SYNACKTIV
DIGITAL SECURITY

TNS bit flip attack

SSTIC 2013

Présenté 24/06/2013
Pour SSTIC
Par Nicolas Collignon

Challenge

- ***Man-In-The-Middle* sur flux TNS**

  ARP poisonning, TNS RAC poisoning, LLMNR, NBT-NS ...

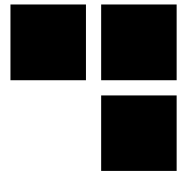
  - Pas de protection de la couche transport par défaut
  - Oracle 11g
  - *challenge-response* lent à brute-forcer

- **Objectifs :**
  - Injection de requêtes SQL arbitraires dans le flux TNS
  - Sans perturber le client
  - Ne pas provoquer une corruption mémoire dans Oracle qui va faire planter la prod (*incoming 0day...*)

Problématiques

- **Les difficultés :**
  - Protocole non documenté
  - Presque aucun outil / dissecteur TNS
  - Pas de structures claires de type TLV
  - Re-synchronisation des numéros de séquence
  - Seulement quelques heures pour dev l'outil, malheureusement nous ne sommes pas à l'ANSSI :)

Houracle : proxy TNS



- **Le résultat :**
  - *Hijacking* du flux TNS
  - Injection à la volée de requêtes SQL arbitraires

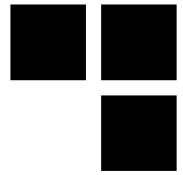
    client Oracle → Houracle (1522/tcp) → serveur Oracle (1521/tcp)

- **Évolutions futures :**
  - Interception des commandes *logout* pour maintenir des sessions dans le proxy
  - Récupération du mot de passe en clair à partir des *hashs* et du *challenge-response*
  - Faire du code propre

Comment se protéger

- **Commander un audit Synacktiv :)**

Houracle : démo



- **Récupération des hashs spare4 en injectant une requête SQL dans une connexion DBA.**

AVEZ-VOUS DES QUESTIONS ?

MERCI DE VOTRE ATTENTION,

SYNACKTIV
DIGITAL SECURITY