# ATAKI NA SIECI BEZPRZEWODOWE

Szkolenie organizowane jest przez **Akademię Linux Magazine**, organizatora cyklu warsztatów i szkoleń poświęconych najnowszej wiedzy związanej z zagrożeniami i bezpieczeństwem systemów IT oraz tworzeniem i administrowaniem sieciami i serwerami komputerowymi.

Proponowane przez Akademię przedsięwzięcia **kierowane są głównie** do sektorów, w których poufność danych posiada najwyższy priorytet. W dzisiejszym świecie jest to kwestia bardzo istotna. Od świadomość zagrożeń i umiejętności ich niwelowania, zarówno w pracy prywatnych firm jak i instytucji użytku publicznego, zależy bezpieczeństwo każdego z nas.

**Zasady uczestnictwa:** Szkolenie to jest organizowane zarówno jako szkolenie otwarte jak i zamknięte. Koszt szkolenia podany w załączonym na ostatniej stronie formularzu dotyczy szkolenia otwartego. W przypadku szkoleń zamkniętych koszt ustalany jest indywidualnie z zamawiającym. Minimalna liczba uczestników szkolenia to 5 osób, maksymalna 12.

Szkolenie zamknięte może odbyć się we współpracującym z nami ośrodku szkoleniowym lub w siedzibie firmy klienta. Dodatkowo zależnie od potrzeb, program danego szkolenia może zostać dostosowany do wymagań zamawiającego.

**Podstawowe informacje o szkoleniu:**

---

**Sieci bezprzewodowe** coraz częściej stanowią atrakcyjną alternatywę dla rozwiązań przewodowych, głównie ze względu na swoją elastyczność, łatwą dostępność oraz niższą cenę. W wielu budynkach i obiektach instalacja sieci przewodowej jest technicznie bardzo trudna, lub wręcz niemożliwa, a tym samym bardzo kosztowna. Naturalnym rozwiązaniem jest zatem sieć bezprzewodowa. **Tylko czy takie rozwiązanie jest bezpieczne?**

**Podczas naszych warsztatów** uczestnicy dowiedzą się na jakie zagrożenia podatna jest sieć bezprzewodowa, **jak w praktyce wygląda atak** na nią – w jak sposób haker skanuje sieć, jak próbuje znaleźć jej słabości oraz jakimi technikami i narzędziami włamuje się do niej. Uczestnicy „uzbrojeni" podczas warsztatów w stosowaną wiedzę teoretyczną z technologii sieci bezprzewodowych oraz standardów szyfrowania i metod zabezpieczania takich sieci, samodzielnie dokonają ataku na specjalnie przygotowaną na potrzeby warsztatów sieć Wi-Fi.

Oczywiście **wiedza o lukach w bezpieczeństwie** i konfiguracji sieci bezprzewodowej, która umożliwia intruzom atak na sieć pozwoli uczestnikom odpowiednio zabezpieczyć całą infrastrukturę – **kwestia zabezpieczeń** będzie również szczegółowo omawiana podczas zajęć.

**Dzięki szkoleniu uczestnicy zdobędą następującą wiedzę i umiejętności:**

- dowiedzą się jakimi technikami i narzędziami posługuje się potencjalny intruz, aby włamać się do sieci,
- dowiedzą się jak wdrożyć bezpieczną sieć bezprzewodową,
- jak bezpiecznie rozbudować już posiadaną infrastrukturę,
- jak wybrać najlepsze komponenty sieci bezprzewodowej ze względu na bezpieczeństwo, niezawodność oraz wydajność,
- a także jak skutecznie monitorować sieć bezprzewodową, wykrywać intruzów i próby penetracji sieci.

**Szkolenie skierowane jest do** osób odpowiedzialnych za niezawodne i bezpieczne funkcjonowanie systemów informatycznych: administratorów, oficerów bezpieczeństwa, szefów działów IT; pracowników firm i instytucji posiadających rozbudowaną infrastrukturę IT – przedsiębiorstw i instytucji z branży: telekomunikacyjnej, finansowej, energetycznej, przemysłu oraz instytucji administracji publicznej.

**Wymagania względem uczestników –** uczestnicy warsztatów powinni posiadać: podstawową wiedzę z zakresu budowy sieci (ruter/switch/okablowanie - warstwa fizyczna), podstawową znajomość stosów protokołów rodziny TCP/IP, podstawową znajomość aspektów bezpieczeństwa (co to jest sniffer, spoofer, DoS, backdoor itd.) oraz podstawowa wiedzę z dziedziny kryptografii (klucz symetryczny, asymetryczny itd.).

**Informacje o prowadzącym: Daniel Kot –** obecnie zajmuje się administrowaniem serwerami w Lufthansa Systems. Przez ostatnie 8 lat zdobywał doświadczenie na stanowiskach Administratorów sieci i systemów operacyjnych. Bezpieczeństwo sieci bezprzewodowych stało się jego pasją w 2002 roku, kiedy zdecydował się na wykonanie dużego projektu sieci Wi Fi, którą później także administrował. Od tego czasu swoje doświadczenie pogłębiał między innymi w krajach Wielkiej Brytanii i Niemczech również przy projektach głosowego sterowania komputerem dla firm BMW, VW oraz Audi.

# Ataki na Sieci Bezprzewodowe

### Agenda - dzień pierwszy

| | |
|---|---|
| **09:30-10:00** | *Rejestracja* |
| **10:00-10:10** | *Powitanie* |
| **10:10-11:10** | **Wykład: Wprowadzenie do sieci Wi-Fi - historia, standardy. Budowa sieci Wi-Fi - warstwa sieciowa, szyfrowanie.**<br>Na wykładzie przedstawiona zostanie historie powstawania oraz ewolucja sieci opartych na standardach 802.11. Opisana zostania struktura warstwy sieciowej. Uczestnicy zdobędą również wiedzę na temat metod szyfrowania protokołu, stosowanych standardach. Przedstawione zostaną tutaj słabe oraz mocne strony wykorzystywania poszczególnych standardów. |
| **11:10-11:30** | *Przerwa kawowa* |
| **11:30-13:00** | **Ćwiczenia: Skanowanie w systemach Linux i Windows, pomiar poziomu sygnału, próba ataku.**<br>Część praktyczna podczas której uczestnicy spróbują własnych sił w łamaniu zabezpieczeń sieci Wi-Fi. Każdy użytkownik będzie mógł wykorzystać narzędzia dostarczone na płytce DVD w celu zbadania sieci dostępnej w laboratorium. Przeprowadzona będzie próba skanowania oraz podłączenia się do nieautoryzowanej sieci. |
| **13:00-13:20** | *Przerwa* |
| **13:20-14:20** | **Wykład: Metody zabezpieczeń - ochrona vs atak.**<br>Uczestnicy dowiedzą się o metodach ataku na sieci Wi-Fi. Zostaną opisane narzędzia wykorzystywane podczas ataków, metody skanowania, metody łamania zabezpieczeń od strony teoretycznej. Opisane zostaną również metody obrony przed typowymi atakami. |
| **14:20-15:00** | *Obiad* |
| **15:00-17:30** | **Ćwiczenia: Łamanie zabezpieczeń sieci bezprzewodowych. Znalezienie klucza WEP oraz próba odnalezienia klucza WPA.**<br>Uczestnicy uzyskają dostęp do zaszyfrowanych nadajników. Przeprowadzona będzie próba znalezienia klucza i podłączenia się do zabezpieczonego nadajnika. |
| **17:30-17:40** | *Podsumowanie I dnia* |

### Agenda - dzień drugi

| | |
|---|---|
| **09:00-09:05** | *Rozpoczęcie drugiego dnia* |
| **09:05-10:00** | **Wykład: Stosowane praktyki zabezpieczenia sieci Wi-FI.**<br>Wykład będzie głównie poświęcony opisowi najlepszych praktyk stosowanych w celu poprawienia bezpieczeństwa sieci Wi-Fi. Uczestnik dowie się jakie rzeczy należy mieć na uwadze dobierając sprzęt sieciowy. |
| **10:00-10:20** | *Przerwa kawowa* |
| **10:20-12:20** | **Ćwiczenia: Łamanie zabezpieczeń sieci bezprzewodowych w systemach Windows i Linux. Inne metody.**<br>Uczestnicy uzyskają dostęp do zablokowanych nadajników. Przeprowadzona będzie próba podłączenia się do nadajnika autoryzującego adresy MAC. |
| **12:20-12:40** | *Przerwa* |
| **12:40-14:00** | **Podsumowanie i Test zdobytej wiedzy**<br>Skrócone podsumowanie wiedzy w zakresie sieci bezprzewodowych. Pokaz konfiguracji punktów dostępowych w celu maksymalnego zabezpieczenia. Test zdobytej wiedzy. |
| **14:00-14:10** | *Podsumowanie i zakończenie* |
| **14:10-15:00** | *Obiad* |

**Dodatkowe informacje i zapisy:**

W celu uzyskania dodatkowych informacji zapraszamy do odwiedzenia naszej strony internetowej. Z chęcią odpowiemy również na wszelkie pytania pod podanymi numerami kontaktowymi. Zapisów na szkolenie można dokonywać na stronie Akademii (**akademia.linuxmagazine.pl**) lub wysyłając zgłoszenie faksem lub emailem.

**Kontakt:**

Akademia Linux Magazine, alm@alm.org.pl, tel.: 022 742 14 57.