**Fiche de séances**

**INFO**

**Durée 2.5h**

| **Pôle d’activité** | **Etude et conception de réseaux informatique** | **U4** |
| --- | --- | --- |
| **Bloc de compétences** | **Concevoir un système informatique** | **C05** |
| **Compétence(s)** |  |  |
| **Objectif pédagogique** | **Module 06-C - Cybersécurité Attaque Man In The Middle 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

1. TP guidé : Attaque SSH Man in the Middle

VM d’attaque ( eve) fournie

Activité de travaux pratiques guidés :

a- Préparation

b- Tester ARP Spoofing

c- Substituer sshd de eve par SSH-MITM

d- Configurer les redirections réseau de eve

e- Activer l’attaque avec un ARP Spoofing

f- Exploitation de l’attaque

g- Fin d’attaque

h- Retour à la normale

Travail en binôme : l’un se comporte comme client, l’autre actionne l’attaque .

Rédaction d’un compte rendu de TP synthétisant les deux points de vue.

| **Ressources pédagogiques :** |
| --- |
| * <https://www.ssh.com/academy/attack/man-in-the-middle> * <https://www.ettercap-project.org/downloads.html> * <https://docs.ssh-mitm.at> |

**Évaluation**

1. Compte rendu de TP