

Spis treści

O autorze (9)

O korektorach merytorycznych (11)

Wstęp (13)

Rozdział 1. Podstawy testów penetracyjnych i aplikacji sieciowych (19)

Aktywne testowanie zabezpieczeń (20)

Kim jest haker (21)

Różne metodyki testowania (21)

Plan operacji (23)

Czarna czy szara skrzynka (23)

Dane kontaktowe klienta (23)

Sposób powiadamiania działu IT klienta (24)

Postępowanie z poufnymi danymi (24)

Spotkania sprawozdawcze (24)

Ograniczenia testów penetracyjnych (25)

Dlaczego należy testować aplikacje sieciowe (26)

Ataki oparte na inżynierii społecznej (28)

Szkolenia z obrony przed atakami z użyciem inżynierii społecznej (29)

Podstawy budowy aplikacji sieciowych dla pentesterów (29)

Protokół HTTP (30)

Nagłówki żądania i odpowiedzi (30)

Metody HTTP ważne w kontekście testów penetracyjnych (33)

Śledzenie sesji przy użyciu ciasteczek (35)

Dane HTML-a w odpowiedzi HTTP (37)

Wielowarstwowe aplikacje sieciowe (38)

Podsumowanie (39)

Rozdział 2. Konfiguracja środowiska pracy w systemie Kali Linux (41)

Kali Linux (41)

Udoskonalenia wprowadzone w Kali Linuksie (42)

Instalowanie Kali Linuksa (43)

Wirtualizacja Kali Linuksa a instalacja na fizycznym sprzęcie (48)

Najważniejsze narzędzia w systemie Kali Linux (49)

Pośredniki aplikacji sieciowych (49)

Sieciowy skaner luk w zabezpieczeniach (53)

Narzędzia do identyfikacji systemów CMS (56)

Fuzzery aplikacji sieciowych (57)

Testowanie penetracyjne przy użyciu narzędzia Tor (57)

Konfiguracja Tora i nawiązywanie anonimowego połączenia (58)

Wizualizacja żądania sieciowego w Torze (60)

Kilka uwag o Torze na zakończenie (61)

Podsumowanie (62)

Rozdział 3. Prowadzenie rekonesansu i profilowanie serwera sieciowego (63)

Rekonesans (64)

Rekonesans pasywny a rekonesans aktywny (64)

Rekonesans - zbieranie informacji (65)

Skanowanie - badanie celu (73)

Skanowanie portów za pomocą narzędzia Nmap (74)

Identyfikacja systemu operacyjnego za pomocą Nmap (78)

Profilowanie serwera (79)

Podsumowanie (98)

Rozdział 4. Najważniejsze wady aplikacji sieciowych (99)

Wycieki informacji (100)

Przeglądanie zawartości katalogów (100)

Wady dotyczące mechanizmów uwierzytelniania (102)

Protokoły uwierzytelniania i związane z nimi błędy (102)

Łamanie haseł i loginów metodą brute force (103)

Przeglądanie ścieżki (105)

Przeglądanie ścieżki za pomocą narzędzia Burp (107)

Luki umożliwiające wstrzykiwanie kodu (109)

Wstrzykiwanie poleceń (109)

Wstrzykiwanie kodu SQL (110)

Ataki typu XSS (112)

Potencjał ataków typu XSS (114)

Ataki typu CSRF (114)

Luki dotyczące sesji (115)

Sposoby kradzieży tokenów (116)

Narzędzia do analizy tokenów (117)

Ataki z wykorzystaniem spreparowanych identyfikatorów sesji (117)

Obrona przed atakami z wykorzystaniem spreparowanych identyfikatorów sesji (118)

Luka związana z dołączaniem plików (119)

Dołączanie plików zdalnych (119)

Dołączanie plików lokalnych (119)

Obrona przed atakami polegającymi na dołączaniu plików (120)

Zatruwanie parametrów HTTP (120)

Obrona (123)

Dzielenie odpowiedzi HTTP (123)

Obrona (124)

Podsumowanie (124)

Rozdział 5. Ataki na serwer metodą wstrzykiwania kodu (127)

Wstrzykiwanie poleceń (128)

Identyfikacja parametrów do wstrzykiwania danych (129)

Komunikaty o błędach i wstrzyknięcia ślepe (130)

Metaznaki do oddzielania poleceń (130)

Szukanie za pomocą skanera luk umożliwiających wstrzykiwanie poleceń (131)

Wstrzykiwanie poleceń za pomocą Metasploita (134)

Wykorzystywanie luki Shellshock (138)

SQL injection (142)

Instrukcje SQL (142)

Możliwości ataku z wykorzystaniem luki typu SQL injection (144)

Ślepe ataki typu SQL injection (145)

Metody testowania aplikacji pod kątem luk typu SQL injection (146)

Automat sqlmap (147)

BBQSQL - środowisko do ślepego wstrzykiwania kodu SQL (150)

Wstrzykiwanie kodu do baz MySQL za pomocą programu sqlsus (151)

sqlninja - MS SQL injection (152)

Podsumowanie (154)

Rozdział 6. Luki umożliwiające przeprowadzanie ataków XSS i XSRF (155)

Historia ataków typu XSS (156)

Wprowadzenie do JavaScriptu (156)

Podstawowe informacje o atakach typu XSS (157)

Typy ataków XSS (159)

Ataki XSS z utrwaleniem (159)

Refleksyjne ataki XSS (161)

Ataki XSS na DOM (161)

Ataki XSS z użyciem metody POST (164)

XSS i JavaScript - śmiertelna mieszanka (165)

Kradzież ciasteczek (165)

Rejestrowanie naciskanych klawiszy (166)

Zmiana wyglądu witryny (166)

Skanowanie w poszukiwaniu luk typu XSS (167)

Zed Attack Proxy (167)

XSSer (172)

w3af (175)

Luki typu XSRF (179)

Warunki powodzenia ataku (179)

Technika ataku (179)

Szukanie luk typu XSRF (180)

Techniki obrony przed atakami XSRF (181)

Podsumowanie (182)

Rozdział 7. Atakowanie witryn SSL (183)

Secure Socket Layer (184)

SSL w aplikacjach sieciowych (185)

Proces szyfrowania SSL (186)

Szyfrowanie asymetryczne a szyfrowanie symetryczne (187)

Zapewnianie nienaruszalności danych za pomocą mieszania (189)

Identyfikacja słabych implementacji SSL (190)

Ataki typu man in the middle na SSL (196)

Podsumowanie (201)

Rozdział 8. Przeprowadzanie ataków przy użyciu frameworków (203)

Socjotechnika (204)

Pakiet narzędzi socjotechnicznych (205)

Ataki spear phishing (206)

Ataki z użyciem strony internetowej (209)

Java Applet Attack (209)

Credential Harvester Attack (210)

Web Jacking Attack (211)

Metasploit Browser Exploit (212)

Tabnabbing Attack (212)

Browser Exploitation Framework (214)

Wprowadzenie do BeEF (214)

Wstrzykiwanie uchwytu BeEF (215)

Atak XSS na Mutillidae za pomocą BeEF (221)

Wstrzykiwanie zaczepu BeEF metodą MITM (223)

Podsumowanie (225)

Rozdział 9. AJAX i usługi sieciowe - luki bezpieczeństwa (227)

Wprowadzenie do technologii AJAX (228)

Składniki technologii AJAX (229)

Zasada działania technologii AJAX (229)

Kwestie bezpieczeństwa w odniesieniu do technologii AJAX (232)

Trudności w wykonywaniu testów penetracyjnych aplikacji AJAX (234)

Przeszukiwanie aplikacji AJAX (234)

Analizowanie kodu klienckiego - Firebug (238)

Usługi sieciowe (241)

Podstawowe informacje o usługach SOAP i usługach REST-owych (242)

Zabezpieczanie usług sieciowych (243)

Podsumowanie (245)

Rozdział 10. Fuzzing aplikacji sieciowych (247)

Podstawy fuzzingu (248)

Typy technik fuzzingu (249)

Fuzzing mutacyjny (249)

Fuzzing generacyjny (250)

Zastosowania fuzzingu (250)

Frameworki fuzzingowe (252)

Etapy fuzzingu (253)

Testowanie fuzzingowe aplikacji sieciowych (254)

Fuzzery aplikacji sieciowych w Kali Linuksie (256)

Podsumowanie (263)

Skorowidz (265)