6, bd maréchal Juin
F-14050 Caen cedex 4

Spécialité Informatique
1re année

ENSICAEN

Rapport de mini projet

# Le piratage informatique

DOGNION Tiphaine
VANDAMME Julien

Suivi Ensicaen
BRUN Myriam

2e semestre 2005-2006

# Table des matières

# Introduction

Notre projet consiste en la réalisation d'un site Internet permettant à un utilisateur lambda d'appréhender le concept du piratage informatique. Ce site contient les bases concernant la sécurité afin d'apprendre à tout utilisateur comment se protéger.

Nous avons choisi ce sujet afin d'approfondir nos connaissances en matière de sécurité informatique. En effet, ce sujet occupe aujourd'hui une place importante dans ce domaine.

Afin de répondre aux exigences du cahier des charges, il nous a fallu réaliser un site Internet à l'aide du langage HTML accompagné de feuilles de style en CSS et d'un Javascript. De plus, il nous avons procédé à d'importantes recherches.

En effet, lors de la première prise d'informations, nous avons constaté l'étendue du sujet, ce qui nous a incité à le traiter en trois grandes parties. La première consiste à définir qui sont les pirates et leurs techniques d'attaques. La seconde présente les virus ainsi que les menaces liées au réseau. Enfin, nous avons essayé de présenter différents moyens pour se protéger contre les multiples agressions.

# 1 Le piratage informatique

## 1.1Qui sont les pirates ?

Le terme de pirate comprend toutes les personnes qui enfreignent les lois de l'informatique. Le pirate est en fait une personne qui viole les droits d'autrui ou des sociétés à son profit. Les plus communs mais aussi les plus connus sont les hackers, les crackers et toute personne copiant du software pour son utilisation personnelle ou pour la vente.

Le jargon informatique définit trois catégories différentes de hackers suivant le niveau de légalité ou de nuisance dans les réseaux informatiques :

* Les white hat hackers : leur but est d'aider à améliorer des systèmes et technologies informatiques et sont généralement à l'origine des principaux protocoles et outils informatiques que nous utilisons aujourd'hui.

* Les grey hat hackers : ils pénètrent dans les systèmes informatiques illégalement. Ils n'ont pas pour but de nuire, ils recherchent généralement l'exploit informatique dans le but de montrer leur agilité.

* Les black hat hackers : créateurs de virus, cyber-espions, cyber-terroristes et cyber-escrocs, ils sont parfois nuisibles et n'ont pas le même sens de l'éthique que les white hat hackers. Diverses motivations les poussent à agir.

## 1.1 Quelques techniques de piratage

### 1.1.1 Attaques par mots de passe

Pour se connecter à un système informatique, il nous est toujours demandé un identifiant (login ou username) et un mot de passe (password). Ce couple identifiant/mot de passe forme ainsi la clé permettant d'obtenir un accès au système. Bien que l'identifiant soit généralement automatiquement attribué par le système ou son administrateur, le choix du mot de passe revient souvent à l'utilisateur. Or, si les données sur le compte de l'utilisateur n'ont pas un caractère stratégique, l'accès au compte de l'utilisateur peut constituer une ouverture vers le système tout entier.

En effet, dès qu'un pirate obtient un accès à un compte d'une machine, il lui est possible d'élargir son champ d'action en obtenant la liste des utilisateurs autorisés à se connecter à la machine. Le pirate peut alors essayer un grand nombre de mots de passe générés aléatoirement ou s'aider d'un dictionnaire (éventuellement une combinaison des deux) pour entrer dans le système. S'il trouve par hasard le mot de passe de l'administrateur, il obtient alors toutes les permissions sur la machine !

Les mots de passe des utilisateurs représentent donc la première défense contre les attaques envers un système, c'est la raison pour laquelle il est nécessaire de définir une politique en matière de mots de passe afin d'imposer aux utilisateurs le choix d'un mot de passe suffisamment sécurisé.

On appelle «attaque par force brute» ou «brute force cracking», parfois également attaque exhaustive, le cassage d'un mot de passe en testant tous les mots de passe possibles. Il existe un grand nombre d'outils, pour chaque système d'exploitation, permettant de réaliser ce genre d'opération. Ces outils servent aux administrateurs système à éprouver la solidité des mots de passe de leurs utilisateurs mais leur usage est détourné par les pirates informatiques pour s'introduire dans les systèmes.

Les outils d'attaque par force brute peuvent demander des heures, voire des jours, de calcul même avec des machines équipées de processeurs puissants. Ainsi, une alternative consiste à effectuer une «attaque par dictionnaire». En effet, la plupart du temps les utilisateurs choisissent des mots de passe ayant une signification réelle. Avec ce type d'attaques, un tel mot de passe peut être craqué en quelques minutes.

Le dernier type d'attaques de ce genre, appelées «attaques hybrides», vise particulièrement les mots de passe constitué d'un mot traditionnel et suivi d'une lettre ou d'un chiffre (tel que «marechal6»). Il s'agit d'une combinaison d'attaque par force brute et d'attaque par dictionnaire.

Il existe enfin des moyens permettant au pirate d'obtenir les mots de passe des utilisateurs :

* les keyloggers ou «enregistreurs de touches», sont des logiciels qui, lorsqu'ils sont installés sur le poste de l'utilisateur, permettent d'enregistrer les frappes de claviers saisies par l'utilisateur.

* l'ingénierie sociale consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur du réseau ou bien à l'inverse appeler l'équipe de support en demandant de réinitialiser le mot de passe en prétextant un caractère d'urgence ;

* l'espionnage représente la plus vieille des méthodes. Il suffit en effet parfois à un pirate d'observer les papiers autour de l'écran de l'utilisateur ou sous le clavier afin d'obtenir le mot de passe. Par ailleurs, si le pirate fait partie de l'entourage de la victime, un simple coup d'œil par-dessus son épaule lors de la saisie du mot de passe peut lui permettre de le voir ou de le deviner.

### 1.1.2 Usurpation d'adresse IP

L'usurpation d'adresse IP est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.

La technique de l'usurpation d'adresse IP peut permettre à un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage de paquets (pare-feu). Ainsi, un paquet spoofé avec l'adresse IP d'une machine interne semblera provenir du réseau interne et sera relayé à la machine cible, tandis qu'un paquet contenant une adresse IP externe sera automatiquement rejetée par le pare-feu.

Usurper une adresse IP revient à modifier le champ source d'un datagramme IP afin de simuler un datagramme provenant d'une autre adresse IP. Toutefois, sur Internet, les paquets sont généralement transportés par le protocole TCP, qui assure une transmission dite «fiable». Avant d'accepter un paquet, une machine doit auparavant accuser réception de celui-ci auprès de la machine émettrice, et attendre que cette dernière confirme la bonne réception de l'accusé.

Dans le cadre d'une attaque par usurpation d'adresse IP, l'attaquant n'a aucune information en retour car les réponses de la machine cible vont vers une autre machine du réseau : la machine spoofée (on parle alors d'attaque à l'aveugle ou blind attack).

La machine «spoofée» prive donc le hacker de toute tentative de connexion, car elle envoie systématiquement un drapeau RST à la machine cible. Le travail du pirate consiste alors à invalider la machine spoofée en la rendant injoignable pendant toute la durée de l'attaque. Lorsque la machine spoofée est invalidée, la machine cible attend un paquet contenant l'accusé de réception et le bon numéro de séquence. Tout le travail du pirate consiste alors à deviner le numéro de séquence à renvoyer au serveur afin que la relation de confiance soit établie. Pour cela, les pirates utilisent généralement la source routing, c'est-à-dire qu'ils utilisent le champ option de l'en-tête IP afin d'indiquer une route de retour spécifique pour le paquet.

Ainsi, grâce au sniffing, le pirate sera à même de lire le contenu des trames de retour... Ainsi, en connaissant le dernier numéro de séquence émis, le pirate établit des statistiques concernant son incrémentation et envoie des accusés de réception jusqu'à obtenir le bon numéro de séquence.

# 2 Virus et menaces liées au réseau

## 2.1 Qu'est-ce qu'un virus ?

Un virus informatique est un logiciel malveillant écrit dans le but de se dupliquer sur d'autres ordinateurs. Lorsqu'on l'exécute, il se charge en mémoire et exécute les instructions que son auteur a programmées. Il peut avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut aussi se répandre à travers tout moyen d'échange de données numériques comme l'Internet, mais aussi les disquettes, les cédéroms, les clefs USB ...

La définition d'un virus pourrait donc être la suivante : «Tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire.»

## 2.2 Les principaux virus

### 2.2.1 Les vers

Un ver est donc un programme qui peut se reproduire et se déplacer à travers un réseau sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier ...) pour se propager ; un ver est donc un virus réseau. Beaucoup de vers pour causer des dégâts très significatifs, utilisent plusieurs méthodes de propagation ainsi que plusieurs techniques d'infections.

Les vers email (Email Worms) se diffusent grâce à l'envoi d'un message électronique infecté. Il peut-être contenu dans un fichier joint ou dans l'email lui-même. Dans le premier cas, il sera activé quand l'utilisateur cliquera sur le fichier joint pour l'ouvrir et dans le deuxième cas lorsque l'utilisateur cliquera sur le lien qui le mènera sur le site infecté. Le ver email recherche ainsi toutes les adresses dans les carnets d'adresses de la victime, ensuite il s'expédie lui-même et infecte ainsi toutes les adresses trouvées.

Le vers Instant Messaging se propage en utilisant des applications comme l'Instant Messaging, en envoyant des liens de sites infectés. Pour cela, ils se servent des adresses trouvées dans la liste de contact de la ou des victimes. La seule différence entre ces vers et les vers email qui envoient vers des liens est la façon choisie pour envoyer ce lien vers le média.

Il est simple de se protéger d'une infection par ver. La meilleure méthode consiste à ne pas ouvrir à l'aveugle les fichiers qui vous sont envoyés en fichiers attachés. Ainsi, tous les fichiers exécutables ou interprétables par le système d'exploitation peuvent potentiellement infecter votre ordinateur. Les fichiers portant notamment les extensions suivantes sont potentiellement susceptibles d'être infectés : exe, com, bat, pif, vbs, src, doc, xls, msi, eml. Contrairement aux fichiers d'extensions précédemment citées, les fichiers comportant les extensions suivantes ne sont pas interprétés par le système et possèdent donc un risque d'infection minime : txt, jpg, gif, bmp, avi, mpg, asf, dat, mp3, wav, mid, ram, rm.

### 2.2.2 Les chevaux de Troie

Ils utilisent une ruse pour agir de façon invisible, le plus souvent en se greffant sur un programme anodin. Ils font partie des grandes menaces que l'on peut rencontrer sur le web, parmi les virus et autres vers. Pourtant, contrairement à ceux-ci, les chevaux de Troie ne se reproduisent pas. Ce sont à la base de simples programmes destinés à être exécutés à l'insu de l'utilisateur. Il est caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à la machine sur laquelle il est exécuté en ouvrant une porte dérobée (en anglais backdoor). Un cheval de Troie peut par exemple voler des mots de passe, copier des données sensibles ou encore exécuter toute autre action nuisible.

Pire, un tel programme peut créer, de l'intérieur de votre réseau, une brèche volontaire dans la sécurité pour autoriser des accès à des parties protégées du réseau à des personnes se connectant de l'extérieur. Les chevaux de Troie sont des programmes ouvrant des ports de la machine, c'est à dire que son concepteur peut s'introduire sur votre machine par le réseau en ouvrant une porte dérobée. C'est la raison pour laquelle on parle généralement de backdoor.

## 2.3 Les spams

Les spams sont des emails non sollicités envoyés par des expéditeurs inconnus et ce sont presque toujours des offres commerciales. Etant donné que l'envoi de messages est peu coûteux, ces emails publicitaires sont envoyés à des millions d'exemplaires. Le pollupostage est un véritable problème car votre boîte aux lettres est submergée chaque jour de messages ne présentant aucun intérêt pour vous et il vous est de plus en plus désagréable de traiter vos emails. Vous devez être très vigilant pour ne pas manquer un message important parmi vos emails.

# 3 Comment se protéger ?

## 3.1 Les antivirus

Les antivirus s'appuient sur la signature propre à chaque virus pour les détecter. Il s'agit de la méthode de recherche de signature (scanning), la plus ancienne méthode utilisée par les antivirus. Cette méthode n'est fiable que si l'antivirus possède une base virale à jour, c'est-à-dire comportant les signatures de tous les virus connus. Toutefois cette méthode ne permet pas la détection des virus n'ayant pas encore été répertoriés par les éditeurs d'antivirus. De plus, les programmeurs de virus les ont désormais dotés de capacités de camouflage, de manière à rendre leur signature difficile à détecter, voire indécelable : il s'agit de «virus polymorphes».

Il existe plusieurs méthodes d'éradication :

* la suppression du code correspondant au virus dans le fichier infecté;

* la suppression du fichier infecté;

* la mise en quarantaine du fichier infecté, consistant à le déplacer dans un emplacement où il ne pourra pas être exécuté.

Les antivirus peuvent scanner le contenu d'un disque dur, mais également la mémoire de l'ordinateur. Pour les plus modernes, ils agissent en amont de la machine en scrutant les échanges de fichiers avec l'extérieur, aussi bien en flux montant que descendant. Ainsi, les courriels sont examinés, mais aussi les fichiers copiés sur ou à partir de supports amovibles tels que cédéroms, disquettes, connexions réseau...

## 3.2 Le FireWall

Un système pare-feu contient des règles prédéfinies permettant :

* d'autoriser la connexion (allow).

* de bloquer la connexion (deny).

* de rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

* soit d'autoriser uniquement les communications ayant été explicitement autorisées : "Tout ce qui n'est pas explicitement autorisé est interdit".

* soit d'empêcher les échanges qui ont été explicitement interdits.

## 3.3 Quelques mesures de sécurité

Il est aisément compréhensible que plus un mot de passe est long, plus il est difficile à casser. D'autre part, un mot de passe constitué uniquement de chiffres sera beaucoup plus simple à casser qu'un mot de passe contenant des lettres. Un mot de passe de 4 chiffres correspond à 10 000 possibilités (10^4). Si ce chiffre paraît élevé, un ordinateur doté d'une configuration modeste est capable de le casser en quelques minutes. On lui préférera un mot de passe de 4 lettres, pour lequel il existe 456972 possibilités (2^64). Dans le même ordre d'idée, un mot de passe mêlant chiffres et lettres, voire également des majuscules et des caractères spéciaux sera encore plus difficile à casser.

Un ordinateur personnel est capable de tester plusieurs centaines de milliers voire quelques millions de mots de passe par seconde. Cela dépend de l'algorithme utilisé pour la protection mais on voit qu'un mot de passe de seulement 6 caractères, eux-mêmes provenant d'un ensemble de 36 symboles (minuscules ou majuscules accompagnés de chiffres), ne tiendrait pas très longtemps à une telle attaque.

Voici une liste non exhaustive des mots de passe à éviter :

* votre identifiant

* votre nom

* votre prénom ou celui d'un proche (conjoint, enfant, ...) ;

* un mot du dictionnaire ;

* un mot à l'envers (les outils de cassage de mots de passe prennent en compte cette possibilité) ;

* un mot suivi d'un chiffre, de l'année en cours ou d'une année de naissance (par exemple «password1999»).

# 4 Notre projet

## 4.1 Prise d'informations

La recherche de données concernant le piratage informatique s'est d'abord faite sur Internet afin de pouvoir cerner entièrement notre sujet. La quantité d'informations récoltée nous a alors montré l'étendue de ce sujet. Une de nos principales sources est un livre intitulé Tout sur la sécurité informatique par François Pillou. Cet ouvrage est en relation avec le site Internet CommentCaMarche.net qui nous a été d'une grande utilité.

Des informations complémentaires ainsi que les images illustrant notre site ont été trouvées sur de nombreux sites Internet. De plus, nous avons trouvé sur le site www.sunrise.ch quelques animations apportant des compléments clairs à notre projet.

## 4.2 Outils utilisés pour notre site

Notre site utilise principalement le langage html accompagné d'une feuille de style en css pour la mise en forme et d'un fichier de fonctions écrites en javascript. Voir annexes.

## 4.3 Les difficultés rencontrées

La première difficulté a été d'adapter notre site Internet à la fois à Internet Explorer et à Firefox. Pour résoudre ce problème il nous a fallu essayer notre site sur chacun jusqu'à obtenir le résultat souhaité.

La seconde difficulté fut de réaliser un site Internet le plus attractif et intéressant possible afin que le lecteur ne s'ennuie pas. Pour cela, nous avons ajouté des images permettant d'illustrer nos propos ainsi que trois vidéos.

De plus, l'utilisation de fonctions javascript nous a permis de rendre le site un peu plus dynamique.

# Conclusion

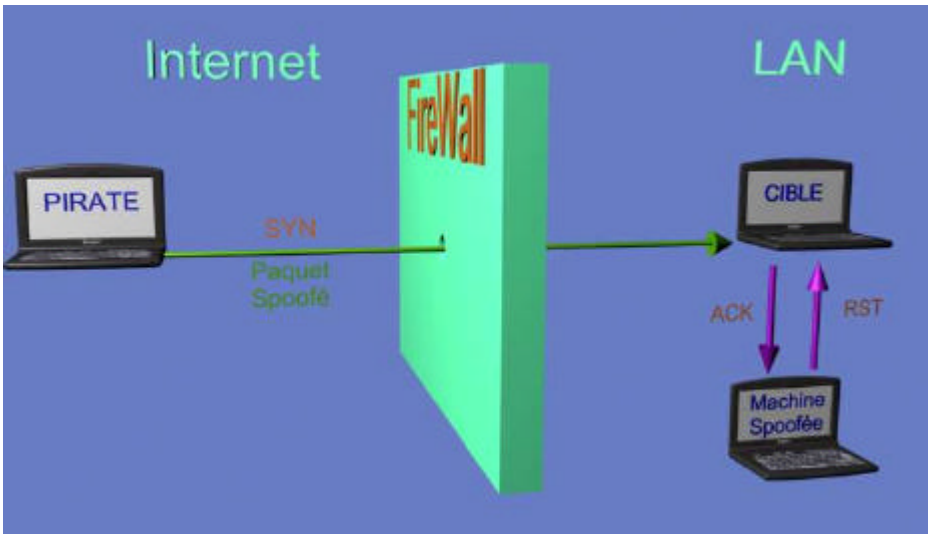
La création d'un site internet accessible à tous nous a poussé à réaliser un travail structuré et le plus exhaustif possible afin de répondre aux questions des utilisateurs. Il nous a aussi fallu adapter notre site pour qu'il s'affiche correctement sur chacun des navigateurs. Enfin, l'organisation et la structure des sources de notre projet permettent facilement d'en changer le contenu ainsi que la forme.

La réalisation de ce dossier nous a permis dans un premier temps d'améliorer nos connaissances du langage HTML et du CSS. Ces deux langages sont à la base de la construction du site Web demandé dans le cahier des charges. De plus, l'utilisation de fonctions écrites en javascript rend notre site plus dynamique. Dans un second temps, la recherche d'informations sur le thème de la sécurité informatique nous a fait prendre conscience de l'importance de ce phénomène dans de nombreux domaines. Nous avons donc pu commencer à assouvir notre curiosité à propos de ce sujet et aspirons à le compléter.

# Annexe A : Schémas

## 1)http://www.ecole.ensicaen.fr/~dognion/Projet1A/projet.html :


## 2)Exemple de schémas : Usurpation d'adresse IP



# Annexe B : Une partie du code HTML

```
<html>
    <head>
    <title>Le piratage informatique par Tiphaine Dognion et Julien Vandamme</title>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1;" />
    <meta name="author" content="Julien Vandamme, Tiphaine Dognion"/>
    <meta name="description" content="Compte rendu du projet de premiere annee"/>
    <link rel="stylesheet" media="screen" type="text/css" title="Style" href="style.css" />
    <script src="affichage.js" language="Javascript" type="text/javascript"></script>

    </head>

    <body>
        <div id="en_tete">
            <table cellpadding="0">
                <tr>
                    <td rowspan="2"  id="logo"></td>
                    <td colspan="3"  id="titre"></td>
                </tr>

                <tr height=54>

                    <td id="sous_titre_gauche"></td>
                    <td id="sous_titre" nowrap>
                        <div class="corps" id="le_site_st">
                            <p >Le site qui vous dira tout !!!</p>
                        </div>
                        <div class="corps" id="piratage_st">
                            <p >Le piratage</p>
                        </div>
                        <div class="corps" id="virus_st">
                            <p >Les Virus</p>
                        </div>
                        <div class="corps" id="securite_st">
                            <p >La s&eacute;curit&eacute;</p>
                        </div>
                        <div class="corps" id="actualite_st">
                            <p >Actualit&eacute;</p>
                        </div>
                        <div class="corps" id="annexe_st">
                            <p >Annexes</p>
                        </div>
                    </td>
                    <td id="sous_titre_droit"></td>

                </tr>
            </table>
```

```
    </table>

</div>

<table id="center">
<tr>
    <td width="128px" valign=top>
        <table id="menu">
            <tr>
                <td valign="center">
                    <a href="#" onclick="return affiche('le_site')">Accueil</a><br/>
                </td>
            </tr>
            <tr>
                <td>
                    <a href="#" onclick="return affiche('piratage')">Le piratage</a><br/>
                </td>
            </tr>
            <tr>

                <td>
                    <a href="#" onclick="return affiche('virus')">Les Virus</a><br/>
                </td>
            </tr>
            <tr>
                <td>
                    <a href="#" onclick="return affiche('securite')">La s&eacute;curit&eacute;</a><br/>

                </td>
            </tr>
            <tr>
                <td>
                    <a href="#" onclick="return affiche('actualite')">Actualit&eacute;</a><br/>
                </td>
            </tr>
            <tr>

                <td>
                    <a href="#" onclick="return affiche('annexe')">Annexes</a><br/>
                </td>
            </tr>
        </table>
```

```
            </td>
            <td id="separateur_vertical"></td>
            <td rowspan="2" valign="top" align="left" >

                <div id="le_site" class="corps">
                    <table class="rubrique"><tr><td>
                    <h3>Pourquoi ce site ?</h3>
                    <P>&#9;Nous sommes actuellement en premi&egrave;re ann&eacute;e
                    informatique &agrave; l'ENSICAEN. Dans le cadre de notre cursus,
                    il nous est demand&eacute; de r&eacute;aliser un projet par
                    bin&ocirc;me de fa&ccedil;on autonome.
                    <br/>&#9;L'objectif du projet est notamment de faire aborder des
                    domaines qui ne sont pas trait&eacute;s dans le cadre des enseignements
                    de l'&eacute;cole.
                    <br/>&#9;Ainsi, notre choix s'est port&eacute; sur l'&eacute;tude
                    du piratage informatique afin d'am&eacute;liorer nos connaissances
                    dans le domaine de la s&eacute;curit&eacute;.
                    </P>
                    </td></tr></table>
                </div>

                <div id="piratage" class="corps">
                    <table class="rubrique"><tr><td>
                    <h2>Introduction</h2>
                    <a href="#" onclick="return new_window('./piratage/presentation.html','presentation')">
                    Qui sont les pirates ?</a><br/>
                    <a href="#" onclick="return new_window('./piratage/motivations.html','motivations')">
                    Les motivations des pirates</a><br/>
                    <br/><br/>
                    <a href="#" onclick="return new_window('./piratage/types_attaques.html','type_attaques')">
                    Les differents types d'attaque</a><br/>

                    </td></tr></table>
                </div>

            </td>
        </tr>
        <tr><td id="deco_sous_menu" colspan="2" valign="top"></td></tr>
        </table>


    </body>
</html>
```

# Annexe C : Une partie du code CSS

```
#titre
{
background-image:url("images/banniere.jpg");
background-repeat:no-repeat;
background-position: center;
height:100px;
}

#titre h1
{
display:inline;
}

#sous_titre_gauche
{
width:100px;
background-image:url('images/deco_entete1.bmp');
}

#sous_titre_droit
{
width:100px;
background-image:url('images/deco_entete2.bmp');
}
#sous_titre
{
color:rgb(104,124,196);
text-align:center;
background-image:url('images/deco_entete_milieu.bmp');
font-weight:bold;
/*font-style:italic;*/
font-size:20px;
font-family:"Arial Black";
}
#sous_titre p
{
display:inline;
}

#separateur_horizontal
{
height:21px;
width:100%;
background-image:url("images/separateurs.bmp");
background-repeat:repeat-x;
}
```

# Annexe D: Une partie du JavaScript

```
// Permet de récupérer tous les éléments dont la classe est "classname"
function getElementByClass(classname)
 {
    //déclarations
    var elt=new Array();
    var alltags=document.getElementsByTagName("*");
    //on parcours tous les éléments du tableau
    for(i=0;i<alltags.length;i++)
        {
            if(alltags[i].className==classname)
                //si on a trouvé le bon on dépile
                elt.unshift(alltags[i]);
        }
        return elt;
}

//Permet de cacher tous les éléments dynamiques
function HideAll()
{
    var sections=getElementByClass("corps");
    for(i=0;i<sections.length;i++)
        {
            sections[i].style.display="none";
        }
}

//permet d'afficher le texte en rapport avec l'élément sur lequel on clique
function affiche(idname)
{
    //il faut d'abort tout cacher
    HideAll();
    document.getElementById(idname).style.display="block";
    //change l'affichage du sous-titre
    document.getElementById(idname+"_st").style.display="inline";
}
```

# Références bibliographiques

[1] Tout sur la sécurité informatique par Jean-François Pillou édition Dunod

[2] www.commentcamarche.net/secu/secuconn.php3

[3] www.xena.ad/lcf/traque/hackers.htm

[4] www.funoc.be/etic/doss004/art002.html

[5] en.wikipedia.org/wiki/

[6] www.symantec.com/region/fr/resources/pirate2.html

[7] www.cases.public.lu/functions/glossaire/index.php?key=S039

[8] wikini.tuxcafe.org/wakka.php?wiki=ActivisteS

[9] www.lefaso.net/article.php3?id_article=12772

[10] www.inoculer.com/vers.php3

[11] www.anti-trojan.info/fr/malwares/vers_réseau/vers_réseau.htm

[12] www.securiteinfo.com/attaques/divers/spyware.shtml

[13] www.sunrise.ch/fr/kundendienst/sicherheit/sicherheit_spam.htm