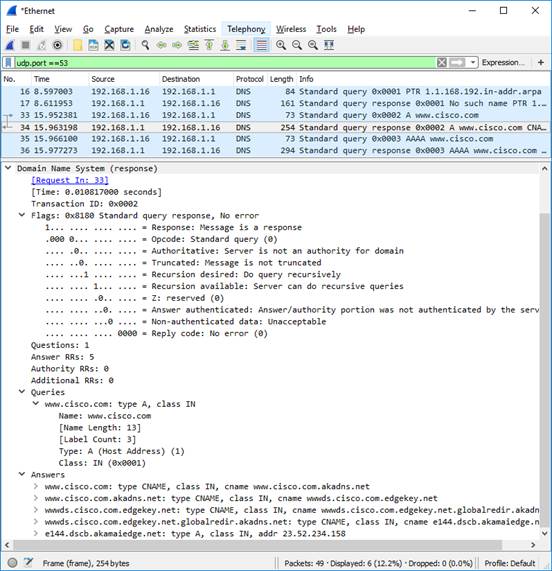
b.     Expanda **Domain Name System (response)**. Então expanda **Flags**, **Queries**, e **Answers**.

c.     Observe os resultados.

#### Pergunta:

O servidor DNS pode fazer consultas recursivas?

Digite suas respostas aqui.



d.     Observe os registros CNAME e A nos detalhes das Respostas.

#### Pergunta:

Como os resultados se comparam aos resultados do nslookup?

Digite suas respostas aqui.

# Reflexão

1.     A partir dos resultados do Wireshark, o que mais você pode aprender sobre a rede ao remover o filtro?

Digite suas respostas aqui.

2.     Como um invasor pode usar o Wireshark para comprometer a segurança da sua rede?

Digite suas respostas aqui.

Fim do documento