

Pentest em Redes de Computadores

ROYCE DAVIS

MANNING

Novatec

Original English language edition published by Manning Publications Co., Copyright © 2020 by Manning Publications. Portuguese-language edition for Brazil copyright © 2021 by Novatec Editora. All rights reserved.

Edição original em Inglês publicada pela Manning Publications Co., Copyright © 2020 pela Manning Publications. Edição em Português para o Brasil copyright © 2021 pela Novatec Editora. Todos os direitos reservados.

© Novatec Editora Ltda. [2021].

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

ISBN do impresso: 978-65-86057-82-9

ISBN do ebook: 978-65-86057-83-6

Histórico de impressões:

Dezembro/2021 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: <https://novatec.com.br>

Twitter: twitter.com/novateceditora

Facebook: facebook.com/novatec

LinkedIn: linkedin.com/in/novatec

GRA20211124

Sumário

- Prefácio 11**
- Agradecimentos..... 14**
- Sobre este livro 15**
- Sobre o autor 18**
- Sobre a ilustração da capa 19**
- Capítulo 1 ■ Pentest em rede de computadores 20**
 - 1.1 Violações de dados corporativos 21
 - 1.2 Como os hackers invadem 22
 - 1.2.1 Papel do defensor..... 22
 - 1.2.2 Papel do invasor..... 23
 - 1.3 Simulação de ataques de adversários: pentest 23
 - 1.3.1 Fluxo de trabalho típico de um INPT 25
 - 1.4 Quando um pentest é menos eficaz 26
 - 1.4.1 Fruto ao alcance das mãos (Low-hanging fruit – LHF)..... 27
 - 1.4.2 Quando uma empresa realmente precisa de um pentest?..... 27
 - 1.5 Executando um pentest na rede 28
 - 1.5.1 Fase 1: Coleta de informações 29
 - 1.5.2 Fase 2: Invasão com foco..... 31
 - 1.5.3 Fase 3: Pós-exploração de falhas e escalção de privilégios..... 32
 - 1.5.4 Fase 4: Documentação 33
 - 1.6 Configurando o seu ambiente de laboratório 34
 - 1.6.1 Projeto Capsulecorp Pentest 35
 - 1.7 Criando a sua própria plataforma virtual de pentest 35
 - 1.7.1 Comece com o Linux..... 35
 - 1.7.2 Projeto Ubuntu 36
 - 1.7.3 Por que não usar uma distribuição para pentest? 37
 - Resumo 38

Fase 1 ■ Coleta de informações..... 40

Capítulo 2 ■ Descobrindo hosts na rede 41

2.1 Entendendo o escopo de seu procedimento de teste.....	44
2.1.1 Escopo caixa-preta, caixa-branca e caixa-cinza	44
2.1.2 Capsulecorp	45
2.1.3 Configurando o ambiente Capsulecorp Pentest.....	47
2.2 Internet Control Message Protocol	47
2.2.1 Usando o comando ping	48
2.2.2 Usando bash para fazer um pingsweep em uma faixa da rede	50
2.2.3 Limitações ao uso do comando ping	52
2.3 Descobrindo hosts com o Nmap.....	53
2.3.1 Principais formatos de saída.....	55
2.3.2 Usando portas de interface de gerenciamento remoto	56
2.3.3 Melhorando o desempenho do scan do Nmap.....	58
2.4 Métodos adicionais para descoberta de hosts	60
2.4.1 Força bruta de DNS	61
2.4.2 Captura e análise de pacotes	61
2.4.3 Buscando sub-redes	62
Resumo	64

Capítulo 3 ■ Descobrindo serviços na rede 65

3.1 Serviços de rede do ponto de vista de um invasor	66
3.1.1 Entendendo a comunicação dos serviços de rede.....	68
3.1.2 Identificando serviços de rede à escuta	69
3.1.3 Banners de serviços de rede.....	70
3.2 Scanning de portas com o Nmap	71
3.2.1 Portas comuns	72
3.2.2 Scanning de todas as 65.536 portas TCP.....	76
3.2.3 Processando a saída de scripts NSE.....	78
3.3 Parsing da saída XML com o Ruby.....	82
3.3.1 Criando listas de alvos específicas por protocolo	89
Resumo	90

Capítulo 4 ■ Descobrindo vulnerabilidades na rede..... 91

4.1 Entendendo a descoberta de vulnerabilidades	92
4.1.1 Seguindo o caminho mais fácil	94
4.2 Descobrindo vulnerabilidades de patching.....	94
4.2.1 Scanning para o MS17-010 Eternal Blue	97
4.3 Descobrindo vulnerabilidades de autenticação	98
4.3.1 Criando uma lista de senhas específica para um cliente	99
4.3.2 Usando força bruta em senhas de contas locais do Windows	102
4.3.3 Uso de força bruta em senhas de bancos de dados MSSQL e MySQL	104
4.3.4 Uso de força bruta em senhas do VNC	108

4.4 Descobrimos vulnerabilidades de configuração.....	111
4.4.1 Instalando o Webshot	112
4.4.2 Analisando a saída do Webshot.....	113
4.4.3 Adivinhando senhas de servidores web manualmente.....	115
4.4.4 Preparando-se para a invasão com foco.....	118
Resumo	118
 Fase 2 ■ Invasão com foco	119
 Capítulo 5 ■ Atacando serviços web vulneráveis	120
5.1 Entendendo a fase 2: invasão com foco.....	121
5.1.1 Implantando web shells backdoor.....	122
5.1.2 Acessando serviços de gerenciamento remoto	122
5.1.3 Explorando patches de software ausentes	123
5.2 Conseguindo um acesso inicial.....	123
5.3 Comprometendo um servidor Tomcat vulnerável	125
5.3.1 Criando um arquivo WAR malicioso.....	125
5.3.2 Implantando o arquivo WAR	127
5.3.3 Acessando o web shell a partir de um navegador	128
5.4 Shells interativos versus não interativos	130
5.5 Fazendo um upgrade para um shell interativo	131
5.5.1 Fazendo um backup de sethc.exe.....	132
5.5.2 Modificando as ACLs de um arquivo com cacls.exe.....	133
5.5.3 Iniciando o Sticky Keys por meio do RDP.....	134
5.6 Comprometendo um servidor Jenkins vulnerável	136
5.6.1 Execução do Groovy Script Console	137
Resumo	138
 Capítulo 6 ■ Atacando serviços de banco de dados vulneráveis	139
6.1 Comprometendo um Microsoft SQL Server.....	140
6.1.1 Procedimentos armazenados do MSSQL	142
6.1.2 Listando servidores MSSQL com o Metasploit.....	143
6.1.3 Ativando o xp_cmdshell	144
6.1.4 Executando comandos do sistema operacional com o xp_cmdshell.....	147
6.2 Roubando hashes de senha de contas Windows	149
6.2.1 Copiando as hives de registro com o reg.exe.....	151
6.2.2 Download das cópias das hives de registro	153
6.3 Extraíndo hashes de senha com o credump.....	155
6.3.1 Entendendo a saída do pwdump.....	156
Resumo	157
 Capítulo 7 ■ Atacando serviços sem patches	159
7.1 Entendendo os exploits de software.....	160
7.2 Entendendo o ciclo de vida típico de um exploit	161

7.3 Comprometendo o MS17-010 com o Metasploit	163
7.3.1 Verificando se o patch está ausente	164
7.3.2 Usando o módulo de exploit ms17_010_psexec	166
7.4 T Payload do shell Meterpreter	168
7.4.1 Comandos úteis do Meterpreter	170
7.5 Cuidados com o banco de dados público de exploits	174
7.5.1 Gerando um shellcode personalizado	175
Resumo	177

Fase 3 ■ Pós-exploração de falhas e escalção de privilégios.....178

Capítulo 8 ■ Pós-exploração de falhas no Windows..... 179

8.1 Objetivos básicos da pós-exploração de falhas	180
8.1.1 Manutenção de um método confiável de reentrada.....	180
8.1.2 Coleta de credenciais	181
8.1.3 Movimentação lateral.....	181
8.2 Manutenção de um método confiável de reentrada com o Meterpreter.....	182
8.2.1 Instalando uma backdoor de execução automática do Meterpreter.....	183
8.3 Coletando credenciais com o Mimikatz	186
8.3.1 Usando a extensão para o Meterpreter.....	186
8.4 Coleta de credenciais do domínio em cache.....	188
8.4.1 Usando o módulo de pós-exploração de falhas do Meterpreter.....	189
8.4.2 Quebrando credenciais do cache com o John the Ripper.....	190
8.4.3 Usando um arquivo de dicionário com o John the Ripper	192
8.5 Coleta de credenciais do sistema de arquivos	194
8.5.1 Encontrando arquivos com findstr e where	195
8.6 Movimentação lateral com o Pass-the-Hash	196
8.6.1 Usando o módulo smb_login do Metasploit	198
8.6.2 Passing-the-hash com o CrackMapExec	200
Resumo	202

Capítulo 9 ■ Pós-exploração de falhas no Linux ou no Unix.....203

9.1 Mantendo um método confiável de reentrada com cron jobs.....	204
9.1.1 Criando um par de chaves SSH.....	205
9.1.2 Permitindo uma autenticação com chave pública	207
9.1.3 Tunelamento com o SSH	209
9.1.4 Automatizando um túnel SSH com o cron	212
9.2 Coletando credenciais	213
9.2.1 Coletando credenciais do histórico do bash	215
9.2.2 Coletando hashes de senha	216
9.3 Escalção de privilégios com binários SUID	217
9.3.1 Encontrando binários SUID com o comando find.....	218
9.3.2 Inserindo um novo usuário em /etc/passwd.....	221
9.4 Passando chaves SSH.....	223

9.4.1 Roubando chaves de um host comprometido	224
9.4.2 Scanning de vários alvos com o Metasploit	225
Resumo	228
Capítulo 10 ■ Controlando toda a rede	229
10.1 Identificando contas de usuários administradores do domínio	232
10.1.1 Utilizando o comando net para consultar grupos do Active Directory	232
10.1.2 Encontrando usuários administradores do domínio que estão logados	233
10.2 Obrendo privilégios de administrador do domínio	235
10.2.1 Personificando usuários logados com o Incognito	236
10.2.2 Coletando credenciais em formato texto simples com o Mimikatz	238
10.3 ntds.dit e as chaves do reino.....	239
10.3.1 Vencendo as limitações com a VSC.....	241
10.3.2 Extraindo todos os hashes com o secretsdump.py.....	245
Resumo	247
Fase 4 ■ Documentação.....	248
Capítulo 11 ■ Limpeza após o procedimento de teste	249
11.1 Encerrando conexões de shell ativas	251
11.2 Desativando contas de usuários locais.....	252
11.2.1 Removendo entradas de /etc/passwd.....	252
11.3 Removendo arquivos remanescentes no sistema de arquivos	253
11.3.1 Apagando cópias das hives de registro	254
11.3.2 Removendo pares de chaves SSH.....	255
11.3.3 Removendo cópias de ntds.dit	256
11.4 Desfazendo mudanças de configuração	257
11.4.1 Desativando os procedimentos armazenados do MSSQL.....	257
11.4.2 Desativando compartilhamentos de arquivo anônimos	258
11.4.3 Removendo entradas do crontab.....	260
11.5 Fechando as backdoors.....	260
11.5.1 Desinstalando arquivos WAR do Apache Tomcat.....	261
11.5.2 Fechando a backdoor Sticky Keys	262
11.5.3 Desinstalando callbacks de persistência do Meterpreter.....	263
Resumo	265
Capítulo 12 ■ Escrevendo um relatório de pentest robusto para o cliente.....	266
12.1 Oito componentes de um relatório de pentest robusto para o cliente	267
12.2 Resumo executivo	269
12.3 Metodologia do procedimento de teste.....	270
12.4 Narrativa do ataque	271
12.5 Observações técnicas.....	271
12.5.1 Recomendações para as descobertas.....	274

12.6 Apêndices	275
12.6.1 Definições de níveis de gravidade	275
12.6.2 Hosts e serviços	276
12.6.3 Lista de ferramentas.....	277
12.6.4 Referências adicionais	277
12.7 Considerações finais	277
12.8 E agora?	279
Resumo	280

Apêndice A ■ Criando uma plataforma virtual de pentest.....281

A.1 Criando uma máquina virtual Ubuntu	281
A.2 Outras dependências do sistema operacional.....	283
A.2.1 Gerenciando pacotes Ubuntu com o apt	283
A.2.2 Instalando o CrackMapExec	284
A.2.3 Personalizando a aparência de seu terminal	284
A.3 Instalando o Nmap.....	285
A.3.1 NSE: Nmap Scripting Engine.....	285
A.3.2 Dependências do sistema operacional.....	287
A.3.3 Compilando e instalando a partir do código-fonte	288
A.3.4 Explorando a documentação	289
A.4 Linguagem de scripting Ruby	290
A.4.1 Instalando o Ruby Version Manager	291
A.4.2 Escrevendo o exemplo Hello World obrigatório.....	292
A.5 Framework Metasploit	295
A.5.1 Dependências do sistema operacional	296
A.5.2 Gemas Ruby necessárias	296
A.5.3 Configurando o PostgreSQL para o Metasploit	298
A.5.4 Navegando no msfconsole	300

Apêndice B ■ Comandos básicos do Linux304

B.1 Comandos CLI.....	304
B.1.1 \$ cat	304
B.1.2 \$ cut	306
B.1.3 \$ grep.....	307
B.1.4 \$ sort e wc	308
B.2 tmux.....	309
B.2.1 Usando comandos tmux	310
B.2.2 Salvando uma sessão tmux	311

Apêndice C ■ Criando a rede de laboratório Capsulecorp Pentest 312

C.1 Requisitos de hardware e de software	313
C.2 Criando os principais servidores Windows	316
C.2.1 Goku.capsulecorp.local.....	316
C.2.2 Gohan.capsulecorp.local.....	317
C.2.3 Vegeta.capsulecorp.local	317

C.2.4 Trunks.capsulecorp.local	318
C.2.5 Nappa.capsulecorp.local e tien.capsulecorp.local	318
C.2.6 Yamcha.capsulecorp.local e Krillin.capsulecorp.local	318
C.3 Criando os servidores Linux	319
Apêndice D ■ Relatório do pentest na rede interna da Capsulecorp	320
Resumo executivo	320
Escopo do procedimento de teste	320
Resumo das observações	320
Metodologia do procedimento de teste	321
Coleta de informações	321
Invasão com foco	322
Pós-exploração de falhas e escalção de privilégios	322
Documentação e limpeza	323
Narrativa do ataque	323
Observações técnicas	324
Apêndice 1: Definições de níveis de gravidade	328
Crítico	328
Alto	328
Médio	328
Baixo	328
Apêndice 2: Hosts e serviços	328
Apêndice 3: Lista de ferramentas	333
Apêndice 4: Referências adicionais	334
Apêndice E ■ Respostas dos exercícios	335
Exercício 2.1: Identificando os alvos de seu procedimento de teste	335
Exercício 3.1: Criando listas de alvos específicas por protocolo	336
Exercício 4.1: Identificando patches ausentes	336
Exercício 4.2: Criando uma lista de senhas específicas para um cliente	337
Exercício 4.3: Descobrimdo senhas fracas	338
Exercício 5.1: Implantando um arquivo WAR malicioso	338
Exercício 6.1: Roubando as hives de registro SYSTEM e SAM	338
Exercício 7.1: Comprometendo tien.capsulecorp.local	339
Exercício 8.1: Acessando seu primeiro host de nível dois	339
Exercício 10.1: Roubando senhas do ntds.dit	339
Exercício 11.1: Fazendo uma limpeza após o procedimento de teste	340
Índice remissivo	341