

# PROSIT 5 : T’es qui toi ?

# Contexte

On organise une réunion pour régler le problème de connexion au LAN par des intrus avec des identifiants d’employés.

# Mots-clés

Le SSO est une méthode d'authentification qui permet à un utilisateur de se connecter à plusieurs systèmes et applications en utilisant une seule paire de nom d'utilisateur et de mot de passe. Lorsque l'utilisateur se connecte initialement, le SSO crée un jeton d'authentification qui est utilisé pour accéder à diverses ressources sans avoir à réintroduire les informations d'identification à chaque fois. Le SSO vise à simplifier l'expérience de l'utilisateur, à renforcer la sécurité et à faciliter la gestion des comptes.

# MiM : MiM signifie "Man-in-the-Middle", soit "L'homme du milieu" en français. Il s'agit d'une attaque où un attaquant intercepte et modifie les communications entre deux parties, souvent sans que ces dernières en aient conscience.

# Keyloggers : Les keyloggers, ou "enregistreurs de frappe" en français, sont des programmes ou des dispositifs matériels conçus pour enregistrer les frappes du clavier d'un utilisateur à son insu. Cela peut être utilisé pour voler des informations sensibles, telles que des mots de passe.

# Extranet : Un extranet est un réseau privé étendu qui permet à des partenaires, clients ou fournisseurs autorisés d'accéder à certaines ressources ou informations internes d'une organisation, généralement via Internet.

# PKI : PKI signifie "Infrastructure à Clé Publique" en français. C'est un ensemble de technologies et de pratiques de sécurité qui permettent de gérer des clés de chiffrement, de certificats numériques et d'assurer l'authentification et la confidentialité des données.

# SSL : SSL signifie "Secure Sockets Layer", soit "Couche de Sockets Sécurisée" en français. C'est un protocole de sécurité qui garantit la confidentialité et l'intégrité des données échangées entre un serveur et un client, souvent utilisé pour sécuriser les connexions Web.

# TLS : TLS signifie "Transport Layer Security", ou "Sécurité de la Couche de Transport" en français. Il s'agit d'une version plus récente et plus sécurisée du protocole SSL, utilisée pour sécuriser les communications sur Internet.

# Problématique

**- Quel procédé mettre en place pour empêcher l’interception des identifiants lors de l’authentification à l’aide du serveur d’annuaire ?**

**- Comment permettre l’accès aux ressources internes aux personnes extérieures ?**

# Contraintes

Pas de contraintes.

# Généralisation

Mettre en place un accès à distance

Mettre en place un processus d’authentification sécurisé

# Livrables

Procédure de sécurisation de la gestion de mot de passe

Schéma de l’infrastructure

# Pistes de solution

Kerberos

VPN

# Plan d’action

Lister les services existants

Etude sur les VPNs, comparer avec autres solutions de connexion à distance.

# Réalisation du plan d’action

Pour l’accès à distance, plusieurs solutions existent : le VPN, SSH, RDP, TeamViewer, VNC . Chacun des ses systèmes peux être utiliser de pair les uns avec les autres et avec SSO.

Un VPN, ou réseau privé virtuel, est une technologie qui permet de créer un tunnel sécurisé sur Internet pour transmettre des données de manière cryptée. Les VPN sont largement utilisés pour sécuriser les communications sur des réseaux publics, tels que l'Internet. Ils permettent aux utilisateurs d'accéder à des ressources réseau de manière sécurisée, de masquer leur adresse IP et de contourner les restrictions géographiques. Les VPN sont couramment utilisés pour la connectivité à distance, le travail à domicile et la protection de la vie privée en ligne. L’ansii conseil TheGreenBow VPN

SSH (Secure Shell) : SSH est un protocole de communication sécurisé qui permet d'accéder à distance à des ordinateurs et de gérer des serveurs de manière sécurisée. Il offre un canal de communication cryptée, ce qui le rend adapté à des tâches telles que l'administration à distance, le transfert de fichiers sécurisé et la tunnelisation de trafic. SSH est largement utilisé dans les environnements Linux et Unix pour une gestion sécurisée des serveurs.

TeamViewer est un logiciel de bureau à distance populaire qui permet aux utilisateurs de contrôler un ordinateur à distance depuis n'importe où dans le monde. Il est couramment utilisé pour des réunions à distance, l'assistance technique à distance et l'accès à des ordinateurs distants. TeamViewer utilise des technologies de sécurité pour protéger les connexions.

RDP (Remote Desktop Protocol) : RDP est un protocole de Microsoft qui permet aux utilisateurs de se connecter à distance à un ordinateur Windows et d'accéder au bureau à distance. Il permet le contrôle complet de l'ordinateur distant, ce qui en fait une solution courante pour l'assistance technique à distance, la gestion de serveurs à distance et le travail à distance sur des ordinateurs Windows.

VNC (Virtual Network Computing) : VNC est une technologie qui permet de visualiser et de contrôler l'écran d'un ordinateur distant. Il est souvent utilisé pour l'administration à distance, le dépannage, la formation à distance et la gestion de serveurs. Il existe différentes variantes de VNC, telles que TightVNC et RealVNC, qui offrent des fonctionnalités de sécurité supplémentaires.