S E C U R I N E T S

C l u b d e l a s é c u r i t é i n f o r m a t i q u e

I N S A T

Atelier: Trojan & Rootkit

Securinetsiens : 1. Abidi Imen
2. Boukari Abdessabour
3. Mdini Chiheb
4. Romdhane Nizar
5. Sassi Maha

1. Présentation :

Cet atelier se situe dans l'étape 4 du PenTesting : Le maintien d'accès. Son objectif est de montrer comment garder un accès facile sur la machine en question tout en évitant les obstacles affrontés lors de la pénétration et ceci en utilisant un trojan et par la suite proposer des outils pour s'en protéger.

2. Outils utilisés :

Les outils sont :

- **Beast 2.07** : Un générateur de trojan
- **Ethereal** : Un Analyseur de trafic
- **Nmap**: Scanneur de port

Les sources sont :

- http://perso.menara.ma//hachattak/dossierbeast.htm consulté le 09/04/08
- fr.wikipedia.org
- www.securinfos.info
- www.hacktrojan.com

3. L'atelier Trojan & Rootkit:

3.1. Définition du Trojan :

Un trojan, ou cheval de troie ou encore troyen, est un programme informatique qui s'installe en se masquant dans un autre programme sain. Il ne se reproduit généralement

pas et sert de base (serveur) afin de permettre des intrusions sur une machine. Le nombre de trojans est aussi impressionnant que la variété des actions qu'ils permettent.
Certains ouvrent simplement un accès aux fichiers de la machine infestée, d'autres permettent une interaction complète avec celle-ci de la même manière que si l'intrus se trouvait devant-elle.

3.2. Fonctionnalités d'un trojan :

Une fois installé sur la machine, le cheval de Troie peut effectuer plusieurs taches selon son type à savoir voler ou changer des mots de passe, donner l'accès à des personnes non autorisées, copier des données sensibles, renommer tous les fichiers du disque dur, détruire la table d'allocation du disque dur, redémarrer le système et se connecter à des serveurs web inconnus.

3.3. Réalisation :

Un ingénieur en informatique au sein d'une société, s'occupe de la conception des produits de l'entreprise, son ordinateur contient des données très sensibles telles que des fichiers importants de conception d'une nouvelle technologie.
Son collègue, un pirate, profite de l'occasion de son anniversaire pour attaquer sa machine afin d'accéder aux fichiers sensibles et les vendre à d'autres entreprises concurrentes. Pour cela, il invite tous leurs collègues à lui envoyer un email contenant une carte virtuelle, lui aussi à son tour lui envoi une carte piégée contenant un trojan.
Lorsque la victime ouvre la carte, le trojan s'installe sur son ordinateur et le pirate reçoit une notification de son installation et par conséquent il peut voir et accéder à

l'arborescence complète de la machine cible, consulter tout ce qu'a été écrit par la victime grâce au Keylogger, fermer sa session ouverte et éteindre sa machine ….

Voici le générateur de trojan qu'on a utilisé afin d'élaborer notre travail :

3.4. Sécurisation :

Pour se protéger de ce type d'attaque, il est nécessaire d'installer, utiliser et maintenir à jour un logiciel antivirus, installer les correctifs pour votre système d'exploitation et vos logiciels, considérer l'utilisation de navigateurs et logiciels de messagerie alternatifs, être prudent en maniant des messages avec des pièces jointes et en téléchargeant des fichiers, configurer votre système d'exploitation convenablement et préservez votre vie privée comme on peut utiliser le mécanisme IDS (Intrusion Detection System) qui reste en écoute sur le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permet ainsi d'avoir une action de prévention sur les risques d'intrusion.
Dans notre atelier on a choisit quelques solutions pour sécuriser la machine de la victime, tout d'abord on a utilisé Nmap pour scanner les ports de la machine cible et voir s'il y en a des ports ouverts qui sont inutiles et peuvent être utilisés par le pirate et donc on les ferme pour assurer notre sécurité, notre deuxième solution était l'utilisation du sniffer réseau Ethereal pour analyser le trafic et voir s'il existe de trafic réseau anormal et donc il permet de nous avertir sur la sainteté de la machine et finalement on a essayé d'utiliser un bon antivirus au niveau du serveur mail et le mettre à jour, cet antivirus nous a permis de limiter la circulation des virus sur le réseau et détecter les trojans qui peuvent être envoyés par le pirate à travers la messagerie.