Incident Cyber

1. Résumé exécutif

Le 20 décembre 2024 à 07:13:12, une intrusion a été détectée sur un serveur critique, le contrôleur de domaine. L'incident, identifié comme une tentative de repérage sans action malveillante confirmée, n'a entraîné aucun impact sur la production. Des mesures immédiates et proactives ont été prises pour sécuriser l'environnement, incluant la désactivation des accès VPN, l'analyse des journaux, le signalement à CERT-FR, et le renforcement des mécanismes d'authentification. Cette documentation détaille le contexte, les mesures techniques mises en œuvre, ainsi que les actions personnelles entreprises dans la gestion de l'incident.

2. Contexte de l'incident

2.1. Chronologie et description

- **Date et heure de l'intrusion** : 20 décembre 2024 à 07:13:12
- **Cible** : Contrôleur de domaine, serveur critique de l'infrastructure
- **Nature de l'incident** : Tentative de repérage sans action malveillante identifiée
- **Impact** : Aucun impact sur la production ou les services opérationnels

2.2. Première réponse

- **Action immédiate** : Désactivation des accès distants VPN SSL liés au LDAP pour limiter les risques d'exploitation supplémentaire.

3. Mesures techniques mises en œuvre

Pour contenir l'incident, analyser ses causes et renforcer la sécurité, les actions suivantes ont été entreprises :

1. **Analyse des journaux** :
    - Extraction et analyse des journaux du serveur compromis (événements système via l'observateur d'événements).
    - Analyse des journaux VPN SSL du pare-feu pour identifier les tentatives d'accès non autorisées.
2. **Signalement** :
    - Notification à CERT-FR avec transmission des informations clés :
        - Horaire précis de l'intrusion : 07:13:12, 20 décembre 2024
        - Adresse IP de l'attaquant
3. **Renforcement de la sécurité du domaine** :

    - Réinitialisation de tous les mots de passe des comptes administrateurs du domaine.
    - Désactivation des comptes obsolètes dans l'Active Directory pour réduire la surface d'attaque.
4. **Déploiement de solutions de détection** :
    - Installation de licences EDR (Endpoint Detection and Response) sur les systèmes critiques pour une surveillance avancée des menaces.
5. **Analyse approfondie** :
    - Exécution de l'outil Oradad sur le contrôleur de domaine pour collecter des données forensiques.
    - Transmission des résultats à club.ssi.gouv.fr pour une analyse collaborative.
6. **Renforcement de l'authentification** :
    - Mise en place de l'authentification multifacteur (MFA) pour les accès VPN SSL liés au LDAP.
    - Déploiement de licences FortiToken pour sécuriser les connexions distantes.
    - Configuration spécifique du MFA avec l'option set username-sensitivity disable pour empêcher le contournement du FortiToken via l'utilisation de majuscules dans les noms d'utilisateur.

4. Rôle et missions personnelles dans la gestion de l'incident

En tant que membre de l'équipe de réponse à l'incident, j'ai contribué aux actions suivantes :

1. **Récupération des journaux** :
    - Extraction des journaux du serveur compromis à l'aide de l'observateur d'événements Windows, permettant une analyse détaillée des événements liés à l'intrusion.
2. **Gestion des comptes VPN** :
    - Création et paramétrage des comptes VPN liés au LDAP pour garantir un accès sécurisé aux utilisateurs autorisés.
3. **Mise en place de MFA** :
    - Configuration de l'authentification multifacteur pour les comptes VPN, incluant l'intégration des licences FortiToken.
    - Paramétrage spécifique du MFA avec l'option set username-sensitivity disable pour renforcer la robustesse du système face aux tentatives de contournement.

5. Enseignements et recommandations

5.1. Enseignements tirés

- La désactivation rapide des accès VPN a permis de limiter l'exposition du système.

- L’absence de comptes obsolètes et l’usage de mots de passe robustes ont réduit la surface d’attaque.
- L’outil Oradad et les solutions EDR ont facilité l’analyse et la détection des anomalies.

5.2. Recommandations

- Effectuer des audits réguliers des comptes Active Directory pour identifier et désactiver les comptes obsolètes.
- Étendre le déploiement de l’EDR à l’ensemble des serveurs et postes de travail.
- Sensibiliser les utilisateurs à l’importance de l’authentification multifacteur et des bonnes pratiques de cybersécurité.
- Planifier des exercices réguliers de simulation d’incidents pour tester la résilience de l’infrastructure.

6. Conclusion

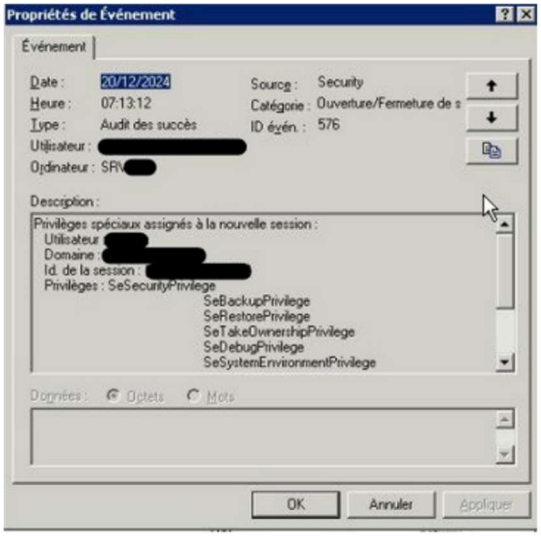
L’incident du 20 décembre 2024 a été géré avec efficacité grâce à une réponse rapide et coordonnée. Les mesures techniques mises en place, combinées aux actions proactives de renforcement de la sécurité, ont permis de contenir la menace sans impact opérationnel. Les recommandations formulées visent à améliorer la posture de sécurité de l’organisation pour prévenir de futurs incidents.

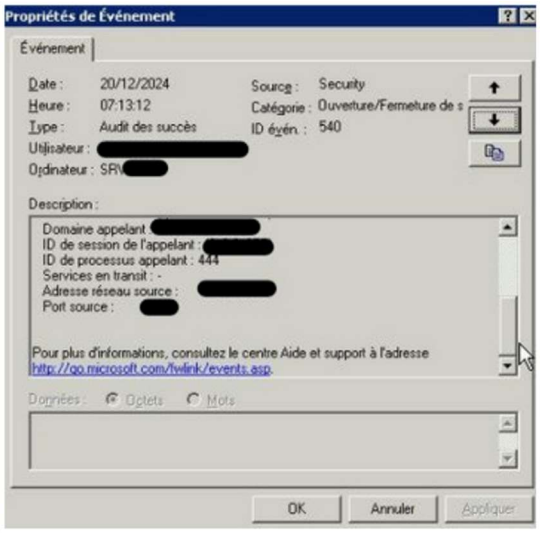
7. Annexes

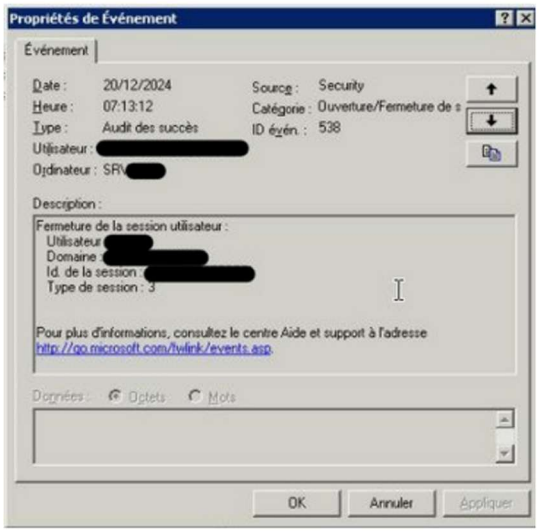
- **Annexe 1** : Extrait des journaux du serveur
- **Annexe 2** : Configuration détaillée du FortiToken et du MFA

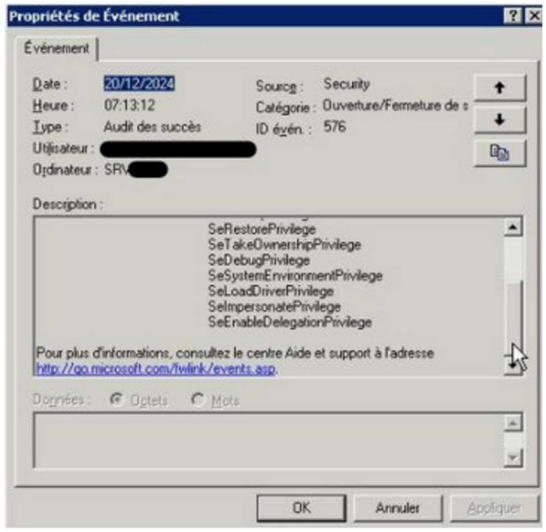
Annexe 1 : Extrait des journaux du serveur

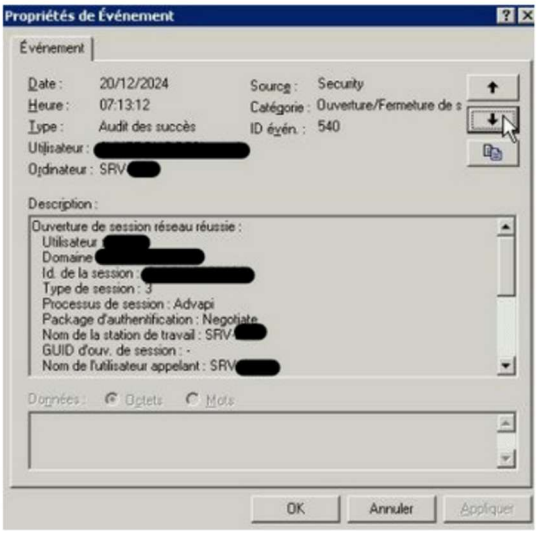
Voici un extrait des journaux de connexions à un compte administrateurs utilisé par l'attaquant :











Annexe 2 : Configuration détaillée du FortiToken et du MFA

```
FW-[redacted]-MASTER # config user local

FW-[redacted]-MASTER (local) # edit nweber

FW-[redacted]-MASTER (nweber) # show full
config user local
    edit "nweber"
        set status enable
        set type ldap
        set two-factor fortitoken
        set fortitoken "FTKMOB[redacted]"
        set email-to "[redacted]@gmail.com"
        set sms-server fortiguard
        set sms-phone "+3306[redacted]"
        set authtimeout 0
        set auth-concurrent-override disable
        set username-sensitivity disable
        set ldap-server "DC-[redacted]"
        set workstation ''
    next
end

FW-[redacted]-MASTER (nweber) #   set username-sensitivity enable

FW-[redacted]-MASTER (nweber) # next

FW-[redacted]-MASTER (local) # end

FW-[redacted]-MASTER #
```

Comparaison de l'activation du facteur à double authentification avant et après configuration, en premier il est à 0 puis il passe à 1 :

```
FW-[redacted]-MASTER # get vpn ssl monitor
SSL-VPN Login Users:
 Index   User    Group   Auth Type      Timeout         Auth-Timeout    From     HTTP in/out    HTTPS in/out    Two-factor Auth
 0       nwebeR          UsersFortiSSL  16(1)            298    28798   [redacted]    0/0     0/0     0

SSL-VPN sessions:
 Index   User    Group   Source IP      Duration        I/O Bytes       Tunnel/Dest IP
 0       nwebeR          UsersFortiSSL  [redacted]      2       0/0     [redacted]


FW-[redacted]-MASTER # config user local

FW-[redacted]-MASTER (local) # edit nweber

FW-[redacted]-MASTER (nweber) #   set username-sensitivity disable

FW-[redacted]-MASTER (nweber) # next

FW-[redacted]-MASTER (local) # end

FW-[redacted]-MASTER # get vpn ssl monitor
SSL-VPN Login Users:
 Index   User    Group   Auth Type      Timeout         Auth-Timeout    From     HTTP in/out    HTTPS in/out    Two-factor Auth
 0       nwebeR          UsersFortiSSL  16(1)            300    28795   [redacted]    0/0     0/0     1

SSL-VPN sessions:
 Index   User    Group   Source IP      Duration        I/O Bytes       Tunnel/Dest IP
 0       nwebeR          UsersFortiSSL  [redacted]      2       0/0     [redacted]


FW-[redacted]-MASTER #
```