

PYTHON **para Pentest**

Daniel Moreno

Novatec

© Novatec Editora Ltda. 2018.

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: Smirna Cavalheiro

Editoração eletrônica: Carolina Kuwabata

Capa: Carolina Kuwabata

ISBN: 978-85-7522-692-6

Histórico de impressões:

Julho/2018 Primeira edição

Novatec Editora Ltda.

Rua Luís Antônio dos Santos 110
02460-000 – São Paulo, SP – Brasil

Tel.: +55 11 2959-6529

Email: novatec@novatec.com.br

Site: www.novatec.com.br

Twitter: twitter.com/novateceditora

Facebook: facebook.com/novatec

LinkedIn: linkedin.com/in/novatec

Sumário

Agradecimentos	11
Isenção de responsabilidade	12
Sobre o autor	13
Prefácio	14
Nota inicial	15
Capítulo 1 = Introdução ao Python	17
1.1 Introdução ao Python	17
1.2 Tipos de dados	18
1.2.1 Inteiros.....	18
1.2.2 Texto	19
1.2.3 Booleano.....	24
1.2.4 Lista.....	25
1.2.5 Tupla	28
1.2.6 Dicionário.....	28
1.2.7 Conjuntos	29
1.3 Atribuição e comparação	31
1.4 Casting e variáveis vazias	31
1.5 Condicionais e laços de repetição	32
1.6 Funções	36
1.7 Exceções	37
1.8 Entrada, saída de dados e comentários	40
1.9 Arquivos	40
1.10 Importação	41
1.11 Classes	43
1.12 Codificação UTF-8	44

Capítulo 2 = Pentest em redes	45
2.1 Coleta de informações	46
2.1.1 Enumeração de servidores DNS.....	46
2.1.2 Transferência de zona	50
2.1.3 Whois	51
2.1.4 Enumeração de usuários via SMTP.....	52
2.1.5 Scapy	53
2.1.6 Coleta de banner	63
2.1.7 Port scanner	64
2.1.8 Integrando Python com Nmap.....	65
2.2 Exploração.....	68
2.2.1 Automatizando a execução de exploits	68
2.2.2 Engenharia social.....	72
2.3 Escalonamento de privilégios.....	77
2.3.1 Escalonamento de privilégios vertical	78
2.3.2 Escalonamento de privilégios horizontal	94
2.4.1 Backdoor em modo texto	126
2.4.2 Backdoor HTTP	142
2.4.3 Funcionalidades comuns em backdoors.....	152
2.4.4 Backdoor downloader	162
2.4.5 Comando e controle via Gmail.....	164
2.4.6 Comando e controle via SSH.....	169
2.4.7 Infectando dispositivos USB.....	173
2.4.8 Evasão de antivírus.....	177
2.5 Negação de serviço.....	177
2.5.1 SYN Flood	177
Capítulo 3 = Pentest em aplicações web	178
3.1 Coleta de informações	179
3.1.1 Coleta de banner (HTTP).....	179
3.1.2 Coleta de banner (HTTPS)	180
3.1.3 Coleta de emails	181
3.1.4 Pesquisando informações no registro.br	182
3.1.5 Testando métodos HTTP	184
3.1.6 Google bot	184
3.1.7 Crawler ativo	188
3.1.8 Crawler passivo	190
3.1.9 Enumeração de usuários	191

3.2 Manutenção do acesso.....	192
3.3 DoS e redes botnet	193
3.3.1 HULK.....	193
3.3.2 TCP Starvation.....	198
3.4 Construindo páginas de phishing.....	200
3.5 Proxy	202
3.6 Força bruta contra o Facebook.....	203
3.7 Força bruta em formulários com tokens.....	208
3.8 Integrando o BEEF ao Python.....	209

Capítulo 4 ■ Pentest em redes sem fio..... 213

4.1 Coleta de informações	214
4.1.1 Sniffer (Beacon)	214
4.1.2 Sniffer (Probe Request)	215
4.1.3 Sniffer (Probe Response)	216
4.2 Exploração	217
4.2.1 Captura do 4-way-handshake	217
4.2.2 Quebra do WPA-WPA2/PSK	218
4.3 Manutenção do acesso.....	223
4.3.1 Obtendo a senha de rede sem fio	223
4.4 DoS e redes botnet.....	225
4.4.1 Negação de serviço	225
4.4.2 Quebra do WPA-WPA2/PSK via processamento distribuído	226

Referências..... 233

Livros	233
Cursos online	234