

Podrobný obsah

Předmluva	8	
Úvod	8	
Dodatečné informace o knize	10	
K etice	10	
Kapitola 1	Nastavení prostředí	11
Příprava prostředí pro penetrační testy	11	
Hardware	11	
Komerční software	12	
Kali Linux	13	
Virtuální stroj s Windows	17	
Shrnutí	19	
Kapitola 2	Skenování sítě	21
Externí skenování	21	
Pasivní odposlech	21	
Externí/interní aktivní odposlech	27	
Postup pro skenování sítě	28	
Skenování webové aplikace	36	
Postup skenování webové aplikace	36	
Samotné skenování	36	
Shrnutí	44	
Kapitola 3	Exploitační nástroje ze skeneru	45
Metasploit	45	
Základní kroky pro konfiguraci vzdálených útoků	46	
Vyhledávání přes Metasploit (použití zranitelnosti MS08-067)	46	
Skripty	48	
Příklad s WarFTP	48	
Shrnutí	50	
Kapitola 4	Exploitační nástroje webových zranitelností	51
Penetrační testování webové aplikace	51	

SQL injection	51
Cross-site scripting (XSS)	59
Cross-Site Request Forgery (CSRF)	66
Tokeny relace	69
Dodatečné fuzz testy a validace vstupů	71
Testování funkční/obchodní logiky	75
Závěr	76

Kapitola 5 Posuny po síti 77

Na síti a bez přihlašovacích údajů	77
responder.py (Kali Linux)	77
Na síti a s přihlašovacími údaji k doméně (ale ne administrátorskými)	81
Preference zásad skupiny	81
Vytažování přihlašovacích údajů v čistém textu	83
Tipy pro post exploitaci	85
Na síti a s místním administrátorským nebo doménovým účtem	85
Přisvojení sítě pomocí PSEXec	85
Útok na řadič domény	91
Post exploitace s PowerSploitem (Windows)	93
Post exploitace s PowerShellem (Windows)	97
Otrávení ARP	100
IPv4	100
IPv6	104
Co dál, když se podařilo zfalšovat ARP	105
Proxy mezi hostiteli	112
Závěr	112

Kapitola 6 Sociální inženýrství 113

Záměna domény	113
Útok se SMTP	113
Útok se SSH	114
Cílený phishing	116
Metasploit Pro – modul Phishing	116
Social Engineering Toolkit (Kali Linux)	118
Odesílání masivních kampaní cíleného phishingu	122
Sociální inženýrství s Microsoft Excelem	123
Závěr	126

Kapitola 7 Útoky vyžadující fyzický přístup 127

Bezdrátová exploitate	127
Pasivní útoky – průzkum	128
Aktivní útoky	130
Fyzické penetrační testy	137
Klonování karty	137
Hardwarový drop box pro penetrační testy	137
Fyzické sociální inženýrství	140
Závěr	140

Kapitola 8 Jak se vyhnout antivirové ochraně 141

Obcházení antivirové ochrany	141
Skrýtí WCE před antivirem (Windows)	141
Python	146
Závěr	150

Kapitola 9 Prolamování hesel, exploits, triky 151

Úvod do prolamování hesel	151
John the Ripper (JtR)	152
oclHashcat	153
Vyhledávání zranitelností	156
Searchsploit (Kali Linux)	156
BugTraq	158
Exploit-DB	158
Dotazy na Metasploit	158
Tipy a triky	160
RC skripty uvnitř Metasploitu	160
Jak obejít ochranu řízení uživatelských účtů	161
Jak obejít filtrování webů pro vaše domény	162
Windows XP – FTP trik ze staré školy	162
Jak skrývat soubory na Windows (ADS)	162
Jak udržet naše soubory na Windows skryté	164
Nahrávání souborů do hostitelů s Windows 7 nebo 8	165

Kapitola 10	Závěrečné zprávy	167
	Jak má vypadat finální zpráva	167
	Seznam mých nejlepších postupů a tipů pro tvorbu reportů	168
Kapitola 11	Nepřestávejte se vzdělávat	171
	Hlavní konference	171
	Školící kurzy	172
	Knihy	172
	Frameworky pro penetrační testování zranitelnosti	173
	CTF hry	174
	Držte krok s nejnovějším vývojem	174
Dodatek	Závěrečné poznámky	175
	Poděkování	176
Rejstřík		177