

Spis treści

Wstęp	21
<i>Michał Sajdak</i>	
Wprowadzenie do cyberoperacji i cyber wojny	25
<i>Lukasz Olejnik</i>	
Cyber wojna – wprowadzenie	27
Cyber atak – model myślowy	29
Cyber operacje	31
Konflikt zbrojny, cyber wojna	32
Cyberatak to nie atak – i co z tego wynika	34
Mierzenie efektów cyber operacji	36
Ranga, wpływ działania	36
Czteropunktowa skala wpływu	37
Podstawowe zasady międzynarodowego prawa humanitarnego	39
Zasada rozróżnienia	40
Zasada proporcjonalności	40
Zasada ostrożności	40
Kiedy, działając w cyberprzestrzeni, cywil staje się nieuprawnionym bojownikiem	41
Podstawowe zasady IHL w kontekście technicznym	42
Rozróżnienie	42
Unikanie absurdów	43
Sygnały ochronne	45
Proporcjonalność i ostrożność	47
Przykład naruszenia – NotPetya	48
Targeting	48
Przykłady koncepcyjne	49
Technika deszyfracji payloadu na podstawie informacji w systemie	50
Wykonanie czynności tylko na maszynie z określonym adresem MAC	51
Podsumowanie	52
Analiza techniczna wybranych cyberoperacji i cybernarzędzi w kontekście IHL	53
Stuxnet	53
Gauss	54
ShadowHammer	54
SolarWinds	55
XZ	56
Viasat	56
Ivanti	57
Podsumowanie	58
Dalsze poszerzanie wiedzy	59

Podstawy bezpieczeństwa Windows – systemy serwerowe	65
<i>Grzegorz Tworek</i>	
Wstęp	67
Specyfika serwerów Windows	67
Najpoważniejsze zagrożenia	68
Higiena tożsamości	69
Zdalny dostęp	72
Bezpieczeństwo protokołu RDP	75
Zarządzanie aktualizacjami	78
Bezpieczeństwo serwisów systemowych	80
Przykład z życia	81
Bezpieczeństwo sieciowe	82
Scentralizowane zarządzanie	84
Ochrona kontrolerów domeny	87
Lista dozwolonych aplikacji	88
Monitorowanie serwerów	89
Obsługa incydentów	91
Studium przypadku	93
Podsumowanie	95
Dalsze poszerzanie wiedzy	95
Podstawy bezpieczeństwa Windows – systemy klienckie	99
<i>Grzegorz Tworek</i>	
Wstęp	101
Aktualizacje	101
Ochrona antywirusowa	104
Lokalne prawa administratora	105
Niedostateczne uprawnienia dla konkretnych obiektów	106
Stacja robocza administratora systemu	107
Uwierzytelnianie	108
Instalacja systemów	110
BitLocker – szyfrowanie	111
Sysmon – rejestrowanie zdarzeń	113
Hardening systemów	114
Podsumowanie	116
Dalsze poszerzanie wiedzy	116
Bezpieczeństwo Active Directory	119
<i>Robert Przybylski</i>	
Wstęp	121
Dla kogo jest ten rozdział	122
Czym jest Active Directory	123
Architektura Active Directory	124
Funkcje Active Directory	127
Zastosowanie Active Directory	128
Metody analizy bezpieczeństwa Active Directory	129
Moduł ADHealthCheck	130

Techniki zabezpieczania Active Directory	132
Tiering	132
Struktura tieringu	133
Wdrażanie tieringu	136
Przygotowanie jednostek organizacyjnych OU	137
Przygotowanie grup zabezpieczeń	142
Delegowanie uprawnień do jednostek organizacyjnych OU	144
Wdrażanie stacji administracyjnej PAW	147
Zasady grupy (GPO)	147
Implementacja zasad grupy (GPO)	149
Polityki audytowania dla kontrolerów domeny	152
Referencyjne polityki bezpieczeństwa	155
Zarządzanie kontami lokalnych administratorów	157
Authentication Policy	162
Dodatkowe techniki	165
Protected Users Group	166
Restricted Admin Mode	167
Zasady grupy zezwalające na wyłączenie kontrolerów domeny	170
Wyłączanie serwisu Print Spooler	172
Włączanie kosza Active Directory	172
Blokowanie możliwości dodawania komputerów do domeny	173
Czyszczenie grup administracyjnych	173
Blokowanie opcji delegowania konta	174
Resetowanie hasła konta krbtgt	175
Konto dostępu awaryjnego	176
Podsumowanie	179
Dalsze poszerzanie wiedzy	179

Bezpieczeństwo Entra ID

Robert Przybylski

Wstęp	185
Dla kogo jest ten rozdział	185
Słownik pojęć	186
Czym jest Entra ID	188
Synchronizacja Active Directory do Entra ID	190
Microsoft Entra Connect	190
Microsoft Entra Cloud Sync	192
Porównanie narzędzi synchronizacyjnych	194
Sposoby analizy bezpieczeństwa Entra ID	194
Moduł AADSecurity	195
Sposoby zabezpieczenia Entra ID	197
Podstawowe sposoby zabezpieczenia Entra ID	198
Ustawienia użytkowników	198
Ustawienia grup	200
Ustawienia aplikacji	200
Ustawienia Entra ID	202
Zabezpieczenie synchronizacji Active Directory i Entra ID	204
Konfiguracja konta synchronizacji w Active Directory	205
Konfiguracja konta serwisowego do uruchomienia serwisu	205

Konfiguracja konta synchronizacji w Entra ID	206
Konfiguracja obiektów objętych synchronizacją	206
Dostęp warunkowy	207
Dostęp bezhasłowy	208
Konta dostępu awaryjnego	214
Zarządzanie kontami uprzywilejowanymi	215
Wdrażanie Identity Protection	219
Wdrażanie Privileged Identity Management (PIM)	220
Ustawienia referencyjne	223
CIS WorkBench	224
Podsumowanie	225
Dalsze poszerzanie wiedzy	225

Linux – zabezpieczanie i utwardzanie konfiguracji 229

Karol Szafranski

Wstęp	231
Po co utwardzać system	233
Podstawowe zasady hardeningu	233
Sprzęt i instalacja systemu a bezpieczeństwo	235
Jak zaplanować bezpieczną instalację	235
Nośniki instalacyjne, czyli jak nie pobrać instalatora z trojanem	236
Weryfikacja podpisu ISO instalacyjnego	237
Profile bezpieczeństwa (CIS, STIG, FIPS)	242
Układ partycji/woluminów logicznych	243
Szyfrowanie dysków	244
Zmiana hasła LUKS	246
Secure Boot w środowisku linuksowym	246
Źródła i aktualność oprogramowania	248
Po co te wszystkie aktualizacje	248
Okres wsparcia dystrybucji	249
Różne źródła programów i ich wpływ na bezpieczeństwo	251
Pakiety z repozytoriów DEB/RPM a bezpieczeństwo	253
Repozytoria dodatkowe – z czego korzystać, a czego unikać	254
Serwery lustrzane i podpisy cyfrowe	256
Bezpieczeństwo pojedynczych pakietów .deb i .rpm	257
Bezpieczeństwo oprogramowania z innych źródeł	258
Aktualizacje automatyczne dla „małych i prostych” systemów	259
Co należy odinstalować?	260
Konta, użytkownicy, uprawnienia	261
Linuksowy model uprawnień – przypomnienie	261
Zapis uprawnień w postaci literowej	262
Postać numeryczna uprawnień	263
Uprawnienia w praktyce: przykłady i problemy	263
„Ślepe przejście” przez katalog	263
Pliki wykonywalne a <i>setuid</i> (u+s) i <i>setgid</i> (g+s)	264
Uprawnienia nowo tworzonych plików: <i>umask</i> , <i>setgid</i> na katalogu	265
Czy można kasować cudze pliki? Czyli o <i>sticky bit</i>	267
Nadawanie uprawnień, zmiana właściciela – czy rozumiesz, co robisz?	267
Mechanizm ACL: listy kontroli dostępu	268

Atrybuty (<i>lsattr</i> , <i>chattr</i>)	270
<i>Capabilities</i>	271
Użytkownicy i grupy	272
Systemowa baza kont	272
Zarządzanie kontami: kwestie praktyczne	274
Okresy ważności i blokowanie kont	274
Powłoka konta	275
Grupy	275
Grupy dające podwyższone uprawnienia	276
Konta usług/systemowe	276
Usuwanie kont	277
<i>Sudo</i> i <i>su</i>	277
Pozornie bezpieczne: <i>sudo</i> a funkcjonalność narzędzi	279
Pozornie bezpieczne: symbole wieloznaczne w regułach	280
Program <i>su</i>	281
Bezpieczniejsze SSH	282
Zabezpieczanie serwera	282
Protokoły szyfrowania i klucze serwera	283
Zaufanie do klucza serwera	284
Ograniczanie uprawnień kont i grup	285
Blokada/zezwolenie na logowanie kont i grup	285
Selektywne ograniczanie uprawnień kont i grup	285
Konta przeznaczone tylko do transferu plików (SFTP-only)	286
Tunele (forwardowanie połączeń)	286
Wyłączenie logowania hasłem dla konta root	290
SSH po stronie klienta – logowanie kluczami	290
Generowanie pary kluczy klienta na potrzeby uwierzytelnienia	290
Logowanie przy użyciu kluczy	292
Plik <i>authorized_keys</i>	293
Agent SSH	293
PuTTY i WinSCP a klucze i agent	294
MFA i klucze sprzętowe	294
Bezpieczna konfiguracja usług	295
Co i dlaczego działa w systemie?	295
<i>Systemd</i> i jego jednostki konfiguracyjne (<i>units</i>)	297
Sekrety na liście procesów	297
Jak bezpiecznie skonfigurować dowolną usługę	298
Lokalne SMTP	299
Synchronizacja czasu z użyciem protokołu NTP	300
Automatyczne uruchamianie zadań	301
<i>cron</i>	301
<i>atd</i>	302
Timery mechanizmu <i>systemd</i>	303
Edycja plików definicji usług <i>systemd</i>	304
Własny plik definicji dla nowej usługi	304
Dwa słowa o logach	305
Studium przypadku: historia jednego włamu	305
Firewall i ochrona warstwy sieciowej	306
Firewall na Linuksie, czyli co?	307
<i>iptables</i> (czyli <i>netfilter</i>)	307

<i>nftables</i> (czyli... <i>netfilter</i> wiele lat później)	308
Nakładki ułatwiające zarządzanie zaporą	308
Co powinna robić zapora?	309
Przykładowy zestaw reguł firewalla	310
Dwa słowa o blokowaniu ruchu ICMP	310
Automatyczne blokowanie ataków <i>brute-force</i>	311
Skanowanie własnego systemu	311
Mechanizmy bezpieczeństwa i ochrona jądra	312
Bootloader/bootmanager i parametry startowe jądra	312
Moduły i ich konfiguracja	313
Ważne ustawienia <i>sysctl</i>	314
Linux Security Modules: SELinux i inne	316
Mechanizmy izolacji aplikacji (<i>sandboxing</i>)	317
Mechanizm <i>ulimit</i>	318
<i>Fork bomb</i> w powłoce: jak się zabezpieczyć	319
Ochrona przed zapełnieniem systemu plików	319
Podsumowanie	320
Przydatne programy i usługi	320
Źródła informacji	321
Dalsze poszerzanie wiedzy	321

Bezpieczne architektury sieci 325

Piotr Wojciechowski

Wstęp	327
Model ISO/OSI	328
Enkapsulacja	331
Media transmisyjne	334
Rozgałęźniki sygnału	338
Adresacja w sieciach Ethernet i IP	339
Typy ruchu	341
Jak działa protokół ARP?	343
Protokoły TCP i UDP	345
Protokół MPLS	351
SAN	353
Segmentacja w sieciach	354
Porównanie IPv4 i IPv6	358
Wskazówki dotyczące segmentacji sieci	361
Spanning Tree	364
Routing i translacja adresów	366
Topologie sieci	369
<i>Point-to-point</i>	369
Topologie sieci – podstawowe schematy	370
<i>Point-to-multipoint</i>	371
<i>Star</i> (gwiazda)	371
<i>Ring</i> (pierścień)	371
<i>Mesh</i> (siatka)	371
Urządzenia sieciowe i ich rola	372
Switche	372
Koncentratory (huby)	373

Routery	375
Firewall	377
Reguły firewalli: model stref (Zone-Based Firewall, ZBFW) vs model CBAC	380
Intrusion Detection System (IDS) oraz Intrusion Prevention System (IPS)	381
Load balancer	382
VPN-y	382
Zasady projektowania bezpiecznej architektury sieci	385
Ochrona fizyczna	385
Klastrowanie i redundancja geograficzna	386
Zarządzanie	387
Bezpieczeństwo komunikacji	388
Wykrywanie awarii	388
Podział na strefy bezpieczeństwa	390
Chmura publiczna	393
Błędy łatwe do uniknięcia	394
Podsumowanie	398
Dalsze poszerzanie wiedzy	399

Bezpieczeństwo globalnego i lokalnego routingu IP

Lukasz Bromirski

Wstęp	409
Studium przypadku	409
BGP w pigułce	410
Słownik pojęć	415
Routing jako fundament Internetu	417
Studium przypadku: atak na BGP	417
Studium przypadku: atak na IGP	422
Logiczny podział ruchu	426
Warstwa kontrolna	427
Warstwa zarządzająca	429
Warstwa danych	430
Bezpieczeństwo procesów routingu i komunikacji między routerami	431
Ochrona protokołów routingu	431
Uwierzytelnianie	431
Weryfikacja pola TTL, czyli GTSM	434
Ochrona routingu przez segmentację	435
Kontrola informacji wymienianych w ramach sesji routingu	437
Podstawy: higiena routingu	437
Studium przypadku: logiczna weryfikacja informacji routingowej	438
Studium przypadku: bezpieczeństwo routingu międzydomenowego	439
Routing jako narzędzie bezpieczeństwa	444
Routing na podstawie informacji o ścieżce powrotnej (uRPF)	444
Remote Triggered BGP Blackholing	447
Remote Triggered BGP Sinkholing	454
Studium przypadku: BGP i FlowSpec	456
Atak i ochrona routingu w praktyce	459
Przejęcie prefiksu w OSPF	459
Przejęcie prefiksu w BGP	472
Podsumowanie	478
Dalsze poszerzanie wiedzy	479

Bezpieczeństwo sieci Wi-Fi	485
<i>Maciej Szymczak</i>	
Wstęp	487
Słownik	488
Architektury sieci Wi-Fi	490
Architektura sieci domowych	490
Bezpieczeństwo sieci domowych	490
Architektura sieci firmowych	492
Bezpieczeństwo sieci firmowych	493
Metody uwierzytelniania w WPA2-Enterprise	493
WPA2-PSK/WPA3-SAE w firmie	495
Sieci otwarte (WPA3)	495
Jak wygląda 4-way handshake w Wi-Fi?	495
Przygotowanie do ataków na sieci Wi-Fi	498
Rodzaje ataków	498
Ataki <i>online</i>	498
Ataki <i>offline</i>	498
Atakowanie innych warstw	499
Narzędzia niezbędne do przeprowadzenia testu bezpieczeństwa sieci Wi-Fi	499
Sprzęt	499
Oprogramowanie	499
Dobór narzędzi do testu bezpieczeństwa sieci	500
Atakowanie	501
Atakowanie sieci zabezpieczonej WPA2-PSK	501
Wifite	501
bettercap	504
PMK	508
Czy zawsze jest tak łatwo?	510
Sieci zabezpieczone WPA3-SAE	510
Atakowanie sieci zabezpieczonej WPA3-SAE (<i>personal</i>)	511
Atakowanie sieci zabezpieczonej WPA2-Enterprise (EAP-PEAP)	512
Atak <i>Evil Twin</i>	514
Narzędzia	515
Atak	515
Atakowanie sieci zabezpieczonej WPA2-Enterprise (EAP-TLS)	518
Ataki na urządzenia	519
FragAttacks	520
TP-Link: wykonanie kodu na punkcie dostępowym	520
Windows 10/11: wykonanie kodu na komputerze ofiary	520
Ataki na użytkowników	521
Monitoring bezpieczeństwa Wi-Fi	521
Na małą skalę	522
... i na dużą	522
Zabezpieczanie	522
Zabezpieczanie sieci domowej	523
Migracja z WPA2-PSK do WPA3-SAE	524
Zabezpieczanie sieci firmowej	524
Bezpieczeństwo sieci otwartych (<i>open</i>)	525
Podsumowanie	526
Dalsze poszerzanie wiedzy	526

Docker - wprowadzenie do bezpieczeństwa	529
<i>Kamil Jaroński</i>	
Wstęp	531
Dockerfile, obrazy, repozytoria i kontenery	532
Dockerfile	532
Budowanie obrazu	534
Repozytoria	538
Uruchamianie kontenera	538
Jak działa sieć?	539
Wolumeny i współdzielenie dysku hosta	541
Problemy z życia wzięte	543
Pamiętaj o gościach	543
Nieaktualne kontenery	544
Kontenery z uprawnieniami administratora	545
Płaska sieć	546
Brak ograniczeń zasobów	548
Uprawnienia R/W na plikach hosta	550
Dostęp do Docker API	551
(Nie)bezpieczne repozytorium obrazów	553
Podsumowanie	554
Dalsze poszerzanie wiedzy	555
 Architektura ARM bez tajemnic	559
<i>Mateusz Wójcik</i>	
Wstęp	561
Poznajemy architekturę ARM	561
Język assembly	563
Sposoby zapisu w pamięci: <i>little-endian</i> vs <i>big-endian</i>	564
Rejestry	565
Analiza kodu	566
Instrukcje warunkowe i skoki	568
Pętla while	571
Odczyt i zapis do pamięci	572
<i>Literal addressing mode</i>	573
Tablice	573
Stos	575
Funkcje	576
Co dalej?	577
Podsumowanie	578
Dalsze poszerzanie wiedzy	578
 Możliwości Ghidry - na przykładzie poszukiwania podatności OS Command Injection	581
<i>Mateusz Wójcik</i>	
Wstęp	583
Ghidra - podstawy	583
Cel	584
Konfiguracja	584
Listing	589

Dekompilator	590
Graf funkcji	590
Skrypty	593
Ghidra – praktyka	596
Plan działania	596
Wnioski	598
Budujemy warsztat	599
OS Command Injection Chain	602
Podsumowanie	610
Dalsze poszerzanie wiedzy	610
Uwierzytelnianie oraz systemy klasy IAM (Identity and Access Management)	613
<i>Paweł Łąka</i>	
Wstęp	615
Uwierzytelnianie	616
Czym jest uwierzytelnianie	617
Klasyfikacja metod uwierzytelniania użytkownika	619
Coś, co użytkownik wie	621
Coś, co użytkownik ma	623
To, kim użytkownik jest (biometria)	624
To, gdzie użytkownik jest	625
To, co użytkownik robi (uwierzytelnianie ciągłe)	626
Rozwiązania IAM (Identity and Access Management)	628
Architektura i klasyfikacja	630
Funkcjonalności IAM	635
Provisioning	635
Cykl życia (ang. <i>life cycle</i>)	636
Uprawnienia (ang. <i>entitlements</i>)	636
Assessment	637
Atestacja – recertyfikacja (ang. <i>access recertification, access attestation, entitlements review</i>)	637
Rozdzielenie obowiązków, SoD (Segregation of Duties)	638
Audytorowanie, raportowanie, analiza	638
Systemy PAM (Privileged Access Management)	639
Architektura i klasyfikacja PAM	639
Przykładowe zastosowania PAM	640
Zarządzanie sesjami	641
Zarządzanie hasłami	641
Monitoring (ang. <i>review</i>)	641
Role i grupy	641
Zatwierdzanie (ang. <i>approvals</i>)	642
Polityki bezpieczeństwa	642
Kiedy warto wdrażać PAM	642
Podsumowanie	643
Dalsze poszerzanie wiedzy	643

Wireshark – wprowadzenie	647
<i>Tomasz Turba</i>	
Wprowadzenie	649
Podstawowe pojęcia	649
Formaty plików	652
Filtrowanie BPF	654
Rodzaje filtrów, czyli różnice pomiędzy <i>capture</i> a <i>display</i>	654
Praca z dużą ilością danych	657
Instalacja	662
Pobieranie	662
Instalacja w systemie Windows	663
Instalacja w systemie Linux	665
Instalacja w systemie macOS	665
Pierwsze kroki z programem	666
Konfiguracja	668
Zmiany w interfejsie użytkownika	668
Tworzenie profili i układ interfejsu	668
Znaczniki czasu	670
Kolorowanie i wzorce	671
Rozwiązywanie nazw hostów	673
Dodatkowe kolumny	673
Funkcje dla zaawansowanych	674
Interpretacja statystyk	674
Analiza komunikacji VoIP	676
Możliwości deszyfrowania ruchu SSL	678
Analiza ruchu sieciowego smartfona	682
Skrypty Lua	684
Narzędzia pomocnicze	687
tshark	688
tcpdump	688
editcap	689
capinfos	690
Analizy przypadków	692
Analiza sieciowa dla administratorów	692
Scenariusz 1: Znaczne wykorzystanie pasma	692
Scenariusz 2: Analiza czasów odpowiedzi serwera	693
Scenariusz 3: Atak DDoS	694
Scenariusz 4: Ruch DNS	694
Scenariusz 5: Skanowanie portów	695
Scenariusz 6: Opóźnienie (ang. <i>jitter</i>) w sieci	696
Analiza sieciowa dla dewelopera	697
Scenariusz 1: Retransmisje TCP	697
Scenariusz 2: Utraczone segmenty TCP	698
Scenariusz 3: Zasyfrowany ruch SSL/TLS	699
Scenariusze 4–6: Analiza API REST, błędy, weryfikacja szyfrowania	699
Wykrycie malware'u w infrastrukturze	700
Wykrycie zagrożenia typu stealer	703
Wykrycie anomalii ataków	707

Podsumowanie	710
Dalsze poszerzanie wiedzy	711
Dokumentacja	711
Skrypty Lua	711
Problemy malware'u	711
Gdy wszystko zawiedzie	712
Monitorowanie zasobów IT za pomocą systemu Zabbix	715
<i>Arkadiusz Siczek</i>	
Wstęp	717
Instalacja Zabbixa	718
Konfiguracja serwera Zabbix	722
Metody monitorowania	725
Omówienie działania agenta Zabbix oraz jego połączenia	725
Jak to działa?	728
Konfiguracja maszyny	728
Panel główny aplikacji webowej: sekcja Monitoring	729
Dodawanie nowych elementów	733
Dodawanie czujek (items)	733
Wyzwalacze (triggers)	735
Media types (powiadomienia)	739
Akcje	740
Szablony	742
Opracowanie planu monitoringu	743
Określenie kluczowych zasobów i usług	743
Określenie poziomów alarmów	745
Konfiguracja monitoringu	746
Utrzymanie infrastruktury	749
Wykrywanie	749
Studium przypadku: reagowanie na alarm monitoringu	750
Scenariusz 1	750
Scenariusz 2	751
Przewidywanie awarii	751
Wykrywanie zagrożeń za pomocą Zabbixa	754
Wykrywanie nowych urządzeń w sieci	754
Tworzenie reguł Discovery	754
Wykrywanie innych zagrożeń w sieci	757
Podsumowanie	759
Baza danych	759
MySQL dla Zabbixa w pigułce	759
Automatyzacja	760
Wysoka dostępność	760
Powiadomienia i własne szablony	760
Szkolenie personelu	760
Dalsze poszerzanie wiedzy	760

Radia definiowane programowo w analizie bezpieczeństwa – praktyczny wstęp do SDR 763

Piotr Rzeszut

Dla kogo jest ten rozdział?	765
Na początek trochę teorii	767
Historia transmisji radiowej (w telegraficznym skrócie)	767
Rodzaje modulacji	768
Typowa konstrukcja nadajnika i odbiornika	770
Radio definiowane programowo – SDR	772
Obserwacja sygnałów w dziedzinie czasu i częstotliwości	774
Przepisy prawne to też źródło wiedzy	776
Warsztaty praktyczne	778
Przygotowanie środowiska i sprzętu	778
Universal Radio Hacker – pierwsze narzędzie na froncie	779
Budowa środowiska testowego dla transmisji 433 MHz	780
Rejestracja i analiza sygnału z pasma 433 MHz	782
Dekodowanie sygnału z pasma 433 MHz do postaci binarnej	786
Nadawanie sygnału i zmiana jego zawartości	789
Budowa środowiska testowego dla modułów nRF24L01 (2.4 GHz)	791
Rejestracja i analiza sygnałów z modułów nRF24L01	792
Dekodowanie sygnałów z modułów nRF24L01	795
Nadawanie sygnałów dla modułów nRF24L01	797
GNU Radio – oprogramowanie do zadań specjalnych	800
Krótki wstęp do obsługi GNU Radio	800
Rejestracja i demodulacja sygnałów z pasma 433 MHz	802
Przeprowadzenie prostego ataku typu <i>repeat</i> na system w paśmie 433 MHz	807
Demodulacja sygnału audio FM (radio FM)	809
Podsumowanie	810
Dalsze poszerzanie wiedzy	811
SDR widziane okiem prawnika	812