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

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

DISCLAIMER : Il est rappelé que les techniques et propos tenus en cours restent dans un cadre pédagogique et ne doivent être en aucun cas utilisés à des fins malveillantes. Chaque étudiant assume devant la justice ses actes. Ma responsabilité ne pourra être engagée, vous voilà prévenus.

Voici un échange que vous avez eu avec l'un de vos utilisateurs.

« Mr Abitbol ?

- Oui ?
- Bonjour, ici Josiane de la comptabilité.
- Bonjour !
- Je vous contacte comme prévu dans la charte informatique, je constate de sérieux ralentissements sur ma machine en ce moment.
- Ah ? C'est arrivé du jour au lendemain ?
- Oui, plus ou moins… En fait, parfois tout va bien, parfois je n'ai plus du tout Internet. J'ai des messages du style « Conflit d'IP détecté ». Je garde mon calme, je redémarre et bizarrement ça part puis ça revient. Vous pensez que c'est le petit jeune qui a mis le photocopieur l'autre jour ?
- Attention, pas de conclusion hâtive, malheureusement je n'ai pas pu suivre son intervention elle n'était pas prévue. Votre voisine de travail est impactée aussi avec ce genre de souci ?
- Oui, Corinne c'est pareil depuis quelques jours, presque en même temps que moi… C'est Vraiment impactant, on est en plein dans la compta de fin d'année !
- D'autres comportements bizarres de votre machine ?
- J'ai l'impression que j'ai un peu plus de trucs bizarres, de temps en temps je suis redirigé vers des sites étranges, des fois non… Cela m'énerve ! J'ai peur d'avoir fait une bêtise !
- Mais non, tout va bien. Je vais regarder de mon côté et je vous tiens au courant.
- Merci d'avance et à tantôt !
- Bonne journée ! »

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. Je vous épargne les autres échanges, tout le monde appelle depuis ce matin pour des problèmes similaires. Des indices pourront être donnés mais idéalement vous trouverez seuls le problème.

Vous serez évalué sur ;

- Votre capacité de diagnostic
- Votre capacité à expliquer le processus du pirate
- Votre capacité à y remédier
- Votre capacité à tirer des conclusions sur ce qui s'est passé
- Votre orthographe, votre ponctualité…

DISCLAIMER 2 : Si vous n'avez pas lu le premier disclaimer, lisez-le sinon relisez-le !

Rapport d'intervention

Mme Cheffe 26/07/2024

Suite a un échange avec Josiane de la comptabilité, le service informatique a détecté une anomalie arrivé soudainement sur plusieurs postes avec comme problèmes principaux :

-Ralentissement fréquent

-coupure du réseau

-Conflit d'IP

-redirection vers des sites non affilié à leurs travails

Quel est le problème ?

Nous somme victime d'un spoofing DNS et DHCP, j'en suis arrivé à cette conclusion en me basant sur plusieurs éléments, tout d'abord, le fait que le problème soit sur plusieurs poste et apparait en même temps indique que l'attaque est sur un des serveurs de l'entreprise et la redirection sur des site peut laisser présager que quelqu'un renvoie les requêtes ou il veut et donc que le problème vient d'un second DNS et DHCP

Comment cela a pu arriver ?

Voici un Scénario Possible de l'Attaque

Intrusion Initiale :

Un attaquant a peut-être profité de l'installation du photocopieur pour connecter un appareil malveillant au réseau interne. Cet appareil aurait alors pu commencer à diffuser des réponses DHCP pour assigner des configurations réseau incorrectes aux utilisateurs légitimes.

Déploiement d'un Serveur DHCP Malveillant :

L'attaquant configure un serveur DHCP capable de répondre plus rapidement que le serveur DHCP légitime. Cela peut être fait en plaçant l'appareil malveillant physiquement plus près des cibles ou en utilisant une technique de spamming DHCP pour inonder le réseau de réponses.

DNS Spoofing :

En complément du spoofing DHCP, le serveur DHCP malveillant peut fournir des informations DNS qui pointent vers un serveur DNS contrôlé par l'attaquant. Cela permet de rediriger les utilisateurs vers des sites web malveillants ou non désirés chaque fois qu'ils tentent d'accéder à des domaines légitimes.

Exploitation du Réseau :

Avec le contrôle sur le trafic réseau, l'attaquant peut collecter des informations sensibles, rediriger les utilisateurs vers des pages de phishing ou injecter du code malveillant.

Propagation et Renforcement :

L'attaquant pourrait installer des logiciels malveillants supplémentaires sur les machines des utilisateurs, renforçant ainsi son contrôle sur le réseau et rendant la détection plus difficile.

Comment régler le problème ?

Pour remédier à cette situation, je pense qu'il faut suivre les étapes suivantes

- **Localisation du serveur DHCP malveillant :** Utilisez des outils de surveillance réseau pour détecter et identifier le serveur DHCP non autorisé.
- **Déconnexion immédiate :** Dès identification, déconnectez le serveur malveillant du réseau.
- **Revérifiez la configuration des serveurs DHCP et DNS :** Assurez-vous que seuls les serveurs autorisés sont actifs et correctement configurés.
- **Mise à jour de tous les systèmes et pare-feu :** Appliquez les correctifs et mises à jour aux systèmes d'exploitation et appareils réseau pour se prémunir contre des vulnérabilités connues.
- **Mettre en place une surveillance continue :** Utilisez des outils de monitoring pour détecter toute activité suspecte future.
- **Sensibiliser le personnel :** Mettez en place des formations pour éduquer les employés sur les meilleures pratiques en matière de sécurité et sur la reconnaissance des tentatives d'ingénierie sociale.
- **Procédures de rapport :** Établissez des procédures claires pour le signalement d'anomalies par les utilisateurs.

Comment faire en sorte que le problème ne se reproduise plus ?

Pour que cela ne se reproduise plus, je suggère l'installation d'un switch afin de faire du snooping, ce serveur va se connecter notre DHCP et lui attribuer l'étiquette de port de confiance et va automatiquement rediriger les requêtes dans les ports de confiance, tout serveur inconnu a notre infrastructure se connectera à se switch sera sur un port qui ne sera pas de confiance et donc les requête ne seront pas redirigé

Sources

ChatGPT

https://community.fs.com/fr/article/what-is-dhcp-snooping-and-how-it-works.html

Fait avec l'aide de Victor I aussi