Roméo DERRUAU
Avec l'aide de Chat GPT

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

Ticket d'intervention

Problèmes principaux :

-Ralentissement fréquent

-coupure du réseau

-Conflit d'IP

-redirection vers des sites non affilié à l'entreprise

Analyse du problème :

Selon mon analyse, nous sommes exposés à un spoofing DNS et DHCP, cette conclusion étant basée sur plusieurs éléments. Notamment, la présence du problème sur plusieurs postes simultanément suggère une attaque sur un serveur de l'entreprise, tandis que la redirection vers des sites laisse penser à une manipulation des requêtes vers un second DNS et DHCP.

Comment c'est arrivé :

Début de l'intrusion :

Un individu malveillant aurait peut-être saisi l'occasion de l'installation du photocopieur pour infiltrer un appareil nuisible dans le réseau interne. Ce dispositif aurait ensuite pu commencer à distribuer des réponses DHCP pour attribuer des paramètres réseau erronés aux utilisateurs autorisés.

Mise en place d'un Serveur DHCP Malveillant :

Le pirate met en place un serveur DHCP qui répond plus rapidement que le serveur DHCP officiel. Il est possible de réaliser cela en rapprochant physiquement l'appareil malveillant des cibles ou en inondant le réseau de réponses en utilisant une technique de spamming DHCP.

Manipulating DNS data to redirect users to malicious websites is known as DNS spoofing.

En plus du spoofing DHCP, un serveur DHCP malveillant peut également donner des informations DNS qui dirigent vers un serveur DNS sous le contrôle de l'attaquant. Cela conduit les utilisateurs vers des sites web malveillants ou indésirables lorsqu'ils essaient d'atteindre des domaines légitimes.

Utilisation du réseau :

En ayant la main sur le trafic réseau, le pirate peut récolter des données confidentielles, rediriger les utilisateurs vers des sites de hameçonnage ou insérer du code malveillant.

Diffusion et Consolidation :

Le pirate informatique pourrait ajouter d'autres programmes malveillants aux ordinateurs des utilisateurs pour renforcer sa prise sur le réseau et compliquer la détection.

Résoudre le problème

- Localisation du serveur DHCP malveillant : Employez des outils de surveillance du réseau afin de repérer et de déterminer le serveur DHCP non autorisé.

- Déconnexion immédiate : Après avoir identifié le serveur malveillant, déconnectez-le immédiatement du réseau.

- Vérifiez à nouveau la configuration des serveurs DHCP et DNS pour vous assurer que seuls les serveurs autorisés sont actifs et correctement configurés.

- Effectuer la mise à jour de tous les systèmes et pare-feu en appliquant les correctifs pour se protéger des failles de sécurité connues.

- Établir une surveillance constante : Employez des outils de suivi pour repérer tout comportement suspect à venir.

- Former le personnel : Organiser des sessions de formation pour sensibiliser les employés aux bonnes pratiques de sécurité et à la détection des tentatives d'ingénierie sociale.

- Mise en place de protocoles de signalement : Mettez en place des protocoles bien définis pour que les utilisateurs signalent les anomalies.

Ne pas avoir le problème

Afin de prévenir les incidents futurs, je propose d'installer un switch pour effectuer du snooping. Ce switch se connectera à notre serveur DHCP et lui assignera le statut de port de confiance, redirigeant automatiquement les requêtes vers les ports de confiance. Tout serveur inconnu à notre infrastructure connecté à ce switch sera placé sur un port non fiable, empêchant ainsi la redirection des requêtes.