TP : Analyse

Objectif : analyser une demande client, en tirer des conclusions, se documenter et expérimenter une solution dans un environnement dédié. Rien que ça.

Après cet échange, expliquez votre démarche permettant de résoudre le souci évoqué.
Seul indice, c'est malheureusement un acte malveillant qui est en cours sur votre réseau.

Résumé de ce que je sais :
Dans un premier temps il faut trouver l'origine du problème
On constate que Josiane à des pertes de réseaux de plus elle obtient un message « Conflit d'IP détecté », elle est redirigée vers des sites « étranges », le redémarrage ne semble n'avoir aucun changement
Sa collègue à le même problème
Puis tout le monde semble avoir le même problème
Une imprimante en réseau a été installé récemment
Je sais que c'est un acte malveillant qui est en cours sur mon réseau

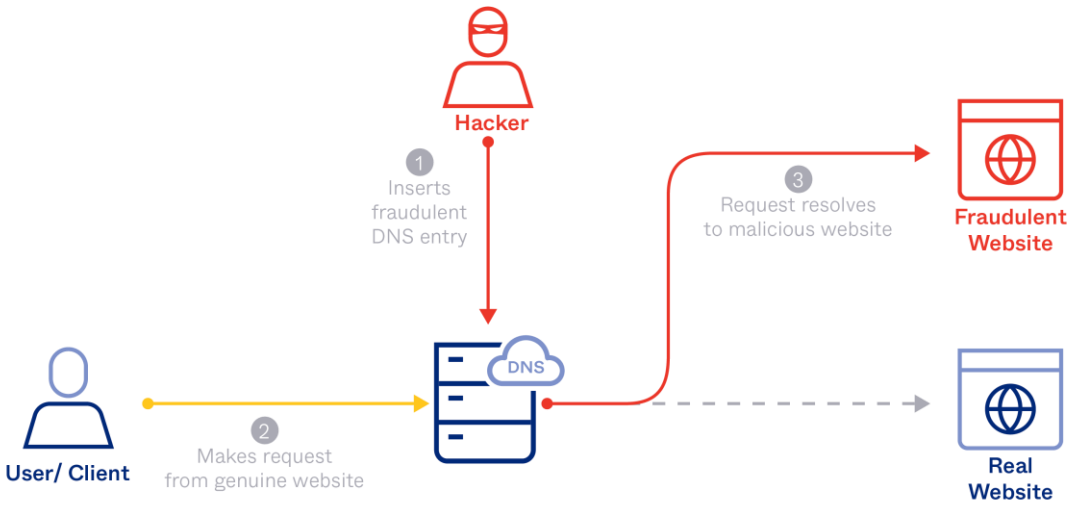
Les premiers gestes :
Je vérifie si la perte de réseau ne touche qu'un service ou tous les services de l'entreprise
S'il touche tous les services → Je redémarre le routeur
Si le redémarrage routeur ne change rien, je vérifie les adresse IP statique ou dynamique et je vérifie la plage DHCP

Diagnostique :
Je sais que les gestes cités ci-dessus ne peuvent pas générer de « site étrange » donc ce n'est pas un problème d'adresse IP statique/Dynamique, ni DHCP
\Suite au diagnostic j'ai appris qu'il y a bien une attaque au niveau du DHCP\

Je sais que ce n'est pas un malware, ni ransomware

Je peux émettre l'hypothèse que ce qui pose un problème c'est l'imprimante (c'est la seule chose qui a changé dans le réseau)

On peut aussi émettre l'hypothèse que l'imprimante est un botnet qui peut faire une attaque par déni de service sur le réseau
Une personne à pus récupérer l'adresse IP de l'imprimante, peut ainsi pénétrer le réseau et ensuite employer la méthode du dns cache poisoning



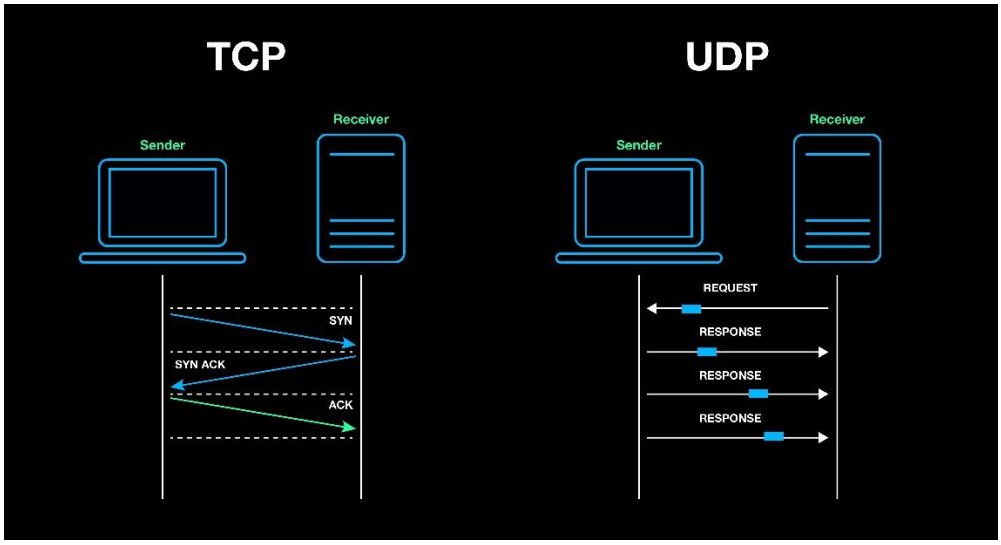
Cette attaque à pour véritable cibles le Serveur de noms DNS, le pirate falsifie la réponse lorsque le résolveur DNS interroge un serveur de nom
De plus les serveurs DNS communiquent avec le protocole UDP ce qui est moins sécurisé car rien ne garantit que la connexion soit ouverte ou que le destinataire soit prêt pour recevoir ce qui le rend plus vulnérable à la falsification

Processus du pirate

Le pirate pénètre le réseau grâce à l'imprimante grâce à son adresse IP, il change les adresses IP cible du résolveur de nom DNS par un autre site sans doute très ressemblant afin de soutirer des informations ou autres (test.com → 10.1.1.50 devient test.com → 10.1.1.51).

Comment y remédier

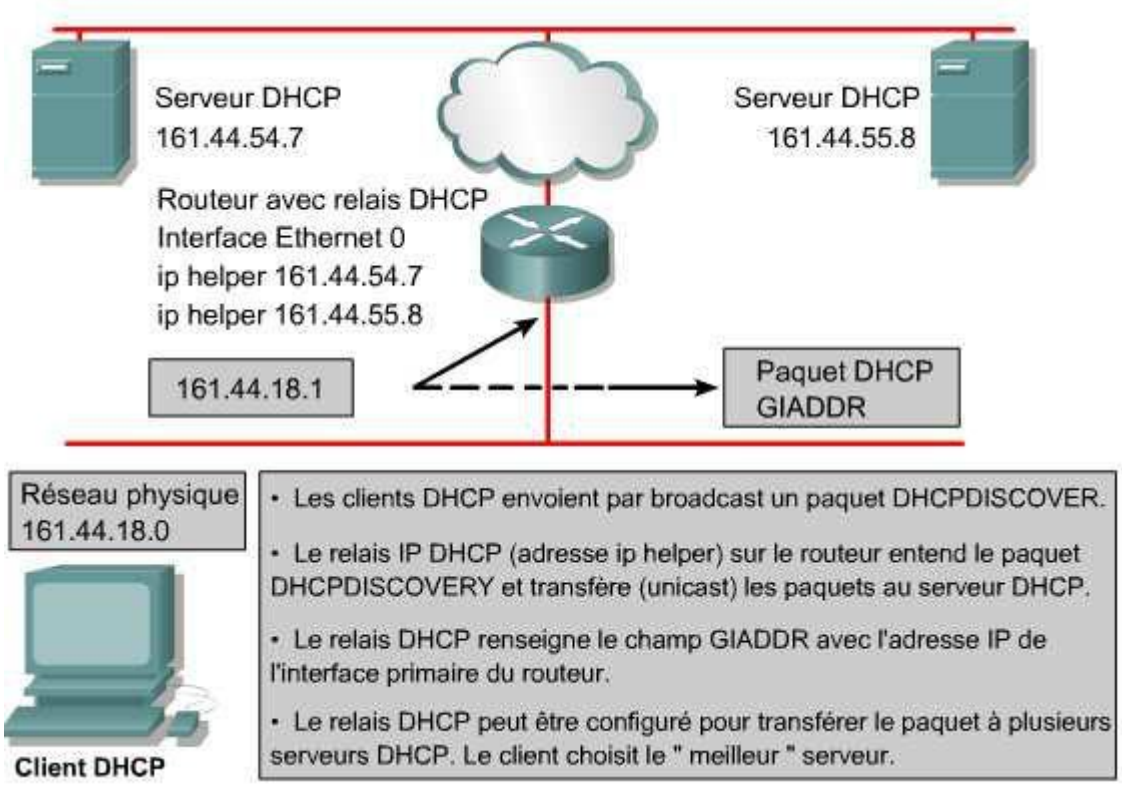
Je sais que cette attaque est rendue possible parce que les serveurs DNS utilisent UDP au lieu de TCP, et parce qu'actuellement il n'y a pas de vérification des informations DNS.



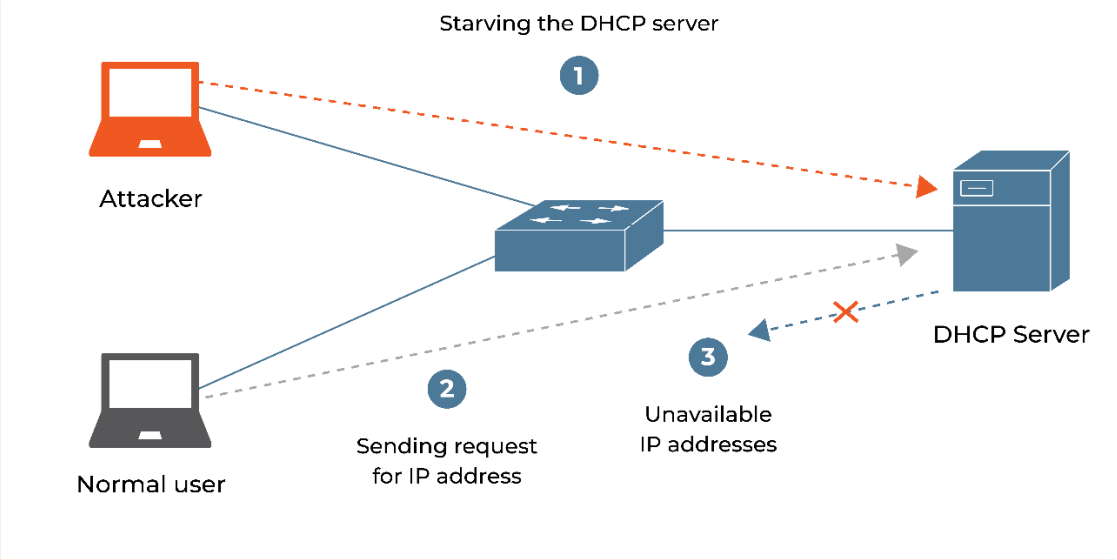
Les résolveurs DNS utilisent maintenant un port aléatoire à chaque fois

Éviter le wifi direct sur les imprimantes d'autant que très souvent le mot de passe reste celui par défaut
Renforcer les sécurités de l'imprimante et du réseau en général
On peut aussi faire une analyse du réseau avec un logiciel tel que Wireshark

Suite du diagnostique
Le DNS cache poisoning explique les fenêtres « étranges » mais n'explique pas le « conflit d'IP détecté » Il peut y avoir une seconde attaque en même temps. Un conflit d'adresse IP unique ne peut venir que d'un appareil, or ici ce sont plusieurs personnes qui sont affectées donc le problème vient sans doute du DHCP, il peut y avoir une attaque par serveur DHCP.
On rappelle le fonctionnement du DHCP



Cette attaque consiste à avoir un serveur DHCP usurpateur qui va entrer en conflit avec le DHCP de l'entreprise et ainsi crée des messages d'erreur



Conclusion

Cette attaque réseau par l'imprimante est assez grave et dangereuse, les répercutions peuvent être désastreuses à cause des fuites d'informations, de ransomware et même l'arrêt complète de l'entreprise. Il est urgent de contrer ce pirate et de mettre en place des dispositifs de protection.