satisnet
streamlining security management

CYBERKOMBAT
REAL WORLD SECURITY TRAINING

HONEYCOMB

CYBER DEFENCE PURPLE SIMULATION TRAINING

Understand Typical Attacks on Corporate Networks in a Simulated Training Environment.
Learn Attack(Red) and Defence(Blue) Perspetives

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
- Operations Engineers
- IT Security Manager and non-technical IT Security Consultants who want to broaden their technical understanding
- IT Forensic staff and Secure Operations Centre (SoC) staff who are just starting out in the field.

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 CyberKombat 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 is divided 10 chapters and 20 scenarios

CHAPTER 1	Awareness and war stories
CHAPTER 2	Introduction to the training environment
CHAPTER 3	Reconnaissance and the limitations of security tools
CHAPTER 4	Man-In-The-Middle Attacks – read and manipulate network traffic
CHAPTER 5	Application security and the limits of tool-based attack detection (WAF)
CHAPTER 6	Windows domain security
CHAPTER 7	Mental training – Breakout session
CHAPTER 8	Ransomware in corporate networks
CHAPTER 9	Social Engineering with malicious attachments
CHAPTER 10	Antivirus (AV) bypasses – The limitations of AV products

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

John McCann

satisnet
streamlining security management

CYBERKOMBAT
REAL WORLD SECURITY TRAINING

HONEYCOMB

TRAINING AGENDA IN DETAIL – RED VS BLUE

Time	Day 1	Day 2	Day 3	Day 4
09:00–12:00	**1. Awareness and War Stories**	**4. Man-In-The-Middle Attacks (MitM)** – ARP Spoofing 1 "Request – ARP Spoofing 1 "Response – SSL/TLS – MitM Attacks – SSL Strip V2.0	**6. Windows Domain Security** – Local NTLM Recovery and Password Cracking – Lateral Movement in a Windows Environment – NTLM Hash Abuse 1 – NTLM Hash Abuse 2	**8. Ransomware in Corporate Networks** **9. Social Engineering with Malicious Attachments**
12:00–13:00	Lunch break	Lunch break	Lunch break	Lunch break
13:00–15:00	**2. Introduction** – Overall Introduction to the Training Environment – Advanced Tool Introduction – Exploit Net API – Exploit vsftpd	**5. Application Security and the Limits of Tool Based Detection** – XSS Vulnerabilities – SQLi Vulnerabilities	**7. Mental Training – Breakout Session** – How to work in high stress situations	**10. Antivirus (AV) Bypasses – The Limitations of AV Products** – Simple AV Bypass
15:00–17:00	**3. Reconnaissance and the Limitations of Security Tools** – High Noise Scans – Low Noise Scans	**5. Application Security and the Limits of Tool Based Detection** – Shell/RCE Vulnerabilities – Upload Vulnerabilities	**7. Mental Training – Breakout Session** – How to work in high stress situations	**10. Antivirus (AV) Bypasses – The Limitations of AV Products** – Complex AV Bypass

We are glad to answer all your remaining questions:

Satisnet Ltd
Suite B, Building 210,
The Village,
Luton,
LU28DL
enquiry@satisnet.co.uk
www.satisnet.co.uk

Honeycomb Technologies Ltd
Hexagon House,
Station Lane,Witney,
Oxfordshire
OX28 4BN

www.honeycomb.co.uk