Training: Mile2
Red Team vs Blue Team

TRAINING GOALS:

The **Red Team vs Blue Team** is a scenario-based, hands-on lab experience. The goal is to put together items learned during Mile2 courses and apply them in this environment. It consists of two days (four scenarios) ranging from easy to intermediate to advanced problem sets.

As a Blue team individual, you will be given approximately 45 minutes to review the target systems within your scenario and potentially patch vulnerabilities. ***NOTE: You cannot disable any services on the system, but you can patch it***. You are authorized to change the default credentials for the user “playerone”, however, that password will be given to the mile2 range monitor. ***NOTE: If credentials are changed after the start of the Red Team portion, there will be a timeout period of up to 15 minutes***.

As a Red team individual, you will be given three hours to attempt to exploit other students’ machines. The intent for the Red team is to gain access to other systems in the network and place their name or team name in the flag.txt file in the root/administrator directory.

Upon Completion:

- Graduates of the Mile2 **Red Team vs Blue Team** scenario-based events allow for individuals to piece together a team that will attack based on skillset. This allows managers to assess their current penetration testing and incident response teams to ensure they are able to attack vulnerabilities and defend against attacks.

Who Should Attend:

- Pen Testers
- Ethical Hackers
- Network Auditors
- Cyber Security professionals
- Vulnerability Assessors
- Cyber Security Managers
- IS Managers

Accreditations & Acknowledgements

Mile2® is:

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.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- ACCREDITED by the NSA CNSS 4011-4016
- MAPPED to NIST / Homeland Security NICCS's Cyber Security Workforce Framework
- APPROVED on the FBI Cyber Security Certification Requirement list (Tier 1-3)

CONSPECT:

- Red Team vs Blue Team Scenarios
- Scenario 1 – Kali vs. Proximo and Gracchus
- Scenario 2 – Kali vs. Priscus and Verus
- Scenario 3 – Kali vs. Maximus and Quintus
- Scenario 4 – Kali vs. Tetraites and Commodus

REQUIREMENTS:

- A minimum of 12 months' experience in networking technologies
- Sound knowledge of TCP/IP
- Knowledge of Microsoft packages
- Basic Knowledge of Linux is essential

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Mile2 (course completion).

TRAINER:

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.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007