ENSICAEN
6, bd maréchal Juin
F-14050 Caen cedex
4

Spécialité Informatique
1re année

ENSICAEN

Rapport de projet

Le piratage informatique

DEJOUR Kévin
SOUVILLE Jean-François

Suivi :
Mokhtari-Brun Myriam

2e semestre 2005-2006

Table des matières :

Introduction

Notre projet consiste en la réalisation d'un site Internet à but pédagogique à propos du piratage informatique. L'objectif était de sensibiliser le visiteur, même néophyte en informatique, sur les notions, les menaces, les techniques et les protections relatives au piratage informatique.

Nous avons choisi ce sujet pour l'intérêt que nous avons à propos de la sécurité en informatique, et cela d'autant plus que le piratage est un sujet d'actualité récurrent qui reste mystérieux pour le grand public.

Le résultat de notre travail est disponible à l'adresse: http://projet.piratage.free.fr.

Il n'a pas été difficile de trouver des informations sur le sujet. En effet, Internet regorge de sites contenant des informations sur le piratage, informations souvent complémentaires, mais parfois contradictoires. Ce qui a posé plus de problème a été d'expliquer simplement les différentes notions abordées, ce qui nous a parfois obligé à supprimer certaines notions et explications afin d'alléger le contenu. En contrepartie nous avons rajouté un certain nombre de liens pour les visiteurs voulant approfondir leurs connaissances sur le sujet.

Enfin, le choix de la structure du site s'est fait en accord avec le sujet: puisque le site est destiné pour tout le monde, il se devait d'être simple à utiliser, avec une navigation simple et la mise en valeur de l'information.

1 Les notions du piratage

1.1 Qui sont les pirates ?

Faut-il dire plutôt pirate ou hacker ? On s'est tous posé cette question. Les journalistes et le grand public confondent souvent les termes.

Les pirates désignent des spécialistes en informatiques dont les actions sont nuisibles. Selon leurs actions ils peuvent êtres qualifiés de hackers blacks hats, de crackers ou encore d'hacktivistes. Voici des définitions rapides de ces termes:

Le hacker black hat est un spécialiste informatique qui utilise ses connaissances de façon nuisible. Il doit être différencié du hacker white hat qui est un spécialiste informatique qui n'a pas de but nuisible. Les hackers white hats sont essentiels: ils sont les moteurs de l'informatique moderne et ils contribuent à sa sécurisation.

Le cracker, ou déplombeur de logiciels, est spécialisé dans le cassage des protections des logiciels. Il possède de très bonnes connaissances en assembleur ainsi que des outils (désassembleur, débogueur…) qui lui permettent d'analyser le code d'un programme transmis au processeur. Cela lui permet de neutraliser ou contourner les mesures de protections d'un logiciel en créant un patch (ou crack), ou bien un « keygen » dans le cas de logiciels protégés par des clefs.

L'hacktiviste est un hacker dont les objectifs sont politiques, et emploie ses connaissances en informatique pour diffuser et promulguer ses opinions. Ses actions les plus spectaculaires sont notamment le piratage de sites informatiques en altérant les données, en détournant des serveurs, en remplaçant des pages d'accueil afin de détourner la signification et l'engagement de ces sites.

1.2 Que risque-t-on ?

On entend souvent aux informations qu'un nouveau virus circule. Mais ce n'est pas la seule menace pour nos ordinateurs. Il existe pleins de programmes malveillants, les paragraphes suivants détaillent quelques unes des principales menaces, notre site en présente d'autres en supplément:

Les virus sont des programmes malveillants qui ont pour but de se reproduire. Souvent, ils sont gênants pour l'utilisateur, puisqu'ils peuvent détruire des fichiers sur l'ordinateur.

Les vers sont des programmes qui se propagent d'ordinateur à ordinateur via un réseau comme l'Internet. Ainsi, contrairement à un virus, les vers n'ont pas besoin d'un programme hôte pour assurer leur reproduction. Leurs poids est très léger, ce qui leur permet de se propager à une vitesse impressionnante sur un réseau, et pouvant donc saturer ce dernier.

Les spywares, ou logiciels espions, sont des logiciels nuisibles qui transmettent à des tiers des informations contenues dans votre ordinateur. Les spywares sont souvent présents dans des gratuiciels (différents des logiciels libres), ou des partagiciels. En général les logiciels à code source libre comme Mozilla FireFox n'en contiennent aucun.

Le spamming (ou encore pourriel, courrier rebut) consiste à envoyer des messages appelés "spam" à une ou plusieurs personnes. Ces spams sont souvent d'ordre publicitaire. Tous les points suivants sont considérés comme du spamming.

- Envoyer un même mail, une ou plusieurs fois à une ou plusieurs personnes en faisant de la publicité.
- Poster un ou plusieurs messages dans un forum qui n'a rien à voir avec le thème.
- Faire apparaître un message publicitaire lorsque l'on navigue sur un site.

1.3 Comment font-ils ?

Les pirates sont capables d'inventer des techniques. Mais, évidemment, ils maîtrisent celles qui sont connues. Notre site présente neuf techniques d'attaques, voici les plus connues:

Le reniflage (en anglais Sniffing) est une technique qui consiste à analyser le trafic réseau. Lorsque deux ordinateurs communiquent entre eux, il y a un échange d'informations (trafic). Mais, il est toujours possible qu'une personne malveillante récupère ce trafic. Elle peut alors l'analyser et y trouver des informations sensibles.

Le cracking consiste à trouver les mots de passe des utilisateurs. Pour y arriver un cracker va utiliser un logiciel qui va tenter d'obtenir un mot de passe par différentes méthodes. Afin de lui compliquer au maximum la tâche il convient de suivre quelques consignes comme ne pas utiliser de mot du dictionnaire, de nom, de date de naissance. Par exemple Daniel14 est un mauvais mot de passe, alors que v-lsélt* en est un.

Man in the Middle signifie l'homme du milieu. Cette attaque a pour but de s'insérer entre deux ordinateurs qui communiquent. Soient deux ordinateurs A et B voulant dialoguer. Maintenant, si un pirate décide de se faire passer pour l'ordinateur A auprès de B et pour B auprès de A, toute communication de A vers B ou B vers A passera par l'ordinateur du pirate: l'homme du milieu. Cette attaque permet de voir toute les informations circulant entre A et B, comme des mots de passes, des informations personnelles...

1.4 Comment se protéger ?

Fort heureusement, il existe des logiciels permettant de mettre en place une politique de sécurité et ainsi éviter certaines attaques. Tout le monde a entendu parler du FireWall (pare-feu en français), ou encore de l'antivirus. Voici de quoi il s'agit:

Un antivirus est un logiciel qui a pour but de détecter et de supprimer les virus d'un système informatique. Pour y arriver, l'antivirus dispose de plusieurs techniques comme la recherche par la signature qui consiste à analyser l'ensemble de la mémoire de stockage (disque dur), ou l'analyse heuristique qui consiste à simuler le comportement des logiciels, ou encore l'analyse du comportement qui consiste à surveiller les logiciels actifs.

Un pare-feu (en anglais FireWall) est un système permettant de séparer un réseau interne d'un réseau externe (souvent l'Internet). Il permet de filtrer les communications dans les deux sens et ainsi protéger le réseau interne des éventuelles menaces provenant de l'extérieur.

1.5 Quels sont les outils ?

Après la théorie, la pratique. On sait que beaucoup de choses sont possibles en informatique, mais encore faut-il connaître quelques outils incontournables

sur Linux comme sur Windows. Voici une liste non exhaustive de logiciels utiles:

Nessus est un outil de sécurité permettant de scanner une machine. Il permet aussi de tester différentes attaques pour savoir cette machine est vulnérable.
Nessus se compose d'une partie serveur (qui contient une base de données regroupant différents types de vulnérabilités) et une partie client. L'utilisateur se connecte sur le serveur grâce au client et après authentification, il ordonne au serveur de procéder aux tests. Le client reçoit ensuite les résultats.
Nessus est disponible sous Linux, Windows, Mac... et il est gratuit.

Ethereal est un sniffer et un analyseur de protocoles, il analyse tous les paquets qui circulent sur le réseau et leur contenu.
Ethereal est un logiciel très utilisé pour l'enseignement des protocoles réseaux, ou pour détecter des comportements anormaux du réseau (intrusions extérieures...). Ethereal est disponible sous Linux et Windows et il est gratuit.

Cain est un logiciel "tout en un": il permet le sniffing, le scanning, le cracking, le spoofing... C'est, entre autre, un logiciel qui permet de voir les mots de passe qui passent sur le réseau local. Pour cela Cain sniffe le réseau, ce qui permet ensuite de faire du spoofing et d'analyser le flux entre deux ordinateurs en utilisant la technique du "Man on the middle", cela fait Cain trie les informations qui passe et peut détecter l'envoi d'un mot de passe par exemple.
Si le mot de passe détecté est crypté, Cain intègre un cracker qui va tenter de le décrypter.
Cain est un logiciel très intéressant à utiliser puisqu'il permet de se familiariser avec les possibilités des réseaux informatiques. Cain est disponible uniquement sur Windows.

1.6 Et le réseau sans fil ?

Il est vrai que la plupart des techniques sont portées sur les réseaux classiques. Mais, les réseaux sans fil sont également vulnérables. En effet, il est possible d'aller sur Internet en prenant la connexion de son voisin. Comme pour tout, il existe des parades plus ou moins efficaces. La rubrique « Wifi » explique justement le Wi-Fi, ses faiblesses et donne quelques conseils de sécurité pour éviter d'être victime de piratage. A l'heure actuelle, le Wi-Fi, c'est très bien pour faire du réseau, mais si on peut le remplacer par un réseau classique, c'est encore mieux.

2 La conception du site Web

Le site a pour objectif d'informer n'importe quel utilisateur sur un sujet souvent mystérieux voire inconnu pour lui, c'est donc un site pédagogique qui doit donc être le plus simple possible à utiliser. Nous avons eu une démarche en ce sens dès le début de la conception du site. Cette démarche s'est concrétisée de différentes manières détaillées ci-après.

2.1 L'aspect visuel

Pour un site Web, l'aspect visuel est très important, puisqu'il va non seulement conditionner la première impression du visiteur, mais aussi participer activement à la lisibilité du site. Dans notre cas et dans le cadre des objectifs du projet, c'est le deuxième point qui nous a préoccupé.

La lisibilité d'un site s'assure par différents moyens allant du choix des rubriques à la mise en page.

2.1.1 Le choix des rubriques

Le piratage informatique est un domaine vaste et complexe, et le décomposer en rubriques n'est pas chose aisée. Pour ce faire, nous nous sommes mis à la place de l'utilisateur lambda et des questions qu'il se pose:

- Qu'est ce qu'un pirate?
- Quels sont réellement les risques liés à Internet?
- Comment font les pirates?
- Comment se protéger?

Cela a donné les rubriques: "Les Acteurs", "Les menaces", "Les techniques" et "Les protections".

L'étape suivante a été d'ajouter deux rubriques. La première est intitulée "Les logiciels" où l'on expose quelques logiciels et utilitaires de sécurité sortants du cadre des logiciels de protections. La seconde est intitulée "Le WIFI" qui traite des connexions réseaux sans fil et de leur sécurisation.

La raison du choix de ces deux dernières rubriques est simple: elles permettent d'illustrer et de concrétiser certaines notions vues dans les quatre premières rubriques: par exemple le logiciel Cain illustre les possibilités offertes par la combinaison de techniques d'attaques comme le sniffing, le cracking....

2.1.2 La mise en page

Facteur déterminant de la lisibilité d'un site, la mise en page est un point auquel il faut faire particulièrement attention. Nous avons choisi de respecter quelques règles et principes de bon sens:

- Insérer des images.
- Eviter les gros blocs de textes.
- Séparer les définitions et les sous parties.
- Mettre en valeur les titres des paragraphes.

Ces règles étant définies, nous avons construit le site en les respectant, grâce notamment aux feuilles de styles. Voilà un exemple de ce que cela donne:

2.2 La navigabilité

La navigabilité d'un site Web est un élément essentiel à sa simplicité. Si l'utilisateur se perd dans le site, il partira prématurément et il ne reviendra pas. C'est donc un élément à prendre en compte avant même le début de la conception du site puisque la navigabilité est directement liée à la structure du site.

Pour que le site soit le plus simple possible à utiliser, nous avons choisi une structure basique avec une navigabilité par onglet. Chaque page est composée de

deux parties: la partie inférieure est composée des articles relatifs à la rubrique de la page. La partie supérieure comporte le nom du site au centre, une phrase de bienvenue sur la gauche, le logo de l'ENSICAEN sur la droite, et enfin les onglets en dessous:

L'onglet correspondant à la page en cours possède un contour rouge.

Cette disposition permet à l'utilisateur de voir en un coup d'oeil où il se trouve, et quelles sont les différentes rubriques du site.

Un autre point relatif à la navigabilité est la présence de nombreux liens internes: par exemple dans la page "Les logiciels", on parle de techniques de piratages comme le phishing ou le cracking, ces mots sont cliquables et permettent d'accéder directement à leur définition dans la page "Les techniques".

2.3 Le code

Afin d'assurer l'homogénéité du site dans toutes ses pages, ainsi qu'une navigation simple et rapide, nous avons choisi de faire le code html le plus simple possible, et de rassembler la majeure partie des règles de mise en page dans une feuille de style. (Voir en annexe)

Une des particularités de notre site réside dans les onglets: le code html relatif à ces onglets est une liste:

```
<ul>
        <li id="current"><a href="index.html">Accueil</a></li>
        <li><a href="acteurs.html">Les acteurs</a></li>
        <li><a href="menaces.html">Les menaces</a></li>
        <li><a href="techniques.html">Les techniques</a></li>
        <li><a href="protections.html">Les protections</a></li>
        <li><a href="logiciels.html">Les logiciels</a></li>
        <li><a href="wifi.html">Le wifi</a></li>
</ul>
```

Le résultat final étant obtenue grâce à un certain nombre de règles css en appliquant aux balises « li » et aux balises « a » des propriétés flottantes et deux images de fond respectives. (Voir en annexe la feuille de style).

Conclusion

Ce projet a été pour nous l'occasion d'approfondir nos connaissances et de découvrir certaines choses sur le monde de la sécurité informatique. Nous avons notamment testé quelques techniques et logiciels présentés (sur nos réseaux privées, bien évidemment).

Il a été aussi l'occasion de concevoir un site de A à Z en respectant un cahier des charges, ce qui nous a amené à faire des choix et à trouver les réponses les mieux adaptées au problème: comment faire un site le plus compréhensible possible sur un sujet technique qui est peu connu du grand public.

En terme d'évolution nous pouvons encore compléter le site en complétant la liste des logiciels présentés dans la rubrique correspondante, en rajoutant quelques articles sur des faits réels de piratage, ou encore en approfondissant le contenu avec, par exemple, des explications sur la façon d'utiliser correctement les firewalls ou les anti-virus.

Références bibliographiques

[1] Eric Cole, "Hackers : Attention danger ! ", 2001, CampusPress.

[2] Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky, "Wi-Foo ", 2005, CampusPress.

[3] http://fr.wikipedia.org/wiki/Accueil

[4] http://www.commentcamarche.net

[5] http://www.erwanhome.org/web/hacker.php

[6] http://www.enseirb.fr/~vincent/RSR/RE-320-2004-2005/Wi-Fi-rapport.pdf

[7] http://www.calle-luna.org/article.php3?id_article=76

Annexes

1. Le code source de la page d'accueil

```
<!DOCTYPE HTML PUBLIC "-W3C//DTD HTML 4.0//EN">
<html>
<head>
<title>Comprendre le piratage informatique</title>
<link rel="stylesheet" type="text/css" href="style.css"/>
</head>

<body>
<div id="header">
	<table>
		<tr>
		<td width="20%">
		Bienvenue sur ce site dédié à la sécurité et au piratage informatique !!<br/>
		Ce site a été élaboré dans le cadre d'un projet de première année de l'ENSICAEN.
		</td>
		<td width="60%">
		<p id="titre">Le piratage informatique</p>
		</td>
		<td width="20%"><a id="logoEnsi" href="http://www.ensicaen.fr">
		<img src="images/logo_ensicaen.jpg" width=140 height=140 align="right"/></a>
		</td>
		</tr>
	</table>
	<ul>
		<li id="current"><a href="index.html">Accueil</a></li>
		<li><a href="acteurs.html">Les acteurs</a></li>
		<li><a href="menaces.html">Les menaces</a></li>
		<li><a href="techniques.html">Les techniques</a></li>
		<li><a href="protections.html">Les protections</a></li>
		<li><a href="logiciels.html">Les logiciels</a></li>
		<li><a href="wifi.html">Le wifi</a></li>

	</ul>
</div>
<br/>
<div id="contenu">

	<h3>Edito:</h3>
	<p>
	Tout d'abord, bienvenue sur ce site consacré au piratage informatique.<br/><br/>
		Ce site à pour vocation d'éclairer la lanterne des néophytes en sécurité informatique.
	Par conséquent si vous êtes déjà connaisseur(se), vous risquez de ne pas apprendre grand
	chose!  Mais vous pouvez toujours nous transmettre vos critiques! On se présente pour ça plus
		bas...<br/><br/>
	Pour remplir cet objectif, le site est divisé en plusieurs sections accessibles via les onglets ci-
	dessus. Vous trouverez dans ces sections un certain nombre de définitions, de conseils et
```

```
		autres que l'on a voulus les plus clairs possibles. Cependant la sécurité et le piratage
		informatique sont des domaines très complexes, il se peut donc parfois que vous ne
		compreniez pas certaines notions. N'hésitez pas à nous contacter pour de plus amples
		explications (On se présente aussi pour ça plus bas...).<br/><br/>
		Ceci dit, je vais pas vous retenir plus longtemps avec cet edito alors que vous êtes sûrement
		très impatient de découvrir le contenu du site (oh oui!!!), je vous souhaite donc une bonne
		visite!!
		</p>
		<hr/>
		<h3>Qui sommes nous ?</h3>
		<p>
		Nous sommes deux étudiants en première année à l'école  nationale supérieure d'ingénieur de
		Caen, dans le département informatique (et non, pas en chimie, mais j'avais pas besoin de le
		dire...):
		</p>
		<ul>
			<li>Dejour Kévin</li>
			<li>Souville Jean-François</li>
		</ul>
		<p><br/>
		Vous pouvez nous contacter à l'adresse mail: projet.piratage@free.fr
		</p>
		<hr/>
		<h3>Pourquoi ce site ?</h3>
		<p>
		Ce site à été réalisé dans le cadre d'un projet de fin de première année 2005-2006 à
		l'ENSICAEN, département informatique.<br/>
		Ce projet est encadré par Mokhtari-Brun Myriam (Myriam.Brun@greyc.ensicaen.fr)
</div>
</body>
</html>
```

2. La feuille de style

```
body {
	background: url(images/arrierePlanElec.jpg);
}

img {
	border: 1px solid grey;
}

p {
	text-indent: 1cm;
	margin-left: 25mm;
}

#titre {
	text-indent: 0cm;
	font-size: 9mm;
	font-family: Comic Sans MS;
}
```

```
h1 {
	font-size: 7mm;
	font-family: Comic Sans MS;
}

h2 {
	text-indent: 15mm;
	font-style: oblique;
	font-size: 6mm;
	font-family: Comic Sans MS;
	color: #95444C;
}

h3 {
	text-indent: 20mm;
}

hr {
	text-indent: 0mm;
}

#contenu ul, #contenu ol, #contenu dl {
	margin-left: 25mm;
}


dt {
	text-decoration: underline;
	font-family: Comic Sans MS;
}

dd {
		text-indent: 1cm;
}

#sommaire ul, #sommaire ol {
	margin-left: 0cm;
}

#contenu {
	border: 2px solid silver;
	margin-left: 5%;
	width: 90%;
	background: url(images/arrierePlanTitre.jpg);
}

ul p,ol p {
	text-indent: 4mm;
	margin-left: 0mm;
	text-decoration : none;
}

/*Pour les onglets*/
```

```
#header {
	border: 3px solid silver;
	float:left;
	width:100%;
	line-height:normal;
	text-align: center;
	background: url(images/arrierePlanTitre.jpg);

}

#header ul {
	margin:0;
	padding:10px 10px 0;
	list-style:none;
}


#header li {
	float:left;
	background:url("images/left3.gif") no-repeat left top;
	margin:0;
	padding:0 0 0 28px;
}

#header ul a {
	float:left;
	display:block;
	background:url("images/right3.gif") no-repeat right top;
	padding:9px 28px 4px 0px;
	text-decoration:none;
	font-weight:bold;
	/*color:#92A2AC;*/
	color:#0099CC
}

/* Commented Backslash Hack
   hides rule from IE5-Mac \*/
#header ul a {float:none;}
/* End IE5-Mac hack */

#header a:hover {
	color:#A56060;
}

#header #current {
	background-image:url("images/left3_on.gif");
}

#header #current a {
	background-image:url("images/right3_on.gif");
	color:#A56060;
}
```