DCIT

Google hacking

Autoři: Martin Mačok, Vít Strádal

DCIT, s.r.o. - Praha, http://www.dcit.cz/

Obsah

DCIT

Úvod

Užitečné stránky a nástroje

Hledání serverů (produktů)

Hledání portálů

Hledání jiných zařízení

Hledání citlivých informací

Hledání slabin

CONSULTING DCIT

Google hacking

DCIT

Google hacking je využití internetových vyhledávačů pro

- nalezení citlivých informací
- nalezení potenciálně zranitelných obětí
- zjištění informací o potenciální oběti útoku

Motto: proč nevyužít obrovských databází?

Útočník nemusí (ale může) útok zaměřit na jednu konkrétní oběť

Užitečné stránky

DCIT

Vyhledávací stroje

- google.com
- yahoo.com
- vista.alexa.com

Netcraft.com

- WWW server - produkt, operační systém, historie

Wayback machine

- archive.org

Google Hacking Database

- johnny.ihackstuff.com

Užitečné nástroje

DCIT

Hledání exploitů

- exploit filetype:c
- apache exploit filetype:c

Network Query Tool (IP, DNS, traceroute)

- inurl:"nqt.php" "network query tool"

Squid Cache Manager (skrytý portscan)

- inurl:"cachemgr.cgi"

Automatizace google hackingu

- SiteDigger, Wikto

Hledání serverů dle verzí

DCIT

Apache 1.2.6

- intitle:"Test Page for Apache Installation" "You are free"

Apache 1.3.0-1.3.9

- intitle:"Test Page for Apache" "It worked!" "this Web site!"

Apache SSL/TLS

- intitle:test.page "Hey, it worked !" "SSL/TLS-aware"

MS IIS 4.0

- intitle:"welcome to IIS 4.0"

MS IIS 5.0

- allintitle:"Welcome to Windows 2000 Internet Services"

Login Portals

DCIT

Virtual Network Computing (VNC)

- "VNC Desktop" inurl:5800

Novell Groupwise Web Access

- Novell inurl:"/servlet/webacc"

Citrix Metaframe

- inurl:"/Citrix/Nfuse17/"

Lotus Domino Admin

- inurl:webadmin filetype:nsf

Microsoft Outlook Web Access

- inurl:"exchange/logon.asp" or intitle:"Microsoft Outlook Web Access - Logon"

CONSULTING DCIT

Tiskárny

DCIT

Canon ImageReady

- intitle:"remote ui:top page"

Xerox 860 and 8200

- intext:"Ready with 10/100T Ethernet"

Konica printers

- intitle:"network administration" inurl:"nic"

Lexmark

- intext:"UAA (MSB)" Lexmark -ext:pdf

CONSULTING DCIT

Webkamery

DCIT

AXIS

- intitle:"Live View / - AXIS"
- intitle:"The Axis 200 home page"
- inurl:"indexFrame.shtml" Axis

SNC-RZ30

- allintitle:SNC-RZ30 HOME

Evocam

- intitle:"EvoCam" inurl:"webcam.html"

CONSULTING DCIT

Jiná zařízení

DCIT

Cisco VPN 3000 Concentrator

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

PacketShaper traffic management

- (intitle:"PacketShaper Login")|(intitle:"PacketShaper Customer Login")

Lantronix Web Manager

- intitle:"lantronix web-manager"

Hledání citlivých informací

DCIT

Uživatelská jména

- filetype:rdp rdp
- inurl:.bash_history intext:ssh intext:cd -inurl:htm

Hesla

- inurl:/etc/shadow intext:"root:"
- "sets mode: +k"
- filetype:log inurl:"password.log"

Jiné

- filetype:xls budget

CONSULTING DCIT

Hledání slabin

DCIT

PHPSHELL

- "stderr-trapping" inurl:php -warning
- slabina: lze spouštět příkazy

Gforge team development manager

- inurl:"scm/viewFile.php" inurl:"file_name"
- slabina: lze spouštět příkazy (file_name=%0Aid%0A)

phpCMS 1.2.x content management system

- inurl:"parser.php?phpcmsaction"
- slabina: lze číst soubory (phpcmsaction=FILEMANAGER&language=de/../../../etc/passwd)

CONSULTING DCIT

Hledání slabin II

DCIT

Loki Download Manager

- inurl:"catinfo.asp?cat" "loki download manager"
- slabina: SQL injection, lze pracovat s databází

Webhints Scripts

- inurl:"/hints.pl" -"reset password"
- slabina: lze spouštět příkazy (hints.pl?lidl)

Scénář: útočník sleduje konferenci Bugtraq a ke zveřejněným slabinám je schopen okamžitě dohledat postižené oběti