TP Découverte « Analyse »

Trouver le problème :

Pour un premier temps, je me suis concentré sur le message d'erreur, « Conflit d'IP détecté ». La recherche m'a donné que la seule source de cette erreur est qu'il existe plusieurs fois la même adresse IP sur un réseau.

Rechercher cela m'a montré qu'il existe un problème avec le serveur DHCP et qu'il est mal configuré, etc., mais M. Jobard disait que réellement ce ne peut pas être le cas, car les serveurs DHCP dans un bureau sont assez bien maintenus.

Après avoir trouvé un lien titré « How to enable unauthorized DHCP server detection » j'ai compris que si les serveurs DHCP sont trop « intelligents » pour faire des erreurs comme cela, la source doit être un deuxième serveur DHCP qui n'est pas administré par les administrateurs du réseau, ce qui donc crée des adresses IP doublés sur le réseau.

Cela explique aussi pourquoi le problème est seulement *quelque fois* présent. La configuration dynamique/automatique/aléatoire cause que quelque fois les mêmes adresses sont distribué, car les deux serveurs ne communiquent pas cette information entre eux. De plus cet explique aussi pourquoi les ordinateurs ouvrent quelque fois des liens externes. Ce trafique est donné par le serveur DHCP non-autorisé. Une autre note est aussi que l'état de ce problème change à chaque fois que l'ordinateur redémarre, alors à chaque fois qu'il requête une adresse IP.

Comment ça marche :

1. Un serveur DHCP non-autorisé (pas reconnu par les administrateurs) s'installe sur le réseau.
2. Un ordinateur s'allume et fait une requête DHCP.
3. Les deux serveurs DHCP répondent sur la requête.
4. L'ordinateur prend l'adresse IP donné par le serveur qui répond le plus rapide.

Si le Rogue serveur DHCP répond en premier, il contrôle le trafique de cet ordinateur.

Comment ce s'est passé :

On ne sait pas exactement comment le serveur pouvait s'installer sur le réseau, mais on a l'indice que le problème commençait après qu'une personne a installé un photocopieur. C'est possible que le photocopieur ait accès sur le réseau et qu'avec cet accès la personne installait le serveur DHCP sur le réseau.

Sur la page de « Rogue DHCP » sur Wikipédia on trouve aussi que la source pourrait être un virus. Cela pourrait dire qu'un employé téléchargeait ce virus en téléchargeant « Star Wars : Revenge of the Sith » illégalement sur l'internet. Je comprends, si j'ai le choix entre payer 10 balles à Disney ou télécharger un virus, je préfèrerai le deuxième.

Pourquoi :

L'attaqueur peut avoir plusieurs motifs pour installer un serveur DHCP sur un réseau mais les raisons les plus probable sont la disruption et l'espionnage.

La disruption est d'essayer d'empêcher l'activité de la boîte pour peu importe quelle raison.

L'espionnage est de collecter des informations, surtout des informations sensibles, qui passe dans le réseau pour peu importe quelle raison.

Comment trouver :

Une simple façon de trouver si le problème est une Rogue serveur DHCP est de regarder le tableau des IPs dans le serveur DHCP. Si on voit que cet ordinateur problématique n'existe pas dans le tableau et qu'il *devrait* être connecté, on peut assumer que c'est causé par un deuxième serveur DHCP.

Solution :

Une solution que je vois beaucoup est d'utiliser Active Directory. Si le serveur DHCP n'appartient pas du domaine, il ne peut pas être ajouté dans le réseau.

Il semble quand-même que la meilleure solution est le « DHCP snooping ». Un switch entre les ordinateurs et les serveurs DHCP laisse passer les requêtes DHCP du serveur autorisé par un port où on sait qu'on peut avoir confiance. Les requêtes DHCP passant par autres ports sont bloquées.

Conclusion :

L'événement d'avoir un serveur DHCP non-autorisé est très rare, en plus car toutes les stratégies de réseau (switch, AD, etc.) protègent par défaut contre cela.

En tout cas, comme pour tous les problèmes du réseau, une bonne pratique est le monitoring. Surveiller le réseau pour des anomalies est la meilleure façon de se protéger. Utiliser des IDS est la façon plus simple de se protéger.

Sources :

How to Find and Deal with Rogue DHCP Servers | Auvik

Rogue DHCP - Wikipedia

What Is DHCP Snooping and How It Works? | FS Community