SZKOLENIE ŚREDNIO ZAAWANSOWANE

Zabezpieczenie transmisji danych w sieci

VPN

Czas trwania: 2 dni (16h)

Cele szkolenia

- Zapoznanie z technikami zabezpieczenia transmisji sieciowej przed podsłuchem i modyfikacją danych
- Omówienie infrastruktury klucza publicznego (ang. Public Key Infrastructure, PKI) wykorzystywanej przy tego typu rozwiązaniach do uwierzytelniania użytkowników mających prawo korzystać z bezpiecznych połączeń
- Poznanie mechanizmów ochrony informacji oraz infrastruktury klucza publicznego na praktycznych przykładach
- Konfiguracja elementów wymaganych do realizacji bezpiecznych tuneli takie jak lokalne centrum certyfikacji
- Wykorzystując wygenerowane certyfikaty uruchomienie protokołu HTTPS oraz zdalnego dostępu z wykorzystaniem systemu OpenVPN

Zalety

- Program kursu obejmuję część teoretyczną oraz dużą liczbę ćwiczeń pozwalających praktycznie sprawdzić działanie omawianych technik
- Praktyka przed teorią - wszystkie szkolenia technologiczne prowadzone są w formie warsztatowej. Konieczna teoria jest wyjaśniana na przykładzie praktycznych zadań
- Konkretne umiejętności - w ramach każdego szkolenia rozwijamy praktyczne umiejętności związane z daną technologią i tematyką
- Nauka z praktykami - wszyscy trenerzy na co dzień pracują w projektach, gwarantuje to dostęp do eksperckiej wiedzy i praktycznego know-how

Dla kogo?

- Szkolenie adresowane jest do administratorów sieci oraz osób odpowiedzialnych za wdrażanie polityki bezpieczeństwa w oparciu o mechanizmy sieciowe
- Prezentowana wiedza może być także przydatna dla osób odpowiedzialnych za tworzenie oraz weryfikowanie wdrożenia polityki bezpieczeństwa

Wymagania

- Od uczestników szkolenia wymagana jest znajomość podstawowych zagadnień związanych z sieciami komputerowymi (podstawowe protokoły i mechanizmy sieciowe, adresacji itp.) oraz

podstawowa znajomość konfiguracji aplikacji w systemie Linux

Program

1. Usługi ochrony informacji
    a. Poufność
    b. Uwierzytelnienie
    c. Ochrona Integralności
    d. Szyfry
    e. Funkcje skrótu
    f. Omówienie i konfiguracja PKI
2. Bezpieczeństwo transmisji
    a. Potrzeba szyfrowania danych
    b. Ataki na niezabezpieczoną transmisję
    c. Proxy szyfrujące
    d. Tunelowanie
    e. Protokoły VPN
    f. IPsec
3. Konfiguracja wybranych mechanizmów
    a. Konfiguracja protokołu HTTPS w serwerze Apache
    b. Konfiguracja tunelu z wykorzystaniem protokołu SSH
    c. Konfiguracja dostępu zdalnego z wykorzystaniem OpenVPN