

# Fiche de séances

**INFO**

**Durée 2x2.5h**

|                             |  |            |
|-----------------------------|--|------------|
| <b>Pôle d'activité</b>      | <b>Etude et conception de réseaux informatique</b> | <b>U4</b>  |
| <b>Bloc de compétences</b>  | <b>Concevoir un système informatique</b>           | <b>C05</b> |
| <b>Compétence(s)</b>        |  |            |
| <b>Objectif pédagogique</b> | <b>Module 05-B - Cryptoanalyse &amp; SSH</b>       |            |

|  |  |          |
|--|--|----------|
| <b>Connaissances issues du référentiel</b> | <ul style="list-style-type: none"><li>Niveaux de sécurité attendus : Chiffrement , protection de communication</li></ul> | Niveau 2 |
| <b>Connaissances opérationnalisées*</b>    |  |          |

\* 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 asymétrique ?
- quels sont les points d'attention d'un chiffrement asymétrique ?

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