

Słowo wstępne (17)

Podziękowania (21)

Wprowadzenie (23)

- Kilka słów podziękowania (24)
- Kilka słów o książce (25)
 - o Część I. Podstawy (25)
 - o Część II. Przygotowania (26)
 - o Część III. Ataki (26)
 - o Część IV. Tworzenie exploitów (27)
 - o Część V. Ataki na urządzenia mobilne (28)

0. Elementarz testów penetracyjnych (29)

- Etapy testów penetracyjnych (30)
 - o Faza wstępna (31)
 - o Zbieranie informacji (32)
 - o Mapowanie zagrożeń (33)
 - o Wykrywanie i analiza podatności (33)
 - o Atak (33)
 - o Powłamaniowa eksploracja skompromitowanego systemu (33)
 - o Raportowanie (34)
- Podsumowanie (36)

I. PODSTAWY

1. Tworzenie wirtualnego środowiska testowego (39)

- Instalowanie pakietu VMware (39)
- Instalacja i konfiguracja systemu Kali Linux (40)
 - o Konfiguracja połączeń sieciowych maszyny wirtualnej (44)
 - o Instalowanie pakietu Nessus (48)
 - o Instalowanie dodatkowych pakietów oprogramowania (52)
 - o Instalowanie emulatorów systemu Android (54)
 - o SPF - Smartphone Pentest Framework (60)
- Instalacja wirtualnych celów ataku (61)
- Tworzenie maszyny-celu z systemem Windows XP (62)
 - o VMware Player w systemie Microsoft Windows (62)
 - o VMware Fusion w systemie Mac OS (65)
 - o Instalowanie i aktywacja systemu Windows (65)
 - o Instalowanie pakietu VMware Tools (68)
 - o Wyłączanie zapory sieciowej systemu Windows XP (70)
 - o Ustawianie haseł dla kont użytkowników (70)
 - o Ustawianie statycznego adresu IP (71)
 - o Konfiguracja systemu Windows XP do pracy jak w domenie (73)
 - o Instalowanie oprogramowania podatnego na ataki (75)
 - o Instalowanie pakietów Immunity Debugger oraz Mona (81)
- Tworzenie maszyny-celu z systemem Ubuntu 8.10 (82)
- Tworzenie maszyny-celu z systemem Windows 7 (83)
 - o Tworzenie konta użytkownika (83)
 - o Wyłączanie automatycznego instalowania aktualizacji (85)

- o Ustawianie statycznego adresu IP (85)
 - o Dodawanie kolejnego interfejsu sieciowego (87)
 - o Instalowanie dodatkowego oprogramowania (88)
- Podsumowanie (90)

2. Praca z systemem Kali Linux (91)

- Wiersz poleceń systemu Linux (92)
- System plików w Linuksie (92)
 - o Zmiana katalogów (92)
- Dokumentacja poleceń - strony podręcznika man (93)
- Uprawnienia użytkowników (94)
 - o Dodawanie kont użytkowników (95)
 - o Dodawanie konta użytkownika do pliku sudoers (96)
 - o Przełączanie kont użytkowników i korzystanie z polecenia sudo (96)
 - o Tworzenie nowych plików i katalogów (97)
 - o Kopiowanie, przenoszenie i usuwanie plików (97)
 - o Dodawanie tekstu do pliku (98)
 - o Dołączanie tekstu do pliku (99)
- Prawa dostępu do plików (99)
- Edytowanie plików (100)
 - o Wyszukiwanie tekstu (101)
 - o Edytowanie plików przy użyciu edytora vi (101)
- Przetwarzanie danych (102)
 - o Zastosowanie polecenia grep (103)
 - o Zastosowanie polecenia sed (104)
 - o Dopasowywanie wzorców za pomocą polecenia awk (104)
- Zarządzanie zainstalowanymi pakietami oprogramowania (105)
- Procesy i usługi (106)
- Zarządzanie połączeniami sieciowymi (106)
 - o Ustawianie statycznego adresu IP (107)
 - o Przeglądanie połączeń sieciowych (108)
- Netcat - uniwersalne narzędzie do połączeń TCP/IP (108)
 - o Sprawdzanie, czy system zdalny nasłuchuje na danym porcie (109)
 - o Proces nasłuchujący poleceń powłoki (110)
 - o "Wypychanie" powłoki do procesu nasłuchującego (111)
- Automatyzacja zadań za pomocą procesu cron (112)
- Podsumowanie (113)

3. Programowanie (115)

- Skrypty powłoki bash (115)
 - o Polecenie ping (115)
 - o Prosty skrypt powłoki bash (116)
 - o Uruchamianie skryptu (117)
 - o Dodawanie nowych możliwości za pomocą polecenia if (117)
 - o Pętla for (118)
 - o Zwiększanie przejrzystości wyników działania (120)
- Skrypty w języku Python (123)
 - o Łączenie z wybranym portem sieciowym (124)

- o Instrukcja if w języku Python (124)
- Pisanie i kompilowanie programów w języku C (125)
- Podsumowanie (127)

4. Pakiet Metasploit Framework (129)

- Uruchamianie pakietu Metasploit (131)
- Wyszukiwanie modułów pakietu Metasploit (132)
 - o Baza modułów pakietu Metasploit (133)
 - o Wbudowane polecenie search (134)
- Ustawianie opcji modułu exploita (137)
 - o Opcja RHOST (138)
 - o Opcja RPORT (138)
 - o Opcja SMBPIPE (138)
 - o Opcja Exploit Target (139)
- Ładunki (kod powłoki) (140)
 - o Wyszukiwanie kompatybilnych ładunków (140)
 - o Przebieg testowy (141)
- Rodzaje powłok (142)
 - o Bind shell (142)
 - o Reverse shell (143)
- Ręczne wybieranie ładunku (143)
- Interfejs wiersza poleceń Msfccli (145)
 - o Uzyskiwanie pomocy (146)
 - o Wyświetlanie opcji (146)
 - o Ładunki (147)
- Tworzenie samodzielnych ładunków za pomocą narzędzia Msfvenom (148)
 - o Wybieranie ładunku (149)
 - o Ustawianie opcji (149)
 - o Wybieranie formatu ładunku (150)
 - o Dostarczanie ładunków (151)
 - o Zastosowanie modułu multi/handler (151)
- Zastosowanie dodatkowych modułów (153)
- Podsumowanie (155)

II. PRZYGOTOWANIA

5. Zbieranie informacji (159)

- OSINT - biały wywiad (160)
 - o Netcraft (160)
 - o Zapytania whois (161)
 - o Zapytania DNS (162)
 - o Poszukiwanie adresów poczty elektronicznej (165)
 - o Maltego (166)
- Skanowanie portów (170)
 - o Ręczne skanowanie portów (170)
 - o Skanowanie portów przy użyciu programu Nmap (172)
- Podsumowanie (180)

6. Wyszukiwanie podatności i luk w zabezpieczeniach (181)

- Od skanu z detekcją wersji do wykrycia potencjalnej luki w zabezpieczeniach (182)
- Nessus (182)
 - o Karta Policies - tworzenie polityki skanowania Nessusa (183)
 - o Skanowanie za pomocą Nessusa (186)
 - o Kilka słów na temat rankingu podatności i luk w zabezpieczeniach (189)
 - o Dlaczego powinieneś używać skanerów podatności? (189)
 - o Eksportowanie wyników skanowania (190)
 - o Odkrywanie podatności i luk w zabezpieczeniach (191)
- NSE - Nmap Scripting Engine (191)
- Uruchamianie wybranego skryptu NSE (194)
- Moduły skanerów pakietu Metasploit (196)
- Sprawdzanie podatności na exploity za pomocą polecenia check pakietu Metasploit (197)
- Skanowanie aplikacji internetowych (199)
 - o Pakiet Nikto (199)
 - o Ataki na pakiet XAMPP (200)
 - o Poświadczenia domyślne (201)
- Samodzielna analiza podatności (202)
 - o Eksploracja nietypowych portów (202)
 - o Wyszukiwanie nazw kont użytkowników (204)
- Podsumowanie (205)

7. Przechwytywanie ruchu sieciowego (207)

- Przechwytywanie ruchu w sieci (208)
- Zastosowanie programu Wireshark (208)
 - o Przechwytywanie ruchu sieciowego (209)
 - o Filtrowanie ruchu sieciowego (210)
 - o Rekonstruowanie sesji TCP (211)
 - o Analiza zawartości pakietów (212)
- Ataki typu ARP Cache Poisoning (213)
 - o Podstawy protokołu ARP (214)
 - o Przekazywanie pakietów IP (216)
 - o Zatrucie tablicy ARP przy użyciu polecenia arpspoof (217)
 - o Zastosowanie zatrucia tablic ARP do podszywania się pod domyślną bramę sieciową (219)
- Ataki typu DNS Cache Poisoning (220)
 - o Zatrucie DNS - podstawy (222)
 - o Zatrucie DNS przy użyciu polecenia dnsspoof (222)
- Ataki SSL (224)
 - o SSL - podstawy (224)
 - o Zastosowanie programu Ettercap do przeprowadzania ataków SSL MiTM (224)
- Ataki typu SSL Stripping (226)
 - o Zastosowanie programu SSLstrip (228)
- Podsumowanie (230)

III. ATAKI

8. Eksploracja środowiska celu (233)

- Powracamy do luki MS08-067 (234)
 - o Ładunki Metasploita (234)
 - o Meterpreter (236)
- Wykorzystywanie domyślnych poświadczeń logowania w dodatku WebDAV (237)
 - o Uruchamianie skryptów na atakowanym serwerze WWW (238)
 - o Kopiowanie ładunku przygotowanego za pomocą programu Msfvenom (239)
- Wykorzystywanie otwartej konsoli phpMyAdmin (241)
 - o Pobieranie plików za pomocą TFTP (243)
- Pobieranie wrażliwych plików (244)
 - o Pobieranie pliku konfiguracyjnego (244)
 - o Pobieranie pliku Windows SAM (245)
- Wykorzystywanie błędów przepełnienia bufora w innych aplikacjach (246)
- Wykorzystywanie luk w zabezpieczeniach innych aplikacji internetowych (248)
- Wykorzystywanie luk w zabezpieczeniach usług (250)
- Wykorzystywanie otwartych udziałów NFS (251)
- Podsumowanie (253)

9. Ataki na hasła (255)

- Zarządzanie hasłami (255)
- Ataki typu online (256)
 - o Listy haseł (257)
 - o Odnajdowanie nazw kont użytkowników i haseł przy użyciu programu Hydra (261)
- Ataki typu offline (263)
 - o Odzyskiwanie haszy haseł systemu Windows z pliku SAM (264)
 - o Pozyskiwanie zahaszowanych haseł z wykorzystaniem fizycznego dostępu do systemu (266)
 - o Algorytm LM kontra NTLM (269)
 - o Problem z haszami haseł w formacie LM (270)
 - o John the Ripper (271)
 - o Łamanie haseł systemu Linux (272)
 - o Łamanie haseł przechowywanych w plikach konfiguracyjnych (274)
 - o Tęczowe tablice (275)
 - o Usługi łamania haseł dostępne w sieci (275)
- Pozyskiwanie haseł z pamięci operacyjnej za pomocą programu Windows Credentials Editor (276)
- Podsumowanie (277)

10. Wykorzystywanie luk w zabezpieczeniach po stronie klienta (279)

- Omijanie filtrowania za pomocą ładunków pakietu Metasploit (280)
 - o Ładunek AllPorts (280)
 - o Ładunki HTTP i HTTPS (282)
- Ataki po stronie klienta (283)
 - o Luki w zabezpieczeniach przeglądarek sieciowych (284)
 - o Exploity dla plików PDF (292)
 - o Luki w zabezpieczeniach środowiska Java (298)
 - o Moduł browser_autopwn (304)
 - o Winamp (307)

- Podsumowanie (309)

11. Ataki socjotechniczne (311)

- Pakiet SET - Social-Engineer Toolkit (313)
- Ukierunkowane ataki phishingowe (314)
 - o Wybieranie ładunku (315)
 - o Ustawianie opcji (315)
 - o Wybieranie nazwy generowanego pliku (316)
 - o Jeden czy wielu adresatów? (316)
 - o Tworzenie szablonu wiadomości e-mail (316)
 - o Definiowanie celu ataku (317)
 - o Tworzenie procesu nasłuchującego (318)
- Ataki z wykorzystaniem stron internetowych (319)
- Masowe ataki e-mailowe (322)
- Ataki wielopłaszczyznowe (325)
- Podsumowanie (326)

12. Omijanie programów antywirusowych (327)

- Trojany (328)
 - o Msfvenom (328)
- Jak działają aplikacje antywirusowe? (331)
- Microsoft Security Essentials (332)
- VirusTotal (333)
- Omijanie programów antywirusowych (334)
 - o Kodowanie (335)
 - o Niestandardowe metody kompilowania (338)
 - o Szyfrowanie plików wykonywalnych przy użyciu programu Hyperion (341)
 - o Omijanie programów antywirusowych przy użyciu pakietu Veil-Evasion (343)
- Ukrywanie na widoku, czyli najciemniej jest pod latarnią (347)
- Podsumowanie (347)

13. Powłamaniowa eksploracja skompromitowanego systemu (349)

- Meterpreter (350)
 - o Zastosowanie polecenia upload (351)
 - o Polecenie getuid (352)
 - o Inne polecenia Meterpretera (352)
- Skrypty Meterpretera (353)
- Moduły Metasploita wspomagające powłamaniową eksplorację systemu (354)
- Railgun (356)
- Lokalne podnoszenie uprawnień użytkownika (356)
 - o Polecenie getsystem w systemie Windows (357)
 - o Moduły typu Local Escalation dla systemu Windows (358)
 - o Omijanie mechanizmu UAC w systemie Windows (359)
 - o Podnoszenie uprawnień w systemie Linux (361)
- Wyszukiwanie informacji w skompromitowanym systemie (366)
 - o Wyszukiwanie plików (367)
 - o Przechwytywanie naciśniętych klawiszy (keylogging) (367)

- o Gromadzenie poświadczeń logowania (368)
 - o Polecenie net (370)
 - o Inne sposoby (371)
 - o Sprawdzanie historii poleceń powłoki bash (372)
- Przechodzenie na kolejne systemy (372)
 - o PsExec (373)
 - o Uwierzytelnianie za pomocą skrótów - ataki typu pass the hash (374)
 - o SSHExec (376)
 - o Tokeny personifikacji (377)
 - o Incognito (378)
 - o Moduł SMB Capture (379)
- Pivoting (382)
 - o Dodawanie tras za pomocą polecenia route (384)
 - o Skanery portów w pakiecie Metasploit (384)
 - o Wykorzystywanie luk w zabezpieczeniach za pośrednictwem pivota (385)
 - o Moduł Socks4a i program ProxyChains (386)
- Utrzymywanie dostępu do skompromitowanego systemu (388)
 - o Tworzenie nowego konta użytkownika (388)
 - o Zapewnianie dostępu za pomocą Metasploita (389)
 - o Tworzenie zadań cron w systemie Linux (391)
- Podsumowanie (392)

14. Testowanie aplikacji internetowych (393)

- Burp Proxy (394)
- Wstrzykiwanie kodu SQL (399)
 - o Testowanie podatności na wstrzykiwanie kodu (400)
 - o Wykorzystywanie podatności na ataki typu SQL Injection (401)
 - o Zastosowanie programu SQLMap (402)
- Wstrzykiwanie kodu XPath (403)
- Ataki typu LFI - Local File Inclusion (405)
- Ataki typu RFI - Remote File Inclusion (408)
- Wykonywanie poleceń (409)
- Ataki typu XSS - Cross Site Scripting (411)
 - o Sprawdzanie podatności na ataki typu reflected XSS (412)
 - o Przeprowadzanie ataków typu XSS za pomocą pakietu Browser Exploitation Framework (BeEF) (414)
- Ataki typu CSRF - Cross-Site Request Forgery (418)
- Skanowanie aplikacji internetowych za pomocą programu w3af (419)
- Podsumowanie (421)

15. Ataki na sieci bezprzewodowe (423)

- Przygotowania (423)
 - o Wyświetlanie listy dostępnych bezprzewodowych interfejsów sieciowych (425)
 - o Wyszukiwanie bezprzewodowych punktów dostępowych (425)
- Tryb monitora (426)
- Przechwytywanie pakietów (427)
- Sieci bezprzewodowe z otwartym dostępem (428)

- Protokół WEP (428)
 - o Słabości protokołu WEP (431)
 - o Łamanie kluczy szyfrowania WEP za pomocą pakietu Aircrack-ng (432)
- Protokół WPA - WiFi Protected Access (437)
- Protokół WPA2 (438)
 - o Podłączanie klientów w sieciach WPA/WPA2 Enterprise (438)
 - o Podłączanie klientów w sieciach WPA/WPA2 Personal (439)
 - o Czteroetapowa negocjacja uwierzytelniania (439)
 - o Łamanie kluczy szyfrowania WPA/WPA2 (440)
- Protokół WPS - WiFi Protected Setup (444)
 - o Problemy z protokołem WPS (445)
 - o Łamanie PIN-u protokołu WPS za pomocą programu Bully (445)
- Podsumowanie (445)

IV. TWORZENIE EXPLOITÓW

16. Przepełnienie bufora na stosie w systemie linux (449)

- Kilka słów o pamięci (450)
- Przepełnienie bufora na stosie w systemie Linux (453)
 - o Program podatny na przepełnienie bufora na stosie (454)
 - o Wymuszanie awarii programu (456)
 - o Praca z debuggerem GDB (457)
 - o Wywoływanie awarii programu w debuggerze GDB (463)
 - o Kontrolowanie wskaźnika EIP (465)
 - o Przejmowanie kontroli nad działaniem programu (467)
 - o Kolejność (starszeństwo) bajtów (469)
- Podsumowanie (471)

17. Przepełnienie bufora na stosie w systemie Windows (473)

- Wyszukiwanie znanych podatności i luk w zabezpieczeniach serwera War-FTP (474)
- Wymuszanie awarii programu (476)
- Lokalizowanie rejestru EIP (479)
 - o Wyszukiwanie offsetu adresu powrotu za pomocą cyklicznego wzorca (480)
 - o Weryfikacja znalezionych offsetów (484)
- Przejmowanie kontroli nad działaniem programu (486)
- Uruchomienie powłoki (492)
- Podsumowanie (498)

18. Zastępowanie strukturalnej obsługi wyjątków (499)

- Exploity nadpisujące procedury SEH (500)
- Przekazywanie sterowania do procedur SEH (506)
- Wyszukiwanie ciągu znaków exploita w pamięci (506)
- POP POP RET (511)
- SafeSEH (512)
- Zastosowanie krótkich skoków (516)
- Wybieranie ładunku (517)
- Podsumowanie (520)

19. Fuzzing, przenoszenie kodu exploitów i tworzenie modułów Metasploita (521)

- Fuzzowanie programów (522)
 - Wyszukiwanie błędów poprzez analizę kodu źródłowego (522)
 - Fuzzowanie serwera TFTP (523)
 - Próba wywołania awarii programu (525)
- Dostosowywanie kodu publicznie dostępnych exploitów do własnych potrzeb (529)
 - Wyszukiwanie adresu powrotu (532)
 - Zamiana kodu powłoki (533)
 - Edytowanie kodu exploita (533)
- Tworzenie nowych modułów Metasploita (535)
 - Tworzenie podobnego modułu exploita (538)
 - Tworzenie kodu naszego exploita (538)
- Techniki zapobiegania atakom (543)
 - Technika Stack Cookies (543)
 - Mechanizm ASLR - randomizacja układu przestrzeni adresowej (544)
 - Mechanizm DEP - zapobieganie wykonywaniu danych (545)
 - Obowiązkowe cyfrowe podpisywanie kodu (545)
- Podsumowanie (546)

V. ATAKI NA URZĄDZENIA MOBILNE

20. Pakiet Smartphone Pentest Framework (549)

- Wektory ataków na urządzenia mobilne (550)
 - Wiadomości tekstowe (550)
 - Połączenia NFC (551)
 - Kody QR (552)
- Pakiet Smartphone Pentest Framework (552)
 - Konfiguracja pakietu SPF (552)
 - Emulatory systemu Android (554)
 - Dołączanie urządzeń mobilnych (555)
 - Budowanie aplikacji SPF dla systemu Android (555)
 - Instalowanie aplikacji SPF (556)
 - Łączenie serwera SPF z aplikacją mobilną (557)
- Ataki zdalne (559)
 - Domyślne poświadczenia logowania SSH na telefonach iPhone (559)
- Ataki po stronie klienta (561)
 - Powłoka po stronie klienta (561)
 - Zdalna kontrola nad urządzeniami mobilnymi za pomocą mechanizmu USSD (563)
- Złośliwe aplikacje (565)
 - Tworzenie złośliwych agentów SPF (566)
- Powłamaniowa eksploracja urządzeń mobilnych (573)
 - Zbieranie informacji (573)
 - Zdalne sterowanie (575)
 - Pivoting z wykorzystaniem urządzeń mobilnych (575)
 - Podnoszenie uprawnień (582)
- Podsumowanie (583)

Materiały dodatkowe (585)

Skorowidz (591)

Pobieranie oprogramowania dla środowiska testowego (608)