Google-Hacking

Google ist nicht nur nützlich, wenn ihr irgendwelche Downloads oder Infos such, sondern ist das Hacker-Tool schlecht hin =D Jetzt fragt ihr euch sicherlich, wie das ganze funktionieren soll, aber keine Angst, es ist ganz einfach =P
Google bietet verschiedene Funktionen an, die ihr in eure Suche einbauen könnt, und damit ganz tolle Ergebnisse bekommt =D Also fangen wir mal an:

intitle:
Die intitle: Funktion such euch nur Webseiten mit einen bestimmten Titel raus. Die Suche nach 'intitle:Welcome' sucht euch zB. Nur Webseiten raus, die im Titel das Wort 'Welcome' haben.

inurl:
Die inrul: Funktion such alle Webseiten raus, die euer Suchwort in der URL beinhalten. So kommen wir mit einer Suche nach 'inurl:admin' zB. An alle Webseiten, die in ihrer URL das Wort 'admin' haben.

filetype:
Mit der filetype: Funktion könnt ihr bestimmen, dass nur Dokumente von einem bestimmten Dateityp durchsucht werden wollen. Die Suche nach 'filetype:c "Hello World"' liefert uns zB. Etliche C-Quellcode Dateien mit Hello-World Programmen.

site:
Die site: Funktion sucht uns nur Webseiten raus, die auf unseren Suchstring passen. 'site:edu' sucht uns zB. Alle .edu Domains heraus. Aber immer daran denken, dass die Suche von Rechts nach Links stattfindet. So würde eine Suche nach 'site=P3pp3r' keine Ergebnisse liefern. Eine Suche nach 'site=P3pp3r.de.vu' jedoch schon. Vielleicht etwas kompliziert erklärt, aber probiert einfach etwas rum =P

So, dass waren auch schon die wichtigsten Bonus-Suchfunktionen von Google. Jetzt liegt es an euch, diese Funktionen richtig zu kombinieren und so an 'wertvolle' Seiten zu gelangen.
Ich werde euch mal ein paar Denkanstöße geben =P

Suchen wir zB. Nach 'intitle:index.of inurl:admin' finden wir unzählige Seiten, die Index-Listing angeschaltet haben und dank inurl:admin finden wir uns dazu meistens in Ordnern mit dem vielversprechenden Namen admin wieder ;) Also schön stöbern, vielleicht ist ja was Interessantes dabei.
Eine Suche nach 'intitle:index.of "Apache/1.3.26 Server at"' liefert uns eine riesige Liste mit Servern, auf denen Apache 1.3.26 läuft.

Zu dieser Technik gibt es ein ausführliches ~30 Seiten langes Paper (in Englisch), das man sich unbedingt durchlesen sollte:
http://johnny.ihackstuff.com/security/premium/The_Google_Hackers_Guide_v1.0.pdf

Suchstrings, die solche wertvollen Informationen offenbaren wurden 'GoogleDorks!' getauft. Ein ziemlich große und täglich Wachsende Sammlung solcher GoogleDorks befindet auf http://johnny.ihackstuff.com. Dort finden wir zB. Den Suchstring 'aboutprinter.shtml'. Wenn wir danach suchen, finden wir einige ungesicherte Xerox Drucker, auf denen wir ohne jegliches Passwort Admin spielen können =P

Wie ihr seht machen GoogleDorks eine riesigen Spaß =D Das Problem ist nur, das öffentlich gepostete GoogleDorks ziemlich schnell ausgelutscht sind. Also immer auf dem neusten Stand bleiben oder noch besser: Selber welche suchen/finden.