Cybersécurité des services informatiques

PROFESSEURS : MR JOBARD

TP N°6 : Analyse

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

Plan :

Pour essayer de résoudre ce problème je vais procéder comme suit :

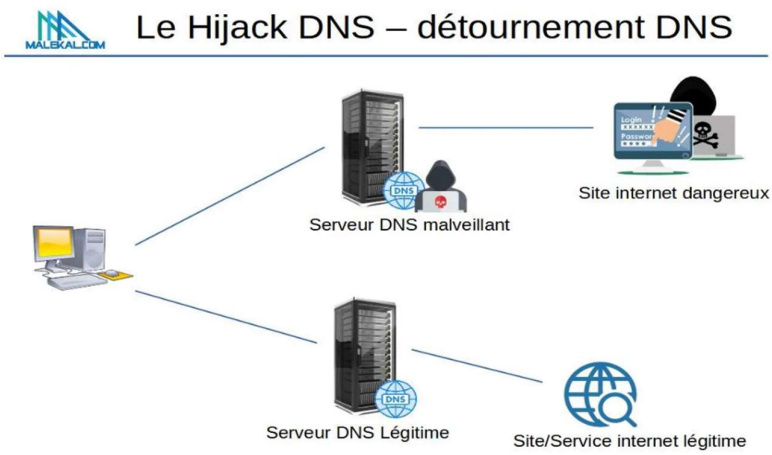
I. **Identifier le ou les Problème(es)**
II. **Faire un diagnostic**
III. **Comprendre le Processus du Pirate**
IV. **Prendre les mesures Correctives**
V. **Faire une Enquête et Conclusion**

I. Identification du Problème

- ✓ D'après notre échange avec l'un des utilisateurs on a observé les Symptômes suivants : Plusieurs utilisateurs rapportent des redirections vers des sites web non légitimes, des conflits d'adresse IP, et des ralentissements réseaux.
- ✓ Pour savoir plus sur le problème j'ai fait une collecte d'Informations supplémentaires : Interroger les utilisateurs affectés pour déterminer le moment où les problèmes ont commencé et notez les sites web auxquels ils sont redirigés. Identifiez les points communs entre les machines affectées.

○ Que peut-être le problème ?

Les informations reçues peuvent être une attaque informatique : **Le Hijack DNS (détournement DNS)** qui est une forme d'attaque informatique très fréquente opérée par les cybercriminels. Les signes courants de détournement de DNS comprennent des pages Web qui se chargent lentement, des publicités contextuelles fréquentes sur des sites Web où il ne devrait pas y en avoir, et des fenêtres contextuelles informant l'utilisateur que sa machine est infectée par des logiciels malveillants. Elle est souvent utilisée pour afficher des publicités, rediriger vers des sites malveillants ou récupérer des données de navigation.



II. Faire un diagnostic

Après avoir collecté toutes les informations nécessaires pour résoudre ce problème, on va commencer notre diagnostic. En commençant par une :

- ✓ Vérification des Paramètres DNS :

  D'abord sur les Machines Utilisateurs : je vérifie les configurations DNS des machines affectées via ipconfig /all (Windows) ou cat /etc/resolv.conf (Linux), Recherche des serveurs DNS non autorisés.

  Ensuite au niveau des Routeur et Switches : j'accède à l'interface de gestion des routeur/switch et vérifie les adresses DNS configurées, puis les Compares avec les adresses DNS officielles de l'entreprise.
- ✓ Vérification des Logs : j'analyse les journaux des routeurs, switches, et serveurs DHCP pour identifier des anomalies ou des accès non autorisés.

III. Comprendre le Processus du Pirate

- ✓ Accès Initial : Le pirate a probablement obtenu un accès au réseau via une méthode telle que le phishing, une vulnérabilité non corrigée, ou un accès physique non autorisé à l'équipement réseau.
- ✓ Modification des Paramètres DNS : Une fois à l'intérieur du réseau, l'attaquant a modifié les configurations DNS sur le routeur ou les machines des utilisateurs pour rediriger le trafic vers des serveurs DNS malveillants sous son contrôle.
- ✓ Résultat : Les utilisateurs sont redirigés vers des sites de phishing, des sites infectés par des malwares, ou des pages de publicité, ce qui peut entraîner le vol de données ou des infections supplémentaires.

IV. Prendre les mesures Correctives

Pour prendre les mesures correctives on va :

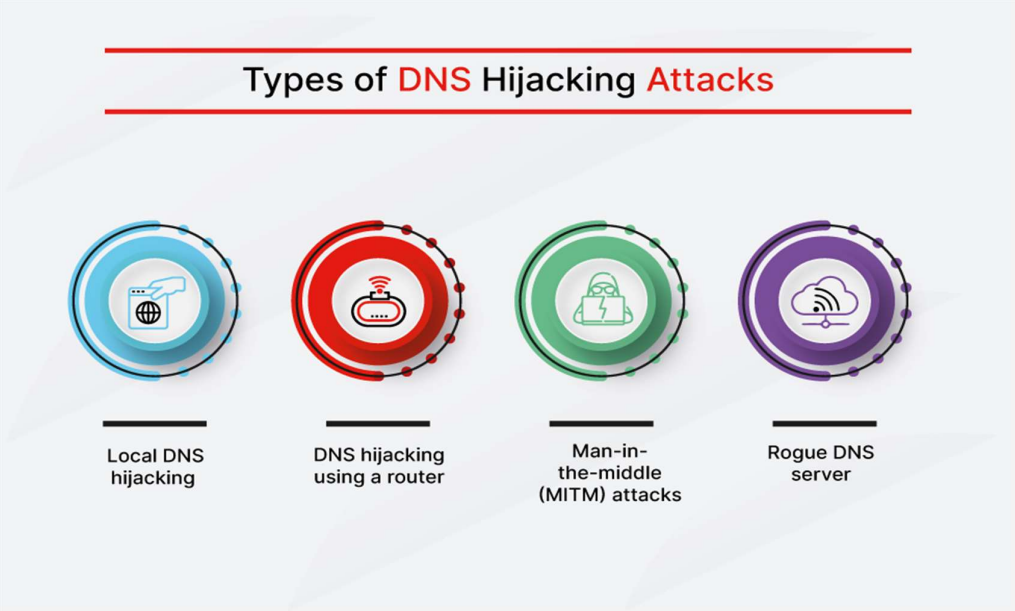
- ✓ Restaurer les Paramètres DNS Légitimes :
  - Sur les Machines Utilisateurs : Corriger manuellement les paramètres DNS pour chaque machine affectée en les rétablissant aux valeurs correctes.
  - Sur le Routeur : Rétablir les paramètres DNS légitimes dans l'interface de gestion du routeur. Désactiver la gestion à distance si elle n'est pas nécessaire.
- ✓ Modifier les Identifiants d'Accès : Changer tous les mots de passe administrateur pour le routeur et autres équipements réseau. Utilisez des mots de passe complexes et uniques.
- ✓ Mettre à Jour le Firmware : Mettre à jour le firmware du routeur et autres équipements pour corriger les vulnérabilités connues.
- ✓ Scan Antivirus/Anti-malware : Effectuer un scan complet des machines affectées pour détecter et éliminer tout malware présent.

V. Enquête et Conclusion

Après avoir résoudre le problème, on va essayer de comprendre comment l'attaquant a pu obtenir un accès initial (ex. : faiblesse dans la sécurité du routeur, phishing, etc.), réaliser aussi un audit complet de la sécurité du réseau pour identifier d'autres faiblesses potentielles. Inclue la vérification des configurations, des permissions, et des accès réseau et faire mise en Place de Contremesures :

Éduquer les utilisateurs sur les dangers du phishing et les incitez à signaler toute anomalie immédiatement.

Implémenter des solutions de sécurité additionnelles comme des pares-feux, des systèmes de détection d'intrusion (IDS), et la segmentation du réseau pour limiter la propagation d'éventuelles infections.



Conclusion

Ce TP m’a permet non seulement d'acquérir des compétences en diagnostic et en remédiation d'incidents de sécurité, mais aussi de renforcer ma capacité à analyser et à documenter des incidents complexes, tout en appliquant des solutions appropriées.