# Projet SSI

**N.B. toute opération d'écoute ou d'interception du trafic ou de scan des ports ou des vulnérabilités illégale d'un réseau où vous n'êtes pas autorisés est contraire à l'éthique et considérée aussi comme un crime.**

## Objectifs du projet

- Analyse du traffic d'un réseau
- Identification de ports ouverts et de failles de sécurité
- Crackage de fichier de mot de passe
- Configuration des mécanismes de cryptage coté client et serveur

### Environnement du projet

Les expérimentations du projet doivent être réalisées sur un réseau de 3 machines (réelles ou virtuelles) ou plus avec des hôtes mobiles. Sur ces machines deux plateformes (ubuntu, arch, centos, …) ou plus doivent être déployées. Les services nécessaires pour les différentes parties du projet sont principalement FTP ou Telnet et SSH (serveur et client)

### Partie A : Sniffing

1. Expliquer brièvement cette attaque passive et donner des exemples d'outils pour l'implanter
2. Collecter les trafics générés et identifier les mots de passe utilisés lors de l'utilisation du protocole d'authentification entre un client et serveur pour les services suivants :
   - FTP ou Telnet
   - SSH

### PARTIE B : Scan des ports et des vulnérabilités

1. Expliquer les différences entre les deux types de scan
2. Pour chaque type de scan, comparer les deux outils les plus utilisés
3. Identifier les ports ouverts sur chaque machine du réseau utilisé
4. Déterminer le système d'exploitation et l'état de chaque machine du réseau
5. Donner l'architecture du réseau utilisé
6. Identifier les vulnérabilités systèmes les plus graves (critique) dans le réseau utilisé

### Partie C : Cracking passwords

1. Ajouter un nouvel utilisateur sur la plateforme utilisée
2. Identifier le fichier de mot de passe sur cette plateforme
3. Utiliser un outil de crack pour divulguer le mot de passe de l'utilisateur ajouté.

**Partie D : cryptographie+**

1. Tester les cryptages symétrique et asymétrique d'un fichier échangé entre un client et un serveur.
2. Utiliser les fonctions de hachage pour vérifier l'intégrité d'un échange crypté entre un client et serveur
3. Générer un certificat électronique, installer le auprès d'un serveur SSH pour assurer l'authentification
4. Tester l'authentification mutuelle en utilisant la signature digitale

## Les livrables : déposez les rapports suivants dans le dirve du groupe en respectant les délais fixés

**Rapport N1 en format PDF : Sniff et scan : date limite 17/03/2024 à minuit**

**Rapport N2 en format PDF: crackage et crypto date limite 28/04/2024 à minuit**