

**Cyberbezpieczeństwo dla zaawansowanych : skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze / Cesar Bravo.
– Gliwice, © 2023**

Spis treści

O autorze	15
O recenzentach	16
Przedmowa	17
Wstęp	19
Część 1. Doskonalenie technik obrony. Podstawy teoretyczne	23
Rozdział 1. Przypomnienie pojęć związanych z cyberbezpieczeństwem	25
Wymagania techniczne	26
Nurkujemy w samo sedno cyberbezpieczeństwa	26
Triada cyberbezpieczeństwa Rodzaje ataków	26
Zarządzanie legendarnym słabym punktem w cyberbezpieczeństwie — hasła	28
Zdekonspirowane hasła	36
Ataki inżynierii społecznej z wykorzystaniem wykradzonych haseł	38
Ataki siłowe	39
Ataki słownikowe	40
Tworzenie bezpiecznego hasła	41
Zarządzanie hasłami na poziomie przedsiębiorstwa	43
Dodatek	45
Doskonalenie obrony w głąb	46
Czynniki, które należy wziąć pod uwagę przy tworzeniu modeli DiD	46
Identyfikacja aktywów	48
Obrona dzięki warstwom	49
Dodatek	53
Drużyny: niebieskich i czerwonych — porównanie	53
Podsumowanie	56
Lektura uzupełniająca	56
Rozdział 2. Zarządzanie zagrożeniami, podatności i ryzyko	57
Wymagania techniczne	58
Zrozumienie podatności i zagrożeń związanych z cyberbezpieczeństwem	58
Przeprowadzenie oceny podatności na zagrożenia	58
Proces oceny zagrożeń	59

Kiedy należy wykonać sprawdzenie pod kątem podatności?	61
Rodzaje podatności	61
Podatności w zabezpieczeniach USB HID	66
Rodzaje ataków USB HID	67
Fałszywe poczucie bezpieczeństwa	72
Ochrona przed atakami USB HID	75
Zarządzanie ryzykiem związanym z cyberbezpieczeństwem	78
Identyfikacja ryzyka	79
Ocena ryzyka	80
Reakcja na ryzyko	82
Monitorowanie ryzyka	83
Ramy cyberbezpieczeństwa NIST	84
Identyfikacja	84
Ochrona	84
Wykrywanie	84
Reakcja	85
Przywracanie	85
Tworzenie skutecznego planu ciągłości działania (BCP)	86
Tworzenie analizy wpływu na biznes (BIA)	87
Planowanie ciągłości działania (BCP)	91
Wdrażanie najlepszego w swojej klasie DRP	95
Tworzenie DRP	95
Wdrażanie DRP	96
Podsumowanie	98
Lektura uzupełniająca	98
Rozdział 3. Zasady, procedury, zgodność i audyty	100
Tworzenie światowej klasy zasad i procedur dotyczących cyberbezpieczeństwa	101
Zasady związane z cyberbezpieczeństwem	101
Procedury związane z cyberbezpieczeństwem	102
Metoda CUDSE	103
Zrozumienie i osiągnięcie zgodności	108
Rodzaje regulacji	108
Osiągnięcie zgodności	110
Eksplorowanie, tworzenie audytów i zarządzanie nimi	113
Wewnętrzne audyty cyberbezpieczeństwa	114
Zewnętrzne audyty bezpieczeństwa cybernetycznego	114
Zarządzanie danymi podczas audytów	115
Rodzaje audytów cyberbezpieczeństwa	117
Kiedy przeprowadzać audyt?	120
Zastosowanie CMM	120
Cele CMM	120
Charakterystyka dobrego CMM	120
Struktura dobrego CMM	121
Analizowanie rezultatów	123

Zalety CMM	124
Podsumowanie	125
Lektura uzupełniająca	125
Rozdział 4. Łatanie ósmej warstwy	126
Warstwa 8 — zagrożenie wewnętrzne	127
Działanie nieumyślne	127
Szkodliwy użytkownik	128
Jak rozpoznać wewnętrznego szkodnika?	129
Ochrona infrastruktury przed wewnętrznymi szkodnikami	130
Doskonalenie sztuki inżynierii społecznej	136
Przebieg ataku w inżynierii społecznej	137
Socjotechniki	138
Rodzaje ataków wykorzystujących inżynierię społeczną	140
Obrona przed atakami socjotechnicznymi (łatanie warstwy 8)	152
Tworzenie strategii szkoleń	153
Prawa administratora	153
Wdrożenie silnej zasady BYOD	154
Przeprowadzanie losowych ataków inżynierii społecznej	154
Podsumowanie	155
Lektura uzupełniająca	155
Rozdział 5. Technologie i narzędzia w cyberbezpieczeństwie	156
Wymagania techniczne	157
Zaawansowane narzędzia bezprzewodowe dla cyberbezpieczeństwa	157
Obrona przed atakami bezprzewodowymi	157
Narzędzia i metody testów penetracyjnych	163
Metasploit	163
Zestaw narzędzi do inżynierii społecznej	164
exe2hex	168
Stosowanie narzędzi i metod kryminalistycznych	168
Postępowanie z dowodami	169
Narzędzia kryminalistyczne	169
Odzyskiwanie skasowanych plików	173
Jak sobie radzić z APT?	174
Techniki obrony	175
Systemy inteligentnego wykrywania zagrożeń w podnoszeniu poziomu cyberbezpieczeństwa	176
Inteligentne wykrywanie zagrożeń — podstawy	176
Wdrażanie systemu inteligentnego wykrywania zagrożeń	177
Przekształcenie zagrożenia w rozwiązanie	178
Problem	179
Rozwiązanie	179
Podsumowanie	179
Lektura uzupełniająca	180

Rozdział 6. Zabezpieczanie infrastruktury działającej pod kontrolą systemów Windows**183**

Wymagania techniczne	184
Utwardzanie systemu Windows w praktyce	184
Utwardzanie przez zespół ds. infrastruktury	184
Tworzenie listy kontrolnej dla procedur utwardzania	185
Tworzenie strategii instalowania łatek	190
Złożoność łatania	190
Rozdzielanie zadań (łatanie ról i przydziałów)	192
Dystrybucja i wdrażanie poprawek	193
Rodzaje łatek	195
Zabezpieczanie AD w praktyce	198
Bezpieczne hosty administracyjne	200
Dokumentacja dotycząca bezpieczeństwa systemu Windows Server	201
Zabezpieczanie końcówek — stacji roboczych	201
Aktualizacje systemu Windows	201
Dlaczego warto przejść na Windows 10?	201
Bezpieczeństwo fizyczne	202
Programy antywirusowe	203
Zapora ogniowa Windows Defender	203
Kontrola aplikacji	204
Filtrowanie adresów URL	204
Filtrowanie spamu	205
Systemy, do których ma dostęp klient	205
Kopie zapasowe	206
Użytkownicy	206
Zabezpieczanie danych	207
Wykorzystanie szyfrowania	207
Konfiguracja programu BitLocker	208
Podsumowanie	208

Rozdział 7. Utwardzanie serwera Unix**209**

Wymagania techniczne	210
Zabezpieczanie usług uniksowych	210
Określ przeznaczenia serwera	210
Skonfiguruj bezpieczny rozruch	211
Zarządzanie usługami	211
Uprawnienia do plików w praktyce	215
Zrozumienie pojęcia „właściciel” i uprawnień	215
Domyślne uprawnienia	218
Uprawnienia w katalogach (folderach)	219
Zmiana domyślnych uprawnień za pomocą umask	220
Hierarchia uprawnień	221
Porównywanie uprawnień do katalogów	222

Zmiana uprawnień i własności pojedynczego pliku	222
Przydatne polecenia do wyszukiwania niechcianych uprawnień	223
Zwiększenie ochrony serwera poprzez ulepszenie kontroli dostępu	224
Przeglądanie ACL	224
Zarządzanie listami ACL	225
Domyślne ACL dla katalogów	225
Usuwanie list ACL	226
Rozszerzona kontrola dostępu	227
Konfiguracja zapory sieciowej	228
Zrozumieć iptables	228
Konfigurowanie iptables	229
Ochrona SSH przed atakami siłowymi przy użyciu iptables	232
Ochrona przed skanowaniem portów za pomocą iptables	233
Zaawansowane zarządzanie dziennikami	233
Wykorzystanie logów	234
Podsumowanie	235
Lektura uzupełniająca	235
Rozdział 8. Zwiększ swoje umiejętności obrony sieci	236
Wymagania techniczne	237
Wykorzystanie eksperckiego narzędzia mapowania sieci — Nmap	237
Fazy cyberataku	238
Nmap	239
Skrypty Nmap	242
Lepsza ochrona sieci bezprzewodowych	246
Podatności w zabezpieczeniach sieci bezprzewodowych	246
Instrukcja bezpieczeństwa użytkownika dla sieci bezprzewodowych	250
Wprowadzenie do programu Wireshark	255
Namierzanie użytkowników korzystających z niezabezpieczonych protokołów	258
FTP, HTTP i inny, nieszyfrowany ruch	263
Wykorzystanie Wiresharka do obrony	264
Praca z IPS i IDS	265
Co to jest IDS?	265
Co to jest IPS?	266
Bezpłatny system IDS/IPS	267
IPS a IDS	267
Podsumowanie	268
Rozdział 9. Nurkujemy w zabezpieczenia fizyczne	269
Wymagania techniczne	270
Zrozumienie zabezpieczeń fizycznych i związanych z nimi zagrożeń	270
Potężny LAN Turtle	270
Podstępny Plunder Bug LAN Tap	271
Niebezpieczny Packet Squirrel	272
Przenośny Shark Jack	273

Niesamowity Screen Crab	273
Zaawansowany Key Croc	275
Zagrożenia związane z USB	276
Kradzież sprzętu	277
Zagrożenia środowiskowe	278
Fizyczne mechanizmy zabezpieczeń	278
Doskonalenie zabezpieczeń fizycznych	280
Zasada czystego biurka	280
Przeglądy zabezpieczeń fizycznych	281
Podsumowanie	282
Lektura uzupełniająca	282

Rozdział 10. Zabezpieczenia IoT w praktyce **283**

Wymagania techniczne	284
Zrozumieć internet rzeczy	284
Ryzyko	285
Podatności	286
Zrozumienie technologii sieciowych w IoT	287
LoRaWAN	287
Zigbee	288
Sigfox	289
Bluetooth	290
Uwagi dotyczące bezpieczeństwa	291
Poprawa bezpieczeństwa IoT	292
Tworzenie sprzętu wspomagającego cyberbezpieczeństwo z wykorzystaniem IoT	295
Wykrywanie fałszywych punktów dostępu	295
Ściana ogniowa i system wykrywania włamań na Raspberry Pi	298
Systemy obrony dla przemysłowych systemów sterowania (SCADA)	299
Bezpieczne kopiowanie z USB na USB	299
Tworzenie przynęty za grosze	300
Zaawansowane monitorowanie aplikacji internetowych i sieci	302
Tworzenie urządzenia blokującego reklamy internetowe	303
Kontrola dostępu i systemy fizycznych zabezpieczeń	303
Dodatkowe informacje: niebezpieczeństwo związane z nieautoryzowanymi urządzeniami IoT	304
Wykrywanie nieautoryzowanych urządzeń IoT	304
Wykrywanie Raspberry Pi	304
Wyłączanie fałszywych urządzeń Raspberry Pi	305
Podsumowanie	306
Lektura uzupełniająca	306

Rozdział 11. Bezpieczne wytwarzanie i wdrażanie oprogramowania w środowisku chmury **307**

Wymagania techniczne	308
Bezpieczna implementacja i wdrożenie aplikacji w chmurze	308

Bezpieczeństwo w różnych modelach chmury	308
Bezpieczeństwo danych w chmurze	310
Zabezpieczanie Kubernetes i API	313
Zabezpieczenia typowe dla chmury	313
Kontrola dostępu do interfejsu API Kubernetes	314
Kontrola dostępu do kubeletu	314
Zapobieganie ładowaniu niepożądanych modułów jądra przez kontenery	314
Ograniczenie dostępu do etcd	315
W systemach produkcyjnych unikaj korzystania z funkcji będących w wersjach alfa lub beta	315
Integracje z elementami innych producentów	315
Zabezpieczanie usług baz danych	316
Testowanie bezpieczeństwa chmury	317
Centrum zabezpieczeń Azure	318
Amazon CloudWatch	318
AppDynamics	319
Nessus — skaner podatności	320
InsightVM	320
Intruder	321
Podsumowanie	322
Lektura uzupełniająca	322

Rozdział 12. Bezpieczeństwo aplikacji internetowych **323**

Wymagania techniczne	324
Zbieranie informacji o Twojej witrynie/aplikacji internetowej	324
Znaczenie gromadzenia publicznie dostępnych danych	325
Wywiad z wykorzystaniem publicznie dostępnych źródeł	325
Informacje o hostingu	327
Sprawdzanie ekspozycji danych za pomocą Google hacking (dorki)	329
Wykorzystanie DVWA	331
Instalacja DVWA na Kali Linux	332
Przegląd najczęstszych ataków na aplikacje internetowe	336
Badanie ataków XSS	336
Korzystanie z pakietu Burp Suite	338
Wersje Burp Suite	338
Konfiguracja Burp Suite na Kali	339
Atak typu wstrzyknięcie SQL na DVWA	340
Naprawienie często występującego błędu	346
Atak siłowy na hasła w aplikacjach internetowych	347
Analiza wyników	350
Podsumowanie	351
Lektura uzupełniająca	352

Część III. Wypływamy na szerokie wody obrony **353**

Rozdział 13. Narzędzia do oceny podatności **355**

Wymagania techniczne	356
Radzenie sobie z podatnościami	356
Kto powinien szukać podatności?	356
Programy nagród za znalezione błędy	356
Wewnętrzne podatności	357
Narzędzia do badania podatności	358
Użycie skanera podatności (OpenVAS)	360
Testy z uwierzytelnieniem	360
Instalacja OpenVAS	361
Używanie OpenVAS	363
Aktualizowanie swoich kanałów	366
Skaner Nexpose	367
Podsumowanie	369
Lektura uzupełniająca	369

Rozdział 14. Analiza złośliwego oprogramowania 370

Wymagania techniczne	371
Dlaczego warto analizować złośliwe oprogramowanie?	371
Funkcjonalność złośliwego oprogramowania	371
Cele złośliwego oprogramowania	371
Z kim i z czym łączy się złośliwe oprogramowanie	372
Zostawianie furtek	373
Narażone systemy	373
Rodzaje i kategorie analizy złośliwego oprogramowania	373
Statyczna analiza złośliwego oprogramowania	373
Dynamiczna analiza złośliwego oprogramowania	374
Hybrydowa analiza złośliwego oprogramowania	374
Analiza właściwości statycznych	375
Interaktywna analiza zachowania	375
Analiza w pełni zautomatyzowana	375
Inżynieria wsteczna kodu	376
Najlepsze narzędzia do analizy złośliwego oprogramowania	376
Process Explorer	377
Process Monitor	377
ProcDOT	378
Ghidra	379
PeStudio	379
Przeprowadzanie analizy złośliwego oprogramowania	379
Zasady bezpieczeństwa	380
Przeprowadzamy analizę	381
Podsumowanie	384
Lektura uzupełniająca	384

Rozdział 15. Wykorzystanie testów penetracyjnych w taktykach obrony 385

Wymagania techniczne	386
----------------------	-----

Zrozumienie znaczenia dzienników	386
Pliki dzienników	386
Zarządzanie dziennikami	387
Dlaczego zadbanie o dzienniki jest ważne	388
Poznaj najlepszego przyjaciela swojego przeciwnika — Metasploit	389
Metasploit	390
Wersje frameworka Metasploit	391
Instalacja Armitage	391
Konfiguracja frameworka Metasploit po raz pierwszy	392
Instalacja Armitage (ciąg dalszy)	393
Eksploracja Armitage	394
Rozpoczęcie ataku z Armitage	396
Uruchamianie frameworka Metasploit	400
Inne hakerskie narzędzia do przeprowadzania ataków	403
Searchsploit	404
sqlmap	405
Weevely	405
Podsumowanie	409
Lektura uzupełniająca	410
Rozdział 16. Informatyka śledcza w praktyce	411
Wprowadzenie do kryminalistyki cyfrowej	412
Techniki śledcze w odzyskiwaniu usuniętych lub brakujących danych	412
Metody i techniki kryminalistyki cyfrowej w zabezpieczaniu infrastruktury	416
Kto powinien zajmować się cyfrową kryminalistyką?	416
Proces cyfrowej kryminalistyki	417
Platformy kryminalistyczne	418
CAINE	418
Stacja robocza SIFT	419
PALADIN	420
Znalezienie dowodów	421
Źródła danych	421
Kryminalistyka urządzeń mobilnych	422
Dochodzenie bez urządzenia	423
Ważne źródła danych na urządzeniach mobilnych	425
Transportowanie urządzeń mobilnych	426
Zarządzanie materiałem dowodowym (z perspektywy prawnej)	426
ISO 27037	427
Podręcznik polityki i procedur dotyczących dowodów cyfrowych	427
Przewodnik po polityce FBI dotyczącej dowodów cyfrowych	427
Regionalne Laboratorium Informatyki Śledczej	428
Amerykańska Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury	428
RFC 3227 — wytyczne dotyczące gromadzenia i archiwizacji dowodów	428
Podsumowanie	428
Lektura uzupełniająca	429

Rozdział 17. Automatyzacja zadań związanych z cyberbezpieczeństwem	430
Po co zawracać sobie głowę automatyzacją?	431
Korzyści z automatyzacji	431
Ryzyko związane z ignorowaniem automatyzacji	431
Rodzaje automatycznych ataków	432
Gromadzenie kont	432
Tworzenie kont	432
Oszustwo reklamowe	432
Porażka CAPTCHA	433
Rozszyfrowywanie kart	433
Carding	433
Wypłata gotówki	433
Łamanie danych uwierzytelniających	434
Faszerowanie danymi uwierzytelniającymi	434
Odmowa z magazynu	434
DoS	434
Przyspieszanie	435
Zbieranie odcisków palców	435
Tropienie	435
Scalping	436
Strzał z ukrycia	436
Zbieranie	436
Wypaczanie	436
Spamowanie	436
Rozgryzanie tokenów	437
Skanowanie podatności	437
Automatyzacja narzędzi cyberbezpieczeństwa z wykorzystaniem języka Python	437
Lokalne wyszukiwanie plików	437
Podstawowe zadania kryminalistyki cyfrowej	439
Zbieranie danych ze stron internetowych	441
Automatyzacja zabezpieczania sieci	442
Automatyzacja zadań związanych z cyberbezpieczeństwem z Raspberry Pi	443
Automatyzacja systemu inteligentnego zbierania informacji za pomocą przynęty Fail2ban na Raspberry Pi	444
Zautomatyzowany system monitorowania internetu za pomocą Raspberry Pi	445
Podsumowanie	447
Lektura uzupełniająca	447
Rozdział 18. Kompilacja narzędzi eksperta. Przydatne zasoby	448
Darmowe szablony dotyczące cyberbezpieczeństwa	449
Szablony planu ciągłości działania i planu odzyskiwania po awarii	449

Zarządzanie ryzykiem	449
Projektowanie i zarządzanie zasadami i procedurami dotyczącymi cyberbezpieczeństwa	450
Niezbędne zasoby internetowe	450
Mapy zagrożeń cybernetycznych lub ataków cyfrowych	451
Certyfikaty w dziedzinie cyberbezpieczeństwa	452
Wiadomości i błogi dotyczące cyberbezpieczeństwa	453
Narzędzia w cyberbezpieczeństwie	453
Narzędzia związane z hasłami	454
Wiodące najlepsze praktyki branżowe	454
Przepisy i normy	454
Ramy, standardy i inne elementy bezpieczeństwa cybernetycznego	455
Podsumowanie	456
Lektura uzupełniająca	456
Skorowidz	457

oprac. BPK