Retour TP SERE

Expérimentation 1 : Packet Sniffing Lab

Il existe de nombreux outils facilement utilisable permettant d'intercepter et interpréter les données sur le réseau. Wireshark m'a permis d'observer des échanges à différents niveaux. Premier constat, le protocole de chiffrement tel que SSH est indispensable, car le protocole telnet n'assure pas le chiffrement des données. On peut facilement retrouver les données personnelles de l'utilisateur. Grâce à SSH, l'échange des identifiants (handshake) est crypté et seul la source et l'identifiant sont en clairs.
Nous avons ensuite travaillé sur le trafic DNS.

Expérimentation 2 : DOS

Dans cette partie nous avons, grâce à 3 machines pirates, essayé de perturber le fonctionnement d'un serveur en le surchargeant.
Nous avons suivi la réponse du serveur à des requêtes simultanées avec HTTP Load.
Nous avons ensuite utilisé TCP SYN Attacks qui est un outil dédié à la surcharge de serveur. En surchargeant le serveur par des requêtes répétitives nous pouvons empêcher le bon déroulement d'une requête standard, ce qui revient à le rendre inaccessible. Ce type de surcharge peut pousser le serveur a crasher.

Expérimentation 3 : Buffer Overflow

Le buffer overflow nous permet d'injecter du code pour modifier le comportement initial d'un programme. A partir d'une taille de zone allouée, on peut insérer des lignes de commandes pour exploiter cette faille comme on le souhaite. Néanmoins, les compilateurs modernes sont souvent protégés contre ce genre de faille d'où la nécessité de maintenir ses outils.

Expérimentation 4 : Cross Site Scripting

Ce dernier point était plus axé sur les failles Web : par exemple la récupération des cookies et son exploitation nous a permis de substituer la place d'un utilisateur sans que lui même n'en prenne conscience.
De la même manière, nous avons impacté des sites par injection de code.