Retours TP AskCyper

Bien qu'évoluants tous dans des milieux informatiques, nous avons été jusqu'ici peu formés aux différents aspects de la sécurité informatique, pourtant un élément central dans la plupart des activités menées.
Ces TP nous ont donc permis de découvrir et de tester différents types d'attaque, d'en apprendre un peu plus sur leur histoire, leur contexte ou les moyens de lutter contre elles, ce qui est à mon sens important afin que la sécurité ne soit plus une composante "annexe" et relevant de la culture générale, mais que lors de nos projets futurs une véritable réflexion autour de cette problématique soit menée.

En ce sens les TP ont très bien fonctionné et donnent envie de s'intéresser plus au monde de la cyber-sécurité.

Packet Sniffing Lab

Cette attaque consistait en l'interception et la lecture de paquets sur un réseau. Ainsi, nous avons pu dans un premier temps constater que le protocole telnet ne chiffrait pas les données envoyées, ce qui nous a permis d'intercepter un username et mot de passe.
Cela a mis en lumière l'utilité du protocole SSH qui chiffre les données et permet donc leur échange de manière sécurisée.
Cette attaque nous a ainsi permis de découvrir wireshark (un packet sniffer), utilisé notamment pour l'interception et l'observation des paquets échangés.

DOS

Pour moi l'attaque la plus marquante des TP AskCyper de par sa simplicité de mise en oeuvre, et de par le peu de moyens de s'en protéger.
En effet il est très simple de mettre en place une attaque DOS, et incapaciter un serveur web.
L'attaque consiste à envoyer (via des logiciels tiers ou non), un nombre de requêtes extrêmement élevé sur un serveur web. Le serveur ne pourra alors pas traiter toutes ces requêtes et sera incapacité donc inaccessible pour tous les autres clients. Nous avons utilisé pour cela HTTP Load puis un outil dédié au SYN flood. Ce dernier était très efficace contre des serveurs non protégés.
Un moyen de contrer cette attaque serait d'examiner les requêtes entrantes pour le serveur, et bloquer celles dont l'adresse IP revient trop régulièrement (si une même adresse IP envoie 200 requêtes par seconde, il y a des chances que ça soit une tentative de DDOS).

Buffer Overflow

Le principe de l’attaque par Buffer Overflow est simple : faire déborder intentionnellement une zone allouée sur la pile afin de pouvoir injecter du code malveillant dans des endroits réservés.
Après avoir déterminé la taille de la zone allouée, on peut exécuter notre code pour par exemple ouvrir un terminal, puis procéder à une escalade des privilèges en se basant sur des failles du système d’exploitation.

Cross Scripting Site

L’objectif de cette dernière partie était de découvrir les failles de sécurité sur le web. Nous avons notamment pu expérimenter le vol de cookies à l’insu d’un utilisateur grâce à un script, ce qui permet par exemple d’accéder à ses informations personnelles.
J’ai trouvé cette attaque intéressante car elle repose grandement sur une erreur humaine (cliquer sur un lien peu fiable reçu par mail) et est donc susceptible de fonctionner souvent si employée à grande échelle.
Nous avons également pu faire l'expérimentation d’injection SQL, qui consiste à entrer une commande SQL dans un champ de formulaire sur un site. Cette commande pourra récupérer des informations sur la base de données ou même l’altérer. Personnellement j’ai trouvé cette attaque moins intéressante. Bien que classique donc importante à connaître, elle est moins spectaculaire et semble plus obsolète aujourd’hui, la plupart des bases de données étant protégées.