CYBERTECH

Built by brothers. Powered by precision. Designed to prevent.

Detailed overview of the Red Team Essentials workshop.

Course master: Timo Puistaja

- **Day 1 (10:00 - 17:00):** Attacking Web applications & Privilege Escalation
  - Identifying and exploiting WordPress vulnerabilites
  - Cracking the admin password and gaining system access
  - Establishing a reverse shell and customizing it
  - Analyzing MySQL and server configuration files
  - Escalating privileges through Linux services

- **Päev 2 (09:00 - ~15:00):** Lateraalne liikumine ja domeeni ülevõtmine
  - Navigating the network using SSH and ProxyChains
  - Performing Kerberocasting and exploiting service accounts
  - Leveraging Metasploit and Mimikatz
  - Taking control of the domain controller
  - Surprise challenge at the end

For RTE, each participant gets access to a personal virtual machine running Kali Linux, accessed via the Windows Remote Desktop app. From this machine, they simulate real red team attacks against a private subnet of target systems, including Windows servers and vulnerable services. No local setup needed — everything runs in a fully isolated, cloud-based lab.

The RTE workshop is built on a guided CTF (Capture The Flag) scoring system that gamifies the full red teaming process. Participants progress step-by-step through attack phases by completing practical tasks, answering scenario-based questions, and capturing flags — all tracked in a live scoreboard. Hints and solutions are available with point deductions, allowing everyone to continue learning without getting stuck. After each challenge, the course master provides detailed feedback and, when time runs out, walks through the correct solution live. The participant with the highest score earns the title of “Top Hacker of the Course.”