



CYBER DEFENCE SIMULATION TRAINING

**Understand Typical Attacks on Corporate Networks
in a Simulated Training Environment**





In the CYBER DEFENCE SIMULATION TRAINING IT Attack Patterns are Demonstrated in Realistic IT Environments.

The Basic Idea

In the unique training concept, typical IT attacks are simulated in “real” corporate networks.

It is the goal of the CYBER DEFENCE SIMULATION TRAINING to create a deep understanding of how attacks on corporate networks work:

- Understand the underlying technical principles of common attacks.
- Learn how to “think like an attacker” in regard to corporate network security.
- Understand the limits of common security products, such as antivirus solutions.
- Prioritize hardening measures correctly.



Target Audience

The CYBER DEFENCE SIMULATION TRAINING is suitable for the following groups:

- System and Network Administrators.
- IT Security Manager and non-technical IT Security Consultants who want to broaden their technical understanding.
- Operations Engineers.

Prerequisites

Hacking experience is not required. However, an affinity for the subject IT security should exist. The required fundamentals are explained in detail at the beginning of each exercise.



The Training in Detail

Attacks against corporate IT infrastructures are simulated in a classical “Red Team vs. Blue Team” approach:

► Red Team – *The attacker site*

The Red Team is represented by experienced SEC Consult trainers.

► Blue Team – *The defender site*

The participants of the training are on the defender side. After a thorough theoretical introduction, the participants learn to, detect, analyze, stop and prevent attacks in various isolated training exercises.

The Training Setup

Every participant receives access to their own simulated corporate IT infrastructure. Various common IT products are deployed in that IT infrastructure:

- Windows domain infrastructure with various clients
- Windows and Linux server systems
- Antivirus solutions
- Web Application Firewalls (WAF)
- IT Monitoring and SIEM solutions.

The Agenda in Detail

The training will cover the typical **Attacker Kill Chain** from start to finish:

- | | |
|-----------------------|------------------------|
| 1. Reconnaissance | 4. Escalate Privileges |
| 2. Initial Compromise | 5. Move Laterally |
| 3. Establish Foothold | 6. Complete Mission |

During the training, the following technical aspects are covered in detail with various Do-It-Yourself demos:

- Windows Domain Specific Security (Pass-The-Hash, etc.)
- Web Based Attacks Including SQL Injection, XSS and others
- Privilege Escalation to Root on Windows and Linux Environments
- Social Engineering with Malicious Attachments
- Anti-Virus (AV) Bypasses
- Network Based Attacks.

“Only if modern attack techniques are understood on a technical level, one can successfully detect, analyze, stop and prevent attacks in the long run.”

Andreas Falkenberg

Training Agenda in Detail – Red VS Blue

Time	Day 1	Day 2	Day 3
09:00–12:00	1. Awareness	5. Attacker Kill Chain: Initial Compromise Through Web Based Attacks <ul style="list-style-type: none"> – XSS Vulnerabilities – SQLi Vulnerabilities – File Uploads 	8. Attacker Kill Chain: Establish Foothold & Escalate Privileges on Windows Domain based Systems <ul style="list-style-type: none"> – Windows Based Hash Attacks – Local Privilege Escalations – Windows Network Pivoting Attacks
12:00–13:00	Lunch	Lunch	Lunch
13:00–15:00	2. Introduction <ul style="list-style-type: none"> – Overall Training Infrastructure Introduction 3. Hack-Like-A-Script-Kiddy <ul style="list-style-type: none"> – Metasploit Tool Introduction 	6. Attacker Kill Chain: Establish Foothold & Escalate Privileges on Web Based Systems <ul style="list-style-type: none"> – Various Root Exploits on Linux Machine 	8. Attacker Kill Chain: Establish Foothold & Escalate Privileges on Windows Domain based Systems <ul style="list-style-type: none"> – Anti-Virus (AV) Bypasses – The Limitations of Security Products – Other Network Based Attacks 9. Attacker Kill Chain: Complete Mission <ul style="list-style-type: none"> – Steal “Crown Jewels”
15:00–17:00	4. Attacker Kill Chain: Reconnaissance and the Limitations of Security Tools <ul style="list-style-type: none"> – High Noise Scans – Low Noise Scans 	7. Attacker Kill Chain: Initial Compromise by (Spear)-Phishing Attacks <ul style="list-style-type: none"> – Malicious Emails / Social Engineering 	10. Crypto Trojans in Corporate Environments 11. Outro

We are glad to answer all your remaining questions:

SEC Consult (Luxembourg) SARL
 Frank Trenz
 25, Avenue de la Gare
 4131 Esch-sur-Alzette,
 office-berlin@sec-consult.com
www.sectower.com

C3 – Cybersecurity competence center
 Dr. Jérôme Jacob
 16 bvd d'Avranches
 L-1160 Luxembourg
 info@securitymadein.lu
www.c-3.lu