Master Cryptographie et Sécurité de l'information

SYLLABUS
Travaux Pratiques et Mini-projets
du module Sécurité des Réseaux Informatique

Travaux Pratiques:

TP n°1 : Réalisation d'attaques informatiques - Utilisation d'Ettercap
Objectif : L'objectif de ce TP est de donner aux étudiants l'occasion de réaliser certaines attaques informatiques classiques. Le but étant de bien sentir le risque et la nécessité de chercher à bien sécuriser les systèmes et réseaux informatiques afin de faire face à ce genre d'attaques.

Nous nous intéressons essentiellement au type d'attaques « man in the middle » à travers la réalisation d'une attaque ARP poisoning.

Les étudiants sont ensuite amenés à réaliser d'autres attaques du même genre, mais concernant d'autres protocoles (ex. DNS, http).

TP n°2 : Mise en place d'un Firewall sous linux
Objectif : Ce TP propose d'installer un firewall sur une machine Linux afin de séparer deux segments de réseau différents et de mettre en place la politique de sécurité nécessaire.

Pour ce faire, nous procédons aux étapes suivantes :
- Configuration des paramètres réseaux des trois machines virtuelles local, distant et firewall ;
- Faire un ensemble de tests avec la configuration par défaut du firewall ;
- Configuration du Firewall Iptables ;
- Tester les configurations effetuées ;

TP n° 3 : Mise en place d'un IDS Snort
Objectif : L'objectif de ce TP est de mettre en place un système de détection d'intrusion en se basant sur le logiciel libre Snort.

Pour ce faire, nous procédons aux étapes suivantes :
- Installer du logiciel Snort et les logiciels requis;
- Configurer de Snort ;
- Effectuer des tests avec Snort dans ses différents modes ;
- Découvrir de la distribution Backtrack ;
- Effectuer des tests avec Snort sous Backtrack.

TP n° 4 : Mise en œuvre d'un VPN avec Open VPN sous Linux
Objectif : L'objectif de ce TP est de mettre en œuvre un Virtual Private Network (VPN) avec Open VPN sous Linux.

Pour ce faire, nous procédons aux étapes suivantes :
- mettre en place un VPN compressé et non-crypté;
- mettre en place un VPN compressé et crypté;
- effectuer les tests nécessaires pour vérifier le bon fonctionnement du VPN;

Mini-Projets :

Mini-Projet 1 : Conception et création d'un virus/antivirus.
Objectif : L'objectif de ce mini projet est de pousser les étudiants à concevoir et réaliser un virus et par la suite créer un antivirus qui permet de le détruire.

Ceci leur permettra de :
- bien comprendre le fonctionnement des différents types de malwares (virus, vers, cheval de troie, etc) ;
- programmer les différentes fonctions sur lesquelles se base le malware ;
- et finalement programmer son antivirus.

Mini-Projet 2 : Mise en place d'un VPN L2TP
Objectif : L'objectif de ce mini projet est de mettre en place un réseau VPN basé sur le protocole L2TP (Layer 2 Tunneling Protocol). L'objectif étant d'apprendre à implémenter sous linux un serveur L2TP et un client L2TP sous windows et sous linux et faire des échanges sécurisés à travers un réseau VPN L2TP.

A travers ce mini projet, les étudiants sont amenés à travailler sur les points suivants :
- Configuration d'IPsec ;
- Configuration de MySQL ;
- Configuration du serveur FreeRADIUS ;
- Installation et configuration du serveur VPN L2TP (l2tpns) ;
- Configuration d'un client VPN windows et d'un client VPN linux.
- Faire les tests nécessaires pour s'assurer du bon fonctionnement de votre implémentation.