TP découverte « Analyse »

Étape 1 : Diagnostic

Analyse des symptômes :

Josianne nous à appeler pour nous signaler des ralentissements, des interruptions fréquentes de connexion internet, des messages d'erreur et des redirections vers des sites qu'elle n'a pas cherchés.

Tests effectués :

1. **Surveillance du réseau** : Utilisation de Wireshark pour capturer le trafic DHCP et voir s'il y a plusieurs serveurs DHCP.
2. **Inspection des configurations IP** : Examiner les adresses IP, passerelles, et serveurs DNS sur les machines affectées pour repérer des éventuelles incohérences.
3. **Examen de la table ARP** : Vérification des tables ARP sur les postes pour chercher des anomalies dans les adresses MAC.

Résultat du diagnostic :

Les tests ont révélé que les utilisateurs recevaient des paramètres réseau (comme les adresses IP et es serveurs DNS) provenant de deux serveurs DHCP différents, l'un d'eux étant non autorisé. Ce constat confirme une attaque de type **DHCP Spoofing**.

Étape 2 : Explication du processus du pirate

Hypothèse sur le déroulement de l'attaque :

Le pirate, peut-être la personne mentionnée par Josiane qui a manipulé le photocopieur, a introduit un serveur DHCP malveillant sur le réseau local. Mais il peut être aussi une personne interne ayant commis une erreur ou ayant fait cela intentionnellement. Cela peut être aussi une entreprise adverse qui souhaite ralentir la nôtre.

Ce serveur DHCP répond aux requêtes des clients avant le serveur de l'entreprise, fournissant des configurations réseau différentes.

Processus de l'attaque :

1. **Mise en place du serveur DHCP malveillant** : Le pirate a probablement installé un appareil (comme un ordinateur ou un routeur modifié) sur le réseau, configuré pour se comporter comme un serveur DHCP.
2. **Réponse rapide aux requêtes DHCP** : Ce serveur malveillant répond plus rapidement que le serveur DHCP original, distribuant des configurations telles que des adresses IP incorrectes ou des serveurs DNS malveillants.
3. **Exploitation de la configuration modifiée** : Grâce à ces paramètres malveillants, le pirate redirige le trafic des utilisateurs vers des sites contrôlés par lui, intercepte des communications sensibles, ou provoque des conflits d'IP qui perturbent le réseau.

Conséquences :

Les utilisateurs reçoivent des configurations réseau incorrectes, ce qui entraîne des ralentissements, des interruptions de connexion, et des risques accrus de sécurité, comme des redirections vers des sites malveillants.

Étape 3 : Comment y remédier

Mesures immédiates :

1. **Déconnexion du serveur DHCP malveillant** : Identifier et déconnecter immédiatement l'appareil à l'origine du DHCP Spoofing en utilisant des outils comme Wireshark pour traquer les réponses DHCP malveillantes.
2. **Réinitialisation des configurations réseau** : Manuellement, reconfigurer les paramètres réseau des appareils touchés (adresse IP, passerelle par défaut, serveurs DNS) pour rétablir les configurations originales.
3. **Sensibilisation** : Informer immédiatement tous les utilisateurs du réseau de l'attaque en cours, leur demande de redémarrer leurs appareils après avoir isolé le serveur malveillant pour s'assurer qu'ils reçoivent les bonnes configurations DHCP.

Mesures préventives à long terme :

1. **Mise en place du DHCP Snooping** : Configurer les switches pour activer le DHCP Snooping, ce qui bloque tout serveur DHCP non autorisé sur le réseau.
2. **Utilisation de VLANs** : Segmente le réseau en plusieurs VLANs pour réduire la portée d'une attaque de ce type et limiter les interactions entre les différents segments réseau.

3. **Contrôle d'accès et surveillance accrue** : Ajouter des contrôles d'accès réseau plus stricts pour s'assurer que seuls les appareils autorisés peuvent se connecter et agir en tant que serveurs DHCP.
4. **Audits réguliers de sécurité** : Effectue des audits réguliers du réseau pour détecter tout appareil non autorisé ou toute activité suspecte avant qu'une attaque ne se produise. (Possibilité d'ajouter un WAF pour prévenir ce genre de soucis ???)

Étape 4 : Conclusion

L'attaque de **DHCP Spoofing** détectée dans ce cas a perturbé le réseau en introduisant des configurations malveillantes, ce qui a provoqué des conflits d'IP, des redirections vers des sites non sûrs, et des interruptions de service pour les utilisateurs. Grâce à une détection rapide et à la mise en place de contre-mesures immédiates, il est possible de neutraliser l'attaque rapidement.

Pour prévenir de futures attaques similaires, il est essentiel de renforcer les mesures de sécurité du réseau, notamment en activant le DHCP Snooping, en segmentant le réseau, et en surveillant activement l'activité réseau. La sensibilisation des utilisateurs et la maintenance régulière des équipements réseau sont également cruciales pour maintenir un environnement sécurisé et performant.