Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEÇON 9
LA MESSAGERIE ÉLECTRONIQUE: SÉCURITÉ ET VIE PRIVÉE

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Conditions d'utilisation de ce support

Ces leçons et supports sont gratuits et disponibles pour le public sous les conditions suivantes d'ISECOM:

Tous les travaux menés dans le cadre du "Hacker HighSchool" sont disponibles à usage non commercial auprès d'élèves du collège, du lycée, dans le cadre d'écoles publiques ou privées, ou encore lors de scolarisations à domicile. Ces supports ne peuvent être reproduits en vue d'un usage commercial. Il est expressément interdit d'utiliser ces supports dans le cadre de cours, leçons et/ou stages payants, à moins d'obtenir une licence pour cela (dans ce cas, veuillez aller sur *www.hackerhighschool.org/license*).

Le projet HSS (Hacker HighSchool) est un outil de travail et d'apprentissage, et en tant que tel, son utilisation relève de la personne qui l'utilise, et non de l'outil lui-même. ISECOM ne peut être mis en cause si cet outil est utilisé à mauvais escient ou de manière illégale.

Le projet HSS est aussi le fruit de l'effort de toute une communautés, et si vous trouvez ce projet intéressant, nous vous serions plus que reconnaissants de votre aide, soit par l'achat d'une licence, soit par un don, soit encore par un quelconque parrainage.

Table des matières

Personnes ayant contribué à ce projet

Stephen F. Smith, Lockdown Networks

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Traduction

Bénoni Martin

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

9.0 Introduction

Tout le monde utilise l'e-mail (le courriel). C'est le deuxième plus utilisé des programmes sur internet après votre navigateur web. Mais ce que vous ne réalisez peut-être pas, c'est qu'une partie significative des attaques et des *compromissions* sur le réseau utilisent l'e-mail (le courriel). En ce qui concerne votre vie privée, l'abus de l'e-mail (du courriel), peut soit révéler le contenu du message, soit donner à un spammeur des informations vous concernant. Le but de ce module est de vous donner des informations sur le fonctionnement de l'e-mail (du courriel) , l'utilisation sûre de l'e-mail (du courriel), les attaques utilisant l'e-mail (le courriel) et des stratégies de sécurité pour l'e-mail (le courriel).

9.1 Comment fonctionne l'e-mail (le courriel)

Tout comme le courrier aérien est envoyé à travers les airs le courrier électronique (e-mail, courriel) est envoyé a travers l' électronique – l'électronique étant dans ce cas les connexions à l'intérieur et entre les réseaux qui constituent Internet.
Lorsque vous envoyez un e-mail (courriel) depuis votre ordinateur, les données sont envoyées depuis votre ordinateur vers un serveur SMTP. Le serveur SMTP cherche ensuite le bon serveur POP3 et envoie votre e-mail (courriel) à ce serveur, où il attend jusqu'à ce que le destinateur prévu aille le chercher.

9.1.1 Les Comptes E-mail (de courriel)

On trouve des comptes e-mail (de courriel) en de nombreux endroits. Vous pouvez en obtenir un de votre école, de votre employeur, de votre FAI. Lorsque vous obtenez un compte e-mail (de courriel), vous recevez une adresse e-mail (de courriel) constituée de deux parties, de la forme : *nomutilisateur@nom.domaine*. La première partie, *nomutilisateur* vous identifie sur votre réseau, vous différenciant de tous les autres utilisateurs de ce réseau. La deuxième partie, *nom.domaine* est utilisée pour identifier votre réseau spécifique. Le nom d'utilisateur doit être unique à l'intérieur de votre réseau, tout comme le nom de domaine doit être unique parmi tous les réseaux sur internet. Cependant, les noms d'utilisateur ne sont pas unique en dehors de leur propre réseau ; il est possible pour deux utilisateurs sur deux réseaux différents d'avoir le même nom d'utilisateur. Par exemple, si un utilisateur a l'adresse *bill@bignetworks.com*, il n'y aura pas d'autre utilisateur de *bignetworks.com* qui aura comme nom d'utilisateur *bill*. Néanmoins, *bill@bignetworks.com* et *bill@smallnetworks.com* sont deux adresses e-mail (de courriel) valides et qui peuvent appartenir à des utilisateurs différents.
Une des premières choses que vous faites lorsque vous créer un compte e-mail (de courriel) est de configurer votre adresse e-mail (de courriel) dans votre programme client e-mail (de courriel). Votre client e-mail (de courriel) est le programme que vous allez utiliser pour envoyer et recevoir des e-mails (du courriel). Outlook Express de Microsoft est probablement le plus largement connu (puisque il est fourni gratuitement avec chaque copie d'un système d'exploitation Microsoft), mais il en existe beaucoup d'autres disponible pour Windows et Linux, dont Mozilla, Eudora, Thunderbird et Pine.

9.1.2 POP et SMTP

Une fois que votre client e-mail (de courriel) connaît votre adresse e-mail (de courriel), il aura besoin de savoir où aller chercher le courrier entrant et où envoyer le courrier sortant.
Votre courrier entrant sera stocké sur un ordinateur appelé *serveur POP*. Le serveur POP – habituellement nommé *pop.smallnetworks.com* ou *mail.smallnetworks.com* – possède un fichier qui est associé à votre adresse e-mail (de courriel) et qui contient tous les messages que l'on vous a envoyé. *POP* veut dire *Post Office Protocol*.
Votre courrier sortant sera envoyé à un ordinateur appelé *serveur SMTP*. Ce serveur – habituellement nommé *smtp.smallnetworks.com* – va regarder le *nom de domaine* dans l'adresse e-mail (de courriel) de tout courrier envoyé, et va exécuter une *résolution DNS* pour déterminer à quelle serveur POP3 il doit envoyer l'e-mail (le courriel). *SMTP* veut dire *Simple Mail Transport Protocol*,
Lorsque vous lancer votre client e-mail (de courriel), les actions suivantes sont effectuées :
1. le client ouvre une connexion réseau vers le serveur POP
2. le client envoie votre mot de passe secret vers le serveur POP
3. le serveur POP envoie vos messages entrants sur votre ordinateur

4. le client envoie votre courrier sortant vers le serveur SMTP
La première chose à noter est que vous n'envoyer pas de mot de passe au serveur SMTP. SMTP est un ancien protocole, conçu dans les débuts de l'e-mail (du courriel), à une époque où presque tout le monde se connaissait personnellement. Le protocole à été écrit en supposant que tous les utilisateurs seraient dignes de confiance, ainsi SMTP ne vérifie pas que vous êtes bien vous. La plupart des serveurs SMTP utilisent d'autres méthodes pour authentifier les utilisateurs, mais – en théorie – n'importe qui peut utiliser n'importe quel serveur SMTP pour envoyer des e-mails (du courriel). (Pour plus d'informations sur le sujet, voir section **9.2.4 En-têtes Falsifiés.**)
La seconde chose à noter est que lorsque vous envoyer votre mot de passe secret au serveur POP, vous l'envoyer au format texte simple. Il peut être caché par des astérisques sur votre écran d'ordinateur, mais il est transmis sur le réseau dans un format facilement lisible. Toute personne surveillant le trafic réseau – en utilisant un analyseur de paquets réseau (sniffeur) par exemple – sera capable de voir votre mot de passe en clair. Vous êtes peut-être persuadé que votre réseau est sûr, mais vous avez peu de contrôle sur ce qui se passe sur d'autres réseaux empruntés par vos données.
La troisième, et probablement plus importantes des choses que vous devez savoir à propos de vos e-mails (courriels) est qu'ils sont – tout comme vos mots de passe – transmis et stockés au format texte simple. Il est possible qu'ils soient surveillés chaque fois qu'ils sont transmis du serveur à votre ordinateur.
Ceci additionné amène une vérité ; *l'e-mail (le courriel) n'est pas un moyen de transfert d'informations sûr.* Certes, c'est très pratique pour s'envoyer des blagues et des canulars, mais s'il y a quelque chose que vous n'aimeriez pas que votre voisin vous entende dire, vous devriez peut-être y réfléchir à deux fois avant de le mettre dans un e-mail (courriel).
Cela paraît-il paranoïaque ? Et bien, oui, c'est paranoïaque, mais ça ne veut pas dire que ce n'est pas vrai. Beaucoup de nos communications par e-mail (courriel) sont à propos de détails insignifiants. Personne à part vous, Bob et Alice ne s'intéresse à vos projets de repas mardi prochain. Et même si Carole aimerait désespérément savoir où vous, Bob et Alice allez manger mardi prochain, il y a peu de chance pour qu'elle ait un analyseur de paquets tournant sur un des réseaux emprunté par vos e-mails (courriels). Mais si une entreprise est connue pour utiliser l'e-mail (le courriel) pour effectuer des transactions par cartes de crédits, il n'est pas improbable de penser que quelqu'un a, ou essaye de, mettre au point une méthode pour extraire les numéros des cartes de crédits du trafic réseau.

9.1.3 Webmail

Un deuxième moyen d'accéder à l'e-mail (le courriel) est d'utiliser un compte webmail. Ceci vous permet d'utiliser un navigateur web pour traiter vos e-mails (courriels). Etant donné que les e-mails (courriels) de ces comptes sont stockés sur le serveur webmail – et non sur votre ordinateur local – il est très pratique d'utiliser ces services depuis différents ordinateurs. Il est possible que votre FAI vous permette d'accéder à votre e-mail (courriel) des deux façons, POP et web.
Vous devez cependant vous rappeler que ces pages web sont *mises en cache* sur l'ordinateur local pour des durées parfois significatives. Si vous vérifiez vos messages sur un système web depuis l'ordinateur de quelqu'un d'autre, il y a de grandes chances que vos messages soient accessibles par d'autres personnes utilisant ce même ordinateur.
Les comptes webmail sont souvent gratuits et faciles à obtenir. Cela veut dire qu'ils vous offrent la possibilité d'avoir plusieurs identités sur le réseau. Vous pouvez par exemple avoir une adresse e-mail (de courriel) que vous utiliser pour vos amis et une autre pour votre famille. Ceci est habituellement considéré comme acceptable, tant que vous n'essayez pas de tromper intentionnellement qui que ce soit.
Exercices :

1. Vous pouvez en apprendre beaucoup sur la façon dont le courrier POP est récupéré en utilisant le programme telnet. Lorsque vous utiliser telnet au lieu de votre client e-mail (de courriel), vous devez entrer toutes les commandes à la main (commandes que le client e-mail effectue automatiquement). En utilisant un moteur de recherche web, trouver les instructions et les commandes nécessaires pour accéder un compte e-mail (de courriel) au moyen du programme telnet. Quels sont les inconvénients de l'utilisation de cette méthode pour récupérer ses e-mails (courriels) ? Citer quelques avantages potentiels ?
2. Trouver trois organismes qui offrent des services webmail. Quels garanties, si il y en a, offrent-ils quand à la sécurité des e-mails (courriels) reçus et envoyés par ces services ? Utilisent-ils des moyens pour authentifier les utilisateurs.
3. (Eventuellement travail à domicile) Trouver le nom du serveur SMTP de l'adresse que vous utilisez le plus souvent.

9.2 Utilisation Sûre de l'E-mail (du Courriel) Partie 1 : Réception

Tout le monde utilise l'e-mail (le courriel), et à la surprise de beaucoup de gens, votre e-mail (courriel) peut être utilisé contre vous. L'e-mail (le courriel) devrait être traité comme une carte postale, que toute personne qui la regarde peut en lire le contenu. Vous ne devriez jamais mettre dans un e-mail (courriel) ordinaire quoi que ce soit que vous ne voudriez pas divulguer. Ceci dit il y a des moyens de sécuriser votre e-mail (courriel). Dans cette section nous allons traiter de l'utilisation sûre et raisonnable de l'e-mail (du courriel) et comment protéger votre vie privée sur le réseau.

9.2.1 Le Spam (le Pourriel), Le Phishing (le Hameçonnage) et la Fraude

Tout le monde aime recevoir des e-mails (courriels). Il y a bien longtemps, dans une très lointaine galaxie on ne recevait du courrier que de gens que l'on connaissait, et c'était au sujet de choses qui nous concernaient. Maintenant on reçoit des e-mails (courriels) de gens dont on a jamais entendu parler qui nous demande d'acheter des programmes, des drogues et de l'immobilier, sans parler des demandes d'aide pour sortir 24 millions de dollars du Nigeria. Ce type de publicité non-sollicitée est appelée spam (pourriel). Beaucoup de gens sont surpris d'apprendre que les e-mails (courriels) qu'ils reçoivent peuvent fournir beaucoup d'informations à un expéditeur, comme quand le message à été ouvert, combien de fois il a été lu, si vous l'avez envoyé à d'autres, etc. Ce type de technologie – appelé web bugs – est utilisée par les spammeurs et les expéditeurs légitimes. De même, répondre à un e-mail (courriel) en cliquant sur un lien 'se désinscrire' indique à l'expéditeur qu'il a atteint une adresse valide. Une autre intrusion de la vie privée de plus en plus courante est l' attaque par "phishing" (hammeçonnage). Avez-vous jamais reçu un e-mail (courriel) vous demandant de vous logger à votre compte de banque ou E-bay pour vérifier vos informations de compte. Pour se protéger de ce type d'attaques il y a quelques mesures simples que nous allons examiner.

9.2.2 E-mail (Courriel) HTML

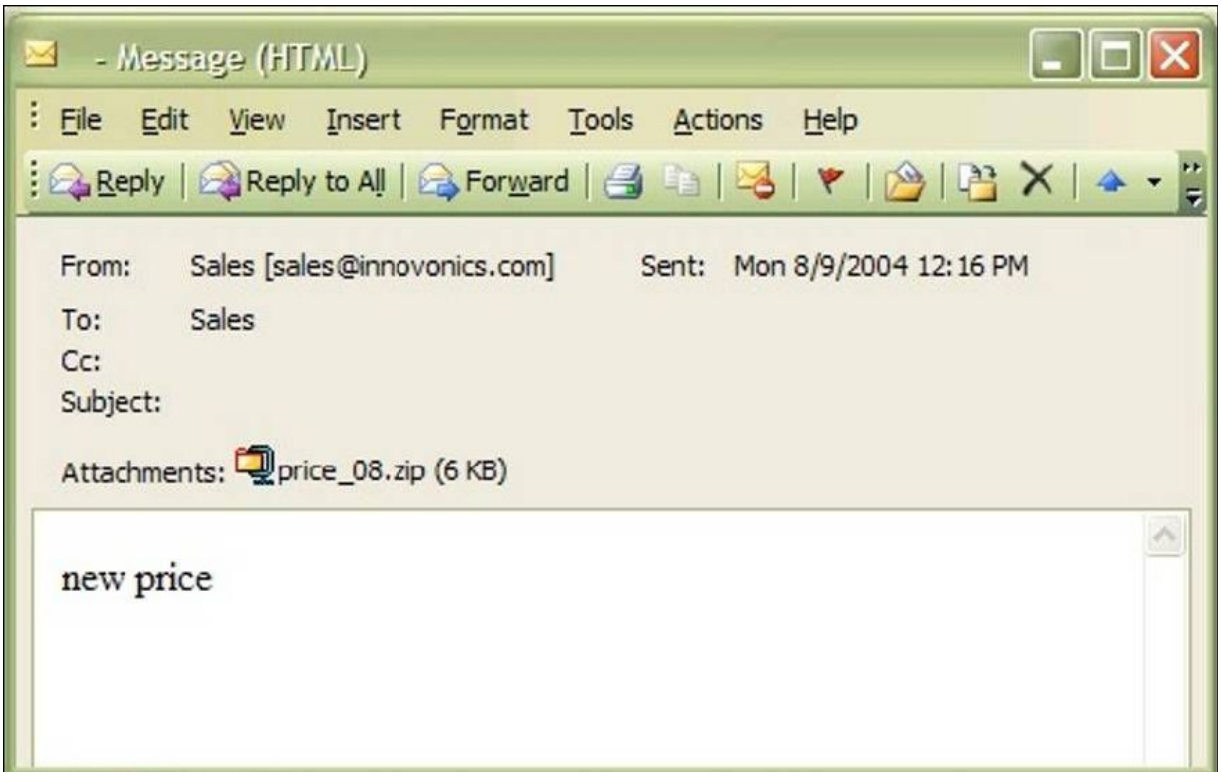
Un des problème de sécurité concernant l'utilisation d'e-mails (courriels) HTML est qu'ils permettent d'utiliser des web bugs. Les web bugs sont des images cachées dans l'e-mail (le courriel) qui contiennent des liens vers le serveur web de l'expéditeur, et l'informe que vous avez reçu ou ouvert le message. Une autre faiblesse des e-mails (courriels) HTML est que l'expéditeur peut inclure des liens dans le message pour identifier la personne qui clique dessus. Ceci peut donner à l'expéditeur des informations sur le statut du message. La règle devrait être d'utiliser un client e-mail (de courriel) qui permet de désactiver le téléchargement automatique des images jointes ou incluses. Un autre problème est lié aux scripts contenus dans le message qui pourraient lancer une application, si votre navigateur web n'a pas été mis à jours avec les derniers correctifs de sécurité.
Pour les clients e-mail (de courriel) utilisant HTML, vous pouvez avoir l'option de désactiver le téléchargement automatique d'images, ou d'afficher les messages au format texte. Les deux sont une bonne mesure de sécurité, Le meilleur moyen de se protéger des attaques contre la sécurité et la vie privée au moyen d'e-mails (courriels) HTML est d'utiliser l'e-mail (le courriel) au format texte,

9.2.3 Sécurité des Pièces Jointes

Un autre vrai problème de sécurité concernant la réception d'e-mails (courriels) sont les pièces jointes. Les attaquants peuvent vous envoyer des logiciels malveillants (malware), des virus, des chevaux de Troie et toutes sortes de vilains programmes. La meilleure protection contre les logiciels malveillants propagés par e-mail (courriel) est de ne jamais rien ouvrir venant de personnes que vous ne connaissez pas. N'ouvrez jamais un fichier avec l'extension . exe ou .src car les fichiers avec ces extensions sont des fichiers exécutables qui pourraient infecter votre ordinateur avec un virus. La bonne façon de procéder serait d'enregistrer toutes pièces jointes sur votre disque dur, et de les analyser avec un programme antivirus, avant de les ouvrir. Méfiez-vous des fichiers qui ressemblent à des types de fichiers connus, comme un fichier zip. Parfois les attaquants peuvent déguiser un fichier en changeant l'icône du fichier ou en cachant l'extension du fichier, et vous ne pouvez savoir que le fichier est exécutable.

9.2.4 En-têtes Falsifiés

De temps en temps vous pouvez recevoir un e-mail (courriel) qui semble provenir de quelqu'un que vous connaissez, ou de "Administrateur" ou "Postmaster" ou "Equipe de sécurité" de votre école ou FAI. Le sujet peut être "Message non délivré" ou "Attaques en cours" ou un autre sujet intéressant. Le problème est que sans connaissance technique et en 10 secondes on peur falsifier une adresse e-mail (de courriel), (Cela peut aussi - suivant où vous habiter - être parfaitement illégal.)
Pour ce faire, il suffit d'une simple modification dans la configuration de votre programme client d'e-mail (de courriel), A l'endroit où vous devez entrer votre adresse e-mail (de courriel) (sous *Options*, *Configuration* ou *Préférences*) entrez une autre adresse. A partir de là, tous les messages que vous envoyez ont une fausse adresse de retour. Cela veut-il dire que vous ne pouvez être identifié ? Non, pas vraiment, Toutes personnes qui sait qui lire un en-tête e-mail (de courriel) et peut effectuer des recherches pourra probablement trouver votre identité à partir des informations contenues dans l'en-tête. Cela implique qu'un spammeur peut se présenter en tant que ce qu'il veut. Ainsi, si Fannie Gyotoku [telecommunicatecreatures@cox.net] vous vends une antenne de téléphone portable magique qui s'avère être une splendide boîte de conserve, vous pouvez vous plaindre à cox.net, mais ne soyez pas étonné s'ils vous répondent que cet utilisateur n'existe pas.
La plupart des FAI authentifient les expéditeurs et empêchent le relaying, ce qui veut dire que vous devez être celui que vous prétendez pour pouvoir envoyer des e-mails (courriels). Le problème est que les hackers et les spammeurs ont souvent leur propre serveur SMTP sur leur ordinateur, et n'ont donc pas à s'authentifier pour envoyer des e-mails (courriels) et peuvent donc se faire passer pour n'importe qui.
La seule façon de savoir si un message est légitime est de connaître l'expéditeur et de l'appeler. Ne répondez jamais à un message que vous pensez être falsifié, car cela indique à l'expéditeur qu'il a atteint une adresse réelle. Vous pouvez aussi voir dans les informations d'en-têtes d'où vient le message, comme dans l'exemple suivant :



Ceci est un e-mail (courriel) venant de quelqu'un que je ne connaît pas, avec une pièce jointes suspecte. Normalement, je l'effacerai simplement, mais je veux savoir d'où il vient. Alors je regarde l'en-tête du message. J'utilise Outlook 2003 comme client e-mail (de courriel), et pour afficher l'en-tête il faut aller dans Affichage>Options et vous verrez les informations d'en-tête suivantes :

```
Microsoft Mail Internet Headers Version 2.0
Received: from srv1.mycompany.com ([192.168.10.53]) by mx1.mycompany.com
over TLS secured channel with Microsoft SMTPSVC(6.0.3790.0);
Mon, 9 Aug 2004 11:20:18 -0700
Received: from [10.10.205.241] (helo=www.mycompany.com)
by srv1.mycompany.com with esmtp (Exim 4.30)
id 1BuEgL-0001OU-8a; Mon, 09 Aug 2004 11:15:37 -0700
Received: from kara.org (67.108.219.194.ptr.us.xo.net [67.108.219.194])
by www.mycompany.com (8.12.10/8.12.10) with SMTP id i79IBYUr030082
for <sales@mycompany.com>; Mon, 9 Aug 2004 11:11:34 -0700
Date: Mon, 09 Aug 2004 14:15:35 -0500
To: "Sales" <sales@mycompany.com>
From: "Sales" <sales@innovonics.com>
Subject:
Message-ID: <cdkdabgurdgefupfhnt@mycompany.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="--------cfwriebwwbnnfkkmojga"
X-Scan-Signature: 178bfa9974a422508674b1924a9c2835
Return-Path: sales@innovonics.com
X-OriginalArrivalTime: 09 Aug 2004 18:20:18.0890 (UTC) FILETIME=
[868FEAA0:01C47E3D]
----------cfwriebwwbnnfkkmojga
```

```
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: 7bit
----------cfwriebwwbnnfkkmojga
Content-Type: application/octet-stream; name="price_08.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="price_08.zip"
----------cfwriebwwbnnfkkmojga—
```

La partie qui m'intéresse est surlignée. Notez que "Received" (reçu) est de kara.org avec une adresse IP qui semble être ligne DSL de chez xo.net, ce qui ne correspond pas à innovonics.com, le prétendu expéditeur.
En outre, si je recherche le serveur mail de innovonics en utilisant nslookup, l'adresse retournée est la suivante :

```
C:\>nslookup innovonics.com
Server: dc.mycompany.com
Address: 192.168.10.54
Non-authoritative answer:
Name: innovonics.com
Address: 64.143.90.9
```

Ainsi mes soupçons étaient justifiés et ceci est un e-mail (courriel) contenant un logiciel malveillant dans un fichier exécutable, se faisant passer pour fichier zip. Le logiciel malveillant à infecté l'ordinateur de la personne sur la ligne DSL, qui est maintenant un zombie, et qui envoie des copies du logiciel malveillant à toutes les adresses trouvées dans le carnet d'adresse de la machine infectée. Je suis bien content de l'avoir vérifié !

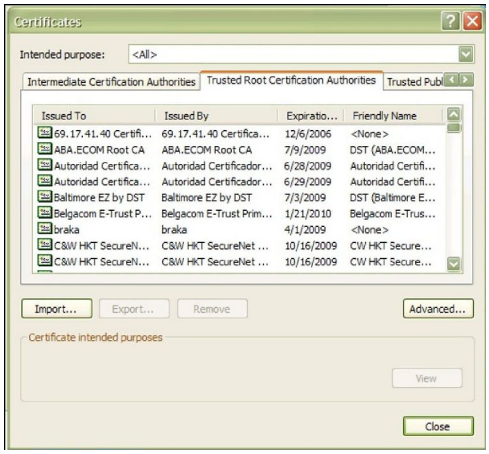
Exercices :
1. Citybank et PayPal sont deux des cibles les plus courantes pour les attaques par phishing (hammeçonnage). Rechercher ce que la Citybank et PayPal font pour contrôler / lutter contre le phishing (hammeçonnage).
2. Recherchez si votre banque ou organisme de cartes de crédits ont des règles éditées à propos de l'utilisation de l'e-mail (du courriel) et des informations personnelles,
3. (Eventuellement travail à domicile) Recherchez un spam que vous avez reçu et essayez de déterminer l'expéditeur réel.

9.3 Utilisation Sûre de l'E-mail (du Courriel) Partie 2 : Envoi

Envoyer des e-mails (courriels) demande moins de précautions. Il y a néanmoins certaines mesures à prendre pour vous assurer que vos conversations soient sûres. La première chose est de s'assurer que votre connexion est sécurisée (voir section **9.4 Sécurité des Connexions** pour plus d'informations). Il existe aussi des méthodes pour signer digitalement vos messages, ce qui garanti que le message vient bien de vous et qu'il n'a pas été modifié en route. Et pour le maximum de sécurité, vous pouvez crypter vos messages afin d'être sur qu'aucune personne non-authorisée ne puisse les lire.
Les signatures digitales prouvent que vous êtes bien l'expéditeur du message et que celui-ci n'a pas été altéré pendant son transfert. Si vous prenez l'habitude d'utiliser les signatures digitales pour vos messages importants, vous aurez une grande crédibilité si vous devez jamais prouver qu'un e-mail (courriel) falsifié ne vient pas de chez vous. Elles permettent aussi de crypter vos e-mails (courriels) de façon à ce personne d'autre que le destinataire ne puissent les lire. PGP en particulier offre de forts taux de cryptage, qui nécessiteraient des capacités de calculs extrêmes pour pouvoir être déchiffrés.

9.3.1 Certificats digitaux

Un certificat digital correspond à une unique personne, un peu comme un permis ce conduire ou un passeport, et est composé de 2 parties. Ces parties sont une clé publique et une clé privée. Le certificat appartient à une unique personne, et est délivré par une Autorité de Certification de Confiance ou CA. La liste des Autorité de Certification en qui vous avez confiance est distribuée automatiquement (si vous êtes un utilisateur de Windows) par Windows Update et la liste est accessible dans votre navigateur web sous Outils > Options Internet > Contenu > Certificats. Vous pouvez aller là pour voir les certificats installé sur votre machine (les vôtres et d'autres), et les autres autorités de certification en qui vous avez confiance.



Vous pouvez désactiver la mise a jour automatique des Cas, et choisir de supprimer toutes les Cas de la liste, même si ce n'est pas recommandé. Des informations sur la marche à suivre se trouvent sur le site web de Microsoft.

9.3.2 Signatures Digitales

Une signature digitale est générée par votre programme e-mail (de courriel) et votre clé privée pour assurer l'authenticité de votre message. Le but de la signature est double. D'une part certifier que le message vient bien de vous. Ceci est appelé la non-répudiation. D'autre part assurer que le contenu du message n'as pas été modifié. Ceci est appelé l'intégrité. La façon dont votre programme e-mail (de courriel) accompli cela est de passer votre message à travers une fonction de hachage à sens unique. Ce processus produit une valeur de sortie de taille fixe
correspondant à votre message, appelé un "message digest" (résumé ou condensé de message). cette valeur est unique, et si l'algorithme de hachage est fort, le message digest a les propriétés suivantes :
- Le message original ne peut être reconstitué à partit de digest
- Chaque digest est unique.

Une fois que le digest est créé, il est crypté avec votre clé privée. Le digest crypté est joint à votre message original avec votre clé publique. Le destinataire ouvre le message, et le digest est décrypté avec votre clé publique. Le digest est ensuite comparé avec un digest généré par le programme e-mail (de courriel) du destinataire. Si les digests sont identiques, le message s'affiche. Dans le cas contraire, le programme e-mail (de courriel) vous informera que le message à été corrompu. Il existe 2 types de fonctions de signature / cryptage, S/MIME et PGP. S/MIME est considéré comme le choix des entreprises et des gouvernements, peut-être parce qu'il utilise un modèle d'autorité de certification pour l'authentification qui nécessite moins de main-d'oeuvre et qu'il est plus facile à implémenter avec le client e-mail (de courriel) Outlook Express de Microsoft. PGP est plutôt le choix de la communauté des utilisateurs, car basé sur un système de confiance non-centralisé, ou la confiance est accordée par le système "l'ami d'un ami" , ou l'on s'accorde que si vous me faites confiance, vous faites aussi confiance au personne en qui j'ai confiance, et parce que les utilisateurs ne s'inquiètent pas s'il leur faut quatre heures pour faire fonctionner PGP avec thunderbird – ils considèrent que ce genre de défi est une forme de récréation.

9.3.3 Obtenir un Certificat

Si vous être intéressé par l'obtention d'un certificat digital ou d'une identité digitale, vous devez contacter une Autorité de Certification (Verisign et thawte sont les plus connues, bien qu'une recherche web vous en trouvera d'autres). Les deux nécessitent que vous fournissiez des informations d'identification pour leur prouver que vous êtes bien qui vous prétendez. Vous pouvez obtenir un certificat gratuit chez thawte, mais ils exigent une quantité significative d'informations personnels, incluant un numéro d'identification du gouvernement (comme un passeport, numéro de contribuable ou permis de conduire). Verisign facture ses certificats et exige que vous payiez par carte de crédits, mais demande moins d'informations personnelles. (Probablement que Verisign se base sur la compagnie de cartes de crédits pour valider vos informations personnelles). Ces demandes d'informations peuvent paraître intrusives, mais rappelez-vous que vous demander à ces entreprises de garantir que vous êtes digne de confiance. Et bien sûr – comme toujours – demandez à vos parents ou tuteurs avant de communiquer quelques informations personnelles que ce soit (or run up large balances on their credit cards).
Le plus grand inconvénient de l'utilisation d'une autorité de certification est que votre clé privée est accessible à quelqu'un d'autre – l'autorité de certification. Si l'autorité de certification est compromise, alors votre identité digitale l'est aussi.

9.3.4 Cryptage

Pour augmenter le niveau de sécurité, vous pouvez crypter vos e-mails (courriels). Crypter vos e-mails (courriels) transformera le texte du message en un ensemble désordonné de chiffres et de lettres, qui ne pourra être lu que par le destinataire prévu. Vos secrets les plus intimes et votre plus mauvaise poésie seront cachés de la vue de tous, sauf des personnes de confiance.
Vous devez cependant garder à l'esprit que, même si cela peut vous paraître très bien - et à nous tous qui n'avons pas particulièrement envie d'être exposé à de la mauvaise poésie - certains gouvernements n'approuvent pas. Leurs arguments peuvent - ou peuvent ne pas - être pertinents (vous pouvez discuter ce point entre vous) , mais la pertinence n'est pas le sujet. Le fait est que, selon les lois du pays dans lequel vous habitez, envoyer un e-mail (courriel) crypté peut être un crime, quelqu'en soit le contenu.

9.3.5 Comment ça Marche ?

Le cryptage est un processus assez compliqué, nous allons donc essayer l'expliquer simplement :
Jason veut envoyer un message crypté. La première chose que fait Jason d'aller chez une autorité de certification et d'obtenir un certificat digital. Ce certificat comporte deux parties, une Clé Publique et une Clé Privée.
Si Jason veut envoyer et recevoir des messages crypter avec son amie Kira, ils doivent d'abord échangé leur Clé Publique. Si vous obtenez une Clé Publique d'une autorité de certification à qui vous faites confiance, la clé peut être vérifiée auprès de cette autorité de certification. Cela veut dire que votre programme e-mail (de courriel) va vérifié que le certificat est valide et n'as pas été révoqué. Si le certificat vient d'une d'une autorité de certification en qui vous n'avez pas confiance, ou est une clé PGP, alors vous devez vérifier l'empreinte de la clé. Ceci est habituellement fait séparément, soit lors d'un échange de clé face à face ou des empreintes digitales.
Maintenant supposons que Kira et Jason utilise un schéma de cryptage compatible et ont échangé des message signés de sorte que chacun a la clé publique de l'autre.
Lorsque Jason veut envoyer un message crypté, le processus de cryptage commence par convertir le texte du message de Jason en un code pré-haché. Ce code est généré en utilisant une formule mathématique appelé algorithme de cryptage. Il existe beaucoup de types d'algorithme, mais pour l'e-mail (le courriel) S/MIME et PGP sont les plus utilisés.
Le code haché du message de Jason est crypté par le programme e-mail (de courriel) en utilisant la clé privée de Jason, Jason utilise ensuite le clé publique de Kira pour crypter le message, de sorte que seule Kira puisse le décrypter avec sa clé privée, et ceci termine le processus de cryptage.

9.3.6 Décryptage

Ainsi Kira a reçu un message crypté de Jason. Ceci est habituellement indiqué dans le message par une icône représentant un verrou dans le programme e-mail (de courriel). Le processus de décryptage est pris en charge par le programme e-mail (de courriel), mais voici ce qui passe en arrière-plan : le programme e-mail (de courriel) de Kira utilise sa clé privée pour décrypter le code pré-haché et le message de Jason. Ensuite le programme e-mail (de courriel) de Kira va chercher la clé publique de Jason stockée (rappeler-vous, ils ont déjà échangé leurs clés). Cette clé publique est utilisée pour décrypter le code pré-haché et vérifier que le message vient bien de Jason. Le programme e-mail (de courriel) de Kira

génère ensuite un code post-haché a partir du message. Si le code pré-haché et le code post-haché sont identiques, le message n'a pas été altéré pendant le transmission.
Note : si vous perdez votre clé privée, vos fichiers cryptés seront utilisables, il est donc important d'avoir une procédure de sauvegarde de vos clés privées et publiques.

9.3.7 Le Cryptage est-il Incassable ?

D'après les chiffres, le niveau de cryptage offert par PGP, par exemple, est incassable. Certainement que un million d'ordinateurs travaillant à le casser pourraient éventuellement réussir, mais pas avant que les millions de singes aient fini d'écrire le manuscrit de *romeo et juliette*, La théorie des nombres utilisée pour ces types de cryptage implique la factorisation de produits de nombres premier très grands, et malgré le fait que les mathématiciens étudient les nombres premiers depuis des années, il n'y a pas de méthode facile pour le faire.
Mais le cryptage et la vie privée ne sont pas qu'une affaire de nombres. Si quelqu'un à accès à votre clé privée, alors il aura accès à tous vos fichiers cryptés. Le cryptage n'est efficace que dans le cadre d'une sécurité globale qui protège votre clé privée et votre phrase de passe.

Exercices :
1. Le cryptage est-il dans le pays où vous résider ? Trouver un autre pays où cela est légal, et un dans lequel c'est interdit.
2. Les auteurs de science-fiction ont imaginé deux types de futur, un dans lequel les vies des gens sont transparentes, et les gens n'ont aucun secret, et un autre dans lequel les communications et les pensées des gens sont complètement privées. Phil Zimmerman, inventeur de PGP, croit en la vie privée en tant que source de liberté. Lisez ses réflexions sur pourquoi vous devriez utiliser PGP sur http://www.pgpi.org/doc/whypgp/en/. Ensuite allez voir l'article de l'auteur de science-fiction Davis Brin 'Une parabole sur la franchise' sur http://www.davidbrin.com/akademos.html dans lequel il relève un certain nombre d'arguments en faveur de la franchise comme source de liberté. Discutez ces deux points de vue opposés. Lequel préférez-vous ? Lequel pensez-vous va s'imposer ? Que pensez-vous que sera l'avenir de la vie privée ?

9.4 Sécurité des connexions

Et finalement, et non des moindres, est la sécurité des connexions. Pour le webmail, assurez-vous que vous utilisez une connexion SSL vers l'e-mail (courriel) de votre FAI. Une petite icône en forme de verrou apparaîtra dans la barre d'état de votre navigateur web. Si vous utilisez POP et un client e-mail (de courriel), assurez-vous d'avoir configuré votre client e-mail pour qu'il utilise POP avec SSL sur le port 995 et SMTP avec SSL sur le port 465. Ceci crypte vos messages entre le serveur et vous, et protège vos nom et mot de passe POP / SMTP. Votre FAI devrait avoir des instructions pour configurer ceci sur leur site, Si il n'offre pas de connexions sécurisées POP / SMTP, changez de FAI !

Exercice :
Si vous avez un compte e-mail (de courriel), trouvez si votre compte est configuré pour utiliser SSL pour ses connexions ? Comment vérifiez-vous ceci dans votre programme e-mail (de courriel) ? Votre FAI fournit-il des informations sur les connexions SSL ?

Pour en savoir plus

Can someone else read my e-mail?
http://www.research.att.com/~smb/securemail.html

MIT's PGP freeware page
http://web.mit.edu/network/pgp.html

General news on Internet privacy issues:
Electronic Privacy Information Center
http://www.epic.org/
and
Electronic Frontier Foundation
http://www.eff.org/

More about PGP
http://www.openpgp.org/index.shtml

How Reading an Email Can Compromise Your Privacy
http://email.about.com/od/staysecureandprivate/a/webbug_privacy.htm

Avoiding E-mail Viruses
http://www.ethanwiner.com/virus.html

A Brief Overview of E-mail Security Questions (with a short advertisement at the end)
http://www.zzee.com/email-security/

A Brief Overview of E-mail Security Questions (with no advertisement)
http://www.claymania.com/safe-hex.html

Windows Based E-mail Precautions
http://www.windowsecurity.com/articles/Protecting_Email_Viruses_Malware.html
http://computer-techs.home.att.net/email_safety.htm

Differences Between Linux and Windows Viruses (with information on why most Linux e-mail programs are more secure)
http://www.theregister.co.uk/2003/10/06/linux_vs_windows_viruses/