**Fiche de séances**

**INFO**

**Durée 2x2.5h**

| **Pôle d’activité** | **Etude et conception de réseaux informatique** | **U4** |
| --- | --- | --- |
| **Bloc de compétences** | **Concevoir un système informatique** | **C05** |
| **Compétence(s)** |  |  |
| **Objectif pédagogique** | **Module 05-B - Cryptoanalyse & SSH** |

| **Connaissances issues du référentiel** | * Niveaux de sécurité attendus : Chiffrage , protection de communication
 | Niveau 2 |
| --- | --- | --- |
|  |  |
| **Connaissances opérationnalisées\*** |  |  |
|  |  |

\* Connaissance opérationnalisée : description de la compétence en fonction du niveau visé par la séance.

Activités

Thème : Mise en place d’une authentification SSH par clé ( connexion inter-VM)

1- Activité de réactivation sous forme de quizz en tableau interactif / Wooclap / Moodle:

 quels sont les avantages d’un chiffrement symétrique ?

 quels sont les points d’attention d’un chiffrement symétrique ?

 quels sont les avantages d’un chiffrement symétrique ?

 quels sont les points d’attention d’un chiffrement symétrique ?

2- Activité d’apports de connaissances:

 Rappel chiffrement symétrique / asymétrique / hybride.

3- Activité d’apports de connaissances :

 Introduction à OpenSSH

4- Activité de travaux pratiques :

SSH - Vérification des empreintes (ssh-keygen -lf)

SSH mode debug

 Observation SSH et changement de clefs de session par wireshark

5- Atelier découverte et compte-rendu:

 En utilisant le man de ssh et le man de sshd, les élèves documentent l’installation d’OpenSSH sur client01 en inventoriant et précisant le rôle des différents fichiers présents.

6- Usage d’un agent d’authentification ( connexion inter-VM)

| **Ressources pédagogiques :**  |
| --- |
| * <https://man.openbsd.org/ssh>
* <https://man.openbsd.org/sshd>
* <https://www.ssh.com/academy>
* Notions de cryptographie de l’ANSSI (<https://secnumacademie.gouv.fr/>)
 |

**Évaluation**

1. Compte rendu de TP