

Analyse attaque réseau

Résumé du contexte :

Ralentissement de la machine.

Déconnexion de temps en temps depuis quelques jours avec message « Conflit d'IP détecté ».
Après redémarrage fonctionne mais revient.

Redirection vers des sites.

Impact sur ses postes voisins.

Intervention d'un jeune pour mettre en place un photocopieur sur le réseau.

Vérifications / hypothèses :

Vérifier qu'est ce qu'a fait le jeune.

Spoofing / usurpation : DHCP, DNS

- ➔ Car ralentissement réseau donc plus de temps pour atteindre le serveur.
- ➔ Conflit d'IP donc plusieurs adresses similaires sur le même réseau
- ➔ Impact sur plusieurs postes donc attaque plus haute que les postes utilisateurs
- ➔ Redirection des sites, donc problème au niveau DNS qui fait une mauvaise redirection

Explication du processus DHCP, DNS Spoofing :

Résumé de l'attaque DHCP Spoofing :

Si la victime et l'attaquant sont sur le même réseau et que l'attaquant déploie un serveur DHCP malveillant, un PC se connectera et obtiendra une adresse IP du paquet qu'il reçoit en premier des deux serveurs.

Résumé de l'attaque DNS Spoofing :

Si la victime et l'attaquant sont sur le même réseau et que l'attaquant déploie un serveur DNS malveillant, alors lorsque les utilisateurs voudront visiter un site internet, l'adresse IP sera erronée et donc renvoyer vers un site malveillant choisit par l'attaquant.

Comment le pirate à réaliser cette attaque :

Pour réaliser cette attaque, je suppose qu'il a introduit le réseau de l'entreprise (physiquement avec l'intervention pour l'imprimante ? ou virtuellement) puis à déployer un serveur avec un

DHCP et DNS malveillant. Une fois configurer et mit en place les PCs du réseau se sont vu recevoir plusieurs paquets :

- ➔ (DHCPACK ; qui contient les paramètres de configuration réseau) des deux serveurs (malveillant et bienfaisant),
- ➔ (DNS response : paquet qui contient la direction IP / adresse)

Si le poste reçoit en premier le paquet malveillant, il sera donc connecté aux mauvais serveurs.

NOTES SUR LES PROTOCOLES ET PAQUETS DHCP / DNS

Protocole et Paquets DHCP

Protocoles :

UDP (User Datagram Protocol) : DHCP utilise UDP comme protocole de transport.

Port 67 : Utilisé par le serveur DHCP pour écouter les demandes des clients DHCP.

Port 68 : Utilisé par le client DHCP pour recevoir les réponses du serveur DHCP.

Paquets :

DHCPDISCOVER : Émis par un client DHCP pour trouver les serveurs DHCP disponibles sur le réseau.

DHCP OFFER : Émis par un serveur DHCP en réponse à un DHCPDISCOVER pour offrir une adresse IP au client.

DHCP REQUEST : Émis par le client DHCP pour demander ou confirmer l'adresse IP proposée par le serveur DHCP.

DHCPACK : Émis par le serveur DHCP pour accuser réception de la demande de l'adresse IP par le client et fournir les paramètres de configuration réseau.

DHCP NAK : Émis par le serveur DHCP si l'adresse IP demandée par le client n'est pas disponible.

DHCP RELEASE : Émis par le client pour libérer l'adresse IP et informer le serveur qu'il n'en a plus besoin.

DHCP DECLINE : Émis par le client pour informer le serveur que l'adresse IP proposée est déjà utilisée sur le réseau.

DHCP INFORM : Émis par un client DHCP qui a déjà une adresse IP mais qui a besoin d'informations supplémentaires du serveur DHCP.

Protocole et Paquets DNS

Protocoles :

UDP (User Datagram Protocol) : Le DNS utilise UDP pour la plupart des requêtes, en particulier pour les requêtes courtes qui tiennent dans un seul paquet.

Port 53 : Le port par défaut pour les requêtes et les réponses DNS.

TCP (Transmission Control Protocol) : Utilisé par le DNS pour les transferts de zone ou lorsque les réponses dépassent la taille maximale des paquets UDP.

Port 53 : Le même port est utilisé pour TCP en DNS.

Paquets :

DNS Query : Requête envoyée par un client DNS pour résoudre un nom de domaine en adresse IP ou obtenir d'autres informations DNS.

DNS Response : Réponse du serveur DNS contenant les résultats de la requête.

DNS Update : Utilisé pour mettre à jour les enregistrements DNS dynamiquement dans les serveurs DNS.

DNS Zone Transfer : Permet de transférer une zone DNS complète d'un serveur DNS maître à un serveur DNS secondaire. Il existe deux types de transferts de zone :

AXFR : Transfert de zone complet.

IXFR : Transfert de zone incrémentiel, qui transmet seulement les changements apportés à la zone.

Comment se protéger de ces attaques ?

- Une technologie est disponible sur les OS des commutateurs : DHCP Snooping, son rôle étant de trier les paquets reçus d'un serveur et donc de connecter les clients au DHCP valide et d'écarter les paquets d'un DHCP non autorisé.
- Mettre en place des ACL afin de filtrer les paquets DHCP et DNS et de bloquer ceux non autorisés.
- Configurer les clients, par exemples les imprimantes en IP fixes, ou certains PC en IP fixes.
- Activer le DNSSEC : une technologie qui permet d'authentifier les réponses DNS, il ajoute une signature cryptographique, lorsqu'une requête DNS est effectuée, alors DNSSEC vérifie l'authenticité et l'intégrité de la réponse.
- Mettre en place une supervision et surveillance accrue au niveau du réseau.
- Mettre en place une procédure pour réagir à ce type d'attaques.

Comment y remédier sur le moment ?

- Analyser le réseau afin de détecter au plus vite les adresses malveillantes et les bloquer sur le pare-feu.
- Isoler les PCs touchés du réseau en les déconnectant.
- Communication aux utilisateurs afin de limiter la casse.

Conclusion :

Pour conclure, on comprend très vite que les utilisateurs sont un maillon vital de la sécurité informatique. Effectivement une communication efficace et claire est indispensable pour réagir au mieux, même si ce n'est pas toujours facile ! Une sensibilisation accrue des utilisateurs afin qu'ils réagissent au mieux lorsqu'un message, panne, action bizarre leurs paraient suspectent est également nécessaire

Une supervision et des contrôles sur le réseau et une connaissance de son environnement est essentiel afin de détecter au plus vite qu'un acteur malveillant agit sur notre structure. Un contrôle sur les interventions physiques sont aussi nécessaires car dans ce cas précis nous ne savons pas ce qu'a fait le jeune qui est venu faire une installation d'imprimante ?