1.06 - Configurer et sécuriser les accès distants

Durée approximative : ***4h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R2 : Installation et qualification***
    - ***C09 : Installer un réseau informatique***
      - ***Protocoles usuels SSH, RDP, WinRM***
      - ***Systèmes d'exploitations (Windows, UNIX)***

- ***U5 - Exploitation et maintenance de réseaux informatiques***
  - ***R3 : Exploitation et maintien en condition opérationnelle***
    - ***C10 : Exploirer un réseau informatique***
      - ***Interface en ligne de commande d'équipements et de système d'exploitation***
      - ***Connexion et prise en main à distance (protocoles et législation associée)***

- ***U6 - Valorisation de la donnée et cybersécurité***
  - ***D5 : Audit de l'installation ou du système***
  - ***C10 : Exploirer un réseau informatique***
    - ***Usage de documents règlementaires, normatifs adoptés au sein de l'entreprise et du secteur de la sécurité des systèmes d'information***

I. Introduction aux protocoles d'accès distants

Parler du principe d'accès distant.

Décrire le contexte législatif, notamment en ce qui concerne la prise en main à distance pour l'utilisateur (consentement, etc..)

Expliquer pourquoi il y a nécessité, à la fois pour des aspect réglementaire et de sécurité, d'utiliser des comptes nominatif et de loguer pour assurer une traçabilité des actions.

II. Le protocole SSH

Expliquer l'utilité et le fonctionnement du protocole SSH.

> **TP** : Faire installer le serveur ssh sur une VM linux et l'activer. Mettre un mot de passe faible et montrer un test de pénétration SSH.

Faire une analyse de risque. Faire chercher le guide des bonnes protiques de configuration SSH de l'anssi.

> **TP** : Reconfigurer le SSH en mode mot de passe et ajouter un compte automation avec authentification par clé.

Valider l'installation.

III. Le protocole RDP

Expliquer l'utilité et le fonctionnement du protocole RDP.

Montrer les failles du protocole. Parler du changement de méthode d'authentification (credssp) pour améliorer sa sécurité.

> **TP** : Faire configurer le RDP.

Faire une analyse de risque et chercher la documentation associée sur le site de l'anssi.

> **TP** : Appliquer les recommandations sur le paramétrage.

Valider l'installation.

IV. Le protocole winRM

Expliquer l'utilité et le fonctionnement du protocole winRM

Montrer les failles du protocole. Parler des listener et des trusted sources.

> **TP** : Faire configurer le winRM.

Faire une analyse de risque et chercher la documentation associée sur le site de l'anssi.

> **TP** : Appliquer les recommandations sur le paramétrage, désactiver le listener http et passer en https.

Valider l'installation.

V. Les autres protocoles

Evoquer les autres protocoles comme VNC, TeamViewer et rustdesk/anydesk (protocoles propriétaires)

Ressources associées :

<mettre ici les liens vers les pages ressources et support de cours>

Revision #1
Created 2026-07-17 13:12:02 UTC by Olivier
Updated 2026-07-17 13:12:02 UTC by Olivier