ETYCZNY HACKING

i testy penetracyjne

Krzysztof Godzisz

Zadbaj o bezpieczeństwo sieci LAN i WLAN

Helion

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą AdobeStock.com.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/siebel
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-289-3507-5

Printed in Poland.

Spis treści

Słowo wstępne — Adrian Kapczyński

Postęp techniczny w obszarze sieci przewodowych i bezprzewodowych otwiera dziś ogromne możliwości. Warto jednak pamiętać, że ta sama infrastruktura, która zapewnia wygodę i dostęp do informacji, jest także atrakcyjnym celem dla cyberprzestępców. Błędy w konfiguracji, przestarzałe standardy czy nieuważne decyzje administratorów stają się lukami, które mogą zostać wykorzystane do przeprowadzenia ataków. Cyberbezpieczeństwo przestało być domeną wyłącznie zamkniętych zespołów IT — stało się obowiązkiem każdego, kto odpowiedzialnie korzysta z technologii.

W tej książce autor skupia się na podstawach łamania i weryfikacji zabezpieczeń sieci WLAN oraz LAN. Czytelnik jest prowadzony od przygotowania własnego laboratorium testowego, przez zrozumienie mechanizmów sieciowych, aż po analizę konkretnych podatności. Cały materiał opiera się na zasadzie: „Uczę się atakować, by wiedzieć, jak skutecznie mogę się bronić". Chodzi nie o imponowanie wiedzą, lecz o zrozumienie ryzyka i umiejętność jego praktycznej oceny.

Materiał zaprezentowany w książce został podzielony na trzy części.

W pierwszej części autor prezentuje fundamenty warsztatu bezpieczeństwa LAN/WLAN. Pokazuje, jak stworzyć własne laboratorium testowe, dobrać sprzęt, skonfigurować środowisko wirtualne oraz przygotować niezbędne narzędzia. To kluczowy etap nauki, który uczy dyscypliny pracy w kontrolowanych warunkach, z dala od systemów produkcyjnych.

Druga część książki jest w całości poświęcona sieciom bezprzewodowym. Autor systematyzuje w niej wiedzę o bezpieczeństwie WLAN, podkreślając, że ochrona sieci to znacznie więcej niż silne hasło. Czytelnik dowie się m.in., dlaczego należy porzucić przestarzałe standardy oraz jak błędne przekonania o dodatkowych zabezpieczeniach mogą uśpić czujność. Autor stawia na zrozumienie mechanizmów, zamiast bezmyślnego powtarzania czynności administracyjnych.

Trzecia część książki koncentruje się na zagrożeniach typowych dla sieci LAN. Autor pokazuje, że bezpieczeństwo nie zależy od typu połączenia, lecz od widoczności urządzeń, segmentacji i higieny konfiguracji. Sieć staje się tu przestrzenią mierzalną — można ją rozpoznawać i diagnozować, a następnie formułować wnioski zrozumiałe także poza środowiskiem stricte technicznym.

Książka wyraźnie podkreśla znaczenie etyki. Pasja odkrywcy nie może przerodzić się w działanie poza prawem. Materiał należy traktować wyłącznie jako podręcznik do pracy w laboratorium lub do testów wykonywanych za wyraźną zgodą właściciela sieci. W świecie rzeczywistym problemem nie jest wiedza, lecz brak odpowiedzialności.

Układ treści sprzyja nauce krok po kroku — od instalacji narzędzi, przez teorię, po konkretne zastosowania. Krótkie rozdziały i duża dawka praktyki pozwalają zdobywać umiejętności we własnym tempie. Jestem przekonany, że lektura tej książki przyniesie wymierną wartość każdemu Czytelnikowi zainteresowanemu bezpieczeństwem sieci.

Owocnej lektury!

Adrian Kapczyński
1753c.io
Clearnet, styczeń 2026

Słowo wstępne — Dagmara Modrzejewska

Po wydanej w 2023 roku książce pt. *Laboratorium cyberbezpieczeństwa w Dockerze. Zrób to sam* wydawnictwa Helion Krzysztof Godzisz ponownie sięga po pióro, tym razem oferując czytelnikom praktyczny poradnik dotyczący parametryzowania sieci wewnętrznych (LAN) i sieci zewnętrznych (WAN). Efektem jest publikacja pt. *Etyczny hacking i testy penetracyjne. Zadbaj o bezpieczeństwo sieci LAN i WLAN*, w którą właśnie zaczynacie się Państwo zanurzać.

Książka stanowi solidną podstawę do tego, jak skutecznie, efektywnie i bezpiecznie budować infrastrukturę sieciową w organizacjach. Autor prezentuje wiedzę w sposób przystępny i jasny, oferując konkretne instrukcje i praktyczne wskazówki dotyczące parametryzowania architektury sieciowej.

Mam zaszczyt znać Krzysztofa osobiście i mogę z pełnym przekonaniem potwierdzić jego pasję do ICT i cyberbezpieczeństwa oraz zaangażowanie w dzielenie się wiedzą. Jego działalność w tym obszarze zasługuje na uznanie: jest konsekwentna, transparentna i realizowana z naturalną pasją od lat — zarówno w praktyce zawodowej, jak i w publikacjach.

Krzysztof wyróżnia się też niezwykłą cierpliwością i skrupulatnością. Potrafi z dużą precyzją i w prostych słowach wyjaśnić nawet najbardziej skomplikowane zagadnienia dotyczące funkcjonowania sieci i bezpieczeństwa cyfrowego. Dlatego cenię nasze merytoryczne dyskusje, wymiany myśli i intensywne burze mózgów.

Książka *Etyczny hacking i testy penetracyjne. Zadbaj o bezpieczeństwo sieci LAN i WLAN* jest kolejnym dowodem na to, że Krzysztof jest praktykiem, który pragnie wspierać innych specjalistów ICT i cyberbezpieczeństwa. W publikacji autor zamieścił gotowe rozwiązania, instrukcje krok po kroku i wskazówki, jak przygotować środowisko sieciowe.

Lektura tej książki będzie wartościowa zarówno dla osób rozpoczynających swoją karierę w ICT i bezpieczeństwie informacji, jak i dla specjalistów zajmujących się zarządzaniem architekturą sieci i jej bezpieczeństwem. To praktyczny przewodnik, który wspomaga rozwój kompetencji i wdrażanie najlepszych praktyk w obszarze sieci i cyberbezpieczeństwa.

Dagmara Modrzejewska
styczeń 2026

Przedmowa

Podstawowym pytaniem, jakie powinien sobie zadać każdy, kto sięga po tę książkę, jest: „Po co mi ta wiedza?". Zastanów się, z czego na co dzień korzystasz. Odpowiesz zapewne, że z internetu. Jednak zanim uzyskasz do niego dostęp, wcześniej musi się coś wydarzyć — musisz połączyć się z siecią. I właśnie o sieci będziemy mówić w tej książce.

Aby haker uzyskał dostęp do Twoich danych, wcale nie musi się włamywać do doskonale zabezpieczonych serwisów. Często wystarczy, że niewłaściwie zabezpieczysz własną sieć, skorzystasz ze starego szyfrowania lub po prostu nie będziesz znał podstawowych zasad bezpieczeństwa. Bezpieczeństwo nie zaczyna się od przeglądania stron internetowych — zaczyna się od sieci. To ona stanowi fundament wszystkiego, co dalej składa się na potocznie rozumiany internet. Jeśli ktoś uzyska dostęp do Twojej sieci, może dotrzeć do wszystkich podłączonych do niej urządzeń, a co za tym idzie — do wszystkiego, co robisz w internecie.

Dlatego tak ważna jest świadomość, w jaki sposób może zostać przeprowadzony atak. Tak, nie pomyliłem się — wiedza o ataku jest niezbędna. Jeśli rozumiesz, w jaki sposób haker może zdobyć dostęp do Twojej sieci, jesteś w stanie realnie ocenić ryzyko. Nie odkrywam tu niczego niezwykłego, ale zadaj sobie pytanie: czy naprawdę wiesz, na jakie zagrożenia narażona jest Twoja sieć? Jeśli nie, ta książka trafiła w odpowiednie ręce.

W kolejnych rozdziałach staram się przekazać swoją wiedzę tak, abyś mógł w pełni zrozumieć naturę zagrożenia. Jeśli poznasz mechanizmy ataku, zrozumiesz, że konieczne jest stosowanie odpowiednich środków bezpieczeństwa, by Twoje dane, pliki i Twoja tożsamość pozostały bezpieczne. Zrozumienie podstaw działania sieci to niezwykle ważny element każdej dziedziny cyberbezpieczeństwa. Można wręcz powiedzieć, że na sieci opiera się całe cyberbezpieczeństwo.

Niezależnie od tego, czy zamierzasz pracować jako analityk w Centrum Operacji Bezpieczeństwa, planujesz prowadzić audyty, czy po prostu chcesz poszerzyć swoją wiedzę w ramach rozwoju kariery, informacje przedstawione w tej w książce okażą się nie tylko pomocne, ale wręcz niezbędne. Zrozumienie sposobów ataku to fundament skutecznej obrony. Mając taką wiedzę, jesteś w stanie dostrzec potencjalne zagrożenia w swojej sieci, często nawet bez użycia specjalistycznych narzędzi.

Należy jednak pamiętać, że narzędzia, z których korzystam podczas pisania tej książki, nieustannie ewoluują. Niestety nie jestem w stanie zagwarantować, że w chwili, gdy trzymasz tę książkę w rękach, wszystko pozostaje aktualne i znajduje się dokładnie tam, gdzie opisałem. Tak jak każda aplikacja, również oprogramowanie związane z bezpieczeństwem ulega zmianom — i warto podchodzić do tego z pozytywnym nastawieniem.

Niestety książki nie da się zaktualizować tak łatwo jak programu, dlatego gdy zauważysz różnice, braki lub zmienione funkcje, warto się zapoznać z dokumentacją nowej wersji. Przy każdym narzędziu, z którego korzystałem, starałem się podać jego wersję. Jeśli chcesz uniknąć ewentualnych problemów, możesz używać dokładnie tych samych. Mimo to pamiętaj, że najważniejsze w nauce jest zrozumienie działania mechanizmów. Dlatego nie zniechęcam do korzystania z nowszych wersji oprogramowania niż te opisane w książce. Może to przynieść wiele korzyści, szczególnie wtedy, gdy napotkasz problem wymagający samodzielnego rozwiązania.

Proste „klikanie według schematu" nie zawsze jest dobrą metodą. Decyzję pozostawiam Tobie — możesz najpierw wykonać wszystko zgodnie z opisem, a dopiero później, przy drugim podejściu, spróbować pracy na najnowszej wersji aplikacji. Taka praktyka może się okazać niezwykle cenna zarówno dla Twojego rozwoju, jak i dla utrwalenia poruszanych tu zagadnień. Często bywa tak, że sam schemat nie tłumaczy, dlaczego coś działa — dopiero samodzielna próba pozwala to w pełni zrozumieć. W końcu tak właśnie wygląda nauka: uczymy się na własnych doświadczeniach, w tym na błędach.

Jeżeli to, co przeczytałeś we wstępie, zachęciło Cię do zapoznania się z resztą książki, zapraszam Cię do mojego świata.

Linki występujące w książce zostały również zebrane na stronie internetowej *https://krzysztofgodzisz.pl/ehitp-zobsliw.html*.

Opinie o książce

Krzysztof to przede wszystkim pasjonat, który omawiane zagadnienia prezentuje na praktycznych przykładach. Przekazuje wiedzę w sposób przystępny dla początkujących, posługując się przy tym licznymi grafikami pozwalającymi jeszcze lepiej zrozumieć temat cyberbezpieczeństwa. Książka pomoże również uniknąć pewnych problemów z konfigurowaniem środowiska — żałuję, że nie wyszła, kiedy byłem w technikum. Jeśli szukasz konkretnego poradnika, jak zacząć przygodę z bezpieczeństwem sieci od strony ofensywnej — ta pozycja na pewno jest warta uwagi!

— Oskar Klimczuk, dziennikarz,
pasjonat cyberbezpieczeństwa w technicznym wydaniu

Połączenie warsztatowego charakteru, świadomej etyki i logicznej struktury. Książka jest naturalnym wyborem dla osób, które chcą naprawdę zrozumieć bezpieczeństwo sieci — od fundamentów po praktykę.

— Artur Markiewicz, fascynat cyberbezpieczeństwa

Merytorycznie i fachowo napisana książka. Zawiera opisane krok po kroku szczegóły wraz z licznymi grafikami, by nawet osoba początkująca mogła zgłębić tajniki i przetestować, czy to coś dla niej.

— Karolina Matkowska, HR & Office Director i pasjonatka cyberbezpieczeństwa

Krzysztof Godzisz to człowiek, który posiada ogromną wiedzę, i warto się od niego uczyć — zarówno teorii i praktyki w zakresie zabezpieczeń sieci, jak i podejścia do samego procesu nauki oraz etycznego hackowania. Na lekturze skorzystają wszyscy zainteresowani bezpieczeństwem, a nie tylko pasjonaci sieci.

Jeśli więc chcesz poznać podstawy łamania zabezpieczeń sieci WLAN i LAN, polecam przeczytać książkę, zakupić adapter, a potem wrócić do niej i ruszyć do nauki. Następnie możesz wykorzystać tę wiedzę do hardeningu infrastruktury czy pentestów — oczywiście bazując na tym, co prawnie i etycznie dozwolone. W moim przypadku lektura ma jeszcze jeden, niespodziewany efekt uboczny — poznawszy temat z perspektywy atakującego, przypuszczam, że niejeden jesienny i zimowy wieczór spędzę, zgłębiając go i reperując zabezpieczenia we własnej sieci. Tak na wszelki wypadek.

— Lena Sędkiewicz, programistka, specjalistka ds. bezpieczeństwa aplikacji.

ROZDZIAŁ 9.

Informacje wokół nas

Ten rozdział stanowi wprowadzenie do zrozumienia, dlaczego sieci bezprzewodowe niosą ze sobą pewne zagrożenia. Wygoda i nowoczesność, z którymi stykamy się na co dzień, mają swoją cenę — a ponieważ zajmujemy się bezpieczeństwem, właśnie o tej „cenie" tu mówimy. Zwróć uwagę, że współczesny dom można w dużej mierze podłączyć do internetu (czyli na początku do naszej sieci). Lodówki, odkurzacze, żarówki czy inne urządzenia pozwalają na zdalne sterowanie z dowolnego miejsca na świecie. Gdy byłem dzieckiem, futurystyczna bajka *Jetsonowie* (choć wielu z Was może jej nie pamiętać) wydawała się czymś oderwanym od rzeczywistości. Mimo że wiele z przedstawionych tam technologii nadal pozostaje poza naszym zasięgiem, tempo rozwoju technologii potrafi zaskakiwać, czasem przerażać, a czasem zachwycać. Kto wie, może za kilka lub kilkanaście lat rzeczywiście będziemy latać jak we wspomnianej kreskówce? Piszę o tym, abyś nie zniechęcił się do sieci bezprzewodowych po lekturze tego rozdziału. Mogłeś odnieść wrażenie, że WLAN to wyłącznie źródło problemów i ryzyka. Tymczasem jest inaczej. Sieci WLAN są niezwykle przydatne, a niekiedy wręcz niezbędne. Dobrym przykładem jest smartfon — trudno wyobrazić sobie urządzenie tego typu podłączone do sieci za pomocą kabla, bo stałby się zupełnie niefunkcjonalne. Naszym zadaniem jako użytkowników jest jednak pamiętać o związanych z tym zagrożeniach i dążyć do maksymalnego zabezpieczenia naszej sieci. Ten rozdział jest wprowadzeniem właśnie do takich działań.

9.1. Sieci w naszym otoczeniu

Jeżeli posiadamy kartę lub adapter bezprzewodowy, za pomocą którego podłączamy urządzenia do sieci, to mieszkając w mieście — szczególnie w gęsto zabudowanej okolicy — bardzo szybko zauważymy, że lista dostępnych sieci WLAN potrafi być ogromna. Im lepszy zasięg ma nasza karta lub adapter (a dokładniej: im skuteczniejsze anteny są w nich zastosowane), tym więcej sieci będzie widocznych. Choć wspominałem o tym już wcześniej, ponownie przestrzegam przed próbami łączenia się z sieciami, do których nie mamy uprawnień. Jest to niezgodne z prawem, nieetyczne i może prowadzić do poważnych konsekwencji. Dlatego nie próbuj tego robić!

Jak dobrze wiecie, sygnał sieci bezprzewodowych nie jest widoczny dla ludzkiego oka, ale musi istnieć — w przeciwnym razie nie moglibyśmy go odebrać. Oznacza to, że nieustannie otaczają nas różnego rodzaju informacje przesyłane w postaci sygnału radiowego. Już sama możliwość połączenia się z daną siecią jest informacją o jej istnieniu.

Zastanówmy się przez chwilę nad tym, co dzieje się, kiedy próbujemy nawiązać połączenie z siecią WLAN. Robimy to bezprzewodowo, więc musimy wysłać odpowiednie dane — w tym hasło. Router lub punkt dostępowy musi te dane odebrać i je zweryfikować. Sam fakt, że to działa, dowodzi, że informacje te muszą zostać przesłane i krążą wokół nas. Po udanym połączeniu korzystamy z internetu. Wchodzimy na różne strony, jak na przykład na stronę wydawnictwa tej książki — *helion.pl*. Router nie domyśla się, dokąd chcemy wejść — to my musimy przesłać mu odpowiedni pakiet z żądaniem. Oznacza to, że wokół nas krążą setki, a nawet tysiące pakietów — często zawierających bardzo poufne dane. Na szczęście w większości przypadków są one zaszyfrowane, więc nie można ich swobodnie odczytać. Do ich odszyfrowania potrzebujemy odpowiedniego klucza. Jednak fakt, że dane są zaszyfrowane, nie oznacza, że nie można ich przechwycić. Wokół nas krąży mnóstwo ruchu sieciowego, który da się wyłapać i analizować. To trochę jak z muchą latającą po pokoju: możesz ją zobaczyć, możesz ją złapać lub sprawić, by przestała bzyczeć, ale to nie znaczy, że wiesz, co myśli. Podobnie jest z pakietami sieciowymi.

Do takich analiz przydaje się adapter sieciowy z funkcją monitorowania, o którym wspominałem w części I. To dzięki niemu możemy wyłapać pakiety. Standardowy tryb `managed`, obecny w każdym adapterze czy karcie sieciowej, pozwala jedynie wykrywać sieci znajdujące się w zasięgu i łączyć się z nimi. Aby jednak wyłapywać pakiety przesyłane w sieci, musimy przełączyć adapter w tryb `monitor`. I właśnie tym zajmiemy się teraz.

9.2. Tryby adaptera bezprzewodowego

Aby wyświetlić szczegółowe informacje o naszym adapterze bezprzewodowym, w tym o trybach pracy, które obsługuje, użyje polecenia:

```
iw list
```

Nie zamieszczam tutaj pełnego wyniku, ponieważ najprawdopodobniej masz zupełnie inny adapter, więc dane będą się różniły od moich. Na swojej liście znajdź następującą informację:

```
Supported interface modes:
* managed
* AP
* AP/VLAN
* monitor
* P2P-client
* P2P-GO
```

To lista trybów obsługiwanych przez mój adapter bezprzewodowy. Spośród nich będziemy korzystać z trzech: `managed`, `AP` i `monitor`. Tryb `managed` omówiliśmy już w poprzednim akapicie. Tryb `monitor` posłuży nam do przechwytywania pakietów. Z kolei tryb `AP` daje możliwość nawiązania połączenia i działa podobnie jak router, umożliwiając dostęp do sieci i internetu. Z tego ostatniego trybu skorzystamy w końcowych rozdziałach tej części. Teraz zobaczmy, w jaki sposób możemy zmienić tryb działania naszego adaptera.

9.3. Adapter działający w trybie monitor

Aby móc przechwytywać pakiety, musimy wskazać naszemu adapterowi, aby to robił. W tym celu należy go przełączyć w tryb monitorowania. Istnieje kilka sposobów, aby to zrobić, lecz ja pokażę dwa — jeden bardziej manualny, a drugi automatyczny. Dlaczego pokazuję dwa sposoby? Mam świadomość, że częściej będziesz używał metody automatycznej — jest szybsza, wymaga mniej wpisywania i szybciej osiągniesz swój cel. Jednak metoda manualna ma tę zaletę, że jeśli coś pójdzie nie tak i wystąpi jakiś problem, umiejętność wykonania tego samego „ręcznie" okazuje się bezcenna.

Musisz mi wybaczyć jedną nieścisłość w nazewnictwie. Ten sposób zmiany trybu pracy adaptera można by nazwać „manualnym", bo często opiera się na modyfikowaniu plików konfiguracyjnych. Ja natomiast skorzystam z polecenia `ifconfig`. Wkrótce sam zauważysz, że między tymi sposobami jest pewna różnica, choć dają one ten sam efekt.

Przejdźmy do omawiania zmiany trybu pracy adaptera sieciowego. Istnieje pewien schemat, z którym zapewne już się spotkałeś. Aby zmienić sposób działania jakiegoś urządzenia lub funkcji, zazwyczaj trzeba najpierw „to" wyłączyć, następnie wprowadzić zmiany, a dopiero potem ponownie włączyć. Tak samo jest w przypadku zmiany trybu działania adaptera. Pierwszym krokiem jest wyłączenie interfejsu naszego adaptera bezprzewodowego. W moim przypadku jest to `wlan0`, jednak aby sprawdzić, jak nazywa się Twój interfejs bezprzewodowy i czy jest aktywny, możesz skorzystać z polecenia `ifconfig`. Znamy je już z wcześniejszych rozdziałów. Wyświetla ono wszystkie interfejsy sieciowe, jakimi dysponujemy. Oczywiście, możemy wyświetlić wybraną specyfikację interfejsu, ale aby to zrobić, musimy znać jego nazwę, co przy takiej liczbie interfejsów może być czasem dość problematyczne. Dlatego w przypadku sieci bezprzewodowych warto skorzystać z polecenia `iwconfig`:

```
iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=3 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
```

Polecenie `iwconfig` również wyświetla listę dostępnych interfejsów, ale szczegółowe informacje pokazuje tylko dla tych, które obsługują komunikację bezprzewodową.

Szczegółowym opisem wyniku tego polecenia zajmiemy się w dalszej części książki. Na razie przejdźmy do metod zmiany trybu działania adaptera na `monitor`.

9.3.1. Zmiana trybu adaptera manualnie

Jak już wiesz, skorzystamy z poleceń systemowych. Pierwszą czynnością, jaką musimy wykonać, jest wyłączenie interfejsu sieciowego naszego adaptera. Robimy to za pomocą polecenia:

```
ifconfig wlan0 down
```

Jeżeli nie otrzymasz żadnej informacji zwrotnej, oznacza to, że wyłączenie adaptera zakończyło się powodzeniem. Co ciekawe, po wpisaniu polecenia `iwconfig` interfejs nadal będzie widoczny. Natomiast gdy użyjesz polecenia `ifconfig`, zauważysz, że interfejs zniknął i wyświetlane są jedynie `eth0` i `lo`. Jest to spowodowane różnicą w sposobie działania obu poleceń. Pierwsze z nich, `iwconfig`, wyświetla wszystkie interfejsy bezprzewodowe, niezależnie od tego, czy są one aktywne, czy wyłączone. Z kolei `ifconfig` pokazuje domyślnie tylko interfejsy aktualnie włączone. Nie ma tu żadnej magii. Skoro interfejs jest już wyłączony, możemy zmienić tryb jego pracy na `monitor`. Robimy to za pomocą polecenia:

```
iwconfig wlan0 mode monitor
```

Jeżeli nie otrzymałeś żadnej informacji zwrotnej, oznacza to, że operacja zakończyła się poprawnie. Aby sprawdzić, czy adapter zmienił tryb działania, wystarczy ponownie wpisać polecenie:

```
iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Tx-Power=3 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

Wróć do wcześniejszego przykładu, gdy po raz pierwszy używaliśmy polecenia `iwconfig`. Możliwe, że zauważyłeś, iż wtedy widniała informacja:

```
Mode:Managed
```

Natomiast teraz otrzymaliśmy komunikat:

```
Mode:Monitor
```

Czyli nasz adapter bezprzewodowy zmienił tryb swojego działania, co potwierdza powyższy wynik. W takiej sytuacji pozostaje uruchomić adapter bezprzewodowy za pomocą polecenia:

```
ifconfig wlan0 up
```

Podobnie jak wcześniej, brak jakiejkolwiek informacji zwrotnej oznacza, że operacja przebiegła pomyślnie. Aby to potwierdzić, wystarczy wpisać polecenie:

```
ifconfig wlan0
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        unspec 6A-7F-27-F4-5C-2D-70-EC-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 4950  bytes 1680115 (1.6 MiB)
        RX errors 0  dropped 4950  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Interfejs ponownie się pojawił, a informacja `UP` potwierdza, że jest on uruchomiony. Dobrą praktyką jest jeszcze wyłączenie całego ruchy sieciowego — do tego wrócimy za chwilę.

Podczas próby zmiany trybu działania adaptera możesz otrzymać następujący komunikat:

```
iwconfig wlan0 mode monitor
Error for wireless request "Set Mode" (8B06) :
SET failed on device wlan0 ; Device or resource busy.
```

Jest to dość często spotykany błąd, szczególnie w przypadku wirtualizacji. Nie ma tu większego znaczenia, z jakiego adaptera korzystamy. Pojawienie się tego komunikatu oznacza, że wystąpił problem uniemożliwiający zmianę trybu pracy adaptera — interfejs jest aktualnie używany przez inny proces lub usługę. W takiej sytuacji najlepszym rozwiązaniem jest fizyczne odłączenie i ponowne podłączenie adaptera.

9.3.2. Zmiana trybu adaptera za pomocą jednego polecenia

Zmiana trybu działania adaptera za pomocą poznanego poprzednio sposobu nieco wydłuża drogę do osiągnięcia celu. Poznałeś jednak metodę wykonania tego procesu krok po kroku, czyli bardziej manualnie. Z czasem jednak może się ona okazać bardzo uciążliwa, gdyż zabiera dużo czasu. Dlatego istnieje możliwość przyspieszenia tego procesu za pomocą polecenia `airmon-ng`.

Jeżeli wykonałeś wszystkie czynności opisane w podrozdziale 9.3.1, uruchom ponownie maszynę wirtualną albo odłącz i ponownie podłącz swój adapter sieciowy.

Polecenia używa się w następujący sposób:

```
airmon-ng start wlan0
```

Tak dokonujemy zmiany trybu monitorowania naszego adaptera. Po nazwie polecenia wpisujemy słowo `start`, a następnie nazwę interfejsu sieciowego obsługującego adapter. Aby potwierdzić, że zmiana została wykonana poprawnie, skorzystajmy z polecenia `iwconfig`:

```
iwconfig
lo        no wireless extensions.
eth0      no wireless extensions.
wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=3 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

Jak widać, adapter zmienił tryb z `mode` na `monitor`. To jednak nie wszystko. Zmieniła się również nazwa interfejsu sieciowego, co zostało jasno zakomunikowane przez narzędzie `airmon-ng`:

```
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)
```

Ta sytuacja występuje zarówno w Kali Linux, jak i Parrot OS. Możesz się zastanawiać, dlaczego tak się dzieje i jakie ma to znaczenie. Otóż nie miało to miejsca podczas zmiany trybu adaptera przy użyciu poleceń `ifconfig` oraz `iwconfig`. Wynika to z faktu, że `iwconfig` nie ma takiej funkcjonalności. Natomiast `airmon-ng`, w przypadku adapterów opartych na chipsecie Mediatek, automatycznie zmienia nazwę interfejsu. Jak można zauważyć, do nazwy dodany jest człon „mon”, będący skrótem od słowa „monitor”. Ma to na celu

ułatwienie rozpoznania interfejsu działającego w trybie monitorowania. W dystrybucji Parrot OS interfejs o nazwie `wlx00c0cab6ceaa` został przez `airmon-ng` zmieniony na `wlan0mon`. W przypadku adapterów opartych na chipsecie Realtek taka zmiana nie występuje. Najważniejsze jest jednak to, że po zmianie nazwy interfejsu należy się już posługiwać wyłącznie nową nazwą, ponieważ stara przestaje istnieć.

9.3.3. Odłączenie zbędnych procesów

Po wpisaniu polecenia `airmon-ng` mogliśmy otrzymać dodatkowy komunikat o treści:

```
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode
    PID Name
    637 NetworkManager
    897 wpa_supplicant
```

Oznacza to, że w systemie działają procesy, które mogą zakłócać poprawne funkcjonowanie adaptera w trybie monitorowania. Mogą na przykład uniemożliwić zmianę trybu jego działania. Ponieważ do próby uzyskania dostępu do sieci bezprzewodowej nie jest nam potrzebne żadne połączenie, można wyłączyć proces sieciowy. Zgodnie z instrukcjami wystarczy wpisać polecenie:

```
airmon-ng check kill
Killing these processes:
    PID Name
    897 wpa_supplicant
```

Zostaliśmy całkowicie odłączeni od sieci oraz internetu. Co ciekawe, `airmon-ng` zaleca wykonanie tej czynności jeszcze przed przełączeniem adaptera w tryb monitorowania. Niemniej ja od zawsze wykonywałem ją już po zmianie trybu i nigdy nie spotkałem się z problemami wynikającymi z takiej kolejności. Jeżeli jednak kiedykolwiek napotkasz trudności z przejściem w tryb monitorowania, a masz pewność, że adapter obsługuje tę funkcję, pierwszą rzeczą, jaką powinieneś zrobić, jest wyłączenie wspomnianych procesów.

9.4. Wyłapywanie pakietów

Jak już wspomniałem, informacje w postaci pakietów krążą wokół nas. Nasz adapter został przełączony w tryb monitorowania, dzięki czemu jest w stanie je wyłapywać. Możesz się teraz zastanawiać: skoro tryb `monitor` umożliwia przechwytywanie pakietów, to do czego służy podstawowy tryb `managed`, w którym domyślnie działają wszystkie karty i adaptery sieciowe? Różnica jest zasadnicza. W trybie `managed` karta sieciowa czy też adapter odbiera wyłącznie te pakiety, które są skierowane bezpośrednio do nich. Każdy router udostępniający sieć wysyła sygnał, który może zostać wykryty przez dowolną kartę sieciową lub adapter znajdujący się w zasięgu, jednak właściwe pakiety danych trafiają tylko do urządzeń, dla których są przeznaczone. W trybie monitorowania sytuacja wygląda inaczej. Adapter przechwytuje cały ruch radiowy znajdujący się w jego zasięgu — niezależnie od tego, do kogo pakiety są skierowane. Jak już jednak wspomniałem, są to informacje w większości przypadków zaszyfrowane. Rodzajami szyfrowania zajmiemy się

w dalszej części książki. Na tym etapie istotne jest zrozumienie, że dane te można przechwycić i analizować. Podstawowym poleceniem służącym do wyłapywania pakietów jest polecenie:

```
airodump-ng wlan0mon
```

Jest to jedno z poleceń należących do pakietu narzędzi **Aircrack-ng**. Jak się zapewne domyślasz, `airodump-ng` służy do przechwytywania pakietów krążących w zasięgu naszego adaptera. Po nazwie programu wpisujemy nazwę interfejsu, który został przypisany do adaptera pracującego w trybie monitorowania. Jeżeli mieszkasz w miejscu o gęstej zabudowie, lista wykrytych sieci może być bardzo długa, tak jak moja. Z uwagi na poszanowanie prywatności innych osób nie zamieszczę pełnego wyniku. Pokażę jedynie te sieci, które zostały przygotowane specjalnie na potrzeby testów opisywanych w książce.

Jeżeli polecenie masz uruchomione już od jakiegoś czasu, możesz chcieć je zatrzymać. W tym celu wystarczy skorzystać ze skrótu klawiszowego *Ctrl+C*. Wyszukiwanie zostanie przerwane, a lista pozostanie wyświetlona na ekranie. Powinieneś otrzymać wynik podobny do poniższego, choć z innymi sieciami:

```
CH  7 ][ Elapsed: 36 s ][ 2025-02-13 20:56
BSSID              PWR  Beacons  #Data, #/s  CH   MB  ENC   CIPHER  AUTH ESSID
DC:62:79:7D:3B:9E   -4       31      0    0   4  130  WPA3  CCMP    SAE  My_Network
A4:98:13:6D:A9:19   -7       17     26    2   9  270  WPA2  CCMP    PSK  My_Network3

BSSID              STATION            PWR  Rate   Lost    Frames  Notes  Probes
A4:98:13:6D:A9:19  BA:2C:04:03:61:E7  -1   24e- 0    0      3
A4:98:13:6D:A9:19  FE:03:59:7D:AC:27  -72  5e- 1e  539     23
A4:98:13:6D:A9:19  C0:10:B1:5D:96:9A  -66  1e- 1    11      4
```

Wynik można podzielić na dwie części. W górnej znajdują się urządzenia, z którymi istnieje możliwość nawiązania połączenia — innymi słowy, są to routery lub punkty dostępowe. Natomiast dolna lista przedstawia urządzenia podłączone do sieci utworzonych przez punkty dostępowej z górnej części. Są to więc urządzenia klienckie, takie jak komputery, laptopy czy smartfony.

Możliwe, że zauważyłeś, iż druga lista nie jest w żaden sposób uporządkowana. Wyświetlane są wszystkie urządzenia, które nasz adapter zdołał wyłapać, jednak nie są one posegregowane chronologicznie ani według przynależności do konkretnej sieci. Na przykład do sieci o `ESSID` (czyli nazwie identyfikującej sieć) `My_Network3` podłączone są urządzenia o adresach MAC `BA:2C:04:03:61:E7`, `FE:03:59:7D:AC:27` i `C0:10:B1:5D:96:9A`. Informacje te znajdują się w kolumnie `STATION`, która zawiera adresy MAC urządzeń klienckich połączonych z danym routerem. Natomiast kolumna `BSSID`, występująca zarówno w górnej, jak i w dolnej części listy, oznacza adres MAC urządzenia typu router lub punkt dostępowy. W górnej części jest to adres MAC punktu dostępowego, a w dolnej — adres MAC routera lub AP, z którym dane urządzenia jest połączone. Dzięki temu jesteśmy w stanie jednoznacznie wskazać, które urządzenia są podłączone do konkretnych sieci i za pośrednictwem jakich punktów dostępowych uzyskują dostęp do sieci lokalnej i, najczęściej, internetu. Pozostałe kolumny oznaczają:

- `PWR` — siła sygnału; im wyższa wartość, tym silniejszy sygnał;
- `Beacons` — liczba danych wysyłanych przez punkt dostępu, router;
- `#Data` — liczba odebranych pakietów danych;

- `#/s` — liczba pakietów przesłanych w ciągu ostatnich 10 sekund;
- `CH` — kanał, na którym działa sieć;
- `MB` — maksymalna szybkość połączenia;
- `ENC` — rodzaj szyfrowania;
- `CIPHER` — szyfrowanie użyte przez sieć;
- `AUTH` — protokół uwierzytelniania.

Natomiast w dolnej części poszczególne kolumny oznaczają:

- `BSSID` — adres MAC routera lub AP;
- `STATION` — adres MAC urządzenia połączonego z routerem;
- `PWR` — siła sygnału;
- `Rate` — szybkość komunikacji urządzenia się z routerem/AP, wyrażona w Mb/s;
- `Lost` — liczba nieodebranych pakietów;
- `Frames` — liczba pakietów wysyłanych z urządzenia do routera/AP; im wyższa wartość, tym większa aktywność;
- `Notes` — dodatkowe informacje, na przykład dotyczące uwierzytelniania;
- `Probes` — nazwy sieci, z którymi urządzenie próbuje się połączyć (jeżeli trafimy na moment wysyłania zapytań).

Pozostała jeszcze kwestia górnej części, czyli:

```
CH  7 ][ Elapsed: 36 s ][ 2025-02-13 20:56
```

W związku z tym, że nie określiliśmy konkretnego kanału, na którym mają być prowadzone nasłuchy, `airodump-ng` automatycznie przeszukuje wszystkie. Dlatego wartość widoczna po `CH` (od ang. *channel*) ulega ciągłym zmianom. Pole `Elapsed` oznacza czas, jaki poświęciliśmy na wyszukiwanie.

Wiem, że na tym etapie nie wszystkie informacje są dla Ciebie w pełni zrozumiałe. Niektórych z tych kolumn tak naprawdę nigdy nie wykorzystasz. Natomiast te najważniejsze poznasz stopniowo w trakcie ćwiczeń praktycznych, które pojawią się w kolejnych rozdziałach.

9.5. Wyłapywanie i przechwytywanie pakietów na określonych częstotliwościach

Sposób poznany w poprzednim podrozdziale umożliwia wyszukiwanie sieci działających wyłącznie w paśmie 2,4 GHz. A co z pozostałymi częstotliwościami? Nic nie stoi na przeszkodzie, aby wskazać, jakie częstotliwości chcemy przeskanować. Aby na przykład skanować tylko 5 GHz, należy użyć polecenia w następujący sposób:

```
airodump-ng --band a wlan0mon
```

Zastosowana opcja `--band` wraz z parametrem `a` pozwala określić zakres częstotliwości, który ma zostać objęty skanowaniem. Jeżeli natomiast chcielibyśmy wyszukiwać sieci zarówno w 2,4 GHz, jak i 5 GHz, wystarczy użyć polecenia:

```
airodump-ng --band abg wlan0mon
```

Nie są to informacje „wzięte z głowy". Jak zawsze pomocna okazuje się magiczna opcja `--help`, dostępna praktycznie w każdym poleceniu, która potrafi wyjaśnić bardzo wiele. Możesz teraz zapytać: „No dobrze, ale co z pasmem 6 GHz?" I właśnie temu zagadnieniu poświęcimy kolejny podrozdział.

9.6. Kanały i częstotliwości

Jeżeli przyjrzałeś się wynikom skanowania, mogłeś zauważyć, że każda sieć działa na określonym kanale. Co więcej, te same kanały często powtarzają się w wielu sieciach. Im większa liczba sieci korzysta z tego samego kanału, tym większe są wzajemne zakłócenia. W takiej sytuacji kluczowe znaczenie ma siła nadajnika oraz odbiornika — wygrywa ten, który dysponuj silniejszym sygnałem. Dlatego podczas konfiguracji własnej sieci bezprzewodowej, gdy po ustawieniu automatycznego wyboru kanału połączenie jest niestabilne, często się zrywa lub ma słaby zasięg, warto sprawdzić, na jakich kanałach działają sieci w pobliżu, i ustawić kanał ręcznie. Trzeba jednak mieć świadomość, że obecnie znalezienie rozwiązania idealnego bywa trudne. Dostęp do internetu ma większość użytkowników, a zdecydowana ich część korzysta z sieci bezprzewodowych, co sprawia, że znalezienie najmniej obciążonego kanału bywa nie lada wyzwaniem. Każde z omawianych pasm częstotliwości ma przypisaną określoną liczbę kanałów oraz konkretne wartości częstotliwości. Na przykład określenie 2,4 GHz odnosi się do całego zakresu częstotliwości, na jakich działa sieć. Poniżej prezentuję listy kanałów dostępnych w Polsce wraz z odpowiadającymi im częstotliwościami.

Dla 2,4 GHz:

KANAŁ	CZĘSTOTLIWOŚĆ
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472

Dla 5 GHz:

KANAŁ	CZĘSTOTLIWOŚĆ
36	5180
40	5200
44	5220
48	5240
52	5260
56	5280
60	5300
64	5320
100	5500
104	5520
108	5540
112	5560
116	5580
120	5600
124	5620
128	5640
132	5660
136	5680
140	5700
149	5745
153	5765
157	5785
161	5805
165	5825
169	5845
173	5865

Dla 6 GHz:

KANAŁ	CZĘSTOTLIWOŚĆ
1	5955
5	5975
9	5995
13	6015

Dla 6 GHz (*ciąg dalszy*):

KANAŁ	CZĘSTOTLIWOŚĆ
17	6035
21	6055
25	6075
29	6095
33	6115
37	6135
41	6155
45	6175
49	6195
53	6215
57	6235
61	6255
65	6275
69	6295
73	6315
77	6335
81	6355
85	6375
89	6395
93	6415

Wszystkie kanały z powyższej listy możesz wyświetlić za pomocą polecenia:

```
iw list
```

Musisz jednak wiedzieć, że w zależności od regionu dostępne są różne kanały oraz przypisane im częstotliwości. Możesz to sprawdzić, wykonując powyższe polecenie. Zauważysz, że niektóre częstotliwości są wyłączone. Przykładowo:

```
2484 MHz [14] (disabled)
```

W Polsce kanał 14 o częstotliwości 2484 MHz jest domyślnie wyłączony i nie można z niego korzystać. Istnieje jednak możliwość zmiany regionu. W ramach przykładu ustawmy region USA, korzystając z polecenia:

```
iw reg set USA
```

Następnie ponownie wyświetlamy listę:

```
iw list
```

Zauważ, że w przypadku USA wyłączone są kanały:

```
2467 MHz [12] (disabled)
2472 MHz [13] (disabled)
2484 MHz [14] (disabled)
```

…które w Polsce są dostępne, z wyjątkiem ostatniego. Jeżeli dokładnie przeanalizujesz wyniki, zobaczysz również, że w paśmie 6 GHz dostępnych jest znacznie więcej kanałów niż w Europie. Należy jednak pamiętać, że kanały 1, 5, 9 oraz 13 są obsługiwane zarówno przez pasmo 2,4 GHz, jak i 6 GHz. Różnica polega na tym, że pracują one na zupełnie innych częstotliwościach.

9.7. Różnica pomiędzy 2,4, 5 i 6 GHz

Powiedzieliśmy już sobie o częstotliwościach, ale do tej pory nie wyjaśniliśmy podstawowych różnic między nimi. Zaczynając od najstarszego pasma 2,4 GHz, należy zaznaczyć, że jest ono wykorzystywane od wielu lat. Dzięki temu obsługiwane jest również przez starsze urządzenia. Jednak nie to stanowi jego największą zaletę. Pasmo 2,4 GHz bardzo dobrze radzi sobie z przeszkodami, takimi jak ściany czy stropy. Mimo niższych prędkości transmisji danych oferuje znacznie lepszy zasięg niż 5 GHz. Innymi słowy, tam, gdzie sygnał 5 GHz już nie dociera, 2,4 GHz często nadal pozostaje dostępne. Z tego powodu pasmo to jest wciąż powszechnie wykorzystywane wszędzie tam, gdzie kluczowy jest zasięg, a nie maksymalna przepustowość.

Pasmo 5 GHz charakteryzuje się znacznie mniejszą przenikliwością przez różnego rodzaju przeszkody. W zamian otrzymujemy jednak zdecydowanie wyższe prędkości transmisji. Dlatego jest idealnym rozwiązaniem w mieszkaniu w bloku — często okazuje się, że taka sieć jest wystarczająca.

Trzecim i najnowszym pasmem jest 6 GHz. Jego największą zaletą jest właśnie nowość. Oznacza to dostęp do zupełnie nowych kanałów oraz częstotliwości, dzięki czemu zakłócenia niemal nie występują. Inną zaletą jest oczywiście prędkość, ale tego zapewne się domyśliłeś.

9.8. Sieci i pakiety z konkretnego kanału

Dużo mówiliśmy o kanałach i częstotliwościach, dlatego na zakończenie chciałbym pokazać, w jaki sposób można wyszukiwać sieci dostępne na konkretnym kanale. Zauważ, że po wpisaniu polecenia:

```
iwconfig wlan0mon
wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=3 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

pojawia się taka informacja:

```
Frequency:2.412 GHz
```

Z angielskiego *Frequency* oznacza częstotliwość (2,412 GHz to kanał 1). Informacja ta pokazuje, że `airodump-ng` w swojej domyślnej konfiguracji skanuje sieci działające w paśmie 2,4 GHz. W praktyce możemy jednak zmienić to zachowanie i wyświetlać tylko sieci działające na konkretnym kanale. Aby to zrobić, wystarczy wpisać polecenie:

```
airodump-ng --channel 36 wlan0mon
```

Dodajemy tu opcję `--channel`, po której wpisujemy numer kanału, na którym urządzenia mają nadawać sygnał. Jak widzisz, to nic trudnego, dlatego dalszą zabawę pozostawiam Tobie.

9.9. Podsumowanie

W dwóch ostatnich rozdziałach przedstawiłem wiedzę o charakterze bardziej merytorycznym niż praktycznym, którą musisz posiadać, aby móc swobodnie poruszać się po zagadnieniach omawianych w tej książce. Na szczęście jest to jeden z ostatnich rozdziałów tej części, w których dominuje teoria. W wyjaśnienie tych zagadnień włożyłem bardzo dużo wysiłku i serca. Wiedz, że teoria nie jest czymś, co szczególnie lubię, a już na pewno nie w formie długich opisów słownych zamiast praktycznych przykładów. Niestety nie zawsze da się tego uniknąć. Mam jednak nadzieję, że praca, jaką włożyłem w te dwa rozdziały, sprawi, iż dalsza część książki okaże się dla Ciebie znacznie łatwiejsza i bardziej zrozumiała.

ETYCZNY HACKING
i testy penetracyjne

Twoja superbezpieczna sieć lokalna

Lokalne sieci komputerowe LAN i bezprzewodowe sieci lokalne WLAN pozwalają łączyć ze sobą urządzenia elektroniczne w ograniczonym obszarze, jakim jest dom, biuro albo budynek. Połączone w ten sposób komputery stacjonarne, laptopy, drukarki, serwery współdzielą zasoby i są podłączone do internetu poprzez router, który zarządza ruchem sieciowym. Ze względu na to, że w ramach takich sieci dostępne są cenne, często wrażliwe dane, zagadnienie ich bezpieczeństwa to kwestia kluczowa zarówno z punktu widzenia administratora, jak i użytkownika.

Na szczęście osoby administrujące siecią LAN czy WLAN nie pozostają bezradne wobec prób wyłudzania haseł i danych czy ataków polegających na przeciążeniu serwera. Można je w pewnym sensie uprzedzić i sprawdzić odporność sieci dzięki zastosowaniu metod etycznego hackingu. Ta książka stanowi kompleksowy podręcznik, dzięki któremu nie tylko dowiesz się, jak stworzyć własne laboratorium do testów penetracyjnych, ale też poznasz zagrożenia czyhające na Twoją sieć bezprzewodową i nauczysz się je rozpoznawać, a także im zapobiegać.

Helion
helion.pl
HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-3507-5
9 788328 935075
Cena: 89,00 zł