

# Obsah

	3
<b>Předmluva autora</b>	7
<b>Co obsahuje tato kniha</b>	7
<b>Zpětná vazba od čtenářů</b>	9
<b>Zdrojové kódy ke knize</b>	10
<b>Errata</b>	10
KAPITOLA 1	
<b>Metodologie a nástroje penetračních testů</b>	11
<b>Úvod</b>	11
<b>Metodologie testování</b>	12
<b>Penetrační testování</b>	14
Typy testů	15
Průběh penetračních testů	18
Nástroje pro testování	22
Metodologie reportu	25
<b>Vzdělávání a trénink</b>	26
<b>Závěr</b>	36
<b>Reference</b>	37
KAPITOLA 2	
<b>Externí penetrační testy firemních sítí</b>	39
<b>Úvod</b>	39
<b>Případová studie</b>	40
<b>Fáze 1: Cíl a rozsah penetračního testu</b>	40
<b>Fáze 2: Sběr dat</b>	44
<b>Fáze 3: Skenování a exploatace</b>	65
<b>Fáze 4: Report</b>	92
<b>Závěr</b>	96
<b>Reference</b>	97

## KAPITOLA 3

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

## KAPITOLA 4

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

## KAPITOLA 5

<b>Penetrační testy webových aplikací</b>	<b>229</b>
<b>Úvod</b>	<b>229</b>
<b>Případová studie</b>	<b>230</b>
<b>Fáze 1: Cíl a rozsah penetračního testu</b>	<b>231</b>
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
<b>Fáze 2: Sběr dat</b>	<b>234</b>
Průzkum veřejně dostupných informací	236
Analýza adresářové struktury serveru	237
Identifikování všech relevantních vstupů	240
Zjištění verzí serverových systémů	241
<b>Fáze 3: Skenování a exploatace</b>	<b>242</b>
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
<b>Fáze 4: Report</b>	<b>290</b>
<b>Závěr</b>	<b>293</b>
<b>Reference</b>	<b>295</b>
<b>Rejstřík</b>	<b>297</b>