

Spis treści

O autorze (13)

O recenzencie (15)

Przedmowa (17)

Rozdział 1. Testy penetracyjne ukierunkowane na osiągnięcie celu (23)

Koncepcyjny przegląd testów bezpieczeństwa (24)

Zmierzch klasycznych testów penetracyjnych, skanowania w poszukiwaniu podatności i działań zespołów Red Team (24)

Metodologia przeprowadzania testów (26)

Wprowadzenie do systemu Kali Linux - jego historia i przeznaczenie (28)

Instalowanie i aktualizowanie systemu Kali Linux (30)

Uruchamianie systemu Kali Linux z urządzenia przenośnego (30)

Instalowanie systemu Kali Linux w maszynie wirtualnej (31)

VMware Workstation Player (32)

VirtualBox (34)

Instalowanie aplikacji Docker (39)

Instalowanie systemu Kali Linux w chmurze - tworzenie instancji AWS (41)

Dostosowywanie systemu Kali Linux (43)

Konfigurowanie i dostosowywanie systemu Kali Linux (44)

Zmiana hasła użytkownika root (44)

Dodawanie zwykłego konta użytkownika (44)

Przyspieszanie działania systemu Kali Linux (45)

Udostępnianie i współużytkowanie folderów z systemem operacyjnym hosta (46)

Dostosowywanie systemu Kali Linux do własnych potrzeb przy użyciu skryptów powłoki bash (48)

Budowanie środowiska testowego (49)

Konfigurowanie sieci wirtualnej z usługą Active Directory (49)

Instalowanie zdefiniowanych celów (52)

Metasploitable3 (52)

Mutillidae (53)

Zarządzanie testami penetracyjnymi przy użyciu pakietu Faraday (54)

Podsumowanie (58)

Rozdział 2. OSINT oraz rozpoznanie pasywne (59)

Podstawowe zasady przeprowadzania rozpoznania (60)

Biały wywiad (OSINT) (61)

Ofensywny biały wywiad (62)

Maltego (63)

CaseFile (66)

Usługi Google Cache (67)

Scraping (68)

Pozyskiwanie nazw kont użytkowników i adresów e-mail (69)

Zbieranie informacji o użytkownikach (70)

Wyszukiwarki Shodan i censys.io (70)

Google Hacking Database (71)

Używanie zaawansowanych operatorów Google (72)

Serwery szybkiej wymiany danych (73)

Zastosowanie skryptów do automatycznego zbierania informacji OSINT (74)

Defensywny biały wywiad (75)

Profilowanie użytkowników pod kątem przygotowywania listy haseł (78)

Tworzenie słowników do łamania haseł (78)

Zastosowanie programu CeWL do mapowania witryny internetowej (79)

Pozyskiwanie listy słów z serwisu Twitter przy użyciu programu Twofi (80)

Podsumowanie (80)

Rozdział 3. Aktywne rozpoznawanie zewnętrznych i wewnętrznych środowisk celu (83)

Trudne do wykrycia techniki skanowania (84)

Modyfikowanie źródłowych adresów IP i dostosowywanie ustawień używanych narzędzi (85)

Modyfikowanie parametrów pakietów (86)

Używanie serwerów proxy i sieci anonimowych (88)

Rozpoznanie DNS i mapowanie sieci (91)

Polecenie whois (92)

Wykorzystywanie kompleksowych aplikacji wspomagających przeprowadzanie rozpoznania (94)

Framework recon-ng (94)

Protokół IPv6 - wybrane narzędzia (99)

Mapowanie trasy do celu (100)

Identyfikowanie zewnętrznej infrastruktury sieciowej (103)

Mapowanie sieci poza zaporą sieciową (104)

Identyfikacja systemów IDS/IPS (105)

Wyszukiwanie hostów (107)

Wykrywanie aktywnych hostów (108)

Wykrywanie otwartych portów, systemu operacyjnego oraz działających usług (109)

Skanowanie portów (109)

Tworzenie własnego skanera portów przy użyciu programu netcat (110)

Identyfikacja systemu operacyjnego zdalnego hosta (111)

Wykrywanie usług działających na zdalnych hostach (112)

Skanowanie dużych środowisk celu (113)

Wykorzystanie danych DHCP (114)

- Wykrywanie oraz identyfikacja hostów w wewnętrznych sieciach środowiska celu (115)
- Wbudowane polecenia konsolowe systemu Windows (116)
- Rozgłoszenia ARP (117)
- Wykrywanie hostów w sieci za pomocą pakietów ping (117)
- Zastosowanie skryptów do łączenia skanów z użyciem programów masscan i nmap (119)
- Wykorzystanie protokołu SNMP (120)
- Pozyskiwanie informacji o kontach użytkowników Windows za pośrednictwem sesji SMB (121)
- Identyfikacja udziałów sieciowych (123)
- Rozpoznawanie serwerów w domenie Active Directory (124)
- Zastosowanie narzędzi złożonych (SPARTA) (125)
- Przykład konfiguracji pakietu SPARTA (126)
- Podsumowanie (127)

Rozdział 4. Wyszukiwanie podatności i luk w zabezpieczeniach (129)

- Trochę nomenklatury (130)
- Lokalne i sieciowe bazy podatności i luk w zabezpieczeniach (131)
- Skanowanie w poszukiwaniu podatności przy użyciu programu nmap (135)
 - Wprowadzenie do skryptów LUA (137)
 - Dostosowywanie skryptów NSE do własnych potrzeb (137)
- Skanery podatności aplikacji sieciowych (139)
 - Wprowadzenie do skanerów Nikto i Vega (140)
 - Dostosowywanie skanerów Nikto i Vega do własnych potrzeb (142)
- Skanery podatności dla aplikacji mobilnych (146)
- Skaner podatności OpenVAS (148)
 - Dostosowywanie skanera OpenVAS do własnych potrzeb (150)
- Specjalizowane skanery podatności (150)
- Modelowanie zagrożeń (151)

Podsumowanie (153)

Rozdział 5. Bezpieczeństwo fizyczne i metody socjotechniczne (155)

Metodologia przeprowadzania ataków (157)

Ataki z wykorzystaniem komputera (157)

Ataki z wykorzystaniem telefonu (158)

Ataki z dostępem fizycznym (159)

Ataki z dostępem do konsoli systemu (159)

Programy samdump2 i chntpw (160)

Ułatwienia dostępu - opcja Sticky Keys (163)

Ataki na pamięć systemową przy użyciu programu Inception (164)

Tworzenie złośliwych urządzeń fizycznych (166)

Ataki z wykorzystaniem urządzeń mikroprocesorowych (168)

Pakiet SET (170)

Ataki na witryny internetowe - atak ze zbieraniem poświadczeń logowania (174)

Ataki na witryny internetowe - atak typu tabnabbing (176)

Ataki na witryny internetowe - ataki złożone (177)

Atak ze wstrzykiwaniem alfanumerycznego kodu shellcode z powłoki Powershell (178)

Ataki z wykorzystaniem aplikacji HTA (179)

Ukrywanie plików wykonywalnych oraz maskowanie adresu URL napastnika (181)

Eskalowanie ataków przy użyciu przekierowań DNS (183)

Ataki typu spear phishing (184)

Przeprowadzanie kampanii phishingowej z wykorzystaniem pakietu Phishing Frenzy (188)

Przeprowadzanie ataku phishingowego (192)

Podsumowanie (194)

Rozdział 6. Ataki na sieci bezprzewodowe (195)

Konfigurowanie systemu Kali Linux do przeprowadzania ataków na sieci bezprzewodowe	(196)
Przeprowadzanie rozpoznania w sieciach bezprzewodowych	(197)
Kismet	(200)
Omijanie zabezpieczenia sieci z ukrytym identyfikatorem SSID	(202)
Omijanie zabezpieczenia sieci z filtrowaniem adresów MAC oraz otwartym uwierzytelnianiem	(204)
Atakowanie sieci z szyfrowaniem WPA i WPA2	(206)
Ataki typu brute-force	(207)
Atakowanie routerów sieci bezprzewodowych przy użyciu programu Reaver	(210)
Ataki typu DoS na sieci bezprzewodowe	(211)
Ataki na sieci WLAN z szyfrowaniem WPA/WPA2-Enterprise	(213)
Praca z pakietem Ghost Phisher	(217)
Podsumowanie	(218)
 Rozdział 7. Rozpoznawanie i przełamywanie zabezpieczeń aplikacji internetowych	(221)
Metodologia	(222)
Planowanie ataku	(224)
Przeprowadzanie rozpoznania witryny internetowej	(225)
Wykrywanie zapór WAF oraz systemów równoważenia obciążenia	(227)
Tworzenie sygnatur aplikacji internetowych i systemów CMS	(228)
Tworzenie lustrzanej kopii strony internetowej z poziomu wiersza poleceń	(231)
Serwery proxy po stronie klienta	(232)
Burp Proxy	(232)
Poszerzanie funkcjonalności przeglądarek internetowych	(237)
Przeszukiwanie sieci i ataki typu brute-force na struktury katalogów	(239)
Skanery podatności wykrywające podatności określonych usług i aplikacji	(239)
Ataki specyficzne dla określonych aplikacji	(241)
Ataki typu brute-force na poświadczenia logowania	(241)

Wstrzykiwanie poleceń systemu operacyjnego przy użyciu narzędzia commix (241)

Ataki ze wstrzykiwaniem danych lub kodu do baz danych (243)

Utrzymywanie dostępu za pomocą powłok webshell (245)

Podsumowanie (247)

Rozdział 8. Ataki na zdalny dostęp (249)

Wykorzystywanie luk w zabezpieczeniach protokołów komunikacyjnych (250)

Przełamywanie zabezpieczeń protokołu RDP (250)

Przełamywanie zabezpieczeń protokołu SSH (253)

Przełamywanie zabezpieczeń protokołu VNC (255)

Ataki na połączenia SSL (257)

Słabe strony i luki w zabezpieczeniach protokołu SSL (257)

Praca z programem Testssl (259)

Rozpoznawanie połączeń SSL (260)

Zastosowanie programu sslstrip do przeprowadzania ataku man-in-the-middle (265)

Ataki typu DoS na połączenia SSL (268)

Ataki na wirtualne sieci prywatne z protokołem IPSec (269)

Skanowanie w poszukiwaniu bramek VPN (270)

Tworzenie cyfrowego odcisku palca bramy VPN (271)

Przechwytywanie kluczy PSK (272)

Łamanie kluczy PSK w trybie offline (272)

Identyfikacja domyślnych kont użytkowników (273)

Podsumowanie (273)

Rozdział 9. Ataki po stronie klienta (275)

Backdooring - tworzenie plików wykonywalnych wyposażonych w tylne wejścia (276)

Atakowanie systemów przy użyciu złośliwych skryptów (279)

Przeprowadzanie ataków za pomocą skryptów w języku VBScript (279)

Atakowanie systemów przy użyciu skryptów powłoki PowerShell (282)

Pakiet XSS Framework (285)

Pakiet BeEF (289)

Konfigurowanie pakietu BeEF (290)

Praca z pakietem BeEF (293)

Integracja pakietów BeEF i Metasploit (296)

Używanie pakietu BeEF jako tunelującego serwera proxy (297)

Podsumowanie (299)

Rozdział 10. Omijanie mechanizmów zabezpieczających (301)

Omijanie zabezpieczeń wprowadzanych przez mechanizm NAC (302)

Weryfikacja przed uzyskaniem dostępu do sieci (303)

Weryfikacja po uzyskaniu dostępu do sieci (305)

Omijanie programów antywirusowych przy użyciu różnych narzędzi (305)

Korzystanie z pakietu Veil Framework (307)

Używanie programu Shellter (312)

Omijanie zabezpieczeń działających na poziomie aplikacji (316)

Zastosowanie protokołu SSH do tunelowania połączeń przez zapory sieciowe działające po stronie klienta (316)

Omijanie białej listy aplikacji (320)

Omijanie zabezpieczeń systemu operacyjnego Windows (322)

Pakiet EMET (Enhanced Migration Experience Toolkit) (322)

UAC - kontrola konta użytkownika (323)

Inne zabezpieczenia systemu operacyjnego Windows (328)

Podsumowanie (331)

Rozdział 11. Wykorzystywanie podatności i luk w zabezpieczeniach (333)

Pakiet Metasploit (334)

Biblioteki (334)

Interfejsy (335)

Moduły (336)

Tworzenie i konfiguracja bazy danych (337)

Atakowanie celów przy użyciu pakietu Metasploit Framework (342)

Atakowanie pojedynczych systemów z użyciem odwróconej powłoki (342)

Atakowanie pojedynczych systemów z użyciem odwróconej powłoki PowerShell (344)

Atakowanie wielu systemów przy użyciu plików zasobów pakietu Metasploit Framework (345)

Atakowanie wielu systemów przy użyciu pakietu Armitage (346)

Używanie publicznych exploitów (349)

Lokalizowanie i weryfikowanie publicznie dostępnych exploitów (349)

Kompilowanie i używanie exploitów (351)

Tworzenie exploitów dla systemu Windows (353)

Identyfikacja podatności i luk w zabezpieczeniach przy użyciu fuzzingu (354)

Tworzenie exploita dla systemu Windows (360)

Podsumowanie (363)

Rozdział 12. Powłamaniowa eksploracja środowiska celu (365)

Eksploracja skompromitowanego systemu lokalnego (366)

Przeprowadzenie szybkiego rozpoznania skompromitowanego systemu (367)

Wyszukiwanie i pobieranie wrażliwych danych - plądrowanie celu (368)

Narzędzia wspomagające powłamaniową eksplorację systemu (MSF, framework Veil-Pillage, skrypty) (372)

Pakiet Veil-Pillage (375)

Eskalacja pozioma i atakowanie innych systemów (379)

Kompromitowanie relacji zaufania między domenami oraz udziałów sieciowych (380)

PsExec, WMIC i inne narzędzia (381)

Eskalacja pozioma z użyciem usług (385)

Pivoting i przekierowywanie portów (385)

Podsumowanie (388)

Rozdział 13. Podnoszenie uprawnień (389)

Typowa metodologia podnoszenia uprawnień (390)

Podnoszenie uprawnień w systemie lokalnym (391)

Podnoszenie uprawnień z poziomu administratora na poziom systemu (392)

Wstrzykiwanie bibliotek DLL (393)

Narzędzie PowerShell Empire (395)

Ataki pozwalające na zbieranie poświadczeń i podnoszenie uprawnień (400)

Sniffery haseł (401)

Responder (402)

Ataki typu SMB relay (405)

Podnoszenie uprawnień w Active Directory (405)

Ataki typu Golden Ticket na protokół Kerberos (412)

Podsumowanie (414)

Rozdział 14. Sterowanie i kontrola (415)

Używanie agentów persystencji (416)

Używanie programu Netcat jako agenta persystencji (417)

Zastosowanie programu schtasks do konfigurowania trwałych zadań (421)

Utrzymywanie trwałego dostępu przy użyciu pakietu Metasploit (422)

Używanie skryptu persistence (423)

Tworzenie samodzielnego trwałego agenta z wykorzystaniem pakietu Metasploit (424)

Utrzymywanie trwałego dostępu za pomocą mediów społecznościowych i poczty Gmail (426)

Eksfiltracja danych (429)

Korzystanie z istniejących usług systemowych (Telnet, RDP i VNC) (430)

Eksfiltracja danych z wykorzystaniem protokołu DNS (431)

Eksfiltracja danych z wykorzystaniem protokołu DNS (433)

Pakiet Data Exfiltration Toolkit (DET) (435)

Eksfiltracja danych z wykorzystaniem powłoki PowerShell (437)

Ukrywanie śladów ataku (437)

Podsumowanie (439)

Skorowidz (441)