

**SEGURANÇA EM SERVIDORES**

**LINUX**

**ATAQUE E DEFESA**

**Chris Binnie**

Novatec

All rights reserved. This translation is published under license with the original publisher John Wiley & Sons, Inc. Copyright © 2016 by John Wiley & Sons, Inc., Indianapolis, Indiana.

Todos os direitos reservados. Tradução autorizada da edição em inglês intitulada Linux® Server Security: Hack and Defend, publicada pela John Wiley & Sons, Inc. Copyright © 2016 por John Wiley & Sons, Inc., Indianapolis, Indiana.

Nenhuma parte deste livro pode ser reproduzida, armazenada ou transmitida em qualquer formato ou por qualquer meio, eletrônico, físico e etc., sem a autorização por escrito do titular original do copyright, John Wiley & Sons, Inc. <http://www.wiley.com/go/permissions>

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: Henrique Cesar Ulbrich

Revisão gramatical: Priscila A. Yoshimatsu

Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-335-6

Histórico de impressões:

Janeiro/2017      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](mailto:novatec@novatec.com.br)

Site: [www.novatec.com.br](http://www.novatec.com.br)

Twitter: [twitter.com/novateceditora](https://twitter.com/novateceditora)

Facebook: [facebook.com/novatec](https://facebook.com/novatec)

LinkedIn: [linkedin.com/in/novatec](https://linkedin.com/in/novatec)

# Sumário

Sobre o autor .....	11
Sobre o editor técnico.....	11
Como este livro é organizado .....	16
Quem deve ler este livro .....	18
Resumo .....	18
<b>Capítulo 1 ■ Manto de invisibilidade.....</b>	<b>19</b>
Contexto .....	19
Sondagem de portas.....	20
Como confundir um scanner de porta .....	20
Instalação do knockd.....	22
Pacotes .....	22
Alteração dos ajustes default .....	23
Alteração dos locais do sistema de arquivos .....	24
Algumas opções de configuração.....	24
Inicialização do serviço.....	24
Alteração da interface de rede default .....	25
Tipos de pacotes e temporizações.....	25
Teste da instalação .....	27
Clientes de port knocking.....	27
Como tornar o servidor invisível .....	28
Teste do iptables .....	28
Gravando as regras do iptables .....	30
Outras considerações.....	31
Cliente para smartphone.....	31
Pesquisa de problemas .....	31
Considerações de segurança.....	32
Sequências efêmeras .....	33
Resumo .....	34

<b>Capítulo 2 ■ Coloque impressão digital em seus arquivos .....</b>	<b>35</b>
Integridade do sistema de arquivos .....	35
Sistema de arquivos como um todo .....	39
Rootkits .....	40
Configuração .....	43
Falso-positivos .....	45
Bem projetado .....	46
Resumo .....	48
 <b>Capítulo 3 ■ Ncat no século 21 .....</b>	<b>49</b>
História .....	49
Pacotes de instalação .....	52
Para começar .....	53
Transferência de arquivos .....	55
Exemplo de bate-papo .....	56
Encadeamento de comandos .....	57
Comunicações seguras .....	58
Executáveis .....	60
Listas de controle de acesso .....	61
Opções diversas .....	62
Resumo .....	63
 <b>Capítulo 4 ■ Negação de serviço .....</b>	<b>64</b>
Infraestrutura NTP .....	65
Ataques reflexivos NTP .....	66
Relatórios de ataques .....	69
Prevenção de reflexões SNMP .....	70
Resolvedores DNS .....	71
Cumplicidade .....	74
Uma nação de joelhos .....	75
Mapeamento de ataques .....	76
Resumo .....	77
 <b>Capítulo 5 ■ Nping .....</b>	<b>79</b>
Funcionalidade .....	79
TCP .....	80
Intérprete .....	82
UDP .....	83

ICMP .....	84
ARP .....	84
Opções de payload .....	85
Modo Eco .....	86
Outras opções Nping .....	90
Resumo .....	91
<b>Capítulo 6 ■ Análise de logs.....</b>	<b>92</b>
Equívocos no uso de ICMP .....	93
tcpdump .....	93
Iptables.....	95
Regras multipartes .....	98
Registro completo para análise forense .....	99
Hardening .....	100
Resumo .....	103
<b>Capítulo 7 ■ O prodigioso NSE do Nmap .....</b>	<b>104</b>
Escaneamento de portas básico .....	104
Motor de script do Nmap .....	107
Modelos de temporização (timing templates) .....	109
Categorização de scripts.....	110
Fatores de contribuição .....	112
Falhas de segurança .....	113
Testes de autenticação .....	114
Descoberta .....	115
Atualização de scripts .....	117
Tipos de script .....	118
Expressões regulares.....	119
Interfaces gráficas de usuário .....	119
Zenmap.....	120
Resumo .....	120
<b>Capítulo 8 ■ Detecção de malware.....</b>	<b>122</b>
Para começar .....	123
Frequência de atualização das definições .....	123
Registro de hashes de malware.....	123
Ameaças prevalentes .....	124
Funcionalidades LMD .....	124
Monitoração de sistemas de arquivos.....	126

Instalação .....	127
Modos de monitoração .....	129
Configuração .....	130
Exclusões .....	130
Execução a partir da CLI .....	131
Relatórios .....	132
Quarentena e limpeza .....	133
Atualização do LMD .....	134
Execução e parada de varreduras.....	135
Tarefa cron .....	136
Relatórios de malware.....	136
Integração com Apache.....	137
Resumo .....	138
<b>Capítulo 9 ■ Quebra de senhas com Hashcat .....</b>	<b>139</b>
História .....	140
Compreensão das senhas .....	140
Keyspace .....	140
Hashes .....	142
Uso da Hashcat.....	144
Capacidades da Hashcat .....	145
Instalação.....	145
Identificação por hash.....	146
Escolha do modo de ataque.....	149
Download de uma wordlist .....	149
Tabelas rainbow .....	150
Execução da Hashcat .....	150
oclHashcat .....	154
Hashcat-utils .....	155
Resumo .....	156
<b>Capítulo 10 ■ Ataques de injeção de SQL.....</b>	<b>157</b>
História .....	158
SQLi básica .....	159
Mitigação de SQLi em PHP .....	161
Exploração de falhas SQL .....	163
Lançamento de um ataque .....	164
Testando a SQLi de forma legal .....	167
Resumo .....	168