KATEGORIA SZKOLENIA

Bezpieczeństwo sieci i testy penetracyjne

Korzyści dla Biznesu:

- Uczestnicy dzięki szkoleniu będą znać techniki ataków i programy wykorzystywane przez współczesnych włamywaczy
- Dowiedzą się w jaki sposób można zabezpieczyć serwery
- Nauczą się korzystać z kilkudziesięciu narzędzi do testowania bezpieczeństwa sieci
- Będą w stanie prowadzić testy penetracyjne

Korzyści dla uczestników

- Celem szkolenia jest poznanie techniki ataków i programów wykorzystywanych przez współczesnych włamywaczy. Uczestnicy dowiedzą się w jaki sposób można zabezpieczyć serwery i usługi na nich pracujące przed atakami oraz poznają rodzaje i etapy testów penetracyjnych oraz metodyki ich prowadzenia.

Zarys Agendy:

1. Wprowadzenie do tematyki testów penetracyjnych
2. Podstawowe testy penetracyjne infrastruktury/sieci
3. Podstawowe testy penetracyjne aplikacji webowych
4. Wtargnięcia i rodzaje ataków
5. Konfiguracja Firewalli
6. Honeypoty
7. Metody ochrony systemów - dobre praktyki
8. Analiza incydentów

Czas trwania	Język szkolenia	Forma szkolenia:
3 dni (21 godzin)	Polski lub Angielski	Wykłady, prezentacje, ćwiczenia

Szkolenie dostosowujemy do jednego z poziomów:

• **PODSTAWOWY** • **ŚREDNIOZAAWANSOWANY** • **ZAAWANSOWANY**

Kontakt

Patryk Dynowski
Business Development Manager

T: +48 577 255 112

E: patryk.dynowski@testarmy.com