Projet de fin d'étude: Maquettage d'une attaque par empoisonnement de cache sur un serveur DNS

Institut Mines-Télécom

Auteurs

Didier Trécherel
Carole Boyer

Partenaires

Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)

OBJECTIFS DU PROJET

- Comprendre les mécanismes de fonctionnement du protocole DNS
- Etablir un état de l'art des attaques existantes sur l'infrastructure DNS
- Réaliser le maquettage d'une attaque par empoisonnement de cache combinant le principe de l'attaque de Kaminsky et la méthode de protection contre les dénis de service du *Response Rate Limiting* (RRL)

Etat de l'art des attaques sur DNS

- Attaque par empoisonnement de cache
  - **Définition**: introduction volontaire par un attaquant de faux enregistrements dans le cache d'un serveur DNS
  - **Attaque par empoisonnement de cache simple:** permet à l'attaquant d'usurper un nom de domaine
  - **Attaque par empoisonnement de cache de Dan Kaminsky**: permet à l'attaquant de rediriger toutes les requêtes DNS concernant une zone légitime vers son serveur de nom.

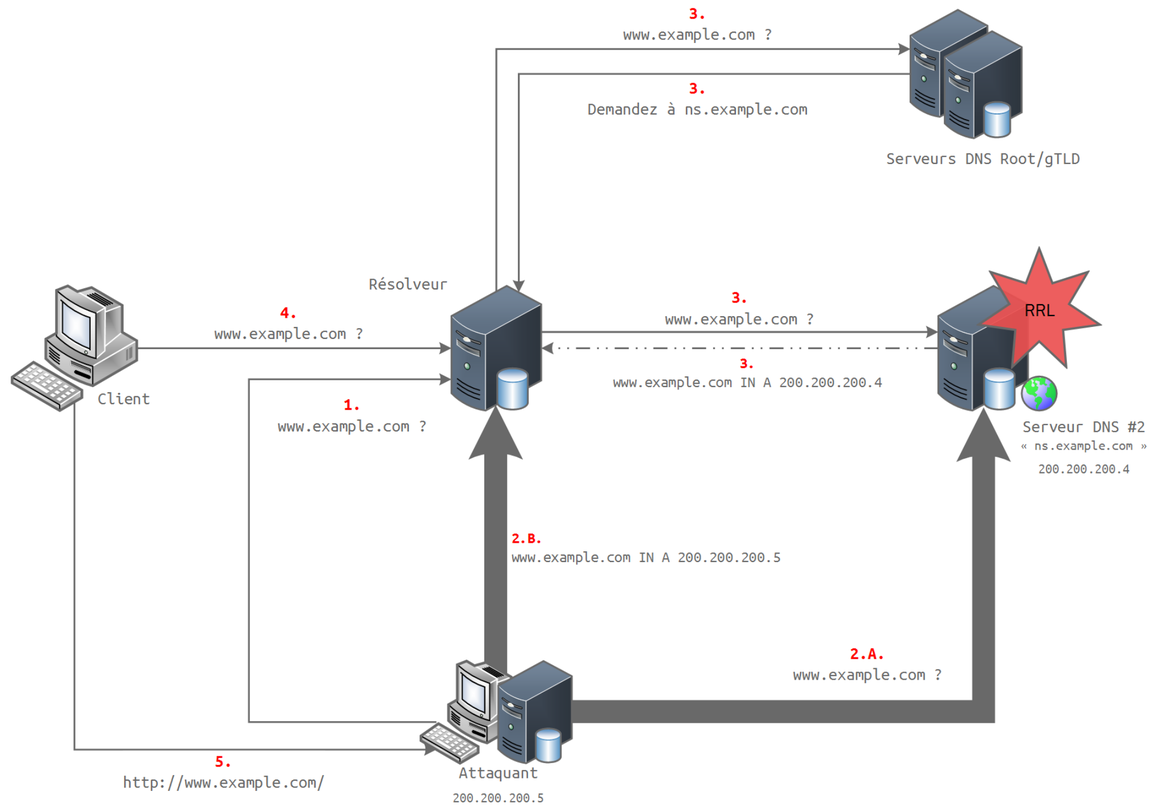
- Attaque par déni de service distribué par réflexion et amplification
  - Exploite le fait qu'une requête DNS de petite taille peut entrainer la génération d'une réponse beaucoup plus grosse
  - L'attaquant va envoyer une multitude de requêtes vers plusieurs serveurs DNS (réflecteurs) en se faisant passer pour la victime (usurpation d'adresse IP)
  - Les serveurs vont alors répondre à la victime, l'innondant de paquets DNS de taille importante

Maquettage de l'attaque de Kaminsky

- 1ère étape: Configuration d'une infrastructure DNS fonctionnelle à l'aide de BIND9
- 2ème étape: Réalisation de l'attaque par empoisonnement de cache simple dans l'environnement virtuel.

  Utilisation du langage python et de l'utilitaire Scapy pour l'écriture des scripts permettant la génération des paquets DNS
- 3ème étape: Réalisation de l'attaque de Kaminsky combiné à RRL

  Utilisation du langage C et de sockets pour la génération des paquets



Projets de fin d'étude de la VAP SSR

Janvier 2015

Contact didier.trecherel@telecom-sudparis.eu

Site web