

Obsah

Předmluva	xvii
-----------	------

Kapitola 1 Základy vyhledávání Googlem 19

Úvod	20
Probádání webového rozhraní Google	20
Vyhledávací stránka Google	20
Stránka Googlu výsledků hledání v sekci Web	22
Vyhledávání obrázků Googlem	25
Nastavení Googlu	26
Jazykové nástroje	28
Vytváříme dotazy Google	30
Zlatá pravidla při vyhledávání v Googlu	31
Základní druhy vyhledávání	33
Booleovské operátory a speciální znaky	33
Redukce při vyhledávání	36
Pracujeme s adresami URL Googlu	39
Speciální znaky	41
Shrnutí	52
Stručná rekapitulace	52
Odkazy na webové stránky	53
Časté dotazy	54

Kapitola 2 Pokročilé operátory 57

Úvod	58
Syntax operátorů	59
Odstraňování chyb v syntaxi	60
Úvod do pokročilých operátorů Googlu	61
Intitle a allintitle – hledání v titulku stránky	61
Allintext – pátrání po řetězci v textu stránky	64
Inurl a allinurl – nalezení textu v URL	64
Site – zúžení vyhledávání na specifické weby	66
Filetype – hledání souborů konkrétního typu	68
Link – hledání odkazů na stránku	72
Inanchor – pátrání po textu odkazů	74
Cache – zobrazení archivované verze stránky	75

Numrange – hledání čísel	75
Daterange – hledání stránek publikovaných v zadaném období	76
Info – zobrazení souhrnných informací Googlu	77
Related – zobrazení podobných webů	78
Author – hledání autora zprávy vystavené na fóru v sekci Groups (Skupiny)	78
Group – hledání v titulcích skupin	80
Insubject – hledá v řádcích předmětu skupin Googlu	81
Msgid – pátrání po publikovaných zprávách skupin podle ID zprávy	82
Stocks – hledá informace o akcích	83
Define – zobrazí definici termínu	83
Phonebook – hledá v telefonních seznamech	84
Kolidující operátory a špatné techniky při hledání	86
Shrnutí	90
Stručná rekapitulace	90
Odkazy na webové stránky	94
Časté dotazy	95

Kapitola 3 Základy hackingu Googlem **97**

Úvod	98
Anonymita s archivem	98
Google jako proxy server	105
Výpisy adresářů	109
Pátráme po výpisech adresářů	110
Nalezení konkrétního adresáře	111
Hledání konkrétního souboru	112
Verze serveru	112
Prekérní situace: techniky traverzování	118
Cestování po adresářích	118
Inkrementální substituce	119
Lovení přípon	120
Shrnutí	124
Stručná rekapitulace	124
Odkazy na webové stránky	126
Časté dotazy	127

Kapitola 4 Předběžná obhlídka

129

Úvod	130
Seznámení	130
Intranety a lidské zdroje	131
Odborná pomoc	132
Nápověda "pomoz si sám" a průvodci "jak na to"	132
Seznamy pracovních zařazení	134
Dlouhé procházky po pláži	134
Jména, jména, a ještě jednou jména	135
Adresy, adresy, a ještě více adres!	141
Romantické večere při svíčkách	149
Jmenovky? Žádný podělaný jmenovky nepotřebujeme!	150
Co je poblíž?	150
Zásady pro dohled nad intranetem	153
Shrnutí	154
Stručná rekapitulace	154
Odkazy na webové stránky	155
Časté dotazy	155

Kapitola 5 Mapování sítě

157

Úvod	158
Metodologie mapování	158
Mapovací techniky	159
Určení domény	159
Prolézání webů	160
Mapování odkazů	164
Sledování skupin	169
Webové utility nepocházející z Googlu	170
Zacílení na síťová zařízení s webovým rozhraním	175
Pátrání po dokumentech se statistikami o síti	176
Shrnutí	179
Stručná rekapitulace	180
Odkazy na webové stránky	180
Časté dotazy	181

Kapitola 6	Pátrání po exploitech a nalézání cílů	183
Úvod		184
Jak vypátráme exploity		184
Jak vypátráme veřejné weby s exploity		184
Jak vypátráme exploity přes běžné řetězce kódu		186
Pátrání po zranitelných cílech		188
Pátráme po cílech přes demonstrační stránky		189
Pátráme po cílech přes zdrojový kód		192
Pátráme po cílech pomocí skenování CGI		199
Shrnutí		201
Stručná rekapitulace		201
Odkazy na webové stránky		202
Časté dotazy		202
 Kapitola 7	 Deset funkčních hledání týkajících se bezpečnosti	 205
Úvod		206
site		206
intitle:index.of		208
error warning		208
login logon		209
username userid employee.ID "your username is"		210
password passcode "your password is"		210
admin administrator		211
-ext:html -ext:htm -ext:shtml -ext:asp -ext:php		213
inurl:temp inurl:tmp inurl:backup inurl:bak		216
intranet help.desk		217
Shrnutí		218
Stručná rekapitulace		218
Časté dotazy		220

Kapitola 8	Vystopování webových serverů, přihlašovacích portálů, síťového hardwaru	221
Úvod		222
Pátrání a vytváření profilu webového serveru		223
Výpisy adresářů		223
Chybové zprávy webových serverů		224

Chybové zprávy aplikačního softwaru	235
Výchozí stránky	238
Standardně dodávaná dokumentace	243
Ukázkové programy	245
Pátrání po přihlašovacích portálech	246
Pátrání po síťovém hardwaru	250
Shrnutí	255
Stručná rekapitulace	255
Časté dotazy	257

Kapitola 9 Uživatelská jména, hesla a utajované informace 259

Úvod	260
Vyhledávání uživatelských jmen	260
Vyhledávání hesel	265
Vyhledávání čísel kreditních karet, čísel sociálního pojištění a jiných důležitých údajů	270
Čísla sociálního pojištění	272
Osobní údaje týkající se financí	273
Vyhledávání dalších pikantních informací	274
Stručná rekapitulace	278
Časté dotazy	280

Kapitola 10 Obrušování dokumentů, kutání v databázích 281

Úvod	282
Konfigurační soubory	283
Soubory protokolů	289
Kancelářské dokumenty	291
Kutání v databázi	293
Přihlašovací portály	293
Podpůrné soubory	295
Chybové zprávy	297
Dumpy databází	299
Opravdové databázové soubory	301
Automatizované obrušování (grinding)	302
Vyhledávání pomocí Google Desktop	305
Shrnutí	307
Stručná rekapitulace	307

Odkazy na webové stránky	308
Časté dotazy	309

Kapitola 11 Chráníme se před hackery Googlu **311**

Úvod	312
Dobrá, solidní bezpečnostní politika	312
Ochranná opatření webového serveru	313
Výpisy adresářů a chybějící indexové soubory	313
Zablokování robotů pomocí Robots.txt	314
NOARCHIVE – zabiják archivovaných dokumentů	317
NOSNIPPET – zbavme se fragmentů	317
Mechanismy pro ochranu hesel	318
Výchozí softwarová nastavení a programy	319
Hackněte svůj vlastní web	321
Vyzkoušejte na sobě operátor site	321
Gooscan	322
Nástroje Windows a .NET Framework	331
Athena	331
API Googlu a licenční klíče	336
SiteDigger	336
Wikto	340
Získávání nápovědy z Googlu	342
Shrnutí	346
Stručná rekapitulace	346
Odkazy na webové stránky	347
Časté dotazy	348

Kapitola 12 Automatizace vyhledávání Googlem **351**

Úvod	352
Co jsou vyhledávací kritéria Googlu	353
Analýza smluvních podmínek pro automatizované googlování ve stylu "zlobivého hochy"	355
Požadavky a podmínky Googlu	356
Co je API Googlu	356
Co je vyhledávací požadavek Google	358
Automatické googlování podle Googlu	362
Ukázkový kód API	363

Co jsou útočné knihovny Googlu	369
Pseudo-programování	370
Implementace v Perlu	371
Implementace v Pythonu	374
Implementace v C# (.NET)	377
Implementace v C	380
Dokumentace ke zdrojovému kódu	386
Skenování webu s útočnými knihovnami Googlu	387
Skenování zranitelnosti CGI	387
Shrnutí	392
Stručná rekapitulace	392
Odkazy na webové stránky	393
Časté dotazy	394

Dodatek A Profesionální testování bezpečnosti **397**

Úvod	398
Profesionální testování bezpečnosti	399
Otevřená metodologie	400
Standardizovaná metodologie	402
Metodologie OSSTMM	408
Shrnutí	412
Časté dotazy	412

Dodatek B Úvod do bezpečnosti webových aplikací **415**

Úvod	416
Co rozumíme bezpečností webové aplikace	416
Unikátnosti ohledně bezpečnosti webové aplikace	417
Zranitelnosti webové aplikace	418
Meze hackingu vyhledávací engine	421
Informace a zranitelnosti v obsahu	422
Rychlá cesta k výpisům adresářů	422
HTML komentáře	425
Chybové zprávy	425
Ukázkové soubory	426
Špatné přípony	426
Systémová dokumentace	428

Skrytá pole formuláře, JavaScript a jiné problémy u klienta	429
Hrajeme si s pakety	430
Prohlížení paketů a manipulace s nimi	432
Zranitelnosti v kódu webových aplikací	434
Útoky na klienta	434
Jak uloupit sezení (session hijacking)	442
Vykonání příkazu: injekce SQL	445
Odhalení schéma databáze	449
Shrnutí	451
Odkazy	451
Stručná rekapitulace	452
Časté dotazy	455

Dodatek C Google Hacking Database

Mnoho rozšířených tabulek a další nástroje pro pen-testy najdete na webových stránkách Syngress Solutions (www.syngress.com/solutions).