
Ocena bezpieczeństwa sieci

Poznaj swoją sieć

Chris McNab

przekład: Marek Włodarz

Spis treści

<i>Przedmowa</i>	<i>ix</i>
1 Ocena bezpieczeństwa sieci	1
Stan wiedzy	1
Zagrożenia i powierzchnia ataku	3
Odmiany sposobów testowania	7
O czym jest ta książka	12
2 Przebieg oceny i narzędzia	13
Metodologia oceny bezpieczeństwa sieci	14
Platforma testowa	20
3 Luki i przeciwnicy	23
Fundamentalne koncepcje hackingu	23
Dlaczego oprogramowanie jest podatne	24
Rozważanie powierzchni ataku	25
Taksonomia błędów zabezpieczeń oprogramowania	26
Modelowanie zagrożeń	27
Atakowanie aplikacji C/C++	33
Błędy logiki i inne bugi	48
Słabości kryptograficzne	49
Luki i przeciwnicy – podsumowanie	51
4 Odkrywanie sieci z Internetu	53
Odpytywanie wyszukiwarek i witryn Web	54
Domenowe WHOIS	62
IP WHOIS	65
Wyliczanie BGP	69
Odpytywanie DNS	69
Sondowanie SMTP	83
Automatyzowanie wyliczania	84
Podsumowanie technik wyliczania	84
Środki przeciwdziałania wylicznaniu	85
5 Lokalne odkrywanie sieci	87
Protokoły łącza danych	87
Lokalne protokoły IP	110

Odkrywanie sieci IPv6	126
Identyfikowanie bram lokalnych	132
Lokalne odkrywanie sieci – podsumowanie	133
Środki przeciwdziałania atakom na sieć lokalną	134
6 Skanowanie sieci IP	137
Wstępne skanowanie sieci przy użyciu Nmap	138
Niskopoziomowa ocena IP	150
Skanowanie podatności przy użyciu NSE	158
Masowe skanowanie podatności	160
Unikanie IDS i IDP	161
Skanowanie sieci – podsumowanie	165
Skanowanie sieci – środki zaradcze	166
7 Ocena typowych usług sieciowych	167
FTP	168
TFTP	171
SSH	174
Telnet	184
IPMI	185
DNS	187
Multicast DNS	192
NTP	193
SNMP	194
LDAP	200
Kerberos	209
VNC	221
Usługi RPC w systemach Unix	223
Ocena typowych usług sieciowych – podsumowanie	228
Wzmacnianie usług i środki zaradcze	229
8 Testowanie usług firmy Microsoft	231
Usługa nazw NetBIOS	233
Server Message Block	235
Usługi pulpitu zdalnego (Remote Desktop Services)	256
Testowanie usług Microsoft – podsumowanie	259
Usługi firmy Microsoft – środki zaradcze i przeciwdziałanie	259
9 Ocena usług pocztowych	261
Protokoły poczty elektronicznej	261
SMTP	262
POP3	282
IMAP	284

	Testowanie usług pocztowych – podsumowanie	286
	Usługi pocztowe – środki zaradcze	287
10	Ocena usług VPN.....	289
	IPsec	289
	PPTP	301
	Podsumowanie testów VPN.....	302
	Środki zabezpieczania usług VPN.....	303
11	Ocena usług TLS	305
	Mechanika TLS	306
	Istota podatności TLS	325
	Uzyskiwanie dostępu do punktów końcowych TLS	331
	Ocena punktów końcowych TLS: podsumowanie	343
	Wzmacnianie TLS	344
	Wzmacnianie aplikacji Web.....	345
12	Architektura aplikacji Web	347
	Typ aplikacji Web	347
	Warstwy aplikacji Web	348
	Warstwa prezentacji	349
	Warstwa aplikacji.....	360
13	Ocena serwerów Web	363
	Identyfikowanie mechanizmów proxy	364
	Wylizanie poprawnych hostów	366
	Profilowanie serwera Web	367
	Aktywne skanowanie	376
	Kwalifikowanie podatności serwera Web.....	380
	Wzmacnianie serwerów Web.....	392
14	Ocena platform aplikacji Web.....	393
	Profilowanie platformy i magazynu danych	394
	Istota typowych podatności	397
	PHP	397
	Apache Tomcat.....	402
	Testowanie JBoss	405
	Apache Struts	415
	JDWP	418
	Adobe ColdFusion.....	419
	Django.....	424
	Rails.....	425

Node.js	428
Microsoft ASP.NET	429
Lista kontrolna zabezpieczenia platform aplikacji	430
15 Ocena magazynów danych	431
MySQL	432
PostgreSQL	436
Microsoft SQL Server	439
Oracle Database	442
MongoDB	448
Redis	450
Memcached	453
Apache Hadoop	454
NFS	455
Apple Filing Protocol	457
iSCSI	458
Środki zaradcze dotyczące magazynów danych	459
A Dobrze znane porty i typy komunikatów	463
Porty TCP	463
Porty UDP	465
Typy komunikatów ICMP	466
B Źródła informacji o podatnościach	467
Konta na Twitterze	467
Bugtrackery	468
Listy mailingowe	468
Wydarzenia i konferencje dotyczące bezpieczeństwa	468
C Niebezpieczne pakiety kryptograficzne TLS	469
<i>Słownik akronimów i pojęć</i>	<i>473</i>
<i>Indeks</i>	<i>489</i>
<i>O autorze</i>	<i>520</i>
<i>Kolofoń</i>	<i>520</i>