# Sécurité et réseaux

Compte rendu de travaux pratique

Valvin Matthieu

## Expérience 1 : Packet Sniffing Lab

Cette première expérience avait pour objectif d'observer, au moyen d'un logiciel fourni, les échanges entre machines client et serveur. Le logiciel utilisé était WireShark et j'ai pu observer le système de requête et de réponses sur le réseau au travers d'exemple précis. J'ai notamment pu utiliser les connaissances acquises en 3IF en examinant les paquets des différents protocoles réseaux (SSH, HTTP, TCP…). J'ai ensuite été plus long en utilisant ces protocoles afin d'exploiter des vulnérabilités (données chiffrées ou non) afin de récupérer des informations. Il a notamment été question de déterminer les informations de connexions dans un paquets.

## Expérience 2 : DDOS

Dans cette expérience nous nous sommes intéressé à une des attaques les plus populaires sur le WEB : l'attaque par déni de service ou *Distributed Denial of Service Attack.* Le concept de cette attaque est d'envoyer un grand nombre de requête sur un serveur afin de le surcharger.Pour mettre en place cette attaque nous avons utilisé une commande linux qui envoie des requêtes et ce depuis une, deux puis trois machines virtuelles différentes afin d'observer le comportement de la page test selon l'amplitude de l'attaque.

## Expérience 3 : Buffer Overflow

L'objectif de cette attaque est de surcharger la pile d'exécution afin d'accéder à une zone précise et de pouvoir y injecter du code exécutable. La première étape de l'attaque est de déterminer la taille de la zone allouée afin de connaître avec exactitude le nombre de caractère qu'il nous faut pour accéder à la zone où injecté le code exécutable. Une fois cette zone déterminée, il suffit de faire déborder la zone alloué et de tenter d'exécuter des lignes de commandes.

## Expérience 4 : Cross Site Scripting

Cette expérience se concentre sur des attaques réalisables, non plus sur le terminal, mais sur des sites web. Une de ces attaques fonctionne de la manière suivante : un lien malicieu est envoyée à la victime, lorsque que celle-ci accède à cette page, un script est exécuté et il nous permet de récupérer les cookies de la victimes et notamment celui correspondant à sa connexion sur le site. Nous pouvons alors utiliser ces cookies pour se connecter sur le site avec le compte de la victime et ce sans que celui-ci s’en rende compte.