



SUCHMASCHINE ALS HACK-WERKZEUG

HACKER-GUCKER

Eine Suchmaschine ist eigentlich ein harmloses und nützliches Werkzeug. Man kann sie aber auch als Einbruchswerkzeug benutzen. Lesen Sie, wie Hacker Google für ihre Zwecke gebrauchen und ahnungslose Betreiber von Web-Servern auszutricksen.

VON SEBASTIAN SCHREIBER

Die Bezeichnung Google-Hacking geht auf den amerikanischen Meister-Hacker und Sicherheitsspezialisten Jonny Long zurück. Er beschreibt damit die Suche nach Schwachstellen und verwundbaren Systemen mit Hilfe der Suchmaschine Google. Ein Beispiel: Manche Webshops übergeben den Preis ihrer Produkte tatsächlich über die

Adresszeile des Browsers. Jeder kann diesen Preis einfach in seinem Browser nach seinen Vorstellungen ändern. Damit zeigt so ein schlecht programmierter Shop nicht mehr den Preis des Händlers, sondern den des Kunden an. Passt der Shop-Besitzer nicht auf, kann ein Hacker sehr billig einkaufen gehen. Um diese Schwächen zu entdecken, braucht man keine speziellen Hacker-Tools. Google genügt.

Hacker sind aber weder auf Google noch auf eine andere Suchmaschine beschränkt. Jede Suchmaschine oder auch Skripte können nach verwundbaren Webservern suchen. Oder aber der Anwender kann selbst gemütlich mit einem Browser „von Hand“ arbeiten. Es gibt unglaublich viele Standard-Installationen von (Web-)Servern und anderen Diensten im Internet, die ihre Schwachstellen hemmungslos an Browser, Suchmaschinen und Skripte verraten.

Damit eine Schwäche oder eine Fehlkonfiguration mit einer Suchmaschine gefunden werden kann, müssen nur zwei Voraussetzungen erfüllt sein.

Das Problem muss von der Suchmaschine indizierbar sein und sollte sich optimalerweise immer in einem festen Muster darstellen. Ein weiteres Beispiel: Im Januar dieses Jahres

meldete Cisco (www.cisco.com/warp/public/707/cisco-sa-20060126-vpn.shtml), dass die VPN 3000 Concentrator (Geräte, die VPN-Verbindungen [Virtual Private Network] vermitteln) anfällig gegenüber einem Denial-of-Service-Angriff sind. So ein Angriff kann die Systeme für einen bestimmten Zeitraum vollständig lahm legen.

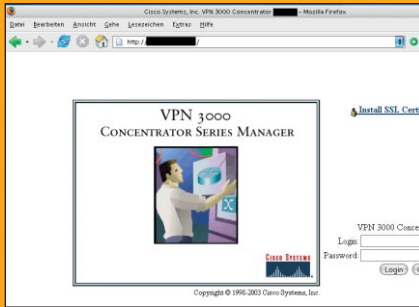
In Web-Foren war zu lesen, dass der Angriff dem HTTP-Interface gilt, das eigentlich vom Web aus nicht erreichbar sein sollte. Es wird nämlich nur zur Verwaltung des Geräts mit dem Browser benötigt. Der Administrator sollte sich deshalb besser selbst per VPN einloggen, um das System zu verwalten. Allerdings ist das nicht bei allen Anwendern der Fall. Interessiert sich ein Angreifer für die erwähnten VPN-Concentrator, muss er also nach Geräten suchen, bei denen dieses Interface versehentlich (oder absichtlich) vom Internet aus erreichbar ist. Warum soll man für diese Suche nicht Google verwenden?

Die Voraussetzungen Indizierbarkeit und festes Muster sind erfüllt. Die Site ist über das Internet erreichbar, also indizierbar. Der Administrator kann die Weboberfläche eines VPN Concentrator nicht modifizieren. Sobald man deren Aussehen kennt, ist eine Suche ohne weiteres möglich:

Erweiterte Google-Befehle

- 🔍 **inurl:** Suche nach Text innerhalb der URL, bis auf das Protokoll-Feld (<http://>).
- 🔍 **intitle:** Suche nach Text innerhalb des Seitentitels, also innerhalb der HTML-tags `<title>` und `</title>`.
- 🔍 **filetype:** Die Suche auf bestimmten Dateityp anhand der Dateinamenserweiterung einschränken. *Filetype* verlangt einen Suchparameter nach dem Muster: *filetype:doc*.
- 🔍 **intext:** Suche auf den Text beschränken, z.B. Text innerhalb von Links nicht beachten.
- 🔍 **site:** Suche auf einen Server oder eine bestimmte Domain einschränken.

Lesen Sie mehr dazu in PC Magazin 4/2005, Seite 32ff.



Hat ein Hacker die Startseite eines VPN Concentrators mit Google gefunden, kann er versuchen, das Passwort zu knacken.



Drucker im Web: Ist ein Printserver – so wie dieser – falsch konfiguriert, können ihn Hacker vom Web aus fernsteuern.

Die Angabe *VPN Concentrator 3000 Series Manager* bei Google führt nicht zum Erfolg, denn der Begriff befindet sich innerhalb eines Bildes. Die anderen Text-Elemente der Seite eignen sich nur beschränkt zum Suchen, da es sich um allzu gängige Begriffe handelt. Außerdem muss man einen großen Aufwand betreiben, um Support-Seiten von Cisco, Preislisten, Handbücher und ähnliches auszuschließen.

Unverwechselbar ist aber der Titel der Webseite *Cisco Systems, Inc. VPN 3000 Concentrator*. Mit dem erweiterten Suchoperator *intitle:* kann damit nach den Concentratoren gesucht werden.

Der Hacker gibt einfach folgende Zeile in Google ein:

```
intitle:"Cisco Systems, Inc. VPN 3000 Concentrator"
```

Der Fehler der Betreiber dieser VPN Concentratoren ist, dass diese Seite im Internet erreichbar ist. Sie kann damit ohne weiteres von einer Suchmaschine indiziert werden. Der Angreifer kann Google verwenden, um das Standard-Passwort der Concentratoren herauszufinden oder gar einen direkten Passwort-Rate-Angriff auf die Systeme zu starten. Dieser Angriff ist allerdings strafbar, im Gegensatz zum reinen Betrachten der Webseite.

Printserver im Visier

Dieses Vorgehen kann praktisch auf alle Systeme angewendet werden, die eine statische Webseite oder unveränderbare Elemente in der Webseite haben. Dies ist z.B. bei Druckern oder genauer gesagt deren Printservern der Fall.

Eine Suche nach dem Titel mit *intitle:* wird hier fehlschlagen, da die Seite keinen hat. Außer-

dem ist die Suche nach Textelementen schwierig, da diese hier sehr allgemeine Begriffe und zum anderen je nach Druckertyp unterschiedlich sind. Identisch und eindeutig ist aber das CGI-Skript *sts_index.cgi*, das über die URL aufgerufen wird. Ein Angreifer benutzt also den Suchoperator *inurl:*, mit dem nach Bestandteilen der URL gesucht wird. Er gibt also folgende Zeile in Google ein:

```
inurl:sts_index.cgi
```

Auch hier kann der Betreiber der Printserver die Struktur der Seite nicht ändern. Das Suchergebnis kann der Angreifer zu weiteren Schlussfolgerungen verwenden: Wenn ein Drucker im Web erreichbar ist, sind es die druckenden Clients vielleicht ebenfalls.

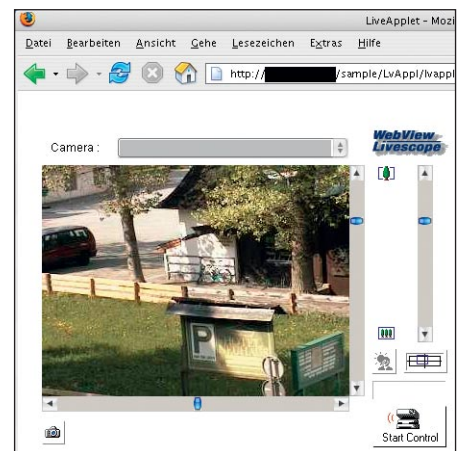
Suche nach Webcams

Problematischer wird die Suche, wenn der Seiteninhalt, den ein Gerät anzeigt, ein Java-Applet ist. Die Suchmaschine kann die Elemente nicht indizieren, weil sie Applets nicht ausführen kann. In diesem Fall helfen die Operatoren *inurl:* und *intitle:* weiter, wie z.B. bei manchen Webcams.

Für ein möglichst unverfälschtes Suchergebnis könnte ein Angreifer folgende Kombination verwenden:

```
inurl:LvAppl intitle:LiveApplet
```

Selbstverständlich beinhalten die Suchergebnisse auch Kameras, die absichtlich erreichbar sind. Ähnlich wie bei den VPN Concentratoren und den Druckern ist hier das Gerät nicht der Grund, warum es mit Google gesucht werden kann, sondern der integrierte Webserver. Bei derartigen Geräten hat der Suchende fast immer den Vorteil, dass der Betreiber die Webseite nicht ändern kann.



Mit den richtigen Suchwörtern finden Sie auch Webcams in Google. Ob jeder Besitzer weiß, dass seine Kamera öffentlich ist?

Schwacher VNC-Server

Dies gilt auch für *http*-basierte Anwendungen aller Art. Diese reichen von administrativen Werkzeugen bis zu Statistik-Tools für Webserver. Ein Beispiel für eine für den Angreifer interessante Anwendung ist VNC, das ebenfalls eine Weboberfläche anbietet.

Auch hier handelt es sich um ein Java-Applet, und zudem läuft die Anwendung nicht auf dem Standard-Port für *http*, 80, sondern auf Port 5800 – dies ist aber Bestandteil der URL und ermöglicht daher eine Suche in der Form:

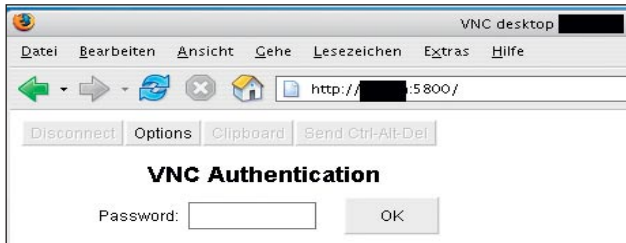
```
inurl:5800 intitle:VNC Desktop
```

Auch hier ist der Dienst für den Angreifer ein interessantes Ziel für eine Passwort-Rate-Attacke.

Sicherheitstest mit Google

inurl: und *intitle:* sind bereits allein mächtige Operatoren für die Suche nach Anwendungen oder Geräten. Sie können dies nach folgendem Prinzip leicht selbst überprüfen: Schauen Sie sich eine beliebige Webanwendung in Ihrem Intranet an und achten Sie auf

Man braucht keine speziellen Hacker-Tools, Google genügt.



Die Portnummer und der Titel der Administrator-Seite haben diesen VNC-Server an Google-Surfer verraten.



So schützen Sie sich vor Suchmaschinen-Hacks!

1 Ordnung halten

Räumen Sie nach getaner Arbeit auf. Entfernen Sie alles vom Webserver, was nicht gebraucht wird, angefangen bei der Dokumentation des Webserver oder weiterer Anwendungen, bis zu Sicherheitskopien, die Editoren angelegt haben, Beispieldateien und alte Versionen von Skripten usw. Wenn mehrere Personen Inhalte auf den Seiten ablegen können oder das System sogar gemeinsam administriert wird, kommen Sie nicht umhin, gelegentlich selbst zu prüfen, ob auch nur gewünschte Inhalte online sind.

2 Keine unnötigen Informationen preisgeben

Ihre Anwendung sollte dem eigentlichen Besucher Ihrer Seite selbst nichts über den Aufbau und die Struktur erzählen. Fehlermeldungen, insbesondere von Datenbanken, sollte er erst gar nicht zu Gesicht bekommen. Anonymisieren Sie die Fehlermeldungen. Leiten Sie den Besucher auf die Startseite um, wenn er eine Datei anfragt, die es nicht gibt.

3 Verschlüsselung

Administrative Werkzeuge aller Art sollten immer durch ein Passwort geschützt und im Idealfall nur über SSL erreichbar sein. Angefangen von Verwaltungs-Software für das System, über Software zur Administration einer Webanwendung bis zu Statistik-Tools – all dies sollte der Besucher der Seite weder sehen, noch finden, und schon gar nicht darauf zugreifen können. Vermeiden Sie hier unnötige Redundanz. Wenn die Administration über einen VPN-Tunnel oder SSL möglich ist, besteht kein Grund dafür, dass weitere Werkzeuge über Klartextprotokolle erreichbar sind.

Überprüfen Sie Ihre Arbeit: Unter den vorgestellten Gesichtspunkten können Sie Ihre Webseite und Anwendung auch selbst überprüfen – und die anderer natürlich auch. Verlassen Sie sich nicht auf die Aussagen von Herstellern oder Skript-Autoren – im Interesse Ihrer eigenen Sicherheit.

4 Lassen Sie keine Sicherheitsmassnahme aus

Überspringen Sie nicht aus Bequemlichkeit einzelne Schritte, nur weil Sie gerade nicht relevant erscheinen. Einzelnen Details Aufmerksamkeit zu schenken, ist das, was der Angreifer typischerweise tut und Sie sollten es daher ebenfalls tun. Dies kann Sie auch vor eigenen Fehlern schützen: Eine `robots.txt` allein ist kein Schutz vor Zugriffen von Nicht-Suchmaschinen, kann Sie aber sehr wohl davor schützen, dass ein kleiner Fehler bei der Konfiguration des Webserver nicht gleich zur globalen Veröffentlichung des Servers führt.

5 Schlüssiges Sicherheitskonzept

Vermeiden Sie alles, was die obigen Schritte unnötig schwierig macht. Unglückliche Kombinationen sind zum Beispiel die vollständige Trennung der Verwaltung des eigentlichen Systems und des Webserver. Dies kann leicht dazu führen, dass ein konsistentes Sicherheitskonzept erst gar nicht angewendet werden kann. Hektik als Problemfaktor sollte eigentlich gar nicht mehr erwähnt werden müssen. Bei vielen Sicherheitstests stellt sich heraus, dass schlichtweg fehlende Zeit bei der Erstellung einer Webanwendung zu banalen, aber fatalen Fehlern führt. Vergessen Sie typische Hacker-Klischees: Sie arbeiten meist nicht gegen einen Menschen, der „Ihnen die Zeit stiehlt“, sondern gegen automatisch ablaufende Skripte. Der Angreifer von heute sitzt wahrscheinlich gemütlich in der Sonne, während seine Systeme arbeiten.

Elemente, die Sie für eine Google-Suche mit `intitle: und/oder inurl:` verwenden können. Dabei ist es unerheblich, ob es ein Gerät, z.B. der Webserver einer USV oder eine Anwendung ist. Mit etwas Glück und bei einer entsprechenden Verbreitung des Systems werden Angreifer mit Google solche Server und Anwendungen finden können.

Beachten Sie dabei, dass Sie nicht unbedingten direkten Zugriff auf das System, nach dem Sie suchen möchten, benötigen: Ein Screenshot in einer Anleitung kann bereits ausreichen.

Auf Passwortsuche

Die vorherigen Beispiele haben uns zu Anwendungen geführt, deren alleinige Präsenz im Internet problematisch sein kann. Allerdings gibt es auch einzelne Dateien, auf die dies zutrifft – insbesondere Dateien, die Passwörter enthalten können.

Sowohl Fehlkonfigurationen in Webservern als auch in Webanwendungen können dazu führen, dass derartige Dateien über das Internet erreichbar sind und damit ebenfalls von einer Suchmaschine indiziert werden können. Der klassischste Suchmaschinen-Hack ist in diesem Bereich die Suche nach Frontpage-Passwort-Dateien. Sehr alte Versionen der Microsoft Frontpage Extensions legten die Datei mit den Passwörtern in einem Pfad ab, der über den Webserver erreichbar war. Mit `inurl:` können damit auch heute noch Dateien gefunden werden:

```
inurl:/_vti_pvt/service.pwd
```

Auch hier ist der Pfadname so eindeutig, dass eine Suche ohne weitere Begriffe möglich ist. Da es sich bei dem Ergebnis um einzelne Dateien im Textformat handelt, muss der Angreifer nicht einmal seine Identität preisgeben. Er kann die Dateien im Google-Cache einsehen. Da sie keine Bilder oder andere Inhalte enthalten, die Google nicht cachen, sondern vom eigentlichen Webserver holen würde, kann das Opfer den Zugriff nicht zurück verfolgen.

Im Falle dieser Dateien liegen die Passwörter als Hash-Werte vor und müssen erst durch ei-

PHP Version 5.0.3	
System	FreeBSD 5.2-RC2 FreeBSD 5.2-RC2 #0: Mon Dec 22 07:23:48 GMT 2003 root@wylu.freebsd.org:/usr/obj/usr/src/sys/GENERIC:1386
Build Date	Aug 6 2005 15:08:42
Configure Command	'./configure' '--enable-versioning' '--enable-memory-limit' '--with-layout=GNU' '--with-config-file-scan-dir=/usr/local/etc/php' '--disable-all' '--enable-libxml' '--with-libxml-dir=/usr/local' '--enable-ssl' '--with-regex=php' '--with-apxs=/usr/local/sbin/apxs' '--disable-ipv6' '--prefix=/usr/local' '1386-portbid-freebsd5.2'
Server API	Apache
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php
additional .ini files parsed	/usr/local/etc/php/extensions.ini
PHP API	20031224
PHP Extension	20041030
Zend Extension	220040412
Debug Build	no
Thread Safety	disabled

Mehr muss man nicht wissen: Das Skript `phpinfo.php` informiert einen Hacker gründlich über den jeweiligen Web-Server.

Wie geht es dem Server? Über eine Google-Abfrage nach Webalizer bekommen Sie Daten der jeweiligen Server geliefert.

Usage Statistics for [redacted] 2006 - Mozilla Firefox	
Summary Period:	2006
Generated:	[redacted]
Year Summary prev next Analog Report webstats home [redacted]	
Daily Statistics Hourly Statistics URLs Entry Exit Sites Referrers Search Users Agents Countries	
Monthly Statistics for [redacted] 2006	
Total Hits	1771116
Total Files	1253714
Total Pages	611846
Total Visits	194835
Total KBytes	225097648
Total Unique Sites	118695
Total Unique URLs	109249
Total Unique Referrers	27498
Total Unique Usernames	10
Total Unique User Agents	2102

nen *Brute-Force*-Angriff erraten werden. Dabei probiert der Hacker systematisch alle in Frage kommenden Passwörter aus. Allerdings ist dies strafbar.

Andere Dateitypen

Bestimmte Versionen von VNC sind ebenfalls betroffen. Das Passwort befindet sich hier in einem Registry-Skript, nach dem wie folgt gesucht werden kann:

```
filetype:reg reg intext:"WINVNC3" password
```

Der Operator `filetype` gibt dabei an, dass nach Registry-Skripten gesucht werden soll und `intext:` gibt einen Text-String an, der in der Datei enthalten sein soll. `filetype` erwartet zusätzlich immer ein Argument, in diesem Fall `.reg`. Da `filetype` nicht immer präzise arbeitet, wird die Suche so auf Dateien, die auch die Endung `.reg` haben, weiter eingeschränkt.

Das Passwort ist in diesen Dateien als Hash hinterlegt, und kann mit einem Passwort-Knacker, z.B. mit `cain` (www.oxid.it) erraten werden. Das Brute-Forcing von Passwörtern und die Verwendung eines derart erhaltenen Passwortes sind allerdings illegal.

Die auf dem Webserver eingesetzte Software ist für den Angreifer natürlich besonders interessant. Hilfreich sind hierbei alle Arten von Standard-Skripten, die zum Installationsumfang einer Software gehören, wie z.B. `phpinfo.php`:

`inurl:/php/phpinfo.php intext:thread`
 Um die Suche auf die interessanten `phpinfo`-Dateien einzuschränken, wurde mit `intext:` ein Wort ausgewählt, das auf der Seite immer zu finden ist. Die Informationen, die das Skript liefert, sind umfangreich. In der Regel wird sowohl das Betriebssystem als auch der Typ des Webservers inklusive seiner Konfiguration weitergegeben. Interessant ist aber auch Software, die Zugriffsstatistiken erzeugt:



```
intitle:"usage statistics" inurl:webalizer
```

Diese Google-Anfrage fördert Systeme, auf denen der `Webalizer` läuft, bzw. dessen Webseiten zu Tage. Auch hier können die gesammelten Informationen dem Angreifer nützliche Anhaltspunkte bieten.

Apache-Server identifiziert

Um den Webserver selbst identifizieren zu können, sind Kenntnisse der jeweiligen Standard-Installation hilfreich. Bekanntestes Bei-

spiel dafür ist sicher die Online-Hilfe des Apache-Webservers. Nach der Installation ist diese für jeden über das Netz erreichbar. Wird sie nicht entfernt, können so Apache-Server gesucht werden:

```
intitle:"Apache HTTP Server" intitle:"Documentation"
```

Hier besteht durch das alleinige Vorhandensein der Webseiten kein Problem. Der Angreifer hofft jedoch, dass eventuell noch andere Software auf dem Server die Standard-Einstellungen hat, was sich gegebenenfalls ausnutzen lässt. Ebenso kann nach den Webseiten gesucht werden, die bei der Installation des Servers angelegt werden:

```
intitle:"Test Page for Apache"
```

Es handelt sich um Server, die nach der Installation nicht weiter konfiguriert worden sind. Das Vorhandensein der Dokumentation ist für den Angreifer ein Indikator dafür, dass der Server eventuell nicht gut gewartet wird.

Fazit

Die hier vorgestellten Google-Suchen sind nur eine kleine Auswahl der Möglichkeiten des Webs. Dennoch beruhen praktisch alle auf demselben Problem: Bestimme Dateien und Verzeichnisse sind im Internet vor dem Zugriff Dritter nicht ausreichend geschützt und können so auch von Suchmaschinen indiziert werden. Dies wiederum macht die jeweilige Sicherheitslücke praktisch öffentlich, denn jede(r), der Google bedienen kann, kann nun das betroffene System finden. **jak**

Weiterführende Literatur-Links: Die Webseite von Johnny Long (<http://johnny.ihackstuff.com>) und sein Buch „Google Hacking“, 480 Seiten, Mitp-Verlag 2005, ISBN: 3826615786

Weitere Informationen zum Thema finden Sie unter www.pc-magazin.de/internet/technik.

CIA-Tools auf Heft-CD/DVD

☞ Glauben Sie nicht, dass Sie mit einem falsch konfigurierten Server lange unentdeckt bleiben. Über Suchmaschinen und Skripte finden potenzielle Angreifer Sicherheitslücken ziemlich schnell. Unterziehen Sie deshalb alle Ihre Systeme einem harten Sicherheitstest. Die richtigen Werkzeuge dafür finden Sie in der *CIA-Toolbox* auf unserer Heft-DVD/CD. Sie enthält Hack-Tools wie Portscanner, Paket-Sniffer, Keylogger, Fernsteuerungs-Tools und Passwortknacker. Achtung! Manche Virens Scanner melden diese Programme als gefährlich. Sie richten aber bei richtigem Gebrauch keinen Schaden an.