

Podziękowania (11)

Współautorzy (13)

Słowo wstępne, wersja 1.5 (17)

Słowo wstępne, wersja 1.0 (21)

Rozdział 1. Włamywacz - któż to taki? (23)

- Wprowadzenie (23)
- Co rozumiemy pod pojęciem "włamania"? (23)
 - Jaki jest cel włamywania? (24)
- Czego należy się spodziewać po zawartości tej książki? (25)
- Klimat i uwarunkowania prawne towarzyszące działalności hakerów (27)
- Podsumowanie (29)
- Najczęściej zadawane pytania (FAQ) (29)

Rozdział 2. Reguły bezpieczeństwa (31)

- Wprowadzenie (31)
- Znaczenie znajomości zasad bezpieczeństwa (32)
- Zabezpieczenia po stronie klienta są nieskuteczne (33)
- Strony komunikacji nie mogą bezpiecznie wymieniać kluczy kryptograficznych bez dostępu do pewnej wspólnej informacji (34)
- Nie można całkowicie zabezpieczyć się przed szkodliwym kodem (37)
- Każdy szkodliwy kod może zostać przekształcony w celu uniemożliwienia jego detekcji na podstawie sygnatury (39)
- Zapory sieciowe nie stanowią pełnego zabezpieczenia przed atakami (41)
 - Inżynieria społeczna (43)
 - Ataki na serwery publiczne (43)
 - Bezpośredni atak na zaporę sieciową (44)
 - Luki po stronie klienta (45)
- Każdy system wykrywania włamań (IDS) może zostać oszukany (45)
- Tajne algorytmy kryptograficzne nie są bezpieczne (47)
- Szyfrowanie bez klucza nie jest szyfrowaniem - jest kodowaniem (49)
- Hasła przechowywane po stronie klienta nie są bezpieczne, chyba że chroni je inne hasło (50)
- System aspirujący do miana bezpiecznego musi być poddany niezależnemu audytowi bezpieczeństwa (53)
- Zabezpieczanie przez ukrywanie jest nieskuteczne (55)
- Podsumowanie (56)
- Zagadnienia w skrócie (57)
- Najczęściej zadawane pytania (FAQ) (59)

Rozdział 3. Klasy ataków (61)

- Wprowadzenie (61)
- Klasyfikacja ataków (61)
 - Odmowa obsługi (62)
 - Wyciek informacji (70)
 - Dostęp do systemu plików (75)
 - Dezinformacja (77)
 - Dostęp do plików specjalnych i baz danych (81)

- Zdalne uruchomienie kodu (84)
 - Rozszerzanie uprawnień (86)
- Metody testowania systemów pod kątem luk w zabezpieczeniach (88)
 - Dowód istnienia luki (88)
 - Standardowe techniki analizy (92)
- Podsumowanie (100)
- Zagadnienia w skrócie (102)
- Najczęściej zadawane pytania (FAQ) (103)

Rozdział 4. Metodologia (105)

- Wprowadzenie (105)
- Metodologie analizy luk w zabezpieczeniach (106)
 - Analiza kodu źródłowego (106)
 - Analiza kodu binarnego (109)
- Znaczenie przeglądu kodu źródłowego (110)
 - Wyszukiwanie niebezpiecznych funkcji (110)
- Techniki inżynierii wstecznej (116)
 - Deasemblerzy, dekompiletory, debuggery (121)
- Czarne skrzynki (125)
 - Układy elektroniczne (126)
- Podsumowanie (127)
- Zagadnienia w skrócie (128)
- Najczęściej zadawane pytania (FAQ) (129)

Rozdział 5. Różnicowanie (131)

- Wprowadzenie (131)
- Na czym polega różnicowanie? (131)
 - Po co porównywać? (134)
 - Zagląwanie w kod źródłowy (135)
- Narzędzia automatyzujące porównywanie plików (140)
 - Narzędzia porównujące pliki (141)
 - Edytory szesnastkowe (143)
 - Narzędzia monitorujące system plików (146)
 - W poszukiwaniu innych narzędzi (151)
- Utrudnienia (152)
 - Sumy kontrolne i skróty (153)
 - Kompresja i szyfrowanie (154)
- Podsumowanie (155)
- Zagadnienia w skrócie (156)
- Najczęściej zadawane pytania (FAQ) (157)

Rozdział 6. Kryptografia (159)

- Wprowadzenie (159)
- Podstawy kryptografii (160)
 - Historia (160)
 - Rodzaje kluczy szyfrujących (160)
- Standardowe algorytmy kryptograficzne (162)

- Algorytmy symetryczne (162)
 - Algorytmy asymetryczne (166)
- Metoda pełnego przeglądu (168)
 - Pełny przegląd - podstawy (169)
 - Wykorzystanie metody pełnego przeglądu do odgadywania haseł (170)
- Niewłaściwe zastosowanie poprawnych algorytmów (173)
 - Niepoprawna wymiana kluczy (174)
 - Generowanie skrótów z fragmentów informacji (175)
 - Korzystanie z krótkich haseł do generowania długich kluczy (176)
 - Nieprawidłowe przechowywanie kluczy tajnych i prywatnych (176)
- Amatorskie próby kryptograficzne (178)
 - Klasyfikacja szyfrogramu (178)
 - Szyfry monoalfabetyczne (180)
 - Inne sposoby ukrywania informacji (181)
- Podsumowanie (186)
- Zagadnienia w skrócie (187)
- Najczęściej zadawane pytania (FAQ) (188)

Rozdział 7. Nieoczekiwane dane wejściowe (191)

- Wprowadzenie (191)
- Dlaczego nieoczekiwane dane wejściowe stanowią zagrożenie (192)
- Identyfikacja sytuacji zagrożonych nieoczekiwanymi danymi (193)
 - Aplikacje i narzędzia lokalne (193)
 - HTTP i HTML (193)
 - Nieoczekiwane dane w zapytaniach SQL (196)
 - Uwierzytelnianie aplikacji (199)
 - Kamuflaż (203)
- Techniki wyszukiwania i eliminacji luk (205)
 - Testowanie metodą czarnej skrzynki (205)
 - Korzystanie ze źródeł (209)
 - Filtracja - odkażanie danych (210)
 - Oznaczanie znaków specjalnych nie zawsze wystarcza (210)
 - Perl (211)
 - Cold Fusion (Cold Fusion Markup Language) (212)
 - ASP (212)
 - PHP (213)
 - Ochrona zapytań SQL (213)
 - Usuwać po cichu czy informować o błędnych danych? (214)
 - Funkcja obsługi niepoprawnych danych (215)
 - Zastępowanie żetonami (215)
- Korzystanie z zabezpieczeń oferowanych przez języki programowania (216)
 - Perl (216)
 - PHP (217)
 - ColdFusion (Cold Fusion Markup Language) (218)
 - ASP (218)
 - MySQL (219)
- Narzędzia związane z nieoczekiwanymi danymi wejściowymi (219)
 - Web Sleuth (219)
 - CGIAudit (219)

- RATS (220)
- Flawfinder (220)
- Retina (220)
- Hailstorm (220)
- Pudding (220)
- Podsumowanie (221)
- Zagadnienia w skrócie (221)
- Najczęściej zadawane pytania (FAQ) (223)

Rozdział 8. Przepelnienie bufora (225)

- Wprowadzenie (225)
- Działanie stosu (225)
 - Obraz stosu (229)
 - Osobliwości stosu (229)
- Ramka stosu (230)
 - Wprowadzenie do ramki stosu (230)
 - Przykładowy program: przekazywanie parametrów do funkcji (231)
 - Ramki stosu i konwencje wywołania funkcji (235)
- Podstawowe techniki przepelnienia bufora (236)
 - Przykładowy program: niekontrolowane przepelnienie bufora (237)
- Pierwsze samodzielne przepelnienie bufora (241)
 - Utworzenie programu podatnego na atak wykorzystujący przepelnienie bufora (241)
 - Atak (244)
- Przepelnienie bufora - techniki zaawansowane (271)
 - Filtrowanie danych wejściowych (272)
 - Nadpisanie wskaźnika funkcji przechowywanego na stosie (274)
 - Przepelnienia sterty (275)
- Konstruowanie ładunku - zagadnienia zaawansowane (278)
 - Korzystać z posiadanego (278)
- Podsumowanie (281)
- Zagadnienia w skrócie (282)
- Najczęściej zadawane pytania (FAQ) (284)

Rozdział 9. Ciągi formatujące (287)

- Wprowadzenie (287)
- Istota błędów ciągów formatujących (289)
 - Gdzie i dlaczego występują błędy ciągów formatujących? (292)
 - Jak wyeliminować te błędy? (294)
 - W jaki sposób ciągi formatujące są wykorzystywane przez włamywaczy? (294)
 - Przebieg ataków z użyciem ciągów formatujących (298)
 - Co nadpisywać (301)
- Analiza podatnego programu (302)
- Testowanie wykorzystujące przypadkowe ciągi formatujące (305)
- Atak z użyciem ciągu formatującego (308)
- Podsumowanie (316)
- Zagadnienia w skrócie (317)

- Najczęściej zadawane pytania (FAQ) (318)

Rozdział 10. Monitorowanie komunikacji (sniffing) (321)

- Wprowadzenie (321)
- Istota monitorowania (322)
 - Sposób działania (322)
- Przedmiot monitorowania (323)
 - Zdobywanie danych uwierzytelniających (323)
 - Przechwytywanie innych danych ruchu w sieci (328)
- Popularne programy służące do monitorowania (329)
 - Ethereal (329)
 - Network Associates Sniffer Pro (330)
 - NT Network Monitor (332)
 - WildPackets (333)
 - TCPDump (334)
 - dsniff (334)
 - Ettercap (337)
 - Esniff.c (337)
 - Sniffit (337)
 - Carnivore (339)
 - Dodatkowe zasoby (341)
- Zaawansowane techniki monitorowania (341)
 - Ataki typu man-in-the-middle (MITM) (341)
 - Łamanie (342)
 - Sztuczki związane z przełącznikami (342)
 - Zmiany wyboru tras (343)
- Interfejsy API systemów operacyjnych (344)
 - Linux (344)
 - BSD (346)
 - libpcap (346)
 - Windows (348)
- Ochronne środki zaradcze (349)
 - Zapewnianie szyfrowania (349)
 - Secure Sockets Layers (SSL) (350)
 - PGP and S/MIME (351)
 - Przełączanie (351)
- Stosowanie technik wykrywania (351)
 - Wykrywanie lokalne (351)
 - Wykrywanie sieciowe (352)
- Podsumowanie (354)
- Zagadnienia w skrócie (355)
- Najczęściej zadawane pytania (FAQ) (357)

Rozdział 11. Przejmowanie sesji (359)

- Wprowadzenie (359)
- Istota przejmowania sesji (359)
 - Przejmowanie sesji TCP (361)
 - Przejmowanie sesji TCP z blokowaniem pakietów (362)

- Przejmowanie datagramów UDP (365)
- Przegląd dostępnych narzędzi (366)
 - Juggernaut (367)
 - Hunt (370)
 - Ettercap (373)
 - SMBRelay (378)
 - Programy nadzoru zakłóceń (378)
- Ataki typu MITM w przypadku komunikacji szyfrowanej (381)
 - Ataki typu man-in-the-middle (382)
 - Dsniff (383)
 - Inne formy przejmowania (383)
- Podsumowanie (385)
- Zagadnienia w skrócie (385)
- Najczęściej zadawane pytania (387)

Rozdział 12. Podrabianie (spoofing): ataki na wiarygodną tożsamość (389)

- Wprowadzenie (389)
- Istota podrabiania (389)
 - Podrabianie jako fałszowanie tożsamości (390)
 - Podrabianie jako atak aktywny (390)
 - Możliwość podrabiania na poziomie wszystkich warstw komunikacji (390)
 - Podrabianie jako atak zawsze zamierzony (391)
 - Różnice pomiędzy podrabianiem a zdradą (393)
 - Podrabianie jako nie zawsze szkodliwe działanie (393)
 - Podrabianie jako nienowa idea (394)
- Rys teoretyczny (394)
 - Znaczenie tożsamości (395)
- Ewolucja zaufania (396)
 - Asymetryczne podpisy wśród ludzi (396)
- Określanie tożsamości w sieciach komputerowych (398)
 - Powrót do nadawcy (399)
 - Na początku była... transmisja (400)
- Wezwania do przedstawienia uprawnień (400)
 - Metodologie konfiguracji: tworzenie indeksu zaufanych uprawnień (413)
- Podrabianie w przypadku maszyn stacjonarnych (415)
 - Plaga aplikacji wykonujących automatyczne aktualizacje (415)
- Wpływ ataków podrabiania (417)
 - Wyrafinowane metody podrabiania i sabotaż ekonomiczny (418)
- "Bрудna robota" - planowanie systemów podrabiania (428)
 - Tworzenie routera szkieletowego w obszarze użytkowników (428)
 - Fałszowanie łączności poprzez asymetryczne zapory sieciowe (447)
- Podsumowanie (454)
- Zagadnienia w skrócie (456)
- Najczęściej zadawane pytania (459)

Rozdział 13. Tunelowanie (463)

- Wprowadzenie (463)
- Strategiczne ograniczenia projektów tuneli (465)

- Poufność: dokąd zmierzają moje dane? (467)
- Możliwość routowania: którędy mogą przejść dane? (467)
- Możliwość wdrożenia: jak trudno wszystko zbudować i uruchomić? (468)
- Elastyczność: w jakim celu można system wykorzystać? (469)
- Jakość: jak kłopotliwe będzie utrzymywanie systemu w ruchu? (471)
- Projektowanie całościowych systemów tunelowania (472)
 - "Drażnienie" tuneli za pomocą SSH (473)
- Uwierzytelnianie (477)
 - Dostęp podstawowy: uwierzytelnianie przez hasło (477)
 - Dostęp przezroczysty: uwierzytelnianie za pomocą klucza prywatnego (478)
- Przekazywanie poleceń: bezpośrednie wykonywanie skryptów i używanie potoków (483)
- Przekazywanie portów: dostęp do zasobów odległych sieci (488)
 - Lokalne przekazywanie portów (488)
 - Dynamiczne przekazywanie portów (490)
 - Zdalne przekazywanie portów (498)
- Przechodzenie przez oporną sieć (500)
 - Dostęp do serwerów pośredniczących przez ProxyCommands (500)
 - Zamienianie swojego ruchu (503)
 - Ograniczone uwierzytelnianie wobec ufortyfikowanej stacji bazowej (504)
 - Eksportowanie dostępu SSHD (506)
 - Wzajemne łączenie maszyn umieszczonych za zaporami sieciowymi (508)
- Dalsze działania (510)
 - Standardowy transfer plików przez SSH (510)
 - Przyrostowy transfer plików przez SSH (512)
 - Wypalanie płyt CD przez SSH (514)
 - Przesyłanie danych audio przez TCP i SSH (516)
- Podsumowanie (520)
- Zagadnienia w skrócie (522)
- Najczęściej zadawane pytania (527)

Rozdział 14. Włamania sprzętowe (529)

- Wprowadzenie (529)
- Istota włamań sprzętowych (530)
- Otwieranie urządzenia: ataki na obudowę i mechaniczne (530)
 - Rodzaje mechanizmów zabezpieczających (532)
 - Interfejsy zewnętrzne (537)
 - Analiza protokołów (538)
 - Zakłócenia elektromagnetyczne i wyładowania elektrostatyczne (540)
- Analiza wewnętrznej budowy produktu: ataki na obwody elektryczne (541)
 - Inżynieria wsteczna urządzenia (541)
 - Podstawowe techniki: typowe formy ataku (542)
 - Techniki zaawansowane: usuwanie warstwy żywicy epoksydowej oraz rozmywanie obudowy układu scalonego (546)
 - Kryptoanaliza i metody zaciemniania (548)
- Potrzebne narzędzia (550)
 - Zestaw początkowy (550)
 - Zestaw zaawansowany (551)
- Przykład: włamanie do nośnika danych uwierzytelniających iButton (553)

- Eksperymentowanie z urządzeniem (553)
 - Inżynieria wsteczna odpowiedzi "losowej" (554)
- Przykład: włamanie do akceleratora E-commerce NetStructure 7110 Accelerator (556)
 - Otwarcie urządzenia (557)
 - Pobranie systemu plików (557)
 - Inżynieria wsteczna generatora haseł (560)
- Podsumowanie (561)
- Zagadnienia w skrócie (562)
- Najczęściej zadawane pytania (FAQ) (564)

Rozdział 15. Wirusy, robaki i konie trojańskie (567)

- Wprowadzenie (567)
- Różnice pomiędzy wirusami, robakami oraz końmi trojańskimi (567)
 - Wirusy (568)
 - Robaki (569)
 - Makrowirusy (569)
 - Konie trojańskie (570)
 - Żarty (571)
- Anatomia wirusa (571)
 - Propagacja (572)
 - Treść zasadnicza (573)
 - Inne wybiegi (574)
- Kwestie wieloplatformowości (575)
 - Java (575)
 - Makrowirusy (576)
 - Rekompilacja (576)
 - Shockwave Flash (576)
- Fakty, którymi należy się martwić (576)
 - Robak Morris (577)
 - ADMw0rm (577)
 - Melissa oraz I Love You (577)
 - Robak Sadmin (582)
 - Robaki Code Red (583)
 - Robak Nimda (584)
- Tworzenie własnego złośliwego kodu (586)
 - Nowe metody dostarczania (586)
 - Metody szybszej propagacji (587)
 - Inne przemyślenia na temat tworzenia nowych odmian złośliwego kodu (588)
- Sposoby zabezpieczeń przed złośliwym oprogramowaniem (589)
 - Oprogramowanie antywirusowe (589)
 - Uaktualnienia i programy korygujące (590)
 - Bezpieczeństwo przeglądarki internetowej (591)
 - Badania antywirusowe (591)
- Podsumowanie (592)
- Zagadnienia w skrócie (592)
- Najczęściej zadawane pytania (FAQ) (594)

Rozdział 16. Pokonywanie systemów wykrywania włamań (595)

- Wprowadzenie (595)
- Istota działania systemów wykrywania włamań opartych na sygnaturach (595)
 - Określanie wyników fałszywie pozytywnych i negatywnych (598)
 - Przeciążanie alarmami (598)
- Wykorzystanie metod pokonywania na poziomie pakietów (599)
 - Opcje nagłówka IP (601)
 - Fragmentacja pakietu IP (601)
 - Nagłówek TCP (603)
 - Synchronizacja TCP (604)
 - Wykorzystanie pakietów Fragrouter oraz Congestant (606)
 - Środki zaradcze (608)
- Wykorzystanie metod pokonywania w protokołach warstwy aplikacji (609)
 - Bezpieczeństwo jako refleksja (609)
 - Unikanie dopasowania (610)
 - Techniki ataku z poziomu sieci WWW (611)
 - Środki zaradcze (612)
- Wykorzystanie metod pokonywania poprzez morfingu kodu (612)
- Podsumowanie (615)
- Zagadnienia w skrócie (616)
- Najczęściej zadawane pytania (FAQ) (617)

Rozdział 17. Zautomatyzowane badanie systemów zabezpieczeń oraz narzędzia ataku (619)

- Wprowadzenie (619)
- Podstawowe wiadomości na temat narzędzi zautomatyzowanych (620)
 - Narzędzia komercyjne (623)
 - Narzędzia darmowe (628)
- Wykorzystanie narzędzi zautomatyzowanych do celów testowania penetracyjnego (631)
 - Testowanie za pomocą narzędzi komercyjnych (632)
 - Testowanie za pomocą narzędzi darmowych (635)
- Kiedy narzędzia nie wystarczą (638)
 - Nowe oblicze testowania luk systemów zabezpieczeń (639)
- Podsumowanie (640)
- Zagadnienia w skrócie (641)
- Najczęściej zadawane pytania (FAQ) (642)

Rozdział 18. Raportowanie o problemach związanych z bezpieczeństwem (643)

- Wprowadzenie (643)
- Zasadność raportowania o problemach związanych z bezpieczeństwem (644)
 - Ujawnienie zupełne (645)
- Określanie terminu przesłania oraz adresata raportu o problemie (648)
 - Określanie adresata raportów o problemach (648)
- Określanie szczegółowości przekazywanych informacji (651)
 - Publikowanie kodu wykorzystującego lukę (652)
 - Problemy (653)
- Podsumowanie (655)
- Zagadnienia w skrócie (656)

- Najczęściej zadawane pytania (FAQ) (657)

Skorowidz (661)