

SEGURANÇA DE DNS

DEFENDENDO O SISTEMA DE NOMES DE DOMÍNIO

Allan Liska
Geoffrey Stowe

Novatec

Copyright © 2016 Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangement with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

This edition of DNS Security: Defending the domain name system - 9780128033067 by Allan Liska and Geoffrey Stowe is published by arrangement with ELSEVIER INC., a Delaware corporation having its principal place of business at 360 Park Avenue South, New York, NY 10010, USA.

Nenhuma parte desta publicação pode ser reproduzida ou transmitida de qualquer forma ou por qualquer meio, eletrônico ou mecânico, incluindo fotocópia, gravação ou qualquer armazenamento de informação e sistema de recuperação, sem permissão por escrito da editora. Detalhes sobre como pedir permissão, mais informações sobre as permissões de políticas da editora e o acordo com organizações como o Copyright Clearance Center e da Copyright Licensing Agency, podem ser encontradas no site: www.elsevier.com/permissions.

Este livro e as contribuições individuais contidas nele são protegidos pelo Copyright da Editora (além de outros que poderão ser aqui encontrados).

Esta edição do livro DNS Security: Defending the domain name system - 9780128033067 de Allan Liska e Geoffrey Stowe é publicada por acordo com a Elsevier Inc., uma corporação de Delaware estabelecida no endereço 360 Park Avenue South, New York, NY 10010, EUA.

© Novatec Editora Ltda. 2016.

Todos os direitos reservados e protegidos pela Lei 9.610 de 19/02/1998. É proibida a reprodução desta obra, mesmo parcial, por qualquer processo, sem prévia autorização, por escrito, do autor e da Editora.

Editor: Rubens Prates

Tradução: Lúcia A. Kinoshita

Revisão gramatical: Priscila A. Yoshimatsu

Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-533-2

Histórico de impressões:

Novembro/2016 Primeira edição

Novatec Editora Ltda.

Rua Luís Antônio dos Santos 110

02460-000 – São Paulo, SP – Brasil

Tel.: +55 11 2959-6529

E-mail: novatec@novatec.com.br

Site: www.novatec.com.br

Twitter: twitter.com/novateceditora

Facebook: facebook.com/novatec

LinkedIn: linkedin.com/in/novatec

Sumário

Sobre os autores.....	13
Agradecimentos.....	14
Capítulo 1 ■ Compreendendo o DNS	16
Introdução.....	16
História do DNS	19
Arquivo hosts.txt	19
Problemas com correio eletrônico	21
RFCs 819 e 920.....	23
Rumo à comercialização.....	24
Raiz (root)	25
Servidores recursivos e autoritativos	31
Servidores de nomes recursivos	31
Servidores de nomes autoritativos.....	35
Arquivos de zona	37
Registros de recursos	40
Registros de endereço.....	41
Registros de nomes canônicos	42
Registros de servidor de mensagens	42
Registros de servidores de nomes.....	43
Registros de ponteiros.....	44
Registros de informações de host.....	45
Registros de servidores.....	45
Registros de texto	46
Conclusões	47
Notas	47

Capítulo 2 ■ Problemas com segurança de DNS	48
Introdução.....	48
Uma breve história das brechas de segurança de DNS	49
Por que a segurança de DNS é importante?	53
Problemas comuns de segurança de DNS.....	55
Desenvolvendo um plano de segurança de DNS	64
Notas	69
Capítulo 3 ■ Erros de configuração de DNS	70
Introdução.....	70
Vulnerabilidades de servidores DNS	71
Fingerprinting em servidores DNS.....	79
Buffer overflows, condições de concorrência e execução com privilégios desnecessários	82
Erros humanos	85
Conclusões	88
Notas	89
Capítulo 4 ■ Exploração de falhas de DNS de origem externa.....	90
Introdução.....	90
Envenenamento de cache.....	91
Caching no navegador web.....	100
DNS spoofing	100
Ataques DDoS usando DNS	104
Usando DNS como canal para Comando e Controle ou exfiltração.....	109
Conclusões	116
Notas	116
Capítulo 5 ■ Reconhecimento de DNS	117
Introdução.....	117
Whois.....	118
Fontes de dados do Whois.....	123
Mapeamento da infraestrutura de DNS	125
Fingerprinting de DNS	127
DNS reverso	129
DNS cache snooping	131
DNS passivo	134

Coleta de dados de consultas	135
Conclusões	139
Notas	140
Capítulo 6 ■ Segurança de rede com DNS	141
Introdução	141
Localização dos servidores DNS	142
Infraestrutura pública e privada de DNS	145
Logging e monitoração de tráfego de DNS	147
Marcando domínios ruins	148
Marcando consultas de DNS	158
DNS e SIEM	161
DNS passivo	163
Domínios fast-flux	170
Firewalls de DNS e RPZ	171
Listas negras, listas brancas e outros dados de inteligência contra ameaças de DNS	174
Conclusões	176
Notas	177
Capítulo 7 ■ Segurança no BIND	178
Introdução	178
Executando o BIND em uma prisão chroot	180
Técnicas de evasão de fingerprint	182
Limitação da taxa de respostas	185
Consultas e transferências	187
Usando TSIG para assinar transferências de zona	189
Zonas de política de resposta	191
Logging	197
Conclusões	201
Notas	201
Capítulo 8 ■ Segurança de DNS no Windows	202
Introdução	202
Garantindo a segurança dos arquivos de DNS no Windows	204
Controle de DNS dinâmico	209
Consultas e transferências	212
DNS em estações de trabalho com Windows	215

Windows e DDoS	216
Servidores de caching no Windows.....	218
DNS no Windows e alta disponibilidade.....	221
Instruções para configuração do Windows	222
Prazo para restauração	223
Implicações quanto à segurança	224
Logging	225
Análise de logs no Windows.....	227
Conclusões	229
Notas	230
Capítulo 9 ■ Terceirização de DNS	232
Introdução.....	232
Terceirização de DNS.....	233
Decidindo quanto deve ser terceirizado.....	237
DNS gerenciado	238
DNS dividido.....	239
Terceirizando o DNS recursivo	243
Trabalhando de forma segura com um provedor de DNS.....	244
Monitorando a infraestrutura de DNS	246
Terceirização de DNS e DDoS	247
Conclusões	249
Notas	249
Capítulo 10 ■ DNSSEC	251
Informações contidas neste capítulo	251
Introdução.....	251
Histórico	252
Descrição geral da criptografia e o TLS.....	253
Protocolo do DNSSEC.....	257
Respostas NXDOMAIN	267
Implementando o DNSSEC no Linux	269
Implementando o DNSSEC no Windows.....	270
Administrando uma zona de DNSSEC.....	271
Administrando os prazos de validade das chaves.....	273
Validação Look-aside do DNSSEC.....	273
Outros usos do DNSSEC.....	274
DNSSEC e a amplificação de DDoS	274

Críticas ao DNSSEC.....	275
Conclusões	277
Notas	278
Capítulo 11 ▀ Anycast e outros protocolos de DNS.....	279
Informações contidas neste capítulo	279
Introdução.....	279
Motivação para o anycast	280
Anycast	283
Implementação do anycast	284
Anycast e DDoS.....	288
DNS multicast	289
Descoberta de serviços de DNS	293
Tor Hidden Services	295
BitTorrent/DNS P2P.....	296
Conclusões	297
Notas	298