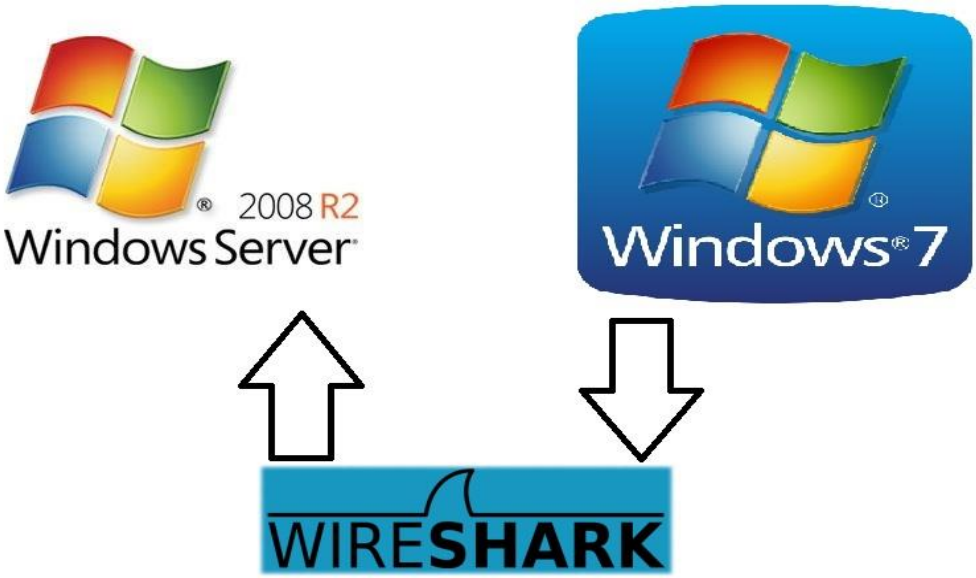
ITIC PARIS

Analyse de trame DHCP

Sous WireShark



Youness Afif, Dineche Radjou, Mehdi Attaf, Aaron Ghezail,
Samuel Benaim, Yassine Baddaoui
29/03/2016

Contexte

WireShark est un analyseur de protocole de réseau pour UNIX et Windows.

Wireshark est analyseur de protocole réseau avant tout et largement utilisé dans le monde. Il vous permet de voir ce qui se passe sur votre réseau à un niveau microscopique et est de facto (et souvent de jure) standard dans de nombreuses entreprises commerciales et sans but lucratif, les organismes gouvernementaux et les établissements d' enseignement. Développement Wireshark prospère grâce aux contributions volontaires des experts à travers le monde et la mise en réseau est la continuation d'un projet lancé par Gerald Combs en 1998.

Installation de la fonction DHCP sur Windows 2008 R2 afin qu'il distribue une adresse IP sur les machines virtuelles Windows 7, …

Les machines d'un parc informatique ont des difficultés à recevoir une adresse IP depuis le serveur DHCP. Pour cela nous allons vérifier les requêtes DHCP via le soft WireShark.

*Nous réaliserons une capture de la trame DHCP via le software **WireShark** afin de pouvoir visualiser les trames. Ce logiciel nous permettra de pouvoir voir si, le serveur DHCP attribue bien une adresse IP ainsi que ses paramètres, mais aussi si la machine reçoit l'adresse IP distribué.*

Prérequis

Machine physique (Avec Windows 10 x64) :

- 3,5 GHz ou plus
- 8 Go de RAM ou plus
- 100 Go d'espace libre sur le disque dur ou plus

Machine virtuelle :

Windows Server 2008 R2

- Minimum : 1 GHz (processeur x86) ou 1,4 GHz (processeur x64)
  Recommandé : 2 GHz ou plus rapide
  Remarque : un processeur Intel Itanium 2 est requis pour Windows Server 2008 pour les systèmes Itanium
- Minimum : 10 Go

Windows XP

- Processeur Pentium 233 mégahertz (MHz) ou supérieur (300 MHz recommandé)
- Au moins 64 méga-octets (Mo) de RAM (128 Mo recommandé)
- Au moins 1,5 giga-octets (Go) d'espace disque dur disponible

Windows 7

- 1 gigahertz (GHz) ou plus rapide
- Une RAM de 1 gigaoctet (Go) (32 bits) ou de 2 Go (64 bits)
- Un espace disque disponible de 16 Go (32 bits) ou de 20 Go (64 bits)

Tutoriel

Les trames DHCP seront visualisées sur une des machines cliente sous Windows.

Nous allons simuler cette opération avec une machine virtuelle cliente qui recevra une adresse IP via un serveur DHCP virtuel sous Windows Server.

Nous allons télécharger le Soft WireShark à l'adresse suivant :
http://www.wireshark.org/download.html , la version la plus stable à cette date est la 2.0.2.

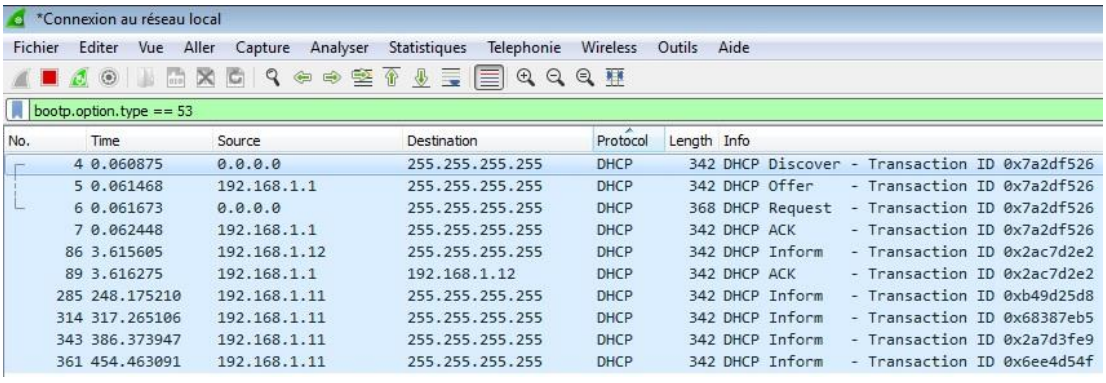
Une fois le téléchargement terminé nous lancerons l'installation avec tous les paramètres par défaut.

Mode Opératoire

Au lancement de WireShark, depuis la page d'accueil nous cliquerons sur **« Connexion au réseau local ».**

Nous constatons que plusieurs trames de divers protocoles ont été capturé. Nous filtrons ces trames pour n'avoir seulement celles du DHCP. La commande utilisée sera **« bootp.option.type ==53 »** qu'il faudra insérer dans le champs alloué.

Voici les trames dhcp capturées :



- DHCPDISCOVER (pour localiser les serveurs DHCP disponibles)
- DHCPOFFER (réponse du serveur à un paquet DHCPDISCOVER, qui contient les premiers paramètres)
- DHCPREQUEST (requête diverse du client pour par exemple prolonger son bail)
- DHCPACK (réponse du serveur qui contient des paramètres et l'adresse IP du client)

- DHCPNAK (réponse du serveur pour signaler au client que son bail est échu ou si le client annonce une mauvaise configuration réseau)
- DHCPDECLINE (le client annonce au serveur que l'adresse est déjà utilisée)
- DHCPRELEASE (le client libère son adresse IP)
- DHCPINFORM (le client demande des paramètres locaux, il a déjà son adresse IP)