|  |
| --- |
| Le hacking  |

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).

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.

Le hacking par l'exemple

Vous trouverez sur notre page de [Challenges de hacking](http://www.securiteinfo.com/attaques/hacking/challengeshacking.shtml) une liste des principaux sites qui organisent des défis intrusifs.

##  L'attaque +++ATHZero

**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".

**Conséquences :**

Déconnexion du modem

**Comment s'en protéger ?**

Pour les systèmes Win32, vous devez rechercher dans la base de registres la clé : HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Class\Modem\000 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.

|  |
| --- |
| L'attaque Boink  |

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.

Conséquences :

* Blocage système
* Crash système

Comment s'en protéger ?

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
| Les challenges de hacking  |

Qu'est-ce que c'est ?A travers la toile internet, on trouve un certain nombre de sites web qui proposent des défis intrusifs. La plupart sont multi-niveaux, et sont tellement diversifiés qu'ils touchent à une large palette de notions de sécurité. Leur but est unique : Se placer dans la peau d'un hacker et essayer d'atteindre un but. C'est souvent didactique :)Une remarque importante : Ces défis sont gratuits. Néanmoins, Securiteinfo.com décline toute responsabilité en ce qui concerne ces challenges. Les challenges

|  |  |  |
| --- | --- | --- |
| **Nom** | **Description** | **Hall Of Fame** |
| [Newbie Contest](http://newbiecontest.n0ne.org)  | Enfin un bon site français qui comporte plein de challenges :)  | Oui |
| [Mod x](http://www.mod-x.co.uk)  | Un site très réussi, ca se corse dès le début, mais les challenges sont plutôt sympas à faire : cryptage, java, cracking...  | Oui |
| [Sly FX](http://www.slyfx.com/main.html)  | Slyfx est un jeu constitué de 10 niveaux (chaque niveau étant lui meme découpé en 3 mini-challenges) qui font appel à la logique, au sens commun mais aussi bien sûr aux connaissances informatiques : javascript, reverse engineering, debug de sources, exploits...  | Oui |
| [NGSEC's challenges](http://quiz.ngsec.biz/)  | Une très bonne compilation de challenges basés sur l'authentification web... Ce site propose 2\*10 challenges d'une difficulté graduelle, ca se corse assez vite et il faut faire quelques recherches en parallèle si on veut progresser, pas facile donc mais très enrichissant ;) La deuxième série est au passage beaucoup plus complexe que la premiere !  | Oui |
| [Sers-Satura](http://sers.sourceforge.net/)  | Pas mal pompé sur cyberarmy (comme beaucoup des sites présentés ici), il reste néanmoins efficace et propose de nombreux challenges intéressants à faire. A mon sens un des sites qui a largement sa place ici !  | Oui |
| [Mindlock](http://mindlock.bestweb.net/challenges/)  | Proposé par un jeune de 16 ans, ce site vous invite à participer à des challenges du même type que HackQuest : 21 challenges orientés Javascript, cracking, stégano, programmation... Chaudement recommandé, interface classique mais propre  | Oui |
| [Try2Hack](http://www.try2hack.nl/)  | Des challenges plutôt sympathiques à faire avec comme d'habitude une difficulté croissante :) Du flash, du cracking d'applications... Dommage que le classement soit inexistant | Non |
| [HackQuest.com](http://www.hackquest.com/user.php)  | Un site bien conçu et agréable, des challenges variés et intéressants : programmation, crack, internet, logique, stéganographie, cryptographie, PHP, JAVA, Javascript, il y a du pain sur la planche.  | Oui |
| HackersLab  | Plutôt balaise et très technique mais réaliste ! A réserver aux spécialistes des buffers overflow et exploit en tout genre  | Oui |
| [Escape](http://www.angelfire.com/ne/warp/)  | Une succession de petits challenges, interface triste, peu intéressant et des pages introuvables au bout de quelques niveaux...  | Non |
| [SuPeR DuPeR HaCKiNG CHaLLeNGe](http://www.geocities.com/famousbruce/hackpage.html)  | 3 challenges à réserver aux newbies quand meme =)  | Non |
| [Security-challenge.com](http://www.security-challenge.com/)  | Des challenges en francais !  | Oui |
| [Area 6](http://www.area-6.net/?q=node/view/13)  | 3 petits challenges sympatiques  | Non |
| [Hiddenbunkerlabs](http://geocities.com/hiddenbunkerlabs/challenge.html)  | 5 challenges  | Non |
| [Fatetek Challenges](http://www.fatetek.net/challenges/index.html)  | Seulement 4 challenges, mais le site a l'air prometteur.  | Non |
| [HackThisSite](http://www.hackthissite.org/)  | 70 challenges (10 niveaux de difficultés). Vraiment excellent !  | Oui |
| [Alphanet](http://alph4net.free.fr/index_challenge.htm)  | 5 challenges.  | Oui |
| [Le Big Challenge](http://bigchallenge.free.fr)  | Votre mission consiste à trouver un fichier top-secret soigneusement dissimulé dans un endroit de Dark-city, la ville underground. A l'aide de ce fameux dossier, vous parviendrez à déjouer les plans machiavéliques de "strator" ! votre ennemi juré !!! Vous devrez franchir des étapes parsemées d'embûches, de pièges mais aussi d'indices.  | Oui |
| [Hack Doudou](http://hack.doudou.net/index.php)  | 8 défis à relever.  | Non |
| [Les Mondes de Hauzgur](http://www.hauzgur.com/challenges/en/index.html)  | 9 challenges de difficultés croissantes.  | Non |
| [SNSCrew](http://www.snscrew.net/site.php?main=challenges)  | 4 challenges en francais  | Non |
| [Xtreme-PC](http://gaetanpsg.free.fr/telechargement/divers/challenge/epreuves.html)  | 5 challenges plutôt sympatiques.  | Non |

RemarquesCette liste n'est pas exhaustive, aussi, n'hésitez pas à me contacter pour me soumettre tout challenge intéressant qui ne figurerai pas dans cette liste ou pour me faire part d'une remarque sur un challenge en particulier : webmaster@securiteinfo.com. Merci à ParadiseLost pour le travail effectué sur cette fiche. Au passage, j'en profite pour saluer les personnes qui m'ont contacté pour m'indiquer des mises à jour de leur site ou me faire part de nouveaux sites intéressants ;)  |

 |  |

 |
|

|  |
| --- |
| http://www.securiteinfo.com/gfx2/gauche_bas.gif |

 |
| L'ARP redirect  |

Qu'est-ce que c'est ?

L'attaque ARP redirect vise les réseaux locaux ethernet, qu'ils soient partitionnés ou non en sous-réseaux (switchés). C'est une technique de spoofing efficace bien que détectable dans les logs d'administration; elle consiste à s'attribuer l'adresse IP de la machine cible, c'est-à-dire à faire correspondre son adresse IP à l'adresse MAC de la machine pirate dans les tables ARP des machines du réseau. Pour cela il suffit en fait d'envoyer régulièrement des paquets ARP\_reply en broadcast, contenant l'adresse IP cible et la fausse adresse MAC. Cela a pour effet de modifier les tables dynamiques de toutes les machines du réseau. Celles-ci enverront donc leur trames ethernet à la machine pirate tout en croyant communiquer avec la cible, et ce de façon transparente pour les switches. De son côté, la machine pirate stocke le traffic et le renvoie à la vraie machine en forgeant des trames ethernet comportant la vraie adresse MAC (indépendament de l'adresse IP).
Cette technique est très puissante puisqu'elle opère au niveau ethernet, permettant ainsi de spoofer le traffic IP et même TCP (cela dépend entre autres des délais engendrés par la machine pirate). D'autre part, elle permet de contourner les barrières que constituent habituellement les switches (partitionnement de réseaux).

Conséquences :

* Compromissions
* DoS (cache poisoning), etc...

Comment s'en protéger ?

* Avoir des logs régulièrement mis à jour et étudiés.
* N'utiliser que des tables ARP statiques.
* Utiliser des logiciels spécialisés pour monitorer les paires IP/MAC.

|  |
| --- |
| Les buffers overflow  |

Qu'est-ce que c'est ?

Un buffer overflow est une attaque très efficace et assez compliquée à réaliser. Elle vise à exploiter une faille, une faiblesse dans une application (type browser, logiciel de mail, etc...) pour executer un code arbitraire qui compromettra la cible (acquisition des droits administrateur, etc...).

En bref

Le fonctionnement gébéral d'un buffer overflow est de faire crasher un programme en écrivant dans un buffer plus de données qu'il ne peut en contenir (un buffer est un zone mémoire temporaire utilisée par une application), dans le but d'écraser des parties du code de l'application et d'injecter des données utiles pour exploiter le crash de l'application.

Cela permet donc en résumé d'exécuter du code arbitraire sur la machine où tourne l'application vulnérable.

L'intérêt de ce type d'attaque est qu'il ne nécessite pas -le plus souvent- d'accès au système, ou dans le cas contraire, un accès restreint suffit. Il s'agit donc d'une attaque redoutable. D'un autre côté, il reste difficile à mettre en oeuvre car il requiert des connaissances avancées en programmation; de plus, bien que les nouvelles failles soient largement publiées sur le web, les codes ne sont pas ou peu portables. Une attaque par buffer overflow signifie en général que l'on a affaire à des attaquants doués plutôt qu'à des "script kiddies".

Technique

Le problème réside dans le fait que l'application crashe plutôt que de gérer l'accès illégal à la mémoire qui a été fait. Elle essaye en fait d'accéder (lire, exécuter) à des données qui ne lui appartiennent pas puisque le buffer overflow a décalé la portion de mémoire utile à l'application, ce qui a pour effet (très rapidement) de la faire planter.

D'un point de vue plus technique, la pile (stack en anglais) est une partie de la mémoire utilisée par l'application pour stocker ses variables locales. Nous allons utiliser l'exemple d'une architecture intel (32 bits). Lors d'un appel à une sous-routine, le programme empile (push) le pointeur d'instruction (EIP) sur la stack et saute au code de la sous-routine pour l'exécuter. Après l'exécution, le programme dépile (pop) le pointer d'instruction et retourne juste après l'endroit où a été appelée la sous-routine, grâce à la valeur d'EIP. En effet, comme EIP pointe toujours vers l'instruction suivante, lors de l'appel de la sous-routine il pointait déjà vers l'instruction suivante, autrement dit l'instruction à exécuter après la sous-routine (= adresse de retour).

D'autre part, lors de l'appel de la sous-routine, celle-ci va dans la majorité des cas créer sa propre pile dans la pile (pour éviter de gérer des adresses compliquées). Pour cela elle va empiler la valeur de la base de la pile (EBP) et affecter la valeur du pointeur de pile (ESP) à celle de la base (EBP).



* ESP est le pointeur du sommet de la pile.
* EBP est le pointeur de la base de la pile.
* EIP est le pointeur de la prochaine instruction à exécuter. Il pointe donc toujours une exécution en avance.

En résumé, on sauvegarde la valeur originale de la base et on décale le tout ensuite. Lors du retour de la sous-routine, on dépile EBP et réaffecte sa valeur originale pour restaurer la pile initiale.

Voici pour le déroulement "normal" des opérations. Un point intéressant à citer est le fait que dans notre architecture, les zones mémoires allouées dans la stack se remplissent dans le sens croissant des adresses (de 0..0H à F..FH) ce qui semble logique. Par contre, l'empilement sur la stack s'éffectue dans le sens décroissant! C'est-à-dire que l'ESB originale est l'adresse la plus grande et que le sommet est 0..0H. De là naît la possibilité d'écraser des données vitales et d'avoir un buffer overflow.
En effet, si notre buffer se trouve dans la pile d'une sous-routine et si nous le remplissons jusqu'à déborder sa taille allouée, nous allons écrire par-dessus les données qui se trouvent à la fin du buffer, c'est-à-dire les adresses qui ont été empilées précédement : EBP, EIP... Une fois la routine terminée, le programme va dépiler EIP et sauter à cette adresse pour poursuivre son exécution. Le but est donc d'écraser EIP avec une adresse différente que nous pourrons utiliser pour accéder à une partie de code qui nous appartient. (par exemple le contenu du buffer)
Un problème à ce stade est de connaitre l'adresse exacte de la stack (surtout sous Windows) pour pouvoir sauter dedans. On utilise généralement des astuces propres à chaque système (librairies, etc..) qui vont permettre -indirectement- d'atteindre notre stack et d'exécuter notre code. Cela nécessite un débogage intensif qui n'est pas à la portée de tout le monde...

Solutions

* Lors du développement : propreté du source (utiliser malloc/free le plus possible, utiliser les fonctions n comme strncpy pour vérifier les limites...), utilisation de librairies de développement spécialisée contre les buffers overflow ([Libsafe d'Avayalabs](http://www.research.avayalabs.com/project/libsafe/))
* Utiliser un langage n'autorisant pas ce type d'attaques : [Java](http://java.sun.com), [Cyclone](http://www.cs.cornell.edu/projects/cyclone/) (qui est issu du C).
* Utiliser des logiciels spécialisés dans la vérification de code source, comme par exemple le compilateur [StackGuard d'Immunix](http://immunix.org/stackguard.html), [Qaudit](http://downloads.securityfocus.com/tools/qaudit.pl) ou [Flawfinder](http://www.dwheeler.com/flawfinder/). [Article français sur Flawfinder](http://www.isecurelabs.com/article39.html)
* Auditer le programme compilé à l'aide d'outils tels que [BFBTester](http://bfbtester.sourceforge.net/). [Article français sur BFBTester](http://www.isecurelabs.com/article64.html)
* Appliquer le plus rapidement possible les patches fournis par les développeurs.
* Fiabiliser l'OS pour qu'il ne soit pas vulnérable aux debordement de buffer, par exemple : [grsecurity](http://www.grsecurity.net/) pour Linux.

|  |
| --- |
| Les trous de sécurité applicatifs.  |

Qu'est-ce que c'est ?

Un trou de sécurité applicatif est le résultat d'un fonctionnement anormal d'une application. Il en résulte un plantage de l'application, ou bien un état non stable. Concrètement, il s'agit de trouver un fonctionnement que n'a pas prévu le programmeur. De ce fait, il est parfois possible d'en exploiter des failles. Cela devient très interessant lorsque c'est un programme réseaux (client/serveur, mail, www, architecture distribuée...). Ce type d'attaque peut être utilisée en local (pour obtenir l'accès root) ou à distance pour s'introduire dans un réseau, ou planter à distance un serveur.

Qui peut provoquer cette attaque ?

Un bon programmeur, qui a la connaissance d'un trou de sécurité, peut créer un programme qui va exploiter cette faille. Certains programmes existent déjà et exploitent les trous de sécurité les plus courants. Dans ce cas, n'importe qui est en mesure de pénétrer un réseau mal sécurisé.

Conséquences :

 Obtention de l'accès root en local.

 Intrusion de réseaux ou d'ordinateur.

 Plantage à distance un serveur.

Comment s'en protéger ?

 Se tenir au courant des logiciels qui comportent des failles. Quelques site web sont spécialisés dans ce domaine.

 Utiliser périodiquement un logiciel dédié à la surveillance du parc logiciel. Lorsqu'une version non fiable d'un logiciel est installée sur un poste, un message de mise en garde est affiché. Ce type de logiciel est disponible sur ce site web. Il s'appelle **Securitor**. Vous pouvez le trouver [ici](http://www.securiteinfo.com/outils/securitor.shtml).

|  |
| --- |
| L'attaque Tear Drop  |

Qu'est-ce que c'est ?

L'attaque Tear Drop vise les systèmes Win32 et Linux inférieur à 2.0.32. Elle consiste à envoyer des packets TCP qui se recouvrent. Lorsque l'ordinateur victime reçoit ces packets, il tente de les reconstruire. N'y arrivant pas, cela provoque un plantage.

Conséquences :

* Blocage système
* Crash système

Comment s'en protéger ?

* Mettre à jour l'OS.
* Utilisation d'un firewall pour refuser les packets qui se recouvrent.

|  |
| --- |
| L'attaque UDP 0  |

Qu'est-ce que c'est ?

Cela consiste à envoyer une trame UDP vers le port zéro d'un ordinateur distant. L'ordinateur cible peut alors planter. Si celui-ci est derrière un firewall, le firewall peut éventuellement planter.

Conséquences :

* Plantage système.
* Plantage du firewall.

Comment s'en protéger ?

* Vérifiez que le firewall que vous utilisez gère correctement cette attaque.
* Bloquez les trames ayant un port de destination égal à zéro.

|  |
| --- |
| Le DNS Spoofing |

Qu'est-ce que c'est ?

L'objectif de cette attaque est de rédiriger, à leur insu, des Internautes vers des sites pirates. Pour la mener à bien, le pirate utilise des faiblesses du protocole DNS (Domain Name System) et/ou de son implémentation au travers des serveurs de nom de domaine. A titre de rappel, le protocole DNS met en oeuvre les mécanismes permettant de faire la correspondance entre une adresse IP et un nom de machine (ex.: www.truc.com). Il existe deux principales attaques de type DNS Spoofing : le DNS ID Spoofing et le DNS Cache Poisoning. Concrètement, le but du pirate est de faire correspondre l'adresse IP d'une machine qu'il contrôle à un nom réel et valide d'une machine publique.

Description de l'attaque

DNS ID Spoofing

Si une machine A veut communiquer avec une machine B, la machine A a obligatoirement besoin de l'adresse IP de la machine B. Cependant, il se peut que A possède uniquement le nom de B. Dans ce cas, A va utiliser le protocole DNS pour obtenir l'adresse IP de B à partir de son nom.
Une requête DNS est alors envoyée à un serveur DNS, déclaré au niveau de A, demandant la résolution du nom de B en son adresse IP. Pour identifier cette requête une numéro d'identification (en fait un champs de l'en-tête du protocole DNS) lui est assigné. Ainsi, le serveur DNS enverra la réponse à cette requête avec le même numéro d'identification. L'attaque va donc consister à récupérer ce numéro d'identification (en sniffant, quand l'attaque est effectuée sur le même réseau physique, ou en utilisant une faille des systèmes d'exploitation ou des serveurs DNS qui rendent prédictibles ces numéros) pour pouvoir envoyer une réponse falsifiée avant le serveur DNS. Ainsi, la machine A utilisera, sans le savoir, l'adresse IP du pirate et non celle de la machine B initialement destinatrice. Le schéma ci-dessous illustre simplement le principe du DNS ID Spoofing.



DNS Cache Poisoning

Les serveurs DNS possèdent un cache permettant de garder pendant un certain temps la correspondance entre un nom de machine et son adresse IP. En effet, un serveur DNS n'a les correspondances que pour les machines du domaine sur lequel il a autorité. Pour les autres machines, il contacte le serveur DNS ayant autorité sur le domaine auquel appartiennent ces machines. Ces réponses, pour éviter de sans cesse les redemander aux différents serveurs DNS, seront gardées dans ce cache. Le DNS Cache Poisoning consiste à corrompre ce cache avec de fausses informations. Pour cela le pirate doit avoir sous son contrôle un nom de domaine (par exemple fourbe.com) et le serveur DNS ayant autorité sur celui-ci ns.fourbe.com. L'attaque se déroule en plusieurs étapes :

* Le pirate envoie une requête vers le serveur DNS cible demandant la résolution du nom d'une machine du domaine fourbe.com (ex.: www.fourbe.com)
* Le serveur DNS cible relaie cette requête à ns.fourbe.com (puisque c'est lui qui a autorité sur le domaine fourbe.com)
* Le serveur DNS du pirate (modifié pour l'occasion) enverra alors, en plus de la réponse, des enregistrements additionnels (dans lesquels se trouvent les informations falsifiées à savoir un nom de machine publique associé à une adresse IP du pirate)
* Les enregistrements additionnels sont alors mis dans le cache du serveur DNS cible
* Une machine faisant une requête sur le serveur DNS cible demandant la résolution d'un des noms corrompus aura pour réponse une adresse IP autre que l'adresse IP réelle associée à cette machine.

Comment s'en protéger ?

* Mettre à jour les serveurs DNS (pour éviter la prédictibilité des numéros d'identification et les failles permettant de prendre le contrôle du serveur)
* Configurer le serveur DNS pour qu'il ne résolve directement que les noms des machines du domaine sur lequel il a autorité
* Limiter le cache et vérifier qu'il ne garde pas les enregistrements additionnels.
* Ne pas baser de systèmes d'authentifications par le nom de domaine : Cela n'est pas fiable du tout.

|  |
| --- |
| Le Mail Bombing  |

Qu'est-ce que c'est ?

Le Mail Bombing consiste 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.

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 connexion),
* **le corps** du message,
* **l'adresse email** de la victime.

Exemple 2



Cet outil est aussi intuitif que le précédent. Cependant il semble nettement plus dangereux. En effet, la possibilité d'attacher une pièce jointe est une sérieuse menace, puisqu'elle permet à l'expéditeur d'insérer virus et troyens dans les messages. Une fois de plus, rappelons qu'il faut impérativement éviter d'ouvrir une pièce jointe ayant pour extension .com, .bat, .pif ou .exe...

Comment réagir ?

Evitez cette attaque

Avant de prendre le risque d'avoir une adresse électronique inutilisable mieux vaut prendre ses précautions :

* Si vous avez une adresse personnelle à laquelle vous tenez, ne la communiquez qu'aux personnes dignes de confiance,
* Créez vous un second compte de messagerie, pour tout ce qui est mailing list par exemple et groupe des discussion, ainsi, vous ne craignez pas de perdre d'informations vitales. Si ce compte est attaqué vous pourrez sans difficulté reprendre une autre adresse et vous ré-abonner.
* Utilisez [eremove](http://www.securiteinfo.com/download/eremove.zip) pour éviter les mail bombers.

Lorsque vous lancez l'installation du programme vous retrouvez cet écran :



Vous allez maintenant pouvoir commencer la configuration en tapant sur next.



Ici, vous devez rentrer les identifiants de votre messagerie, votre mot de passe, le serveur de votre FAI ainsi que le port utilisé (par défaut c'est généralement le 110). Pour les personnes disposant de plusieurs comptes de messagerie différents, il est nécessaire de passer par le mode avancé de configuration. Cliquer sur "Advance" vous amène aux écrans suivants :







L'onglet Account permet de donner les indications sur tous les comptes de messagerie que vous souhaitez protéger. A chaque fois que vous cliquez sur Add vous trouverez un écran similaire à celui que vous avez vu pour votre compte principal. Vous pouvez entrer autant de comptes que vous le désirez.

L'onglet Programs vous permet de déterminer quel est le type de Boîte aux Lettres que vous utilisez (Eudora, Outlook, etc ...).

L'onglet Others vous permet de déterminer si le programme se connecte directement à votre boite aux lettres à son lancement. Vous pouvez aussi spécifier un fichier de logs



Lorsque vous lancez eremove, le programme vous montre le nombre de messages, ainsi que la taille de chacun et l'émetteur. Il vous suffit ensuite de sélectionner le ou les messages que vous ne souhaitez pas recevoir et ils seront directement détruits sur le serveur de messagerie.





Vous pouvez au préalable vérifier le contenu du message en faisant un clic gauche avec la souris sur le message. Cela vous donnera des éléments sur le corps du message et sur l'expéditeur.

Vous avez été attaqué :

Si vous avez été victime d'un mail bombing, il est parfois possible de remonter jusqu'à l'émetteur.
En effet, il existe des informations dans chaque message qui donnent des informations sur leur auteur.
Voici un exemple de propriétés de message :

* Return-Path: <eyrill@hotmail.com> *Ici vous trouvez l'email de l'émetteur*
* Received: from hotmail.com (f88.law14.hotmail.com [64.4.21.88]) by servertoto.pourexemplejenevaispsvousmonserveur.net (8.9.3/8.9.3-NoSpam-Rbl-ORBS) with ESMTP id PAA19370 *Ici vous trouvez le serveur par lequel l'attaquant à envoyé les messages. Si la personne débute il se peut que ce serveur soit réel et il vous faut vous rapprocher de son propriétaire pour vous plaindre.*
* For commercial@securiteinfo.com; Sat, 22 Dec 2001 15:45:34 +0100 *Ici vous trouvez normalement votre adresse de messagerie ainsi que des indications horaires*

Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
Sat, 22 Dec 2001 06:33:00 -0800
Received: from XXX.XXX.XXX.XXX by lw14fd.law14.hotmail.msn.com with HTTP;
Sat, 22 Dec 2001 14:33:00 GMT
* X-Originating-IP: [XXX.XXX.XXX.XXX] *Ici vous trouvez les indications sur l'IP d'où sont partis les messages. Attention, il est possible mais assez rare que l'adresse IP soit modifiée*
* From: "Eyrill ROMOS" <eyrill@hotmail.com> *De nouveau l'émetteur*
* To: <commercial@securiteinfo.com> *De nouveau le destinataire*
* Subject: =?iso-8859-1?B?UHJvcHJp6XTpcyBkJ3VuIG1lc3NhZ2Ug?= *Le sujet du message encodé*
* Date: Sat, 22 Dec 2001 15:33:00 +0100 *Date et heure*
* Mime-Version: 1.0 *Version Mime utilisée pour l'encodage du message*
* Content-Type: text/plain; charset=iso-8859-1; format=flowed *Type de contenu*
* Message-ID: <F88lyg35sQtgTIFprhM000098e1@hotmail.com> *Identifiant interne du message*
* X-OriginalArrivalTime: 22 Dec 2001 14:33:00.0561 (UTC) FILETIME=[8E825010:01C18AF5] *Heure et date d'arrivée du message*

Si vous retrouvez des informations comme l'adresse email ou le serveur qui ont permis l'arrivée des messages, il est important de se plaindre auprès du fournisseur d'accès. En effet, dans la plupart des cas les fournisseurs d'accès n'apprécient pas ce type de procédés via leurs serveurs et prennent toutes les mesures nécessaires pour empêcher les auteurs de recommencer.

Conclusion

Le mail bombing n'est, à priori, pas illégal. Il n'existe pas de limite légale déterminant le nombre maximum de messages à envoyer à un internaute. Cependant, les fournisseurs d'accès à Internet n'apprécient pas ce type de procédés. En effet, cela leur cause des soucis de bande passante et la saturation de leurs serveurs de messagerie. En conséquence, n'hésitez surtout pas à les solliciter si vous êtes victime d'une telle attaque. Ils réagissent généralement rapidement pour éviter que leurs abonnés recommencent. Par ailleurs, prendre le temps d'installer eremove est indispensable si l'on désire éviter tout soucis et ne pas se retrouver contraint à changer d'adresse électronique. Une fois installé vous pouvez en toute quiétude ne plus craindre les attaques par mail bombing :o) !!!

|  |
| --- |
| Le FTP Bounce  |

Qu'est-ce que c'est ?

Le FTP Bounce signifie Rebond FTP. C'est un cas de spoofing d'adresse IP. Cette technique est ancienne et ne devrait plus être d'actualité.
Cette technique est en accord avec les RFC, ce qui fait une cible potentielle de tous les serveurs FTP. Elle est basée sur une utilisation de la commande PORT du protocole FTP lorsque le serveur FTP est en mode actif. En effet, cette commande permet de se connecter à n'importe quel autre serveur distant, et à un port donné. Dans ce cas, il est possible que la sécurité du serveur cible soit compromis, dans le cas ou il effectue une vérification des adresses IP d'orinigine. En effet, l'adresse IP que le serveur cible verra sera l'adresse IP du serveur FTP, et non de l'adresse IP de l'attaquant.

Ce petit schéma explique la technique utilisée :



Conséquences :

* Vol d'identité
* Permet d'accéder à des données confidentielles lorsque le serveur filtre les adresses IP entrantes.

Comment s'en protéger ?

* Dû au fait que l'attaque est compatible avec le protocole (cf RFC), la politique de sécurité peut-être variable selon les implémentations.
* Nous suggérons de supprimer la commande PORT sauf dans le cas ou celle-ci est utilisée vers le client d'origine (celui qui a demandé la connexion FTP).

|  |
| --- |
| Les attaques WinArp - Poink  |

Qu'est-ce que c'est ?

Deux noms sont donnés pour une même attaque : WinArp et Poink. Elle vise les systèmes Win32. Elle consiste à envoyer plusieurs packets ARP à l'ordinateur victime. Pour chaque packet ARP reçu, Windows affiche une boite de message avec un bouton "Ok". Imaginez si plusieurs milliers de packets ARP sont envoyés à la cible... L'origine de l'attaquant est connue car l'adresse MAC est à l'intérieur du packet ARP.

Conséquences :

* Ralentissement système
* Consommation des ressources systèmes

Comment s'en protéger ?

* Pas de solutions connue.

|  |
| --- |
| L'attaque WINS 53 flood  |

Qu'est-ce que c'est ?

Cette attaque vise les systèmes WinNT qui exécutent le service WINS (Windows Internet Name Service). Elle consiste à envoyer un flot de packets aléatoires en taille et en contenu au port 53 (DNS) de l'ordinateur cible. Le serveur peut alors se planter.

Conséquences :

* Crash système

Comment s'en protéger ?

* Installer le service pack 4.

|  |
| --- |
| L'attaque SMTPd overflow  |

Qu'est-ce que c'est ?

Cela consiste à envoyer la commande "HELP" avec un argument trop long vers un serveur SMTP. Si le gestionnaire SMTP n'est pas patché pour prévenir de cette attaque, il plante.

Conséquences :

* Plantage du démon SMTP.
* Impossibilité d'envoyer ou recevoir un mail.

Comment s'en protéger ?

* Pour les démons qui ne supportent pas une commande "HELP" trop longue, il existe certainement un patch. Mettre à jour votre démon SMTP.

|  |
| --- |
| L'attaque sPing - Jolt - IceNewk  |

Qu'est-ce que c'est ?

Cette attaque, qui comporte trois noms différents, visent les systèmes Win32. Elle consiste à envoyer un très grand nombre de packets ICMP très fragmentés à l'ordinateur victime. Les conséquences sont diverses : Les systèmes Win32 ont beaucoup de mal à s'y retrouver dans la défragmentation des packets.

Conséquences :

* Blocage système.
* Etc...

Comment s'en protéger ?

* WinNT 4.0 : Installer le service Pack 3 + patch ICMP.
* WinNT 3.51 : Installer le service Pack 5 + patch ICMP.
* Win95 : Installer le patch ICMP.

|  |
| --- |
| L'attaque "Smurf"  |

Qu'est-ce que c'est ?

C'est un ping flooding un peu particulier. C'est une attaque axée réseaux, faisant partie de la grande famille des Refus De Service (DOS : Denial Of Service).
Ce procédé est décomposé en deux étapes:

* La première est de récupérer l'adresse IP de la cible par spoofing.
* La seconde est d'envoyer un flux maximal de packets ICMP ECHO (ping) aux adresses de Broadcast. Chaque ping comportant l'adresse spoofée de l'ordinateur cible.

Si le routeur permet cela, il va transmettre le broadcast à tous les ordinateurs du réseau, qui vont répondre à l'ordinateur cible. La cible recevra donc un maximum de réponses au ping, saturant totalement sa bande passante...
Bien entendu, plus de réseau comporte de machines, plus c'est efficace...

Conséquences :

* Perte de la bande passante
* Ralentissement système
* Perte du réseau
* Blocage système
* Crash système

Comment s'en protéger ?

* Configurer le firewall pour filtrer les packets ICMP echo ou les limiter à un pourcentage de la bande passante.
* Configurer le routeur pour désactiver le broadcast.

|  |
| --- |
| Les attaques Smack - Bloop  |

Qu'est-ce que c'est ?

Ces attaques visent tous les systèmes. Elles ressemblent à l'attaque Click : Elles consistent à envoyer des messages d'erreur ICMP (typiquement, ICMP inaccessible) à l'ordinateur cible. Mais, ces attaques n'ont pas pour but de déconnecter l'ordinateur victime. Elles provoquent un flood qui visent les transferts dits connectés (FTP, IRC, telnet, ICQ, ...).

Conséquences :

* Ralentissement des transferts connectés.
* Déconnexion des transferts connectés.

Comment s'en protéger ?

* Configurer les firewalls/routeurs pour gérer ces messages.

|  |
| --- |
| L'attaque Pong  |

Qu'est-ce que c'est ?

L'attaque "Pong" est aussi connue sous le nom d'"Echo Reply Without Request" ou "ICMP echo reply attack". Elle consiste à envoyer à l'ordinateur victime le résultat d'un Ping (autrement dit, un Pong), alors que la victime n'a pas envoyé de Ping.

Conséquences :

* **Détermination de l'architecture réseau derrière un firewall.** En effet, la plupart des firewall laissent passer les requêtes ping/pong. Si un routeur reçoit un pong à destination d'un ordinateur qui n'existe pas, il renverra un message "ordinateur inexistant (host unreachable)" à l'envoyeur, c'est à dire à l'attaquant. L'attaquant pourra donc déterminer le nombre de machines derrière le firewall, et plus encore, il aura les adresses IP de ces ordinateurs.
* **Communication avec un cheval de Troie**. Les requêtes ICMP passant sans problème par les firewalls, certains chevaux de Troie utilisent ces trames pour signaler leur présence.
* **Attaques distribuées**. Les requêtes ICMP passant sans problèmes par les firewalls, une attaque par abondance de requêtes Pong (type "flooding") permet de saturer un routeur ou un ordinateur derrière un firewall.
* **Attaques "spoofed"**. Une attaque par ping flooding peut se produire contre un ordinateur en simulant que ces pings viennent de votre ordinateur (de votre adresse IP). Vous recevez donc uniquement les pongs provenant de l'ordinateur victime de l'attaque.

Comment s'en protéger ?

* Utilisation d'un firewall pour enregistrer les pongs reçus alors qu'il n'y a pas eu de pings envoyés.

|  |
| --- |
| L'attaque Snork  |

Qu'est-ce que c'est ?

L'attaque Snork vise les systèmes WinNT. Elle consite à envoyer une trame UDP provenant du port 7 (Echo), 19 (Chargen) ou 135, et ayant pour destination le port 135 (Microsoft Location Service). Si les services sont lancés, cela a pour conséquence d'établir une communication de durée infinie, et génère des trames non nécessaires. Cela réduit considérablement la bande passante et la puissance CPU.

Conséquences :

* Ralentissement système
* Perte de bande passante

Comment s'en protéger ?

* Configurer les routeurs et firewalls pour bloquer les packets UDP ayant une destination de port 135 et ayant un port source de 7,19 ou 135 et qui proviennent de l'extérieur de votre réseau.
* Microsoft a fourni un patch.

|  |
| --- |
| L'attaque par requête HTTP incorrecte  |

Qu'est-ce que c'est ?

Cette attaque vise tous les systèmes, y compris IIS. Elle consiste à envoyer une requête HTTP déformée vers le site web cible. Le serveur peut alors se planter.
Cette attaque à cette forme :

GET / HTTP/1.0

hostname: aaaaaaaaaaaa... (256 octets)
hostname: aaaaaaaaaaaa... (256 octets)
... 10,000 lignes ...
hostname: aaaaaaaaaaaa... (256 octets)

Conséquences :

* Crash système, plantage du site web

Comment s'en protéger ?

* Mettre à jour votre serveur web.

|  |
| --- |
| Ping flooding  |

Qu'est-ce que c'est ?

Ce procédé consiste à envoyer un flux maximal de ping vers une cible.

Qui peut provoquer cette attaque ?

N'importe qui, du moment qu'il a un logiciel permettant de le faire.
Plus il a de personnes qui font un ping flooding vers une cible, et plus la situation devient critique pour cette cible..

Conséquences :

Ralentissement système
Blocage système
Crash système

Comment s'en protéger ?

Utilisation d'un firewall.

|  |
| --- |
| Ping of death  |

Qu'est-ce que c'est ?

Un ping a normalement une longueur maximale de 65535 ((2 exp 16) - 1) octets, incluant une entête de 20 octets. Un ping of death c'est un ping qui a une longueur de données supérieure à la taille maximale. Lors de sont envoi, le ping of death est fragmenté en packets plus petits. L'ordinateur victime qui reçoit ces packets doit alors les reconstruirent. Certains systèmes ne gèrent pas cette fragmentation, et se bloquent, ou crashent complètement. D'où le nom de cette attaque.

Qui peut provoquer cette attaque ?

N'importe qui, du moment qu'il a un logiciel permettant de le faire.

Conséquences :

* Crash système.
* Blocage système.

Comment s'en protéger ?

* Mettre à jour l'OS.
* Effectuer un test avant que quelqu'un d'autre le fasse à votre place. Si le système réagit correctement, il n'y a pas de problème.

|  |
| --- |
| L'attaque Oshare  |

Qu'est-ce que c'est ?

L'attaque Oshare vise tous les systèmes. Elle consiste à envoyer une entête IP invalide à la victime. Cette entête IP est rendue invalide en jouant sur la valeur des champs de l'entête qui spécifient la longueur du datagramme. Ce sont les champs "IHL" (mot de 32 bits indiquant la longueur du header) et "Total lenght" (mot de 16 bits indiquant la longueur du datagramme en octets, entête comprise), qui sont modifiés pour cette attaque. Les conséquences sont multiples : Elles dépendent du hardware de la carte réseau. Néanmoins, cette attaque ne peut porter que sur le même sous réseau. En effet, ces packets invalides (somme de contrôle IP incorrect dû à la mauvaise longueur du datagramme), ne peuvent passer les routeurs.

Conséquences :

* Déconnexion du réseau
* Ralentissement système
* Blocage système
* Plantage système

Comment s'en protéger ?

* Protection inconnue.

|  |
| --- |
| L'attaque NT Stop  |

Qu'est-ce que c'est ?

L'attaque NT Stop vise les systèmes WinNT 4.0. Elle consiste à envoyer une requête SMB logon avec une taille spécifiée incorrecte. L'ordinateur victime génère une corruption de mémoire causant une erreur "STOP 0x0000000A" ou "STOP 0x00000050" et provoque un plantage.

Conséquences :

* Blocage système
* Crash système
* Reboot système

Comment s'en protéger ?

* Mettre à jour l'OS.

|  |
| --- |
| Land attack  |

Qu'est-ce que c'est ?

C'est une attaque axée réseaux, faisant partie de la grande famille des Refus De Service (DOS : Denial Of Service). Les systèmes visés sont Win32.
Ce procédé est décomposé en trois étapes:

* La première est de récupérer l'adresse IP de la cible par spoofing.
* La seconde est de scanner tous les ports ouverts de l'ordinateur victime.
* La dernière est d'envoyer un packet à chaque port ouvert. Mais ces packets ont deux caractéristiques : Ils ont le flag SYN positionné, et les adresses source et destination du packet est la même : Celle de l'ordinateur cible.


*Un exemple de paquet Land.*

Conséquences :

En fonction du système d'exploitation, et de la gestion de la couche TCP/IP, les conséquences sont différentes :

* Blocage système
* Crash système
* Consomation 100% CPU
* Perte des couches réseaux

Les systèmes d'exploitation vulnérables sont :

AIX 3
AmigaOS AmiTCP 4.2 (Kickstart 3.0)
BeOS Preview Release 2 PowerMac
BSDI 2.0
BSDI 2.1 (vanilla)
Digital VMS ???
FreeBSD 2.2.5-RELEASE
FreeBSD 2.2.5-STABLE
FreeBSD 3.0-CURRENT
HP External JetDirect Print Servers
IBM AS/400 OS7400 3.7
IRIX 5.2
IRIX 5.3
MacOS MacTCP
MacOS 7.6.1 OpenTransport 1.1.2
MacOS 8.0
NetApp NFS server 4.1d
NetApp NFS server 4.3
NetBSD 1.1
NetBSD 1.2
NetBSD 1.2a
NetBSD 1.2.1
NetBSD 1.3\_ALPHA
NeXTSTEP 3.0
NeXTSTEp 3.1
Novell 4.11
OpenVMS 7.1 with UCX 4.1-7
QNX 4.24
Rhapsody Developer Release
SCO OpenServer 5.0.2 SMP
SCO OpenServer 5.0.4
SCO Unixware 2.1.1
SCO Unixware 2.1.2
SunOS 4.1.3
SunOS 4.1.4
Windows 95 (vanilla)
Windows 95 + Winsock 2 + VIPUPD.EXE
Windows NT (vanilla)
Windows NT + SP3
Windows NT + SP3 + simptcp-fix

Les équipements vulnérables sont :

3Com SuperStack II Switch 1000
Apple LaserWriter
BinTec BIANCA/BRICK-XS 4.6.1 router
Cisco Classic IOS < 10.3, early 10.3, 11.0, 11.1, and 11.2
Cisco IOS/700
Cisco Catalyst
Digital VT1200
HP Envizex Terminal
Livingston Office Router (ISDN)
Livingston T1/E1 OR
Milkyway Blackhole Firewall 3.0 (SunOS)
Milkyway Blackhole Firewall 3.02(SunOS)
NCD X Terminals, NCDWare v3.1.0
NCD X Terminals, NCDWare v3.2.1
Netopia PN440 v2.0.1

Comment s'en protéger ?

* Configurer le firewall ou le routeur pour filtrer les packets qui ont la même adresse IP en source et destination, sur tous les ports.
* Mettre à jour son système d'exploitation.

|  |
| --- |
| L'attaque Out Of Band (OOB)  |

Qu'est-ce que c'est ?

L'attaque OOB est plus connue sous le nom de "Nuke". Elle est courante, car il y a de nombreux "utilitaires" qui permettent d'exploiter la faille. Les systèmes visés sont Win32. Le port visé est le 139 (Netbios Session Service port). Lorsqu'un packet est envoyé sur le port 139 avec le flag "Urgent", Win95/NT/3x attend des données qui doivent suivre le flag. S'il n'y a pas de données qui arrivent, le système ne sait pas gérer cette absence...

Conséquences :

* Ecran bleu de la mort
* Perte de la connexion internet
* Blocage système
* Crash système

Comment s'en protéger ?

* Win95 : Mettre à jour Winsock avec la version 2.
* Win NT 3.51 : Installer le service pack 5 + le patch oob-fix.
* Win NT 4.0 : Installer le service pack 4.
* Utilisation d'un firewall et blocage du port 139.
* Utilisation d'un écouteur des ports du système.

|  |
| --- |
| Le Déni de Service Distribué (DDoS)  |

Background

Le "Distributed denial-of-service" ou déni de service distribué est un type d'attaque très évolué visant à faire planter ou à rendre muette une machine en la submergeant de trafic inutile (voir fiche DoS). Plusieurs machines à la fois sont à l'origine de cette attaque (c'est une attaque distribuée) qui vise à anéantir des serveurs, des sous-réseaux, etc. D'autre part, elle reste très difficile à contrer ou à éviter. C'est pour cela que cette attaque représente une menace que beaucoup craignent.

Les outils

Pour mieux comprendre le phénomène, il parait impossible de ne pas étudier les outils les plus importants dans ce domaine, qui doivent leur notoriété à des célèbres attaques ayant visé des grands sites sur le net.

Un réseau typique se compose donc d'un maître (point central) et de nombreux hôtes distants, encore appelés démons. Pendant le déroulement de l'attaque, le hacker se connecte au maître qui envoie alors un ordre à tout les hôtes distants (via UDP, TCP ou ICMP). Ces communications peuvent également dans certains cas être chiffrées. Ensuite, les hôtes distants vont attaquer la cible finale suivant la technique choisie par le hacker. Ils vont par exemple se mettre à envoyer un maximum de paquets UDP sur des ports spécifiés de la machine cible. Cette masse de paquets va submerger la cible qui ne pourra plus répondre à aucune autre requête (d'où le terme de déni de service). D'autres attaques existent, tel que l'ICMP flood, le SYN flood (TCP), les attaques de type smurf, les attaques dites furtives, les attaques de déni de service dites agressives (dont le but est bel et bien de faire crasher complètement la cible), ou encore des attaques de type "stream attack" (TCP ACK sur des ports au hasard)...
Certains outils se sont même inspiré des chevaux de Troie (voir fiche sur les [chevaux de Troie](http://www.securiteinfo.com/attaques/divers/troie.shtml)) qui installent de petits serveurs irc permettant au hacker de les commander via cette interface.

Mode opératoire

Les DDoS se sont démocratisées depuis 2-3 ans. En effet dans les premiers temps, cette attaque restait assez compliquée et nécessitait de bonnes connaissances de la part des attaquants; mais ceux-ci ont alors développé des outils pour organiser et mettre en place l'attaque. Ainsi le processus de recherche des hôtes secondaires (ou zombies) a été automatisé. On cherche en général des failles courantes (buffer overflows sur wu-ftpd, les RPCs...) sur un grand nombre de machines sur Internet et l'attaquant finit par se rendre maître (accès administrateur) de centaines voir de milliers de machines non protégées. Il installe ensuite les clients pour l'attaque secondaire et essaye également d'effacer ses traces (corruption des fichiers logs, installation de rootkits). Une fois le réseau en place, il n'y a plus qu'à donner l'ordre pour inonder la victime finale de paquets inutiles.
Il est intéressant de noter que les victimes dans ce type d'attaques ne sont pas que celles qui subissent le déni de service; tous les hôtes secondaires sont également des machines compromises jusqu'au plus haut niveau (accès root), tout comme l'hôte maître.
La menace provient du fait que les outils automatisant le processus ont été très largement diffusés sur Internet. Il n'y a plus besoin d'avoir des connaissances pointues pour la mettre en place, il suffit de "cliquer" sur le bouton.

Contre-mesures

Il n'est pas évident de se prémunir contre ces attaques par déni de service, car la mise en place du réseau offensif par l'attaquant repose sur le fait que beaucoup de machines sont peu ou pas sécurisée et présentent des failles. Ces failles sont tellement nombreuses et d'autre part il existe tellement de machines vulnérables sur Internet qu'il devient impossible d'empêcher de telles attaques.
Ainsi, si un outil de DDoS est détecté sur un système, cela signifie sûrement que il a été installé sur de nombreux autres systèmes sans être décelé. D'autre part, la présence de cet outil signifie également que le système a été intégralement compromis, qu'il présente sûrement des backdoors et qu'on y a peut-être installé un rootkit (type Adore). Il est donc urgent et nécessaire de retirer complètement cette machine du réseau et de l'inspecter pour éventuellement la réinstaller.

Pour détecter un tel outil, on pourra chercher des noms évocateurs parmi les processus système s'il n'y a pas de rootkit installé et si l'attaquant à laissé un nom par défaut. Ces noms peuvent être regroupés dans la liste suivante (non exhaustive):

Trinoo maître: master
Broadcast: ns

TFN client: tfn
Démon: td

Stacheldraht Handler: mserv
Agent: td

Shaft Handler: shaftmaster
Agent: shaftnode

mstream Handler: master
Agent: server

Trinity Agent: /usr/lib/idle.so
Portshell: /var/spool/uucp/uucico
Alt. Portshell: /var/spool/uucp/fsflush

Il peut être également fort utile de connaître les outils (au nombre de 4, principalement) utilisés par les hackers. Des analyses sont disponibles pour 3 d'entres eux :

* <http://staff.washington.edu/dittrich/misc/trinoo.analysis>
* <http://staff.washington.edu/dittrich/misc/tfn.analysis>
* <http://staff.washington.edu/dittrich/misc/stacheldraht.analysis>

Il existe également un compte-rendu de congrès scientifique sur le sujet qui apporte beaucoup d'idées pour se défendre et récupérer après de tels incidents :

* <http://www.cert.org/reports/dsit_workshop.pdf>

Le Pushback : une contre-mesure en développement

Face aux menaces grandissantes provoquées par ce type d'attaques, les scientifiques se penchent de plus en plus sur des techniques capables de les contrer; une des plus récentes est la technique du Pushback. Nous ne rentrerons pas dans les détails ici, tous les papiers étant disponibles sur le site [ACC and Pushback](http://www.icir.org/pushback/).
Très brièvement, cette technique a pour but d'identifier les attaques de DoS et surtout de DDoS grâce à des heuristiques, de les contrer en remontant à leur source, enfin de maintenir et de protéger le bon trafic qui souffre également la plupart du temps des congestions engendrées par de telles attaques.
Cette mé

|  |
| --- |
| L'attaque NT Inetinfo  |

Qu'est-ce que c'est ?

L'attaque NT Stop vise les systèmes WinNT 4.0. Elle consiste à se connecter au port 1031 (inetinfo) et à envoyer n'importe quoi. Quelques fois, il suffit juste de se connecter à ce port et de se déconnecter immédiatement. Le processus Inetinfo utilise alors énormément de ressources système et peut provoquer un plantage ou un reboot.

Conséquences :

* Blocage système
* Crash système
* Reboot système

Comment s'en protéger ?

* Mettre à jour l'OS.

thode utilise un contrôle de congestion basé sur des agrégats, un agrégat étant défini comme un sous-ensemble du trafic présentant une propriété identifiable. Exemples de propriétés :

* Paquets TCP SYN
* Paquets à destination de X
* Paquets IP dont les checksums sont incorrects
* ...

Le but est d'identifier les aggrégats responsables de la congestion et de les éliminer pour rétablir un trafic normal. Une fois la signature (c'est-à-dire la propriété identifiante, le trait caractéristique de l'attaque) établie, le flux est comparé en temps réel dans le routeur le plus proche de la cible du DDoS. Ce routeur commence à rejeter (drop) les paquets correspondants à la signature et envoie également un message d'alerte aux routeurs en amont sur les brins d'où lui parvient le trafic incriminé. Ce message d'alerte contient entre autres choses la signature qui va permettre à ces routeurs d'éliminer à leur tour les paquets correspondants à l'attaque. Et ces routeurs vont également envoyer des messages d'alerte aux routeurs situés en amont.
Cette technique récursive a pour avantage de pouvoir remonter jusqu'aux sources de l'attaque; elle permet également de décongestionner le coeur même du réseau, ce qui était impossible avec les techniques centrées sur la protection pure de la cible. Enfin, même si une partie du trafic légitime est tout de même perdue, les résultats finaux sont plutôt positifs.

|  |
| --- |
| Le Cross Site Scripting |

Introduction

Le Cross Site Scripting (CSS) est une attaque qui est rarement prise au sérieux par les non-initiés. En effet, à la différence de nombreuses techniques de piratage, celle-ci ne s'attaque pas à un serveur mais à l'internaute via une faille au niveau d'un serveur Web ou d'une application Web.

Le principe

Il est plus simple d'expliquer cette faille par l'exemple. Soit le site www.unsitecomplice.fr, le moyen de vérifier s'il est vulnérable à une attaque de type CSS est de demander l'affichage d'une page inexistante. La particularité du nom de cette page est le fait qu'il contient des balises HTML :

http://www.unsitecomplice.fr/<B>nimportequoi</B>.html

Le site renvoie une page du type :

Erreur la page **nimportequoi**.html est introuvable.

Le site est bien vulnérable puisqu'il a renvoyé une page contenant le nom du fichier introuvable mais surtout parce que les balises HTML sont conservées. Le navigateur interprète donc le code HTML (ici les balises mettent simplement le texte en gras).

Les conséquences possibles

Les conséquences semblent anodines au premier abord. Mais le CSS est exploitable de la manière suivante. Un pirate va envoyer un mail en HTML à sa victime. Ce mail comporte un lien sur un site vulnérable à un CSS que la victime a pour habitude de visiter. Les conséquences deviennent graves à partir du moment où le code HTML passé dans l'URL permet l'exécution de Javascript (balise <SCRIPT>) sur la machine de l'utilisateur. Effectivement, le pirate connaissant bien le Javascript peut facilement récupérer le cookie de la victime utilisé sur ce même site. La gravité croît alors avec la sensibilité des informations contenues dans le cookie (authentification, identificateur de session, ...)

Le CSS est une technique déclinable pour les applications Web, cette attaque fonctionne dès que l'application restitue dans un message le nom d'un fichier ou d'un paramètre présent dans une URL sans prendre en compte l'éventuelle présence de balises HTML.

Comment éviter ce type de faille

Chaque élement de l'URL subissant un traitement doit obligatoirement être filtré afin d'ôter toutes les balises HTML. Une simple transformation peut suffir pour les rendre inexécutables (par exemple le caractère < est remplacé par &lt; que le navigateur affiche bien < mais sans l'interpréter).

|  |
| --- |
| Le Déni de Service (DoS)  |

Background

Le "Denial-of-service" ou déni de service est une attaque très évoluée visant à rendre muette une machine en la submergeant de traffic inutile. Il peut y avoir plusieurs machines à l'origine de cette attaque (c'est alors une attaque distribuée, voir fiche DDoS) qui vise à anéantir des serveurs, des sous-réseaux, etc. D'autre part, elle reste très difficile à contrer ou à éviter.

Définition

D'une manière générale, on parle de déni de service quand une personne ou une organisation est privée d'un service utilisant des ressources qu'elle est en droit d'avoir en temps normal. On trouvera par exemple des dénis de service touchant le service de courrier électronique, d'accès à Internet, de ressources partagées (pages Web), ou tout autre service à caractère commercial comme Yahoo! ou EBay.
Quoiqu'il en soit, le déni de service est un type d'attaque qui coûte très cher puisqu'il interrompt le cours normal des transactions pour une entreprise; les sommes et les enjeux sont énormes et cela ne peut aller qu'en s'agravant tant que des parades réellement efficaces n'auront pas été trouvées.

Types d'attaques

Il existe de nombreuses façons pour faire planter une machine; en fait, on peut s'appuyer sur presque toutes les attaques existantes (voir sur la page d'accueil de SecuriteInfo) car en faisant planter la machine cela résultera inévitablement en un déni de service sur cette machine. La différence se situe au niveau des intentions du hacker, c'est-à-dire savoir si le déni de service est intentionnel ou s'il n'est que la résultante d'une attaque plus aggressive visant à détruire une machine. Il ne faut plus aujourd'hui négliger cet aspect intentionnel, au vu des sommes qui entrent en jeu.

Parmi les attaques propres à créer un déni de service, nous pouvons rappeler entre autres :

* les buffers overflows (mails, ping of Death...)
* l'attaque SYN
* l'attaque Teardrop
* l'attaque SMURF
* les virus
* ...

Contre-mesures

Les contre-mesures sont très compliquées à mettre en place et très ciblées vis-à-vis du type de déni de service envisagé. En effet, d'un point de théorique, la plupart des attaques visant à créer des dénis de service sont basées sur des services ou protocoles normaux sur Internet. S'en protéger reviendrait à couper les voies de communications normales avec Internet, alors que c'est bien là la raison d'être principale des machines concernées (serveurs web, etc...). Il reste tout de même la possibilité de se protéger contre certains comportement anormaux (voir les attaques précédentes) comme une tentative de flooding, un trop grand nombre de paquets ou de requêtes de connexion provenant d'un petit nombre de machines. Mais cela implique beaucoup de choses en fait : il faut monitorer le traffic (ce qui est loin d'être simple, du fait de la quantité de données qui transitent), établir des profils types de comportement et des écarts tolérables au-delà desquels on considérera que l'on a affaire à une attaque; il faut également définir les types d'attaques auxquelles on souhaite se protéger (analyses de risques à l'appui) car il est impossible de toutes les prévoir. On est donc loin de la protection absolue; il s'agit de metter en place une protection intelligente et flexible.

C'est ce que l'on retrouve à l'heure actuelle dans la plupart des systèmes de protection contre les dénis de service. Ainsi Cisco propose des produits incluant à différents niveaux des services spécifiques :

* test de la taille des paquets
* test des adresses source et destination (ainsi que loop-back, unicast, multicast...)
* test de la fragmentation
* utilisation d'adresses IP virtuelles pour validation de sessions et ACK (contre attaques TCP)
* test du nombre de SYN (contre attaques TCP)
* NAT d'adresses locales vers IP virtuelles basées sur IP globales
* contrôles de flux
* contrôles de contenus (port, tag, url, extensions de fichiers)
* autres fonctions de firewall, le tout basé sur du load-balancing et de la redondance.

Comme on peut le remarquer, l'accent est mis sur la sécurité du système de protection en lui-même pour qu'il puisse faire face à des situations extrêmes (traffic énorme, etc...) D'autre part, il reste que la plupart des contre-mesures visent à protéger contre un type d'attaque particulier. L'efficacité d'un tel système se révèlera par sa capacité à détecter et prévenir de nouveaux types d'attaques.

|  |
| --- |
| L'attaque Coke  |

Qu'est-ce que c'est ?

L'attaque Coke vise les systèmes WinNT qui exécutent le service WINS (Windows Internet Name Service). Elle consiste à se connecter à la cible et à envoyer n'importe quoi. En fonction de la configuration de l'ordinateur cible, celui ci inscrira un message d'erreur dans le log pour chaque packet invalide reçu. Ceci a pour but de ralentir le système, et d'utiliser de place disque. De façon extrème, le disque peut arriver à saturation, écroulant considérablement les performances, et pouvant bloquer le système.

Conséquences :

* Ralentissement système
* Blocage système
* Crash système

Comment s'en protéger ?

* Configurer les routeurs et firewalls pour bloquer les packets dirigés vers le service WINS qui proviennent de l'extérieur de votre réseau.

|  |
| --- |
| L'attaque Cisco ® 7161  |

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.

Conséquences :

* Plantage du routeur Cisco ®.

Comment s'en protéger ?

* Contactez Cisco ® pour obtenir une solution.

|  |
| --- |
| L'attaque Bonk  |

Qu'est-ce que c'est ?

L'attaque Bonk vise les systèmes WinNT 3.51 et 4.0. Elle consiste à envoyer des packets UDP corrompus sur le port 53. Chaque packet UDP corrompu est consitué de deux fragments IP assemblés en un UDP. Les offsets qui se superposent ont pour conséquence de faire écraser la seconde moitié de l'entête UDP par le second packet IP. L'ordinateur victime ne gère pas ces paquets et provoque un plantage (message STOP 0x0000000A) dû à une allocation excessive de la mémoire du noyau.

Conséquences :

* Blocage système
* Crash système

Comment s'en protéger ?

* Mettre à jour l'OS (le fichier concerné est tcpip.sys).
* Utilisation d'un firewall pour refuser les packets UDP corrompus.

|  |
| --- |
| L'attaque Click - WinNewk  |

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.

Conséquences :

* Déconnexion

Comment s'en protéger ?

* Configurer les firewall/routeurs pour gérer ces messages.

|  |
| --- |
| L'attaque WINS 137 flood  |

Qu'est-ce que c'est ?

Cette attaque vise les systèmes Win32 qui exécutent le service WINS (Windows Internet Name Service).. Elle consiste à envoyer un flot de packets UDP aléatoires en taille et en contenu au port 137 (UDP) de l'ordinateur cible. Après 5 secondes, le service WINS s'arrête. Le service doit être redémarré manuellement.

Conséquences :

* Perte du service WINS

Comment s'en protéger ?

* Configurer le firewall et/ou les routeurs pour filtrer les packets UDP.

|  |
| --- |
| Les types d'attaque  |

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.

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.



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.

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.



L'attaque [FTP Bounce](http://www.securiteinfo.com/attaques/hacking/ftpbounce.shtml) 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.

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.



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

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.

|  |
| --- |
| L'attaque BrKill  |

Qu'est-ce que c'est ?

L'attaque BrKill vise les systèmes Win32. Elle consiste à générer des packets qui génèrent un reset, permettant à l'attaquant de couper la connexion de la victime, à distance. Les transferts dits connectés (FTP, IRC, telnet, ICQ, ...) sont alors les cibles potentielles de cette attaque.

Conséquences :

* Déconnexion du réseau.

Comment s'en protéger ?

* Protection inconnue.

|  |
| --- |
| L'attaque Tear Drop  |

Qu'est-ce que c'est ?

L'attaque Tear Drop vise les systèmes Win32 et Linux inférieur à 2.0.32. Elle consiste à envoyer des packets TCP qui se recouvrent. Lorsque l'ordinateur victime reçoit ces packets, il tente de les reconstruire. N'y arrivant pas, cela provoque un plantage.

Conséquences :

* Blocage système
* Crash système

Comment s'en protéger ?

* Mettre à jour l'OS.
* Utilisation d'un firewall pour refuser les packets qui se recouvrent.

|  |
| --- |
| L'attaque sPing - Jolt - IceNewk  |

Qu'est-ce que c'est ?

Cette attaque, qui comporte trois noms différents, visent les systèmes Win32. Elle consiste à envoyer un très grand nombre de packets ICMP très fragmentés à l'ordinateur victime. Les conséquences sont diverses : Les systèmes Win32 ont beaucoup de mal à s'y retrouver dans la défragmentation des packets.

Conséquences :

* Blocage système.
* Etc...

Comment s'en protéger ?

* WinNT 4.0 : Installer le service Pack 3 + patch ICMP.
* WinNT 3.51 : Installer le service Pack 5 + patch ICMP.
* Win95 : Installer le patch ICMP.