

Avaliação de segurança de redes

CONHEÇA A SUA REDE

Chris McNab

Novatec

Authorized Portuguese translation of the English edition of *Network Security Assessment*, 3rd Edition ISBN 9781491910955 © 2016 Chris McNab. This translation is published and sold by permission of O'Reilly Media, Inc., the owner of all rights to publish and sell the same.

Tradução em português autorizada da edição em inglês da obra *Network Security Assessment*, 3rd Edition ISBN 9781491910955 © 2016 Chris McNab. Esta tradução é publicada e vendida com a permissão da O'Reilly Media, Inc., detentora de todos os direitos para publicação e venda desta obra.

© Novatec Editora Ltda. 2017.

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: Priscila A. Yoshimatsu

Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-565-3

Histórico de impressões:

Abril/2017 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

Prefácio	17
Capítulo 1 ■ Introdução à avaliação de segurança de redes	30
O estado da arte	30
Ameaças e superfícies de ataque	32
Atacando softwares clientes	32
Atacando software de servidores	33
Atacando aplicações web	34
Lógica exposta	35
Diferentes tipos de avaliação	36
Análises estáticas.....	37
Testes dinâmicos	39
O que este livro inclui	42
Capítulo 2 ■ Fluxo de trabalho e ferramentas para avaliação.....	43
Metodologia para avaliação de segurança de redes	44
Reconhecimento	44
Scanning de vulnerabilidades	45
Investigação das vulnerabilidades.....	45
Exploração de vulnerabilidades.....	48
Uma abordagem iterativa para a avaliação	49
Sua plataforma de testes.....	50
Atualizando o Kali Linux.....	50
Instalando um servidor vulnerável	51
Capítulo 3 ■ Vulnerabilidades e adversários	52
O conceito fundamental de hacking	52
Por que os softwares são vulneráveis.....	53
Considerando a superfície de ataque.....	54
Uma taxonomia para os erros de segurança de software.....	55
Modelagem de ameaças.....	57
Componentes do sistema	57
Objetivos dos adversários.....	58

Acesso ao sistema e contexto de execução	59
Sistema econômico dos invasores	61
Atacando aplicações C/C++	62
Layout de memória em tempo de execução	63
Registradores do processador e memória	66
Escrevendo na memória	67
Lendo da memória.....	69
Recursos de segurança de compiladores e de sistemas operacionais	72
Esquivando-se de recursos comuns de segurança.....	74
Falhas na lógica e outros bugs	79
Pontos fracos da criptografia	80
Revisão sobre vulnerabilidades e adversários	83
Capítulo 4 ■ Descoberta de redes na internet	84
Consultando ferramentas de pesquisa e sites.....	85
Pesquisas no Google	85
Consultando o Netcraft	89
Usando o Shodan	90
DomainTools.....	92
Servidores de chaves PGP públicas	93
Pesquisando o LinkedIn.....	93
WHOIS para domínios	94
Consultas manuais ao WHOIS	95
WHOIS para IPs.....	97
Ferramentas de consulta de IP no WHOIS e exemplos	97
Listagem de BGP.....	101
Consultas de DNS.....	102
Consultas de DNS direto (forward DNS)	103
Técnicas para transferência de zona DNS	105
Descoberta de DNS direto.....	108
Varredura de DNS reverso.....	111
Listagem de hosts IPv6	113
Referências cruzadas em conjuntos de dados de DNS	115
Sondagem de SMTP	116
Automatizando listagens	117
Revisão das técnicas de listagem.....	118
Medidas de proteção contra listagens	119
Capítulo 5 ■ Descoberta de redes locais.....	120
Protocolos de link de dados.....	120
Testes de Ethernet 802.3	121
VLAN 802.1Q.....	125

PNAC 802.1X.....	132
CDP	137
STP 802.1D	140
Protocolos IP locais.....	143
DHCP	144
PXE.....	146
LLMNR, NBT-NS e mDNS	148
WPAD	150
Protocolos de roteamento interno.....	151
Descoberta de redes IPv6	160
Identificando gateways locais	166
Revisão sobre descoberta de redes locais	166
Medidas de proteção contra ataques a redes locais	168
Capítulo 6 ■ Scanning de redes IP	170
Scanning inicial de rede usando Nmap	171
ICMP	171
TCP	173
UDP	175
SCTP	178
Reunindo tudo	182
Avaliação de baixo nível de IP	184
Compondo pacotes arbitrários	185
Fingerprinting da pilha TCP/IP	187
Análise do ID de IP	188
Manipulando o TTL para uma engenharia reversa das ACLs	191
Descobrindo endereços IP internos.....	192
Scanning de vulnerabilidades com o NSE	193
Scanning de vulnerabilidades em massa	195
Evasão de IDS e de IPS	196
Manipulação de TTL.....	197
Inserção e scrambling (desorganização) de dados com o SniffJoke	197
Configurando e executando o SniffJoke.....	198
Revisão sobre scanning de rede	200
Medidas de proteção contra scanning de rede	201
Capítulo 7 ■ Avaliação de serviços comuns de rede	203
FTP	204
Fingerprinting de serviços FTP	205
Vulnerabilidades conhecidas de FTP	205
TFTP	207
Vulnerabilidades conhecidas de TFTP	209

SSH.....	210
Fingerprinting	211
Listando recursos	213
Credenciais default e fixas.....	217
Chaves de host geradas sem segurança	219
Falhas em softwares de servidores SSH.....	219
Telnet	220
Credenciais default de Telnet	221
Falhas em softwares de servidores Telnet.....	221
IPMI.....	222
DNS	224
Fingerprinting	224
Testando se há suporte para recursão	226
Falhas conhecidas de servidores DNS.....	226
DNS multicast	228
NTP	229
SNMP	231
Explorando falhas do SNMP.....	232
LDAP	238
Autenticação no LDAP.....	238
Operações de LDAP.....	240
Estrutura de diretórios do LDAP.....	241
Fingerprinting e vinculação anônima	243
Quebra de senha por força bruta	244
Obtendo dados confidenciais	245
Falhas de implementações de servidores LDAP.....	246
Kerberos.....	247
Chaves Kerberos.....	249
Formato do ticket	250
Superfície de ataque do Kerberos.....	252
Ataques locais	252
Ataques remotos sem autenticação	257
Falhas em implementações de Kerberos.....	259
VNC	259
Atacando servidores VNC.....	261
Serviços RPC no Unix.....	262
Consultando manualmente os serviços RPC expostos.....	263
Vulnerabilidades de serviços RPC	265
Revisão sobre avaliação de serviços comuns de rede.....	266
Deixando os serviços mais robustos e possíveis medidas de proteção.....	267

Capítulo 8 ■ Avaliação dos serviços da Microsoft.....	269
Serviço de nomes do NetBIOS.....	271
SMB	273
Serviços RPC da Microsoft.....	273
Atacando o SMB e o RPC.....	274
Mapeando as superfícies de ataque da rede.....	275
Acesso anônimo ao IPC via SMB.....	276
Falhas em implementações de SMB	278
Identificando serviços RPC expostos	278
Quebra de senha por força bruta	285
Autenticação e uso do acesso	287
Serviços de Remote Desktop	294
Quebra de senha por força bruta	294
Avaliando a segurança de transporte	295
Falhas em implementações de RDP	296
Revisão sobre testes de serviços da Microsoft.....	297
Medidas de proteção para serviços da Microsoft	297
Capítulo 9 ■ Avaliação de serviços de email	299
Protocolos de email.....	299
SMTP	300
Fingerprinting do serviço	301
Mapeando a arquitetura de SMTP	302
Listando comandos e extensões aceitos	306
Falhas remotamente exploráveis.....	308
Listagem de contas de usuário.....	310
Quebra de senha por força bruta	311
Evasão de sistemas de verificação de conteúdo	313
Revisão dos recursos de segurança de emails	314
Phishing via SMTP	318
POP3.....	321
Fingerprinting do serviço	321
Quebra de senha por força bruta	321
IMAP	322
Fingerprinting do serviço	323
Quebra de senha por força bruta	323
Falhas conhecidas de servidores IMAP	324
Revisão sobre testes de serviços de email	324
Medidas de proteção para serviços de email.....	325

Capítulo 10 ■ Avaliação de serviços VPN	327
IPsec.....	327
Formato do pacote.....	328
ISAKMP, IKE e IKEv2.....	329
Avaliação de IKE	330
Pontos fracos exploráveis do IPsec	334
PPTP	340
Revisão dos testes de VPN	342
Medidas de proteção para serviços VPN	342
Capítulo 11 ■ Avaliação de serviços TLS	344
Funcionamento do TLS.....	345
Negociação de sessão.....	346
Pacotes de criptografia	349
Troca de chaves e autenticação	351
Autenticação no TLS	356
Restabelecimento de sessão.....	362
Renegociação de sessão.....	363
Compactação	365
STARTTLS	365
Compreendendo as vulnerabilidades de TLS	366
Falhas exploráveis.....	367
Medidas para atenuar exposições de TLS	371
Avaliando endpoints TLS	372
Identificando a biblioteca de TLS e a versão.....	373
Listando protocolos e pacotes de criptografia aceitos	374
Listando recursos e extensões aceitos	378
Análise de certificado.....	381
Testes de estresse em endpoints TLS	383
Acessando serviços encapsulados com TLS manualmente.....	385
Revisão da avaliação de serviços TLS	385
Deixando o TLS mais robusto	386
Deixando as aplicações web mais robustas	387
Capítulo 12 ■ Arquitetura de aplicações web	389
Tipos de aplicações web	389
Camadas das aplicações web	390
A camada de apresentação	391
TLS.....	392
HTTP	392
CDNs.....	401
Distribuidores de carga	401

Formatos de dados na camada de apresentação	402
A camada de aplicação.....	402
Formatos de dados na camada de aplicação	403
A camada de dados.....	404
Capítulo 13 ■ Avaliação de servidores web	406
Identificando mecanismos de proxy.....	407
Listando hosts válidos.....	409
Gerando o perfil de servidores web.....	411
Analizando as respostas do servidor	411
Análise de cabeçalhos HTTP	413
Crawling e investigação de conteúdo	417
Scanning ativo	420
Detecção de WAF	421
Fingerprinting do servidor e do framework de aplicação	422
Identificando conteúdos expostos.....	423
Classificando as vulnerabilidades de servidores web	425
Analizando conteúdos expostos	425
Quebra de senha por força bruta	427
Investigando os métodos HTTP aceitos.....	428
Vulnerabilidades conhecidas do Microsoft IIS	431
Falhas conhecidas do Apache HTTP Server.....	433
Pontos fracos conhecidos do Apache Coyote.....	434
Defeitos conhecidos do Nginx.....	435
Deixando o servidor web mais robusto	436
Capítulo 14 ■ Avaliação de frameworks de aplicações web	437
Gerando o perfil de frameworks e de repositórios de dados	438
Compreendendo falhas comuns	441
PHP.....	441
Consoles de gerenciamento de PHP	442
Pacotes CMS escritos em PHP	444
Apache Tomcat	447
A aplicação de gerenciamento.....	447
Falhas conhecidas do Tomcat.....	448
Atacando o AJP (Apache JServ Protocol)	449
Testes de JBoss	450
Gerando o perfil de servidores via HTTP	451
Consoles web e servlets de chamada.....	452
Identificando MBeans.....	452
Explorando falhas de MBeans.....	454
Explorando falhas do coletor de lixo distribuído de RMI	457

Vulnerabilidades conhecidas de JBoss	457
Scanning automatizado de JBoss.....	458
Apache Struts	459
Explorando o DefaultActionMapper	461
JDWP.....	463
Adobe ColdFusion	463
Gerando o perfil do ColdFusion.....	464
Interfaces de gerenciamento expostas	465
Defeitos conhecidos do software do ColdFusion	466
Vulnerabilidades do Apache Solr	467
Django	469
Rails.....	470
Usando o token secreto de uma aplicação	471
Node.js.....	472
Microsoft ASP.NET	473
Checklist de segurança para frameworks de aplicação.....	475
Capítulo 15 ■ Avaliação de repositórios de dados	476
MySQL.....	477
Quebra de senha por força bruta	478
Ataques ao MySQL com autenticação.....	479
PostgreSQL.....	481
Quebra de senha por força bruta	482
Ataques ao PostgreSQL com autenticação.....	483
Microsoft SQL Server.....	485
Quebra de senha por força bruta	486
Autenticação e avaliação de configuração	486
Banco de dados Oracle.....	488
Interagindo com o listener TNS.....	489
Quebra de SID do Oracle	491
Quebra de senha de contas do banco de dados	492
Autenticação no Oracle Database	493
Escalação de privilégios e pivoteamento	494
MongoDB.....	495
Redis	497
Pontos fracos conhecidos	498
Memcached	500
Apache Hadoop	501
NFS.....	502
Apple Filing Protocol	504
iSCSI	506
Medidas de proteção para repositórios de dados	507

Sumário	15
Apêndice A = Portas e tipos de mensagem comuns	509
Portas TCP	509
Portas UDP.....	511
Tipos de mensagem ICMP.....	512
Apêndice B = Fontes com informações sobre vulnerabilidades	514
Contas do Twitter	514
Sistemas de rastreamento de bugs.....	514
Listas de discussão.....	515
Eventos e conferências sobre segurança	515
Apêndice C = Pacotes de criptografia sem segurança para TLS	516
Glossário de termos.....	518