

Budowa wydajnych systemów Firewall w oparciu o rozwiązania Open Source

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.

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:

Najważniejszą kwestią związaną z bezpieczeństwem infrastruktury informatycznej przedsiębiorstwa czy instytucji, jest zapewnienie właściwej ochrony przed niepożądanym dostępem z zewnątrz. Zadanie to spełniają systemy firewall. **Współczesne firewalle** nie tylko chronią naszą sieć przed intruzami z zewnątrz, ale także zapewniają szereg dodatkowych usług w postaci: kontrolowania i analizy ruchu w sieci, blokowania potencjalnych ataków, udostępnienia lub ograniczenia dostępu do usług sieciowych użytkownikom zewnętrznym i wewnętrznym oraz umożliwiającą zdalną pracę poprzez wirtualne sieci prywatne.

Celem szkolenia jest pokazanie w jaki sposób, w oparciu o dostępne darmowe oprogramowanie i narzędzia Open Source, stworzyć wydajny system Firewall, umożliwiający właściwą ochronę sieci wewnętrznej przed intruzami oraz posiadający pełną funkcjonalność nowoczesnego firewalle. Poprzez zmiany parametrów konfiguracyjnych systemu dostępnych w katalogu `/proc/` zwiększymy jego stabilność oraz wydajność. Pokażemy również w jaki sposób, dzięki wykorzystaniu mechanizmów uwierzytelniania i proxowania, kontrolować dostęp do Internetu dla użytkowników sieci.

Tematyka:

- architektura systemów firewall (funkcjonalność, mechanizm działania, ewolucja i rodzaje nowoczesnych zapór)
- przystosowanie systemu Linux do pracy jako zaporę firewall
- narzędzia Open Source pozwalające na stworzenie zapory firewall
- zasady tworzenia zapory firewall
- logowanie działań zapory firewall
- translacja adresów za pomocą NAT
- optymalizacja wydajności systemu poprzez zmiany w jego parametrach konfiguracyjnych (katalog `/proc/`)
- Squid jako narzędzie uwierzytelniania użytkowników i kontroli dostępu do Internetu
- VPN - wirtualne sieci prywatne

Szkolenie skierowane jest do administratorów sieci, osób odpowiedzialnych za bezpieczeństwo oraz budowę i administrację systemów IT w firmach i instytucjach, którzy chcą zbudować wydajny i szczelny system firewall wykorzystując dostępne darmowe narzędzia Open Source.

Dzięki szkoleniu uczestnicy dowiedzą się:

- 1) Z jakich systemów i narzędzi Open Source należy skorzystać, aby stworzyć wydajny firewall. Gdzie może je znaleźć (oprogramowanie, dokumentację)
- 2) Jak zainstalować system zapory (krok po kroku)
- 3) Jak skonfigurować firewalle (reguły zapory, zasady translacji adresów, uwierzytelnianie użytkowników, dostęp do zasobów); o czym trzeba pamiętać, aby zaporę była bezpiecznie skonfigurowana
- 4) Jak skonfigurować serwer proxy tak, aby zapewnić kontrolę nad dostępem do stron www.
- 5) Jak filtrować ruch w sieci (np. uniemożliwić dostęp do programów P2P, czy stron HTTPS)
- 6) Jak monitorować pracę firewall (obciążenie sieci, aktywność użytkowników, próby penetracji sieci, automatyczne reguły działania)
- 7) Jak zoptymalizować skonfigurowanego wcześniej firewalle

Wymagania względem uczestników: Każdy z uczestników szkolenia powinien posiadać podstawową wiedzę na temat zagadnień dotyczących sieci TCP/IP, protokołów sieciowych TCP/IP - TCP, UDP, ICMP, podstawowych komend w systemach Linux, pozwalających na swobodne poruszanie się po systemie w trybie konsoli, podstawowego programowania skryptów w języku BASH.

Informacja o prowadzącym: *Michał Kustosik* jest absolwentem Politechniki Łódzkiej. Od kilkunastu lat zajmuje się zagadnieniami związanymi z bezpieczeństwem systemów i sieci informatycznych. W ciągu swojej kariery zawodowej zdobył szereg certyfikatów, potwierdzających jego specjalistyczną wiedzę z tej dziedziny. Obecnie pracuje jako kierownik działu IT i odpowiada za koordynację działań związanych z bezpieczeństwem systemów informatycznych i sieci komputerowych. Swoją rozległą wiedzę i doświadczenie wykorzystuje również podczas prowadzenia zajęć akademickich i szkoleń.

Budowa wydajnych systemów Firewall w oparciu o rozwiązania Open Source

Agenda - dzień pierwszy

09:20-09:50	<i>Rejestracja</i>
09:50-10:00	<i>Powitanie</i>
10:00-10:45	WYKŁAD: „Zasady działania i konfiguracji systemów firewall, translacja adresów” Na wykładzie przedstawiony zostanie krótki rys historyczny systemów firewall w oparciu o system operacyjny Linux. Poruszone zostaną teoretyczne podstawy projektowania wydajnych systemów firewall i ich konfiguracji. Przedstawione zostaną różnice między adresami prywatnymi i publicznymi oraz poruszony zostanie temat związany z translacją adresów IP, zarówno jej zaletami jak i wadami.
10:45-11:05	<i>Przerwa</i>
11:05-12:05	ĆWICZENIA: „Instalacja systemu Linux i przystosowanie go do pracy jako szczelny i wydajny firewall” Na zajęciach uczestnicy zainstalują system operacyjny Linux i zoptymalizują jego działanie do pracy jako szczelny i wydajny firewall.
12:05-12:25	<i>Przerwa</i>
12:25-14:00	ĆWICZENIA: „Konfiguracja systemu Linux do pracy jako firewall w oparciu o dostępne narzędzia Open Source - część 1/2” Uczestnicy poznają znaczenia komend stosowanych przy budowie systemów firewall oraz praktyczne aspekty dotyczące jego konfiguracji. Zbudowana zostanie szczelna zaporą skutecznie chroniąca sieć LAN.
14:00-14:40	<i>Obiad</i>
14:40-17:00	ĆWICZENIA: „Konfiguracja systemu Linux do pracy jako firewall w oparciu o dostępne narzędzia Open Source - część 2/2” Uczestnicy zapoznają się z możliwościami logowania zdarzeń oraz ich analizy jako pierwszego etapu wykrywania intruzów. Porównają również możliwości skonfigurowanego firewalla Linux z możliwościami niektórych urządzeń sprzętowych.
17:00-17:10	<i>Podsumowanie I dnia</i>

Agenda - dzień drugi

09:00-09:10	<i>Rozpoczęcie drugiego dnia</i>
09:10-11:00	ĆWICZENIA: „Praktyczne zastosowanie mechanizmów translacji adresów” W trakcie laboratorium uczestnicy w praktyce zastosują translację adresów. Zoptymalizują również wydajność zapory firewall poprzez zmianę w systemowym katalogu /proc/
11:00-11:20	<i>Przerwa</i>
11:20-12:05	WYKŁAD: „Serwery proxy w systemach Linux” Na wykładzie omówione zostaną zasady działania serwera proxy, poznamy różnicę między działaniem zwykłego a transparentnego serwera proxy. Uczestnicy dowiedzą się również o wymaganiach sprzętowych oraz o możliwościach uwierzytelniania za pomocą proxy.
12:05-12:25	<i>Przerwa</i>
12:25-14:50	ĆWICZENIA: „Praktyczne aspekty proxy na przykładzie serwera Squid” W trakcie zajęć uczestnicy zainstalują serwer Squid oraz poznają znaczenie podstawowych elementów plików konfiguracyjnych. Uczestnicy będą mogli zaznajomić się z możliwościami uwierzytelniania użytkowników oraz blokowania dostępu do Internetu w połączeniu z wykorzystaniem systemów firewall.
14:50-15:00	<i>Podsumowanie i zakończenie</i>
15:00-15:40	<i>Obiad</i>

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 emaillem.

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

