

# National Cyber Storm Competition

## **Hands-On Security Challenges**

### OWASP AppSec Beijing 2013

Ivan Bütler

[ivan.buetler@compass-security.com](mailto:ivan.buetler@compass-security.com)

Compass Security AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

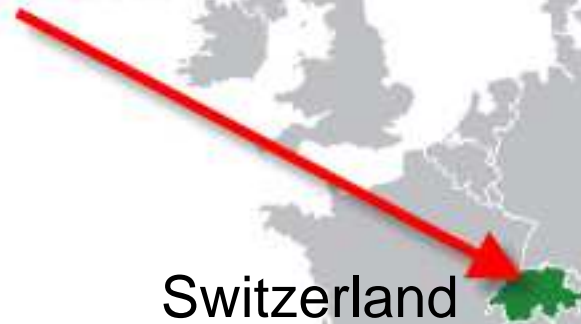
Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

My Name is «Ivan Bütler»

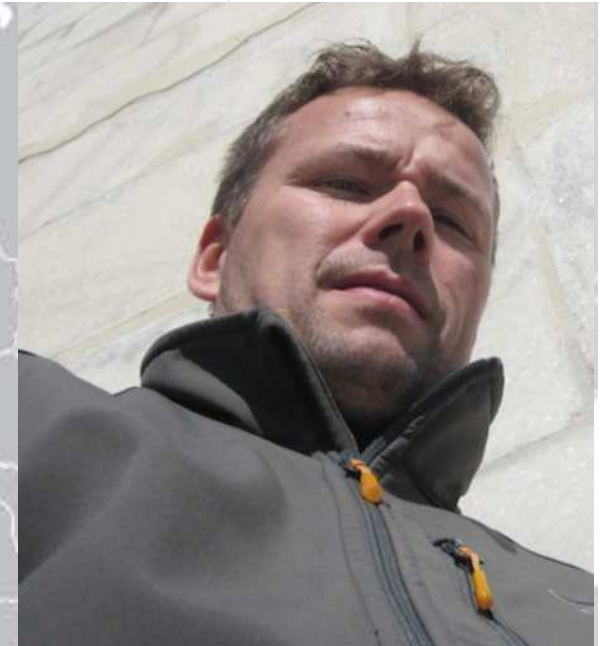


CEO Compass Security AG

This is \$HOME for me



Switzerland



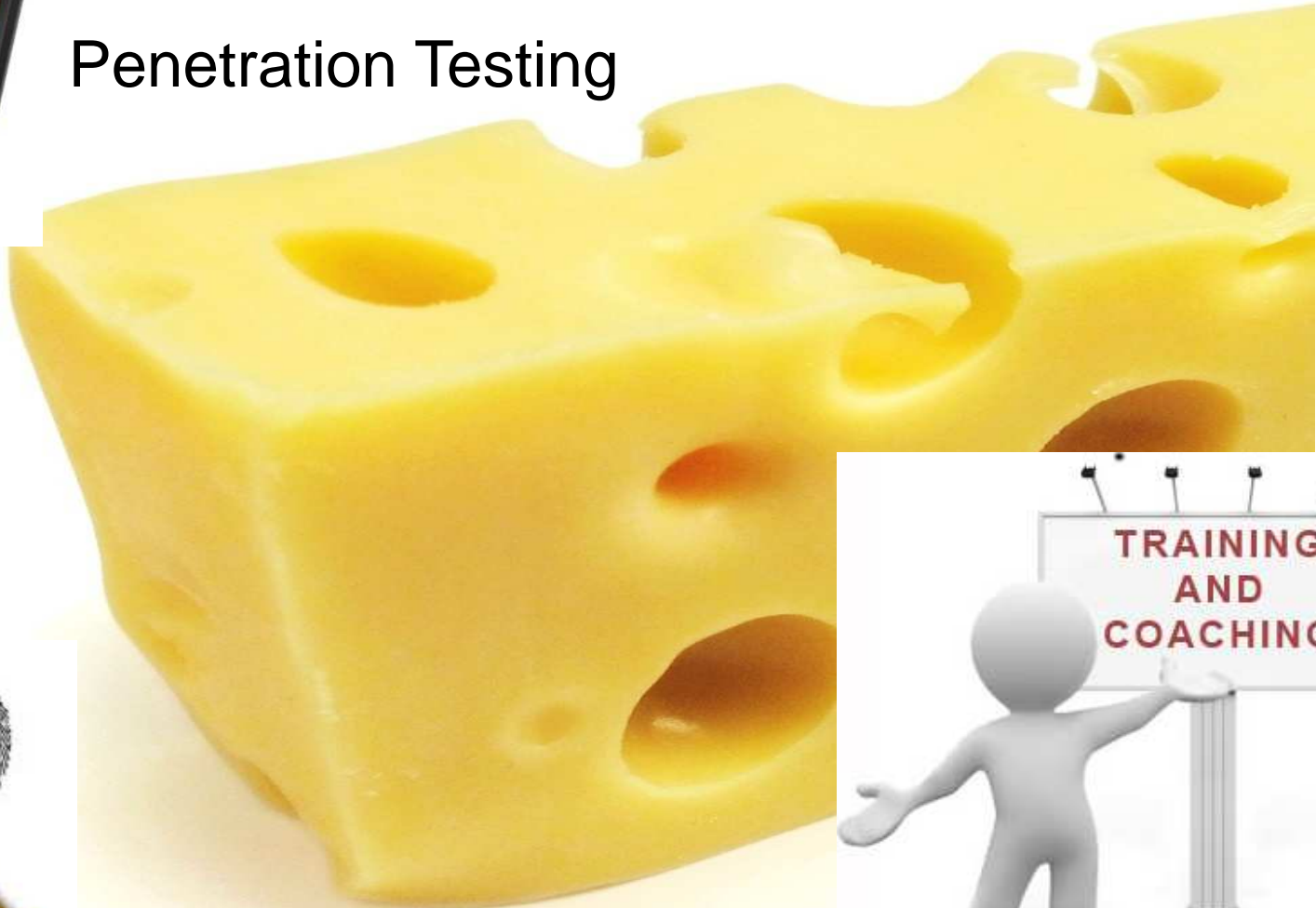
# My Home, Switzerland







## Penetration Testing



## Forensic Analysis



# Why am I here?



HACKING-LAB

- Because we run a Remote Security Lab in Switzerland. It is called **Hacking-Lab**

**Security Puzzles / Challenges / Hands-On**



- Because OWASP is offering free Hacking-Lab **OWASP TOP 10** Web Security Challenges



- Because Hacking-Lab is being used for **NATIONAL CYBER STORM COMPETITIONS**

**At the end:** You should understand how to setup your own **security lab** and how to use the **free** OWASP challenges

A long time ago ...



I was looking for a young jedi knight

俗塵 - 絕地武士

CTF 2007 in Switzerland 







## Fist Swiss Cyber Talent Competition

瑞士的網絡天賦競爭





# 2011 – Swiss Cyber Storm 3



International CTF @ SCS3 in Switzerland



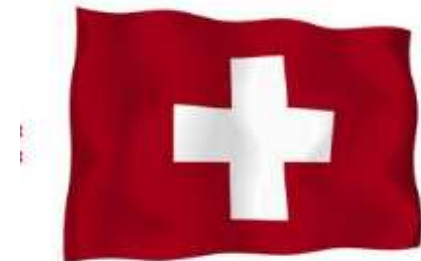
Prize獎 = **New Car**新車



# 2013 - Swiss Cyber Storm 4



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra



# Challenge Categories



Web Security



Malware / Trojan / Bugs



Windows Security



Apple Security



Penetration Testing



Networking



Forensics



Reverse Engineering



VoiP / SS7 / GSM



Wireless Security



Unix / Linux Security



Crypto Challenges



Programming



Fun Challenge



iPhone Challenge



Android Challenge

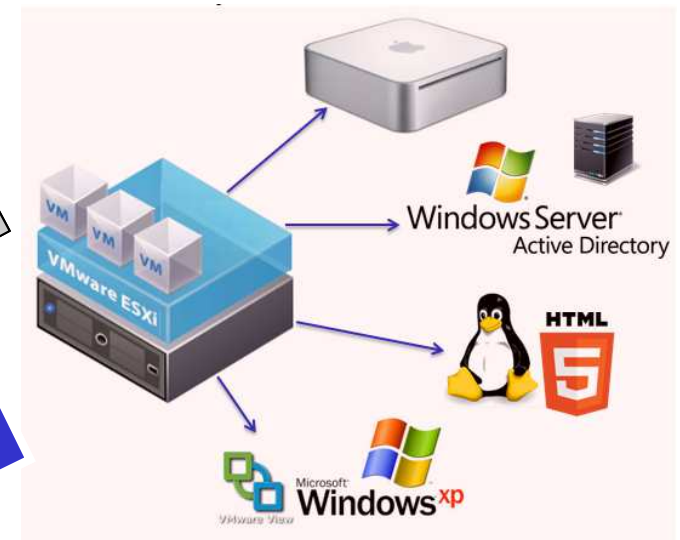
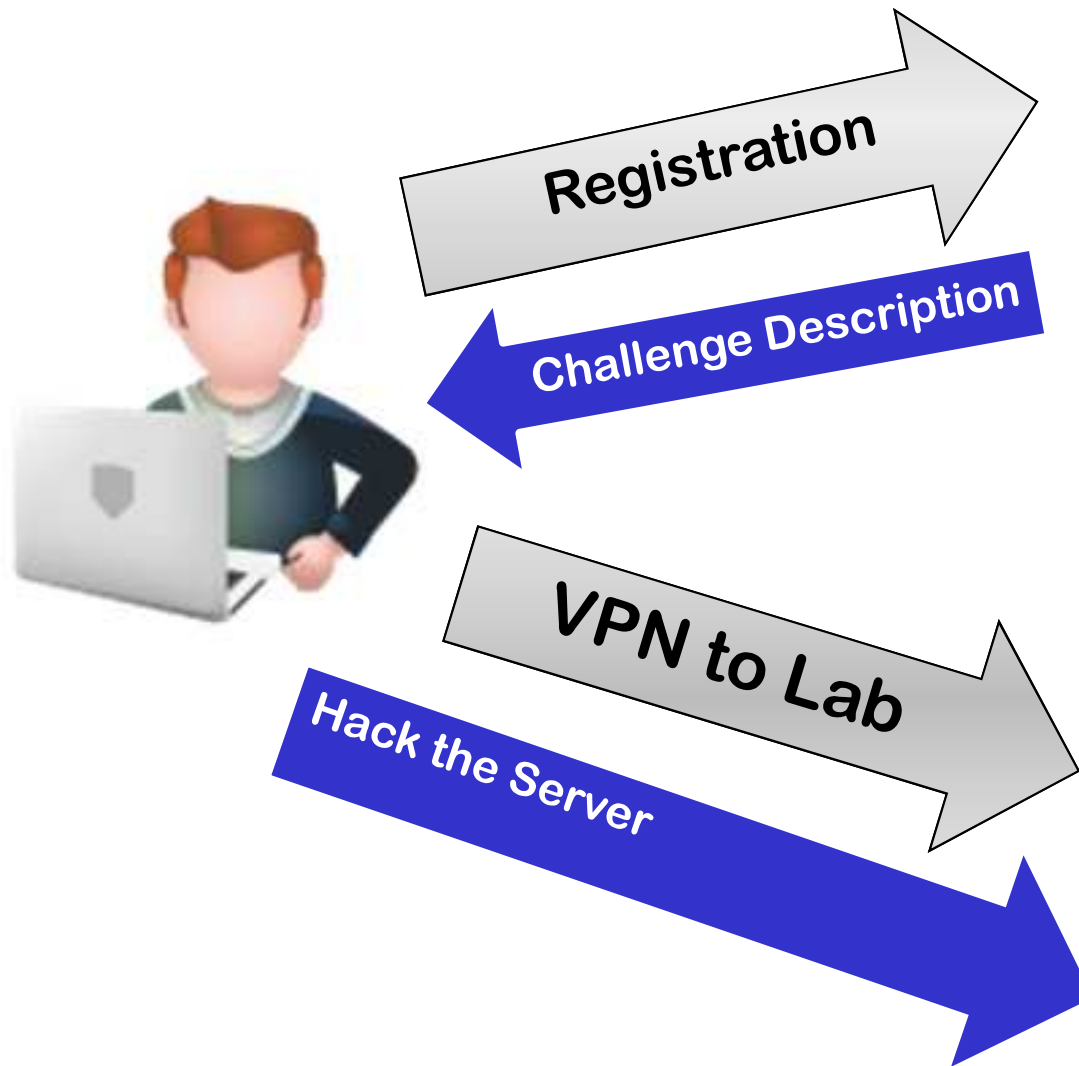


# What is «Hacking-Lab»?????

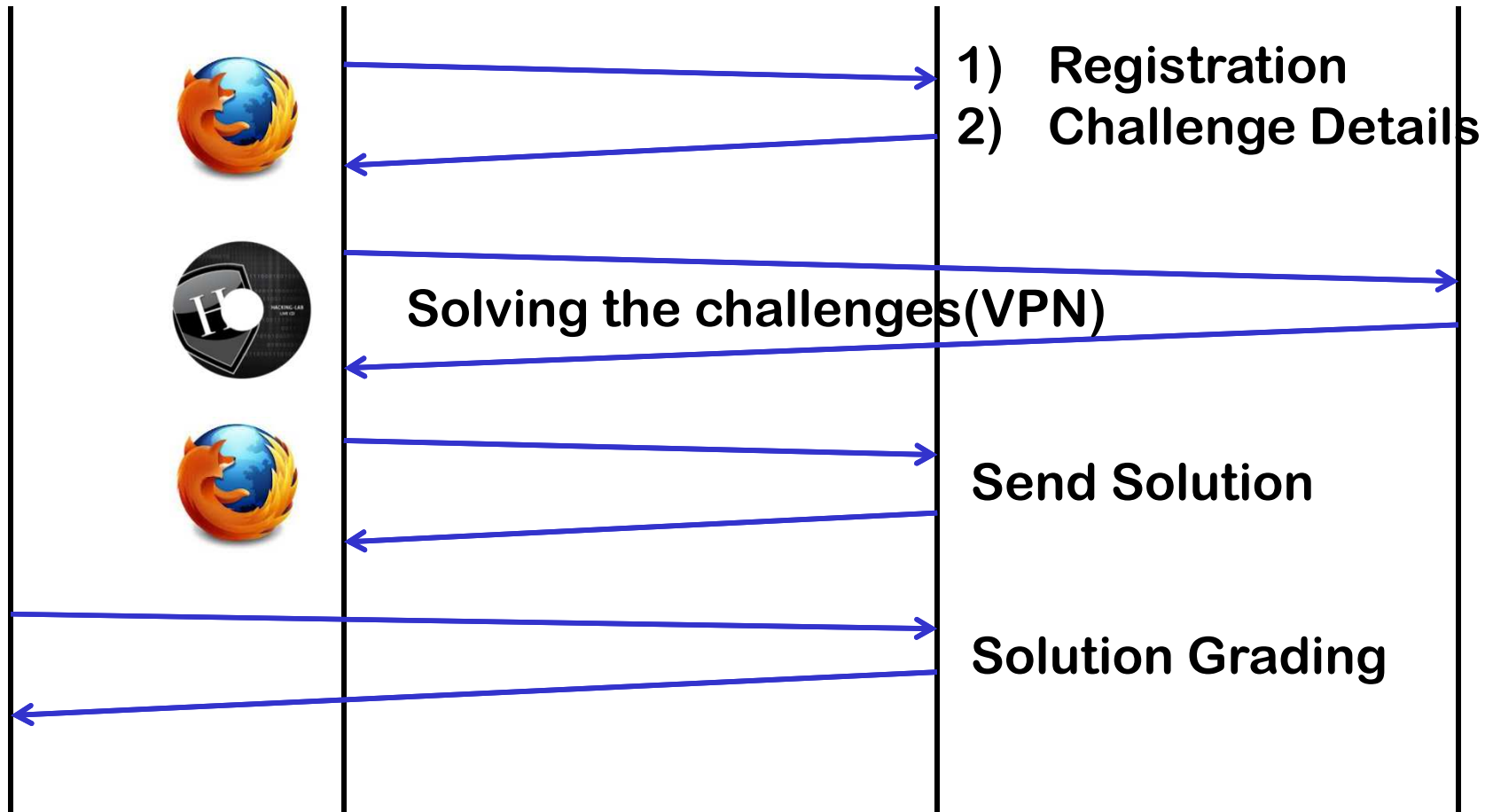
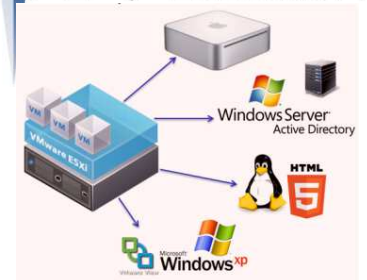
Compass Security AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
team@csnc.ch  
www.csnc.ch

# What is «Hacking-Lab»????



# Understanding Hacking-Lab





# Demonstration Hacking-Lab

SQL Injection & XML External Entity Attack

Compass Security AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
team@csnc.ch  
www.csnc.ch

## Details about «Hacking-Lab»



Compass Security AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
team@csnc.ch  
www.csnc.ch

# What is «Hacking-Lab»????



- (1) Vulnerable Servers and Applications (Web, Windows, Linux, iOS, Android)



- (2) Description about the security challenges



- (3) Tools required for solving the challenges



- (4) Teacher functions (accept/reject solutions) solutions, solution movies



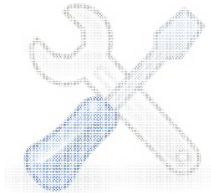
# Details about Hacking-Lab (1/4)



- (1) Vulnerable Servers and Applications (Web, Windows, Linux, iOS, Android)



- (2) Description about the security challenges



- (3) Tools required for solving the challenges



- (4) Teacher function (accept/reject solutions)

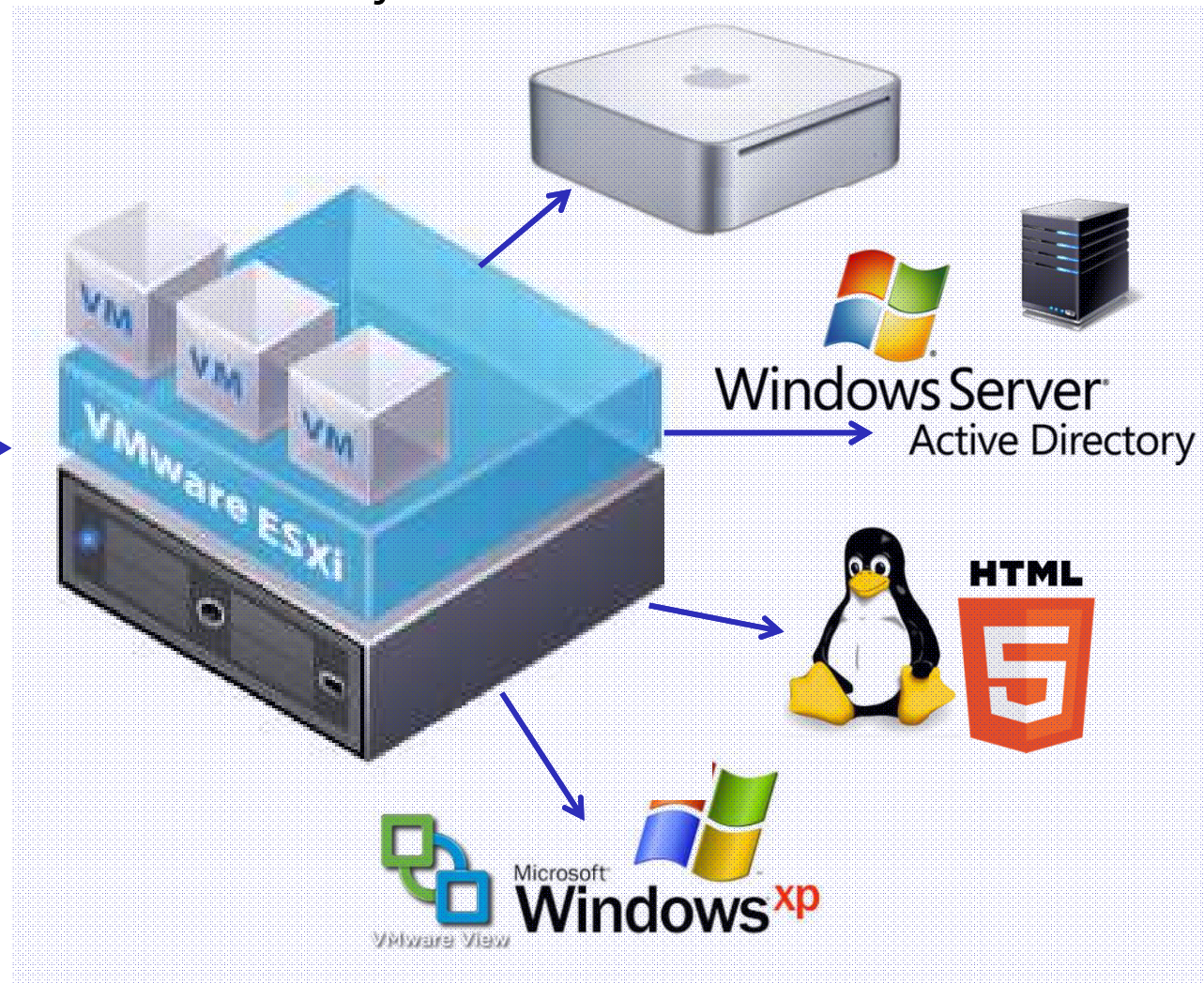
# Details about Hacking-Lab



Vulnerable **Mobile**  
Apps



Vulnerable **Servers**  
Remote Security Lab



**Automatic Revert to Snapshot**

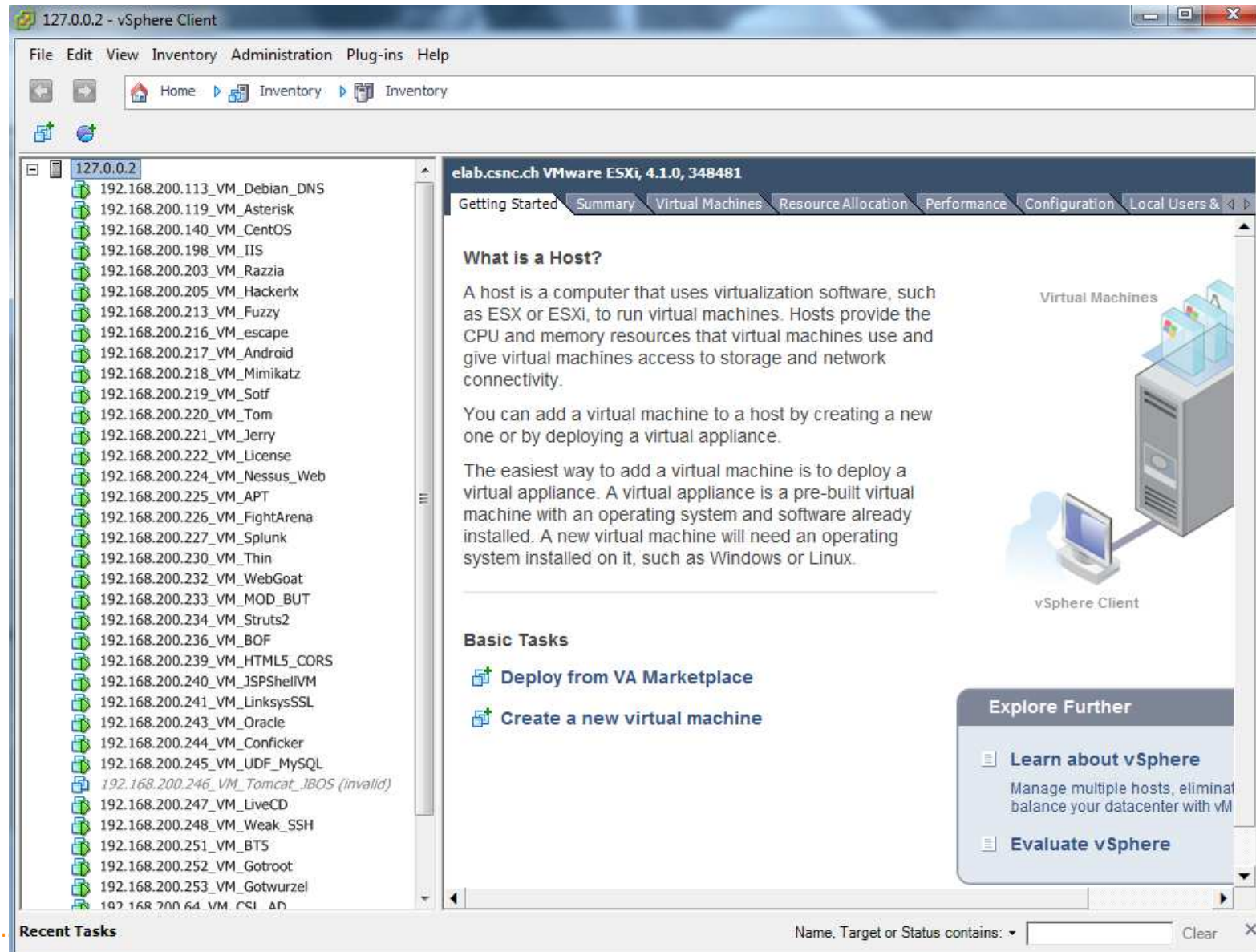
# Movie 1: Vulnerable Servers (ESXi)

Compass Security AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
team@csnc.ch  
www.csnc.ch



# Vulnerable Servers (ESX Virtualization)



# Vulnerable Servers (ESX Virtualization)



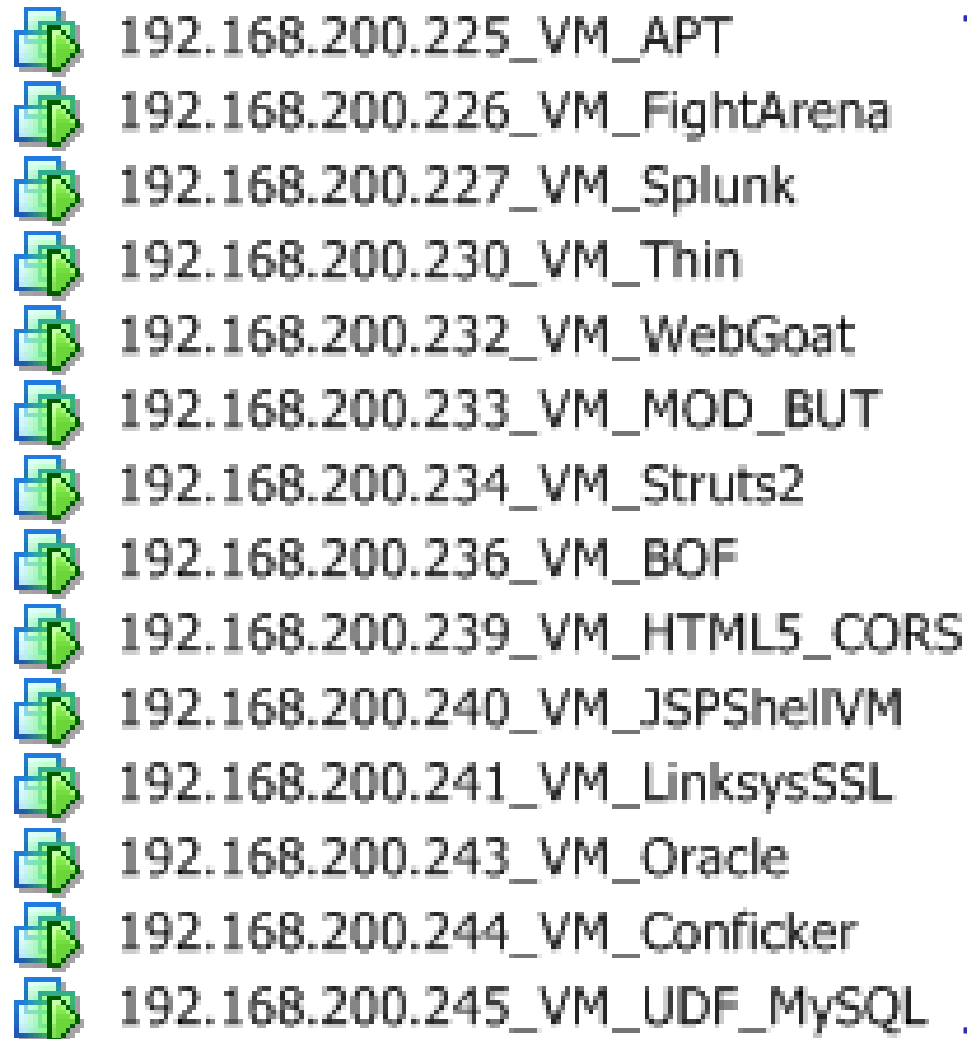
[-] [Icon] 127.0.0.2

- [Icon] 192.168.200.113\_VM\_Debian\_DNS
- [Icon] 192.168.200.119\_VM\_Asterisk
- [Icon] 192.168.200.140\_VM\_CentOS
- [Icon] 192.168.200.198\_VM\_IIS
- [Icon] 192.168.200.203\_VM\_Razzia
- [Icon] 192.168.200.205\_VM\_Hacker1x
- [Icon] 192.168.200.213\_VM\_Fuzzy
- [Icon] 192.168.200.216\_VM\_escape
- [Icon] 192.168.200.217\_VM\_Android
- [Icon] 192.168.200.218\_VM\_Mimikatz
- [Icon] 192.168.200.219\_VM\_Soft
- [Icon] 192.168.200.220\_VM\_Tom
- [Icon] 192.168.200.221\_VM\_Jerry
- [Icon] 192.168.200.222\_VM\_License
- [Icon] 192.168.200.224\_VM\_Nessus\_Web

## Vulnerable Servers

- \* SIP Gateway
- \* IIS
- \* Web Security
- \* Fuzzing Challenge
- \* Python Challenge
- \* Mimikatz
- \* Shell of the Future
- \* License Challenge
- \* Nessus Scanning

# Vulnerable Servers (ESX Virtualization)


A list of 15 IP addresses and VM names, each preceded by a small icon of a folder with a green arrow pointing right. The list is enclosed in a blue bracket on the right side.

192.168.200.225\_VM\_APT  
192.168.200.226\_VM\_FightArena  
192.168.200.227\_VM\_Splunk  
192.168.200.230\_VM\_Thin  
192.168.200.232\_VM\_WebGoat  
192.168.200.233\_VM\_MOD\_BUT  
192.168.200.234\_VM\_Struts2  
192.168.200.236\_VM\_BOF  
192.168.200.239\_VM\_HTML5\_CORS  
192.168.200.240\_VM\_JSPShellVM  
192.168.200.241\_VM\_LinksysSSL  
192.168.200.243\_VM\_Oracle  
192.168.200.244\_VM\_Conficker  
192.168.200.245\_VM\_UDF\_MySQL

## Vulnerable Servers

- \* Splunk Engine
- \* Java Script Arena
- \* Web Goat
- \* Struts Challenge
- \* Buffer Overflow
- \* HTML5 Challenge
- \* JSP Challenge
- \* Oracle Challenges
- \* Conficker
- \* Metasploit Lab

# Vulnerable Servers (ESX Virtualization)



A list of nine server identifiers, each preceded by a small icon of a blue folder with a green arrow pointing right. The list is as follows:

- 192.168.200.247\_VM\_LiveCD
- 192.168.200.248\_VM\_Weak\_SSH
- 192.168.200.251\_VM\_BT5
- 192.168.200.252\_VM\_Gotroot
- 192.168.200.253\_VM\_Gotwurzel
- 192.168.200.64\_VM\_CSL\_AD
- 192.168.200.65\_VM\_CSL\_TS
- chat.hacking-lab.com
- elab

## Vulnerable Servers

- \* Server LiveCD
- \* SSH Challenge
- \* Backtrack
- \* Unix Challenge
- \* Active Directory
- \* Terminal Server
- \* Chat

The Hacking-Lab servers will  
**revert to snapshot** ever 1, 2  
or 4 hours



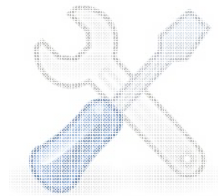
## Details about Hacking-Lab (2/4)



- (1) Vulnerable Servers and Applications (Web, Windows, Linux, iOS, Android)



- (2) Description about the security challenges



- (3) Tools required for solving the challenges



- (4) Teacher function (accept/reject solutions)

[Home](#)[About](#)[Partner & Sponsors](#)[Job Opportunities](#)[News](#)[Events](#)[Case Overview](#)[Remote Security Lab](#)[Chat](#)[Ranking](#)[Avatar](#)[Services](#)[Tutorials](#)[Download](#)[Login / Sign up](#)

### My Menu

[Edit My Profile](#)[Inbox](#)[Organisation Manager](#)[Logout](#)

## Test Event - AppSec USA 2011 OWASP University Challenge

[Ranking](#) [Event Channel](#) [Group](#) [Event Participants](#)

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	-	2310 Web Security: SQL-Injection with UNION	2	0/20	30	0	
	WG	7000 Web Security: Observation Plugin - Live Http Headers	3	0/10	90	0	
	WG	7010 Network Security: DNS Host Name Change	3	0/15	45	0	
	WG	7019 AES Bit-Flipping Attack	2	0/10	60	0	
	WG	7025 Database Hijack CarGame Challenge	3	0/30	120	0	
	WG	7039 Music Hero	1	0/20	20	0	
	WG	7101 Hack The Client	1	0/35	15	0	
	WG	7103 Crack The Channel	1	0/20	15	0	
	WG	7104 Web Shell	1	0/25	15	0	
	WG	7105 eNotary	1	0/25	15	0	
	WG	7106 Fake The MAC	1	0/30	15	0	

[Home](#)[About](#)[Partner & Sponsors](#)[Job Opportunities](#)[News](#)[Events](#)[Case Overview](#)[Remote Security Lab](#)[Chat](#)[Ranking](#)[Avatar](#)[Services](#)[Tutorials](#)[Download](#)[Login / Sign up](#)

## My Menu

[Edit My Profile](#)[Inbox](#)[Organisation Manager](#)[Logout](#)

## Test Event - AppSec USA 2011 OWASP University Challenge

[Ranking](#) [Event Channel](#) [Group](#) [Event Participants](#)

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
		2310 Web Security: SQL-Injection with UNION	2	0/20	30	0	
	WG	7000 Web Security: Observation Plugin - Live Http Headers	3	0/10	90	0	
	WG	7010 Network Security: DNS Host Name Change	3	0/15	45	0	
	WG	7019 AES Bit-Flipping Attack	2	0/10	60	0	
	WG	7025 Database Hijack CarGame Challenge	3	0/30	120	0	
	WG	7039 Music Hero	1	0/20	20	0	
	WG	7101 Hack The Client	1	0/35	15	0	
	WG	7103 Crack The Channel	1	0/20	15	0	
	WG	7104 Web Shell	1	0/25	15	0	
	WG	7105 eNotary	1	0/25	15	0	
	WG	7106 Fake The MAC	1	0/30	15	0	



[Home](#)[About](#)[Partner & Sponsors](#)[Job Opportunities](#)[News](#)[Events](#)[Case Overview](#)[Remote Security Lab](#)[Chat](#)[Ranking](#)[Avatar](#)[Services](#)[Tutorials](#)[Download](#)[Login / Sign up](#)

## My Menu

[Edit My Profile](#)[Inbox](#)[Organisation Manager](#)[Logout](#)

## Test Event - AppSec USA 2011 OWASP University Challenge























[Ranking](#) [Event Channel](#) [Group](#) [Event Participants](#)

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	-	2310 Web Security: SQL-Injection with UNION	2	0/20	30	0	
	WG	7000 Web Security: Observation Plugin - Live Http Headers	3	0/10	90	0	
	WG	7010 Network Security: DNS Host Name Change	3	0/15	45	0	
	WG	7019 AES Bit-Flipping Attack	2	0/10	60	0	
	WG	7025 Database Hijack CarGame Challenge	3	0/30	120	0	
	WG	7039 Music Hero	1	0/20	20	0	
	WG	7101 Hack The Client	1	0/35	15	0	
	WG	7103 Crack The Channel	1	0/20	15	0	
	WG	7104 Web Shell	1	0/25	15	0	
	WG	7105 eNotary	1	0/25	15	0	
	WG	7106 Fake The MAC	1	0/30	15	0	



## Test Event - AppSec USA 2011 OWASP University Challenge

Ranking Event Channel Group Event Participants

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	-	2310 Web Security: SQL-Injection with UNION	2	0/20	30	0	
	WG	7000 Web Security: Observation Plugin - Live Http Headers	3	0/10	90	0	
	WG	7010 Network Security: DNS Host Name Change	3	0/15	45	0	
	WG	7019 AES Bit-Flipping Attack	2	0/10	60	0	
	WG	7025 Database Hijack CarGame Challenge	3	0/30	120	0	
	WG	7039 Music Hero	1	0/20	20	0	
	WG	7101 Hack The Client	1	0/35	15	0	
	WG	7103 Crack The Channel	1	0/20	15	0	
	WG	7104 Web Shell	1	0/25	15	0	
	WG	7105 eNotary	1	0/25	15	0	
	WG	7106 Fake The MAC	1	0/30	15	0	

Home

About

Partner &amp; Sponsors

Job Opportunities

News

Events

Case Overview

Remote Security Lab

Chat

Ranking

Avatar

Services

Tutorials

Download

Login / Sign up



## My Menu

Edit My Profile

Inbox

Organisation Manager

Logout

Home  
About  
Partner & Sponsors  
Job Opportunities  
News  
Events  
Case Overview  
Remote Security Lab  
Chat  
Ranking  
Avatar  
Services  
Tutorials  
Download  
Login / Sign up

























## My Menu

Edit My Profile  
Inbox  
Organisation Manager  
Logout

## Test Event - AppSec USA 2011 OWASP University Challenge























Ranking Event Channel Group Event Participants

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	-	2310 Web Security: SQL-Injection with UNION	2	0/20	30	0	
	WG	7000 Web Security: Observation Plugin - Live Http Headers	3	0/10	90	0	
	WG	7010 Network Security: DNS Host Name Change	3	0/15	45	0	
	WG	7019 AES Bit-Flipping Attack	2	0/10	60	0	
	WG	7025 Database Hijack CarGame Challenge	3	0/30	120	0	
	WG	7039 Music Hero	1	0/20	20	0	
	WG	7101 Hack The Client	1	0/35	15	0	
	WG	7103 Crack The Channel	1	0/20	15	0	
	WG	7104 Web Shell	1	0/25	15	0	
	WG	7105 eNotary	1	0/25	15	0	
	WG	7106 Fake The MAC	1	0/30	15	0	



## Test Event - AppSec USA 2011 OWASP University Challenge

Ranking Event Channel Group Event Participants

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	-	2310 Web Security: SQL-Injection with UNION	2	0/20	30	0	
	WG	7000 Web Security: Observation Plugin - Live Http Headers	3	0/10	90	0	
	WG	7010 Network Security: DNS Host Name Change	3	0/15	45	0	
	WG	7019 AES Bit-Flipping Attack	2	0/10	60	0	
	WG	7025 Database Hijack CarGame Challenge	3	0/30	120	0	
	WG	7039 Music Hero	1	0/20	20	0	
	WG	7101 Hack The Client	1	0/35	15	0	
	WG	7103 Crack The Channel	1	0/20	15	0	
	WG	7104 Web Shell	1	0/25	15	0	
	WG	7105 eNotary	1	0/25	15	0	
	WG	7106 Fake The MAC	1	0/30	15	0	

Home

About

Partner &amp; Sponsors

Job Opportunities

News

Events

Case Overview

Remote Security Lab

Chat

Ranking

Avatar

Services

Tutorials

Download

Login / Sign up



## My Menu

Edit My Profile

Inbox

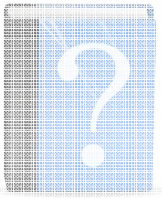
Organisation Manager

Logout

## Details about Hacking-Lab (3/4)



- (1) Vulnerable Servers and Applications (Web, Windows, Linux, iOS, Android)



- (2) Description about the security challenges



- (3) Tools required for solving the challenges



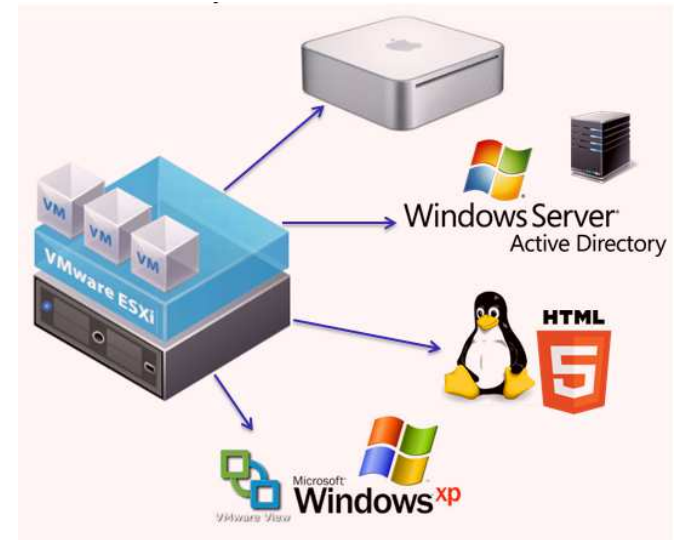
- (4) Teacher function (accept/reject solutions)



# Tools required to solve the Challenges



**VPN to Lab**



**LiveCD**

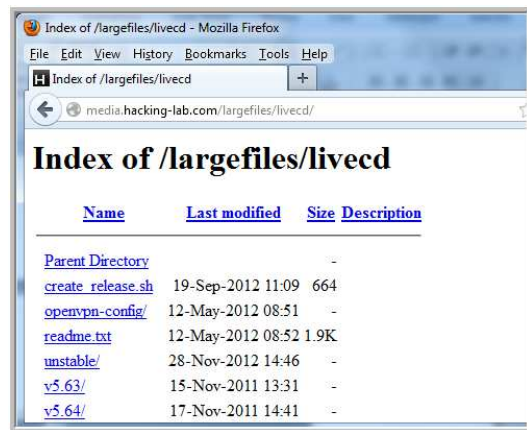


**OpenVPN** into ESX Server  
Infrastructure

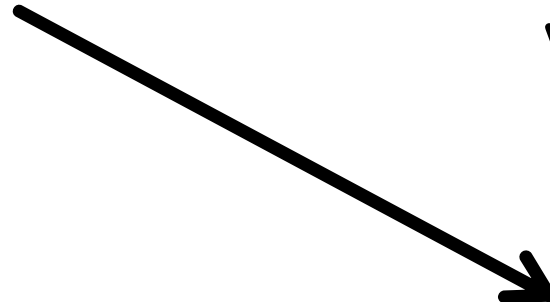
# LiveCD **free** Download



<http://media.hacking-lab.com>



**LiveCD  
VirtualBox OVA**



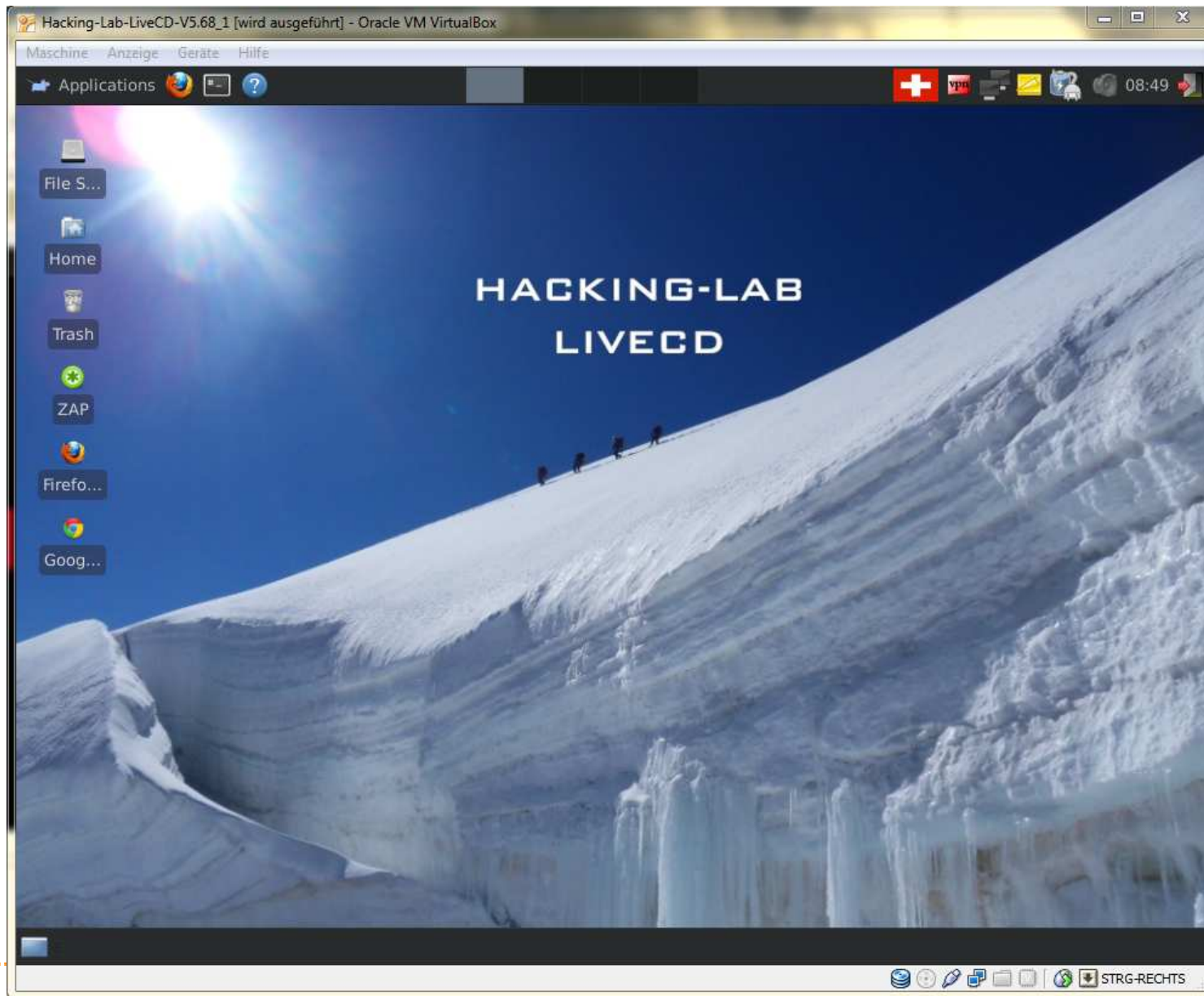
**LiveCD  
Vmware OVA**



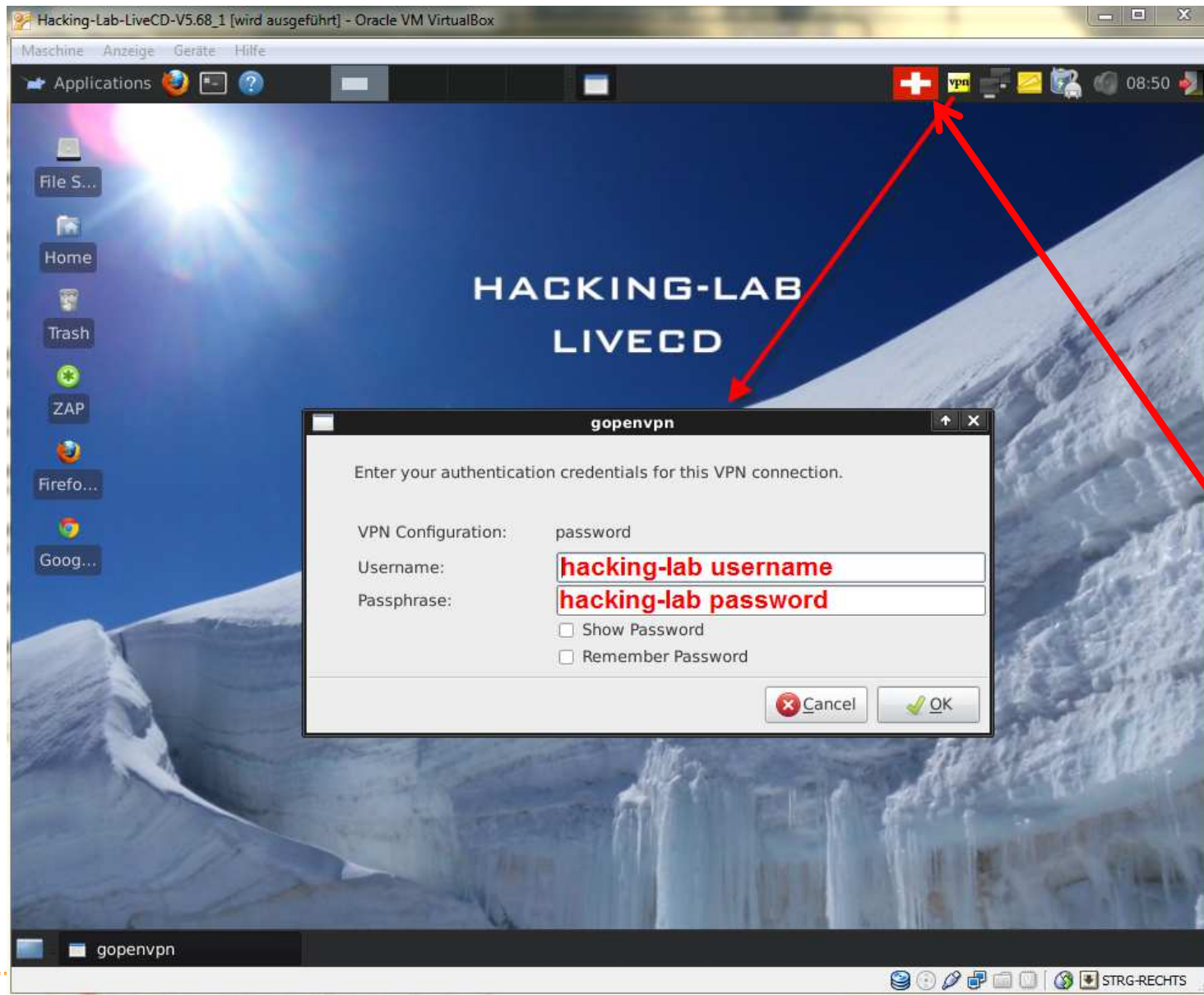
**LiveCD ISO**

# Hacking-Lab LiveCD Project

**COMPASS**  
SECURITY



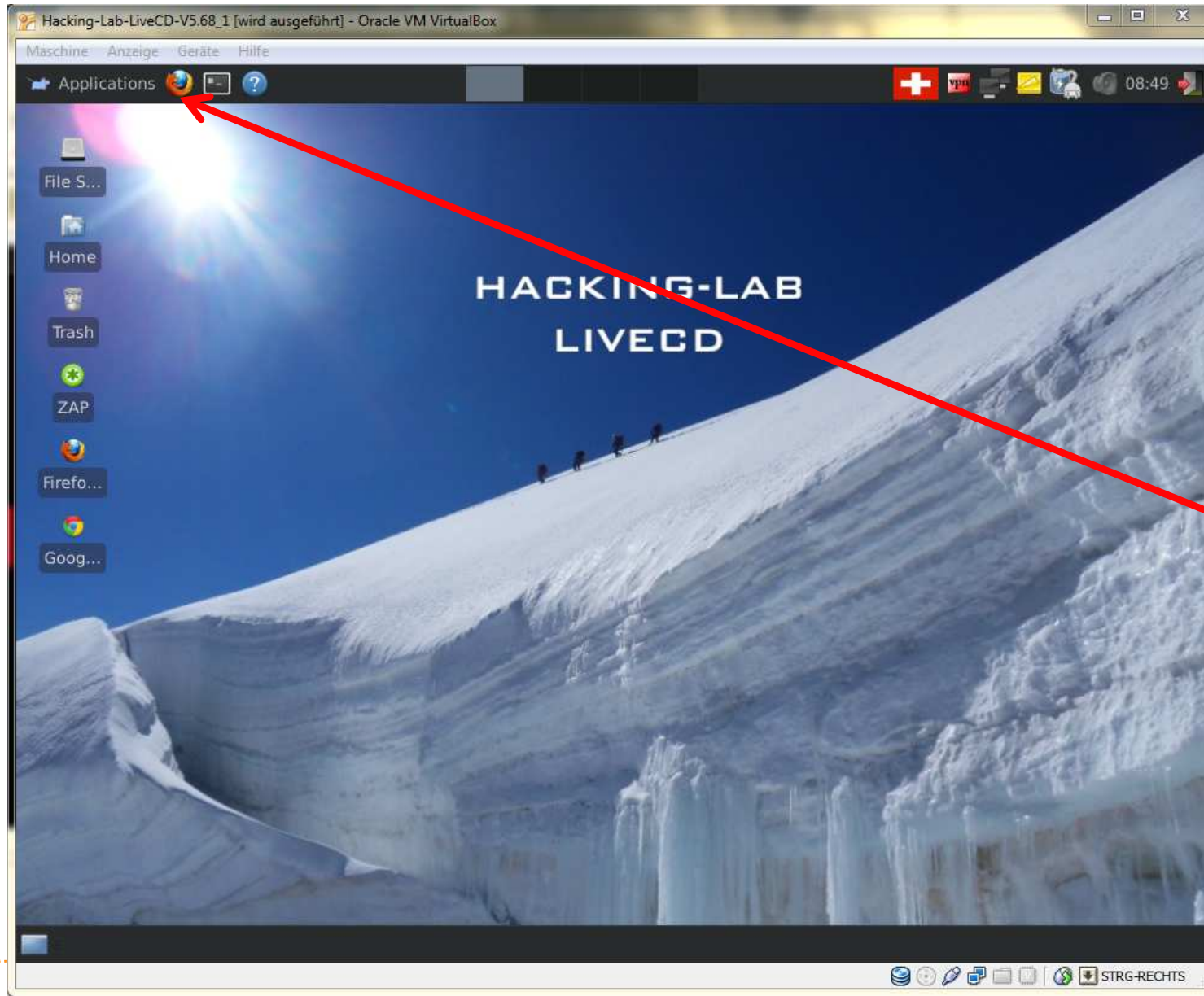
# How to connect using VPN



VPN



# How to use the Browser



## Browser

- 1) Two profiles
- 2) Attacker
- 3) Victim
- 4) SwitchProxy
- 5) LiveHttpHeader
- 6) ... more

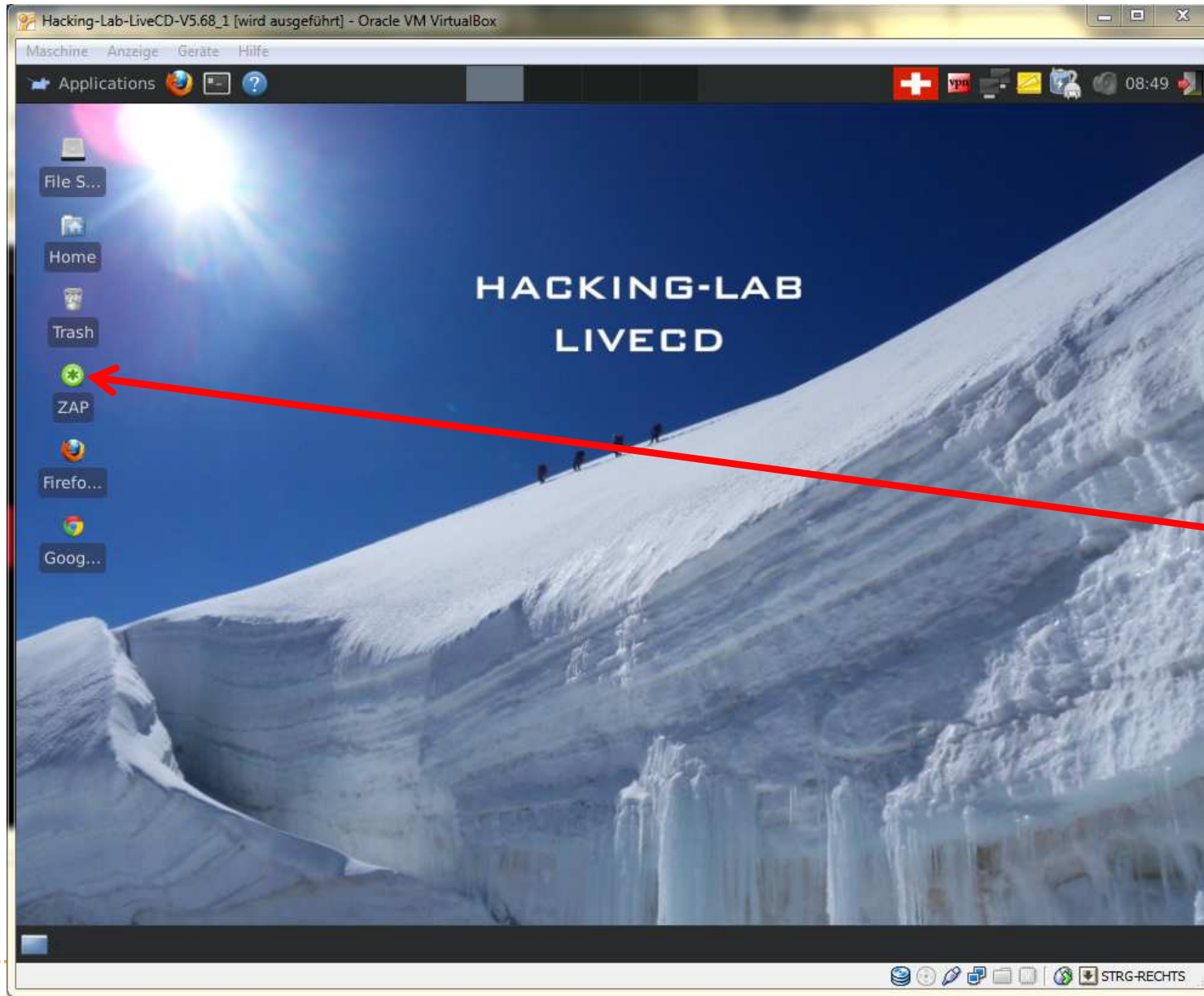


# How to use ZAP Proxy

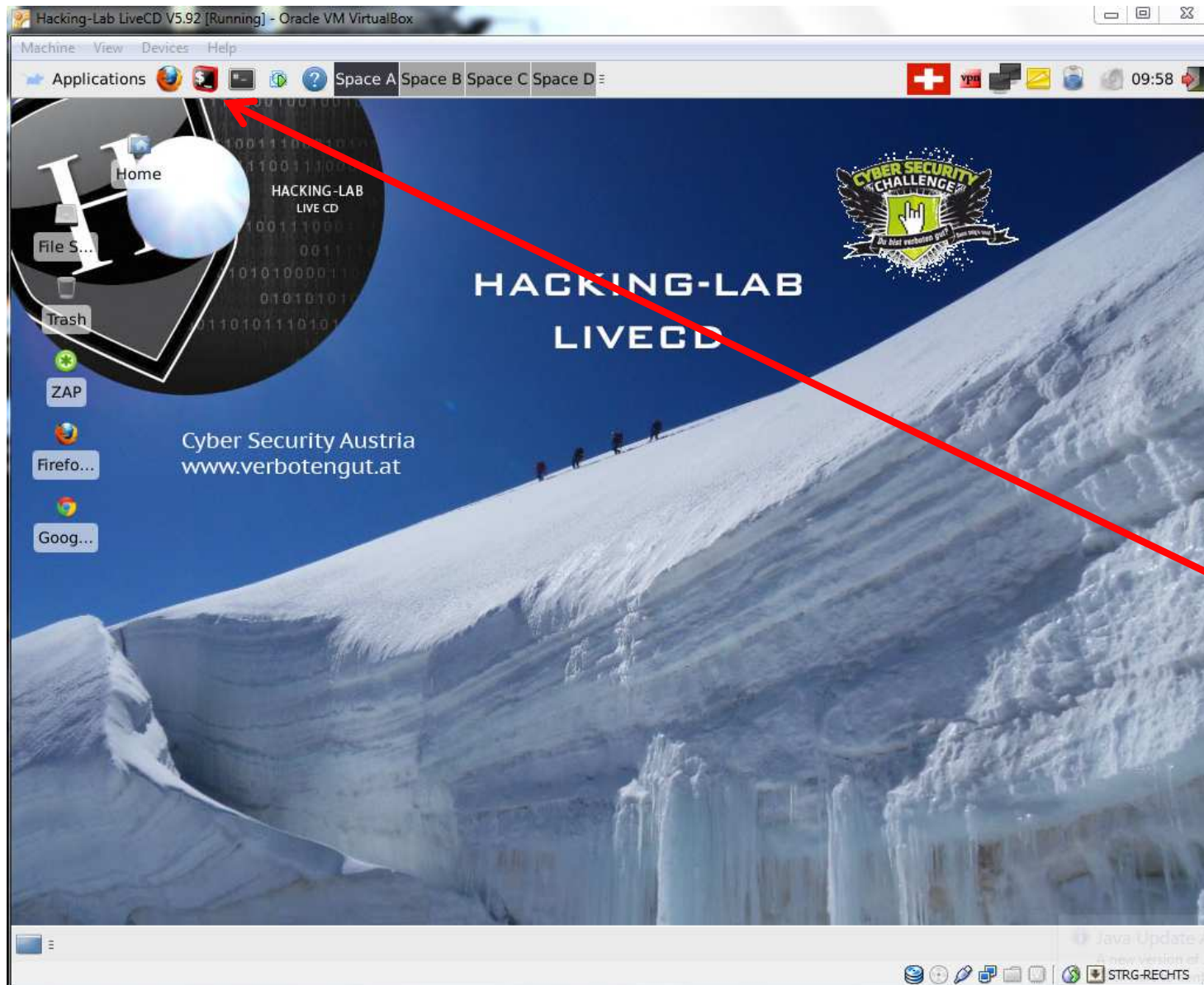


## ZAP Inspection Proxy

- 1) Web Analysis
- 2) Man in the Middle
- 3) Open Source
- 4) Java based
- 5) Loading = slow



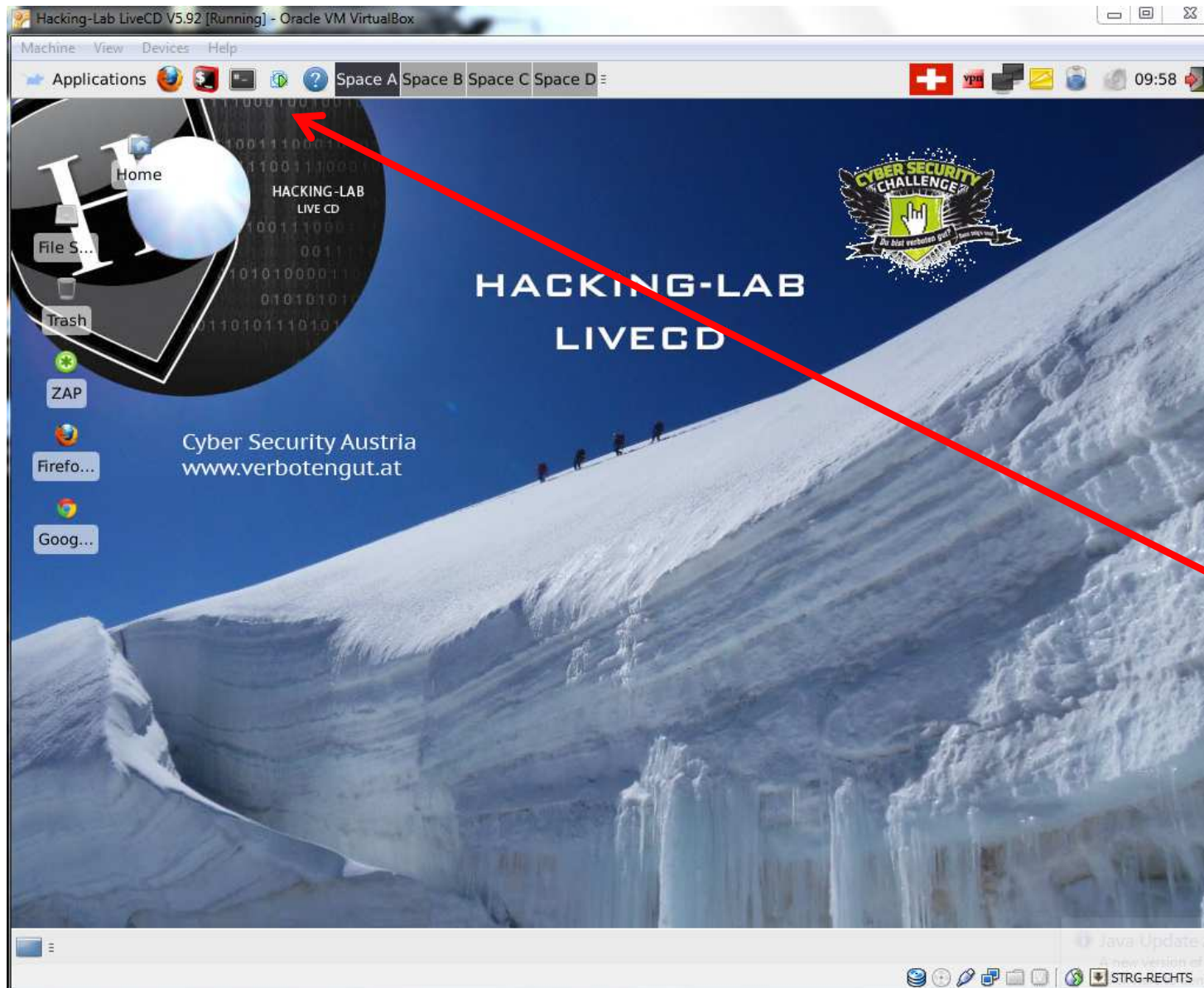
# How to get a Root Shell



**ROOT  
Shell**

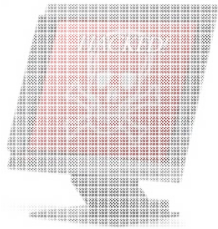


# How to access Microsoft XP (VDI)

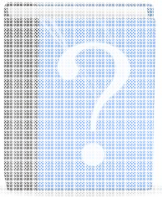


**Vmware  
View  
VDI**

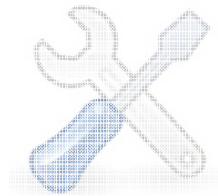
# Details about Hacking-Lab (4/4)



- (1) Vulnerable Servers and Applications  
(Web, Windows, Linux, iOS, Android)



- (2) Description about the security challenges




- (3) Tools required for solving the challenges



- (4) Teacher function (accept/reject solutions)

# Solution Grading as «Teacher»





## HACKING-LAB

HOME NINA

15718

- Home
- About
- Volunteer
- Partner & Sponsors
- Events
- Available Challenges
- Remote Security Lab
- Chat
- Wall of Fame
- Scoring System
- Avatar
- Mobile Services
- Video Tutorials
- Download
- FAQ
- Research
- Login / Sign up

### Solved Cases of Event: OWASP Top Ten

Nick	Surname	Name	Email	Case	Status	Points	Date
duelle	null	null	thfrdue@gmx.de	6112 - OWASP 2010 - A2 - Cross-Site Scripting	+	0	2013-09-17 22:43:51
thushjandan	null	null	thushjandan@gmail.com	6111 - OWASP 2010 - A1 - Injection	+	0	2013-09-13 14:45:22
nuker222	null	null	mattiamato@gmail.com	6111 - OWASP 2010 - A1 - Injection	+	0	2013-09-12 10:58:13
cg			christopher_guy@swissre.com	6111 - OWASP 2010 - A1 - Injection	+	0	2013-09-10 14:08:54
schaetcke	null	null	michjos@hotmail.com	6111 - OWASP 2010 - A1 - Injection	+	0	2013-09-09 19:26:49
flyfar	Marco	Vergari	marco@vergari.ch	6112 - OWASP 2010 - A2 - Cross-Site Scripting	+	0	2013-09-08 23:46:34



# Solution Grading as «Teacher»



## Check Solution

User: duelle  
Name: null null  
Email: thfrdue@gmx.de  
Case: 6112 - OWASP 2010 - A2 - Cross-Site Scripting  
Teacher Solution:   
Points received: 0  
Rating:

rt89	★★★★★
M.	★★★★★
Kori	★★★★★
john do	★★★★★
oilles	★★★★★

show only solutions rated by admins

**Fully Accept**  
**Partial Accept**  
**Reject**

### Attachments

XSS.txt XSS-Screenshots.zip

### Solution History

back

Date	User	Text
2013-09-17 22:43:51	duelle	See XSS.txt file for solution and the zip-file for corresponding screenshots.

# Hacking-Lab for China

Compass Security AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
team@csnc.ch  
www.csnc.ch



- Problems with **https://www.hacking-lab.com/**  
It is not working from everywhere in China
- Problems with **OpenVPN**  
It is not working from everywhere in China



## Proposed Solution

- **Translating** the OWASP TOP 10 to the Chinese language
- Hosting a Chinese server  
<http://china.hacking-lab.com>

# Future **Plans** for China



<http://china.hacking-lab.com>



HTTPS

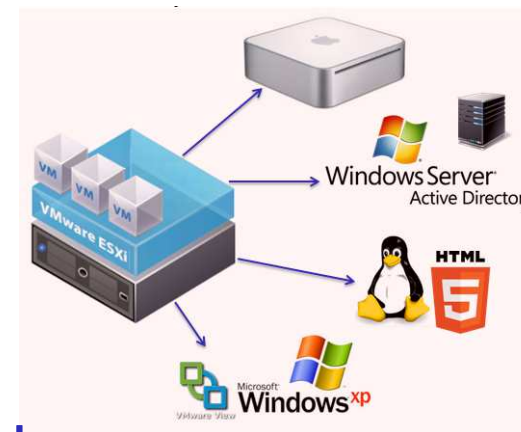
VPN



HTTPS

VPN to Lab

China



Switzerland

PS: Must be checked with Chinese law!!!



**Movie:** [china.hacking-lab.com](http://china.hacking-lab.com)

This is a prototype – not ready yet!!!

## ➤ OWASP TOP 10 Challenges in Chinese Language

### 6111 OWASP A1 盲 SQL 注入攻击

SQL 注入是一种利用应用程序在数据库层漏洞的技术。用户输入的字符串可能会嵌入到 SQL 指令中，当这些字符串没有被正确的过滤，或者不是强类型而且被意外执行的时候，漏洞就会存在。事实上，在一种程序或者脚本嵌入到另外一种中的时候，这种类型的漏洞普遍存在。



### 要求

Web 浏览器 (火狐)

存在漏洞的 Hacking-Lab 应用

## 6116 OWASP A6 安全配置错误

XXE (Xml 外部实体) 攻击是针对应用程序的, 这些应用程序的 XML 解析是从使用错误配置 XML 解析器的不被信任的源输入的。应用还可能强制打开任意文件或者 TCP 连接。



The screenshot shows a web application with a blue sidebar menu on the left containing links like '首页', '新闻', '产品', '产品搜索', 'WebService', '公司简介', '联系方式', '我的账户', '成员领域', and '供应商领域'. The main content area has a title 'XML搜索来源' and a description 'This form constructs the request from the given parameters.' Below this are three input fields: 'Bell name' (containing 'mysql'), 'Destination' (highlighted with a red arrow and labeled '搜索字符串'), and 'Sender' (containing 'localhost').

### 要求

Web 浏览器 (火狐)

有漏洞的 Hacking-Lab 应用

### 目标

找到数据库连接属性 (MySQL 用户名和密码)。(mysql.properties 文件在 /opt/applic/ 目录中)

## Conclusion

How to **build** your own **security lab**



# Conclusion



**Free OWASP TOP 10 challenges**  
**<https://www.hacking-lab.com/sh/yrNdMqk>**

What do you think?



Compass Security AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
team@csnc.ch  
www.csnc.ch

Thank you very much!

Ivan Bütler

[ivan.buetler@compass-security.com](mailto:ivan.buetler@compass-security.com)

Compass Security AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)