Szkolenie: Mile2
Red Team vs Blue Team

Cel szkolenia:

Szkolenie **Red Team vs Blue Team** to oparte na scenariuszach i rywalizacji praktyczne ćwiczenia laboratoryjne, wykonywane w czasie rzeczywistym pod okiem instruktora, który monitoruje działania i postępy uczestników.

Taka forma ćwiczeń daje możliwość wykorzystanie wszystkich posiadanych umiejętności i wiedzy (np. zdobytej w trakcie pozostałych **kursów Mile2**) podczas symulowanych rzeczywistych sytuacji, gdzie w zależności od swojej roli: atakujący (Red) lub obrońca (Blue), atakujemy lub bronimy wskazane zasoby.

Szkolenie trwa dwa dni i składa się z czterech scenariuszy. Trudność poszczególnych scenariuszy jest narastająca, zaczynamy od prostego a kończymy trudnymi zbudowanymi w oparciu o zaawansowane problemy.

Będąc członkiem zespołu niebieskiego (**Blue Team**), będziesz mieć około 45 minut na zapoznanie się z ze swoimi systemami w danym scenariuszu i na załatanie ich potencjalnych podatności. Obrońcy muszą się też trzymać kilku ustalonych zasad np. nie można wyłączać żadnych usług w chronionych systemach, ale można je łatać.

Jako osoba z drużyny czerwonej (**Red Team**) otrzymasz trzy godziny na próby spenetrowania maszyn obrońców. Celem członków zespołu Red jest uzyskanie dostępu do innych systemów w sieci i umieszczenie swoich imion lub nazwy zespołu w pliku flag.txt w katalogu administratora danego systemu.

Po ukończeniu szkolenia **Red Team vs Blue Team**, będziesz:

- Udział w ćwiczeniach Mili2 **Red Team vs Blue Team** pozwala sprawdzić od strony praktycznej posiadaną wiedzę i umiejętności poszczególnych osób mających tworzyć zespoły bezpieczeństwa: ofensywne (wykonujące autoryzowane, okresowe ataki weryfikujące poziom bezpieczeństwa systemów, aplikacji i ludzi) lub zespoły defensywne (zespoły reagowania na incydenty) i upewnić się, że potrafią wykorzystywać aktywnie wyszukane luki w zabezpieczeniach lub też skutecznie bronić się przed atakami. Jest to dobry sprawdzian pozwalający **menadżerom zespołów bezpieczeństwa** mierzyć ich postęp nauki i skuteczność działania.

Kto powinien wziąć udział w szkoleniu:

Przede wszystkim członkowie zespołów red i blue, ale też:

- pracownicy **centrów monitorowania bezpieczeństwa** (SOC)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- pentesterzy
- pasjonaci bezpieczeństwa
- audytorzy sieciowi
- analitycy podatności
- specjaliści ds. bezpieczeństwa
- kierownicy działów bezpieczeństwa
- kierownicy działów IT

Akredytacje i wyróżnienia

Mile2® jest:

- AKREDYTOWANE przez NSA CNSS 4011-4016
- WSKAZANE przez NIST / Homeland Security NICCS's Cyber Security Workforce Framework
- ZAAKCEPTOWANE przez FBI Cyber Security Certification Requirement list (Tier 1-3)

Plan szkolenia:

Scenariusze Red Team vs Blue Team:

- Scenariusz 1 – Kali vs Proximo i Gracchus
- Scenariusz 2 – Kali vs Priscus i Verus
- Scenariusz 3 – Kali vs Maximus i Quintus
- Scenariusz 4 – Kali vs Tetraites i Commodus

Wymagania:

- Minimum 12 miesięczne doświadczenie praktyczne w zakresie technologii sieciowych
- Dobra znajomość protokołu TCP/IP
- Znajomość rozwiązań Microsoft
- Niezbędna jest podstawowa znajomość systemów Linux

Poziom trudności

Certyfikaty:

Uczestnicy szkolenia otrzymują **certyfikat** ukończenia szkolenia wystawiony imiennie oraz na firmę sygnowany przez firmę **Mile2**.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Prowadzący:

Autoryzowany instruktor Mile2 (Certified Mile2 Instructor).

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001