# Sécurité - Réseaux

Debriefing des TPs

Durant notre formation, nous n'avons pas eu l'occasion de travailler sur des sujets liés à la sécurité. Nous avons tous conscience (j'espère) que la sécurité informatique est l'affaire de tous, et que lors de la conception et du développement de logiciels/technologies tous les acteurs doivent y prêter attention.

Cependant c'est la première fois que nous abordons le problème selon un autre point de vue : pendant ces TPs nous avons pu comprendre les faiblesses de certaines technologies en essayant de les compromettre et en exploitant des failles de sécurité. L'approche utilisée est originale aussi dans le sens où l'on va devoir attaquer des systèmes vulnérables et non concevoir des systèmes le moins vulnérable possible.

## Expérimentation 1 : Packet Sniffing Lab

Nous avons pu expérimenter dans cette partie l'interception de paquets sur un réseau. Nous avons utilisé le protocole telnet pour commencer car il ne chiffre pas les données qu'il transmet. Ainsi nous avons pu intercepter un échange d'identifiants (un nom d'utilisateur et un mot de passe) complètement en clair. On comprend donc l'utilité du protocole SSH, qui permet de chiffrer les données et de sécuriser l'échange des identifiants.

## Expérimentation 2 : DDOS

Dans cette partie, nous avons pu expérimenter une attaque simple à mettre en oeuvre sur un serveur web. Chaque attaquant envoie énormément de requêtes sans attendre de réponse vers le serveur, l'obligeant à traiter chaque requête et donc à surcharger son processeur en opérations, ainsi il ne peut plus traiter les requêtes "normales" des utilisateurs qui ne peuvent plus accéder au site hébergé sur le serveur. Nous avons commencé par utiliser HTTP Load, qui se montrait limité. Nous avons ensuite utilisé un outil dédié permettant d'envoyer énormément de requêtes afin de surcharger le serveur. Ces outils sont simples à mettre en place et à utiliser, mais l'attaque peut être contrée par le serveur, par exemple en vérifiant l'IP qui envoie les requêtes et en ne traitant pas ses requêtes si l'on détecte un DDOS.

## Expérimentation 3 : Buffer Overflow

Les attaques par Buffer Overflow sont courantes, elles reposent sur un principe simple : faire déborder une zone allouée sur la pile afin de pouvoir injecter du code dans des endroits réservés. Nous commençons par déterminer la taille de la zone allouée, puis en exécutant un certain code nous pouvons procéder, par exemple, à une escalade de privilèges, pour pouvoir exécuter un shell comme root. Aujourd'hui il existe des solutions pour prévenir ces attaques, mais des failles existeront toujours et aucun système n'est infaillible.

## Expérimentation 4 : Faille XSS

Dans la dernière partie du deuxième TP, nous avons pu utiliser la faille XSS afin de voler les cookies d'un utilisateur à l'aide d'un script. L'utilisateur ne se rend pas compte que ses données ont été volées en cliquant sur un lien dans un mail. C'est une bonne sensibilisation à la sécurité sur le web.

Dans un second temps, nous avons pu réaliser une injection SQL au travers d'un champ de recherche sur un site web. Nous sommes parvenus à obtenir des informations sur la base de données et sur tous les utilisateurs inscrits. On se rend aussi compte que ces failles sont critiques et qu'il faut les éviter dès le développement du site.

## Conclusion

En conclusion, ces TPs ont été une véritable découverte du monde de la sécurité et des attaques réalisables, même si certaines sont dépassées. Chaque sujet m'a permis de découvrir des nouvelles technologies au travers d'attaques. Le site mis en place est pratique et plutôt rapide, nous n'avons pas eu beaucoup de difficulté à l'utiliser.