Licence 3

Système d'Information

Les IDS
Systèmes de détection d'intrusions

Dr Souheila Bouam

Maître de conférences
Université Batna-2
Département Informatique

sz,bouam@gmail.com

Plan

- Définition intrusion
- Systèmes de détection d'intrusion
- Objectifs de la sécurité
- Services de sécurité
- Mécanismes de défense
- Attaques existantes
- Notions supplémentaires de sécurité

Définition Intrusion

- **qu'est ce qu'une intrusion ?**
  - ✓ **Une action qui vise à compromettre:**
    - **la confidentialité**
    - **l'intégrité**
    - **la disponibilité**
    - **La non-répudiation**
  - ✓ **Cette action peut :**
    - **avoir réussi**
    - **avoir échoué**
    - **être en cours**
    - **être une simple phase préparatoire**
  - ✓ **Le système d'information visé peut être :**
    - **un réseau**
    - **une machine, un système d'exploitation**
    - **une application**

Système de détection d'intrusion IDS

- **Rôle d'un IDS**
  - ✓ Détection des attaques
  - ✓ Détection des intrusions
  - ✓ Aide à l'administration
  - ✓ Établissement de statistiques
  - ✓ Mettre en avant les menaces et les vulnérabilités
- **comment fonctionne un IDS?**
  - ✓ Surveiller les évènements nouveaux dans le système
  - ✓ Analyser ces évènements
  - ✓ Filtrer les actions suspectes
  - ✓ Les signaler au système

Notions de base

- **Faux positif**
  - ✓ Fausse alerte mise par l'IDS
- **Faux négatif**
  - ✓ Attaque non repérée par l'IDS

- **Evasion**
  - ✓ Technique utilisée pour masquer une attaque pour que l'IDS ne puisse la détecter
- **Sonde**
  - ✓ Composante de l'architecture de l'IDS qui collecte les informations

  (il peut y avoir une ou plusieurs sondes)

Types d'IDS

- **NIDS (Network Intrusion Detection Systems)**
  - ✓ **Détectent les intrusions sur le réseau**
- **HIDS (Host Intrusion Detection Systems)**
  - ✓ **Détectent les intrusions au niveau d'un seul nœud ou hôte**
- **Hybrid IDS**
  - ✓ **Détectent aussi bien les intrusions sur le réseau qu'au niveau hôte**
- **IPS (Intrusion Prevention Systems)**
  - ✓ **Ils essayent de prévoir les intrusions avant qu'elles ne puissent arriver**

Types d'IDS (2)

- **KIDS/KIPS (Kernel Intrusion Detection/Prevention Systems)**
  - ✓ **Détectent les intrusions au niveau du noyau, càd le système d'exploitation lui-même**
- **Les pare feu (Firewall)**
  - ✓ **Ne se contentent pas de détecter, mais de bloquer et éliminer les intrusions**
- **Honey pots (les pots de miel)**
  - ✓ **Des pièges pour découvrir s'il y a des menaces au système**

Conclusion

- Les IDS ne sont pas parfaits et peuvent se tromper
- Les IDS restent un bon moyen d'aide à la sécurité
- Utiliser un IDS n'est pas recommandable dans tous les cas, car ils consomment des ressources non négligeables

FIN