Przedmowa (7)
0x100 Wprowadzenie (9)
0x200 Programowanie (15)

- 0x210 Istota programowania (16)
- 0x220 Nadużywanie programów (19)
- 0x230 Uogólnione techniki nadużyć (22)
- 0x240 Uprawnienia dostępu do plików w środowiskach wieloużytkownikowych (23)
- 0x250 Pamięć (25)
    - 0x251 Deklaracja pamięci (26)
    - 0x252 Zakończenie bajtem NULL (26)
    - 0x253 Podział na segmenty pamięci programu (27)
- 0x260 Przepełnienia bufora (31)
- 0x270 Przepełnienia stosowe (32)
    - 0x271 Wykorzystywanie kodu nadużycia (37)
    - 0x272 Wykorzystanie środowiska (40)
- 0x280 Przepełnienia w przypadku segmentów heap oraz bss (49)
    - 0x281 Podstawowe przepełnienie stertowe (49)
    - 0x282 Przepełnienia wskaźników funkcyjnych (54)
- 0x290 Ciągi formatujące (61)
    - 0x291 Ciągi formatujące i instrukcja printf() (61)
    - 0x292 Podatność ciągów formatujących na ataki (66)
    - 0x293 Odczyt spod dowolnych adresów pamięci (68)
    - 0x294 Zapis pod dowolnymi adresami pamięci (69)
    - 0x295 Bezpośredni dostęp do parametrów (76)
    - 0x296 Obejścia z użyciem sekcji dtors (79)
    - 0x297 Nadpisywanie globalnej tabeli przesunięć (85)
- 0x2a0 Pisanie kodu powłoki (88)
    - 0x2a1 Podstawowe instrukcje asemblera (89)
    - 0x2a2 Wywołania systemowe Linuksa (90)
    - 0x2a3 Hello, world! (91)
    - 0x2a4 Kod wywołania powłoki (94)
    - 0x2a5 Unikanie wykorzystywania innych segmentów (96)
    - 0x2a6 Usuwanie bajtów zerowych (98)
    - 0x2a7 Dalsze zmniejszenie objętości kodu powłoki poprzez wykorzystanie stosu (102)
    - 0x2a8 Instrukcje w postaci drukowalnych znaków ASCII (106)
    - 0x2a9 Polimorficzny kod powłoki (107)
    - 0x2aa Polimorficzny kod powłoki z drukowalnymi znakami ASCII (107)
    - 0x2ab Dissembler (121)
- 0x2b0 Powracanie do funkcji biblioteki libc (131)
    - 0x2b1 Powrót do funkcji system() (132)
    - 0x2b2 Wiązanie wywołań powrotnych do biblioteki libc (134)
    - 0x2b3 Użycie programu opakowującego (135)
    - 0x2b4 Zapisywanie bajtów zerowych z powróceniem do biblioteki libc (137)
    - 0x2b5 Zapis wielu słów w ramach pojedynczego wywołania (139)

0x300 Sieci (143)

- 0x310 Czym są sieci? (143)

    - 0x311 Model OSI (144)
- 0x320 Szczegółowe przedstawienie niektórych warstw OSI (145)
    - 0x321 Warstwa sieci (146)
    - 0x322 Warstwa transportowa (147)
    - 0x323 Warstwa łącza danych (149)
- 0x330 Podsłuchiwanie w sieci (150)
    - 0x331 Aktywne podsłuchiwanie (153)
- 0x340 Przejęcie TCP/IP (159)
    - 0x341 Rozłączanie przy pomocy RST (160)
- 0x350 Odmowa usługi (163)
    - 0x351 Atak Ping of Death (164)
    - 0x352 Atak Teardrop (164)
    - 0x353 Zalew pakietów ping (Ping Flooding) (164)
    - 0x354 Atak ze wzmocnieniem (Amplification) (164)
    - 0x355 Rozproszony atak DoS (165)
    - 0x356 Zalew pakietów SYN (SYN Flooding) (165)
- 0x360 Skanowanie portów (166)
    - 0x361 Ukryte skanowanie SYN (166)
    - 0x362 Skanowanie FIN, X-mas i Null (167)
    - 0x363 Skanowanie z ukrycia (167)
    - 0x364 Skanowanie z użyciem bezczynnego komputera (167)
    - 0x365 Aktywne zabezpieczenie (Shroud) (169)

0x400 Kryptologia (177)

- 0x410 Teoria informacji (178)
    - 0x411 Bezwarunkowe bezpieczeństwo (178)
    - 0x412 Szyfr z kluczem jednorazowym (178)
    - 0x413 Kwantowa dystrybucja kluczy (179)
    - 0x414 Bezpieczeństwo obliczeniowe (180)
- 0x420 Rozległość algorytmów (180)
    - 0x421 Notacja asymptotyczna (182)
- 0x430 Szyfrowanie symetryczne (182)
    - 0x431 Kwantowy algorytm przeszukiwania (183)
- 0x440 Szyfrowanie asymetryczne (184)
    - 0x441 RSA (184)
    - 0x442 Kwantowy algorytm rozkładu na czynniki (189)
- 0x450 Szyfry hybrydowe (190)
    - 0x451 Ataki z ukrytym pośrednikiem (191)
    - 0x452 "Odciski palców" komputerów w protokole SSH (193)
    - 0x453 Rozmyte "odciski palców" (196)
- 0x460 Łamanie haseł (201)
    - 0x461 Ataki słownikowe (202)
    - 0x462 Ataki na zasadzie pełnego przeglądu (203)
    - 0x463 Tablica wyszukiwania skrótów (205)
    - 0x464 Macierz prawdopodobieństwa haseł (205)
- 0x470 Szyfrowanie w sieci bezprzewodowej 802.11b (215)
    - 0x471 Protokół Wired Equivalent Privacy (WEP) (215)
    - 0x472 Szyfr strumieniowy RC4 (217)
- 0x480 Ataki na WEP (218)

    - 0x481 Ataki na zasadzie pełnego przeglądu w trybie offline (218)
    - 0x482 Ponowne użycie strumienia klucza (218)
    - 0x483 Tablice słownikowe z wektorami IV (220)
    - 0x484 Przekierowanie IP (220)
    - 0x485 Atak Fluhrera, Mantina i Shamira (FMS) (222)

0x500 Podsumowanie (231)

- Bibliografia i dodatkowe informacje (232)

Skorowidz (235)