ARISHTI
CONSOLIDATED

AUTOMATE THE RED TEAM
LINUX MALDEV

2025

WHAT IS IT

An beginner-level live training course designed for cyber security professionals looking to enhance their offensive development skills. The program is NOT for beginners in offensive cybersecurity / red team; it is tailored for those planning to enhance their skillset and expertise in red team automation, & offensive development targeting Linux platform.

The live training format provides ~30 intensive hours of interactive lectures, where participants can engage with the trainers and their peers while learning these techniques.

Our curriculum is constantly revised, and updated to incorporate new research and techniques, ensuring you remain a step ahead.

WHAT YOU WILL LEARN

By enrolling in the live training, you will learn:

- Modern defense techniques
  - A guided walkthrough of various techniques used by modern defensive tools, their strengths and weaknesses.
- Offensive techniques
  - Deep dive into techniques related to injections, privilege escalations, stealth techniques, EDR evasion methods etc.
- C2 and payload development
  - Build your own multi-stage payload with a basic C2; deploy custom evasion, propagation methods; and bypass various protections in Linux.

SYLLABUS

- Lab deployment (local / cloud)
- Linux programming primer
- Preparing the common framework (C2 and payload)
- Building the payload (single and multi-stage payload, extensible payloads)
- Injection methods
- Stealth techniques to cover own tracks (hiding process, network, file etc.)
- Persistence techniques
- Privilege escalation
- EDR internals and bypass methods (evading from process monitoring, file integrity monitoring etc.)
- Lateral movement
- Handling network segmentation (pivoting, proxies, network tunnels etc.)
- Capstone project: automating the attack chain

PREREQUISITES

To ensure participants are prepared for the live training, students should meet the following prerequisites:

- **Prior programming experience:** proficiency in C++ (**C++14 or above**), POSIX API, and shell scripting is crucial to understand most of the techniques.
- **Familiarity with C2 frameworks:** basic understanding of how command & control systems operate.
- **Linux internals:** basic knowledge about process and threads, permissions, process management, memory, system calls is required.
- **Curios mind:** Motivation to learn difficult techniques, practice them until they become second nature, and complete the labs.

TARGET AUDIENCE

The course is ideal for:

- Penetration testers
- Red Team folks
- Blue Team folks
- Security researchers
- Security analysts

If you are someone:

- trying to advance your malware development skills
- interested in deepening your understanding of attack and defense methods
- interested in learning how to deploy offensive tools in complex scenarios

This course is for you.