Technologia i rozwiązania

# Kali Linux
## Audyt bezpieczeństwa sieci Wi-Fi dla każdego

**Wydanie II**

Odkryj słabe punkty infrastruktury sieciowej!

**Vivek Ramachandran**
**Cameron Buchanan**

Helion

[PACKT] PUBLISHING open source community experience distilled

Tytuł oryginału: Kali Linux Wireless Penetration Testing: Beginner's Guide, Second Edition

Tłumaczenie: Grzegorz Kowalczyk

ISBN: 978-83-283-1611-9



Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

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

Printed in Poland.

# Spis treści

ROZDZIAŁ 9

# Metodologia testów penetracyjnych sieci bezprzewodowych

*„Nie mów hop, póki nie przeskoczysz”.*

*Popularne przysłowie*

W tym rozdziale postaramy się połączyć zagadnienia i techniki omawiane w poprzednich rozdziałach i wykorzystać je podczas przeprowadzania prawdziwego testu penetracyjnego sieci bezprzewodowej.

## Testy penetracyjne sieci bezprzewodowych

Aby skutecznie przeprowadzić test penetracyjny sieci bezprzewodowych, powinieneś zawsze postępować zgodnie z ogólnie przyjętą i sprawdzoną metodologią. Proste uruchomienie programów takich jak `airbase` czy `airodump` z pewnością nie przyniesie oczekiwanych rezultatów. Jako pentester, powinieneś zawsze upewnić się, że działasz zgodnie ze standardami organizacji, dla której pracujesz, a jeżeli nie zostały one formalnie wyznaczone, powinieneś zawsze starać się przeprowadzać testy penetracyjne w sposób jak najbardziej profesjonalny.

Ogólnie rzecz biorąc, proces przeprowadzania testów penetracyjnych sieci bezprzewodowej można podzielić na cztery główne etapy:

- Faza planowania.
- Faza rozpoznania.
- Faza ataku.
- Faza raportowania.

W kolejnych podrozdziałach omówimy oddzielnie każdy z tych etapów.

# Planowanie

W tej fazie należy zająć się następującymi zagadnieniami:

- **Zakres planowanego testu** — klient zatrudniający specjalistę do przeprowadzenia testów penetracyjnych powinien z góry zdefiniować zakres testu, jaki należy przeprowadzić. Zazwyczaj obejmuje to takie informacje, jak:
  - Lokalizacja sieci, która będzie testowana.
  - Całkowity obszar pokryty zasięgiem sieci na terenie firmy i terenach przyległych.
  - Przybliżona liczba zainstalowanych punktów dostępowych oraz autoryzowanych klientów bezprzewodowych.
  - Lista identyfikatorów sieci bezprzewodowych, które mają być poddane testowi.
  - Oświadczenie klienta, czy zezwala na eksploatację wykrytych podczas testu podatności i luk w zabezpieczeniach.
  - Oświadczenie klienta, czy zezwala na przeprowadzanie ataków na użytkowników testowanej sieci bezprzewodowej.
  - Oświadczenie klienta, czy zezwala na przeprowadzanie ataków typu DoS na badane sieci i ich użytkowników.
- **Oszacowanie czasu i zasobów niezbędnych do przeprowadzenia testów** — po ustaleniu zakresu testów, jakie mają zostać przeprowadzone, powinieneś przystąpić do oszacowania czasu i zasobów niezbędnych do ich zrealizowania. Pamiętaj, że często zakres przeprowadzanego testu może ulec zmianie na żądanie klienta.
- **Dokumenty prawne** — przeprowadzanie testów penetracyjnych to bardzo poważne zadanie i zawsze istnieje możliwość, że może się wydarzyć coś nieprzewidzianego, co doprowadzi do mniejszych bądź większych perturbacji w funkcjonowaniu testowanej sieci. Z tego powodu zawsze powinieneś mieć pod ręką odpowiednią, podpisaną z klientem umowę o zwolnieniu z odpowiedzialności, zapewniającą, że ani osoba przeprowadzająca testy penetracyjne, ani firma czy organizacja, którą reprezentuje, nie będą pociągnięte do odpowiedzialności za żadne szkody mogące

powstać w wyniku przeprowadzania testów penetracyjnych. Bardzo często zdarza się również, że klient żąda podpisania umowy o zachowaniu poufności (ang. *NDA — Non Disclosure Agreement*), która zapewnia, że dane zebrane podczas testów penetracyjnych nie będą udostępniane podmiotom trzecim, niebędącym stronami umowy.

Po pomyślnym zakończeniu fazy planowania i przygotowań możemy rozpocząć działania operacyjne.

# Rozpoznanie

W tej fazie celem naszych działań będzie skanowanie ruchu w sieci bezprzewodowej w celu odszukania i zidentyfikowania punktów dostępowych oraz klientów bezprzewodowych znajdujących się w środowisku celu.

Wszystkie techniki niezbędne do przeprowadzenia tej fazy zostały szczegółowo omówione w poprzednich rozdziałach naszej książki, ale dla przypomnienia poniżej zamieszczamy krótkie zestawienie najważniejszych celów, które powinieneś osiągnąć w fazie rozpoznania:

- Identyfikacja wszystkich widocznych i niewidocznych sieci bezprzewodowych znajdujących się w obszarze środowiska celu.
- Identyfikacja wszystkich urządzeń bezprzewodowych działających w obszarze środowiska celu oraz wyodrębnienie tych, które są podłączone do sieci będących celem naszego testu penetracyjnego.
- Mapowanie obszarów fizycznej dostępności poszczególnych sieci bezprzewodowych oraz identyfikacja lokalizacji, z których potencjalny napastnik mógłby w ukryciu przeprowadzać ataki na badane sieci (na przykład pobliska kawiarnia znajdująca się w zasięgu badanej sieci).

Wszystkie pozyskane w tej fazie informacje powinny zostać skrupulatnie zanotowane. Jeżeli uzgodniony zakres testu penetracyjnego sprowadzał się wyłącznie do fazy rozpoznania, działania operacyjne zostaną zakończone na tym etapie i pentesterowi pozostanie już tylko napisanie odpowiedniego raportu, zawierającego między innymi wnioski i rekomendacje oparte na pozyskanych danych. W raporcie mogą się znaleźć między innymi takie informacje, bardzo cenne dla klienta:

- Liczba wykrytych urządzeń, które były powiązane zarówno z sieciami otwartymi, jak i siecią klienta.
- Liczba wykrytych urządzeń powiązanych z sieciami, które mogą być zlokalizowane za pomocą takich usług jak WiGLE.
- Informacje o wykrytych urządzeniach wykorzystujących słabe algorytmy szyfrowania.
- Wszelkie inne informacje, które mogą być przydatne dla klienta.

# Atak

Po zakończeniu fazy rozpoznania możesz rozpocząć fazę ataku, której celem będzie dokonanie próby wykorzystania wykrytych wcześniej podatności i luk w zabezpieczeniach. Rodzaj i natężenie przeprowadzanych ataków zależą w dużej mierze od uzgodnionego z klientem zakresu przeprowadzanego testu penetracyjnego.

W fazie ataku możesz wykonywać następujące zadania:

- Ataki i łamanie kluczy szyfrowania sieci.
- Ataki na infrastrukturę sieci bezprzewodowych w środowisku celu.
- Przełamywanie zabezpieczeń klientów.
- Identyfikacja klientów podatnych na ataki.
- Wykrywanie nieautoryzowanych klientów sieci bezprzewodowych.

## Łamanie klucza szyfrowania sieci

Pierwszym i najważniejszym elementem ataku będzie zazwyczaj próba pozyskania klucza szyfrowania wykorzystywanego w atakowanej sieci. Jeżeli dana sieć bezprzewodowa wykorzystuje szyfrowanie WEP, powinieneś dokonać próby ataku na klucz szyfrowania z wykorzystaniem metod opisywanych w rozdziale 4., „Słabe strony protokołów szyfrowania w sieciach WLAN". Jeżeli sieci w środowisku celu używają szyfrowania WPA2, masz do wyboru dwie możliwości. Jeśli przeprowadzasz „ukryty" test penetracyjny, powinieneś pojawić się w zasięgu sieci w czasie, kiedy pracownicy firmy lub organizacji będą się logować do sieci i z niej wylogowywać. Zazwyczaj największe natężenie takich zdarzeń ma miejsce w następujących porach:

- Rozpoczęcie dnia pracy.
- Okolice lunchu.
- Zakończenie dnia pracy.

W takich porach możesz dokonać próby przeprowadzenia ataku na klucz WPA, tak jak to pokazywaliśmy w rozdziale 4., „Słabe strony protokołów szyfrowania w sieciach WLAN". W razie potrzeby możesz również wymusić ponowne logowanie się użytkowników do sieci, przeprowadzając atak wymuszający anulowanie uwierzytelnienia użytkowników podłączonych do punktu dostępowego badanej sieci bezprzewodowej. Przykłady takich ataków opisywaliśmy w rozdziale 6., „Ataki na klienta sieci WLAN".

Z oczywistych względów przeprowadzanie takich ataków generuje znacznie więcej „hałasu" w sieci, co zdecydowanie zwiększa szansę na to, że odpowiednie służby informatyczne atakowanego klienta będą w stanie wykryć taki atak.

Jeżeli badana sieć wykorzystuje szyfrowanie WPA-Enterprise, pamiętaj, że będziesz musiał użyć informacji zebranych w fazie rozpoznania do utworzenia i skonfigurowania odpowiedniego podstawionego środowiska sieciowego, tak jak to opisywaliśmy w rozdziale 8., „Ataki na sieci WLAN z szyfrowaniem WPA-Enterprise i serwerami Radius", w sekcji „Ataki na protokół PEAP".

Oczywiście, zawsze możesz dokonać próby złamania dowolnego hasła czy klucza szyfrowania, ale jednocześnie musisz się pogodzić z tym, że niektórych z nich nie da się po prostu złamać w rozsądnym czasie i przy użyciu rozsądnych zasobów. W każdym przypadku po zakończeniu testu penetracyjnego powinieneś skontaktować się z administratorem sieci bezprzewodowej i omówić z nim zagadnienia związane z bezpieczeństwem używanych haseł.

## Ataki na infrastrukturę sieci bezprzewodowych

Jeżeli udało Ci się złamać klucz szyfrowania i uzyskać dostęp do atakowanej sieci, możesz rozpocząć przeprowadzanie pozostałej części testu penetracyjnego (o ile oczywiście przeprowadzenie takiego testu wchodzi w zakres umowy uzgodnionej z klientem). Zazwyczaj podczas tej fazy testu penetracyjnego przeprowadzane są co najmniej następujące operacje:

- Skanowanie portów.
- Wykrywanie oraz identyfikacja usług sieciowych działających w środowisku celu.
- Wykrywanie oraz identyfikacja otwartych usług sieciowych, umożliwiających dostęp bez konieczności przeprowadzania uwierzytelniania, takich jak FTP, SMP czy HTTP.
- Wykorzystywanie wykrytych podatności i luk w zabezpieczeniach do przełamywania zabezpieczeń atakowanych systemów.

## Atakowanie klientów sieci bezprzewodowych

Po zakończeniu wykrywania oraz identyfikacji bezprzewodowych hostów sieciowych działających w środowisku celu możesz rozpocząć przeprowadzanie różnego rodzaju ataków.

Na przykład, jeżeli to konieczne, po wykryciu hostów podatnych na ataki typu Karma możesz utworzyć Honeypot i spróbować zmusić je do podłączenia się do niego, tak jak to opisywaliśmy w rozdziale 8., „Ataki na sieci WLAN z szyfrowaniem WPA-Enterprise i serwerami Radius”, w sekcji „Ataki na protokół PEAP”. Za pomocą takiej metody możesz zebrać ogromną ilość bardzo użytecznych informacji, choć zawsze powinieneś się upewnić, że gromadzone informacje są pozyskiwane, przesyłane i przetwarzane w etyczny i bezpieczny sposób oraz że zostaną wykorzystane wyłącznie na potrzeby uzgodnionego z klientem testu penetracyjnego.

# Tworzenie raportów

Po zakończeniu fazy ataku wiesz już, jakie są słabe strony testowanej sieci, a zatem musisz przystąpić do utworzenia raportu, który przedstawisz zleceniodawcy. Ze względu na fakt, że klient będzie widział rezultaty przeprowadzonego testu penetracyjnego przez pryzmat przedstawionego przez Ciebie raportu, do jego tworzenia powinieneś zawsze podchodzić z takim samym zaangażowaniem jak do samego testu. Poniżej przedstawiamy krótkie zestawienie elementów, które powinien zawierać raport końcowy z przeprowadzonych testów penetracyjnych:

1. Podsumowanie dla zarządu.
2. Podsumowanie techniczne.
3. Zestawienie ważnych elementów odkrytych podczas testu:
   - Opis wykrytych podatności i luk w zabezpieczeniach.
   - Kategorie zagrożeń.
   - Lista urządzeń podatnych na ataki.
   - Rodzaje wykrytych podatności i luk w zabezpieczeniach — podatności programowe/sprzętowe/konfiguracyjne.
   - Opis rekomendowanych sposobów szybkiego naprawienia wykrytych podatności.
4. Dodatki.

Podsumowanie dla zarządu powinno zostać napisane prosto i przejrzyście, tak aby kadra zarządzająca — niemająca zbyt dużego doświadczenia technicznego — była w stanie zrozumieć wyniki przeprowadzonego testu i ewentualną konieczność wprowadzenia takich czy innych programów naprawczych. Pisząc podsumowanie dla zarządu, powinieneś zdecydowanie unikać używania skomplikowanego języka technicznego i omawiania złożonych detali oraz zawsze umieścić ogólny opis wyników testu i rekomendowanych rozwiązań.

Podsumowanie techniczne powinno być etapem pośrednim pomiędzy podsumowaniem dla zarządu a zestawieniem elementów odkrytych podczas testu. Ta część raportu jest zazwyczaj przeznaczona dla kierownika działu rozwoju bądź innego działu technicznego IT, dlatego powinna się koncentrować na rekomendowanych rozwiązaniach i sposobach ich ewentualnego wdrażania w badanym środowisku.

Zestawienie elementów powinno zawierać szczegółowe, precyzyjne opisy poszczególnych podatności i luk w zabezpieczeniach odkrytych podczas przeprowadzanego testu penetracyjnego oraz opis sposobu wykrycia i wykorzystania poszczególnych podatności.

Dodatki do raportu mogą zawierać dowolne dodatkowe informacje przydatne dla klienta, które z takich czy innych powodów nie powinny się znajdować w głównej części raportu. Przykładami takich elementów mogą być różnego rodzaju zrzuty ekranów, kody wykorzystanych exploitów czy skryptów PoC (ang. *proof-of-concept*) lub szczegółowe zestawienia danych, do jakich udało się dotrzeć pentesterowi podczas przeprowadzania testu.

# Podsumowanie

W tym rozdziale pokazaliśmy, w jaki sposób możesz przeprowadzać testy penetracyjne sieci bezprzewodowych przy użyciu narzędzi i technik opisywanych w poprzednich rozdziałach naszej książki. Omawialiśmy również zagadnienia związane z prezentowaniem wyników przeprowadzanych testów penetracyjnych, zwłaszcza dla osób z kadry menedżerskiej, nieposiadającej odpowiedniego przygotowania technicznego. W ostatnim rozdziale naszej książki omówimy nowe techniki, jakie pojawiły się na rynku od czasu ukazania się pierwszego wydania tej książki, takie jak WPS czy monitorowanie prób sondowania sieci.

# Skorowidz

## K



## L



## M



## O



## P

## R



## S



## T



## U



## W, Z

# Kali Linux

## Audyt bezpieczeństwa sieci Wi-Fi dla każdego

### Wydanie II

Sieci Wi-Fi obecnie można znaleźć wszędzie — coraz trudniej o miejsce, w którym nie będziemy w zasięgu przynajmniej jednej z nich. Taka sytuacja ma jedną wadę: brak możliwości fizycznej kontroli dostępu do sygnału. Zastanawiasz się, czy Twoja sieć jest bezpieczna i czy żadna postronna osoba nie ma możliwości podłączenia się do wewnętrznych zasobów? To są kluczowe pytania, na które musisz poznać odpowiedź, od tego zależy bezpieczeństwo użytkowników i przetwarzanych danych.

Jak się przekonać, czy Twoja sieć jest całkowicie bezpieczna? Spróbuj się do niej włamać! Testy penetracyjne to najskuteczniejsza technika weryfikacji bezpieczeństwa systemów informatycznych. Kali Linux to popularna i zaawansowana dystrybucja systemu Linux, zawierająca zestaw niezbędnych narzędzi każdego pentestera. Jeżeli chcesz wykorzystać jej potencjał, w tej książce znajdziesz szczegółowe omówienie dostępnych narzędzi oraz sposobów prowadzenia ataków. Szyfrowania WEP, WPA/WPA2 mają swoje słabe strony, które może wykorzystać potencjalny intruz, a ataki typu Honeypot, Misassociation, Caffe Latte to tylko niektóre z opisanych tu technik. Dzięki lekturze kolejnych rozdziałów będziesz w stanie sprawdzić podatność na zaawansowane ataki Man-in-the-Middle oraz poznasz metodologię prowadzenia testów penetracyjnych. Sięgnij po tę książkę i zbuduj własne laboratorium do testowania bezpieczeństwa sieci Wi-Fi.

**Zainwestuj w bezpieczeństwo Twojej sieci bezprzewodowej!**

**Sięgnij po tę książkę i:**

- poznaj metody zabezpieczania sieci bezprzewodowych
- przeanalizuj typowe ataki na sieci Wi-Fi
- wykryj ukryte sieci
- przechwyć dane przesyłane przez sieć bezprzewodową
- uzyskaj klucze szyfrujące transmisję

**Vivek Ramachandran** — związany z bezpieczeństwem sieci Wi-Fi od ponad 12 lat. Pomysłodawca ataku znanego pod nazwą Caffe Latte. Złamał sposób szyfrowania WEP. W środowisku znany jako założyciel serwisu SecurityTube.net. Występuje jako prelegent na wielu konferencjach poświęconych bezpieczeństwu.

**Cameron Buchanan** — pentester, autor książek. W swojej karierze przeprowadził audyty bezpieczeństwa dla wielu organizacji.

[PACKT] open source
PUBLISHING
community experience distilled

Helion

37699 numer katalogowy
księgarnia internetowa
http://helion.pl
zamówienia telefoniczne
0 801 339900
0 601 339900

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Informatyka w najlepszym wydaniu

sięgnij po WIĘCEJ
KOD KORZYŚCI

ISBN 978-83-283-1611-9

cena: 49,00 zł