FeedBack sur les TPs de CyberSécurité

Expérimentation 1 : Packet Sniffing Lab

L'interception des données est très facile lorsque celles-ci circulent en clair sur un réseau. En effet des outils tels que wireshark (packet sniffer) permettent d'intercepter ce qui passe sur le réseau.
Le protocole telnet n'assure pas le chiffrement des données ce qui les rends vulnérables d'où l'utilité de protocole de chiffrement tel que SSH. Grâce à SSH, l'échange des identifiants (handshake) est crypté et seul la source et l'identifiant sont en clairs : l'échange est sécurisé.

NB : Les ack que l'on peut voir en observant les données permettent la synchronisation du serveur et du client.

Une analyse du trafic DNS permet de comprendre comment le serveur DNS peut être interrogé afin d'obtenir les adresses recherchées à partir d'un nom d'hôte. Il y a deux types de requêtes (A et AAAA) qui distingue le traitement des adresses IPv4 et IPV6. Le serveur répond aux requêtes en renvoyant cette requête suivi de la réponse et de la durée pendant laquelle celle-ci est valide.

Expérimentation 2 : DOS

Dans cette partie nous avons essayé de perturber le fonctionnement d'un serveur en le surchargeant de requêtes depuis 3 machines pirates. Pour cela, nous avons dans un premier temps utilisé HTTP Load qui permet de tester la réponse d'un serveur à un certain nombre de requêtes simultanées, cela nous a permis de parfois le surcharger. Dans un second temps nous avons utilisé TCP SYN Attcks qui est un outil dédié à la surcharge de serveurs. Cette fois, le serveur est totalement dépassé dès que l'on lance plusieurs machines pirates sur lui. Il devient inaccessible pour les autres clients (d'où l'appellation : déni de service) et peut aller jusqu'à crasher.

Expérimentation 3 : Buffer Overflow

Le principe du buffer overflow est de venir faire "déborder" une zone allouée en mémoire dans la pile et ainsi injecter du code pour modifier le comportement initial d'un programme. On doit commencer par déterminer la taille de la zone allouée. Une fois que cela est fait on

peut insérer des lignes de commandes pour exploiter cette faille comme on le désire (ouvrir un terminal avec des droits supérieurs par exemple). Les compilateurs modernes sont pour la plupart protégés contre ce genre de faille d'où la nécessité de maintenir ses outils et de ne pas laisser vieillir les architectures.

Expérimentation 4 : Cross Site Scripting

Cette partie permet de découvrir certaine des failles de sécurité sur le web. Ainsi on a pu voir comment un script pouvait récupérer les cookies d'un utilisateur à son insu et les utiliser pour substituer son identité en ligne. Ce qui est surprenant est que l'utilisateur peut n'avoir aucune conscience de ce vol et continuer sa navigation comme si de rien n'était.

Nous avons également pu nous intéresser à l'injection sql qui consiste à venir insérer du code dans un champ quelconque. Cela aura pour effet de venir perturber le comportement du site en accédant ou en modifiant certaines données grâce la requête que l'on aura insérées.