-= Les cours de Zi Hackademy =-

Newbie : Cours 2, by Clad

Plan du cours :

- Recherche d'infos
. méthodes de recherche, moteurs de recherche, mots-clefs...
. astalavista.com, crackstore.com, hackers.com
. sites d'exploits: à quoi ça sert
. docs nécessaires : listes de ports, defaults passwords, rfc

- Crypto
. le besoin de la crypto
. les clefs et les tailles

. PGP : pratique

- Espionnage :
. keylogger
. sniffer
. trojan (netbus) avec un exercice pratique: "retrouvez le trojan et identifiez le"
. autres moyens

- Base de registre
. présentation de la base (regedit.exe), recherche de clefs, etc.

Newbie : Cours 2, by Clad

1 - La recherche de données sur Internet :
Qu'elle soit informaticienne, pirate ou novice, une personne doit être à même de mettre à sa contribution toutes les ressources qui lui sont à portée de main. La première zone d'information qu'ait une personne dans ce domaine n'est plus la littérature. C'est Internet.
Savoir mener des recherches efficaces sur Internet est la clef de la réussite. Personne n'a la science infuse, mais le rassemblement des masses de données sur un seul et même réseau permet à n'importe qui d'avoir accès à n'importe quel savoir,

Les sources d'informations sur le piratage ne sont pas aussi rares que l'on pourrait le croire. Certes, les sites illégaux diffusant moults "cracks" ou tutoriaux illégaux sont difficilement repérables. En revanche les sites légaux et sur le thème du piratage sont aussi nombreux que leurs sujets sont diversifiés.
Les sites sur la sécurité informatique sont de biens meilleures sourcesd'informations que des pages personnelles sur le piratage. En effet ce sont en général des personnes qualifiées qui adminisitrent ces sites, et non pas des personnes en carence de savoir. Par conséquent l'on ne saurait trop vous ecommender ces sites. Ils fournissent une documentation généralement riches en information et offrent de nombreux points d'accès vers des tutoriaux qui s'adressent aussi bien aux débutants qu'à des personnes qualifiées. Notons aussi que les vrais sites sur
Nous n'oserions pas vous assaillir d'adresses URL dans cette partie du cours, pour au moins deux raisons:
- Il n'existe pas de site référentiel à la sécurité informatique
- Des adresses URL sont disponibles à la fin de ce cours.

Les sites sur les vulnérabilités sont des mines d'or en matière de piratage. Ils servent (malheureusement ?) aussi bien aux administrateurs réseaux soucieux d'établir des stratégies de sécurité planifiées qu'aux pirates. Ce sont souvent de véritables bases de données en matières de failles, de bugs, et de problèmes relatifs à la sécurité informatique. Il serait dommage pour un pirate de chercher à s'attaquer à un serveur sans jamais se référrer à ces sites phares. Ainsi n'importe qui peut évaluer la sécurité de son système à partir es failles connues et recensées par ces sites. A l'identique des sites sur la sécurité informatique, vous trouverez quelques adresses phares en fin de cours.
Les moteurs de recherche sont également de puissants alliés. Permettant de rechercher des sites en tout genres sur le sujet, ils sont toutefois à mettre dans des catégories à part. Les liens vers les nombreux sites qu'ils créent ne sont parfois pas de bonnes références. En revanche, avec un peu d'habitude, vous apprendrez rapidement à mener des recherches efficaces. Les mots clefs à taper sont par exemple:
. "sécurité + n" (où n représente l'objet sur lequel vous portez vos recherches)
. "sécurité des n" (où n représente cette fois plusieurs objets tels que "serveurs" "routeurs" "ordinateurs", etc.)

Vous pouvez également rechercher de la documentation plus généralisée sur des dispositifs de sécurité en ne tapant que des mots clefs comme "firewalls".
Les rebonds de sites en sites s'effectuent grâce aux sections de liens que mettent en place les webmasters, D'un lien sur un site vous passez à un autre. Cette solution de recherche a un double côté. D'une part vous tomberez souvent sur des sites rarement visités, car mal représentés, et qui sont pourtant d'excellentes sources d'informations. D'autre part vous tomberez souvent sur des liens morts ou des sites non mis à jour. C'est Une chasse au trésor, en moins fastidieux: on voit du paysage!

Remarque: vous noterez que l'on n'aborde dans nos sujets de recherche qu'un angle de vue sur la sécurité informatique. En effet, si le piratage peut amener à mieux comprendre la sécurité, alors le contraire est tout aussi vérifiable. Pouvoir effectuer ce chemin en double-sens est un atout.

II - Espionnage de systèmes informatiques

1 - Keylogging
Le Keylogger (traduction littérale: "enregistreur de clefs") est un dispositif en apparence simple, dont le concept est de se placer, à un niveau logiciel, entre l'utilisateur et le traitement des données qu'il effectue par le clavier, En clair celà veut dire que tout traitement, toute frappe, fait au clavier sera enregistré par le logiciel et stocké sous forme d'un fichier consultable par la suite. Ainsi le Keylogger s'avère être un système de surveillance fiable qui permet d'enregistrer de nombreuses choses comme des saisies de mots de passes, des saisies d'adresses, de rédactions de textes, etc. Pratiquer le Keylogging n'est pas une chose illégale en soi à condition qu'il soit effectué sur votre machine, ou, si ça n'est pas le cas, que la personne qui est surveillée ne le soit pas à son insu. la plupart des Keyloggers sont invisibles. C'est à dire qu'ils fonctionnent en arrière plan de toutes les applications Windows, de façon cachée, et qu'un utilisateur non averti ne s'apercevra nullement de la présence d'un tel outil d'espionnage.
Il existe foule d'applications de ce type, plus ou moins performantes, et dont le prix varie du "tout gratuit" au "tout payant" en passant par les versions d'évaluations et les sharewares.
Nous ne saurions trop vous recommender de tester en premier lieu les versions gratuites afin de trouver chaussure à votre pied. Faites par exemple un petit tour sur www.download.com en tapant comme mot clef pour votre recherche "keyloggers".

Avant de vous en présenter quelques uns, sachez qu'un bon keylogger, qui est parfaitement invisible, ne doit:
. Manifester sa présence à aucun moment que ce soit;
. Etre visible ni depuis la barre des tâches ni depuis le gestionnaire d'applications (CTRl+AlT +DEL).
Pour illustrer le propos, prenons un très bon exemple: iOpus STARR PC.

a-Installation

l'installation ne devrait poser aucun problème, même au moins initié. Sur la fenêtre de sélection de la zone d'enregistrement des "fichiers de log" (comprenez les fichiers où sont stockées les informations qu'a enregistré le logicien, vous avez trois possibilités:
. Garder les logs sur l'ordinateur où est installé le logiciel (par défaut, nous l'avons installé avec cette option). Si l'installation se fait avec cette option celà veut dire que vous êtes obligés d'avoir un accès à la machine où STARR est installé.
. D'enregistrer les fichiers de log sur un autre ordinateur du réseau local, sur un répertoire en partage. . D'envoyer, par e-mail (et discrètement, celà s'entend) les fichiers de log.

A la fin de l'installation, le logiciel s'ouvre vous présentant sa fenêtre de gestion. Parmi les différents onglets à disposition seuls "Dashboard" et "Monitoring" sont susceptibles de nous intéresser. le logiciel est entièrement en anglais mais n'en reste pas moins très facile d'utilisation.

b - Utilisation

le lancement d'une session de capture d'informations s'effectue par la touche "Start". Vous pouvez spécifier l'endroit où vous désirez placer le fichier de log, et aussi le format sous lequel vous désirez l'enregistrer, le format par défaut étant HTML. Nous vous conseillons de garder un format des fichiers de log en HTMl, cette option permettant une lecture pratique et esthétique de l'activité enregistrée de l'ordinateur.

Par l'onglet "Monitoring" vous pouvez spécifier sur quelles applications et quels processus vous souhaitez porter votre surveillance. De même, en haut de l'écran, vous pouvez moduler la configuration concernant les captures d'écran ("screenshot") à votre guise.

1. lancez une séance de capture (touche lecture/"Start"), et fermez STARR. Une fenêtre s'ouvrira vous rappelant comment réouvrir STARR au besoin. Celle-ci indique qu'il vous faut passer par "Démarrer" "Exécuter" puis taper starrcmd.
2. Pour tester le logiciel, menez vos activités comme vous le faites courra ment, et au bout d'une dizaine de minutes par exemple relancez STARR.
3. Pour afficher le résultat de l'enregistrement des données, cliquez d'abord sur le bouton "Creat Report from STARR log". Cette étape est obligatoire, sinon le logiciel ne créera pas le fichier log.
4. Ensuite cliquez sur View Report, ce qui vous ouvrira l'éditeur de texte ou de page approprié selon l'option d'enregistrement que vous avez choisi. Si vous avez gardé l'option d'un fichier log au format HTML alors ce sera votre navigateur web qui s'ouvrira.

La magie de l'espionnage a fait son chemin, vous voici maintenant en possession d'un fichier de log complet, structuré et détaillé de toute l'activité de votre Pc. Quelles protections à cette technique?

2 - Protection contre le Keylogging et les applications cachées
Si vous avez pris le temps de le faire, vous vous serez aperçu que STARR n'est visible ni par le gestionnaire de tâches ni dans la barre de tâches. A ce problème, pas de solution miracles. Il faut faire appel à un logiciel adapté. Nous en avons pris un, qui recense tous les processus actifs sur votre machine (comprenez toutes les applications qui tournent).

WinForce est un utilitaire gratuit, léger et très simple d'utilisation. Vous pourrez le trouver sur http://www.down-load.com. la fenêtre de gestionnaires d'applications de WinForce comporte deux fonctions essentielles:
. Actualiser
. Tuer

La fonction Actualiser s'obtient par le bouton bleu en forme de flèche. Sélectionnez l'application à fermer et appuyez sur "KiIl". L'application se fermera de force.
Autrement des séries de symptômes peuvent être indices qu'un logiciel inconnu tourne en tâche de fond:
. La protection antivirus du BIOS vous informe d'un accès à la zone d'amorçage du disque dur.
. Lorsque vous lancez votre ordinateur, un message vous indique qu'il ne peut pas démarrer à partir du disque dur.
. Windows refuse de charger les pilotes de disque dur 32 bits.
. Au lancement de Windows, un message vous informe qu'un programme TSRforce le démarrage en modecom-patible MS-DOS.
. ScanDisk détecte des fichiers à liaison croisées ou d'autre problèmes.
. ScanDisk indique des secteurs défectueux sur les disques durs ou les disquettes.
. La taille des fichiers éxécutables augmente subitement.

. La date de création ou de modification des fichiers comporte des valeurs erronées.
. Vous constatez que l'ordinateur se bloque fréquemment alors que vous n'avez ajouté aucun nouveau composant logiciel ou matériel.
. L'ordinateur se bloque et indique une erreur de parité.
. L'ordinateur semble être plus lent sans raisons apparentes.
. le clavier et la souris ne fonctionnent plus de manière fiable, même après un nettoyage.
. Des fichiers ou des dossiers disparaissent de votre ordinateur de façon inexpliquée.
. Dans vos documents des mots disparaissent ou s'ajoutent subitement.
. Votre ordinateur a des réactions imprévues, voire devient incontrôlable.

Ces symptômes sont plus globalement liés à l'activité de virus, mais certains d'entre eux sont récurrents pour divers types d'applications malicieuses.
C'est le cas des ralentissement ou des disfonctionnement.

3 - Le sniffing
le sniffing, d'un point de vue théorique, est une méthode qui consiste à relever toutes les informations composantes d'un paquet réseau. Quel que soit le type de paquet (défini, par un protocole), le snifter peut l'analyser. Ainsi le sniffin9 devient une méthode efficace pour relever toutes sortes d'informations dans le champ de la zone de donnees d'un paquet. Tout peut y passer: noms d'utilisateurs, mots de passe, informations confidentielles, discutions, etc.

De plus le sniffing est invisible. En effet les informations contenues dans les paquets réseaux ne sont que subtilisées, et les paquets continuent de circuler comme si de rien n'était. Faire du sniffing n'implique pas même de perte de temps au niveau du transfert des données: la victime ne se rend compte de rien, car aucun ralentissement ne vient l'alerter.
Le sniffing est plutôt pratiqué dans des réseaux locaux, munis de hub ou sur des machines individuelles à l'aide de trojans, par exemple.

Ainsi défnirons-nous le sniffing comme une méthode qui consiste à subtiliser des informations qui circulent sur un réseau à l'insu des utilisateurs concernés. Réferrez vous aux explications détaillées et pratiques sur le Sniffing dans votre cours Newbie + pour en savoir davantage.

4 - Espionnage à distance et prises de contrôles
Le meilleur système d'espionnage à distance qui ait jamais été conçu reste le trojan. Un trojan est une application de type dit "cheval de troie". Car, tout comme le cheval de Troie, il s'installe discrètement sur une machine à l'insu de l'utilisateur.

a - Comment marche un trojan ?
L'immense majorité des trojans se dissimulent dans des applications éxécutables au format ".exe". Ces fichiers n'ont l'air de rien lorsqu'ils s'éxécutent : des petits jeux, des animations, des faux messages d'erreurs... Mais ils installent en arrière plan, sur la machine qui a éxécuté le logiciel, une application serveur invisible. "Invisible" car l'utilisateur n'a jamais eut connaissance ni de son installation ni de son fonctionnement. Ce serveur va ouvrir un port, et attendre passivement des demandes de connections de la part d'un client adapté.
Le pirate, lui, dispose de l'application client, qui est la seule à pouvoir communiquer avec le serveur. Une fois connecté il va pouvoir interragir avec la machine de la victime ce qui va lui permettre de faire tout ce que le troian lui permet. Ainsi deux trojans différents ne permettront pas forcément à un pirate de faire les mêmes choses. Au fur et à mesure que les années se sont écoulées, les troyens ("trojan" au pluriel) ont fini par se complexifier, à se diversifier, à envahir d'autres systèmes d'exploitation... Le plus complet et l'un des plus célèbre de nos jours reste certainement Back Orifice 2000, mais le plus iIlustratif et démonstratif, de par sa simplicité d'utilisation, est Netbus.

b - Expérimentation
Afin de bien vous mettre en conditions, nous allons expérimenter, tester, et ainsi voir quelle peut-être l'utilité d'un trojan. Dans cet exercice nous allons prendre deux machines. L'une d'elle représentera la victime, l'autre le pirate. le but de l'exercice est d'arriver à prendre un contrôle total et utile de la machine piratée. Nous utiliserons Netbus 1.7, car, bien que ce ne soit pas la dernière version, elle est largement suffisante pour nos démonstrations.
Nous avons pris pour faire les essais deux machines dans un réseau local. L'une est infectée, l'autre sert à simuler la machine du pirate.

L'interface graphique de Netbus ne se compose que de boutons (grand bien en fasse aux Script-Kiddies). Par défaut l'adresse IP entrée dans "Hostname/IP" est la vôtre. Et le port indiqué est "12345", qui est en fait le port qu'utilise le serveur de Netbus par défaut. Pas de danger lorsque vous éxécutez le client; il n'est pas infecté, quoiqu'en dise votre anti-virus.

Connection :

1. Utilisez la zone "Host name/IP" et indiquez-y l'adresse IP (ou le nom d'hôte) de la machine infectée
2. Cliquez sur "Connect!"

3. Une fois connecté, le logiciel devrait vous le signaler

Espionnage

1. la première fonction d'espionnage que vous pourrez exploiter sous Netbus est certainement "Screendump", qui sert à faire des photos d'écrans de la victime et à vous les envoyer directement.

2. Ensuite vous pourrez toujours visualiser les processus actifs de la victime, comme si vous utilisiez son gestionnaires d'applications, grâce à la commande "Active wnds" ("Active windows", en français: "Fenêtres actives")

Ce qui vous offre, par l'intermédiaire d'une fenêtre interne, un listing des applications ouvertes. Il est nécessaire de rafraîchir régulièrement cette liste afin de maintenir une surveillance continue sur une cible.

3. le gestionnaire de fichiers à distance est aussi très pratique et même effroyable. lancez le par l'intermédiaire de la touche "File manager"

Cliquez ensuite sur "Show files", ce qui aura pour fonction de télécharger toute l'arborescence du disque dur de la victime. Il devient désormais possible d'envoyer, d'effacer, de télécharger n'importe quel fichier sur le disque dur de la victime à son insu.

4. Les fonctions de Keylogging vues préalablement sont toujours actives: en effet Netbus intègre un gestionnaire de clavier très performant puisque, non seulement vous pouvez lire en direct ce qu'écrit la victime, mais vous pouvez aussi écrire à sa place! Ceci grâce à la fonction "Listen"

Une fois dans le gestionnaire de frappe de Netbus, sachez que toutes les touches (Oui, toutes! Même ALI, TAB ou ENTREE) sont prises en compte.

Après quoi vous avez la possibilité d'enregistrer ce qui a été frappé par la touche "Save text". Démonstration d'une prise de contrôle

L'utilisation de trojans est quelque chose que beaucoup de pirates ont en horreur: c'est trop simple, ce sont des logiciels qui ne s'adressent quasiment qu'à l'attaque d'internautes, et non pas de véritables serveurs d'entreprise... Bref, la réputation du trojan au sein de l'underground laisse fort à désirer.
Cependant un bon pirate peut faire une utilisation intelligente et calculée d'un trojan. Plutôt que de bêtement redémarrer l'ordinateur de la victime, on va essayer d'en prendre le contrôle afin de perpétuer nos attaques sous le couvert de l'anonymat le plus total. "Total", pourquoi?
Petit Scénario

1. Le pirate Clad désire attaquer le serveur X.
2. Il sait que s'il l'attaque de front ce serveur, son adresse IP risque d'être repérée au niveau des systèmes de sécurité du serveur X (firewalls, 105, systèmes de 10gs...1
3. Il va donc utiliser un système par lequel il fera transiter ses demandes de connections, comme un routeur.
4. Sauf que, si il y a une enquête approfondie sur l'attaque, Clad sait qu'ayant laissé son adresse IP sur le routeur il prend des risques.
5. Il va donc utiliser l'ordinateur d'un malheureux particulier pour se connecter sur le routeur et ensuite attaquer le serveur X.
6. Il prendra ensuite soin d'effacer toute trace de ses manipulations chez la victime. Si l'opération se passe bien, il y aura une prise de risque quasi nulle, et, au pire, ce sera sa victime qui se fera inculper.

Pratique :

. Il s'assure ensuite que la communication a bien été établie et ceci par le gestionnaire d'applications distant ou la fonction "Screendump"

. En premier temps CIad se connecte à la victime, et ce une fois fait, il lance une application telnet, afin de se connecter au routeur, par le biais du bouton "Start Program". Ce qui est brouillé sur l'image représente l'adresse IP que nous avons tenue au secret.

. Il s'agit maintenant d'entamer la procédure d'authentification au niveau du routeur en entrant un bon mot de passe. la procédure est simple: il suffit au pirate d'utiliser le gestionnaire de touches de Netbus.

. l'authentification depuis la machine de la victime a réussie. Maintenant, si l'adresse IP est enregistrée sur le système piraté, ce sera celle de la victime infectée par Netbus, et non celle de Clad, qui sera retenue.
. Clad utilise maintenant le système pour se connecter au serveur X.

Effacer les traces :

Maintenant que le pirate a réussit son coup, il doit effacer toutes traces de ses activités. En premier temps il va fermer toutes les applications qu'il a lancé à distance, grâce au gestionnaire d'applications. Ensuite il va restaurer le contrôle du clavier grâce à "Key manager" et "Restore all keys". Enfin il va supprimer le trojan de la machine, afin que la victime ne s'aperçoive jamais de son infection, grâce à "Server admin" et "Remove server". la victime ne pourra jamais prouver sa bonne foi dans le cadre d'une enquête judiciaire.

c - les scanneurs de ports
Un scanneur de port vous permettra d'identifier si une application serveur est installé sur une machine, un port étant passivement ouvert. Puis, une liste des ports adaptée (des listes de ports pour trojans circulent sur Internet) vous permettra d'identifier s'il s'agit d'un port utilisé par un trojan ou non.
Certains logiciels automatisent cette fonction de recherche en vous proposant des scans sur les ports les plus connus. Nautilus NetRanger en est un très bon exemple.

d - Protection
Un trojan est une application cachée, donc il n'échappe pas à la règle du "WinForce", comme expliqué dans la partie KeyLogging. De plus de nombreux symptômes trahissent les trojans : seuls les intrus modérés sauront vous pirater sans vous alerter. Sinon des outils de surveillance des communications réseaux peuvent se révéler bien utiles. Fourni avec Windows, et fonctionnant sous DOS, Netstat (Network Statu sI vous affiche quelles communications sont établies, avec qui, et par quels ports. Pour cela il suffit d'aller en mode MS-DOS et de taper netstat. La commande netstat /? vous permettra de voir comment utiliser des fonctions supplémentaires.

Scanner vos propres ports (sur l'adresse IP 127.0.0.11 est aussi très utile: cette méthode s'avère beaucoup plus efficace dans le repérage de trojans que l'utilisation d'un traditionnel anti-virus... Mais surtout, et c'est ce qu'il y a de plus important, votre prudence est votre plus grand facteur de sécurité.

Remarque: tant qu'un trojan, tout comme un virus, n'a pas été éxécuté il ne représente pas de danger. Mais les risques de l'éxécuter de quelque façon que ce soit sont trop importants pour que vous ne preniez pas la peine de l'effacer.

Mini-fiche de l'article :

Sujet: Espionnage

Outils abordés:
. iOpus STARR PC - http://www.iopus.com
. WinForce - http://www.donutstudios.de
. NetBus - Partout...
. Nautilus NetRanger - http://www.nautidigital.com

III - cryptographie & encodage

Avant toute chose, rappelons qu'il y a une distinction à faire qui est nécessaire, incontournable, et que vous vous devez d'apprendre par coeur. Elle est simple. Elle consiste à séparer d'une part la cryptographie et d'une autre part l'encodage. En effet ces deux éléments sont totalement dissociés.
L'encodage est le processus qui consiste à transformer des données initiales en d'autres données, différentes. Supposons que les données initiales soient des textes. L'encodage va modifier ces textes, grâce à un et un seul algorithme mathématique, en d'autres textes, totalement différents. Pour retrouver les textes initiaux c'est l'utilisation inverse du processus mathématique qui intervient. Ainsi l'encodage utilise toujours un seul et même processus mathématique pour fonctionner.

Le cryptage, quant à lui, utilise des algorithmes différents, qui nécessitent une clef. Les vieilles méthodes de cyrptage utilisaient une clef unique, pour crypter et décrypter un message. Les méthodes actuelles nécessitent deux clefs:
. Une clef publique: cette clef est mise en libre accès à qui le souhaite. Disponible en téléchargement sur des sites, sur des serveurs dédiés, ou par envoi d'e-mail, la clef publique est celle qui va être utilisée au cryptage des données. Ces données, une fois cryptée, ne s'adressent qu'à une, et une seule, personne. Celle possédant la clef privée.
. Une clef privée: cette clef permet de décrypter les messages encryptés à l'aide d'une clef publique. Le processus de décryptage n'est pas l'inverse du processus de cryptage, c'est pourquoi il est difficile de décrypter un message crypté avec une clef sans posséder l'autre clé.

Petit scénario simple : Prenons Raoul et Raymonde, Raoul désire envoyer un message à Raymonde.
1. Il va l'encrypter avec la clef publique que lui a passé Raymonde.

2. Il va envoyer le message ainsi crypté à Raymonde.
3. Raymonde va le décrypter à l'aide de sa clef privée.
4. Raymonde va répondre à Raoul avec la clef publique qu'il lui a passée. 5. Raymonde va ainsi envoyer le message cryptée à Raoul.
6. Raoul va le décrypter avec sa clef privée.

Ainsi quatre clefs entrent en jeu, soit deux paires de clefs. Chaque paire a une clef privée et une clef publique. Mais attention! Si l'on suit notre exemple précédent, il faut bien voir que jamais Raoul n'aurait pu décrypter le message de Raymonde avec une clef privée autre que la sienne. Par ailleurs il n'est pas censé avoir d'autres clefs privées que les siennes. Ainsi l'on associe toujours à une clef publique, une et une seule, clef privée.

Sans vouloir vous assassiner avec un cours historico-mathématique au sujet de la cryptographie, sa chez toutefois que le système vu précédemment a vu ses bases naître grâce à Whitfield Diffie et Martin Hellman. Ce fut ensuite au tour de trois mathématiciens de génie, Rivest Shamir et Adleman, de mettre au point le système RSA, premier système de cryptographie moderne, encore très réputé. Si la fabuleuse histoire de ces trois mathématiciensetles calculs mathématiques vous intéressent, je ne saurais trop vous recommenderdevous référrez en fin du cours pour y trouver des liens utiles.
Un utilitaire très intéressant vous permettra d'appliquer des processus cryptographiques (cryptage, décryptage, signatures) de façon très simple. Il s'agit de PGP. PGP (Pretty Good Privacy) est un outil populaire qui s'adresse au grand public et qui permet bien plus qu'un simple cryptage. Utilisant différents systèmes de cryptage, cet utilitaire s'avère être une référence. Actuellement la version 6.5.1 en français est gratuite. Sur :/ /wvvw.pgp.com vous ne trouverez que les dernières versions récentes, et payantes, de PGP. En revanc e le projet GPG (GnuPG, The GNU Privacy Guard) permet de développer une version libre de PGP, n'utilisant plus l'algorithme IDEA. Vous la trouverez sur http://wvvw.gnupg.org. La différence entre les deuxse trouve certainement au niveau de leur practicité.

GPG :

les deux logiciels présentent les mêmes fonctionnalités. Cependant les allergiques de l'anglais et des lignes de commandes préfèreront nettement
PGP à son petit frère. Afin de contenter tout le monde, nous expliquerons comment utiliser les deux.

PGP :

1. Après avoir installé PGP, lancez PGPTray. PGPtray va permettre à PGP de rester en application permanente, jusqu'à ce que vous ayez besoin de lui.
2. Faites un clic droit sur PGPtray (le cadenas gris en bas à droite dans la barre de tâches) et lancez PGPtools.
3. l'interface de PGPtoois est très simple.

Etape 1 : Créer des clefs (PGP)

le premier icône est celui concernant la gestion et la génération des clefs. la création de clefs esttrès simple, l'assistant, en français, ne fait que simplifier le processus.
Si vous n'en avez pas déjà créé, vous pouvez toujours en créer de nouvelles.
1. Dans les champs "Nom complet" et "Adresse électronique" entrez un nom d'utilisateur (évitez d'entrer de vraies informations!, dans "adresse électronique" vous pouvez par contre mettre la vôtre.
2. Puis choisissez le type de clefs que vous souhaitez créer. Dans notre exemple nous choisirons RSA.
3. Choisissez ensuite la taille de la clef, nous prendrons ici 2048 bits. Sa chez que plus la taille (en bits) d'une clef est grande, plus grande est sa force. Une clef d'une toute petite taille ne garantit qu'une maigre sécurité face à des méthodes de décryptage: c'est une coquille d'oeuf.
4. Choisissez ensuite la date d'expiration de la paire de clefs. Permettre à une clef d'expirer a un avantage, et un inconvénient. l'avantage est que, si votre clef privée est un jour découverte ou votre cryptage cassé, renouveller vos clefs vous permettra de communiquer à nouveau sans vous soucier de ce fait, car le cryptage que vous utiliserez, basé sur de nouvelles clefs, n'est pas cassé. l'inconvénient c'est qu'il vous faudra envoyer votre clef publique à tout vos correspondants, mettre à jour toutes vos zones de diffusions, etc. Il se peut qu'un jour un correspondant vous envoye un message crypté avec une vieille clef publique, vous ne serez pas à même de le décrypter. Ainsi pour notre exemple nous ne prendrons pas de date d'expiration.
5. Entrez ensuite une phrase secrète, qui a pour valeur de mot de passe. le mot "phrase" est censé inciter l'utilisateur à rentrer une phrase (soit une longue suite de caractères) plutôt qu'un simple mot. Une phrase a une plus grande valeur de sécurité qu'un mot. PGP inclut d'ailleurs un indicateur de qualité de la phrase qui doit vous guider sur le choix de la longueur de votre phrase. Cette phrase vous sera demandée lors de l'utilisation de votre clef privée (donc au décryptage). Quel intérêt celà a-t-il? Si quelqu'un arrive à copier votre clef privée, il ne pourra pas s'en servir sans le mot de passe adéquat.
6. Après que la génération se soit terminée, vous avez la possibilité d'envoyer votre clef publique sur un serveur de clefs. Celà permettra à quelqu'un qui ne connait que votre adresse e-mail, par exemple, de voir si vous avez mis en ligne une clef publique. Ce n'est pas du tout obligatoire.
7. le processus s'est achevé, vous voici en possession de votre nouvelle paire de clefs.

Nous allons maintenant voir comment utiliser cette paire de clefs dans le cryptage et le décryptage de nos données. Sachez au préalable que n'importe quel type de donnée peut-être crypté : tout ce qui est fichier sur votre disque dur peu l'être.

Etape 2 : Encoder et signer (PGP)

Le processus de signature d'un message est simple. Il permet à Raymonde de savoir que c'est bien Raoul qui lui a envoyé ces messages crypté avec la clef publique de Raymonde. En effet comment Raymonde pourraitelle savoir si c'est bien Raoul qui lui envoye ces messages alors que sa clef publique peut-être utilisée par n'importe qui?
1. Raoul va crypter son message avec sa clef privée à lui, puis avec la clef publique de Raymonde. Donc il y a un double cryptage.
2. Raymonde va décrypter avec sa clef privée le message encrypté avec la clef publique (qui est la sienne), puis va redécrypter à nouveau le message avec la clef publique de Raoul car - et on ne vous l'avait pas dit pour ne pas sombrer dans la contusion - une clef publique peut décrypter un message encrypté avec une clef privée, à condition bien sur qu'elles soient de la même paire.

Ainsi Raymonde est sure que les messages proviennent bien de Raoul car elle a pu décrypter avec sa clef publique, le message encrypté avec la clef privée
de Raoul, qu'il est le seul à posséder.

PGP vous facilite la tâche: quelques clics suffisent à signer et à encrypter ses messages. Voyons cela.

1. Créez un fichier texte de tests dans un répertoire de test.
2. Nommez le "tesUxt" par exemple et écrivez-y une phrase et sélectionnez la donnée à crypter.
3. Cliquez sur Chiffrer répertoire "test"
4. Choisissez les clefs publiques avec lesquelles vous allez chiffrer votre message, en les sélectionnant et en les faisant glisser vers les "destinataires". En clair il s'agit de sélectionner les personnes à qui sont destinées les données cryptées, ceci par sélection des clefs publiques adéquates.
5. Vous pouvez sélectionner plusieurs options: . Sortie sous forme texte (si vous désirez que le contenu crypté soit lisible). Cette option n'a aucune implication sur la sécurité de vos données.
. Effacer "original peut être une option qui peut-être vue comme une précaution, car, une fois la donnée originale effacée, seul la donnée cryptée subsiste et il n'y a aucune chance pour qui que ce soit d'accéder aux données en clair, sans avoir la clef privée adéquate.
. Visualisation sécurisée est une option applicable uniquement aux fichiers texte. lorsque le destinataire décryptera votre donnée avec sa clef privée, le texte sera ouvert dans une "visionneuse de texte sécurisé". Cette visionneuse affiche un message d'alerte rappelant à l'utilisateur que il ne doit lire ce texte que dans des conditions de sécurité et de confidentialité les plus sûres. Si l'utilisateur clique autre part que dans cette visionneuse, la fenêtre de la visionneuse se fermera automatiquement.
.l'option d'archive auto-extractible et de chiffrement conventionnel ne sont pas des options essentielles. Vous pouvez toutefois les essayer. Par exemple l'option d'archive auto-extractible vous permettra de mettre votre donnée sous forme d'un éxecutable qui extraiera les données cryptées. Cette option ne peut-être utilisée qu'avec l'option de chiffrement conventionnel qui elle, applique une option de chiffrement à l'aide d'une phrase qui joue le rôle d'une clef. Cette option est moins sure sur le plan de la sécurité de vos données, mais ne nécessite pas l'utilisation d'une paire de clefs. Ainsi PGP peut utiliser une phrase-clef (qui est la même lors du cryptage et du décryptage) plutôt qu'un système à base de paires de clefs.
6. Dans notre exemple nous ne choisissons que sortie sous forme texte comme option.
7. Cliquez sur "Ok" et le cryptage est fait.
8. Allez dans le répertoire "test" pour y voir votre fichier crypté en format .ase. Vous pouvez ouvrir ce fichier comme étant du texte (renommez le "test2.txt" par exemple). Mais n'oubliez pas de le remettre au format .asc après lecture. En effet le format .asc est reconnu par PGP. Ceci dit un fichier texte au format .txt peut aussi être déchiffrable.
9. Voyons maintenant comment signer ses données. Rappelons qu'une signature n'est pas obligatoire.
10. Cliquez sur Signer
11. Choisissez le fichier à signer, fichier qui a du être préalablement crypté. Etant donné qu'une signature s'effectue avec votre clef privée, vous aurez besoin de saisir votre phrase secrète.
12. Vous pouvez choisir une Signature détachée qui crée un fichier .sig qui ne se colle pas au fichier crypté. Vous aurez ainsi deux fichiers séparés: un fichier crypté, et un fichier signature. Nous n'appliquerons pas cette option.
13. l'option Sortie sous forme texte permet à la signature d'être lisible en format texte, tout comme la même option qui sert au cryptage.
14. Vous validez avec "Ok"
15. la signature a été faite. Vous pouvez toutefois faire cette opération en une seule étape grâce au bouton Chiffrer & signer - ,----

Etape 3 : Decryptage (PGP)

Le décryptage des données est une chose très simple. Pour décrypter des données qui vous sont adressées (donc on suppose que vous avez la clef privée adéquate, ou la clef conventionnelle dans le cas d'un chiffrement conventionne!), double-cliquez sur le fichier .pgp ou .asc, ou utilisez le bouton:

Déchiffrer & vérifier

1. Cliquez sur le bouton
2. Sélectionnez le fichier à décrypter
3. Rentrez votre phrase secrète pour l'utilisation de votre clef privée 4. Choisissez d'enregistrer le fichier de nouveau en clair

Etape 4 : Aiout de defs publiques téléchargées (PGP)

Double-cliquez sur le fichier .asc (qui porte les clefs en question) et choisissez, grâce à la fenêtre qui s'ouvre, les clefs que vous désirez importer.
les deux autres fonctionnalités de PGP (détruire et nettoyage de l'espace inutilisé) ne sont pas utiles à la cryptographie.

GPG :

Nous venons de présenter en détail comment faire fonctionner PGP. Il n'est donc pas nécessaire de recommencer de zéro avec GPG. En effet GPG fonctionne comme PGP (Cryptage avec clef, décryptage, etc...). Voyons juste comment procéder, par étapes, à l'utilisation de GPG pour une genération des clefs, une exportation de celles-ci, un chiffrage, un déchiffrage.

Etape 1 : Génération des defset ajouts de defs distantes (GPG)

GPG ne fonctionne que par ligne de commandes, nous allons en tracer les principales. Je ne conseille l'utilisation de GPG qu'à tous ceux qui maîtrisent les systèmes à ligne de commande, et aux courageux.

1. Passez en mode MS-DOS et allez dans le repertoire où se trouve "gpg.exe"
2. gpg --gen-key est la commande à taper. Elle vous lancera dans l'invite de création des clefs de GPG
3. Suivez les instructions (en anglais) qui défilent. Ce sont sensiblement les mêmes étapes qu'avec PGP.
4. Une fois votre paire de clefs crée tapez gpg --export >mesclefs
5. Ceci fait, vous avez dans le fichier "mesclefs", vos clefs publiques prêtes à être diffusées.
6. Pour importer des clefs depuis un fichier de clefs que vous avez téléchargé, utilisez la commande gpg --import nomdufichier

Etape 2 : Encryptage (GPG)

Pour encrypter un fichier, toujours en ligne de commandes

1. Utilisez la commande gpg -e test.txt
2. Indiquez l'identifiant de la clef publique
3. Une fois l'identifiant rentré, le fichier "test.gpg" est créé.

Etape 3 : Décryptage (GPG)

Décrypter un fichier gpg est très simple. Il vous suffit d'entrer la commande: gpg test.gpg puis de saisir le mot de passe pour l'utilisation de votre clef privée.

Plus de documentation sur GPG dans le "README" et "gpg.man" (accessible via la commande gpg --help). Toute la documentation est en anglais.

Remarque: Vous pouvez vous amuser à comparer différents textes en clair et cryptés afin de voir comment peut varier un cryptage d'après les différentes options que vous choisissez. Une petite astuce concernant le cryptage de vos données. Plutôt que de crypter un à un vos fichiers sensibles, que des gens malfaisant pourraient trouver (le SEFTI ?), mettez les en un .zip et encryptez le fichier .zip contenant toutes vos données. Vous ferez en deux passes une opération qui peut prendre beaucoup de temps.

Mini-fiche de l'article :

Sujet: Cryptographie
Outils abordés:
. PGP - http://www.pgp.com ou http://www.download.com
. GPG - http://www.gnupg.org

IV - Stéganographie
Des informations à faire passer, des données à faire circuler? Et le tout discrètement? la stéganographie vous aidera. Cette méthode consiste à cacher des données, des informations, dans un support anodin. Par exemple, dans la Chine ancienne, on écrivait des messages sur de la soie fine que l'on roulait en boule avant de l'enrober dans de la cire. Un messager n'avait plus qu'à avaler la boule, et à faire son voyage.
Faire passer des informations numériques est tout aussi simple. Cacher sa signature dans une image afin que personne ne puisse se l'approprier et en revendiquer la possession est un jeu d'enfant. Munissez-vous tout d'abord d'un logiciel adéquat: un éditeur hexadecimal. Pour notre exemple nous choisirons WinHEX, téléchargeable sur http://www.winhex.com

Trouvez une image pour effectuer vos tests. Ici nous prendrons l'image "test.jpg", qui représente une soi-disant empreinte de pas de l'homme ayant marché sur la lune.

L'image test.jpg, l'image sur laquelle va se porter nos travaux.

1. Ouvrez Hexedit et faites Ouvrir
2. Ouvrez votre image (ou n'importe quel autre type de fichier tant qu'il ne s'agit pas d'une application)
3. A gauche se trouvent la translation HexaDécimale des données qui s'affichent à droite (et qui sont incompréhensibles) 5. Peu nous importent les données HexaDécimales. Repérez en haut, dans la colonne de droite, les espaces vides (caractérisées par des points qui s'ensuivent sur plusieurs lignes)
5. C'est dans cette zone que devront se porter nos travaux. A la place de ces points, écrivez un petit mot. Ici nous écrirons: stegano, et, très important, ne laissez jamais d'espaces dans vos messages, mettez y des points. Notez que cela aurait tout aussi bien pu être le nom d'une société, d'une personne, propriétaire des droits de l'image.
6. Sauvegardez l'image sous un autre nom (dans le menu: File puis Save as). Il est très important de prendre cette précaution car une mauvaise manipulation peut avoir des résultats désastreux sur ce type de fichiers. Nous verrons cela après.
7. Ouvrez de nouveau l'image afin de voir si les modifications n'ont pas posées de problèmes.

L'image obtenue s'avère être l'identique de la première. Pourtant l'une d'elle contient un petit mot. Pour s'en assurer il suffit de la réouvrir avec WinHEX.

Remarque: Si l'on avait remplacé des données essentielles, l'image aurait été déformée, voire illisible !

MIni-fiche de l'article :

Sujet: Stéganographie
Outils abordés:
. WinHEX - http://www.winhex.com
. ou tout autre éditeur hexadecimal - http://www.download.com

Initiation à la base de registre Windows :

La base de registre est actuellement le support fondamental sur lequel repose l'éxécution de Windows. C'est dans cette base de donnée que sont entrées toutes les variables du systèmes. Certaines variables sont plus utiles que d'autres: certaines déterminent des mots de passe, d'autres des associations aux formats de fichiers, d'autres encore les programme qui démarrent lors de l'initialisation de Windows, etc.

Il est très facile de manipuler la base de Registre, il suffit d'en comprendre le fonctionnement. Une fois que vous aurez bien assimilé comment manipuler votre BDR (Base de Registre), vous pourrez, sans danger, y apporter les modifications désirées.
L'utilitaire de gestion de la BDR est Regedit. c'est un utilitaire Windows que vous pouvez lancer via "Démarrer", "Exécuter" puis en tapant regedit.

1 - Structure
La structure de la base de registre est simplissime. Ce sont six répertoires racines et des ensembles de sous--répertoires qui forment des arborescences.

A voir la structure de la BDR, en développant les répertoires, on se rend très vite compte de plusieurs choses:
1. C'est très mal organisé
2. Il n'y a aucun repère
3. Certaines donnees sont incompréhensibles

La BDR n'est qu'un ensemble de variables auxquelles se réferrent Windows et les applications qui y sont installées pour fonctionner. Pour les développeurs nul besoin d'informer l'utilisateur des modifications qui interviennent sur la BDR, ni quelles sont ces modifications ou à quoi elles servent.

Les répertoires sont ce qu'on appelle des "clefs", à l'intérieur de ces clefs, se trouvent des valeurs. A ces valeurs ("Nom" étant le nom que l'on attribue à la valeur) on attribue des variables ("Données" étant les données variables d'une valeur). Il existe trois types de valeurs:
1. Chaine, à laquelle peuvent être rattachés des données au format ASCII (tous caractères)
2. Binaire, à laquelle ne peuvent être rattachées que des
données au format binaire (base 2, des série de l et de 0)
3. DWORD, à laquelle ne peuvent être rattachées que des données au format décimal ou héxadécimal

Ce sont à ces variables que se réferrent les logiciels. Par exemple le logiciel X va aller chercher la valeur "Faire" dans la clef "HKEY_CLASSES_ROOT/Programme X" et vérifier quelle donnée lui a été attribuée. Si la donnée est "Oui", alors le logiciel X se lancera complètement, si cette donnée est "Non", alors le logiciel X se bloquera.
C'est tout ce qu'il y avait à savoir contenant la structure de la BDR.

Remarque: La valeur par défaut "(Défaut)" qui est une valeur Chaine non définie, se trouve dans toutes clefs, dès lors qu'elles sont crées.

2 - Manipulation

Vous n'avez que quatre possibilités au niveau de la BDR:
1. Effacer: des clefs, des valeurs.
2. Créer: Créer des clefs et des valeurs.
3. Modifier: modifier des données, renommer des clefs, ...
4. Transposer des informations de BDR.

. Pour effacer une clef ou une valeur, sélectionnez la et cliquez sur "Suppr" ou faites un clic droit puis "Supprimer", ou encore le menu de regedit :
"Edition", "Supprimer", après avoir sélectionné l'élément à supprimer..
. Pour créer une clef ou une valeur, allez dans la colonne de droite correspondant à la clef dans laquelle vous voulez créer vos éléments, et utilisez le clic droit puis "Nouveau" ou directement le menu de regedit, par "Edition", "Nouveau", et choisissez l'élément à créer.
. Pour renommer
- des clefs: faites un clic droit sur la clef et choisissez "Renommer".
- des valeurs: faites un clic droit sur la valeur puis choisissez "Renommer"
- des données (les modifier) : faites un clic droit puis "Modifier"ou directement un double clic sur les valeurs dont vous voulez modifier les données.

. Dans le cadre des transpositions, pour
- Copier le nom d'une clef: faites un clic droit sur une clef et choisissez "Copier le nom clef", ou utilisez le menu par "Edition", "Copier le nom clef".
- Copier une valeur ou des données: faites "Modifier" et copiez coller le texte dans les cases respectives des valeurs/données.

Remarque: Le copiage de clefs, de valeurs ou de données, ne servent qu'à la retransposition de ces données textes dans un environnement d'édit de texte.
Vous ne pouvez copier une clef, une valeur, comme vous copiez un fichier courant.

3 - les valeurs nécessaires au démarrage des applications Windows :
Vous le saviez très certainement, certaines applications windows se lancent par l'intermédiaire du menu "Démarrer", "Programmes", "Démarrage".
Mais la BDR et les fichiers systèmes windows sont aussi des lieux de lancement des applications. En effet Windows va vérifier dans certaines clefs fixes de la BDR, ou à certains endroits précis des fichiers systèmes de Windows, quelles applications il doit lancer. Ces clefs, elles ne sont pas nombreuses.

A partir des répertoires racines, il suffit de rechercher l'existance d'une clef "Run" ou similaires dans "Software \Microsoft\Windows\CurrentVersion". Si il n'y a pas de clef qui s'y apparente, c'est qu'aucun logiciel n'en a crée. Au niveau de ces clefs, vous avez les valeurs (aux noms des logiciels en général) qui ont pour données le répertoire où se trouve le logiciel à lancer.

Dans notre exemple ce sont ICQ et MSN Messenger qui se lancent au démarrage depuis les répertoires où ils ont été installés.
Vous pouvez, par sécurité, par confort, ou dans un but nuisible, enlever des applications trop lourdes au démarrage ou en rajouter. C'est dans ces clefs que s'installe, par exemple, Netbus pour s'auto-relancer au démarrage de Windows et c'est dans ces mêmes clefs que s'installent beaucoup d'applications malicieuses (keyloggers et trojans entre autres).