Google Hacks :-)

><><><><><><><><><><><><><><><by><><Sky.Out><><

Wie benutze ich Google Hacks und was bringen diese mir?

Die im folgenden Dokument beschriebenen Kommandos, also zum Beispiel **site:google.com fox** gibt man ganz einfach in die Suchleiste von Google ein, wie jeden anderen Begriff auch, wenn man bei Google nach etwas sucht. Google beinhaltet verschiedene Kommandos dieser Art (**site**, **intitle** und so weiter) um die Suche einzuschränken und bessere Ergebnisse zu liefern. Das Kombinieren dieser Kommandos verhilft uns nun ganz spezielle Ergebnisse zu erhalten, wie zum Beispiel eine Liste von Apache Servern.

Google-Kommandos

Da Google Hacks „nur“ die Kombination mehrerer Kommandos sind, sollten wir uns erst einmal mit den allgemeinen Google-Kommandos vertraut machen, damit du die vorgehensweise besser verstehen kannst:

site Beschränkt die Ergebnisse auf Seiten, die sich in einer bestimmten Domain befinden

site:google.com fox — Dieser Befehl findet alle Seiten, welche das Wort „fox“ enthalten und sich in der Domain *.google.com befinden

intitle Beschränkt die Ergebnisse auf Seiten, welche den angegebenen Text im Titel enthalten

intitle:fire fox — Dieser Befehl findet alle Seiten, welche das Wort „fire“ im Titel tragen und „fox“ im Text

allintitle Beschränkt die Ergebnisse auf Seiten, welche den angegebenen Text im Titel enthalten

allintitle:fire fox — Dieser Befehl findet Seiten, die sowohl „fire“ als auch „fox“ im Titel enthalten, dieser Befehl ist das gleiche wie „intitle:fire intitle:fox“

inurl Beschränkt die Ergebnisse auf Seiten, welche den angegebenen Text in der URL-Adresse enthalten (www.google.de <= das ist eine URL-Adresse)

inurl:fire fox — Dieser Befehl findet all die Seiten, welche das Wort „fire“ in ihrer URL enthalten und fox im Text

allinurl Beschränkt die Ergebnisse auf Seiten, welche alle angegebenen Wörter in der URL enthalten

allinurl:fire fox — Dieser Befehl findet Seiten, welche sowohl „fire“ als auch „fox“ in der URL enthalten, funktioniert also wie „inurl:fire inurl:fox“

filetype, ext — Beschräkt die Ergebnisse auf Dokumente, welche vom angegebenen Typ sind

filetype:pdf fire oder filetype:doc fire — Der erste Befehl würde all jene Dokumente auflisten, welche vom Typ PDF sind und das Wort fire enthalten, der zweite würde das gleiche für Word-Dokumente bewirken

numrange — Beschränkt die Ergebnisse auf Seiten, welche eine Zahl aus dem angegebenen Zahlenbereich im Content enthalten

numrange:1-100 fire — Dieser Befehl findet alle Seiten, welche eine Zahl aus dem Bereich 1 bis 100 und das Wort „fire“ enthalten, das gleiche würde „1..100 fire“ bewirken

link — Beschränkt die Ergebnisse auf Seiten, welche Links zur angegebenen Lokalisierung enthalten

link:www.google.de — Dieser Befehl findet Seiten, welche mindestens einen Verweis auf „google.de“ enthalten

inanchor — Beschränkt die Ergebnisse auf Seiten, welche Links mit dem angegebenen Text enthalten

inanchor:fire — Dieser Befehl liefert Seiten, welche einen Link mit dem Wort „fire“ in der Beschreibung enthalten, also nicht die URL ist hier entscheidend, sondern das beschreibende Wort

allintext — Beschränkt die Ergebnisse auf Dokumente, die die angebenen Wörter im Text enthalten, jedoch weder im Titel, bei den Links oder der URL-Adresse

allintext:“fire fox“ — Dieser Befehl liefert alle Dokumente, welche „fire fox“ im Text enthalten

\+ — Dieser Befehl ordnet die Seiten nach der Häufigkeit des Auftretens des gegebenen Wortes

+fire — Dieser Befehl würde die Seiten also nach der Anzahl des Auftretens des Wortes „fire“ ordnen

\- — Dieser Befehl liefert Seiten, welche das angegebene Wort nicht enthalten

-fire — Dieser Befehl liefert nur Seiten, welche das Wort „fire“ im Text nicht enthalten

“ “	Dieser Befehl sucht nach Seiten, welche die gesamte Phrase enthalten und nicht nur eines des mindestens zwei Wörter
“fire fox“	Dieser Befehl würde all jene Seiten liefern, welche die Phrase „fire fox“ im Text enthalten und zwar nur Seiten, welche auch wirkliche beide Wörter in dem Zusammenhang enthalten
.	Dieses Zeichen steht stellvertretend für ein beliebiges anderes Zeichen
fire.fox	Dieser Befehl würde also Seiten liefern, welche zum Beispiel das Wort „fire1fox“, „fire2fox“ und ähnliches enthalten, immer genau ein Zeichen
*	Dieses Zeichen steht für ein beliebiges Wort
fire * fox	Dieser Befehl liefert zum Beispiel Seiten welche „fire or fox“, „fire in fox“ und ähnliches im Text enthalten
!	Steht für das aus der Programmierung bekannte OR
„fire fox“ ! firefox	Dieser Befehl liefert alle Dokumente, welche entweder die Phrase „fire fox“ ODER das Wort „firefox“ enthalten

So nun kennen wir schon einmal die Kommandos, welche Google verwendet beziehungsweise welche man verwenden kann, um die Suchergebnisse einzuschränken. Google Hacks sind schließlich logische und trickreiche Kombinationen dieser Kommandos, um ganz spezielle Suchergebnisse zu erhalten.

GOOGLE HACKS IN DER PRAXIS

Suchanfragen nach verschiedenen Typen von WWW-Servern

“Apache/1.3.28 Server at“ intitle:index.of

Hier sieht man einen kleinen Ausschnitt aus dem, was uns Google liefert, wenn wir nach **“Apache/1.3.28 Server at“ intitle:index.of** suchen, rechts sieht man, dass Google 381.000 Treffer meldet, eine enorme Anzahl an Servern dieser Version und ganz einfach zu finden ;-)
Genau das ist das Prinzip der Google Hacks, die Befehle **“ “** und **intitle** kombiniert halfen uns innerhalb kürzester Zeit viele Server zu lokalisieren. Um jetzt herauszufinden welche IP der Server hat können wir unter Windows und Linux schon vorinstallierte Programme verwenden, jedoch auch spezielle Programme. Unter Windows gehst du bitte auf Start > Ausführen > cmd.exe und gibst dann den Befehl „**nslookup**“ ein unter Linux empfehle ich gleich einen Webserver Scanner zu benutzen, dieser führt den Lookup (=URL-Adresse in IP, zum Beispiel „www.google.de“ = 66.102.9.99) automatisch durch und scannt auch gleich auf Lücken, ich kann „**Nikto**“ nur empfehlen.
(Wenn du es richtig gemacht hast, solltest du folgende IP erhalten: **217.24.218.165**)

“Apache/1.3.28 Server at“ intitle:index.of Apache 1.3.28

“Apache/2.0 Server at“ intitle:index.of Apache 2.0 Server

“Apache/* Server at“ intitle:index.of Beliebige Version von Apache Server

“Microsoft-IIS/4.0 Server at“ intitle:index.of Microsoft Internet Information Services 4.0

“Microsoft-IIS/5.0 Server at“ intitle:index.of Microsoft Internet Information Services 5.0

“Microsoft-IIS/6.0 Server at“ intitle:index.of Microsoft Internet Information Services 6.0

“Microsoft-IIS/* Server at“ intitle:index.of Beliebige Version von Microsoft Internet Information Services

“Oracle HTTP Server/* Server at“ intitle:index.of Beliebige Version des Oracle-Servers

“IBM_HTTP_SERVER/* * Server at“ intitle:index.of Beliebige Version eines IBM Servers

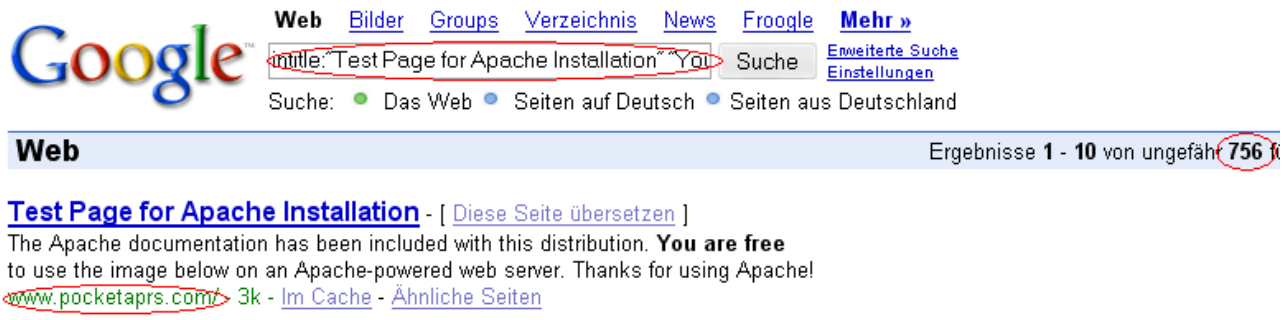
“Netscape/* Server at“ intitle:index.of Beliebige Version eines Netscape Servers

“Red Hat Secure/*“ intitle:index.of Beliebige Version eines Red Hat Secure-Servers

“HP Apache-based Web Server/*“ intitle:index.of Beliebige Version eines HP-Servers

Abfragen nach Standardseiten von WWW-Servern nach der Installation

intitle:“Test Page for Apache Installation“ “You are free“



Mit dem oben gezeigten Befehl erhältst du eine Liste von Apache Servern, welche noch die Standardseite enthalten, dies ist die Seite, welche ein Apache Server kurz nach der Installation aufweist. Mit diesem Kommando finden wir also alle Apache Server, welche gerade neu installiert wurden und somit wahrscheinlich noch nicht gut konfiguriert sind, was es uns einfacher machen wird sie zu hacken.

intitle:“Test Page for Apache Installation“ “You are free“ Apache 1.2.6

intitle:“Test Page for Apache Installation“ “It worked!“ “this Web site!“

Apache 1.3.0 – 1.3.9

intitle:“Test Page for Apache Installation“ “Seeing this instead“ Apache 1.3.11 – 1.3.33, 2.0

intitle:“Test Page for the SSL/TLS-aware Apache Installation“ “Hey, it worked!“

Apache SSL/TLS

intitle:“Test Page for the Apache Web Server on Red Hat Linux“

Apache im Red Hat-System

intitle:“Test Page for Apache Http Server on Fedora Core“ Apache im Fedora-System

intitle:“Welcome to Your New Home Page!“ Debian Apache im Debian-System

intitle:“Welcome to IIS 4.0!“ IIS 4.0

intitle:“Welcome to Windows 2000 Internet Services“ IIS 5.0

intitle:“Welcome to Windows XP Server Internet Services“ IIS 6.0

Programme, die Statistiken über die Systemarbeit erstellen

“Generated by phpSystem“

General Info	
System Time:	Sun Feb 5 13:35:23 EST 2006
Kernel:	Linux 2.4.20-18.7smp
CPU:	2 GenuineIntel Pentium III (Katmai) 596 MHz Processor(s)
Cache:	512 KB
Bogomips:	1192.75
Uptime:	**1:35pm up 69 days, 15:57, 1 user, load average: 0.14, 0.07, 0.13**

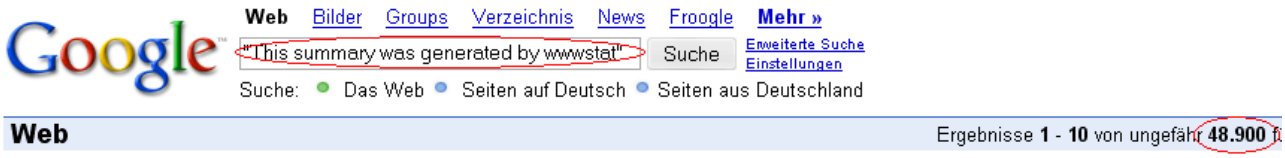
Memory: 1030732 kB		
	Total	Usage	%
Used	1013040	98%
Free	17692 kB	2%
Buffered	219072 kB	21%
Cached	580324 kB	56%

Swap: 265064 kB		
	Total	Usage	%
Used	95020	36%
Free	170044 kB	64%

Partitions					
Mount	Size	Free	Used	Usage	Percent
/	139446064	73527056	58835548		45%
/boot	101089	81547	14323		15%
/dev/shm	515364	515364	0		0%

Generated by phpSystem

In diesem Fall suchen wir nach Seiten, welche Statistiken über den Server zeigen, dies sind meist sehr interessante und hilfreiche Informationen, die zu einem erfolgreichen Angriff beitragen können. Wir erhalten 514 Treffer, also über 500 Server, die uns dank phpSystem ein paar Informationen liefern. Oben sieht man eine derartige Seite, wie sie von phpSystem generiert wird, interessant sind zum Beispiel die Partitionen, welche dort klar aufgelistet werden oder auch die allgemeine Nutzung der Ressourcen. Manch andere Programme liefern sogar noch weit mehr Informationen.



Bei dieser Suchanfrage erhalten wir fast 50.000 Ergebnisse, eine enorme Zahl und Menge an interessanten Informationen.

“Generated by phpSystem“

Typ und Version des Betriebssystems, Hardware-Konfiguration, eingeloggte Benutzer, geöffnete Verbindungen, Belegung der Speicher und der Festplatte, Mount-Punkte

“This summary was generated by wwwstat“

Statistiken über die Arbeit des WWW-Servers, Dateistruktur im System

“These statistics were produced by getstats“

Statistiken über die Arbeit des WWW-Servers, Dateistruktur im System

“This report was generated by WebLog“

Statistiken über die Arbeit des WWW-Servers, Dateistruktur im System

intext:“Tobias Oetiker“ “traffic analysis“

Statistiken über die Systemarbeit in Form von MRTG-Diagrammen, Netzkonfiguration

intitle:“Apache::Status“ (inurl:server-status | inurl:status.html | inurl:apache.html)

Serverversion, Typ des Betriebssystems, Liste der Tochterprozesse und aktuelle Verbindungen

intitle:“ASP Stats Generator *.*“ “ASP Stats Generator“ “2003-2004 wepos“

Aktivität des WWW-Servers, viele Informationen über die Besucher

intitle:“Multimon UPS status page“

Statistiken über die Arbeit der UPS-Geräte

intitle:“statistcs of“ “advanced web statistics“

Statistiken über die Arbeit des WWW-Servers, Informationen über die Besucher

intitle:“System Statistics“ +“System and Network Information Center“

Statistiken über die Systemarbeit in Form von MRTG-Diagrammen, Hardware-Konfiguration, funktionierende Dienste

intitle:“Usage Statistics for“ “Generated by Webalizer“

Statistiken über die Arbeit des WWW-Servers, Informationen über die Besucher, Dateistruktur im System

inurl:“Web Server Statistics fo **“**

Statistiken über die Arbeit des WWW-Servers, Informationen über die Besucher, Dateistruktur im System

inurl:“/asx/ax-admin.pl“ -script

Statistiken über die Arbeit des WWW-Servers, Informationen über die Besucher

inurl:“/cricket/grapher.cgi“

MRTG-Diagramme von der Arbeit der Netzinterfaces

inurl:server-info “Apache Server Information“

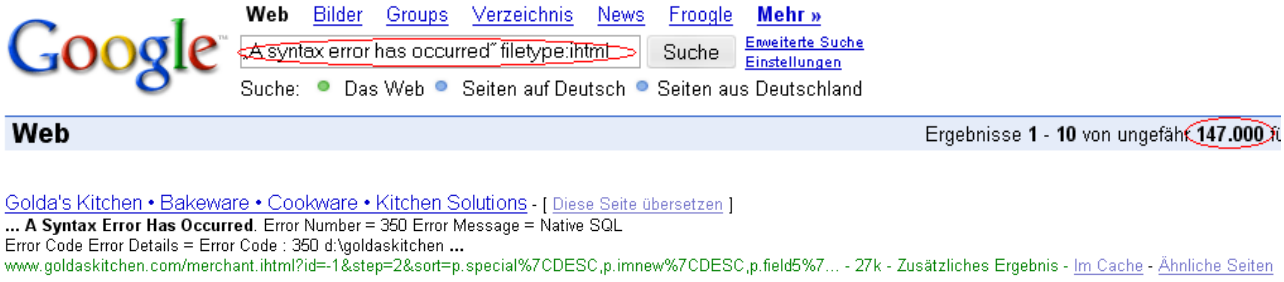
Version und Konfiguration des WWW-Servers, Typ des Betriebssystems, Dateistruktur im System

“Output produced by SysWatch *“

Typ und Version des Betriebssystems, eingeloggte Benutzer, Belegung der Speicher und der Festplatte, Mount-Punkte, aktivierte Prozesse, System-Logfiles

Fehlermeldungen

„A syntax error has occurred“ filetype:ihtml



A Syntax Error Has Occurred

Error Number = 350

Error Message = Native SQL Error Code

Error Details = Error Code : 350
d:\goldaskitchen.com\htdocs\merchant.ihtml
iSQLMORE ALIAS="data" DBNAME="[removed]" LOGIN="[removed]" SQL="
SELECT name
FROM category
WHERE active=1 AND id=:data_parent AND storeid=1"
[Microsoft][ODBC SQL Server Driver][SQL Server]Line 4: Incorrect syntax near ':'.

SELECT name
FROM category
WHERE active=1 AND id=:data_parent AND storeid=1

SQL Error: [Microsoft][ODBC SQL Server Driver][SQL Server]Line 4: Incorrect syntax near ':'.

SQL Statement:
SELECT name
FROM category
WHERE active=1 AND id=:data_parent AND storeid=1

Oben siehst du, dass wir bei der Suche nach **"A syntax error has occured" filetype:ihtml** 147.000 Treffer erhalten, außerdem siehst du noch einen typischen Ausschnitt aus so einer Seite. Aufgrund dieser Fehlermeldung erhalten wir auch hier wieder interessante Informationen, welche auf Dateistruktur und ähnliches schließen lassen. Je mehr Informationen man sammelt, desto besser vorbereitet wird man sein und desto wahrscheinlich ist der Erfolg der ganzen Aktion.

"A syntax error has occured" filetype:ihtml

Fehler der Informix-Datenbank - sie können Funktionsnamen, Dateinamen, Informationen über die Dateistruktur, Fragmente des SQL-Codes und Passwörter enthalten

"Access denied for user" "Using password"

Fehler bei Autorisierung - sie können Benutzernamen, Funktionsnamen, Informationen, Informationem über die Dateistruktur und Fragmente des SQL-Codes enthalten

"The script whose uid is " "is not allowed to access"

PHP-Fehler, die mit der Zugangskontrolle verbunden sind - sie können Dateinamen, Funktionsnamen, Informationen über die Dateistruktur enthalten

"ORA-00921: unexpected end of SQL command"

Fehler der Oracle-Datenbank - sie können Dateinamen, Funktionsnamen und Informationen über die Dateistruktur enthalten

"error found handling the request" cocoon filetype:xml

Fehler des Cocoon-Programms - sie können Versionsnummer von Cocoon, Dateinamen, Funktionsnamen und Informationen über die Dateistruktur enthalten

“Invision Power Board Database Error“

Fehler des Invision Power Board - Diskussionsforum - sie können Funktionsnamen, Dateinamen, Informationen über die Dateistruktur im System und Fragmente des SQL-Codes enthalten

“Warning: mysql_query()“ “invalid query“

Fehler der MySQL-Datenbank - sie können Benutzernamen, Funktionsnamen, Dateinamen und Informationen über die Dateistruktur enthalten

“Error Message : Error loading required libraries.“

Fehler des CGI-Scripts - sie können Informationen über den Typ des Betriebssystems und der Software-Version, Benutzernamen, Dateinamen und Informationen über die Dateistruktur im System enthalten

“#mysql dump“ filetype:sql

Fehler der MySQL-Datenbank – sie können Informationen über die Struktur und den Inhalt der Datenbank enthalten

Passwörter

intitle:“Index of“ pwd.db

Das Aufspüren von passwortenthaltenden Dateien ist per Google einfach zu realisieren, so erhalten wir recht schnell und einfach eine Liste mit derartigen Dateien, im obigen Beispiel listet uns Google Seiten auf, von welchen wir Passwortdateien des Typs „ .db “ herunterladen können, dies ist auf eine schlechte Konfiguration seitens des Administrators zurückzuführen. Solche und ähnliche Ergebnisse erhältst du bei den nachfolgenden Kommandos.

“http://*:*@www“ site

Zeigt Passwörter zur Seite „site“ an, in der Form: http://username:password@www...

filetype:bak inurl:“htaccess|passwd|shadow|htuser“

Backups, der Dateien. Die Informationen über Benutzernamen und Passwörter enthalten

filetype:mdb inurl:“account|users|admin|administrators|passwd|password“

Dateien vom Typ „mdb“, die Informationen über Passwörter enthalten können

intitle:“Index of“ pwd.db

pwd.db - Dateien können Benutzernamen und verschlüsselte Passwörter enthalten

inurladmin inurl:backup intitle:index.of

Verzeichnisse, die in ihrem Namen die Wörter „admin“ und „backup“ enthalten

“Index of/“ “Parent Directory“ “WS_FTP.ini“ filetype:ini WS_FTP PWD

Konfigurationsdateien, des WS_FTP-Programms, die Passwörter zu den FTP-Servern enthalten können

ext:pwd inurl:(service|authors|administrators|users) “# -FrontPage-“

Dateien, die Passwörter des „Microsoft FrontPage“ - Programms enthalten

filetype:sql (“passwd values **“ | “password values ****“ | “pass values ****“)**

Dateien, die SQL-Code und in Datenbanken enthaltene Passwörter enthalten

intitle:index.of trillian.ini

Konfigurationsdatei des Trillian-Messengers

eggdrop filetype:user user

Konfigurationsdatei von Eggdrop-IRCbot

filetype:conf slapd.conf

Konfigurationsdatei der OpenLDAP-Applikation

inurl:“wvdial.conf“ intext:“password“

Konfigurationsdatei des WV Dial-Programms

ext:ini eudora.ini

Konfigurationsdatei des Eudora-Mailprogramms

filetype:mdb inurl:users.mdb

„Microsoft Access“-Dateien, die Informationen über die Konten enthalten können

intext:“powered by Web Wiz Journal“

WWW-Dienste, welche die „Web Wiz Journal“-Applikation benutzen, die in der Standardkonfiguration das Herunterladen der Datei mit dem Passwort ermöglichen; anstelle der Default-Adresse http://<host>/journal schreibt man http://<host>/journal/journal.mdb hinein

“Powered by DUclassified“ -site:duware.com
“Powered by DUcalendar“ -site:duware.com
“Powered by DUdirectory“ -site:duware.com
“Powered by DUclassmate“ -site:duware.com
“Powered by DUdownload“ -site:duware.com
“Powered by DUpaypal“ -site:duware.com
“Powered by DUforum“ -site:duware.com
intitle:dupics inurl:(add.asp | default.asp | view.asp | voting.asp) -site:duware.com

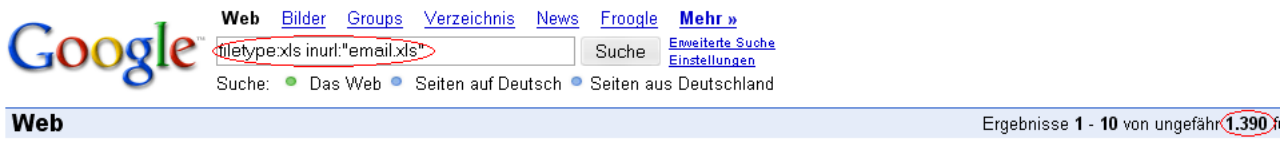
WWW-Dienste, welche die DUclassified, DUcalendar, DUdirectory, DUclassmate, DUdownload, DUpaypal, DUforum oder DUpics verwenden, welche in der Standardkonfiguration das Herunterladen der Datei mit dem Passwort ermöglichen; anstelle der Default-Adresse (z.B. für DUclassified) http://<host>/duClassified/ schreibt man httP://<host>/duClassified/_private/duclassified.mdb hinein

intext:“BiTBOARD v2.0“ “BiTSHiFTERS Bulletin Board“

WWW-Dienste, welche die „Bitboard2“-Applikation verwenden, die in der Standardkonfigurationdas Herunterladen der Datei mit dem Passwort ermöglicht; anstelle der Default-Adresse http://<host>/forum/forum.php schreibt man http://<host>/forum/admin/data_passwd.dat hinein

Such nach personenbezogenen Daten und sensiblen Dokumenten

filetype:xls inurl:“email.xls“



[XLS] email
Dateiformat: Excel 2002 - HTML-Version
email. A, B, C. 1, 2, Name. House #. E MAIL address. 3, Jerry and Angela Davis. 3467. 4, Ron, Millie and Devin Wilson. 3479. rwilson4@cfl.rr.com. 5, Pat and Maria ...
www.geocities.com/fortnelsonlane/Email.xls - Zusätzliches Ergebnis - Ähnliche Seiten
[Weitere Ergebnisse von www.geocities.com]

Name	House #	E MAIL address
Jerry and Angela [redacted]	3467	
Ron, Millie and Devin [redacted]	3479	nwilson4@[redacted]rr.com
Pat and Maria [redacted]	3472	[redacted] mel@hotmail.com

Hier sieht man recht eindrucksvoll, wie leicht und schnell man an Email-Adressen kommt, mit zugehörigem Vor- und Nachnamen der jeweiligen Personen. Solche Dokumente, wie dieses, welche personenbezogene Informationen enthalten, können uns helfen mehr über eine Person herauszufinden oder über die Firma, für welche die jeweilige Person arbeitet. Diese Informationen können durchaus zu einem erfolgreichen Angriff verhelfen.

filetype:xls inurl:“email.xls“

email.xls-Dateien, welche Daten wie Telefonnummern und Adressen enthalten können

“phone * * *“ “address *“ “e-mail“ intitle:“curriculum vitae“

CV-Dokumente (curriculum vitae = Lebenslauf)

“not for distribution“ confidential

mit der „confidential“-Klausel versehene Dokumente

buddylist.blt

Kontakliste des „AIM“-Messengers

intitle:index.of mystuff.xml

Kontakliste des „Trillian“-Messenger

filetype:ctt “msn“

Kontakliste des „MSN“-Messengers

filetype:QDF QDF

Datenbank des Finanzprogramms „Quicken“

intitle:index.of finances.xls

finances.xls-Dateien, die Informationen über Bankkonten, Finanzaufstellungen und Kreditkartennummern enthalten können

intitle:“Index of“ -inurl:maillog maillog size

maillog-Dateien, welche Emails enthalten können

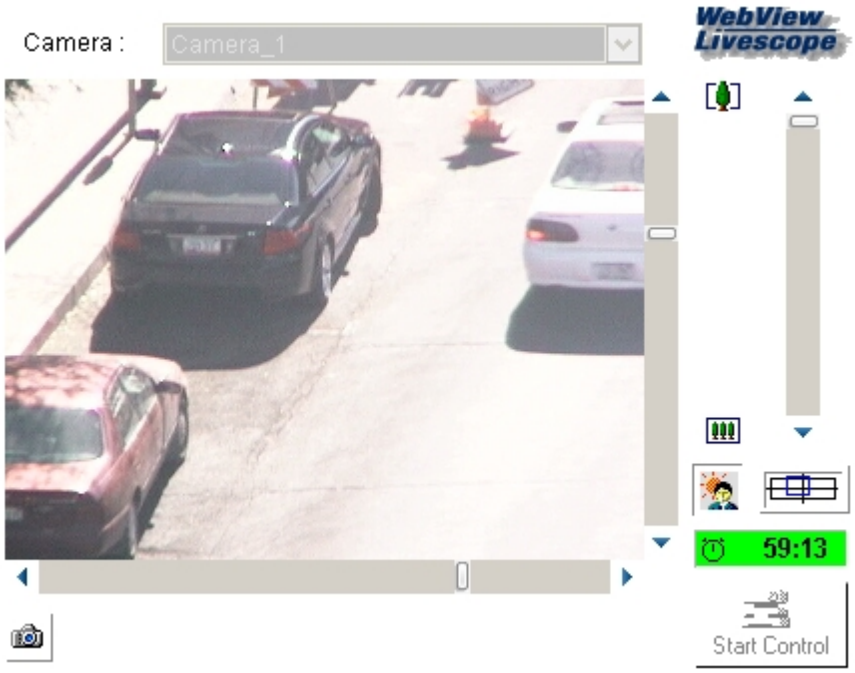
“Network Vulnerability Assessement Report“
“Host Vulnerability Summary Report“
filetype:pdf “Assessement Report“

“This file was generated by Nessus“

Berichte über die Untersuchung der Netzwerksicherheit, Penetrationstests etc...

Charakteristische Zeichenfolgen für Netzgeräte

intitle:liveapplet inurl:LvAppl



In diesem Beispiel sucht man nach physischen Geräten, welche mit dem Internet verbunden sind, hier sieht man zum Beispiel eine Webcam, welche sich ganz einfach kontrollieren lässt, man kann sie in alle Richtungen bewegen. Dies ist eher als Spaß anzusehen, solche Suchergebnisse werden uns bei dem Einbruch in ein Computersystem nicht weiterhelfen.

“Copyright (c) Tektronix, Inc.“ “printer status“ PhaserLink-Drucker

inurl:“printer/main.html“ intext:“settings“ Brother-Drucker

intitle:“Dell Laser Printer“ ews Dell-Drucker mit der EWS-Technologie

intext:centreware inurl:status Drucker Xerox Phaser 4500/6250/8200/8400

inurl:hp/device/this.LCDispatcher HP-Drucker

intitle:liveapplet inurl:LvAppl Canon-Webview-Webcams

intitle:“EvoCam“ inurl:“webcam.html“ Evocam-Webcams

inurl:“ViewerFrame?Mode=“ Panasonic Network Camera-Webcams

(intext:“MOBOTIX M1“ | intext:“MOBOTIX M10“) intext:“Open Menu“ Shift-Reload

Mobotix-Webcams

inurl:indexFrame.shtml Axis Axis-Webcams

SNC-RZ30 HOME Sony SNC-RZ30-Webcams

intitle:“my webcamXP server!“ inurl:“:8080“

über die WebcamXP Server-Applikation vefügbare Webcams

allintitle:Brains, Cop. Camera über die mmEye-Applikation verfügbare Webcams

intitle:“active webcam page“ Webcams mit USB-Interface

><><><><><><><><><><><><><><><><><><><><><

Nun noch ein paar abschließende Worte zum Schluss.
Wie wir gesehen haben lassen sich mit Google Informationen und Dokumente verschiedenster Art finden, seien es Email-Adressen, geheime Dokumente oder sogar physische Geräte, wie Webcams, all dies macht nicht nur Spaß, sondern ist auch sehr aufschlussreich für den Hacker, welcher den Einbruch in ein System plant. Generell gilt, auch wenn du ungeschützte Server über Google sehr leicht findest, so ist das Einbrechen in diese weiterhin verboten und du solltest dir über das, was du tust immer bewusst sein. Überdies sollte es nicht dein Ziel sein, dieses Dokument zu benutzen um möglichst viele potenzielle Opfer zu finden, nur um Schaden anzurichten, vielmehr soll es ein besseres Sicherheitsbewusstsein schaffen.

><><><><><><><><><><><><><><><><><><><><><

DIESES DOKUMENT ENTSTAND ALS TUTORIAL FÜR „PROJECT-69“, ES IST ÜBERDIES AUCH AUF MEINER WEBSEITE VERFÜGBAR , SOWIE VIELE WEITERE DOKUMENTE.

..::-- www.project-69.com --::..

..::-- www.sky-out.de.vu --::..
..::-- sky_out@gmx.net --::..

Für weitere Informationen besuchst du am besten folgende Webseite:

http://johnny.ihackstuff.com/