

SPIS TREŚCI

Słowo wstępne	xvii
Przedmowa	xxi
Podziękowania	xxiii
Wstęp	1

CZĘŚĆ I FORMATY BINARNE

Rozdział 1 Anatomia pliku binarnego	11
Rozdział 2 Format ELF	29
Rozdział 3 Format PE: krótkie wprowadzenie	53
Rozdział 4 Tworzenie programu ładującego pliki binarne przy użyciu libbfd	63

CZĘŚĆ II PODSTAWY ANALIZY BINARNEJ

Rozdział 5 Podstawowa analiza binarna w Linuksie	85
Rozdział 6 Deasemblacja i podstawy analizy binarnej	109
Rozdział 7 Proste metody wstrzykiwania kodu dla ELF	147

CZĘŚĆ III ZAAWANSOWANA ANALIZA BINARNA

Rozdział 8 Dostosowywanie deasemblacji do potrzeb	181
Rozdział 9 Instrumentacja binarna	213
Rozdział 10 Zasady dynamicznej analizy taint	255
Rozdział 11 Praktyczna dynamiczna analiza taint z libdft	269
Rozdział 12 Podstawy wykonywania symbolicznego	297
Rozdział 13 Praktyczne wykonywanie symboliczne z Tritonem	321

CZĘŚĆ IV DODATKI

Dodatek A Błyskawiczny kurs asemblera x86	361
Dodatek B Implementacja nadpisywania PT_NOTE przyt użyciu libelf	379
Dodatek C Spis narzędzi analizy binarnej	399
Dodatek D Dalsza lektura	403
Indeks	407