

SPIS TREŚCI

Przedmowa	7
Wprowadzenie	9
Rozdział 1. Przed grą — konfiguracja	13
Przygotowanie komputera do testów penetracyjnych	13
Sprzęt	13
Oprogramowanie komercyjne	14
Kali Linux	15
Maszyna wirtualna z systemem Windows	20
Podsumowanie	22
Rozdział 2. Przed gwizdkiem — skanowanie sieci	23
Skanowanie zewnętrzne	23
Analiza pasywna	23
Discover Scripts (dawniej BackTrack Scripts) — system Kali Linux	24
Realizacja analizy pasywnej	25
Użycie adresów e-mail i danych uwierzytelniających, które wyciekły do internetu	27
Analiza aktywna — wewnętrzna i zewnętrzna	31
Proces skanowania sieci	31
Skanowanie aplikacji webowych	40
Proces skanowania witryn	40
Skanowanie aplikacji internetowych	41
Podsumowanie	49
Rozdział 3. Ciąg — wykorzystywanie słabości wykrytych przez skanery	51
Metasploit	51
Podstawowe kroki związane z konfiguracją zdalnego ataku	52
Przeszukiwanie Metasploita (stara, dobra luka MS08-067)	52
Skrypty	54
Przykładowa luka w WarFTP	54
Podsumowanie	56

Rozdział 4. Rzut — samodzielne znajdowanie luk w aplikacjach webowych	57
Testy penetracyjne aplikacji webowych	57
Wstrzykiwanie kodu SQL	57
Wykonywanie skryptów między witrynami (XSS)	66
Atak CSRF	73
Tokeny sesji	76
Dodatkowe sprawdzenie danych wejściowych	78
Testy funkcjonalne i logiki biznesowej	82
Podsumowanie	83
Rozdział 5. Podanie boczne — poruszanie się po sieci	85
W sieci bez danych uwierzytelniających	85
Narzędzie Responder.py (Kali Linux)	86
Kroki do wykonania, gdy posiadamy podstawowy dostęp do domeny	89
Preferencje zasad grupy	90
Pobieranie danych uwierzytelniających zapisanych jawnym tekstem	92
Wskazówki dotyczące tego, co robić po włamaniu się do systemu	94
Kroki do wykonania, gdy posiadamy dostęp do lokalnego konta administracyjnego lub konta administratora domeny	95
Przejęcie kontroli nad siecią za pomocą poświadczeń i narzędzia PsExec	95
Atak na kontroler domeny	101
Użycie narzędzia PowerSploit po wstępnym włamaniu (Windows)	103
Polecenia	105
PowerShell po wstępnym włamaniu (Windows)	108
Zatrucie ARP	111
IPv4	111
IPv6	115
Kroki do wykonania po zatruciu ARP	117
Tworzenie proxy między hostami	123
Podsumowanie	124
Rozdział 6. Ekran — inżynieria społeczna	125
Podobieństwo domen	125
Atak wykorzystujący SMTP	125
Atak wykorzystujący SSH	127
Ataki phishingowe	128
Metasploit Pro — moduł do phishingu	128
Social-Engineer Toolkit (Kali Linux)	131
Wysyłanie dużej ilości e-maili w ramach kampanii phishingowych	134
Inżynieria społeczna i Microsoft Excel	135
Podsumowanie	138
Rozdział 7. Wykop na bok — ataki wymagające fizycznego dostępu	141
Włamywanie się do sieci bezprzewodowych	141
Atak pasywny — identyfikacja i rekonesans	142
Atak aktywny	144

SPIS TREŚCI

Atak fizyczny	152
Klonowanie kart	152
Testy penetracyjne z podrzuconej skrzynki	153
Fizyczne aspekty inżynierii społecznej	156
Podsumowanie	156
Rozdział 8. Zmyłka rozgrywającego — omijanie programów antywirusowych ...	157
Oszukiwanie skanerów antywirusowych	157
Ukrywanie WCE przed programami antywirusowymi (Windows)	157
Skrypty w języku Python	161
Podsumowanie	167
Rozdział 9. Zespoły specjalne — łamanie haseł, nietypowe luki i inne sztuczki	169
Łamanie haseł	169
Narzędzie John the Ripper (JtR)	171
Narzędzie oclHashcat	171
Poszukiwanie słabych punktów	175
Searchsploit (Kali Linux)	175
Bugtraq	176
Exploit Database	176
Odpytywanie za pomocą narzędzia Metasploit	178
Wskazówki i sztuczki	178
Skrypty RC w Metasploit	178
Ominięcie UAC	179
Ominięcie filtrowania ruchu dla swoich domen	180
Windows XP — stara sztuczka z serwerem FTP	181
Ukrywanie plików (Windows)	181
Zapewnienie ukrycia plików (Windows)	182
Przesyłanie plików do komputera w systemach Windows 7 i Windows 8	184
Rozdział 10. Analiza po grze — raportowanie	185
Raport	185
Lista moich zaleceń i sprawdzonych rozwiązań	186
Rozdział 11. Kontynuacja edukacji	189
Główne konferencje	189
Konferencje, które polecam z własnego doświadczenia	189
Kursy	190
Książki	190
Książki techniczne	191
Ciekawe książki poruszające tematykę bezpieczeństwa informatycznego	191
Frameworki dotyczące testów integracyjnych	191
Zdobywanie flagi	192

PODRĘCZNIK PENTESTERA

Bądź na bieżąco	192
Kanał RSS i strony WWW	193
Listy mailingowe	193
Listy na Twitterze	193
Dodatek A: Uwagi końcowe	195
Podziękowania	196
Skorowidz	197