

Obsah

	3
Předmluva autora	7
Co obsahuje tato kniha	7
Zpětná vazba od čtenářů	9
Errata	10

KAPITOLA 1

Metodologie a nástroje penetračních testů	11
Úvod	11
Metodologie testování	12
Penetrační testování	14
Typy testů	15
Průběh penetračních testů	18
Nástroje pro testování	22
Metodologie reportu	25
Vzdělávání a trénink	26
Závěr	36
Reference	37

KAPITOLA 2

Externí penetrační testy firemních sítí	39
Úvod	39
Případová studie	40
Fáze 1: Cíl a rozsah penetračního testu	40
Fáze 2: Sběr dat	44
Fáze 3: Skenování a exploitace	65
Fáze 4: Report	92
Závěr	95
Reference	97

KAPITOLA 3

Interní penetrační testy firemních sítí	99
Úvod	99
Případová studie	100
Fáze 1: Cíl a rozsah penetračního testu	101
Fáze 2: Sběr dat	103
Fáze 3: Skenování a exploitace	116
Fáze 4: Report	151
Závěr	154
Reference	156

KAPITOLA 4

Penetrační testy bezdrátových sítí	159
Úvod	159
Případová studie	160
Fáze 1: Cíl a rozsah penetračního testu	161
Vnější testování	162
Vnitřní testování	162
Fáze 2: Sběr dat	163
Příprava	163
Testování	165
Fáze 3: Skenování a exploitace	170
I. Vnější testování	171
II. Vnitřní testování	190
Fáze 4: Report	220
Závěr	224
Reference	226

KAPITOLA 5

Penetrační testy webových aplikací	229
Úvod	229
Případová studie	230
Fáze 1: Cíl a rozsah penetračního testu	231
Zranitelné místo: Injekce	231
Zranitelné místo: Cross-Site Scripting (XSS)	232
Zranitelné místo: Zabezpečení autentifikace a managementu relací	233
Zranitelné místo: Zabezpečení přímého odkazu na objekt	233
Fáze 2: Sběr dat	234
Průzkum veřejně dostupných informací	236
Analýza adresářové struktury serveru	237
Identifikování všech relevantních vstupů	240
Zjištění verzí serverových systémů	241
Fáze 3: Skenování a exploitace	242
Zranitelné místo: Injektování SQL a LDAP kódu	242
Zranitelné místo: XSS	258
Zranitelné místo: Zabezpečení autentifikace a managementu relací	271
Zranitelné místo: Zabezpečení přímého odkazu na objekt	278
Dodatek na závěr	282
Další inspirace	288
Fáze 4: Report	290
Závěr	293
Reference	295
Rejstřík	297