Chapitre 1

Les attaques

1.1 Le hacking

1.1.1 Qu'est-ce que c'est ?

Le hacking est un ensemble de techniques informatiques, visant à attaquer un réseau, un site, etc. Ces attaques sont diverses. On y retrouve :

- L'envoi de "bombes" logicielles.
- L'envoi et la recherche de chevaux de Troie.
- La recherche de trous de sécurité. Le détournement d'identité.
- La surcharge provoquée d'un système d'information (Flooding de Yahoo, eBay...).
- Changement des droits utilisateur d'un ordinateur. La provocation d'erreurs non gérées.
- Etc.

Les attaques peuvent être locales (sur le même ordinateur, voir sur le même réseau) ou distantes (sur internet, par télécommunication).

1.1.2 Le but du hacking

Le but du hacking est divers. Selon les individus (les "hackers"), on y retrouve : Vérification de la sécurisation d'un système. Vol d'informations (fiches de paye...). Terrorisme. Espionnage "classique" ou industriel. Chantage. Manisfestation politique. Par simple "jeu", par défi. Pour apprendre. Etc.

1.1.3 Le hacking légal

Le site anglophone Cyberarmy comporte une idée originale. Cette armée virtuelle est composée de hackers de tout niveau. Lorsque vous vous inscrivez vous êtes un Trooper (soldat de 2e classe). Le site propose plusieurs niveaux de protection qu'il faut hacker, et ce, en toute légalité. Au fur et à mesure que vous passez les niveaux de protection de cyberarmy, vous montez en grade. Bien sûr, plus vous montez en grade, plus le niveau est difficile. Pour information le webmaster de securiteinfo.com est Colonel de la cyberarmy (Kernel scrap). L'inscription se fait sur Zebulun

1.2 Les types d'attaque

1.2.1 Introduction

Les hackers utilisent plusieurs techniques d'attaques. Ces attaques peuvent être regroupées en trois familles différentes :

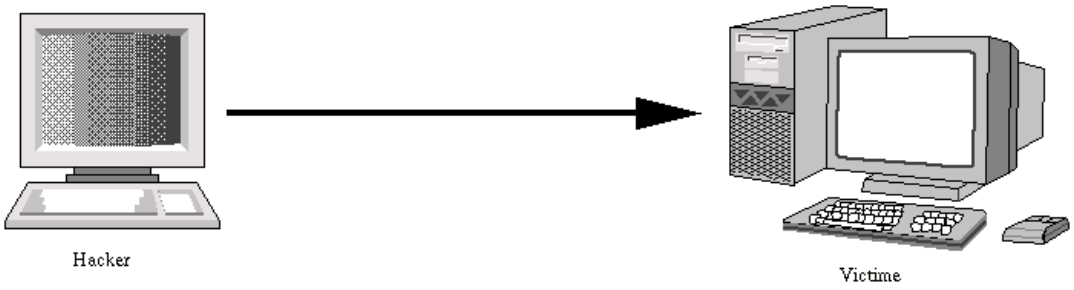
- Les attaques directes.
- Les attaques indirectes par rebond.

– Les attaques indirectes par réponses.

Nous allons voir en détail ces trois familles.

1.2.2 Les attaques directes

C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur. La plupart des "script kiddies" utilisent cette technique. En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les packets à la victime.



Attaque directe

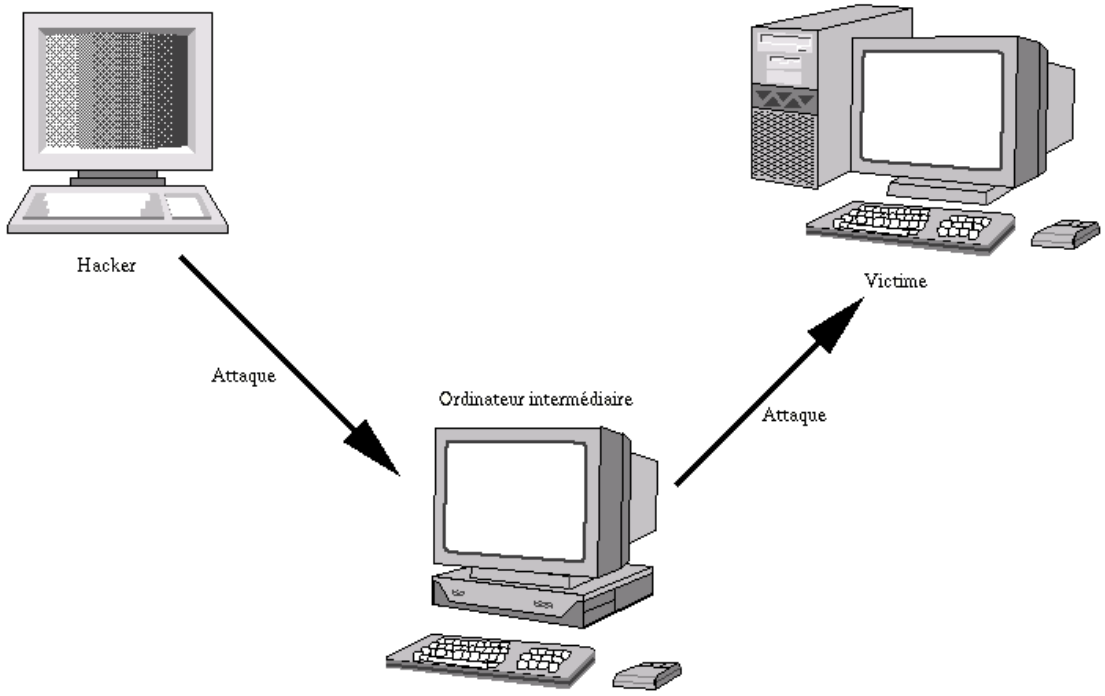
Si vous vous faites attaqués de la sorte, il y a de grandes chances pour que vous puissiez remonter à l'origine de l'attaque, identifiant par la même occasion l'identité de l'attaquant.

1.2.3 Les attaques indirectes par rebond

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

– Masquer l'identite (l'adresse IP) du hacker.
– Eventuellement, utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante...) pour attaquer.

Le principe en lui même, est simple : Les packets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où le terme de rebond.

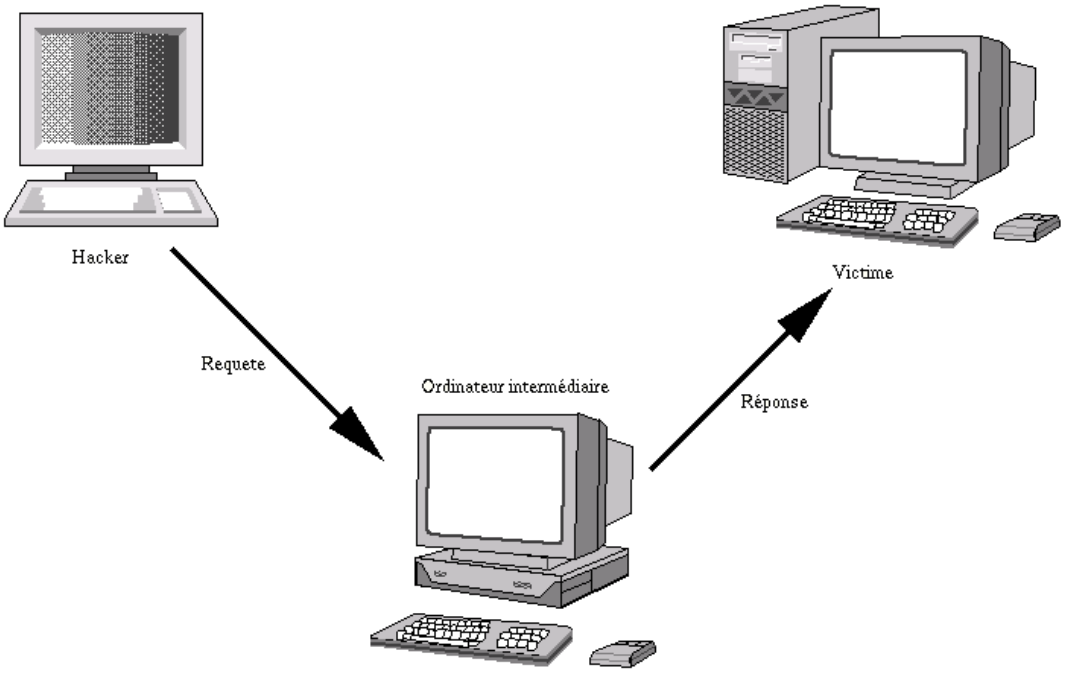


Attaque indirecte par rebond

L'attaque FTP Bounce fait partie de cette famille d'attaque. Si vous êtes victime de ce genre d'attaque, il n'est pas facile de remonter à la source. Au plus simple, vous remontrez à l'ordinateur intermédaire.

1.2.4 Les attaques indirectes par réponse

Cette attaque est un dérivé de l'attaque par rebond. Elle offre les même avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.



Attaque indirecte par réponse

Là aussi, il n'est pas aisé de remonter à la source...

1.2.5 Conclusion

Lorsque vous vous faites attaquer, cela peut se faire en direct ou via un ou plusieurs ordinateurs intermédiaires. Le fait de comprendre l'attaque va vous permettre de savoir comment remonter au hacker.

1.3 L'attaque +++ATHZero

1.3.1 Qu'est-ce que c'est ?

L'attaque +++ATH0 vise certains modems compatibles Hayes. Lorsque ce type de modem reçoit la commande +++ATH0, il risque de se déconnecter. En effet, cette commande permet de positionner le modem en commande manuelle. En pratique, cela se traduit par l'envoi d'un "Ping" contenant la chaîne de caractères "+++ATH0".

1.3.2 Conséquences

- Déconnexion du modem

1.3.3 Comment s'en protéger ?

- Pour les systèmes Win32, vous devez rechercher dans la base de registres la clé : HKEY_LOCAL_MACHINE\Sy et créer la chaîne "UserInit", ayant pour valeur "s2=255".
- Pour tous les autres systèmes, ajouter la commande "S2=255" dans la chaine d'initialisation du modem. Cela donne "ATZ ATS2=255&W". Cette commande ajoutée permet de désactiver la commande de mode manuel.

Si des problèmes persistent, jetez un oeil dans le manuel de votre modem.

1.4 L'attaque Boink

1.4.1 Qu'est-ce que c'est ?

L'attaque Boink vise les systèmes Win32. Elle est semblable à l'attaque Bonk. Elle consiste à envoyer des packets UDP corrompus sur tous les ports ouverts. L'ordinateur victime ne gère pas ces paquets et provoque un plantage.

1.4.2 Conséquences

Blocage système Crash système

1.4.3 Comment s'en protéger ?

Mettre à jour l'OS. Utilisation d'un firewall pour refuser les packets UDP corrompus.

1.5 L'attaque Cisco ® 7161

1.5.1 Qu'est-ce que c'est ?

Cela consiste à se connecter au port 7161 d'un routeur Cisco ® et d'envoyer un retour chariot. Le routeur peut alors planter.

1.5.2 Conséquences

Plantage du routeur Cisco ®.

1.5.3 Comment s'en protéger ?

Contactez Cisco ® pour obtenir une solution.

1.6 L'attaque Click - WinNewk

1.6.1 Qu'est-ce que c'est ?

Cette attaque vise tous les systèmes. Elle consiste à envoyer un message d'erreur ICMP (typiquement, ICMP inaccessible) à l'ordinateur cible ou au serveur auquel la victime est connectée. La victime risque alors d'être déconnectée du réseau ou du serveur.

1.6.2 Conséquences

Déconnexion

1.6.3 Comment s'en protéger ?

Configurer les firewall/routeurs pour gérer ces messages

1.7 Le Mail Bombing

1.7.1 Qu'est-ce que c'est ?

Le Mail Bonbing constite à envoyer un nombre faramineux d'emails (plusieurs milliers par exemple) à un ou des destinataires. L'objectif étant de :

- saturer le serveur de mails
- saturer la bande passante du serveur et du ou des destinataires,
- rendre impossible aux destinataires de continuer à utiliser l'adresse électronique.

1.7.2 L'attaque

Il est nécessaire pour l'auteur de l'attaque de se procurer un logiciel permettant de réaliser le mail bombing. Voici comment cela fonctionne

Exemple 1

- L'attaquant ici choisi différents options :
- l'adresse qu'il veut faire apparaître en tant qu'émetteur du message ;
- le sujet du message,
- le nombre de messages à envoyer, le serveur de mail à partir duquel les messages seront émis, (bien souvent si les administrateurs de serveurs mails ne se protègent pas assez, des serveurs "innocents" servent de relais sans le savoir, et le danger pour leurs propriétaires est de se retrouver "black listés" c'est à dire voir son fournisseur d'accès internet lui couper sa connection),
- le corps du message,
- l'adresse email de la victime.