Journée de Formation Technique du 1 Octobre 2013

Les attaques de réseau, cas de figures
Prise en compte par l'expert

Dominique VAN EGROO
dve@fintoo.fr
Tél : 06 27 14 39 91

Sommaire

- Les grandes techniques d'attaque
- Techniques utilisées
- Tests d'intrusion : les étapes
- Les sources de preuve
- L'intervention de l'expert
- Attaque des applications (exemples)
- Rechercher où ?

Les grands types d'attaque

- Attaques passives
  - capture du trafic (analyse, déchiffrement,..)
- Attaques actives
  - exploitation de vulnérabilités
  - contournement des mécanismes de sécurité
  - introduction de codes malicieux
- Attaques internes
- Attaques distribuées
  - DDoS
- Social engineering – Phishing

Techniques utilisées

- Attaques sur les mots de passe
  - Brute force
  - Mots de passe par défaut
- Exploitation de vulnérabilités
  - Scanning de ports / vulnérabilités
  - SQL Injection
  - Buffer Overflow, exploit
- Chevaux de troie
- Hijacking
- Spoofing
- Phishing
- Social engineering

Tests d'intrusion les étapes

- 2 étapes principales
- 1ère étape
  - Recherche d'informations
  - Cartographie du réseau
- 2ème étape
  - Exploitation des vulnérabilités
- Puis bouclage sur étape 1

Les sources de preuve

- Fichiers d'audit
- Contenu des disques durs
- Traffic réseau
- IDS (HIDS, NISD) - Firewall
- Contenu des bases de données
- Contenu de la mémoire
- Connexions réseau
- Toute trace laissée…

Attention :

- Date / heure du système
- Dépend de l'incident et du cas

L'intervention de l'expert

- L'identification de l'incident
  - Incident identifié / non identifié
  - Constat/analyse ou recherche ?
  - Impact sur la conservation des preuves
- Analyse des traces
  - Démonstration de l'intention
  - Pas de conclusion hative (requête GET/POST)
- Capture et conservation de la preuve
  - Le système est-il compromis ?
    - Conservation pour analyse ultèrieure
  - Adaptation selon les cas

Attaque des applications (exemples)

- SQL injection
  - http://www.site.com/identification.php?id=dom&pass=pwd
  - http://www.site.com/identification.php?iddom&pass=%
- Contournement de l'authentification
  - http://www.site.com/cmd.php?id=1241&cle=12AEF584A54DA01247
  - http://www.site.com/cmd.php?id=1242&cle=12AEF584A54DA01247
  - http://www.site.com/cmd.php?id=1243&cle=12AEF584A54DA01247
- Quelles traces dans quels fichiers ?

Rechercher où principalement ?

- Tentatives d'intrusion
  - Scanning de ports
    - IDS, Firewall
  - Attaque par mots de passe
    - Logs serveur Web, Logs applicatifs

- Accès non autorisés à une application Web / Attaque par injection SQL
  - Logs serveur Web, Logs applicatifs
  - IDS, Proxy Web

Rechercher où ?

- Attaque par chevaux de troie / Intrusion dans un système
  - Logs serveur Web, Logs applicatifs
  - Contenu des disques durs
  - Contenu de la mémoire
  - Connexions réseau
  - Traffic réseau
  - IDS
  - Pièces attachées des mails

- Bien comprendre la typologie de l'attaque pour identifier ou rechercher et quoi rechercher
  - Connaitre les faiblesses / vulnérabilités de l'environnement

Merci de votre attention

Dominique VAN EGROO
dve@fintoo.fr
Tél : 06 27 14 39 91