DNS - Transfert de Zone

Description

Le transfert de zone DNS est une fonctionnalité du protocole DNS qui permet la mise à jour dynamique d'un serveur DNS secondaire en synchronisant les informations d'un serveur DNS primaire.

Un attaquant a la possibilité d'exploiter une mauvaise configuration du serveur DNS qui implémenterait cette fonctionnalité. En cas de succès, l'attaquant obtient alors des informations précieuses sur la topologie de la cible, y compris des informations sur des serveurs particuliers, leur rôles dans la structure et éventuellement des informations sur les systèmes d'exploitation fonctionnant sur le réseau.

Prérequis d'exploitation

Pour exploiter cette vulnérabilité, il est nécessaire d'avoir accès à un serveur DNS qui est configuré de manière à accepter les transferts de zone.

Connaissances nécessaires

- Connaissance de base des systèmes de noms de domaine et de la structure des enregistrements DNS ;
- Connaissance des configurations et des fonctionnalités de transfert de zone.

Outils nécessaires

- Outil capable d'interagir avec le serveur DNS ou un utilitaire de ligne de commande tel que nslookup ou dig.

Flux d'exécution

Explorer

Rechercher des serveurs DNS vulnérables en utilisant des outils de découverte de réseau tels que nmap.

Vérifier les configurations de transfert de zone pour identifier les serveurs qui seraient potentiellement vulnérables.

Expérimenter

Tester les limites de la fonctionnalité de transfert de zone en utilisant des commandes de transfert de zone pour mettre à jour des enregistrements DNS. Vérifier les impacts de ces modifications sur les clients DNS.

Exploiter

Conséquences potentielles

Une exploitation réussie de ce type de vulnérabilité peut permettre :

- Une attaque de type DoS/DDoS qui rendra inaccessible un site web ou une application en empêchant les utilisateurs de résoudre les noms de domaine correspondants ;
- La redirection des utilisateurs vers des sites frauduleux.

Contres-mesures

Les contre-mesures suivantes peuvent être mises en œuvre :

- **Utilisation de protocoles de sécurité DNS robustes tels que DNSSEC (Domain Name System Security Extensions) et DNS-over-HTTPS (DoH) peut aider à protéger les systèmes contre ce type d'attaque.** Ces protocoles permettent de garantir l'intégrité et l'authenticité des enregistrements DNS, et de sécuriser les communications entre les clients et les serveurs DNS.
- **Utilisation de la liste noire DNS (DNSBL) qui contient une liste de serveurs DNS malveillants**. Les administrateurs de système peuvent configurer leurs serveurs DNS pour bloquer les requêtes provenant de ces serveurs. Il existe des listes noires DNS publiques et gratuites, mais il est important de s'assurer que ces listes sont mises à jour régulièrement.

Comment cela fonctionne ?

Le scénario suivant peut être joué via l'exploitation de cette vulnérabilité :

- **Attaque par cache poisoning** : un attaquant peut envoyer des requêtes malveillantes aux serveurs DNS pour mettre à jour leurs enregistrements avec de fausses informations, redirigeant les utilisateurs vers des sites malveillants ou capturant des informations sensibles.

Exemple 1

Il existe plusieurs façons de configurer un serveur DNS pour permettre les transferts de zone, mais voici un exemple de configuration vulnérable qui pourrait être exploitée :

<ode> zone “example.com” {

```
type master;
file "example.com.zone";
allow-transfer { any; };
```

}; </code>

Cette configuration indique que le serveur DNS est le serveur maître pour la zone **example.com** et que les fichiers de zone sont stockés dans le fichier **example.com.zone**. La ligne **allow-transfer {any ;};** indique que n'importe quel serveur DNS peut effectuer un transfert de zone pour cette zone.

Cette configuration est vulnérable car elle permet à n'importe quel serveur DNS de récupérer les données de la zone **example.com**, y compris les enregistrements de noms et les adresses IP associées. Si un attaquant parvient à configurer un serveur DNS malveillant pour effectuer un transfert de zone avec ce serveur, il pourrait alors obtenir des informations sensibles sur la topologie réseau de la cible.

Exemple 2

Voici un exemple permettant l'exploitation des transferts de zone DNS avec la commande dig :

```
$ dig axfr @<DNS_SERVER> <DOMAIN>
example.com.        86400        IN        SOA        ns0.wexample.com. hostmaster.example.com.
2013030122 43200 7200 1209600 3600
example.com.        3600        IN        A        208.80.152.201
example.com.        86400        IN        NS        ns0.example.com.
example.com.        86400        IN        NS        ns1.example.com.
example.com.        86400        IN        NS        ns2.example.com.
example.com.        3600        IN        MX        50 preprod2981.dev.example.com.
```

Dans cette commande DNS_SERVER est l'adresse IP du serveur DNS à attaquer et DOMAIN est le nom de domaine dont la zone doit être transférée. Si le serveur DNS autorise les transferts de zone non autorisés, cette commande permettra à un attaquant de récupérer toutes les informations de la zone DNS, y compris les noms d'hôtes, les adresses IP et les enregistrements de ressources.

References

URL :

- https://digi.ninja/projects/zonetransferme.php
- https://lig-membres.imag.fr/sicard/tpRES/DNSRICM2-TP.pdf

Retour fiches vulnérabilités

- Cyber fiches vulnérabilités