

Security/Bezpieczny administrator - praktyczny warsztat z bezpieczeństwa IT



Przeznaczenie szkolenia

Celem przeprowadzenia warsztatów jest przygotowanie personelu działów IT do oceny bezpieczeństwa organizacji za pomocą wybranych narzędzi.



Korzyści wynikające z ukończenia szkolenia

- Ocena realnego stanu bezpieczeństwa infrastruktury firmy
- Podniesienie wiedzy i umiejętności personelu technicznego odpowiedzialnego za utrzymanie systemów
- Zapoznanie się z najlepszymi praktykami związanymi zabezpieczeniami infrastruktury IT
- Poznanie wybranych narzędzi stosowanych w bezpieczeństwie IT
- Możliwość wykonywania audytów bezpieczeństwa we własnym zakresie



Oczekiwane przygotowanie słuchaczy

- Podstawowa znajomość obsługi komputera



Język szkolenia

- Szkolenie: polski
- Materiały: polski



Czas trwania

1 dni / 7 godzin

Agenda szkolenia

1. Wprowadzenie do warsztatów

- Omówienie podstawowych zagadnień dotyczących bezpieczeństwa IT (terminologia, ryzyko i elementy zarządzania ryzykiem, czym jest „hardening” systemów i gdzie szukać źródeł informacji dotyczących utwardzania systemów)

2. Przygotowanie do ćwiczeń

- Omówienie środowiska laboratoryjnego (VMware Workstation, topologia sieci, systemy operacyjne)

3. Elementy „białego wywiadu”

- Omówienie gdzie i jakie informacje dotyczące firmy, jej infrastruktury oraz pracowników potencjalni intruzy mogą znaleźć w Internecie

4. Skanowanie sieci i wykrywanie szczegółów dotyczących systemów operacyjnych i uruchomionych usług

- Omówienie narzędzi wykorzystywanych przy rozpoznawaniu dostępnych systemów, usług oraz urządzeń pracujących w sieci

5. Wyszukiwanie i analiza podatności

- Omówienie przykładowych narzędzi służących do zautomatyzowanego poszukiwania podatności (OpenVAS) w systemach oraz wygenerowanie raportów podsumowujących poziom bezpieczeństwa testowanego środowiska

6. Przełamywanie zabezpieczeń systemów i urządzeń

- Omówienie przykładowych narzędzi i sposobów przełamywania zabezpieczeń systemów. Przejmowanie podatnego systemu na przykładzie Windows, przechwytywanie haseł, obrazu z kamery, plików oraz wejścia klawiatury. Eskalacja uprawnień i przykłady ataków na Active Directory

7. Bezpieczeństwo sieci bezprzewodowych i łamanie haseł

- Analiza bezpieczeństwa sieci bezprzewodowych oraz przechwytywanie ruchu, który umożliwi łamanie haseł dostępowych. Omówienie przykładowych narzędzi. Łamanie haseł WEP i WPA2

8. Socjotechniki w praktyce

- Omówienie wybranych narzędzi wykorzystywanych w atakach socjotechnicznych, przygotowanie środowiska do kampanii socjotechnicznej