Google Hacking Tutorial 2005 Edition

Google Hacking

#1. Vorwort
#2. Wie funktioniert Google?
#3. Einige wichtige Befehle
#4. Richtige Kombination
#5. Passwörter suchen und finden
#6. Web Server Detection
#7. Weitere sensible Daten
#8. Quellen

#1. Vorwort

16 August 2005 / 8.168.684.336 Sites @Google
31 Juli 2004 / 4.285.199.774 Sites @Google

#2. Wie funktioniert Google?
Google ist zu nächst mal eine voll automatische Suchmaschine, die mit Hilfe von so genannten Spidern (Webcrawler/Suchrobotern), das
gesamte Web durchsucht und die gefunden Websites indiziert. D.h. es ist eigentlich nicht mal notwendig seine Website bei Google anzumelden, die Suchrobots werden sie früher oder später sowieso finden.

#3. Einige wichtige Befehle
Bevor wir gleich zum "**Google hacking**" übergehen einige wichtige Befehle, die man in seinem Google Query nutzen kann.

filetype:
Mit filetype lassen sich bestimmte Dateitypen finden.
Bsp: filetype:txt

+
Mit + lassen sich alle Webseiten finden, die ein bestimmtes Wort enthalten.
Bsp: +FBI +Agent

-
Mit - werden nur Seiten gefunden, die ein bestimmtes Wort nicht enthalten.
Bsp: -public –user

intitle:
Per Intitle: lässt sich das <title> tag durchsuchen.
Bsp: intitle:index

intext:
Mit intext: findet man bestimmte Wörter auf einer Webseite.
Bsp: intext:Hacker

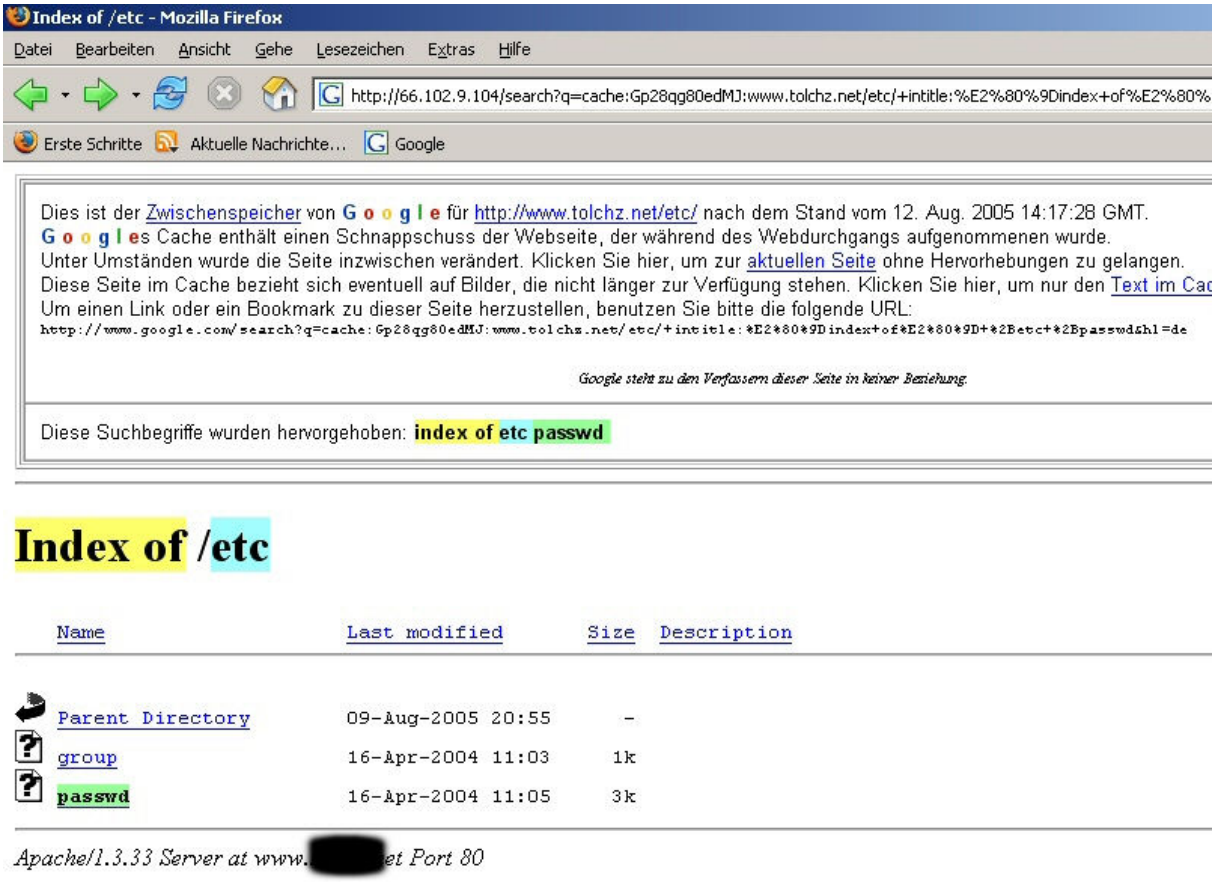
inurl:
Über inurl: lassen sich Wörter in einer URL festlegen.
Bsp: inurl:etc inurl:bin

site:
Mit site: kann man auf bestimmten Domains suchen.
Bsp: site:com site:de

“”
Mit “” lassen sich aufeinander folgende Wörter suchen.
Bsp: “index of”

#4. Richtige Kombination
Das die oben genannten Befehle alleine nicht viel bringen dürfte klar sein, also müssen wir kombinieren.
Bsp:

intitle:”index of” +etc



Über solche Ergebnisse kann man sich nur wundern!

```
man:!:6:6:/tmp:/bin/false
lp:!:7:7:/tmp:/bin/false
nobody:8iDCdEydfoQQk:5000:5000:/home/nobody:/bin/bash
httpd:jgMexQlmAbwGc:5003:5003:/home/httpd:/bin/bash
```

Warum gibt es immer noch Systeme auf denen man ohne Probleme sich über Google, die passwd anschauen kann? Für **potenzielle Cracker** sind solche Umstände ein **El Dorado**.

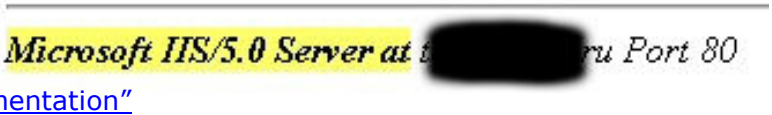
Achtung: Viele vermeintliche, für Google Hacking anfällige Systeme könnten auch sog. **Honeypots** sein (http://ghh.sourceforge.net/).

„Als ein **Honeypot** (deutsche Übersetzung: Honigtopf) wird ein Programm (oder ein kompletter Server) bezeichnet, das die Aufgabe hat, Angriffe in einem Netzwerk auf sich zu ziehen und Aktionen des Angreifers zu protokollieren.“
http://de.wikipedia.org/wiki/Honeypot

#5. Passwörter suchen und finden
Mit Google lässt sich alles finden, auch oder geradezu Passwörter.
Einige Beispiele:

filetype:dat "password.dat"
filetype:ini +ws_ftp +pwd
filetype:log inurl:"password.log"
intitle:Index.of etc shadow
intitle:"Index of..etc" passwd

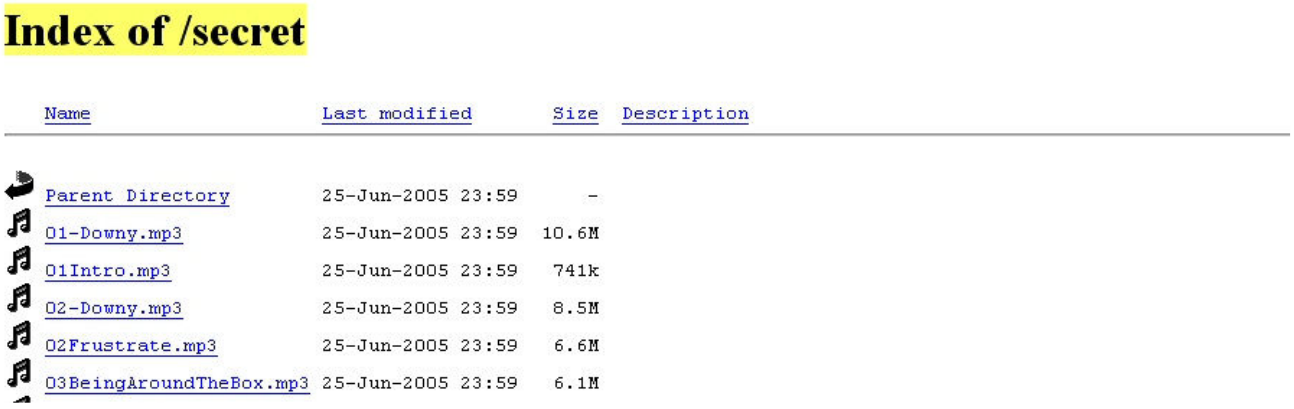
#6. Web Server Detection (Webserver Erkennung)
Es ist dank Google kein Problem mehr Webserver zu identifizieren.
Einige Beispiele:



"Microsoft-IIS/5.0 server at"
intitle:"Apache HTTP Server" intitle:"documentation"
intitle:"Welcome to IIS 4.0"
"powered by openbsd" +"powered by apache"

#7. Weitere sensible Daten in diversen Verzeichnissen
Was man nicht so alles findet…
Einige Beispiele:

intitle:index.of.private
intitle:index.of.secret
intitle:"index.of.secure"



#8. Quellen

http://johnny.ihackstuff.com/
http://www.google.de/
http://de.wikipedia.org/