

Compass Training

Expand your security skills



Compass Security AG
Werkstrasse 20
Postfach 2038
CH- 8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch



Compass Education Lab

Ivan Bütler [ivan.buetler@csnc.ch]

What does Compass Education offer?

Only those who know current and future attacking techniques will be able to protect themselves effectively from hacker attacks in the long run. Compass Security AG has developed its own security lab which is available for **hands-on trainings, in-company trainings, hacking demonstrations and the organisation of wargames**. Trainings can be held on site or via the Internet. This laboratory is being expanded continuously and complemented with the latest cases in theory and practice. This flyer informs you about the presently existing "cases", giving you an overview of the many topics already covered.



The core of the Web App security lab is a webshop programmed in Java called "**Glocken-Emil**" (or "cow-bell shop"). The participant can train web based attacks and counter measures in practical exercises.. For each topic there is a theory module as well as a practice exercise provided in the lab.

Why a bell shop and not the solution of OWASP with WebGoat? In the bell shop there is a business case with products, login, payment, transactions, news, comment windows, talk, RSS feed, SOAP interface and further features. The participant learns on the base of an application which makes the topics much more comprehensible.

OWASP - Web Application Security

The bell shop is built up according the topics of OWASP security in theory and in the laboratory.



The topics include the following basic lab exercises:

- ✦ Authentication Attacks
- ✦ Session Fixation Attacks
- ✦ Session Prediction Attacks
- ✦ Cookie Security
- ✦ Cross Site Scripting
- ✦ Cross Site Tracing
- ✦ Cross Site Request Forgery
- ✦ Second Order Injection
- ✦ Simple and Advanced SQL Injection
- ✦ URL Redirection Attacks
- ✦ Authorisation Bypass Attacks
- ✦ Application Logging / Forensic

For each attacking vector the appropriate counter measure is imparted.



Web 2.0 / AJAX

The cow-bell shop additionally contains XML, SOAP and WSDL interfaces as well as AJAX/Web 2.0 lab exercises. With this extension the participant is also able to practise the following issues in the lab:

- ✦ Social Software Worm Attack (AJAX)
- ✦ AJAX Framework Threats and Exploits
- ✦ XMLHttpRequest Object Analysis (Web 2.0)
- ✦ XSS Shell Attacks
- ✦ RSS/Atom Feed Injection
- ✦ XML External Entity Attacks
- ✦ XML File Inclusion Attacks
- ✦ XML Port Scan
- ✦ XML URL Enumeration
- ✦ XML Path Traversal
- ✦ Flash Hacking & ActiveX Hacking
- ✦ Applet Hacking
- ✦ WSDL Hacking / SOAP Attacks

Virus & Trojan Horses

In current IT security trend analysis the computer of the user is regarded as the weakest link in the chain. From the attacker's point of view the question arises how a Virus/Trojan can be delivered to the computer of the user. After that the attacker must solve the problem of activating the Trojan. If the Trojan is started, the attacker can consider what functionality the Trojan should have. Is it about a Denial of Service attack? Should the Trojan load further malware? Should the Trojan gain Local Admin rights? Should a RootKit

be installed? Should the recently revised files be re-delivered to the Internet? The course environment of Compass Security allows it to practise the three steps of Viruses/Trojans and to learn the defence strategies for each phase.

The course modules dealing with Viruses/Trojans include the following cases:

- ✦ Bypassing Anti-Virus Protection
- ✦ Bypassing Content Filters (SMTP, HTTP/S)
- ✦ Fuzzing & Zero-Day Exploits in the Browser
- ✦ Client Software Exploitation
- ✦ Sony Rootkit
- ✦ USB & U3 Stick Virus
- ✦ Shatter Attack





Spyware Analysis & Forensic

The lab contains some tasks and solutions dealing with the topics Spyware analysis and forensics. The aim is to understand how and where a Trojan can settle and how to analyse its behaviour systematically.

The lab exercises consist of Debugging and Reverse Engineering tasks with OllyDbg, RegMon, FileMon and other Sysinternal tools. The cases included in the relevant scope of topics are:

- ✦ Windows Autostart Analysis
- ✦ EFS File Analysis
- ✦ MS Word Fast Save
- ✦ MS Word Meta Data and Temp Files
- ✦ MS Word Track Changes
- ✦ Uncover PDF
- ✦ File Analysis
- ✦ ADS
- ✦ Steganography
- ✦ Slackspace
- ✦ Sleuthkit Analysis
- ✦ Search for illegal pictures
- ✦ Crypto Analysis Isrunase.exe
- ✦ TCPDUMP Analysis



Terminal Server Security

Many enterprises allow external access to company applications via Citrix or Terminal Server applications. But are those safe? Compass Security has selected some typical Terminal Server (TS) attacks and provided them for the participant in the lab:

- ✦ TS Application Breakout
- ✦ TS Resource Hacking (Shares, Printers)
- ✦ TS Bypass Copy/Paste Protection
- ✦ TS Logon Script Breakout
- ✦ TS Visual Binary Transfer Mode

You will not only learn the tricks of the attacker, but also the practical support in the safeguarding of TS applications.

Man in the Middle Attacks

Since the appearance of „Phishing“ the issue of Man in the Middle has become known. The lab of Compass Security comprises the following MitM cases:

- ✦ Reverse Proxy Man in the Middle
- ✦ Man in the Browser (MitB)
- ✦ Smart Card APDU Man in the Middle
- ✦ Crypto Downgrade Attack with SSL
- ✦ Crypto Downgrade Attack with SSH
- ✦ ARP Spoofing Attacks
- ✦ DNS Cache Poisoning Attacks
- ✦ Firefox Observation Plugin
- ✦ Internet Explorer Observation BHO



Unix Security

Compass Security has gained wide experience in Solaris, but also in the Linux and BSD environment. The know-how has been embedded in the following cases:

- ✦ Restricted Shell Breakout
- ✦ Got R00t
- ✦ Incident Handling / Tripwire / Solaris
- ✦ Process Security – Apache Webserver
- ✦ Chroot'ing Apache Webserver
- ✦ Monitoring Shell Activity

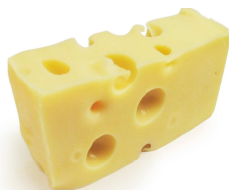
Wireless Security

Things have quieted down regarding Wireless Security since the introduction of WPA2. Wireless lab exercises are provided for the following topics:

- ✦ WLAN/WPA Cracking
- ✦ Rogue Access Point Security
- ✦ Bluetooth Attacks

Bypass Firewall Attacks

A Trojan can attempt to build up a RAT (Remote Administration Toolkit) from inside out to the Internet. Thus an attacker can operate the computer of a victim from the Internet by remote control. Are our IT infrastructures as full of holes as Swiss cheese?



The following lab cases deal with the issues of Tunnelling, Covert Channel and Inside-out attacks:

- ✦ Covert Channel Attacks
- ✦ DNS Tunnel
- ✦ HTTP/S Tunnel
- ✦ SSH Tunnel
- ✦ HTTP Content Based Tunnels
- ✦ GoToMyPC, NetViewer Sessions
- ✦ Netcat Tunnels
- ✦ IPv6 NAT Attack - Teredo
- ✦ TOR Anonymiser Network
- ✦ Web Anonymiser Network



Special Cases

The following cases are additionally provided in the Compass lab:

- ✦ SIP Attacks (VoIP)
- ✦ VLAN Double Encapsulation Attacks
- ✦ VLAN Trunking Attacks
- ✦ DNS Hostname Change Attacks
- ✦ PortSecurity Attacks (EAP)



What kind of training do we provide?

Based on the available cases and the mobile lab environment, individual customer workshops are organised and conducted in Switzerland and abroad. These educational blocks of up to three days support you with the training of IT responsables, developers and Security Officers.

Live Hacking Events

Your company event will be upgraded with Live-Hacking demonstrations by an experienced Compass Security analyst and the spectators will be sensitised concerning IT security. Have you gathered your IT security officers for a meeting? Would you like to make security a real experience and sensitise your staff? Then choose one of our demonstrations. The range is wide!

Training via the Internet?

Would you like to provide an IT security training via the Internet? Take advantage of the online version of Hacking-Lab! You can access our security lab fast and conveniently from all over the world and integrate it into your own seminars.

Hack&Learn - Wargames

Yet in IT, knowledge is consolidated mainly by the relation to practice, by testing out the technique and by the solution of problems. This is the idea of Compass! Hack&Learn!



Public Courses

Please note: These courses are held in German! For courses in English please contact us.

Web Application Security: Basics

The participants know the OWASP Top 10 weaknesses and counter measures. For each attack such as SQL injection, XSS, XSRF or authorisation bypass there is a theoretical and a lab exercise. In addition, the ability for self-assessment and the main basics of HTTP/HTTPS are trained.

Jona (CH):	March 6/7, 2012
Munich (DE):	July 3/4, 2012
Frankfurt (DE):	September 18/19, 2012
Munich (DE):	October 9/10, 2012
Frankfurt (DE):	November 12/13, 2012

Web Application Security: Advanced

The participants expand their knowledge from LAB-WAB in respect of Web 2.0/AJAX and Web Application Firewall. They comprehend additional risks with Web 2.0 applications, the significance of the Same Origin Policy and also Cross Domain (XDR) topics and Mash-Ups.

Jona (CH):	March 8/9, 2012
Munich (DE):	July 5/6, 2012
Frankfurt (DE):	September 20/21, 2012
Munich (DE):	October 11/12, 2012



iPhone & iPad Security

After the course, the participants will be able to identify and eliminate security relevant weaknesses with the iOS devices integration in their own enterprise. They can apply general rules and measures for the safe operation of the common wireless technologies and they are aware of the basic risks involved in the usage of mobile devices. All course topics can be consolidated with practical exercises.

Jona (CH): March 15/16, 2012
Frankfurt (DE): May 3/4, 2012
Cologne (DE): June 5/6, 2012
Hamburg (DE): June 12/13 2012
Munich (DE): June 28/29 2012
Frankfurt (DE): September 12/13, 2012
Munich (DE): October 15/16, 2012
Frankfurt (DE): November, 6/7, 2012

Wireless & Mobile Security

The participant learns how to detect, evaluate and mitigate wireless network weaknesses. Additionally, he will be trained how to design and implement a secure Wifi service based on common wireless technologies and knows their risks.

Jona (CH): April 16/17, 2012
Frankfurt (DE): October 22/23, 2012
Munich (DE): November 21/22, 2012

Networking & Penetration Testing

The participants are aware of the dangers of network attacks. They are able to check their company independently on weaknesses and to initiate and apply the respective counter measures.

Jona (CH): April 18/19, 2012

Network Analysis - Sniffing

The participant learns in theory and on many practical examples the usage of network sniffers and network analysis tools. You will be able to locate and isolate network or firewall problems and determine their causes.

Jona (CH): May 7/8, 2012
Munich (DE): November 19/20, 2012

Forensic Investigation

Despite Data Leak Prevention you have become the victim of a hacker attack. How do you react? How do you analyse the traces? What questions do arise - legally or technically? In the course we are simulating this "case" from A - Z. Part of it are judicial basic considerations, but also Web log analyses, OSX File Carving, the search for Windows Trojans, traces on the data base server, investigations on iPhone and social media.

Jona (CH): February, 2/3, 2012

Further information is available for you on <http://www.csnc.ch/en/securitytraining/> where you may also enrol for these courses.



Offer for Companies

Compass offers individual, company specific trainings on various security topics.

Your advantages:

- ✦ The basic and advanced trainings are tailor-made to suit your needs (topic, level, duration).
- ✦ You benefit from our Hacking-Lab, the security portal for hacking and defence strategies.
- ✦ The IT infrastructure is provided by Compass: Laptops and Hacking-Lab infrastructure.
- ✦ You are trained by competent presenters with a broad and profound expert knowledge and ample practical know-how.
- ✦ The share of hands-on training of min. 50 % guarantees a high level of knowledge transfer.
- ✦ Your participants will be coached by two tutors.
- ✦ You select the location.
- ✦ You benefit from our long term training experience.
- ✦ You receive detailed course documentation.

For further details we remain gladly at your disposal - please do not hesitate to call us!

Interested?

Would you like to know more about your individual company course? Via the Internet or on-site? Are you interested in Hack&Learn? Please do not hesitate to contact us. We look forward to hearing from you.

team@csnc.ch | www.csnc.ch | www.hacking-lab.com