

Przedmowa (7)

Część I Modyfikowanie i eksplorowanie narzędzi bezpieczeństwa (13)

1. Pisanie dodatków dla programu Nessus (15)

- Architektura Nessusa (15)
- Instalowanie Nessusa (16)
- Korzystanie z programu Nessus (17)
- Interpreter języka NASL (21)
- Przykład "Hello World" (22)
- Typy danych i zmienne (22)
- Operatory (25)
- Instrukcja if...else (26)
- Pętle (27)
- Funkcje (28)
- Predefiniowane zmienne globalne (29)
- Najważniejsze funkcje języka NASL (31)
- Dodatki Nessusa (37)

2. Programowanie narzędzi sekcjonujących i dodatków dla szperacza sieciowego Ettercap (53)

- Instalacja i korzystanie z programu Ettercap (53)
- Pisanie narzędzia sekcjonującego dla Ettercapa (54)
- Pisanie dodatków dla programu Ettercap (61)

3. Poszerzanie możliwości programów Hydra i Nmap (67)

- Rozszerzanie możliwości programu Hydra (67)
- Dodawanie nowych sygnatur do programu Nmap (81)

4. Pisanie dodatków dla skanera luk Nikto (85)

- Instalowanie programu Nikto (85)
- Jak korzystać z programu Nikto? (86)
- Jak działa program Nikto? (88)
- Istniejące dodatki programu Nikto (89)
- Dodawanie własnych pozycji do baz dodatków (91)
- Korzystanie z biblioteki LibWhisker (94)
- Piszemy dodatek NTLM łamiący hasła metodą brutalnej siły (96)
- Pisanie samodzielnego dodatku atakującego serwer Lotus Domino (99)

5. Pisanie modułów dla oprogramowania Metasploit Framework (103)

- Wprowadzenie do MSF (103)
- Zasada ataków polegających na przepełnieniu bufora stosu (104)
- Pisanie ataków testowych pod MSF (113)
- Moduł ataku przepełnienia bufora przeciw wyszukiwarce MnoGoSearch (117)
- Pisanie pod MSF modułu badającego sygnaturę systemu operacyjnego (125)

6. Rozszerzanie analizy kodu na aplikacje WWW (131)

- Atakowanie aplikacji WWW z wykorzystaniem błędów w kodzie źródłowym (131)
- Toolkit 101 (136)
- PMD (139)
- Rozszerzanie możliwości narzędzia PMD (141)

Część II Pisanie narzędzi do kontroli bezpieczeństwa sieci (165)

7. Zabawa z modułami jądra Linuksa (167)

- Witaj, świecie! (167)
- Przechwytywanie funkcji systemowych (169)
- Ukrywanie procesów (177)
- Ukrywanie połączeń przed narzędziem netstat (181)

8. Tworzenie narzędzi i skryptów do badania serwisów WWW (185)

- Środowisko aplikacji WWW (185)
- Projekt skanera (189)
- Analizator składni pliku dziennika (194)
- Piszemy skaner (196)
- Praca ze skanerem (210)
- Pełny kod źródłowy (210)

9. Automatyczne narzędzia exploitów (217)

- Exploity wstrzykiwania kodu SQL (217)
- Skaner exploitów (219)
- Praca ze skanerem (243)

10. Pisanie szperaczy sieciowych (245)

- Biblioteka libpcap - wprowadzenie (245)
- Zaczynamy pracę z libpcap (247)
- libpcap i sieci bezprzewodowe 802.11 (260)
- libpcap i Perl (268)
- Leksykon funkcji biblioteki libpcap (269)

11. Narzędzia do wstrzykiwania pakietów (279)

- Biblioteka libnet (279)
- Początek pracy z biblioteką libnet (280)
- Zaawansowane funkcje biblioteki libnet (287)
- Jednoczesne wykorzystanie libnet i libpcap (289)
- AirJack - wprowadzenie (296)

Skorowidz (303)