

TP Découverte « Analyse » - Bloc 3 – JOBARD Guillaume – 2023/2024 – Mewo Tiago GOMES

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

Pour commencer je vais décortiquer chaque symptôme données par l'utilisatrice et chaque hypothèse à ce symptôme :

Lenteur d'internet : Si un périphérique a été ajouté au réseau et que les différentes requêtes le traversent, les performances du réseau dépendront des capacités de calcul de ce périphérique. Dans le contexte d'une attaque malveillante, il est possible que ce périphérique analyse, collecte, et transmette les données de navigation à un cybercriminel, ce qui ralentirait considérablement la connexion.

Perte de connexion / Conflit d'IP : Un conflit d'adresses IP peut survenir si le serveur DHCP attribue une adresse IP qui entre en conflit avec la configuration d'un dispositif malveillant sur le réseau. Cela pourrait entraîner des interruptions de connexion.

Résolution temporaire par redémarrage : En redémarrant le PC, celui-ci obtient probablement une adresse IP valide du serveur DHCP légitime. Cependant, si l'ordinateur finit par se connecter au serveur DHCP malveillant, le problème peut réapparaître.

Propagation du problème à d'autres machines : Ce phénomène pourrait indiquer la présence d'un appareil malveillant introduit sur le réseau, capable d'interagir avec plusieurs machines et de répandre le problème.

Redirection vers des sites étrangers : Lorsque l'ordinateur se connecte au mauvais serveur DHCP, ce dernier pourrait lui fournir un DNS compromis, ce qui expliquerait les redirections vers des sites non sécurisés ou étrangers.

Conclusion : Il semble probable que quelqu'un ait introduit un appareil malveillant ou compromis un appareil existant sur le réseau, perturbant ainsi les adresses IP et contrôlant le flux de données au sein du bureau. Cet appareil pourrait fournir des informations erronées aux ordinateurs connectés, avec l'objectif de les détourner. Le but de cette attaque pourrait être de générer un profit par le biais d'une rançon, ou de nuire aux activités de l'entreprise. Les symptômes que vous et votre collègue Corinne avez constatés – perte de connexion, conflits d'IP, redirections vers des sites étrangers – sont cohérents avec cette hypothèse d'une intrusion malveillante.

TP Découverte « Analyse » - Bloc 3 – JOBARD Guillaume – 2023/2024 –
Mewo
Tiago GOMES

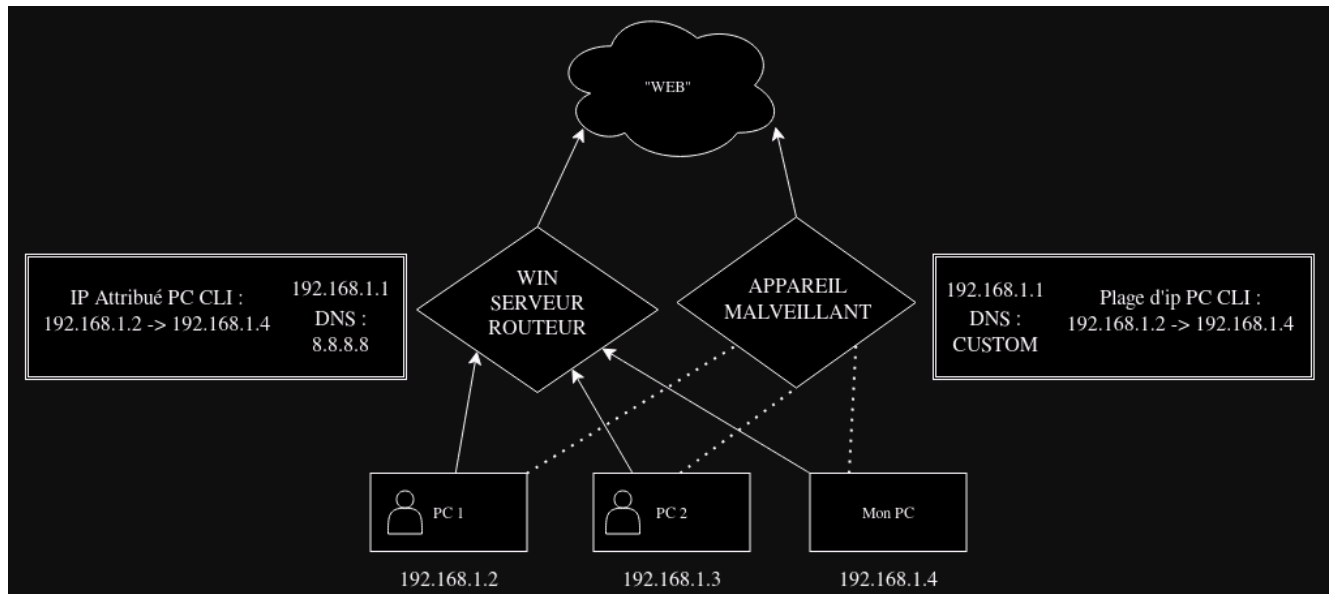


Schéma exemple type de l'attaque par DHCP illégitime

Le comportement des ordinateurs de Josiane et Corinne peut être expliqué par la présence de deux serveurs DHCP sur le réseau. En réseau, lorsqu'un appareil, comme un ordinateur, demande une adresse IP, il envoie une requête DHCP à tous les serveurs disponibles.

L'ordinateur accepte la réponse du serveur qui répond le plus rapidement. Cependant, si deux serveurs DHCP sur le même réseau ont des temps de réponse similaires, les petites variations dans ces temps de réponse peuvent entraîner un comportement erratique, où les ordinateurs passent d'un serveur à l'autre.

C'est ce qui explique que l'attaque peut avoir lieu, ce type d'attaque s'appelle Rogue DHCP qui rentrerait dans la catégorie Man-in-the-middle. Elle consiste à qu'une personne malveillante grâce à un serveur DHCP malveillant détourne le trafic réseaux d'une entreprise vers ses propres serveurs dans le but de récupérer des données où tout simplement stopper l'activité de l'entreprise.

Pour confirmer si une attaque de ce genre se produit dans votre entreprise, il suffit d'utiliser les outils de surveillance réseau disponibles pour vérifier si le port UDP 67 est utilisé par une autre machine que le serveur DHCP légitime. Si une activité suspecte est détectée sur ce port par un appareil non autorisé, il sera nécessaire de localiser cet appareil. Cela peut généralement se faire en identifiant l'adresse MAC de l'appareil suspect et en utilisant l'interface de gestion de vos switches pour tracer son emplacement physique sur le réseau. Selon l'infrastructure en place, cela vous permettra de remonter jusqu'à l'appareil attaquant et de neutraliser la menace.

TP Découverte « Analyse » - Bloc 3 – JOBARD Guillaume – 2023/2024 – Mewo Tiago GOMES

Pour lutter contre cette menace, il est essentiel de maintenir vos serveurs DHCP à jour avec les dernières mises à jour de sécurité. De plus, il est crucial d'être proactif en surveillant régulièrement votre réseau pour détecter tout serveur DHCP non autorisé qui pourrait y être présent. Une vérification périodique permet d'identifier rapidement toute intrusion ou mauvaise configuration susceptible de créer des conflits d'adresses IP ou de compromettre la sécurité du réseau.

Il est également important de sensibiliser les utilisateurs à l'importance de signaler tout comportement suspect sur leur ordinateur, même s'il semble minime. Des symptômes tels que des ralentissements, des déconnexions intermittentes, ou des redirections vers des sites web inhabituels peuvent être des signes d'une configuration réseau compromise. En signalant ces anomalies, les utilisateurs permettent à l'équipe de sécurité d'intervenir rapidement pour vérifier et sécuriser le réseau.

Microsoft a également mis en place un système de détection et de blocage des serveurs DHCP non autorisés, connu sous le nom de **DHCP Snooping**. Cette fonctionnalité, disponible sur les switches compatibles, permet de filtrer et d'autoriser uniquement les réponses DHCP provenant de serveurs légitimes, bloquant ainsi les tentatives d'attaques de serveurs DHCP rogue. L'activation de DHCP Snooping sur vos équipements réseau constitue une couche de protection supplémentaire, réduisant considérablement le risque que des serveurs DHCP non autorisés perturbent le fonctionnement du réseau.

En combinant une surveillance régulière, des mises à jour systématiques, la sensibilisation des utilisateurs, et l'utilisation de technologies comme DHCP Snooping, vous pouvez renforcer la sécurité de votre réseau contre les menaces liées aux serveurs DHCP rogue.

**TP Découverte « Analyse » - Bloc 3 – JOBARD Guillaume – 2023/2024 –
Mewo
Tiago GOMES**

Sources :

<https://support.microsoft.com/fr-fr/topic/r%C3%A9soudre-des-conflits-d-adresses-ip-en-double-sur-un-r%C3%A9seau-dhcp-d68499da-69a3-da3b-4630-d17e502adf50>

https://en.wikipedia.org/wiki/Rogue_DHCP

<https://www.auvik.com/franklyit/blog/rogue-dhcp-server/>

[https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-dhcpe/8f730fca-2fe1-4db0-a454-a4b0dd0d50ba#Appendix A Target 50](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-dhcpe/8f730fca-2fe1-4db0-a454-a4b0dd0d50ba#Appendix_A_Target_50) <50> Section 3.3

Corrigé par ChatGPT