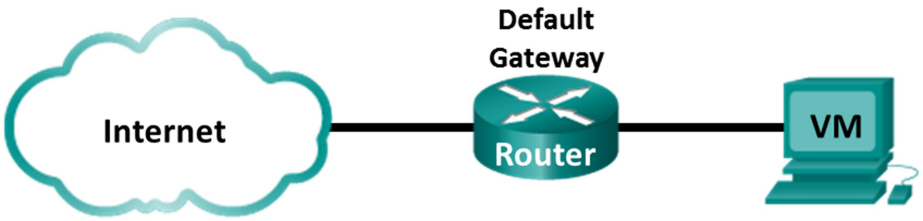
Laboratório - Usando o Wireshark para Examinar uma Captura UDP DNS

Topologia



Objetivos

Parte 1: Registrar as Informações de Configuração IP de um PC

Parte 2: Usar o Wireshark para Capturar Consultas e Respostas DNS

Parte 3: Analisar Pacotes DNS ou UDP Capturados

Histórico/Cenário

Ao usar a Internet, você usa o Sistema de Nomes de Domínio (DNS). O DNS é uma rede distribuída de servidores que traduz nomes de domínio de fácil utilização, como www.google.com, para um endereço IP. Quando você digita uma URL de um site no navegador, o computador executa uma consulta DNS ao endereço IP do servidor DNS. A consulta DNS do seu PC e a resposta do servidor DNS usam o User Datagram Protocol (UDP) como o protocolo da camada de transporte. O UDP é sem conexão e não requer uma configuração de sessão como o TCP. As consultas e as respostas DNS são muito pequenas e não exigem a sobrecarga do TCP.

Neste laboratório, você se comunicará com um servidor DNS enviando uma consulta DNS usando o protocolo de transporte UDP. Você usará o Wireshark para examinar as trocas de consulta e de respostas DNS com o mesmo servidor.

Recursos Necessários

- Máquina Virtual CyberOps Workstation
- Acesso à Internet

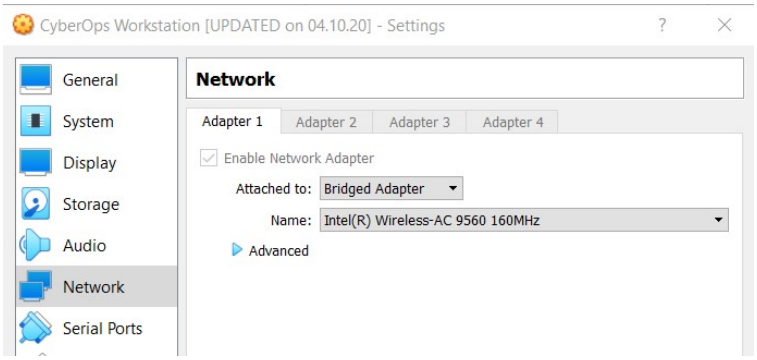
Instruções

Parte 1: Registre as Informações de Configuração de IP da VM

Na Parte 1, você usará comandos em sua CyberOps Workstation VM para encontrar e registrar os endereços MAC e IP da placa de interface de rede virtual (NIC) de sua VM, o endereço IP do gateway padrão especificado e o endereço IP do servidor DNS especificado para o PC. Anote essas informações na tabela fornecida. As informações serão usadas em partes deste laboratório com a análise de pacotes.

Descrição	Configurações
Endereço IP	
Endereço MAC	
Endereço IP do gateway padrão	
Endereço IP do servidor DNS	

a. As configurações de rede da VM do CyberOps Workstation devem ser definidas como adaptador de ponte. Para verificar as configurações de rede, acesse: **Máquina** > **Configurações**, Selecione **Rede**, a Guia Adaptador 1, Conectado a: **Adaptador em Ponte**.



b. Abra um terminal na VM. Digite **ifconfig** no prompt para exibir as informações da interface. Se você não tiver um endereço IP em sua rede local, execute o seguinte comando no terminal:

```
[analyst@secOps~]$ sudo lab.support.files/scripts/configure_as_dhcp.sh
Configurando a NIC para solicitar informações de IP via DHCP...
Solicitando informações de IP ...
Configuração de IP bem-sucedida.
```

Observação: Na Parte 1, seus resultados variam dependendo das configurações de rede local e da conexão com a Internet.

```
[analyst@secOps ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.8.10 netmask 255.255.255.0 broadcast 192.168.8.255
        inet6 fe80::a00:27ff:fe82:75df prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:82:75:df txqueuelen 1000 (Ethernet)
        Pacotes RX 41953 bytes 14354223 (13,6 MiB)
        Erros RX 0 eliminados 0 excedem 0 quadros 0
        TX packets 15249 bytes 1723493 (1.6 MiB)
        Erros de TX 0 descartados 0 exceções 0 portadora 0 colisões 0
<some output omitted>
```

c. No prompt do terminal, digite **cat /etc/resolv.conf** para determinar o servidor DNS.

```
[analyst@secOps ~]$ cat /etc/resolv.conf
# Resolver configuration file.
# Consulte resolv.conf (5) para obter detalhes.
nameserver 8.8.4.4
nameserver 209.165.200.235
```

d. No prompt do terminal, digite **netstat -rn** para exibir a tabela de roteamento IP para o endereço IP do gateway padrão.

```
[analyst@secOps ~]$ netstat -rn
Tabela de roteamento IP do kernel
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 192.168.8.1 0.0.0.0 UG 0 0 0 enp0s3
192.168.8.0 0.0.0.0 255.255.255.0 U 0 0 0 0 enp0s3
192.168.8.1 0.0.0 255.255.255.255 UH 0 0 0 enp0s3
```

Observação: O endereço IP do DNS e o endereço IP do gateway padrão geralmente são os mesmos, especialmente em redes pequenas. No entanto, em uma rede de negócios ou escolar, os endereços provavelmente seriam diferentes.

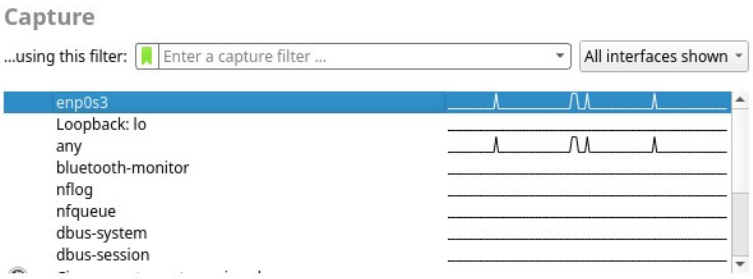
Parte 2: Usar o Wireshark para Capturar Consultas e Respostas DNS

Na Parte 2, você configurará o Wireshark para capturar pacotes de consulta e resposta DNS. Isso demonstrará o uso do protocolo de transporte UDP enquanto se comunica com um servidor DNS.

a. Na janela do terminal, inicie o Wireshark e clique em **OK** quando solicitado.

```
[analyst@secOps ~]$ wireshark &
```

b. Na janela Wireshark, selecione e clique duas vezes em **enp0s3** na lista de interface.



c. Abra o navegador da web e navegue até **www.google.com**.

d. Clique em **Stop** para interromper a captura do Wireshark ao ver a página inicial do Google.

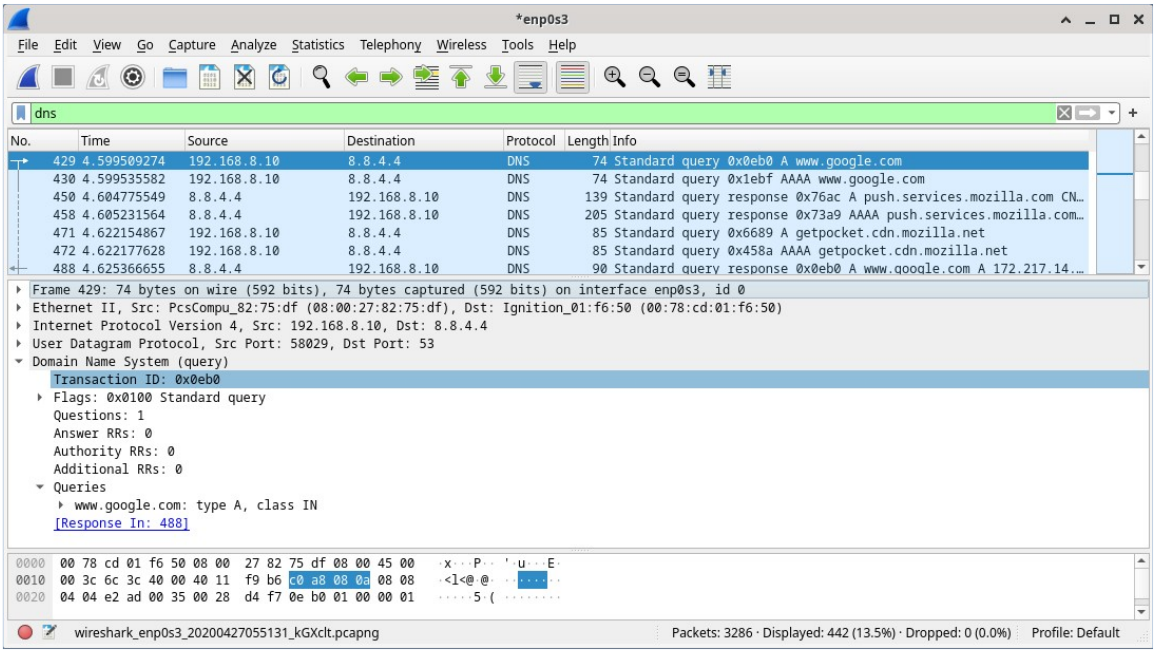
Parte 3: Analisar Pacotes DNS ou UDP Capturados

Na Parte 3, você examinará os pacotes UDP gerados ao se comunicar com um servidor DNS para os endereços IP de www.google.com.

Etapa 1: Filtrar os pacotes DNS.

a. Na janela principal do Wireshark, digite **dns** no campo **Filter** . Clique em **Aplicar**.

Observação: se não vir nenhum resultado após ter aplicado o filtro DNS, feche o navegador Web. Na janela do terminal, digite ping **www.google.com** como uma alternativa ao navegador da Web.



b. No painel da lista de pacotes (seção superior) na janela principal, localize o pacote que inclui **Standard query** (Consulta padrão) e **A www.google.com**. Veja o quadro 429 acima como exemplo.

Etapa 2: Examine os campos em um pacote de consulta DNS.

Os campos de protocolo, destacados em cinza, são exibidos no painel de detalhes do pacote (seção do meio) da janela principal.

a. Na primeira linha do painel de detalhes do pacote, o quadro 429 tinha 74 bytes de dados na transmissão. Este é o número de bytes necessários para enviar uma consulta DNS a um servidor nomeado solicitando os endereços IP de www.google.com. Se você usou um endereço da Web diferente, como www.cisco.com, a contagem de bytes pode ser diferente.

b. A linha Ethernet II exibe os endereços MAC origem e destino. O endereço MAC de origem é de sua VM porque sua VM originou a consulta DNS. O endereço MAC destino é o endereço do gateway padrão, porque esta é a última parada antes desta consulta sair da rede local.

O endereço MAC de origem é o mesmo registrado na Parte 1 para a VM?

c. Na linha do protocolo da Internet versão 4, a captura do Wireshark do pacote IP indica que o endereço IP de origem desta consulta DNS é 192.168.8.10 e o endereço IP de destino é 8.8.4.4. Neste exemplo, o endereço de destino é o servidor DNS.

Você pode identificar os endereços IP e MAC para a origem e os destinos deste pacote?

Dispositivo	Endereço IP	Endereço MAC
Estação de Trabalho de Origem		

Dispositivo	Endereço IP	Endereço MAC
Servidor DNS de Destino/Gateway Padrão		

Observação: O endereço IP de destino é para o servidor DNS, mas o endereço MAC de destino é para o gateway padrão.

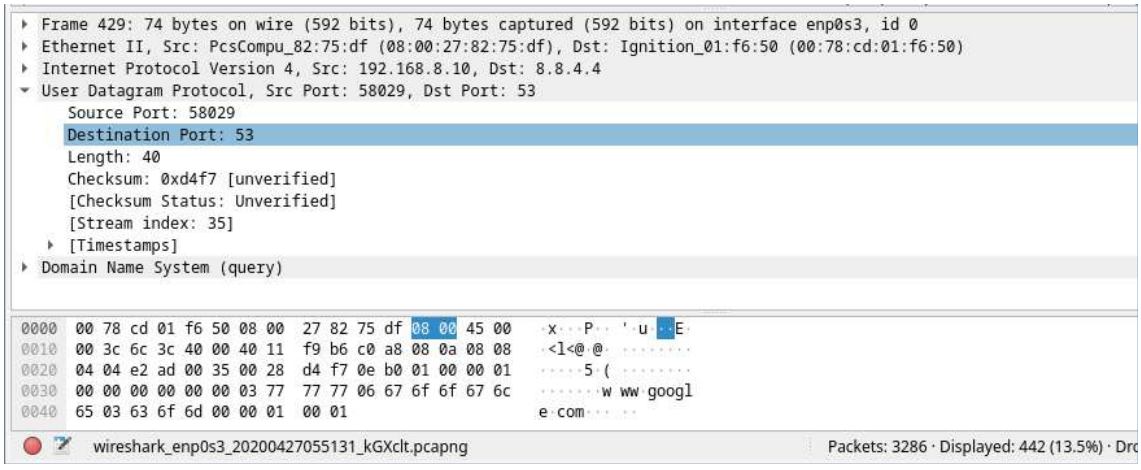
O pacote IP e o cabeçalho encapsulam o segmento UDP. O segmento UDP contém a consulta DNS como os dados.

d. Um cabeçalho UDP tem apenas quatro campos: porta de origem, porta de destino, comprimento e checksum. Cada campo em um cabeçalho UDP possui somente 16 bits conforme descrito abaixo.

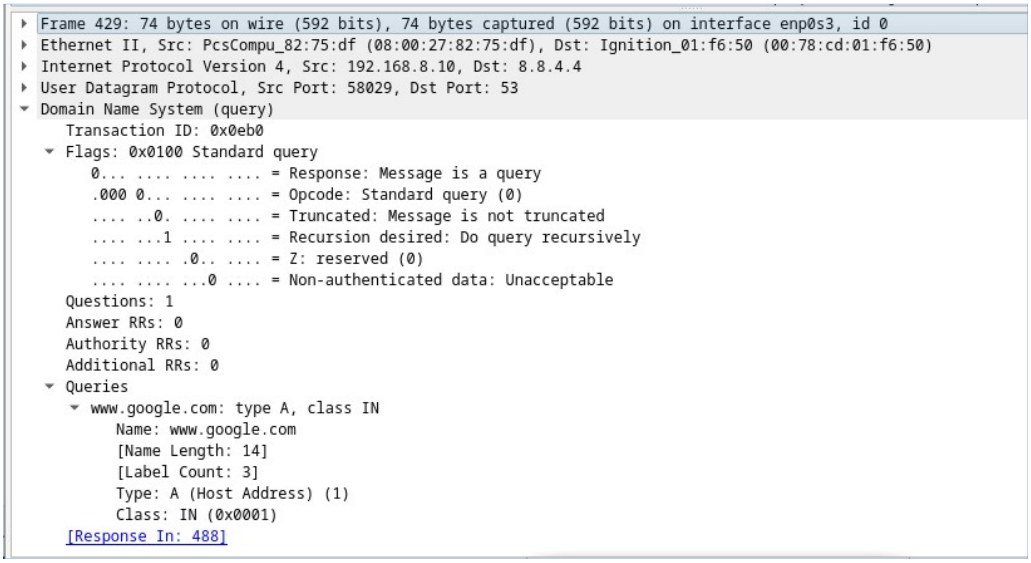
UDP SEGMENT

0	16	31
UDP SOURCE PORT	UDP DESTINATION PORT	
UDP MESSAGE LENGTH	UDP CHECKSUM	
DATA		
DATA ...		

Clique na seta ao lado de User Datagram Protocol para exibir os detalhes. Observe que há apenas quatro campos. O número da porta dorigem neste exemplo é 58029. A porta de origem foi gerada aleatoriamente pela VM usando números de porta que não são reservados. A porta de destino é 53. A porta 53 é uma porta muito conhecida reservada para uso do DNS. Os servidores DNS ouvem na porta 53 as consultas DNS dos clientes.



Neste exemplo, o tamanho do segmento UDP é 40 bytes. O comprimento do segmento UDP em seu exemplo pode ser diferente. Dos 40 bytes, 8 bytes são usados como cabeçalho. Os outros 32 bytes são usados por dados da consulta DNS. Os 32 bytes de dados de consulta DNS estão na ilustração a seguir no painel de bytes de pacote (seção inferior) da janela principal do Wireshark.



A soma de verificação é usada para determinar a integridade do cabeçalho UDP depois que ele cruzou a Internet.

O cabeçalho UDP tem pouca sobrecarga visto que o UDP não tem campos associados ao handshake triplo do TCP. Todos os problemas de confiabilidade da transferência de dados que ocorrem devem ser tratados pela camada de aplicação.

Expanda conforme necessário para ver os detalhes. Registre os resultados do Wireshark na tabela abaixo:

Descrição	Resultados Wireshark
Tamanho do quadro	
Endereço MAC origem	
Endereço MAC destino	
Endereço IP de origem	
Endereço IP de destino	
Porta de origem	
Porta de destino	

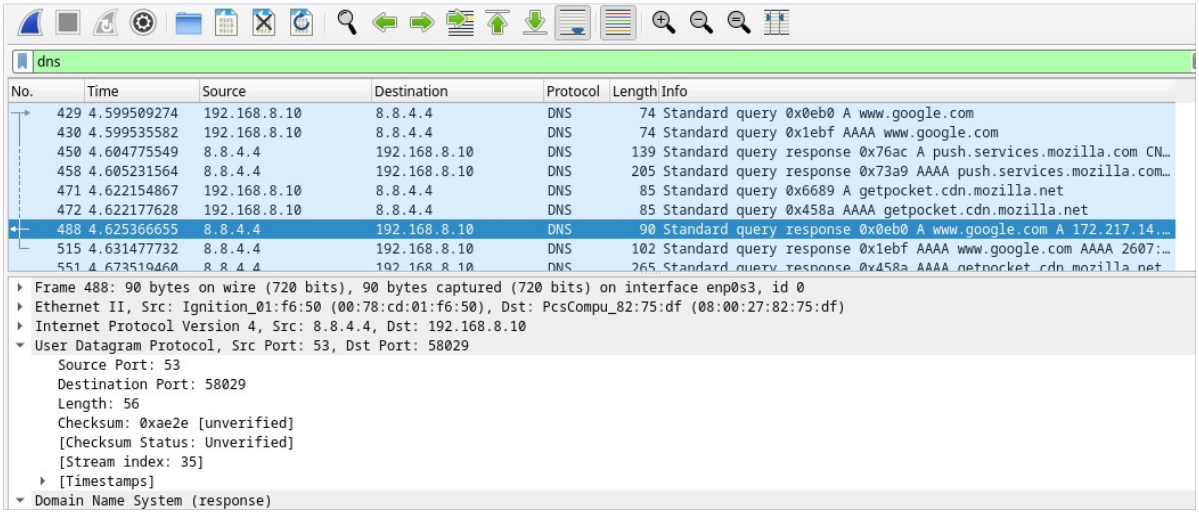
O endereço IP origem é o mesmo que o endereço IP do computador local registrado na Parte 1?

O endereço IP de destino é o mesmo do gateway padrão observado na Parte 1?

Etapa 3: Examine os campos em um pacote de resposta DNS.

Nesta etapa, você examinará o pacote de resposta DNS e verificará se o pacote de resposta DNS também usa o UDP.

a. Neste exemplo, o quadro 488 é o pacote de resposta DNS correspondente. Observe que o número de bytes no fio é 90. É um pacote maior em relação ao pacote de consulta DNS. Isso ocorre porque o pacote de resposta DNS incluirá uma variedade de informações sobre o domínio.



b. No quadro Ethernet II para a resposta DNS, de qual dispositivo vem o endereço MAC origem e de qual dispositivo é o endereço MAC destino?

c. Observe os endereços IP de origem e destino no pacote IP.

Qual é o endereço IP de destino?

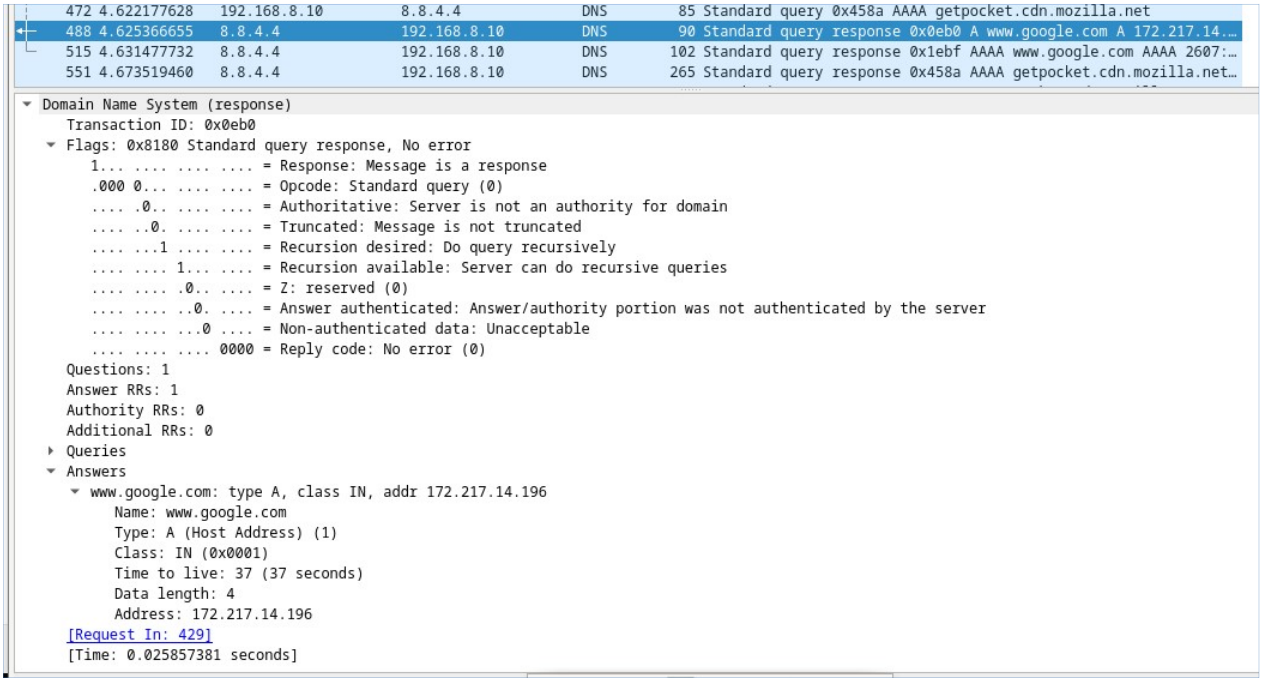
Qual é o endereço IP de origem?

O que aconteceu com as funções de origem e destino da VM e do gateway padrão?

d. No segmento UDP, a função dos números de porta também foi invertida. O número da porta de destino é 58029. O número da porta 58029 é a mesma que foi gerada pela VM quando a consulta DNS foi enviada ao servidor DNS. Sua VM escuta uma resposta DNS nesta porta.

O número da porta de origem é 53. O servidor DNS ouve uma consulta DNS na porta 53 e depois envia uma resposta DNS com um número de porta de origem 53 de volta ao autor da consulta DNS.

Quando a resposta DNS é expandida, observe os endereços IP resolvidos para www.google.com na seção **Answers (Respostas)**.



Perguntas para reflexão

Quais são os benefícios de usar o UDP em vez do TCP como um protocolo de transporte para o DNS?