

O autorze (13)

Przedmowa (15)

Wprowadzenie (17)

Rozdział 1. Czynniki wpływające na obniżenie bezpieczeństwa sieci (29)

- Typowy poranek (29)
- Dlaczego bezpieczeństwo sieciowe jest istotne? (31)
- Czynniki wpływające na obniżenie bezpieczeństwa sieci (32)
- Zarządzanie i procedury (32)
 - o Zarządzanie i nieprzekraczalne terminy (32)
 - o Sprzedaż załadowanego pistoletu (33)
 - o Dwuminutowa zmiana (34)
 - o Środowisko projektowe a środowisko pracy (34)
 - o Zdarzeniowa koncepcja utrzymania bezpieczeństwa sieci (35)
- Błędy techniczne w zabezpieczeniach sieciowych (36)
 - o Mamy serwer w strefie zdemilitaryzowanej (36)
 - o Mamy firewalla (37)
 - o Mamy sieciowy system wykrywania włamań (38)
 - o Mamy jednostkowy system wykrywania włamań (39)
 - o Wykorzystujemy protokół SSL (39)
- Podsumowanie (40)

Rozdział 2. Raporty CIS dotyczące serwera Apache (41)

- Raporty CIS dotyczące serwera Apache dla systemu Unix - zagadnienia związane z systemem operacyjnym (41)
 - o Zabezpieczenie usług innych niż HTTP (41)
 - o Przykład ataku na usługę - wykorzystanie serwera FTP (7350wu) (46)
 - o Wpływ błędów w usługach na bezpieczeństwo serwera Apache (49)
 - o Uaktualnienia dostawców systemów operacyjnych (49)
 - o Dostosowanie stosu IP (50)
 - o Odmowa obsługi (51)
 - o Grupy i konta użytkowników sieciowych (53)
 - o Zablokowanie konta serwera WWW (56)
 - o Wprowadzenie limitów dyskowych (57)
 - o Dostęp do poleceń systemowych (59)
 - o Zmiana właściciela i praw dostępu do poleceń systemu (64)
 - o Tradycyjny mechanizm chroot (65)
 - o Wady mechanizmu chroot (65)
 - o Moduł chroot mod_security (66)
 - o Konfiguracja mechanizmu chroot (66)
- Podsumowanie (73)

Rozdział 3. Instalacja serwera Apache (75)

- Wybór wersji (75)
- Pakiety binarne czy kod źródłowy? (76)
- Pobranie kodu źródłowego (78)
 - o Czy potrzebna jest weryfikacja MD5 i PGP? (78)
- Rozpakowanie archiwum (84)

- o Nakładki (85)
 - o Śledzenie komunikatów o błędach i nakładkach (86)
 - o Które moduły uwzględnić? (89)
- Podsumowanie (98)

Rozdział 4. Konfiguracja - plik httpd.conf (99)

- Ustawienia uwzględnione w raporcie CIS (102)
- Plik httpd.conf (102)
- Wyłączenie niepotrzebnych modułów (103)
- Dyrektywy (104)
- Dyrektywy związane z serwerem (105)
 - o Moduły pracy wieloprocessorowej (MPM) (105)
 - o Dyrektywa Listen (105)
 - o Dyrektywa ServerName (106)
 - o Dyrektywa ServerRoot (106)
 - o Dyrektywa DocumentRoot (106)
 - o Dyrektywa HostnameLookups (106)
- Dyrektywy związane z kontami użytkowników (108)
 - o Dyrektywa User (108)
 - o Dyrektywa Group (109)
 - o Dyrektywa ServerAdmin (109)
- Dyrektywy związane z ochroną przed atakami DoS (109)
 - o Test domyślnej konfiguracji (110)
 - o Dyrektywa Timeout (111)
 - o Dyrektywa KeepAlive (112)
 - o Dyrektywa KeepAliveTimeout (112)
 - o Dyrektywa MaxKeepAliveRequests (112)
 - o Dyrektywa StartServers (113)
 - o Dyrektywy MinSpareServers i MaxSpareServers (113)
 - o Dyrektywa ListenBacklog (113)
 - o Dyrektywy MaxClients i ServerLimit (114)
 - o Test serwera po zamianie konfiguracji (114)
 - o Zapowiedź (115)
- Dyrektywy utajniające oprogramowanie (116)
 - o Dyrektywa ServerTokens (116)
 - o Dyrektywa ServerSignature (117)
 - o Dyrektywa ErrorDocument (117)
- Dyrektywy katalogów (121)
 - o Parametr All (121)
 - o Parametr ExecCGI (121)
 - o Parametry FollowSymLinks i SymLinksIfOwnerMatch (121)
 - o Parametry Includes i IncludesNoExec (122)
 - o Parametr Indexes (122)
 - o Dyrektywa AllowOverride (123)
 - o Parametr Multiviews (123)
- Dyrektywy kontroli dostępu (123)
- Uwierzytelnianie (124)
- Autoryzacja (125)
 - o Dyrektywa Order (126)

- Kontrola dostępu - informacje o kliencie (127)
 - o Nazwa komputera lub domeny (127)
 - o Adres IP lub zakres adresów IP (128)
 - o Zmienne środowiskowe żądania (128)
 - o Ochrona katalogu głównego (128)
- Zmniejszenie liczby metod HTTP (129)
- Ogólne dyrektywy rejestracji zdarzeń (130)
 - o Dyrektywa LogLevel (130)
 - o Dyrektywa ErrorLog (130)
 - o Dyrektywa LogFormat (131)
 - o Dyrektywa CustomLog (131)
- Usunięcie domyślnych i przykładowych plików (132)
 - o Pliki kodu źródłowego Apache (132)
 - o Domyślne pliki HTML (132)
 - o Przykładowe skrypty CGI (133)
 - o Pliki użytkownika webserv (134)
- Zmiana praw dostępu (134)
 - o Pliki konfiguracyjne serwera (134)
 - o Pliki katalogu dokumentów (134)
 - o Katalog cgi-bin (135)
 - o Katalog logs (135)
 - o Katalog bin (135)
- Modyfikacja skryptu apachectl (136)
- Test Nikto po zmianach konfiguracji (137)
- Podsumowanie (137)

Rozdział 5. Najważniejsze moduły zabezpieczeń (139)

- Protokół SSL (139)
 - o Dlaczego należy korzystać z protokołu SSL? (140)
 - o Jak działa mechanizm SSL? (142)
 - o Wymagane oprogramowanie (144)
 - o Instalacja oprogramowania SSL (145)
 - o Tworzenie certyfikatów SSL (146)
 - o Sprawdzenie wstępnej konfiguracji (147)
 - o Konfiguracja modułu mod_ssl (149)
 - o Podsumowanie mechanizmu SSL (155)
- Moduł mod_rewrite (155)
 - o Włączenie modułu mod_rewrite (156)
 - o Podsumowanie modułu mod_rewrite (158)
- Moduł mod_log_forensic (158)
- Moduł mod_evasive (159)
 - o Do czego służy moduł mod_evasive? (159)
 - o Instalacja modułu mod_evasive (160)
 - o Jak działa moduł mod_evasive? (160)
 - o Konfiguracja (161)
 - o Podsumowanie modułu mod_evasive (165)
- Moduł mod_security (165)
 - o Instalacja modułu mod_security (166)
 - o Ogólne informacje na temat modułu (166)

- o Opcje i możliwości modułu mod_security (167)
 - o Techniki przeciwdziałania maskowaniu ataków (168)
 - o Specjalne wbudowane procedury sprawdzające (169)
 - o Reguły filtrowania (172)
 - o Akcje (173)
 - o Pozostałe funkcje (176)
- Podsumowanie (177)

Rozdział 6. Test konfiguracji - narzędzie CIS Apache Benchmark Scoring Tool (179)

- Pobranie, rozpakowanie i uruchomienie aplikacji (180)
 - o Rozpakowanie archiwum (181)
 - o Uruchomienie programu (182)
- Podsumowanie (186)

Rozdział 7. Klasyfikacja zagrożeń sieciowych WASC (187)

- Współautorzy dokumentu (188)
- Charakterystyka dokumentu WASC (188)
 - o Cele (189)
 - o Wykorzystanie dokumentacji (189)
 - o Przegląd (189)
 - o Tło (190)
- Klasy ataków (190)
 - o Format podrozdziałów (191)
- Uwierzytelnianie (192)
 - o Metoda siłowa (192)
 - o Niedostateczne uwierzytelnienie (196)
 - o Niedoskonały mechanizm odzyskiwania haseł (198)
- Autoryzacja (200)
 - o Predykcja danych uwierzytelniających (danych sesji) (200)
 - o Niedostateczna autoryzacja (202)
 - o Niewłaściwe wygasanie sesji (204)
 - o Ustawienie sesji (205)
- Ataki na jednostki klienckie (209)
 - o Podmiana treści (209)
 - o Wykonywanie kodu w ramach witryny (211)
- Wykonywanie poleceń (213)
 - o Przepełnienie bufora (213)
 - o Atak z wykorzystaniem ciągu formatującego (218)
 - o Wstrzyknięcie danych LDAP (220)
 - o Wykonanie poleceń systemu operacyjnego (222)
 - o Wstrzyknięcie instrukcji SQL (224)
 - o Wstrzyknięcie instrukcji SSI (229)
 - o Wstrzyknięcie instrukcji XPath (230)
- Ujawnienie informacji (231)
 - o Indeksowanie katalogu (232)
 - o Wyciek informacji (235)
 - o Manipulacja ścieżkami (237)
 - o Przewidywanie położenia zasobów (240)

- Ataki logiczne (241)
 - o Zakłócenie funkcjonowania (241)
 - o Odmowa obsługi (244)
 - o Niedostateczne zabezpieczenie przed automatyzacją (247)
 - o Niedostateczna walidacja procesu (248)
- Podsumowanie (250)

Rozdział 8. Zabezpieczenie aplikacji sieciowej Buggy Bank (251)

- Instalacja serwisu Buggy Bank (252)
 - o Pliki witryny Buggy Bank (253)
 - o Wyłączenie zabezpieczeń (253)
 - o Testowanie instalacji (254)
- Funkcje (255)
 - o Konta użytkowników (256)
- Metodologia działań (257)
 - o Ogólne zagadnienia (257)
 - o Wykorzystane narzędzia (257)
 - o Konfiguracja programu Burp Proxy (258)
- Luki w zabezpieczeniach serwisu Buggy Bank (260)
 - o Komentarze w kodzie HTML (260)
 - o Ustalenie numerów kont (261)
 - o Jaka jest wartość entropii? (262)
 - o Ustalenie numerów kont metodą siłową (263)
 - o Wyznaczenie identyfikatorów PIN (266)
 - o Odblokowane konto (266)
 - o Zablokowane konto (266)
 - o Ustalenie identyfikatorów PIN metodą siłową (267)
 - o Wstrzykiwanie poleceń (269)
 - o Wykonanie polecenia netstat (269)
- Wstrzyknięcie instrukcji SQL (273)
 - o Zapobieganie wstrzykiwaniu instrukcji SQL (275)
- Wykonywanie skryptów w ramach witryny (XSS) (277)
 - o Zapobieganie (280)
- Zakłócenie działania funkcji przelewu (280)
 - o Zapobieganie (282)
- Podsumowanie (283)

Rozdział 9. Ochrona i przeciwdziałanie (285)

- Dlaczego firewalle nie chronią w dostateczny sposób serwerów i aplikacji? (286)
- Dlaczego systemy wykrywania włamań są również nieskuteczne (288)
- Szczegółowa analiza pakietów, wtrącone systemy IDS i firewalle aplikacji WWW (292)
 - o Firewalle z funkcją szczegółowej analizy pakietów (293)
 - o Wtrącone systemy IDS (294)
 - o Firewalle aplikacji WWW (295)
- Rozwiązania systemów wykrywania włamań (297)
 - o Metoda sygnaturowa (298)
 - o Polityka zdarzeń pozytywnych (białe listy) (301)

- o Analiza nagłówków (311)
 - o Analiza protokołów (314)
 - o Analiza identyfikatora zasobu URI (320)
 - o Analiza heurystyczna (322)
 - o Wykrywanie anomalii (323)
- Techniki oszukiwania systemów IDS i ochrona przed maskowaniem ataków (325)
 - o Możliwości oszukania systemu IDS (325)
 - o Mechanizmy zapobiegania maskowaniu żądań (328)
 - o Oszukiwanie przez zakłócenie działania serwera Apache (330)
- Wykrywanie sondowania i blokowanie niebezpiecznych stacji (333)
 - o Sondowanie za pomocą programów robaków (333)
 - o Blokowanie znanych niebezpiecznych stacji (334)
 - o Aplikacja nmap - identyfikacja właściciela procesu (337)
 - o Aplikacja nmap - sprawdzenie wersji oprogramowania (338)
 - o W jakim celu zmienia się baner informacyjny serwera? (340)
 - o Ukrywanie baneru informacyjnego serwera (341)
- Rozpoznanie serwera WWW (343)
 - o Różnice w implementacji protokołu HTTP (344)
 - o Zbieranie informacji z banerów (348)
 - o Zaawansowane procedury rozpoznawania serwerów WWW (348)
 - o Aplikacja HTTPrint (349)
 - o Obrona przed procedurą rozpoznawania serwerów WWW (351)
- Niebezpieczne roboty, ciekawscy klienci i superskanery (356)
 - o Niebezpieczne roboty i ciekawscy klienci (357)
 - o Superskanery (359)
- Reagowanie na ataki DoS, wykorzystanie metod siłowych i modyfikacja stron (365)
 - o Ataki DoS (365)
 - o Wykorzystanie metod siłowych (366)
 - o Modyfikacja stron (368)
 - o Zapobieganie modyfikowaniu stron (373)
- Alarmy i śledzenie działań włamywaczy (374)
 - o Powołanie zmiennych (377)
 - o Rejestrowanie danych do późniejszej analizy (377)
 - o Filtracja nieistotnych żądań i sprawdzenie liczby wysłanych powiadomień (378)
 - o Rejestracja żądania i odsyłacze do aplikacji śledzenia włamywacza (378)
 - o Wysłanie powiadomienia na pager (379)
 - o Wstrzymanie działania skryptu (379)
 - o Przesłanie dokumentu HTML (379)
 - o Przykładowe powiadomienia e-mail (379)
- Monitorowanie dzienników pracy serwera i analiza ich zawartości (386)
 - o Ciągły monitoring za pomocą programu SWATCH (387)
 - o Sgrep - analiza dziennika modułu mod_security (391)
- Systemy-pułapki (394)
 - o Wabiące systemy-pułapki (395)
 - o Fałszywy skrypt PHF (396)
 - o Identyfikacja i śledzenie przypadków wykonywania poleceń systemowych (397)
 - o Moduł mod_rewrite 2.1 - ostatnia deska ratunku (398)
- Podsumowanie (399)

Rozdział 10. Otwarty serwer proxy jako system-pułapka (401)

- Po co instalować otwarty serwer proxy w roli systemu-pułapki? (401)
 - Brak informacji o wystąpieniu ataku (402)
 - Brak szczegółowych (dostatecznych) informacji o transakcjach HTTP (402)
 - Brak zainteresowania ujawnieniem informacji o ataku (402)
- Czym są serwery proxy? (403)
- Podstawowe informacje na temat otwartych serwerów proxy (404)
- Otwarty serwer proxy jako system-pułapka (405)
 - Router-firewall firmy Linksys (405)
 - Wyłączenie niepotrzebnych usług sieciowych (406)
 - Konfiguracja serwera Apache jako jednostki proxy (406)
- Sterowanie danymi (408)
 - Moduł mod_evasive (409)
 - Moduł mod_security (409)
 - Wykorzystanie sygnatur systemu Snort (410)
 - Ataki z wykorzystaniem metod siłowych (411)
- Przechwytywanie danych (412)
 - Ciągłe monitorowanie za pomocą programu Web spy (413)
- Skan miesiąca - wyzwanie nr 31 w projekcie Honeynet (414)
 - Wyzwanie (414)
 - Czynności przygotowawcze (415)
- Pytanie: W jaki sposób włamywacze odnaleźli proxy-pułapkę? (416)
- Pytanie: Jakiego rodzaju ataki można zidentyfikować? Dla każdej kategorii ataku podaj przynajmniej jeden przykład wpisu i dołącz jak najwięcej informacji na temat samego ataku (np. identyfikatory CERT, CVE i sygnatur wirusów). Ile kategorii ataków można wyróżnić? (417)
 - Wyszukiwanie ciągu mod_security-message (418)
 - Wykorzystanie funkcji przekazywania AllowCONNECT (419)
 - Wyszukiwanie niestandardowych kodów statusowych HTTP (420)
 - Niestandardowe metody żądań HTTP (422)
 - Żądania niezgodne z protokołem HTTP (423)
 - Kategoria ataku - spam (425)
 - Kategoria ataku - uwierzytelnianie metodą siłową (426)
 - Kategoria ataku - skanowanie luk w zabezpieczeniach (427)
 - Kategoria ataku - robaki internetowe (432)
 - Kategoria ataku - pozorne kliknięcie baneru reklamowego (435)
 - Kategoria ataku - połączenia IRC (436)
- Pytanie: Czy włamywacze wybierali jako cele ataków serwery WWW obsługujące protokół SSL? (437)
 - Czy celem była również usługa SSL proxy-pułapki? (438)
 - Dlaczego chcieli korzystać z protokołu SSL? (439)
 - Dlaczego nie korzystali wyłącznie z usług SSL? (439)
- Pytanie: Czy są jakiegolwiek oznaki, że w ataku pośredniczyły inne serwery proxy? Opisz, w jaki sposób można wykryć takie działanie. Wymień inne zidentyfikowane serwery proxy. Czy można potwierdzić, że dane jednostki są rzeczywiście serwerami proxy? (439)
 - Identyfikacja aktywności (440)
 - Potwierdzenie informacji o serwerach proxy (442)
 - Wykorzystanie określonych otwartych serwerów proxy (445)

- o Wykorzystanie określonych serwerów docelowych (445)
- Pytanie: Wyodrębnij przypadki zastosowania metod siłowych do uwierzytelnienia. Czy można pozyskać dane uwierzytelniające (nazwę użytkownika i hasło) w formie otwartego tekstu? Opisz metody analizy (447)
 - o Żądania HTTP GET (447)
 - o Żądania HTTP POST (447)
 - o Uwierzytelnienie HTTP typu Basic (448)
 - o Uzyskanie danych uwierzytelniających w formie otwartego tekstu (450)
 - o Rozproszone skanowanie metodą siłową kont serwisu Yahoo! (451)
 - o Skanowanie w przód i odwrotne (452)
- Pytanie: Co oznacza komunikat modułu mod_security o treści Invalid Character Detected? Jaki był cel działania włamywacza? (457)
 - o Dyrektywa SecFilterCheckURLEncoding - sprawdzenie kodowania URL (457)
 - o Dyrektywa SecFilterCheckUnicodeEncoding - sprawdzenie kodowania Unicode (457)
 - o Dyrektywa SecFilterForceByteRange - sprawdzenie zakresu wartości bajtowych (458)
 - o Sprawdzenie dostępności usługi SOCKS (458)
 - o Ataki robaków internetowych Code Red i NIMDA (459)
- Pytanie: Zarejestrowano kilka prób przesłania spamu, o czym świadczą próby wykorzystania adresu URL: <http://mail.sina.com.cn/cgi-bin/sendmsg.cgi>. List zawierał załącznik HTML (pliki wymienione w katalogu /upload). Jaka była treść strony WWW spamu? Kim byli odbiorcy spamu? (460)
 - o Odbiorcy spamu (461)
- Pytanie: Opracuj kilka statystyk (461)
 - o Dziesięciu najaktywniejszych włamywaczy (461)
 - o Dziesięć najczęściej atakowanych jednostek (462)
 - o Dziesięć najczęściej wykorzystywanych przeglądarek (wraz z fałszowanymi nazwami) (462)
 - o Powiązanie włamywaczy z danymi serwisu DShield i innymi źródłami informacji (464)
- Pytanie dodatkowe: Dlaczego włamywacze wybierali witryny pornograficzne jako cel ataków z wykorzystaniem metod siłowych (poza oczywistą fizyczną gratyfikacją)? (464)
 - o Czy mimo że adres IP i nazwa proxy-pułapki zostały zamaskowane we wpisach dziennika, można wskazać prawdopodobnego właściciela segmentu sieci? (466)
- Podsumowanie (468)

Rozdział 11. Podsumowanie prezentowanych rozwiązań (471)

- Przykładowe ostrzeżenie o błędzie systemu zabezpieczeń (471)
- Sprawdzenie wersji oprogramowania (472)
- Sprawdzenie dostępności nakładki (472)
- Szczegółowe informacje o błędzie w zabezpieczeniach (473)
 - o Utworzenie filtra mod_security (476)
 - o Test filtra (476)
 - o Pierwsza pomoc czy szpital (477)
- Bezpieczeństwo sieci - zagadnienia niezwiązane z serwerem WWW (478)

- o Przejęcie domeny (478)
 - o Zatrucie pamięci podręcznej DNS (478)
 - o Zakłócenie pracy buforującego serwera proxy (479)
 - o Podmiana baneru reklamowego (481)
 - o Zakłócenie działania serwisu informacyjnego (481)
 - o Podmiana czy nie? (482)
- Podsumowanie (482)

Dodatek A Słownik WASC (485)

Dodatek B Wykaz modułów Apache (495)

Dodatek C Przykładowy plik httpd.conf (511)

Skorowidz (521)