Travaux pratiques – Utiliser Wireshark pour examiner une capture DNS UDP

1. Topologie



1. Objectifs

Partie 1 : Enregistrer les informations de configuration IP d'un ordinateur

Partie 2 : Utiliser Wireshark pour capturer les requêtes et les réponses DNS

Partie 3 : Analyser les paquets DNS ou UDP capturés

1. Contexte/scénario

Lorsque vous utilisez Internet, vous utilisez un système DNS (Domain Name System). DNS est un réseau distribué de serveurs qui traduit des noms de domaine faciles à utiliser comme www.google.com en adresse IP. Lorsque vous tapez l'adresse URL d'un site web dans votre navigateur, votre PC envoie une requête DNS à l'adresse IP du serveur DNS. La requête de votre ordinateur au serveur DNS et la réponse du serveur DNS utilisent le protocole UDP (User Datagram Protocol) comme protocole de couche transport. À la différence du protocole TCP, le protocole UDP est sans connexion et ne nécessite aucune configuration de session. Les requêtes et les réponses DNS sont très petites et ne génèrent pas de surcharge comme le protocole TCP.

Dans le cadre de ces travaux pratiques, vous communiquerez avec un serveur DNS en envoyant une requête DNS à l'aide du protocole de transport UDP. Vous utiliserez Wireshark pour examiner les échanges de requêtes et de réponses DNS avec le même serveur.

1. Ressources requises

* Poste de travail virtuel CyberOps
* Accès Internet

1. Enregistrer les informations de configuration IP de la machine virtuelle

Dans la première partie, vous utiliserez les commandes de votre poste de travail virtuel CyberOps pour trouver et enregistrer les adresses MAC et IP de la carte d'interface virtuelle de votre ordinateur, l'adresse IP de la passerelle par défaut spécifiée et l'adresse IP du serveur DNS spécifiée pour l'ordinateur. Enregistrez ces informations dans la table fournie. Elles seront utilisées dans les sections suivantes de ces travaux pratiques avec l'analyse des paquets.

|  |  |
| --- | --- |
| Adresse IP |  |
| Adresse MAC |  |
| Adresse IP de la passerelle par défaut |  |
| Adresse IP du serveur DNS |  |

* + 1. Ouvrez un terminal sur la machine virtuelle. Saisissez **ifconfig** à l'invite pour afficher les informations liées à l'interface.

[analyst@secOps ~]$ **ifconfig**

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.1.19 netmask 255.255.255.0 broadcast 192.168.1.255

inet6 fe80::997f:9b16:5aae:1868 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:c9:fa:a1 txqueuelen 1000 (Ethernet)

RX packets 1381 bytes 87320 (85.2 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 24 bytes 1857 (1.8 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

device interrupt 19 base 0xd000

<some output omitted>

* + 1. À l'invite du terminal, saisissez **cat /etc/resolv.conf** pour déterminer le serveur DNS.

[analyst@secOps ~]$ **cat /etc/resolv.conf**

# Generated by resolvconf

nameserver 192.168.1.1

* + 1. À l'invite du terminal, saisissez **netstat - r** pour afficher la table de routage IP à l'adresse IP de la passerelle par défaut.

[analyst@secOps ~]$ **netstat -r**

Table de routage IP du noyau

Destination Gateway Genmask Flags MSS Window irtt Iface

default 192.168.1.1 0.0.0.0 UG 0 0 0 enp0s3

192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s3

**Remarque** : l'adresse IP du serveur DNS et l'adresse IP de la passerelle par défaut sont souvent les mêmes, surtout dans les petits réseaux. Toutefois, sur le réseau d'une entreprise ou d'un établissement scolaire, les adresses sont généralement différentes.

1. Utiliser Wireshark pour capturer les requêtes et les réponses DNS

Dans la partie 2, vous allez configurer Wireshark pour capturer des paquets de requêtes et de réponses DNS. Cet exercice permet de tester l'utilisation du protocole de transport UDP lors de la communication avec un serveur DNS.

* + 1. Dans la fenêtre de terminal, lancez Wireshark et cliquez sur **OK** lorsque vous y êtes invité.

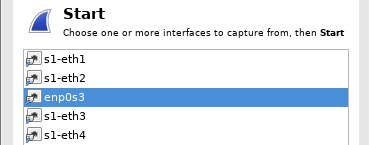
[analyst@secOps ~]$ **sudo wireshark-gtk**

[sudo] password for analyst:

\*\* (wireshark-gtk:950): WARNING \*\*: Couldn't connect to accessibility bus: Failed to connect to socket /tmp/dbus-REDRWOHelr: Connection refused

Gtk-Message: GtkDialog mapped without a transient parent. This is discouraged.

* + 1. Dans la fenêtre Wireshark, sélectionnez **enp0s3** dans la liste de l'interface et cliquez sur **Start**.



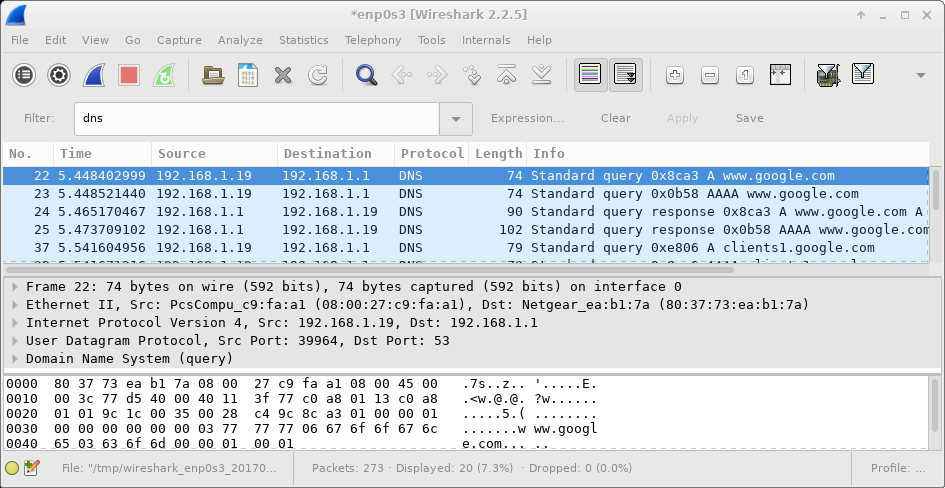
* + 1. Après avoir sélectionné l'interface souhaitée, cliquez sur Start pour capturer les paquets.
    2. Ouvrez un navigateur web et tapez **www.google.com**. Appuyez sur Entrée pour continuer.
    3. Cliquez sur **Stop** (Arrêter) pour arrêter la capture Wireshark lorsque la page d'accueil de Google s'affiche.

1. Analyser les paquets DNS ou UDP capturés

Dans la troisième partie, vous examinerez les paquets UDP qui ont été générés lors de la communication à un serveur DNS des adresses IP pour www.google.com.

* 1. Filtrez les paquets DNS.
     1. Dans la fenêtre principale de Wireshark, saisissez **dns** dans le champ **Filter**. Cliquez sur **Appliquer**.

**Remarque**: si aucun résultat ne s'affiche après l'application du filtre DNS, fermez le navigateur web. Dans la fenêtre de terminal, saisissez ping [**www.google.com**](http://www.google.com) comme alternative au navigateur web.



* + 1. Dans le volet de la liste des paquets (section supérieure) de la fenêtre principale, localisez le paquet qui inclut « Standard query » et « A www.google.com ». Voir la trame 22 ci-dessus en guise d'exemple.
  1. Examinez les champs d'un paquet de requêtes DNS.

Les champs de protocole, surlignés en gris, s'affichent dans le volet des informations sur les paquets (section centrale) de la fenêtre principale.

* + 1. Dans le volet de détails des paquets, la trame 22 possède 74 octets de données sur le câble comme indiqué à la première ligne. Il s'agit du nombre d'octets nécessaires pour envoyer une requête DNS à un serveur nommé demandant les adresses IP de www.google.com. Si vous avez utilisé une adresse web différente, comme www.cisco.com, le nombre d'octets peut varier.
    2. La ligne Ethernet II affiche les adresses MAC source et de destination. L'adresse MAC source provient de votre machine virtuelle, car c'est elle qui a émis la requête DNS. L'adresse MAC de destination provient de la passerelle par défaut, car c'est le dernier arrêt avant la sortie de cette requête du réseau local.

L'adresse MAC source est-elle identique à celle enregistrée dans la première partie pour la machine virtuelle ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

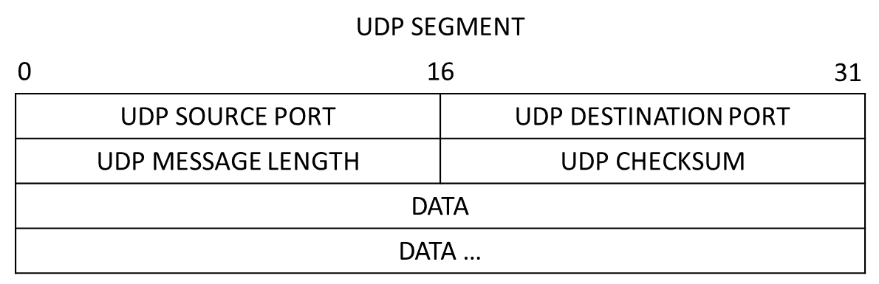
* + 1. Sur la ligne Internet Protocol Version 4, la capture Wireshark de paquets IP indique que l'adresse IP source de cette requête DNS est 192.168.1.19 et l'adresse IP de destination est 192.168.1.1. Dans cet exemple, l'adresse de destination est la passerelle par défaut. Le routeur est la passerelle par défaut sur ce réseau.

Pouvez-vous identifier les adresses IP et MAC des périphériques source et de destination ?

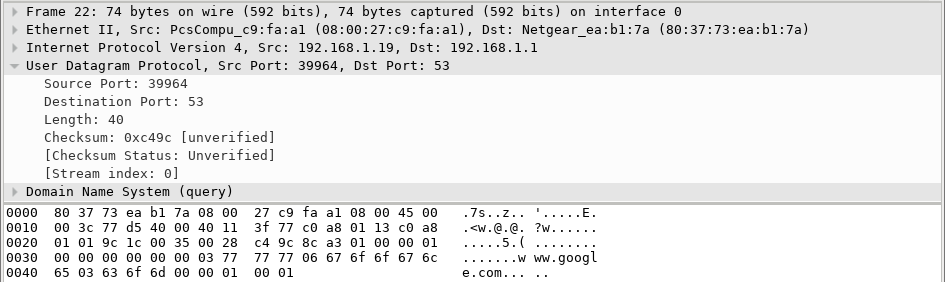
|  |  |  |
| --- | --- | --- |
| Appareil | Adresse IP | Adresse MAC |
| VM |  |  |
| Passerelle par défaut |  |  |

L'en-tête et le paquet IP encapsulent le segment UDP. Le segment UDP contient la requête DNS comme données.

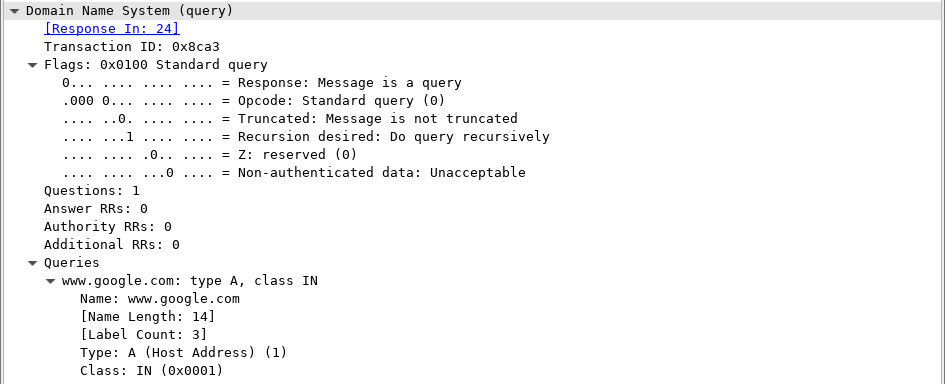
* + 1. Cliquez sur la flèche située à côté de User Datagram Protocol pour afficher les détails. Un en-tête UDP comporte uniquement quatre champs : source port (port source), destination port (port de destination), length (longueur) et checksum (somme de contrôle). Chaque champ de l'en-tête UDP ne dispose que de 16 bits comme indiqué ci-dessous.



* + 1. Cliquez sur la flèche située à côté de User Datagram Protocol pour afficher les détails. Notez qu'il n'existe que quatre champs. Le numéro du port source dans cet exemple est 39964. Le port source a été généré aléatoirement par la machine virtuelle parmi les numéros de port qui ne sont pas réservés. Le port de destination est le 53. Le port 53 est un port réservé destiné à une utilisation avec DNS. Les serveurs DNS écoutent sur le port 53 les requêtes DNS provenant des clients.



Dans cet exemple, la longueur du segment UDP est de 40 octets. La longueur du segment UDP dans votre exemple peut être différente. Sur 40 octets, 8 sont utilisés pour l'en-tête. Les 32 autres octets sont utilisés par les données de requête DNS. Les 32 octets de données de requête DNS sont mis en évidence dans l'illustration suivante du volet d'octets des paquets (section inférieure) de la fenêtre principale de Wireshark.



La somme de contrôle est utilisée pour déterminer l'intégrité du paquet UDP une fois qu'il a transité par Internet.

L'en-tête UDP surcharge peu le réseau parce que le protocole UDP n'a pas de champs associés à l'échange en trois étapes du protocole TCP. Tous les problèmes de fiabilité liés au transfert des données doivent être gérés par la couche application.

Notez les résultats de Wireshark dans le tableau ci-dessous :

|  |  |
| --- | --- |
| Taille de trame |  |
| Adresse MAC source |  |
| Adresse MAC de destination |  |
| Adresse IP source |  |
| Adresse IP de destination |  |
| Port source |  |
| Port de destination |  |

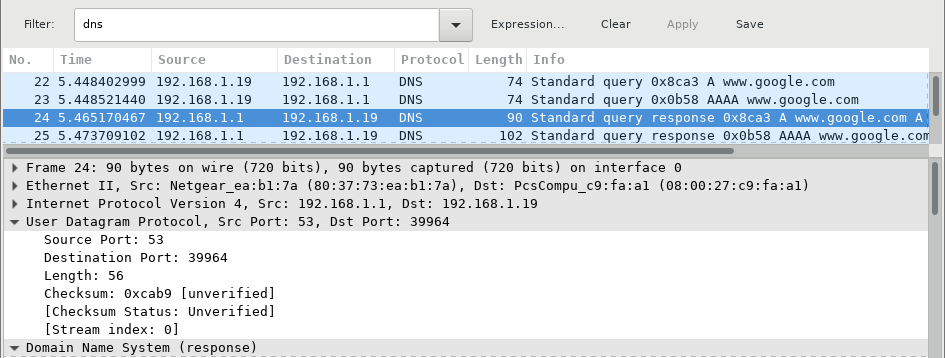
L'adresse IP source est-elle identique à l'adresse IP du PC local enregistrée dans la première partie ? \_\_\_\_\_\_\_\_\_\_\_\_\_

L'adresse IP de destination est-elle identique à la passerelle par défaut notée dans la première partie ? \_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Examinez les champs d'un paquet de réponses DNS.

Dans cette étape, vous examinerez le paquet de réponse DNS et vérifierez que le paquet de réponse DNS utilise aussi le protocole UDP.

* + 1. Dans cet exemple, la trame 24 est le paquet de réponse DNS correspondant. Notez que le nombre d'octets sur le câble est égal à 90. Il s'agit d'un paquet plus gros par rapport au paquet de requête DNS. C'est parce que le paquet de réponses DNS comprend diverses informations sur le domaine.



* + 1. Dans la trame Ethernet II pour la réponse DNS, de quel périphérique provient l'adresse MAC source et à quel périphérique correspond l'adresse MAC de destination ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Notez les adresses IP source et de destination du paquet IP. Quelle est l'adresse IP de destination ? Quelle est l'adresse IP source ?

Adresse IP de destination : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Adresse IP source : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Qu'est-il arrivé aux rôles de la source et de la destination pour la machine virtuelle et la passerelle par défaut ?

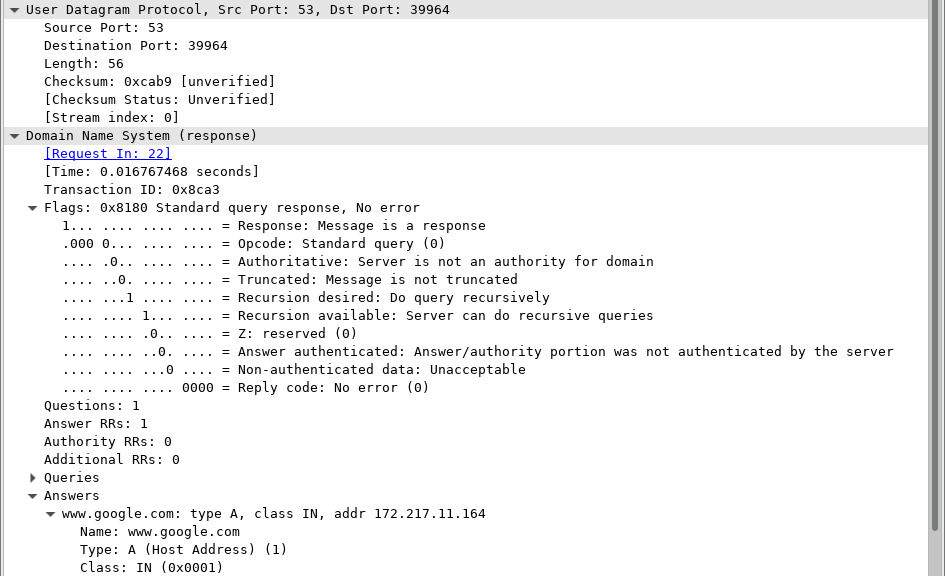
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Dans le segment UDP, le rôle des numéros de port a également été inversé. Le numéro du port de destination est 39964. Le numéro de port 39964 est le même port que celui qui a été généré par la machine virtuelle lorsque la requête DNS a été envoyée au serveur DNS. Votre machine virtuelle attend une réponse DNS sur ce port.

Le numéro du port source est 53. Le serveur DNS écoute une requête DNS sur le port 53, puis envoie une réponse DNS avec le numéro de port source 53 à l'émetteur de la requête DNS.

Lorsque la réponse DNS est développée, examinez les adresses IP résolues pour www.google.com dans la section **Answers** (Réponses).



1. Remarques générales

Quels sont les avantages du protocole UDP par rapport au protocole TCP comme protocole de transport sur un serveur DNS ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_