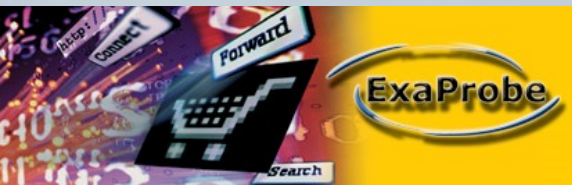
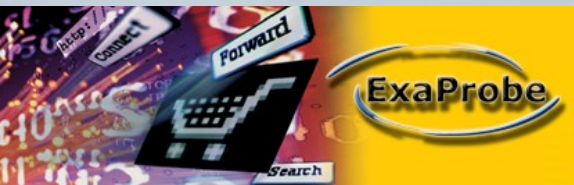
Recherche de vulnérabilités, localisation et faux négatifs



Plan

- [1] Introduction
- [2] Explication de termes
- [3] Réalisation des tests
- [4] Interprétation des résultats
- [5] Conclusion



Introduction

- Papier publié en Avril 2003
- Démystifie la recherche de vulnérabilités
- Evoque une nouvelle famille de faux négatifs
- Axé sur les tests intrusifs
- Concerne les environnements non anglophones

Explication de termes (1/3)

- Scanners de vulnérabilités
  - Exemples de produits
    - ISS, Nessus, outils spécifiques
  - Exemples d'utilisateurs
    - Pen-testers, administrateurs réseaux, ...
  - Résultats considérés comme fiables
    - Manque de temps, de compétences

Explication de termes (2/3)

- Localisation
  - Traduction
    - Menus, bannières, messages d'erreur
  - Principalement dans le monde commercial
    - SQL Server, Windows, ...
  - Ne peut que se développer
    - Plus « user-friendly »

Explication de termes (3/3)

- Faux négatifs
  - Non détection d'une vulnérabilité présente
  - Difficile à détecter
  - Peut mener à :
    - Un faux sens de sécurité
    - Une brèche de sécurité (selon l'« exploit »)
  - *« Celui qui sait qu'il ne sait pas en sait plus que celui qui ne sait pas qu'il ne sait rien »*

Réalisation des tests (1/3)

- Démonstration du problème
  - SQL Server et les mots de passe nuls
    - Localisé, fortement déployé
    - Présence de failles connues (CAN-2000-1209)
  - Autres pistes possibles
    - unicoder.pl => recherche de « Directory of »
    - Compte super-utilisateur Windows

Réalisation des tests (2/3)

- « Modus operandi »
  - Installation par défaut MS-SQL8/Win2K SP3
  - Le mot de passe du compte « sa » est nul
  - 4 langues installées (FR, US, DE, JP)
  - Test de chacun des outils sur la version US
  - Si détection OK => test sur les autres versions

Réalisation des tests (3/3)

- Panel d'outils de recherche de vulnérabilités
  - Outils testés
    - ISS Database Scanner/Vigilante NX/Retina
    - Nessus
    - Sensepost senseql/Spida Scanner
  - Outils non testés ou non testables
    - Symantec NetRecon/NetIQ/GFI LanGuard/...

Résultats et interprétations (1/3)

Outil	Version US	Autres versions
ISS Database Scanner		
Vigilante Secure NX		
eEye Retina Scanner		
eEye Spida Scanner		
Nessus		
Sensepost senseql		

Résultats et interprétations (1/3)

Outil	Version US	Autres versions
ISS Database Scanner	OK	
Vigilante Secure NX	OK	
eEye Retina Scanner	OK	
eEye Spida Scanner	OK	
Nessus	OK	
Sensepost senseql	OK	

Résultats et interprétations (1/3)

Outil	Version US	Autres versions
ISS Database Scanner	OK	OK
Vigilante Secure NX	OK	Faux négatif
eEye Retina Scanner	OK	Faux négatif
eEye Spida Scanner	OK	Faux négatif
Nessus	OK	Faux négatif
Sensepost senseql	OK	Faux négatif

Résultats et interprétations (2/3)

- ~ 80% de faux négatifs

- Anciennes versions d'eEye Retina Scanner
  - Détection des versions localisées
- SQLPoke, vers Spida
  - Compromet n'importe quelle version
  - Opération réalisée au niveau applicatif

Résultats et interprétations (3/3)

- Correction du problème
  - Nessus/senseql => patchs fournis
  - eEye => correction effectuée par l'éditeur
  - Vigilante => WIP côté éditeur

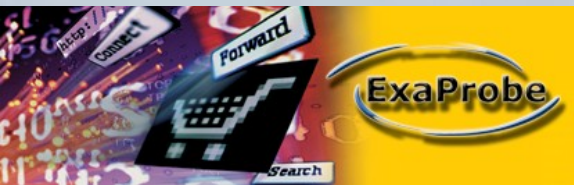
Conclusion (1/2)

- Travail côté éditeurs d'outils de VA
  - Prise en compte de la localisation lors de la génération des signatures
  - Utilisation de tests réalisés au niveau applicatif

Conclusion (2/2)

- Travail côté auditeurs/pen-testers
  - Doivent fournir leur valeur ajoutée au niveau de l'élimination des faux positifs et faux négatifs
  - Utilisation de plusieurs outils en vue de recouper les résultats
  - Parfaite maîtrise des outils employés (disponibilité du code source ?)

Des questions ?



Merci ...