kod szkolenia: LX-BS010 / PL AA 3d

# Bezpieczeństwo w systemach Linux

## Przeznaczenie szkolenia

Szkolenie przeznaczone jest dla administratorów systemów Linux, osób odpowiedzialnych za bezpieczeństwo infrastruktury serwerowej w firmie, entuzjastów wolnego oprogramowania oraz chcących podnieść kwalifikacje w zakresie administracji systemami Linux i ochrony systemów informatycznych.
Ma na celu uczulić na aspekt bezpieczeństwa pracy systemu, współzależności jego elementów i wynikających z tego konsekwencji.
Warsztatowy charakter szkolenia pozwoli szybko nabyć umiejętnosci praktycznych w zakresie zabezpieczania systemów Linux.
Szkolenie prowadzone jest glównie w oparciu o system CentOS, ale zaprezentowane rozwiązania sprawdzą się niezależnie od używanych dystrybucji.
Jeśli zastanawiasz się czy Twój system jest bezpieczny, miałeś incydent bezpieczeństwa we własnej firmie – to szkolenie jest wlaśnie dla Ciebie

## Korzyści wynikające z ukończenia szkolenia

Uczestnicy po szoleniu:

- nabiorą wiekszej świadomosci pracy systemu Linux pod kątem cybersecurity
- bedą mogli dokonać analizy bezpieczeństwa zarządzanych przez siebie środowisk
- nabiorą umiejętności wdrożenia automatyzacji zabezpieczeń serwerów
- szybko usprawnią pracę własnych instalacji
- naprawią ewentualne błędy bezpieczeństwa
- właściwie zabezpieczą wlasne dane
- zapobiegną wyciekowi danych

Poznanie mechanizmów zabezpieczeń działających w systemach Linux, umiejętność ich prawidłowej konfiguracji, celne diagnozowanie oraz skuteczne monitorowanie to glówne korzyści dla uczestników tego szkolenia. Po szkoleniu uczestnicy będą mogli samodzielnie przeprowadzić audyt bezpieczeństwa systemów Linux.

## Oczekiwane przygotowanie słuchaczy

Wymagana znajomość systemów Linux na poziomie RHCSA, sprawne posługiwanie się terminalem, znajomość protokołu TCP/IP.

## Język szkolenia

- Szkolenie: polski
- Materiały: angielski

## Czas trwania

3 dni / 21 godzin

## Agenda szkolenia

1. Monitorowanie systemu Linux pod kątem bezpieczeństwa
   - Integralność plików
   - Wyszukiwanie rootkitów, trojanów itp.
   - Skanowanie systemu w celu wykrycia podatności
2. Zabezpieczanie systemu
   - Konfiguracja metod uwierzytelniania i autoryzacji
   - Wdrożenie centralnego systemu uwierzytelniania
   - Konfiguracja firewall
   - SELinux
3. Zabezpieczanie logów systemowych
   - Konfiguracja serwisów logujących
   - Wdrożenie centralnego logowania zdarzeń
   - Auditd
4. Bezpieczeństwo fizyczne serwera

- Kontrola pamięci typu USB
- Bezpieczeństwo rozruchu systemu
- Szyfrowanie dysków

5. System okiem hakera
   - Skanowanie systemu pod kątem podatności
   - Sniffing – metody obrony
6. Elementy kryptografii
7. Kali Linux – system Linux okiem hakera