

Testes de Invasão

Uma introdução prática ao hacking

Georgia Weidman

Copyright © 2014 by Georgia Weidman. Title of English-language original: *Penetration Testing: A Hands-On Introduction to Hacking*, ISBN 978-1-59327-564-8, published by No Starch Press. Portuguese-language edition copyright © 2014 by Novatec Editora Ltda. All rights reserved.

Copyright © 2014 por Georgia Weidman. Título original em inglês: *Penetration Testing: A Hands-On Introduction to Hacking*, ISBN 978-1-59327-564-8, publicado pela No Starch Press. Edição em português copyright © 2014 pela Novatec Editora Ltda. Todos os direitos reservados.

© Novatec Editora Ltda. 2014.

Todos os direitos reservados e protegidos pela Lei 9610 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: Marta Almeida de Sá

Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-407-6

Histórico de impressões:

Outubro/2014 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: novatec.com.br

Twitter: twitter.com/novateceditora

Facebook: facebook.com/novatec

LinkedIn: linkedin.com/in/novatec

Sumário

Sobre a autora	19
Apresentação	20
Agradecimentos.....	23
Introdução	25
Nota de agradecimento	25
Sobre este livro	26
Parte I: Definições básicas.....	27
Parte II: Avaliações.....	28
Parte III: Ataques.....	28
Parte IV: Desenvolvimento de exploits.....	29
Parte V: Hacking de dispositivos móveis.....	29
Capítulo 0 ■ Introdução aos testes de invasão	30
Fases de um teste de invasão	31
Preparação	32
Coleta de informações	33
Modelagem das ameaças.....	34
Análise de vulnerabilidades	34
Exploração de falhas.....	34
Pós-exploração de falhas	35
Geração de relatórios	35
Resumo	37

Parte I ■ Definições básicas..... 38

Capítulo 1 ■ Configurando o seu laboratório virtual 39

Instalando o VMware	39
Instalando o Kali Linux.....	40
Configurando a rede de sua máquina virtual	43
Instalando o Nessus.....	48
Instalando softwares adicionais.....	51
Configurando emuladores de Android	54
Smartphone Pentest Framework	58
Máquinas virtuais-alvo.....	60
Criando o alvo Windows XP.....	60
VMware Player no Microsoft Windows.....	60
VMware Fusion no Mac OS	63
Instalando e ativando o Windows.....	63
Instalando o VMware Tools.....	67
Desativando o Windows Firewall	69
Configurando as senhas dos usuários	69
Configurando um endereço IP estático	70
Fazendo o XP atuar como se fosse membro de um domínio Windows	72
Instalando softwares vulneráveis.....	73
Instalando o Immunity Debugger e o Mona	79
Instalando o alvo Ubuntu 8.10	81
Criando o alvo Windows 7	81
Criando uma conta de usuário.....	81
Desativando as atualizações automáticas	83
Configurando um endereço IP estático	84
Adicionando uma segunda interface de rede.....	85
Instalando softwares adicionais.....	86
Resumo	88

Capítulo 2 ■ Usando o Kali Linux..... 89

Linha de comando do Linux	89
Sistema de arquivos do Linux.....	90
Mudando de diretório	90
Conhecendo os comandos: as man pages	91
Privilégios dos usuários.....	92
Adicionando um usuário	92

Adicionando um usuário ao arquivo sudoers	93
Trocando de usuário e utilizando o sudo	94
Criando um novo arquivo ou diretório	95
Copiando, movendo e apagando arquivos	95
Adicionando texto a um arquivo	95
Concatenando texto a um arquivo	96
Permissões de arquivo	96
Editando arquivos	98
Pesquisando textos	98
Editando um arquivo com o vi	99
Manipulação de dados	100
Usando o grep	100
Usando o sed	101
Correspondência de padrões com o awk	102
Administrando pacotes instalados	102
Processos e serviços	103
Administrando redes	103
Configurando um endereço IP estático	104
Visualizando as conexões de rede	105
Netcat: o canivete suíço das conexões TCP/IP	106
Verificando se uma porta está ouvindo	106
Abrindo um shell de comandos listener	107
Enviando um shell de comandos de volta a um listener	108
Automatizando tarefas com o cron	109
Resumo	111

Capítulo 3 ■ Programação 112

Scripts com o Bash	112
Ping	112
Script Bash simples	113
Executando o nosso script	114
Adicionando funcionalidades por meio de instruções if	114
Laço for	115
Organizando os resultados	117
Scripts com Python	120
Fazendo a conexão com uma porta	121
Instrução if no Python	121
Criando e compilando programas em C	122
Resumo	124

Capítulo 4 ■ Utilizando o Metasploit.....	125
Iniciando o Metasploit	126
Encontrando módulos no Metasploit.....	128
Banco de dados de módulos.....	129
Pesquisa embutida.....	130
Configurando as opções do módulo	133
RHOST.....	133
RPORT	134
SMBPIPE	134
Exploit Target	134
Payloads (ou Shellcode)	135
Encontrando payloads compatíveis.....	136
Execução de teste.....	137
Tipos de shell.....	138
Bind Shells	138
Reverse Shells	138
Definindo um payload manualmente	139
Msfcli	141
Obtendo ajuda	141
Mostrando as opções	142
Payloads.....	143
Criando payloads standalone com o Msfvenom.....	144
Selecionando um payload	145
Configurando as opções	145
Selecionando um formato de saída	145
Servindo payloads	146
Usando o módulo Multi/Handler.....	147
Utilizando um módulo auxiliar	148
Resumo	151

Parte II ■ Avaliações153

Capítulo 5 ■ Coleta de informações.....	154
Coleta de informações de fontes abertas.....	154
Netcraft	155
Lookups com o Whois.....	156
Reconhecimento com DNS	157

Procurando endereços de email	160
Maltego	162
Scanning de portas	165
Scanning manual de portas	166
Scanning de portas com o Nmap	167
Resumo	176

Capítulo 6 ■ Descobrimo vulnerabilidades 177

Do scan de versões do Nmap à vulnerabilidade em potencial	177
Nessus	178
Políticas do Nessus	178
Realizando um scanning com o Nessus	182
Observação sobre as classificações do Nessus	184
Por que usar scanners de vulnerabilidade?	185
Exportando os resultados do Nessus	185
Pesquisando vulnerabilidades	186
Nmap Scripting Engine	187
Executando um único script no NSE	189
Módulos de scanner do Metasploit	192
Funções para verificação de exploits no Metasploit	193
Scanning de aplicações web	194
Nikto	195
Atacando o XAMPP	196
Credenciais default	196
Análise manual	197
Explorando uma porta estranha	197
Encontrando nomes de usuário válidos	200
Resumo	200

Capítulo 7 ■ Capturando tráfego 202

Configuração da rede para capturar o tráfego	202
Usando o Wireshark	203
Capturando tráfego	203
Filtrando o tráfego	205
Seguindo um stream TCP	206
Dissecando os pacotes	207
ARP Cache Poisoning	208
Básico sobre o ARP	208

IP Forwarding	211
ARP cache poisoning com o Arpspoof.....	212
Usando o ARP cache poisoning para personificar o gateway default	213
DNS Cache Poisoning	214
Iniciando.....	216
Usando o Dnsspoof	217
Ataques SSL	218
Básico sobre o SSL	218
Usando o Ettercap para ataques SSL do tipo man-in-the-middle	219
SSL Stripping.....	221
Usando o SSLstrip	222
Resumo	224

Parte III ■ Ataques225

Capítulo 8 ■ Exploração de falhas 226

Retornando ao MS08-067	227
Payloads do Metasploit.....	227
Meterpreter	229
Explorando as credenciais default do WebDAV	230
Executando um script no servidor web do alvo	231
Fazendo o upload de um payload do Msfvenom.....	231
Explorando o phpMyAdmin aberto	234
Fazendo download de um arquivo com o TFTP	235
Fazendo o download de arquivos críticos	237
Fazendo o download de um arquivo de configuração	237
Fazendo download do arquivo SAM do Windows	238
Explorando um buffer overflow em um software de terceiros	239
Explorando aplicações web de terceiros.....	240
Explorando um serviço comprometido.....	243
Explorando os compartilhamentos NFS abertos	244
Resumo	246

Capítulo 9 ■ Ataques a senhas 247

Gerenciamento de senhas	247
Ataques online a senhas	248
Listas de palavras	249
Descobrimo nomes de usuário e senhas com o Hydra.....	253

Ataques offline a senhas	255
Recuperando hashes de senha a partir de um arquivo SAM do Windows ...	256
Fazendo o dump de hashes de senha por meio de acesso físico	258
Algoritmos de hashing LM versus NTLM.....	261
Problema com hashes de senha LM.....	262
John the Ripper	263
Quebrando senhas do Linux.....	266
Quebrando senhas de arquivos de configuração	267
Tabelas rainbow	267
Serviços online para quebra de senhas	268
Fazendo o dump de senhas em formato texto simples	268
Resumo	269

Capítulo 10 ■ Exploração de falhas do lado do cliente..... 270

Evitando filtros com payloads do Metasploit	271
Todas as portas	271
Payloads HTTP e HTTPS	272
Ataques do lado do cliente	274
Exploração de falhas de navegadores	275
Exploits para PDF	283
Exploits de Java	288
browser_autopwn.....	295
Winamp	298
Resumo	300

Capítulo 11 ■ Engenharia social..... 302

Social-Engineer Toolkit.....	303
Ataques spear-phishing	304
Selecionando um payload	305
Configurando as opções	306
Dando nome ao seu arquivo.....	307
Um ou vários emails	307
Criando o template.....	308
Definindo o alvo.....	309
Configurando um listener.....	310
Ataques web	311
Ataques de email em massa	314
Ataques em várias direções	317
Resumo	317

Capítulo 12 ■ Evitando aplicações antivírus 318

Cavalos de Troia (trojans)	318
Msfvenom	319
Como funcionam os aplicativos antivírus.....	322
Microsoft Security Essentials	322
VirusTotal	324
Passando por um programa antivírus.....	325
Efetuando uma codificação	325
Cross-compilação personalizada	328
Criptografando executáveis com o Hyperion	331
Evitando os antivírus com o Veil-Evasion	333
Escondendo-se à vista de todos	337
Resumo	338

Capítulo 13 ■ Pós-exploração de falhas 339

Meterpreter	340
Utilizando o comando upload.....	341
getuid	342
Outros comandos do Meterpreter.....	342
Scripts do Meterpreter	342
Módulos de pós-exploração de falhas do Metasploit	344
Railgun.....	346
Escalção de privilégios locais.....	346
getsystem no Windows	347
Módulo de escalção de privilégios locais para o Windows	347
Evitando o UAC no Windows	349
Escalção de privilégios com o udev no Linux	350
Coleta de informações locais.....	356
Procurando arquivos	356
Keylogging (registro de teclas)	356
Obtendo credenciais	357
Comandos net.....	360
Outra maneira de acessar um sistema	361
Verificando o histórico do Bash.....	361
Movimento lateral.....	362
PSExec	362
Pass the Hash (Passe a hash)	364
SSHExec	366

Token para personalização	368
Incognito	368
Captura de SMB.....	370
Pivoteamento	372
Adicionando uma rota no Metasploit	374
Scanners de porta do Metasploit	375
Executando um exploit por meio de um pivô	376
Socks4a e ProxyChains	376
Persistência	378
Adicionando um usuário	379
Persistência no Metasploit	380
Criando um cron job no Linux	381
Resumo	382

Capítulo 14 ■ Testes em aplicações web 383

Utilizando o Burp Proxy	383
Injeção de SQL.....	388
Testando a existência de vulnerabilidades de injeção de SQL.....	390
Explorando vulnerabilidades de injeção de SQL.....	391
Usando o SQLMap.....	391
Injeção de XPath	393
Inclusão de arquivos locais	395
Inclusão de arquivos remotos.....	398
Execução de comandos.....	398
Cross-site Scripting	401
Verificando a existência de uma vulnerabilidade de XSS refletido	401
Tirando proveito do XSS com o Browser Exploitation Framework.....	403
Cross-site Request Forgery	408
Scanning de aplicações web com o w3af.....	408
Resumo	410

Capítulo 15 ■ Ataques wireless 412

Instalação	412
Visualizando as interfaces wireless disponíveis.....	413
Scan para descobrir pontos de acesso	414
Modo monitor	414
Capturando pacotes	416
Wireless aberto	416

Wired Equivalent Privacy	417
Pontos fracos do WEP	420
Efetuando o cracking das chaves WEP com o Aircrack-ng	421
Wi-Fi Protected Access.....	425
WPA2.....	426
Processo de conexão corporativa	426
O processo de conexão pessoal.....	427
Handshake de quatro vias	427
Quebrando chaves WPA/WPA2	429
Wi-Fi Protected Setup.....	433
Problemas com o WPS.....	433
Cracking do WPS com o Bully	434
Resumo	434

Parte IV ■ Desenvolvimento de exploits435

Capítulo 16 ■ Buffer overflow com base em pilha no Linux 436

Teoria de memória	436
Buffer overflow no Linux.....	440
Um programa vulnerável	440
Provocando uma falha	442
Executando o GDB.....	444
Provocando uma falha no programa com o GDB	449
Controlando o EIP	452
Sequestrando a execução.....	454
Ordem dos bytes (endianness)	456
Resumo	458

Capítulo 17 ■ Buffer overflow com base em pilha no Windows 459

Procurando uma vulnerabilidade conhecida no War-FTP	460
Provocando uma falha.....	463
Localizando o EIP	465
Gerando um padrão cíclico para determinar o offset	466
Verificando os offsets	470
Sequestrando a execução	472
Obtendo um shell	478
Resumo	484

Capítulo 18 ■ Sobrescritas de SEH 485

Exploits de sobrescrita de SEH.....	486
Passando o controle ao SEH	491
Encontrando a string de ataque na memória	492
POP POP RET	497
SafeSEH.....	498
Usando um short jump	503
Selecionando um payload.....	505
Resumo	506

Capítulo 19 ■ Fuzzing, porte de exploits e módulos do Metasploit 507

Efetuando fuzzing em programas	507
Encontrando bugs em revisão de código.....	508
Efetuando fuzzing em um servidor Trivial FTP	508
Tentativa de provocar uma falha.....	510
Portando exploits públicos para atender às suas necessidades.....	515
Encontrando um endereço de retorno	518
Substituindo o shellcode	519
Alterando o exploit	519
Criando módulos para o Metasploit	521
Um módulo semelhante com string de exploit	524
Portando o código de nosso exploit.....	525
Técnicas para atenuação de exploração de falhas.....	530
Cookies de pilha	530
Address Space Layout Randomization	531
Data Execution Prevention.....	532
Assinatura obrigatória de código	532
Resumo	533

Parte V ■ Hacking de dispositivos móveis535**Capítulo 20 ■ Utilizando o Smartphone Pentest Framework 536**

Vetores de ataque móvel	537
Mensagens de texto	537
Near Field Communication.....	538
Códigos QR	538

Smartphone Pentest Framework	538
Configurando o SPF	539
Emuladores de Android	541
Associando um modem móvel	541
Criando o aplicativo Android.....	541
Instalando o aplicativo.....	542
Associando o servidor do SPF e o aplicativo.....	544
Ataques remotos	546
Login default do SSH no iPhone	546
Ataques do lado do cliente	548
Shell do lado do cliente.....	548
Controle remoto com o USSD	550
Aplicativos maliciosos	552
Criando agentes SPF maliciosos	553
Pós-exploração de falhas em dispositivos móveis.....	561
Coleta de informações	561
Controle remoto	563
Efetuando o pivoteamento por meio de dispositivos móveis	564
Escalação de privilégios	570
Resumo	571
Recursos	572
Fazendo o download dos softwares para criar o seu laboratório virtual	575