

# Black Hat Python

*Programação Python para  
hackers e pentesters*

**Justin Seitz**

Novatec

Copyright © 2015 by Justin Seitz. Title of English-language original: *Black Hat Python*, ISBN 978-1-59327-590-7, published by No Starch Press. Portuguese-language edition copyright © 2015 by Novatec Editora Ltda. All rights reserved.

Copyright © 2015 by Justin Seitz. Título original em Inglês: *Black Hat Python*, ISBN 978-1-59327-590-7, publicado pela No Starch Press. Edição em Português copyright © 2015 pela Novatec Editora Ltda. Todos os direitos reservados.

Copyright © 2015 da Novatec Editora Ltda.

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  
Revisão gramatical: Patrizia Zagni  
Editoração eletrônica: Carolina Kuwabata  
Assistente editorial: Priscila A. Yoshimatsu

ISBN: 978-85-7522-420-5

Histórico de impressões:

Março/2015          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: [novatec.com.br](http://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

<b>Apresentação</b> .....	<b>10</b>
<b>Prefácio</b> .....	<b>11</b>
<b>Agradecimentos</b> .....	<b>13</b>
<b>Capítulo 1 ■ Configurando o seu ambiente Python</b> .....	<b>14</b>
Instalando o Kali Linux .....	14
WingIDE .....	16
<b>Capítulo 2 ■ Redes: o básico</b> .....	<b>23</b>
Redes com Python em um parágrafo .....	23
Cliente TCP .....	24
Cliente UDP .....	25
Servidor TCP .....	26
Substituindo o netcat .....	27
Criando um proxy TCP .....	36
SSH com Paramiko .....	43
Tunelamento SSH .....	48
<b>Capítulo 3 ■ Redes: sockets puros e sniffing</b> .....	<b>53</b>
Criando uma ferramenta UDP para descoberta de hosts .....	54
Sniffing de pacotes no Windows e no Linux .....	54
Decodificando a camada IP .....	57
Decodificando o ICMP .....	61
<b>Capítulo 4 ■ Dominando a rede com a Scapy</b> .....	<b>68</b>
Roubando credenciais de email .....	68
Envenenamento de cache ARP com a Scapy .....	72
Processamento de PCAPs .....	78

<b>Capítulo 5 ■ Web hacking .....</b>	<b>84</b>
A biblioteca de socket da Web: a urllib2.....	84
Fazendo o mapeamento de instalações de aplicações web com código aberto.....	86
Usando a força bruta em diretórios e arquivos.....	89
Usando a força bruta em formulários de autenticação HTML .....	93
<b>Capítulo 6 ■ Estendendo o Burp Proxy.....</b>	<b>101</b>
Configurando o ambiente.....	102
Fuzzing com o Burp .....	103
Bing com o Burp.....	114
Transformando o conteúdo do site em uma mina de ouro de senhas .....	121
<b>Capítulo 7 ■ Comando e controle com o GitHub .....</b>	<b>128</b>
Criando uma conta no GitHub.....	129
Criando módulos.....	130
Configuração do cavalo de Troia .....	131
Criando um cavalo de Troia que utilize o GitHub.....	132
<b>Capítulo 8 ■ Tarefas comuns para cavalos de Troia no Windows .....</b>	<b>139</b>
Diversão com logging de teclas .....	139
Capturando imagens de tela .....	143
Execução de shellcode usando Python .....	145
Detecção de sandbox.....	147
<b>Capítulo 9 ■ Diversão com o Internet Explorer .....</b>	<b>153</b>
Man-in-the-browser .....	153
Automação de COM com o IE para extração de dados.....	159
<b>Capítulo 10 ■ Escalação de privilégios no Windows.....</b>	<b>169</b>
Instalando os pré-requisitos.....	170
Criando um monitor de processos .....	171
Privilégios do token do Windows .....	174
Vencendo a corrida .....	177
Injeção de código .....	181
<b>Capítulo 11 ■ Automatizando estratégias forenses para ataques.....</b>	<b>185</b>
Instalação .....	186
Perfis .....	186
Capturando hashes de senha .....	187
Injeção direta de código .....	190