

BEZPIECZEŃSTWO APLIKACJI WINDOWS

Omijanie SafeSEH, ASLR, DEP, ROP i obrona.

-K~?04□iē\$V-2g0Y;ÁR',qI>ZÉy·0 E'>0e6□00*
y·ē-0É-+.□cæbE□i?□9Ç"97□ kX>+



WINDOWS 7

WINDOWS VISTA

WINDOWS XP

BEZPIECZEŃSTWO APLIKACJI WINDOWS 7, VISTA, XP



Tytuł: Bezpieczeństwo aplikacji Windows 7, Vista, XP
ISBN: 978-83-923745-5-8

Copyright © 2012 by Wydawnictwo CSH.
All Rights Reserved.

Autorzy: Piotr Planeta (Rozdziały 1 - 4 oraz Dodatek 1)
 Bogdan Drozdowski (Dodatek 2)
Redakcja: Robert Dylewski
Prezentacja video: Michał Kowalczyk
Ścieżka audio: Jacek Zagórski

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autorzy oraz wydawnictwo CSH dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autorzy oraz wydawnictwo CSH nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce oraz na dołączonych nośnikach.

Wydawnictwo CSH
82-500 Kwidzyn
ul. Długa 27

e-mail: wydawnictwo@csh.pl
tel: 55 620 34 36 (pn-pt, 8:00-16:00)

Najnowsze informacje związane z projektem oraz pełną ofertę wydawniczą znajdziecie Państwo pod adresem <http://www.SzkolaHakerow.pl> oraz pod numerem telefonu 55 620 34 36 (od poniedziałku do piątku, w godzinach 8:00 – 16:00). Serdecznie zapraszamy!

Printed in Poland.

Spis treści

Wskazówki prawne	11
Art. 267.	11
Art. 268.	12
Art. 268a.	12
Art. 269.	12
Art. 269a.	13
Art. 269b.	13
Wstęp	15
Konwencja zapisu liczb	17
Rozdział 1. Informacje wstępne	19
Podstawowe pojęcia	19
Podstawowe informacje o budowie procesorów z rodziny IA-32	20
Tryb pracy	21
Rejestry	22
Rejestry segmentowe	23
Rejestr flag	24
Zapis instrukcji (kodowanie i dekodowanie instrukcji)	25
Rozdział 2. Podatności i ich wykorzystywanie	29
Przepełnienie bufora na stosie	29
Wykorzystywanie przepełnienia stosu	30
Wykonanie kodu użytkownika	36
Kod powłoki	38
Podsumowanie	45

Przepełnienia sterty	45
Serta procesu	46
Sterty dynamiczne	46
Obsługa sterty	46
Działanie sterty	46
Wykorzystanie przepełnień sterty	53
Podsumowanie	57
Rozdział 3. Zabezpieczenia systemu Windows	59
Zabezpieczenia stosu	61
Ciasteczka na stosie	61
Zmienianie kolejności zmiennych	65
Mechanizmy bezpiecznych bramek obsługi wyjątków	67
Zabezpieczenia sterty	70
Bezpieczne używanie struktur FreeList	70
Ciasteczka na stercie	71
Data Execution Prevention	72
Sprzętowy DEP	72
Programowy DEP	73
Konfiguracja DEP dla systemu Windows	74
Podsumowanie	75
Randomizacja rozkładu przestrzeni adresowej - ASLR	76
Sposób działania ASLR	76
Przegląd innych mechanizmów bezpieczeństwa	80
Podsumowanie	81
Rozdział 4. Polityka bezpieczeństwa	85
Zasady bezpieczeństwa dla programistów	85
Zasady bezpieczeństwa dla administratorów	88
Podsumowanie	93
Dodatek 1. Format pliku PE i analiza kodu	95
Format Portable Executable	95
Nagłówek MS-DOS	97
Nagłówek PE	97

Nagłówki sekcji (tabele sekcji)	97
Sekcje (dane sekcji)	98
Sekcja importów (tabela importów)	98
Sekcja eksportów (tabela eksportów)	100
Sekcja zasobów (katalog zasobów)	102
Inne sekcje	102
Deasemblacja	102
Debugger	105
Rezultaty analizy kodu binarnego otrzymane w wyniku działania programu PEDUMP	106
Dodatek 2. Podstawowy kurs języka assembler	111
Wstęp	111
Część 1 - Podstawy, czyli czym to się je	117
Część 2 - Pamięć, czyli gdzie upchać coś, co się nie mieści w procesorze	135
Część 3 - Podstawowe instrukcje, czyli poznajemy dialekt procesora	159
Część 4 - Pierwsze programy, czyli przełamywanie pierwszych lodów	167
Część 5 - Koprocesor, czyli jak liczyć na ułamkach	183
Część 6 - SIMD, czyli jak działa MMX	201
Część 7 - Porty, czyli łączność między procesorem a innymi urządzeniami	213
Część 8 - Operacje na bitach, czyli to, w czym assembler błyszczyc najbardziej	219
Część 9 - Pętle i warunki, czyli o tym, jak używać bloków kontrolnych	231
Część 10 - Nie jesteśmy sami, czyli jak łączyć assemblera z innymi językami	241
Bibliografia	247

Zamów pozostałe publikacje

■ Szkoła Hakerów Edycja 2.0



Bestseller Wydawnictwa CSH. Szkolenie poruszające najważniejsze aspekty bezpieczeństwa IT. Przedstawia zarówno metody ataku, jak i obrony.

Kompleksowe szkolenie, które składa się z poręcznika, filmów instruktażowych oraz szkoleniowego systemu operacyjnego.

■ Intensywne Wprowadzenie do Hackingu



Intensywny kurs składający się z 11 godzin wykładów nagranych w jakości HD na 5 płytach DVD oraz podręcznika zawierającego 532 strony wiedzy.

Szkolenie skierowane w szczególności do osób, które rozpoczynają swoją przygodę z hackingiem.

Dowiedz się więcej na stronie internetowej:

www.SzkolaHakerow.pl

Skorzystaj z **10% RABATU** dla aktualnych uczestników.

Wpisz w formularzu zamówienia kod promocyjny: **678900**

i skorzystaj z rabatu!

■ Raport Specjalny #1 Ataki na Sieci Bezprzewodowe



Poznaj metody zabezpieczeń w sieciach bezprzewodowych i dowiedz się jakie są wady dzisiejszych rozwiązań (WEP, WPA, WPA2). Zaledwie 3 minuty - tylko tyle potrzebuje atakujący, aby uzyskać dostęp do nieprawidłowo zabezpieczonej sieci Wi-Fi.

■ Metody Inwigilacji i Elementy Informatyki Śledczej



Szkolenie porusza zagadnienia informatyki śledczej - m.in. pozyskiwanie śladów, ukrywanie danych. Omawia problemy takie jak: inwigilacja, lokalizacja IP, szyfrowanie, keyloggery, odzyskiwanie haseł i wiele innych zagadnień z dziedziny Computer Forensics oraz Data Recovery.

**Jesteśmy do Twojej dyspozycji - zadzwoń:
tel. 55 620 34 36 (pn-pt, 8-16)**

Skorzystaj z **10% RABATU** dla aktualnych uczestników.

Wpisz w formularzu zamówienia kod promocyjny: **678900**