

Manual do Hacker

Adrian Pruteanu

Packt

Novatec

Copyright © Packt Publishing 2019. First published in the English language under the title 'Becoming the Hacker – (9781788627962)'

Copyright © Packt Publishing 2019. Publicação original em inglês intitulada Becoming the Hacker – (9781788627962)'

Esta tradução é publicada e vendida com a permissão da Packt Publishing.

© Novatec Editora Ltda. [2019].

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: Tássia Carvalho

Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-753-4

Histórico de impressões:

Abril/2019 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

Prefácio	13
Capítulo 1 ■ Introdução ao ataque de aplicações web	18
Regras da campanha de testes	20
Comunicação.....	20
Considerações sobre privacidade	22
Limpeza	23
Kit de ferramentas do pentester	25
Kali Linux	25
Alternativas ao Kali Linux.....	26
Proxy de ataque	27
Burp Suite.....	27
Zed Attack Proxy.....	29
Infraestrutura na nuvem.....	30
Recursos.....	31
Exercícios	32
Resumo	32
Capítulo 2 ■ Descoberta eficaz	34
Tipos de avaliação.....	34
Mapeamento do alvo.....	36
Masscan	39
WhatWeb	40
Nikto.....	41
Scanners de CMS.....	42
Uso eficaz de força bruta	43
Descoberta de conteúdo	46
Burp Suite.....	46
OWASP ZAP	47
Gobuster	48

Persistência na descoberta de conteúdo.....	50
Processamento de payloads	53
Payloads políglotas.....	63
Mesmo payload, contextos diferentes.....	68
Ofuscamento de código.....	70
Recursos.....	73
Exercícios	73
Resumo	74

Capítulo 3 ■ Frutos ao alcance das mãos 75

Avaliação da rede	75
Procurando uma rota de entrada	78
Adivinhando credenciais.....	81
Uma maneira melhor de ter acesso ao shell	88
Limpeza.....	92
Recursos.....	93
Resumo	93

Capítulo 4 ■ Força bruta avançada 95

Password spraying.....	96
Scraping do LinkedIn.....	99
Metadados.....	102
Cluster bomb.....	104
Por trás de sete proxies	108
Usando o Tor.....	109
ProxyCannon	116
Resumo	121

Capítulo 5 ■ Ataques de inclusão de arquivos..... 122

RFI.....	123
LFI.....	126
Inclusão de arquivo para execução remota de código.....	134
Outros problemas com upload de arquivo	136
Resumo	142

Capítulo 6 ■ Exploração de falhas out-of-band..... 143

Um cenário comum.....	144
Comando e controle.....	146
Comunicação com o Let's Encrypt.....	147

Simulação com o INet	152
Confirmação.....	156
Exfiltração de dados assíncrona.....	157
Inferência de dados	160
Resumo	162

Capítulo 7 ■ Testes automatizados 163

Estendendo o Burp.....	163
Exploração de autenticação e autorização.....	166
Fluxo do Authorize	168
Canivete suíço	170
Auxiliar do sqlmap	171
Web shells	174
Ofuscando o código.....	177
Burp Collaborator.....	180
Servidor público do Collaborator.....	182
Interação com serviços	183
Cliente do Burp Collaborator	184
Servidor privado do Collaborator.....	187
Resumo	192

Capítulo 8 ■ Serialização mal-intencionada 194

Explorando a desserialização.....	195
Atacando protocolos personalizados.....	203
Análise de protocolo	204
Explorando a desserialização.....	207
Resumo	215

Capítulo 9 ■ Ataques do lado do cliente na prática 216

SOP	217
Cross-Origin Resource Sharing	221
XSS	222
XSS refletido	222
XSS persistente	224
XSS baseado em DOM.....	225
CSRF.....	228
BeEF.....	231
Hooking.....	236
Ataques de engenharia social.....	241

Keylogger.....	244
Persistência.....	249
Exploração automática de falhas.....	251
Tunelamento de tráfego.....	257
Resumo	259

Capítulo 10 ■ Ataques do lado do servidor na prática260

Referências internas e externas	261
Ataques XXE	263
Ataque billion laughs	264
Falsificação de requisições.....	265
Scanner de portas	270
Vazamento de informações.....	273
XXE cego	279
Execução remota de código	285
Shells interativos	287
Resumo	290

Capítulo 11 ■ Atacando APIs.....291

Protocolos de comunicação com APIs	292
SOAP	293
REST.....	295
Autenticação junto à API.....	297
Autenticação básica.....	298
Chaves de API.....	298
Autenticação de portador	299
JWTs.....	300
Idiossincrasias do JWT	301
Suporte ao JWT no Burp.....	304
Postman	305
Instalação	307
Proxy de upstream	309
Ambiente.....	311
Coleções.....	312
Collection Runner.....	319
Considerações sobre o ataque.....	321
Resumo	323

Capítulo 12 ■ Atacando um CMS	324
Avaliação da aplicação.....	325
WPScan	325
sqlmap.....	332
droopescan.....	333
Scanner web Arachni	335
Porta dos fundos no código	338
Persistência	339
Exfiltração de credenciais.....	350
Resumo	361
Capítulo 13 ■ Invadindo containers	362
Cenário vulnerável com o Docker.....	365
Garantindo o acesso.....	366
Reconhecimento da situação	375
Saindo do container	383
Resumo	389