



BTS SIO

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

[TP] Synthèse- Gestion des utilisateurs :
Analyse des évènements de connexion
(AD & RDP)

Candidat : Alenzo Wauters

Spécialité : SISR (Solutions d'infrastructure, systèmes et réseaux)

Réalisation professionnelle : Audit de sécurité des accès et analyse des journaux d'événements Windows Server.

Table des matières

1. Tentative (Génération du log)	2
2. Analyse (Collecte & Filtrage)	2
3. Diagnostic (Interprétation)	2
4. Remédiation (Action corrective).....	3
5. Boucle de surveillance continue.....	3
6. Conclusion	3

1. Tentative (Génération du log)

- Action utilisateur ou automatisée
 - Connexion à une session
 - Connexion distante (RDP)
 - Changement de mot de passe
- Serveur concerné
 - SRV.SISR.LOCAL
- Journal Windows
 - Journal **Sécurité**
- IDs d'événements
 - **4624** : Connexion réussie
 - **4625** : Échec de connexion
 - **4723** : Changement MDP utilisateur
 - **4724** : Reset MDP par admin

Objectif : tracer toute tentative d'accès

2. Analyse (Collecte & Filtrage)

- Outil utilisé
 - Script PowerShell
 - Audit-Connexions.ps1
- Actions réalisées
 - Lecture des journaux Sécurité
 - Filtrage des événements critiques
 - Extraction des données utiles
- Données analysées
 - Nom d'utilisateur
 - Date / heure
 - Adresse IP
 - Type de connexion

Objectif : automatiser la supervision

3. Diagnostic (Interprétation)

- Identification de la source
 - IP locale
 - IP distante

- Type de connexion
 - **Type 2** : Connexion locale
 - **Type 3** : Connexion réseau
 - **Type 10** : Bureau à distance (RDP)
- Analyse des erreurs
 - Code erreur : 0xc000006d
 - Mot de passe incorrect
 - Compte inexistant ou bloqué
- Évaluation du risque
 - Erreur humaine
 - Tentative de brute force
 - Accès non autorisé

Objectif : distinguer incident / attaque

4. Remédiation (Action corrective)

- Cas normal
 - Connexion légitime validée
- Cas suspect
 - Blocage de l'IP (pare-feu Windows)
 - Réinitialisation du mot de passe
 - Désactivation temporaire du compte
- Alerte
 - Notification administrateur
 - Journalisation de l'incident

Objectif : sécuriser et réagir rapidement

5. Boucle de surveillance continue

- Surveillance permanente
- Amélioration des scripts
- Adaptation des règles de sécurité

Prévention + réaction

6. Conclusion

Ce cycle permet d'assurer la traçabilité, l'analyse et la sécurisation des accès au système, en automatisant la détection des événements critiques et en appliquant des actions correctives adaptées.