LE SOCIAL ENGINEERING

Cédric de Clarens de-cla_c@epita.fr
Sébastien Hurlin hurlin_s@epita.fr

Le 24 mars 2003

Table des matières

Chapitre 1

Définition du social engineering

C'est l'art de " hacker "[1] sans ordinateur, ou l'ensemble des techniques qui exploitent les faiblesses humaines en vue d'obtenir des informations qui peuvent aider à " hacker ", créer, détruire, forcer, espionner.

C'est une technique ayant pour but d'extirper des informations pouvant être plus ou moins confidentielles par la seule force de persuasion. Les faiblesses, humaines, sont en effet responsables de beaucoup de problèmes de sécurité que ce soit dans le domaine de la sécurité informatique ou dans tout autre domaine.

[1] pirater

Chapitre 2

Les techniques connues

Les quatre moyens les plus connus et utilisés sont :
- le téléphone
- le courrier postal
- l'Internet
- le contact direct

D'autres techniques complémentaires existent comme la fouille des poubelles " trashing ", le sexe, ou tout simplement l'utilisation de la bêtise des autres.

Il s'agit de duper des gens afin de leur faire révéler leur mot de passe ou autre info qui pourrait compromettre la sécurité du système visé.

Les informations que vont chercher à récupérer les " hackers "[1] vont généralement être des mots de passe ou des informations qui pourraient compromettre la sécurité d'un système.

Ces informations peuvent également être des renseignements d'ordre privé sur la victime, afin de deviner un mot de passe. Par manque de temps, et par défaut de formation, il est fréquent que les mots de passe soient composés de noms de proches, d'animaux familiers, de dates de naissance.

[1] pirates

2.1 Exemple

Voici un petit exemple :

" Bonjour, Nicolas Brissot du service informatique. Je suis nouveau dans le service, et je dois vérifier le bon fonctionnement de votre boîte aux lettres. Pourriez-vous me rappeler votre mot de passe car la personne qui s'en occupe habituelement est en congé maladie. Bien sûr, c'est User1 "

2.1.1 Analyse de l'exemple

Voici une communication habituelle dans une entreprise. Pourtant, Nicolas Brissot n'existe pas et il ne travaille pas dans le service informatique.

La personne s'étant fait passer pour Nicolas Brissot vient de réussir à se procurer un accès complet à votre boîte aux lettres. Il peut intercepter tous vos messages, y compris bien sûr les pièces jointes.

Cette technique, qui consiste à se faire passer pour une autre personne, est souvent utilisée par des pirates informatique pour obtenir l'accès FTP[2] à un serveur ou à un réseau.

Elle peut également fonctionner dans beaucoup de cas par exemple avec un hébergeur donnant les mots de passe des FTP, bases de données par téléphone. Et même si le fait de donner des mots de passe par téléphone parait incroyable, cela se fait très souvent.

2.2 Explication générale

Peu d'entreprises, et plus particulièrement leurs employés sont formées aux risques encourus par cette technique qu'est le social engineering. Or, ce sont les erreurs humaines les plus dangereuses et il est très facile, avec un peu de bon sens et de savoir faire d'obtenir les informations désirées. Il suffit souvent de savoir le demander.

Pour réussir à récupérer des informations en utilisant cette technique il y a quelques principes à connaître :

[2]File Transfert Protocol

Il faut tout d'abord faire attention à la formulation de chaque phrase.
- le choix du vocabulaire
- le ton employé
- l'ordre des mots

Le but étant de paraître naturel et sûr de soi, on se ne jette pas sur son téléphone sans avoir rien préparé.

Voici quelques règles élémentaires avant de commencer :

1. Téléphonez à partir d'une cabine afin d'être sûr de ne pas être retrouvé. Si vous devez utiliser Internet faites cela d'un cybercafé par exemple sans avoir, bien sûr, donné de nom ou votre réelle identité aux personnes responsables de ces lieux.
2. Faites le " 3651 " avant de composer le numéro appelé pour cacher le numéro aux correspondants. Attention, celà ne veut pas dire que l'on ne peut pas retrouver le lieu de l'appel de la cabine téléphonique.
3. Si vous prenez une autre identité, apprenez par coeur vos nouveaux nom, prénom, adresse, etc.

Comme indiqué précédemment, le discours que vous allez tenir doit être préparé :

Ne jamais proférer de menaces, ni même hausser un petit peu le ton. Il vous faut attirer la sympathie de celui à qui vous parlez !

Il ne faut donc pas non plus lui faire croire qu'il peut y gagner quelque chose, car il pourrait se sentir manipulé.

Surtout être direct et ne pas hésiter en tournant autour du pot. Exprimez votre demande d'une phrase pertinente, dès le début. Il faut lui faire sentir en quoi c'est important pour vous (pour susciter l'éveil de la bonne volonté de l'interlocuteur), ceci par des expressions comme " vous me rendriez un immense service ", " ce qui m'aiderait beaucoup, c'est... ", " vous me seriez d'une infinie utilité si vous m'expliquiez... ", ou encore " je vous serais infiniment reconnaissant si vous me portiez secours en me disant... ", etc.

Vous devez donc :

1. faire confiance à la bonne volonté de l'autre
2. Ne surtout pas lui forcer la main : s'il refuse, n'insistez pas, cherchez plutôt à savoir la raison de ce refus, peut-être obtiendrez-vous ainsi les

éléments suffisants pour le faire revenir sur sa décision...

3. exprimer en une seule phrase l'annonce de votre demande et son objet précis, puis rester à l'écoute...
4. bien remercier votre interlocuteur de son aide

A éviter surtout :

1. " tourner autour du pot ", ce qui va déclencher un sentiment d'incertitude chez votre interlocuteur qui va donc commencer a se poser des questions.
2. Se dire que cela ne peut pas marcher, car celà va entraîner une demande mal formulée. C'est très mauvais ! L'autre peut ressentir votre peur et exprimer alors de l'inquiétude et donc de la méfiance. Soyez sûr de vous, pas de défaitisme !
3. donner des ordres : sans hausser le ton !
4. reprocher quelque chose à votre interlocuteur.

Le but de votre manœuvre est de persuader votre interlocuteur, donc d'arriver à le ranger de votre côté. La sincérité est donc la clé. Mais vous ne pouvez pas être réelement sincère compte tenu de la situation. Il va donc falloir simuler à la perfection.

Pour avoir un discours crédible il va falloir vous mettre à la place de votre cible et essayer de prévoir les réactions qu'elle pourrait avoir pendant votre conversation. Vous ne devez jamais vous opposer aux objections et contre-arguments de votre interlocuteur. Ecoutez-le et arrangez-vous pour exploiter ceux-ci à votre profit, mais sans les démonter. Si votre interlocuteur est de votre avis, vous pouvez faciliter sa tâche par diverses propositions, l'aidant ainsi à passer à l'action.

Il faut également prévoir que votre interlocuteur puisse demander des informations pour plusieurs raisons. Il faut donc vous être renseigné sur le plus de points possibles.

Le tout est donc de rester simple, poli, explicite, et de ne pas rentrer en opposition avec votre interlocuteur.

Après cet introduction générale sur le social engineering, nous allons maintenant voir en détail les différentes techniques utilisées.

Chapitre 3

Le social engineering au téléphone

3.1 Les bases

C'est de loin la méthode la plus fréquemment utilisée car elle est rapide et accessible à tous.

Un bon " hacker "[1] aura donc préparé son personnage et son discours. Il sera sûr de lui. Le téléphone permet quelques options qui se révèleraient impossibles pendant une discussion en face à face. Il est par exemple envisageable de changer sa voix ou de faire passer des bruits comme fond sonore pour être plus crédible.

3.2 L'équipement

Le seul équipement réellement nécessaire est un bon téléphone. Evitez de faire cette intervention de chez vous et préférez une cabine téléphonique pour une question de sécurité. Mais évitez une cabine téléphonique avec des bruits de rue, car cela ne fait pas très professionnel.

Un petit filtre sur le téléphone permettant de changer la voix, peut être utile.

Tout ce matériel est assez coûteux mais vous assure la qualité d'un bon

[1] pirate

appel.

Au téléphone, seulement 13% des informations verbales sont réellement captées par l'utilisateur. En revanche des détails comme le timbre de la voix et les intonations représentent plus de 70% de ce qui touche en profondeur votre correspondant.

3.3 La technique

Pour commencer vous devez tâter le terrain. Nous prendrons l'exemple d'une université.

Appelez le service de gestion du parc informatique en expliquant que vous n'arrivez pas a accéder à votre compte. Si les personnes ne sont pas formées aux risques encourus par le fait de donner des mots de passe par téléphone, ils vous donneront un nouveau mot de passe. Si cela a marché pour vous il vous est donc possible de recommencer cette intervention mais en utilisant le nom d'un autre étudiant. S'ils sont conscients des risques ils vont procéder à quelques vérifications avant.

Il faut bien choisir la personne pour qui vous voulez vous faire passer.

Par exemple, un autre étudiant que vous connaissez ou un professeur que vous arrivez particulièrement bien à imiter. Le transformateur de voix peut être très utile dans ce cas car la voix change quand elle est transportée par le téléphone, ce qui peut aider.

Une technique fonctionnant particulièrement bien est de se faire passer pour une femme (si vous êtes un homme) et de faire sentir a votre interlocuteur que vous êtes un peu perdue (que vous ne comprenez pas toutes les subtilités de l'informatique) et que vous avez absolument besoin de lui. Pour cela, utilisez un transformateur de voix.

On vous demandera certainement de confirmer votre identité d'une façon ou d'une autre. Il va donc falloir vous renseigner sur la personne pour laquelle vous voulez vous faire passer. Il est souvent demandé le numéro de sécurité sociale.

La préparation avant l'appel est souvent plus importante que l'appel lui même. Voila pourquoi il faudra rassembler un maximum de renseignements sur la personne que vous allez simuler. Si vous vous faites passer pour quel-

qu'un que vous n'êtes pas et que vous butez sur une simple question de vérification par manque d'informations, vos interlocuteurs deviendront suspicieux et il sera encore plus difficile de pénétrer le système ultérieurement.

Une fois que vous avez convaincu votre correspondant de votre fausse identité, demandez un nouveau mot de passe, numéro telnet etc. N'en demandez pas trop en même temps, cela peut éveiller la suspicion. Vous devez avoir les sonorités d'un honnête citoyen.

Prenez bien vos marques, entraînez-vous à l'imiter (lui ou elle). Cette personne a-t-elle des tics verbaux, utilise-t-elle un langage châtié ou vulgaîre, un accent particulier, des mimiques ? Tous ces renseignements peuvent aisément être récoltés. Il suffit d'appeler la personne en se faisant passer pour une agence de télémarketing qui fait son enquête sur tel ou tel sujet. Même si celà se solde par un refus au téléphone, celà permet d'être informé sur la façon de parler. Dans le cas contraire, c'est une bonne opportunité pour leur demander des informations personnelles (adresse, numéro de sécurité sociale et autres informations basiques).

3.4 Comment parer cette méthode ?

Si vous recevez un coup de téléphone d'une personne que vous ne connaissez pas, ne donnez aucun renseignement. Restez dans le vague, et débarrassez-vous de lui : soit vous mettez un terme à cet appel, soit vous demandez une confirmation par écrit (par fax) de la demande. Par fax, on obtient le numéro appelant, et il est donc facile de l'identifier. Et ainsi, on garde une trace écrite, cela pouvant être d'une grande importance pour déposer une plainte.

Malheureusement, un bon " hacker " vous aura étudié avant, et se fera passer pour un client, un fournisseur, ou un de vos collègues situé dans un autre bureau dans le cas d'une grande entreprise. Pire encore, il attaquera au moment le plus propice pour lui : par exemple, lorsque le responsable d'un client est en vacances. Il devient très dur alors, de se douter d'une mauvaise intention... Attention aux entreprises qui externalisent leur sécurité informatique...

Chapitre 4

Le social engineering par la Poste (Le snail mail)

4.1 Le Snail Mail est-il vraiment utile ?

Le " hacker " va réaliser une lettre la plus professionnelle possible. Pour cela il n'hésitera pas récupérer des papiers à lettre comprenant des logos ou un filigrane. Pour cela il est possible de voir un imprimeur ou de s'arranger pour récupérer ces papiers directement dans l'entreprise visée ou même avoir un exemple trouvé dans les poubelles de l'entreprise afin d'en réaliser une copie.

Le fait de " fouiller les poubelles " d'une entreprise peut se révéler très intéressant car très peu de papiers pouvant être sensibles sont détruits. Il va donc être également possible par exemple, de récupérer des noms d'employés et des renseignements sur ceux-ci. Il utilisera très certainement une boîte postale pour l'adresse de sa société fictive.

Cette méthode est très efficace car les gens ont tendance à avoir beaucoup plus confiance envers des documents écrit, car ils pensent les renvoyer à une adresse de société existante. Ils s'imaginent donc qu'il est facile de retrouver les personnes si jamais il y a un quelconque problème.

4.2 L'équipement

Il faudra, bien sûr, des enveloppes et des timbres, et une bonne imprimante (pour faire du papier et des enveloppes à en-tête). C'est la qu'interviennent des talents subtils comme la création de logos, le choix du nom de la société, pour le retour du courrier. La crédibilité de votre fausse société dépend énormément de son image de marque et le logo en est la vitrine.

Une boite postale est idéale pour ce type d'action, cela fait très professionnel et il est possible d'en avoir une sous un faux nom, pour une sécurité maximum.

4.3 La technique

En général le Social Engineering par courrier, s'adresse à un large groupe de personnes. Le courrier devra ressembler à un mailing de masse. Adressage par étiquettes imprimées (plus crédible).

Il faudra se procurer une liste d'employés de cette société et leurs adresses (par exemple en regardant les papiers jetés aux ordures).

Pour avoir un modèle il suffit de regarder dans sa boite aux lettres : en-têtes et formulaires.

Dans les infos récoltées, n'oubliez pas de demander le numéro de sécurité sociale.

Astuce : demander de choisir un mot de passe pour confirmer l'activation du compte par téléphone, 9 fois sur 10 il s'agit du mot de passe utilisé sur le compte Internet.

Dans le choix de la mise en page, préférez les questions à réponses simples (genre QCM), concises et non ambiguës. Evitez les choix difficiles, un formulaire trop compliqué se retrouve directement à la poubelle.

Après avoir cacheté, adressé et timbré vos courriers, envoyez les et attendez. Les réponses ne tarderont pas à arriver. Après cette étape, utilisez la méthode téléphonique pour les exploiter, le numéro de sécurité sociale étant le plus souvent demandé. Si vous pensez qu'il va vous manquer des informations, n'hésitez pas à les demander dans vos courriers en adaptant vos formulaires.

4.4 Comment parer cette méthode ?

L'idéal serait de filtrer tout le courrier entrant de l'entreprise. Pour chaque source inconnue de l'entreprise, il faudrait faire une vérification de l'existence réelle de celle-ci. Ne pas hésiter à regarder dans l'annuaire et à appeler l'entreprise en question pour confirmation.

Chapitre 5

Le social Engineering par Internet

5.1 Est ce juste une forme de hacking ?

La méthode utilisant Internet est semblable à celle du téléphone. Le " hacker " se fera facilement passer pour un opérateur système, un responsable informatique ou un ingénieur système.

Le hacking exploite les trous de sécurité des systèmes informatiques alors que le social engineering exploite les trous de sécurité du sens commun des gens (naïveté, sensibilité, etc..).

Préparer sa cible en faisant un " FINGER " [1] sur un système est une bonne façon de débuter dans l'engineering. Ces opérations donnent souvent le nom complet, le lieu et autres infos sur les derniers logins. Il va falloir choisir dans la liste celui ou celle qui ne s'est pas connecté depuis longtemps.

Autre schéma classique : se faire passer pour un administrateur sur un channel IRC[2] ou dans un chatroom[3] peut vous permettre de récupérer de multiples informations.

[1] commande pour avoir un renseignement sur un utilisateur sous un système UNIX
[2] Internet Relay Chat
[3] Forum Internet

5.2 Comment parer cette méthode ?

Comme pour le téléphone, ne donnez pas de renseignements à quelqu'un que vous ne connaissez pas. Par Internet, c'est plus facile d'obtenir une bonne crédibilité, tant il y a de noms de domaines et d'adresses emails. Il n'est donc pas facile de faire la part des choses. Une bonne étude de la gestion de l'extranet et de la mise en place d'une structure matérielle et personnelle adéquate est la meilleure solution.

Chapitre 6

Le social engineering par contact direct

C'est le social engineering le plus dur de la part du " hacker ". Il sera équipé pour que vous ne vous rendiez compte de rien : costume, cravate, très bien habillé, très propre, attaché-case , agenda rempli, documents divers, carte de visite, badge... Si le hacker prend de tels risques, c'est qu'il est déterminé à obtenir les renseignements souhaités. Il sera donc très persuasif.

6.1 Pourquoi y aller ?

C'est dans certains cas indispensable, car même si l'on peut faire énormément de choses par le téléphone ou par courrier, il est parfois nécessaire de se rendre sur le terrain pour constater par soi même l'état des lieux, prendre un mot de passe écrit sur un papier (souvent sous le clavier), compter le nombre de terminaux etc.

6.2 L'équipement

La première chose à savoir est que l'apparence va énormément compter. Il faut donc presque tout baser dessus.

Bien sûr être habillé d'un costume cravate. Des chaussures " habillées "

et être physiquement présentable (ne pas avoir de cheveux trop longs, être rasé, etc..)

Il faudra avoir une attitude sûre, le regard fixe et la tête haute, cheveux bien coiffés et petite mallette.

Vous devez faire sentir que vous faites partie des bureaux et vous vous y sentez chez vous.

Une fausse carte magnétique avec votre photo dessus, le logo de la société et le nom d'une opération ou d'un programme d'entreprise vous donneront un look plus officiel.

Dans le pire des cas, un autocollant " visiteur " fera l'affaire et pourra faire accepter une apparence peu officielle.

6.3 La technique

Baladez-vous dans les bureaux avec un air sûr, portez dignement le badge de visiteur, ou faites comme si vous apparteniez à cette société, ce sont vos apparences qui comptent. Des bureaux à compartiments constituent le terrain idéal, car ils vous permettent de bien faire l'inventaire du contenu des tables de travail et des affaires personnelles, facilitant ainsi l'identification de l'ordinateur administrateur et du profil de l'utilisateur. Avec un peu de chance, vous trouverez la machine UNIX [1] de l'entreprise, qui en général se trouve derrière une grande baie vitrée, ce qui vous permet d'identifier rapidement les modes de connexion possibles. Surtout ne jamais essayer de hacker sur place car c'est un comportement qui laisse rapidement place à la suspicion.

6.4 Comment parer cette méthode ?

C'est très difficile, car vous avez été directement confronté au charisme du hacker. S'il a réussi, vous êtes persuadé de son honnêteté. Cependant, lors d'une discussion, n'hésitez pas à demander un maximum de renseignements " concrets " (nom de votre interlocuteur, nom et adresse de la société, etc.),

[1] Système d'exploitation

et par la suite, vérifiez auprès des organismes compétents l'existence réelle de votre interlocuteur. N'hésitez pas à téléphoner à la société pour savoir si la personne existe, et si elle est bien au courant qu'elle vous a vu ces dernières heures...

Chapitre 7

Exemples

7.1 Exemple 1

Mr Patrice Rouau essaye de récolter des informations grâce au social engineering, malheureusement, il ne sait pas réellement comme s'y prendre.

Patrice Rouau : bonjour, je suis nouveau dans l'entreprise...

L'opérateur téléphonique : Oui, bonjour monsieur, que puis-je pour vous ?

PR : Euh, oui, en fait, on... euh... enfin, je ne suis pas très doué en informatique et, euh...

OT : Oui, je vous écoute, que puis-je faire pour vous ? (pointe d'exaspération !)

PR : Je me suis dis en fait que vous pourriez m'aider à me connecter au réseau intranet...

OT : (un peu énervé) Je ne peux pas vous aider monsieur, demandez à votre responsable !

PR : (déçu) pouvez-vous me passer ce responsable ?...

OT (agacé !) : Il n'y a personne au bureau en ce moment, rappelez demain !

PR : (d'un ton sec) : " je vous remercie beaucoup de votre aide, comment je vais faire maintenant ? !

OT : ce n'est pas de ma faute, monsieur, au revoir.

Mr Rouau a tout faux ! II n'est pas sûr de lui, il tourne autour de la demande, il monte le ton et reproche à son interlocuteur de ne pas pouvoir l'aider. Voyons maintenant le même hacker après avoir préparé son discours :

PR : Bonjour monsieur, je suis nouveau dans l'entreprise, et je n'arrive pas à me connecter au réseau intranet, vous me rendriez un immense service en m'indiquant la procédure à suivre...

OT : Bien sûr, je vais vous passer quelqu'un qui saura vous aider, ne quittez pas...

H : je vous remercie beaucoup, vous me sauvez...

Voilà, le but a été atteint.

7.2 Exemple 2

PR : Bonjour, passez-moi le service informatique s'il vous plaît...

OT : C'est de la part de qui ?

PR : Euh... je suis stagiaire et j'ai perdu le numéro direct, je voulais parler à mon responsable...

OT : Je crains que ce ne soit pas possible pour l'instant.

PR : Ah oui, et pourquoi donc ?

OT : Je ne peux pas vous dire.

PR : Qu'est-ce que cela peut bien vous faire ?

OT : Rien du tout, je vous assure que cela n'a rien de personnel.

PR : (le coupant) Alors pourquoi ? etc. Ceci est mal parti.

7.2.1 Analyse de l'exemple 2

Pour commencer, il donne un ordre sec et autoritaire sans aucune formule de politesse (voudriez-vous me rendre le service de... ou autre) Ensuite, il n'a pas préparé son texte et son identité : il réfléchit quand on lui demande qui il est... II agresse l'opérateur : "Ah oui, et pourquoi donc ?" Et il va à l'encontre de ses objections, il s'oppose à lui au lieu d'aller dans son sens !

7.2.2 Reformulation de l'exemple 2

Voila la même situation après une petite préparation :

PR : Je suis bien au standard de l'entreprise X ?

OT : C'est bien ça monsieur, que puis-je pour vous ?

PR : Peut-être pourriez vous me rendre un immense service en me passant le service informatique...

OT : Bien sur, qui êtes vous ?

PR : (d'une voix joviale) Marc, le nouveau stagiaire...

OT : C'est que je ne sais pas si c'est possible...

PR : Je comprends, je suis désolé d'avoir perdu le numéro d'accès direct... je dois les contacter pour une affaire urgente, j'implore votre aide, je dirai que j'ai téléphoné directement sans passer par vous...

OT : Si vraiment ça peut vous rendre service, d'accord, je vous le passe...

PR : Merci beaucoup, vous me sauvez...

OT : Ce n'est rien, ne quittez pas...

7.2.3 Analyse après reformulation

Bonne utilisation des expressions clés, qui vont dans le sens de l'interlocuteur. Il donne le beau rôle à l'autre, c'est-à-dire à la personne qui décide et qui rend service. Il facilite l'action de l'opérateur téléphonique, et il remercie.

7.3 Exemple réel

7.3.1 Comment Mitnick a gaché le Noël de Tsutomu ?

Après sa sortie de prison, le FBI a essayé de garder un oeil sur Mitnick.

En décembre 1994, un pirate attaque les ordinateurs de Tsutomu Shimomura, expert en sécurité, qui travaille maintenant pour les autorités.

Le pirate a utilisé une technique qui, à l'époque des faits, était connue en théorie ... mais son application pratique n'avait jamais été réalisée.

La veille vers 22h : plusieurs sondages en provenance de csn.org (Colorado SuperNet) et plusieurs tentatives d'intrusion avaient échoué. Puis deux tentatives d'intrusion provenant d'adresses au nom douteux (wiretap-spies.com, suspects.com)

14h09 : ARIEL est sondé (à l'aide de l'instruction finger -1 @ariel.sdsc.edu). L'ordinateur renvoie des informations : ARIEL est actuellement connecté à ASTARTE, RIMMON, et OSIRIS.

14h09 à 14h11 : six nouveaux sondages visant différents aspects du réseau sont effectués.

14h11 : procédure de télécommande sur OSIRIS.

14h18 : demande de connexion extérieure pour RIMMON (provenant de 130.92.6.97) en utilisant la requête " SYN "[1]. Plusieurs autres demandes successives

14h18 : SYN adressé à OSIRIS par un ordinateur identifié par l'adresse appolo.it.luc.edu 1. un " SYN " est envoyé à OSIRIS. Il est accompagné d'un numéro d'ordre afin d'établir le contact 2. OSIRIS accuse réception du message en renvoyant un SYN-ACK 3. Mais au lieu de répondre par un 3ème numéro d'ordre la machine du pirate donne l'instruction " RST " [2] et recommence l'opération une vingtaine de fois !

7.3.2 Comment Tsutomu a retrouvé Mitnick

Les fichiers de journalisation ont été " réduits " [3]. La longueur anormalement petite met la puce à l'oreille d'un responsable, qui appelle Tsutomu. Il commence alors à vérifier tous les fichiers de ses stations, un travail de longue haleine.

Le déclic proviendra d'un coup de téléphone d'un usager du WELL[4]. Celui-ci s'est vu envoyer un mail qui lui demandait de nettoyer son compte, car celui-ci dépassait la taille réglementaire. Il y a découvert des fichiers qui lui étaient inconnus. Au milieu de ces fichiers figuraient de nombreux mails à l'intention d'un certain Tsutomu Shimomura, il a donc décidé de l'appeler.

[1] synchronisation
[2] reset
[3] une partie a été effacée
[4] acronyme de Whole Earth ELectronic Link

A partir de là, tout va être facilité.

Tsutomu va réaliser des " monitoring " [5] à partir du WELL et ainsi suivre le pirate dans toutes ses manoeuvres.

L'intrus dispose de plusieurs comptes sur le WELL et se sert de ce serveur comme plate-forme d'attaque.

Très vite, il va pouvoir localiser le pirate. A Raleigh, les appels semblent entrer par un central de la compagnie téléphonique GTE, dont les listings renvoient vers une autre compagnie : SPRINT. A cause d'une manipulation des logiciels du réseau, GTE pensait que les appels venaient de Sprint, et vice versa. Aucune des deux compagnies n'avaient donc de données sur l'utilisateur du téléphone - ni ne lui a jamais envoyé de facture d'ailleurs ! Shimomura va donc parcourir les rues de Raleigh avec une antenne de détection et localisera ainsi l'appartement de Kevin Mitnick.

[5] surveillances

Chapitre 8

Conclusion

Il ne faut pas perdre de vue que le " hacker " ne se limitera pas à une seule de ces techniques, mais au contraire, utilisera une combinaison de toutes les méthodes. Par exemple : téléphoner pour obtenir un rendez-vous, confirmer par écrit, après avoir récupéré des documents dans la poubelle, et passer une heure en votre compagnie...

Il est important, de la part d'une entreprise, de former le personnel à ce problème. Un bon " hacker " s'attaquera à la personne la plus faible de l'entreprise, à savoir le personnel non technique (secrétaires, comptables...) et les personnes récemment recrutées. La paranoïa reste l'arme ultime contre ce genre d'attaque.

Annexe A

Glossaire

FTP : (File Transfert Protocole) protocole en vigueur sur Internet qui permet la transmission de n'importe quel fichier entre deux ordinateurs.

IRC : (Internet Relay Chat) : Outil de communication en temps réel. IRC a été concu par le finlandais Jarkko Oikarinen en 1988. Il a participé notamment au RFC1459. IRC est basé sur l'utilitaire "talk" sur système Unix. Les serveurs IRC Undernet sont maintenant codés par Run. C'est un protocole de communication permettant à des utilisateurs de discuter par écrit et en temps réel sur Internet. Le "Chat" est apprécié pour son aspect convivial. L'accès à IRC nécessite un logiciel client IRC (comme mIRC32 sous Windows) souvent gratuit, il faudra alors se connecter sur un serveur IRC puis rejoindre un canal. On peut alors converser avec tous les membres du canal en même temps ou entamer une discussion en tête à tête avec l'un d'entre eux.

UNIX : Système d'exploitation installé sur une grande partie des serveurs, stations de travail et gros systèmes informatiques. Il est fortement implanté dans les universités, les laboratoires de recherche et certains secteurs d'activités de l'industrie. Au bout de 30 ans de carrières, son niveau de performance et sa fiabilité ne sont plus à démontrer et il a joué un rôle fondamental dans le développement d'Internet.

Annexe B

Références

B.1 URL

1. Site portail sur les hackers
   - *http ://www.paranos.com/internet/*

2. Page sur la politique de sécurité de l'information
   - *http ://www.guerreco.com/article.php3 ?sid=126*

3. Page proposant plusieurs documents classés en Offensif/Défensif
   - *http ://hackoolique.tripod.com/txtsse.htm*

B.2 DVD

Film sur la vie de de Kevin Mitnick
- *Cybertr@ck*