RESEAUX

Labo 4b - Wireshark | DNS

RESUME

Durant ce laboratoire, vous allez découvrir le fonctionnement de DNS.

Olivier Masit

SE - BLOC1 - UE02 – Réseaux – Labo 4

DUREE ESTIMEE

2h00

1 Introduction

Durant ce laboratoire, vous allez analyser des transmissions DNS.

2 Objectifs

- Approfondir la maîtrise de l'outil Wireshark.
- Maîtriser le mécanisme de résolution des noms DNS.

3 Exercices

Ouvrez le fichier **dns.pcap** fourni pour ce labo.

1. Isolez les traces pour ne garder que des paquets utilisant le protocole DNS.
2. Combien de paquets ont été transmis en TCP ? (8)
3. Combien de paquets ont été transmis en UDP ? (88)
4. Cette capture a-t-elle été effectuée sur une machine client ou sur une machine serveur ?
5. Par quel(s) service(s), deamon(s) ou logiciel(s) ce trafic a-t-il été généré ?
6. Filtrez les paquets sur dns et udp et analysez chaque transaction DNS/UDP en détail.
7. Quelle différence y-a-t-il entre la transaction qui a débuté à 1603204787.483469000 Epoch Time et celle qui a débuté à 1603204787.512905000 ?
   7.1. De quelle machine vient la requête ?
   7.2. Quelle est cette demande ?
   7.3. Quelle est la réponse ?
8. Quelle différence y-a-t-il entre la transaction qui a débuté à 1603204787.483469000 Epoch Time et celle qui a débuté à 1603204822.580222000 ?
9. Quelle différence y-a-t-il entre la transaction qui a débuté à 1603204787.483469000 Epoch Time et celle qui a débuté à 1603204895.523279000 ?
10. Que peut-on dire de la transaction qui a débuté à 1603204905.980035000 Epoch Time ? Pourquoi est-elle si courte ?
11. Pour chacune des transactions analysées ci-dessus
    11.1. Quel serveur DNS a renvoyé la réponse à la demande A ?
    11.2. La réponse était-elle « authoritative » ?
    11.3. La réponse était-elle récursive out itérative ?

3.1 Résolution de problème.

1. Ouvrez le fichier **Cdns.pcap**.
   1.1. Examinez la trace DNS. Quel est le problème ? D'où peut-il provenir ?
2. Ouvrez le fichier **Wdns.pcap**
   2.1. Un de vos collègues du support a reçu un appel d'un utilisateur qui trouve que certains sites sur lesquels il se rend régulièrement ont parfois une interface légèrement différente.
   2.2. Votre collègue du support a capturé le trafic réseau et pense sans en être certain que le problème pourrait soit venir du serveur DNS soit serait dû à un problème de sécurité.
   2.3. Vous constatez que le serveur DNS fonctionne normalement.

```
PS C:\Users\Administrator> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-G17RQS6HK4D
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : 00-15-5D-58-A1-0A
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.27.54.70(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.27.48.1
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
PS C:\Users\Administrator> Get-Service dns

Status   Name               DisplayName
------   ----               -----------
Running  dns                DNS Server


PS C:\Users\Administrator> Get-DnsServerForwarder


UseRootHint         : True
Timeout(s)          : 3
EnableReordering    : True
IPAddress           : 1.1.1.1
ReorderedIPAddress : 1.1.1.1



PS C:\Users\Administrator> _
```

2.4. Analysez la capture faite par votre collègue et expliquez ce qu'il s'est passé.