HACKING-LAB INTRODUCTION

Remote Security Lab, powered by Compass Security

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

LEARNING GOAL

1. Hacking-Lab is a remote security lab
2. You can practice what you (may) have heard in theory
3. This slide deck shall help you understanding how you can use Hacking-Lab and how to access challenges and the lab

HACKING-LAB

HOME NINA 16027

E-Mail: Password: Login »

Status: 9 october 2013

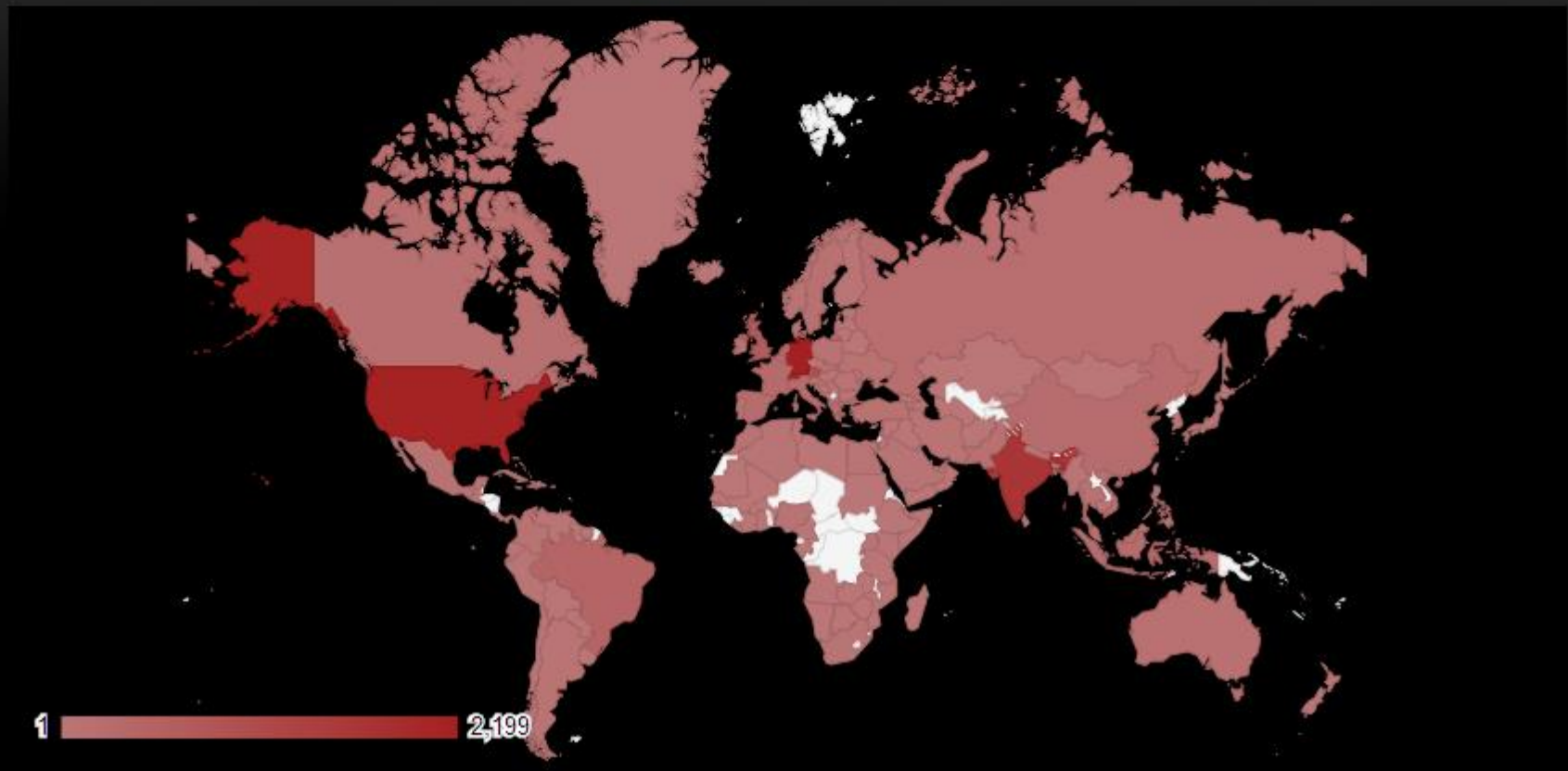
Anonymous User

- 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

Don't have an account?
Create a free account now!

Welcome at Hacking-Lab

Location of Hacking-Lab Users in the World



HACKING-LAB CHECK-LIST

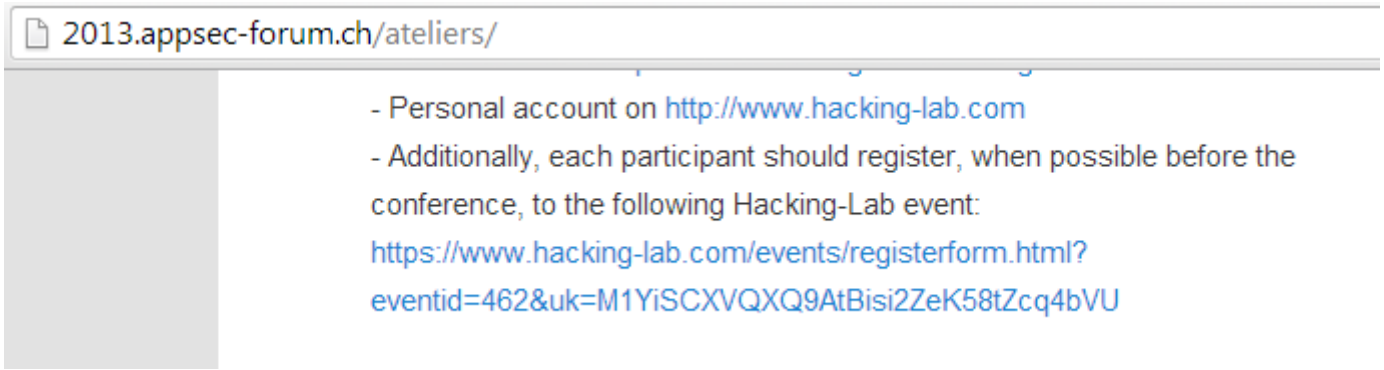
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

BEFORE TALKING TOO MUCH…

Prerequisites

- Each participant has a laptop with either
  - Virtual Box or VMware 8 installed & matching disk image downloaded from http://media.hacking-lab.com/largefiles/livecd/
  - Or ability to boot a live CD & having the latest version of the media downloaded from http://media.hacking-lab.com/largefiles/livecd/
- Personal account on https://www.hacking-lab.com
- Additionally, each participant registered on the following Hacking-Lab event: https://www.hacking-lab.com/events/registerform.html?eventid=462&uk=M1YiSCXVQXQ9AtBisi2ZeK58tZcq4bVU

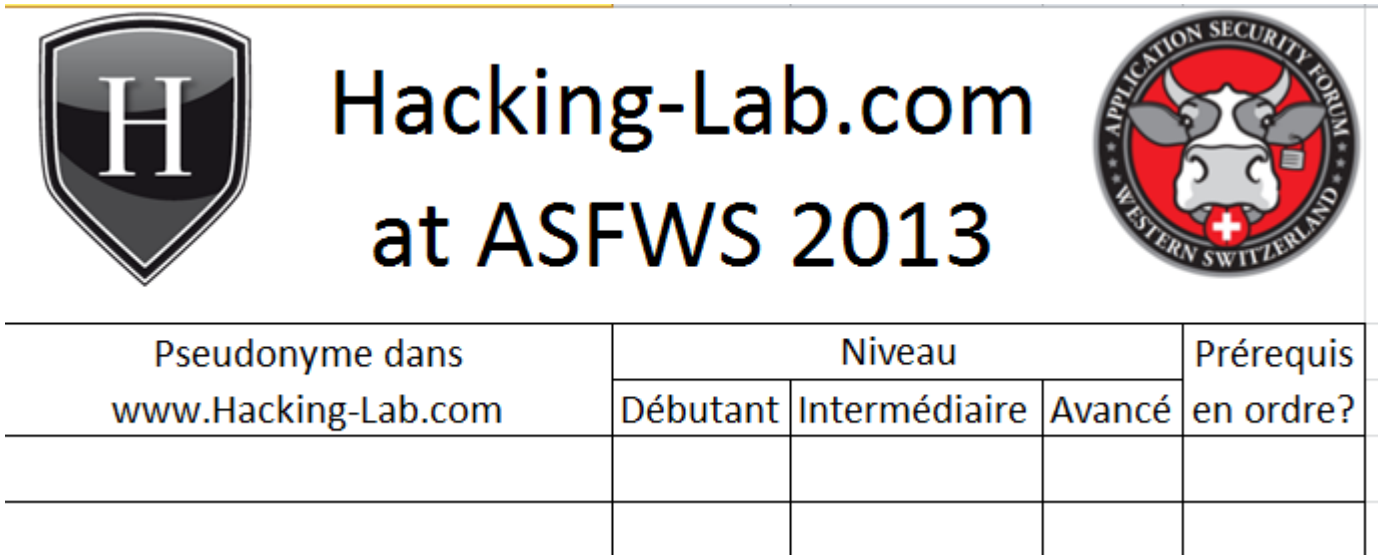


BEFORE TALKING TOO MUCH…

Short presentation of yourself

- What are your expectations for this "atelier"?
- Do you know the OWASP top 10?
- How would you rate your web / Linux technical knowledge?
- How would you rate your "hacking" knowledge?

Meanwhile please fill out the paper form



Hacking-Lab.com
at ASFWS 2013

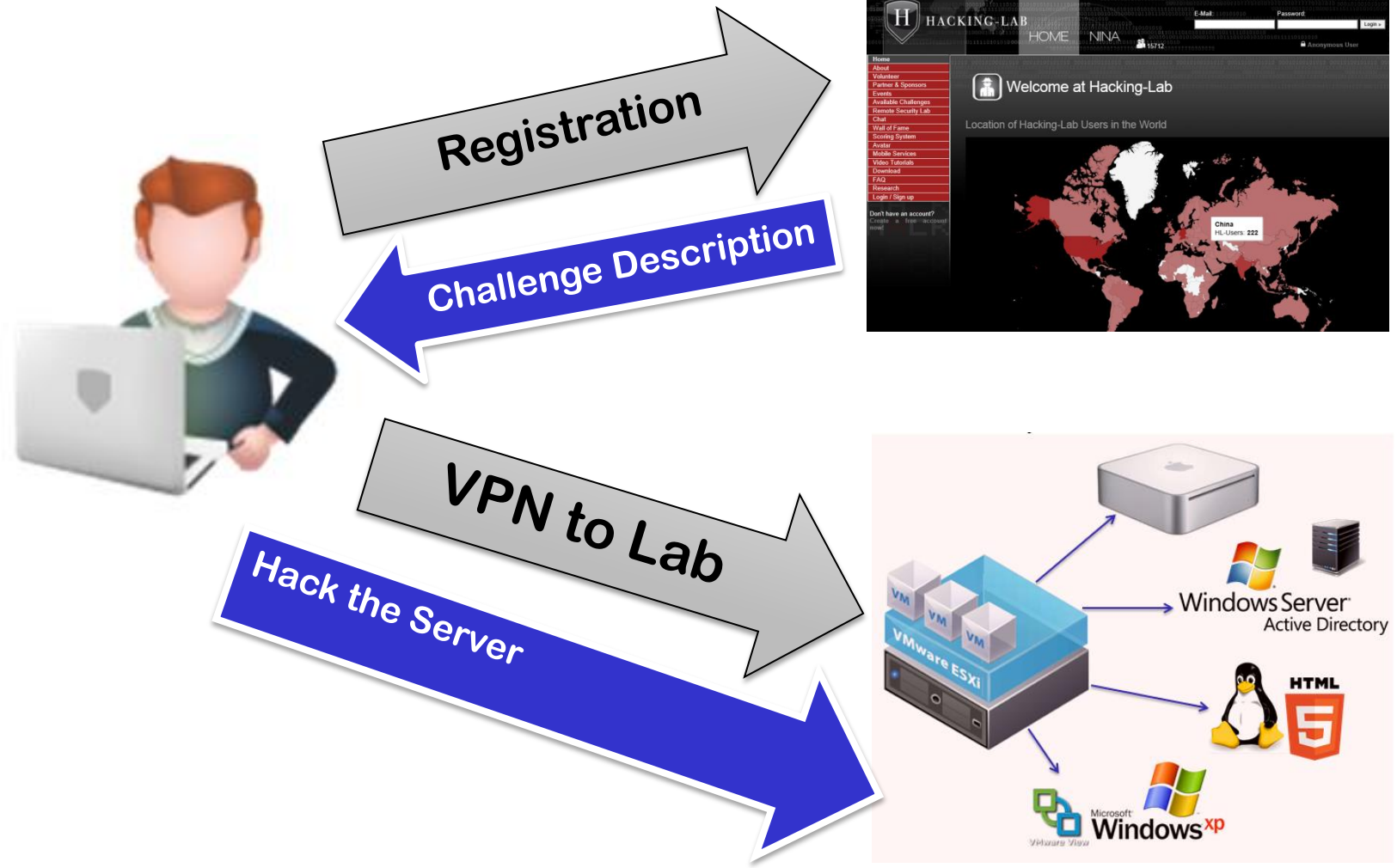
Pseudonyme dans www.Hacking-Lab.com	Niveau			Prérequis en ordre?
	Débutant	Intermédiaire	Avancé	

HOW TO USE HACKING-LAB

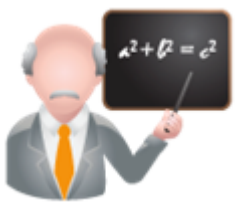
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

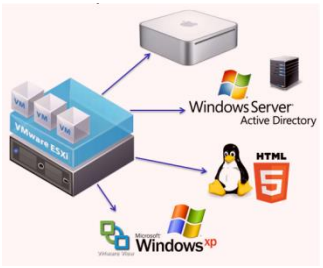
Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

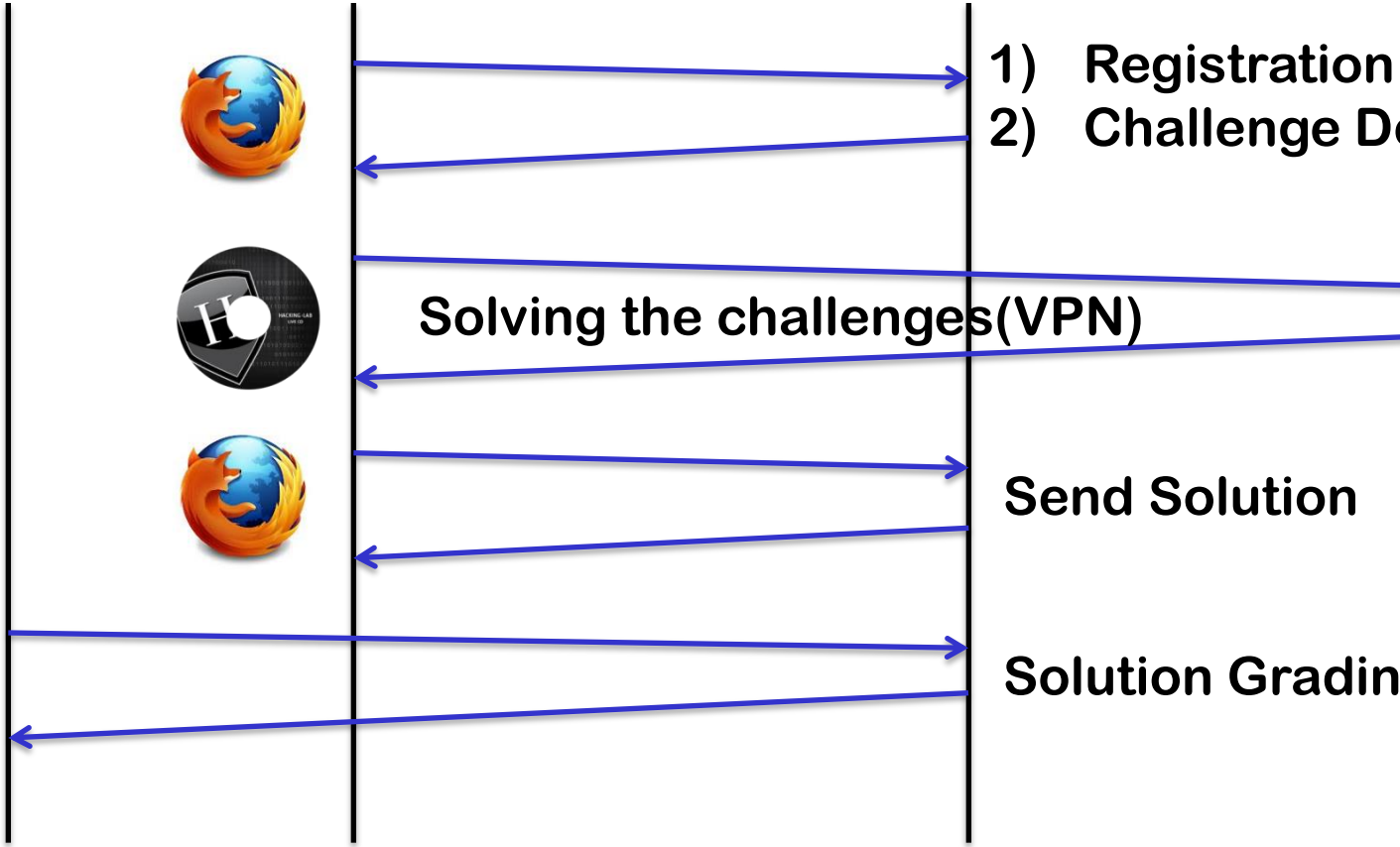
WHAT IS «HACKING-LAB»????



UNDERSTANDING HACKING-LAB







HACKING-LAB ROLES

- Student

1. Choose the challenge(s)
2. Solve the challenge
3. Answer the questions (submit)
4. Wait

- Teacher

1. Responsible for challenges
2. Receiving your submissions
3. Solution Grading
   a) FULLY ACCEPT
   b) PARTIALL ACCEPT
   c) REJECT

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

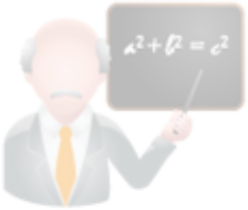
- (4) Teacher functions (accept/reject solutions) solutions, solution movies

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)

VULNERABLE SERVICES

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

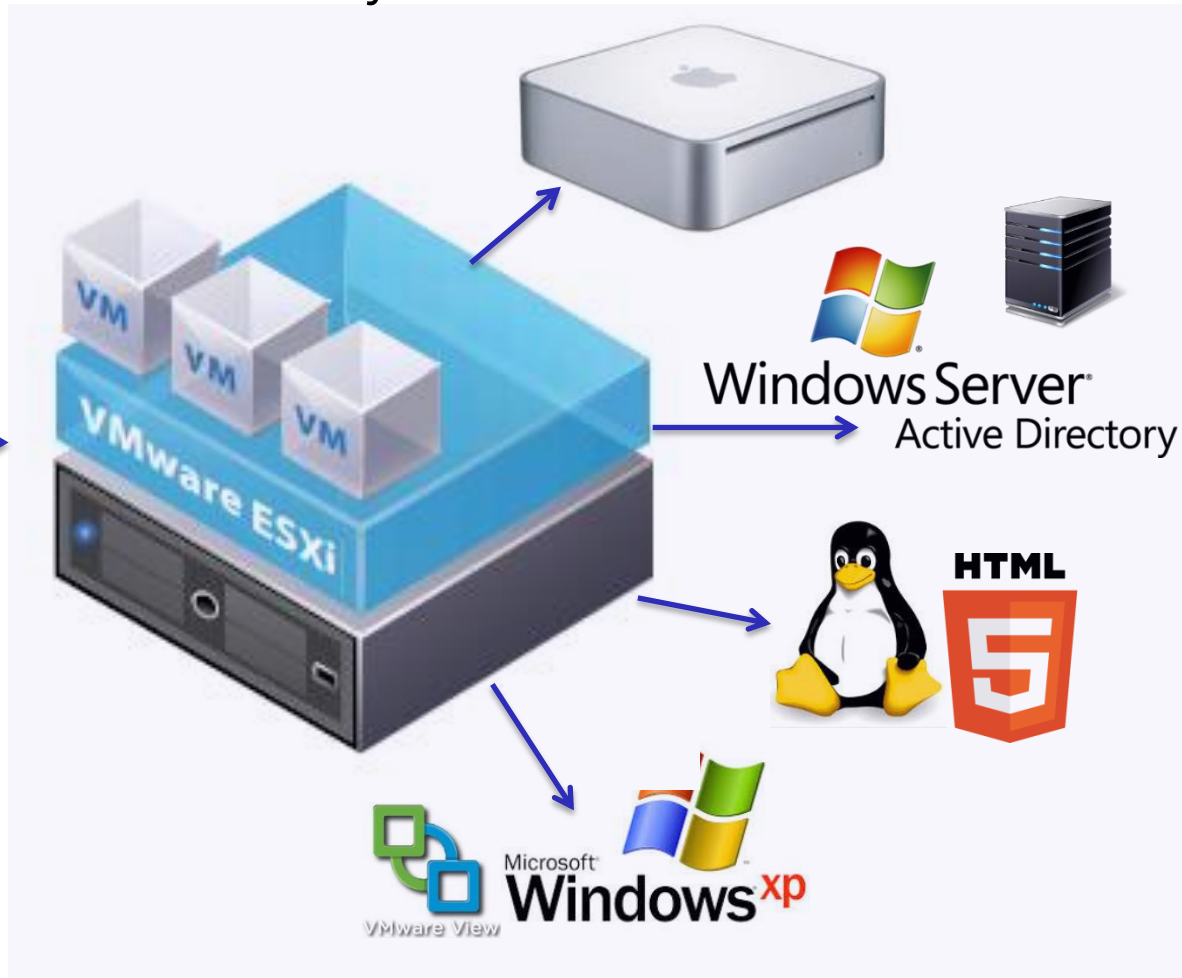
Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

DETAILS ABOUT HACKING-LAB

Vulnerable **Mobile** Apps

Vulnerable **Servers** Remote Security Lab

Automatic Revert to Snapshot



MOVIE: INTRODUCTION ESXI

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

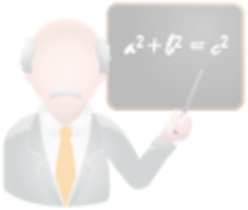
Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

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)

HACKING-LAB WEB SITE

www.hacking-lab.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
www.csnc.ch

HACKING-LAB WEB SITE

1. **Sign-Up** a Hacking-Lab Account
2. **Register** to your Hacking-Lab Event (classroom)
   1. Private Link
   2. Public Link
3. **Read** the Challenge **Instruction** (the mission)
   1. What is the mission?
   2. Where is the vulnerable services
   3. What are the security questions
4. **Submit** your solution
   1. Describe vulnerability
   2. Describe exploit
   3. Describe mitigation

OWASP
The Open Web Application Security Project

OWASP Top Ten

Ranking Event Channel Event Participants

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	WG	6111 - OWASP 2010 - A1 – Injection	1	0/10	60	525	
	WG	6112 - OWASP 2010 - A2 - Cross-Site Scripting	1	0/10	30	175	
	WG	6113 - OWASP 2010 - A3 – Broken Authentication and Session Management	1	0/10	30	132	
	WG	6114 - OWASP 2010 - A4 – Insecure Direct Object References	1	0/10	60	136	
	WG	6115 - OWASP 2010 - A5 – Cross Site Request Forgery	2	0/20	60	90	
	WG	6116 - OWASP 2010 - A6 – Security Misconfiguration	2	0/20	60	78	
	WG	6117 - OWASP 2010 - A7 – Insecure Cryptographic Storage	2	0/20	60	89	
	WG	6118 - OWASP 2010 - A8 – Failure to Restrict URL Access	1	0/10	30	76	
	WG	6119 - OWASP 2010 - A9 – Insufficient Transport Layer Protection	1	0/10	30	67	
	WG	6120 - OWASP 2010 - A10 – Unvalidated Redirects and Forwards	1	0/10	10	59	

OWASP
The Open Web Application Security Project

Challenge Category

OWASP Top Ten

Ranking Event Channel Event Participants

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	WG	6111 - OWASP 2010 - A1 – Injection	1	0/10	60	525	
	WG	6112 - OWASP 2010 - A2 - Cross-Site Scripting	1	0/10	30	175	
	WG	6113 - OWASP 2010 - A3 – Broken Authentication and Session Management	1	0/10	30	132	
	WG	6114 - OWASP 2010 - A4 – Insecure Direct Object References	1	0/10	60	136	
	WG	6115 - OWASP 2010 - A5 – Cross Site Request Forgery	2	0/20	60	90	
	WG	6116 - OWASP 2010 - A6 – Security Misconfiguration	2	0/20	60	78	
	WG	6117 - OWASP 2010 - A7 – Insecure Cryptographic Storage	2	0/20	60	89	
	WG	6118 - OWASP 2010 - A8 – Failure to Restrict URL Access	1	0/10	30	76	
	WG	6119 - OWASP 2010 - A9 – Insufficient Transport Layer Protection	1	0/10	30	67	
	WG	6120 - OWASP 2010 - A10 – Unvalidated Redirects and Forwards	1	0/10	10	59	

CHALLENGES CATEGORIES IN HACKING-LAB

- 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

OWASP
The Open Web Application Security Project

OWASP Top Ten

Challenge Type
WG = Wargame
SBS = Step by Step

Ranking Event Channel Event Participants

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	WG	6111 - OWASP 2010 - A1 – Injection	1	0/10	60	525	
	WG	6112 - OWASP 2010 - A2 - Cross-Site Scripting	1	0/10	30	175	
	WG	6113 - OWASP 2010 - A3 – Broken Authentication and Session Management	1	0/10	30	132	
	WG	6114 - OWASP 2010 - A4 – Insecure Direct Object References	1	0/10	60	136	
	WG	6115 - OWASP 2010 - A5 – Cross Site Request Forgery	2	0/20	60	90	
	WG	6116 - OWASP 2010 - A6 – Security Misconfiguration	2	0/20	60	78	
	WG	6117 - OWASP 2010 - A7 – Insecure Cryptographic Storage	2	0/20	60	89	
	WG	6118 - OWASP 2010 - A8 – Failure to Restrict URL Access	1	0/10	30	76	
	WG	6119 - OWASP 2010 - A9 – Insufficient Transport Layer Protection	1	0/10	30	67	
	WG	6120 - OWASP 2010 - A10 – Unvalidated Redirects and Forwards	1	0/10	10	59	

CHALLENGES – SBS VERSUS WG

SBS

SBS
Step by Step

SBS challenges are used in commercial trainings.

Trainees do not have the time to spend 1-2 hours per challenge. They will be guided through the challenge.

WG

WG
Wargame

WG challenges are used in free trainings, CTF and talent quest.

Solving a WG challenge is more difficult and needs more knowledge.

Every challenge in Hacking-Lab is available as SBS and WG

SBS = Step by Step Instruction of the challenge

WG = Wargame instruction (without further details about the procedure)

CHALLENGES - SBS VERSUS WG

WG Challenges

- WG = Wargame
- The mission of the challenge is given, but without further details
- For the more advanced users
- Level 1 = 10 points
- Level 2 = 20 points
- Level 3 = 30 points

SBS Challenges

- SBS = Step by Step
- The mission of the challenge is given, including a step by step instruction
- For the beginners
- Level 1 = 5 points (50% of WG)
- Level 2 = 10 points (50% of WG)
- Level 3 = 15 points (50% of WG)

OWASP
The Open Web Application Security Project

OWASP Top Ten

Link to the description (mission) of the challenge

Ranking Event Channel Event Participants

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	WG	6111 - OWASP 2010 - A1 – Injection	1	0/10	60	525	
	WG	6112 - OWASP 2010 - A2 - Cross-Site Scripting	1	0/10	30	175	
	WG	6113 - OWASP 2010 - A3 – Broken Authentication and Session Management	1	0/10	30	132	
	WG	6114 - OWASP 2010 - A4 – Insecure Direct Object References	1	0/10	60	136	
	WG	6115 - OWASP 2010 - A5 – Cross Site Request Forgery	2	0/20	60	90	
	WG	6116 - OWASP 2010 - A6 – Security Misconfiguration	2	0/20	60	78	
	WG	6117 - OWASP 2010 - A7 – Insecure Cryptographic Storage	2	0/20	60	89	
	WG	6118 - OWASP 2010 - A8 – Failure to Restrict URL Access	1	0/10	30	76	
	WG	6119 - OWASP 2010 - A9 – Insufficient Transport Layer Protection	1	0/10	30	67	
	WG	6120 - OWASP 2010 - A10 – Unvalidated Redirects and Forwards	1	0/10	10	59	

OWASP
The Open Web Application Security Project

OWASP Top Ten

Level 1 = Easy
Level 2 = Medium
Level 3 = Advanced

Ranking Event Channel Event Participants

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	WG	6111 - OWASP 2010 - A1 – Injection	1	0/10	60	525	
	WG	6112 - OWASP 2010 - A2 - Cross-Site Scripting	1	0/10	30	175	
	WG	6113 - OWASP 2010 - A3 – Broken Authentication and Session Management	1	0/10	30	132	
	WG	6114 - OWASP 2010 - A4 – Insecure Direct Object References	1	0/10	60	136	
	WG	6115 - OWASP 2010 - A5 – Cross Site Request Forgery	2	0/20	60	90	
	WG	6116 - OWASP 2010 - A6 – Security Misconfiguration	2	0/20	60	78	
	WG	6117 - OWASP 2010 - A7 – Insecure Cryptographic Storage	2	0/20	60	89	
	WG	6118 - OWASP 2010 - A8 – Failure to Restrict URL Access	1	0/10	30	76	
	WG	6119 - OWASP 2010 - A9 – Insufficient Transport Layer Protection	1	0/10	30	67	
	WG	6120 - OWASP 2010 - A10 – Unvalidated Redirects and Forwards	1	0/10	10	59	

OWASP
The Open Web Application Security Project

OWASP Top Ten

How many score points you get for successfully solving the challenge.

0/10 means that the max score is 10 points, but this user has not yet solved it,

Ranking Event Channel Event Participants

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	WG	6111 - OWASP 2010 - A1 – Injection	1	0/10	60	525	
	WG	6112 - OWASP 2010 - A2 - Cross-Site Scripting	1	0/10	30	175	
	WG	6113 - OWASP 2010 - A3 – Broken Authentication and Session Management	1	0/10	30	132	
	WG	6114 - OWASP 2010 - A4 – Insecure Direct Object References	1	0/10	60	136	
	WG	6115 - OWASP 2010 - A5 – Cross Site Request Forgery	2	0/20	60	90	
	WG	6116 - OWASP 2010 - A6 – Security Misconfiguration	2	0/20	60	78	
	WG	6117 - OWASP 2010 - A7 – Insecure Cryptographic Storage	2	0/20	60	89	
	WG	6118 - OWASP 2010 - A8 – Failure to Restrict URL Access	1	0/10	30	76	
	WG	6119 - OWASP 2010 - A9 – Insufficient Transport Layer Protection	1	0/10	30	67	
	WG	6120 - OWASP 2010 - A10 – Unvalidated Redirects and Forwards	1	0/10	10	59	

OWASP
The Open Web Application Security Project

OWASP Top Ten

How many minutes we expect an intermediate user to solve the challenge. Could be double or three times for beginners.

Ranking Event Channel Event Participants

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	WG	6111 - OWASP 2010 - A1 – Injection	1	0/10	60	525	
	WG	6112 - OWASP 2010 - A2 - Cross-Site Scripting	1	0/10	30	175	
	WG	6113 - OWASP 2010 - A3 – Broken Authentication and Session Management	1	0/10	30	132	
	WG	6114 - OWASP 2010 - A4 – Insecure Direct Object References	1	0/10	60	136	
	WG	6115 - OWASP 2010 - A5 – Cross Site Request Forgery	2	0/20	60	90	
	WG	6116 - OWASP 2010 - A6 – Security Misconfiguration	2	0/20	60	78	
	WG	6117 - OWASP 2010 - A7 – Insecure Cryptographic Storage	2	0/20	60	89	
	WG	6118 - OWASP 2010 - A8 – Failure to Restrict URL Access	1	0/10	30	76	
	WG	6119 - OWASP 2010 - A9 – Insufficient Transport Layer Protection	1	0/10	30	67	
	WG	6120 - OWASP 2010 - A10 – Unvalidated Redirects and Forwards	1	0/10	10	59	

OWASP
The Open Web Application Security Project

Number of users who have solved the challenge until now...

OWASP Top Ten

Ranking Event Channel Event Participants

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	WG	6111 - OWASP 2010 - A1 – Injection	1	0/10	60	525	
	WG	6112 - OWASP 2010 - A2 - Cross-Site Scripting	1	0/10	30	175	
	WG	6113 - OWASP 2010 - A3 – Broken Authentication and Session Management	1	0/10	30	132	
	WG	6114 - OWASP 2010 - A4 – Insecure Direct Object References	1	0/10	60	136	
	WG	6115 - OWASP 2010 - A5 – Cross Site Request Forgery	2	0/20	60	90	
	WG	6116 - OWASP 2010 - A6 – Security Misconfiguration	2	0/20	60	78	
	WG	6117 - OWASP 2010 - A7 – Insecure Cryptographic Storage	2	0/20	60	89	
	WG	6118 - OWASP 2010 - A8 – Failure to Restrict URL Access	1	0/10	30	76	
	WG	6119 - OWASP 2010 - A9 – Insufficient Transport Layer Protection	1	0/10	30	67	
	WG	6120 - OWASP 2010 - A10 – Unvalidated Redirects and Forwards	1	0/10	10	59	

OWASP
The Open Web Application Security Project

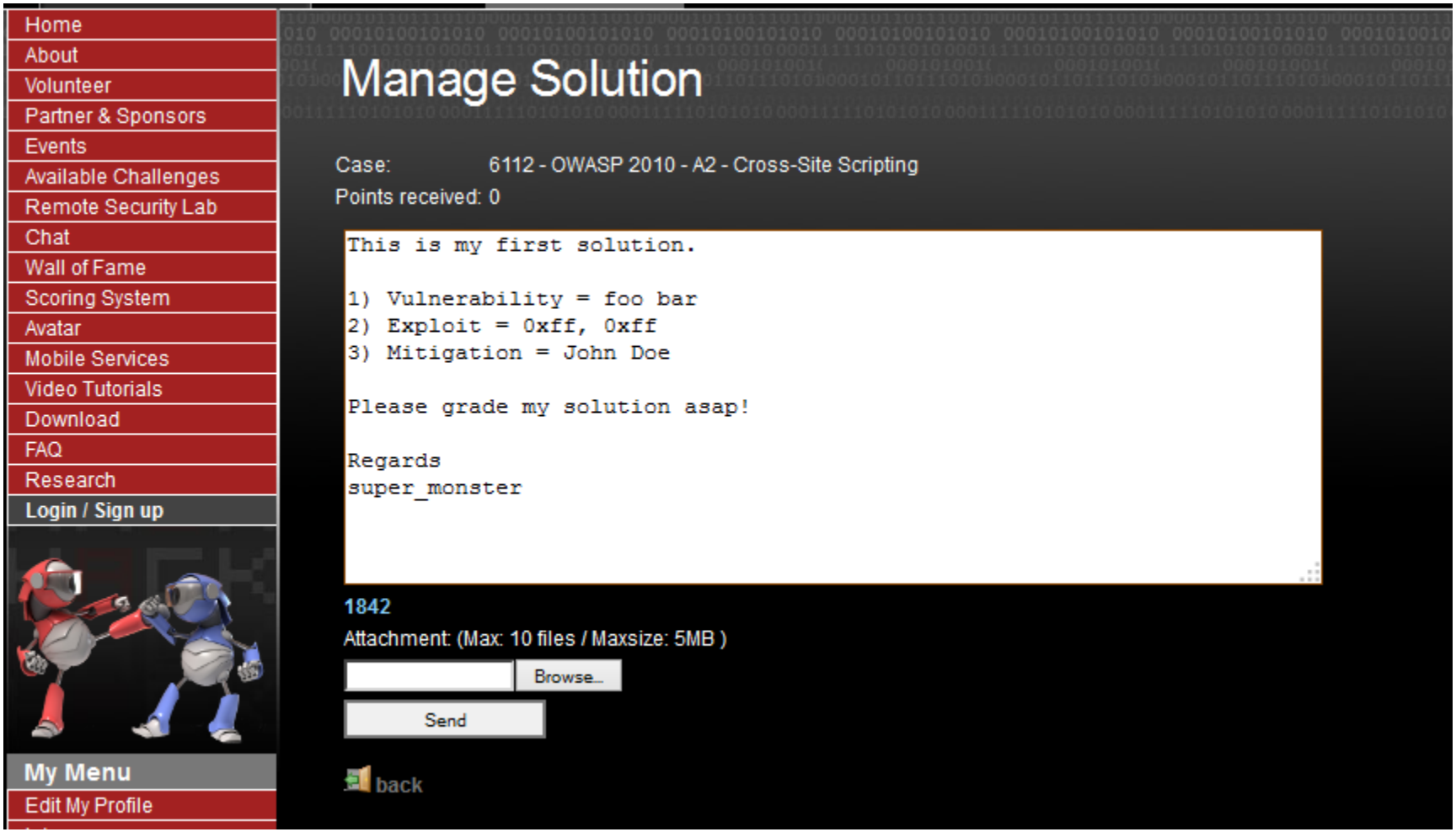
Link to the solution form
Press this link to submit your solution

OWASP Top Ten

Ranking Event Channel Event Participants

Topic	Type	Name	Level	Points	Duration	Solved by	Solution
	WG	6111 - OWASP 2010 - A1 – Injection	1	0/10	60	525	
	WG	6112 - OWASP 2010 - A2 - Cross-Site Scripting	1	0/10	30	175	
	WG	6113 - OWASP 2010 - A3 – Broken Authentication and Session Management	1	0/10	30	132	
	WG	6114 - OWASP 2010 - A4 – Insecure Direct Object References	1	0/10	60	136	
	WG	6115 - OWASP 2010 - A5 – Cross Site Request Forgery	2	0/20	60	90	
	WG	6116 - OWASP 2010 - A6 – Security Misconfiguration	2	0/20	60	78	
	WG	6117 - OWASP 2010 - A7 – Insecure Cryptographic Storage	2	0/20	60	89	
	WG	6118 - OWASP 2010 - A8 – Failure to Restrict URL Access	1	0/10	30	76	
	WG	6119 - OWASP 2010 - A9 – Insufficient Transport Layer Protection	1	0/10	30	67	
	WG	6120 - OWASP 2010 - A10 – Unvalidated Redirects and Forwards	1	0/10	10	59	

SOLUTION FORM (INCLUDING ATTACHMENTS)



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)

HACKING-LAB TOOLS

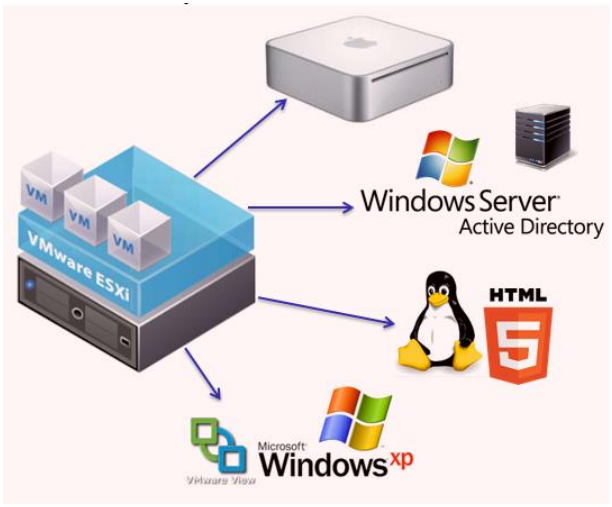
www.hacking-lab.com

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
www.csnc.ch

TOOLS REQUIRED TO SOLVE THE CHALLENGES

VPN to Lab



LiveCD

OpenVPN into ESX Server Infrastructure

HACKING-LAB TOOL OVERVIEW

LiveCD

Windows XP VDI clients

iRAPP **OSX** Terminal Server

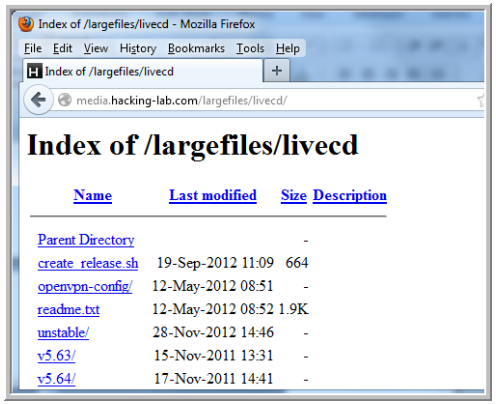
LIVECD

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

LIVECD FREE DOWNLOAD

http://media.hacking-lab.com



LiveCD
VirtualBox OVA

LiveCD
Vmware OVA

LiveCD ISO

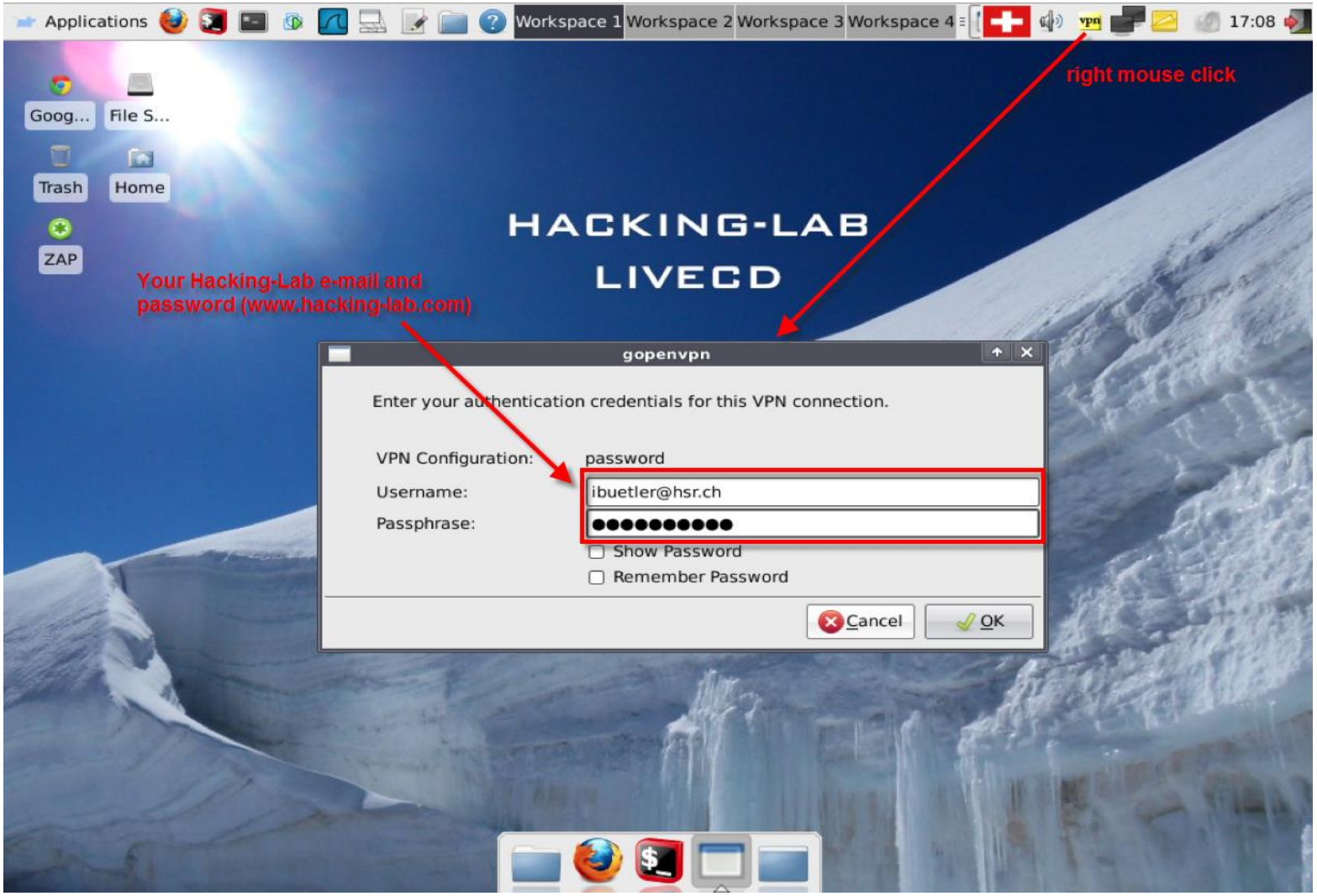
LIVECD FEATURES

1. VPN Icon

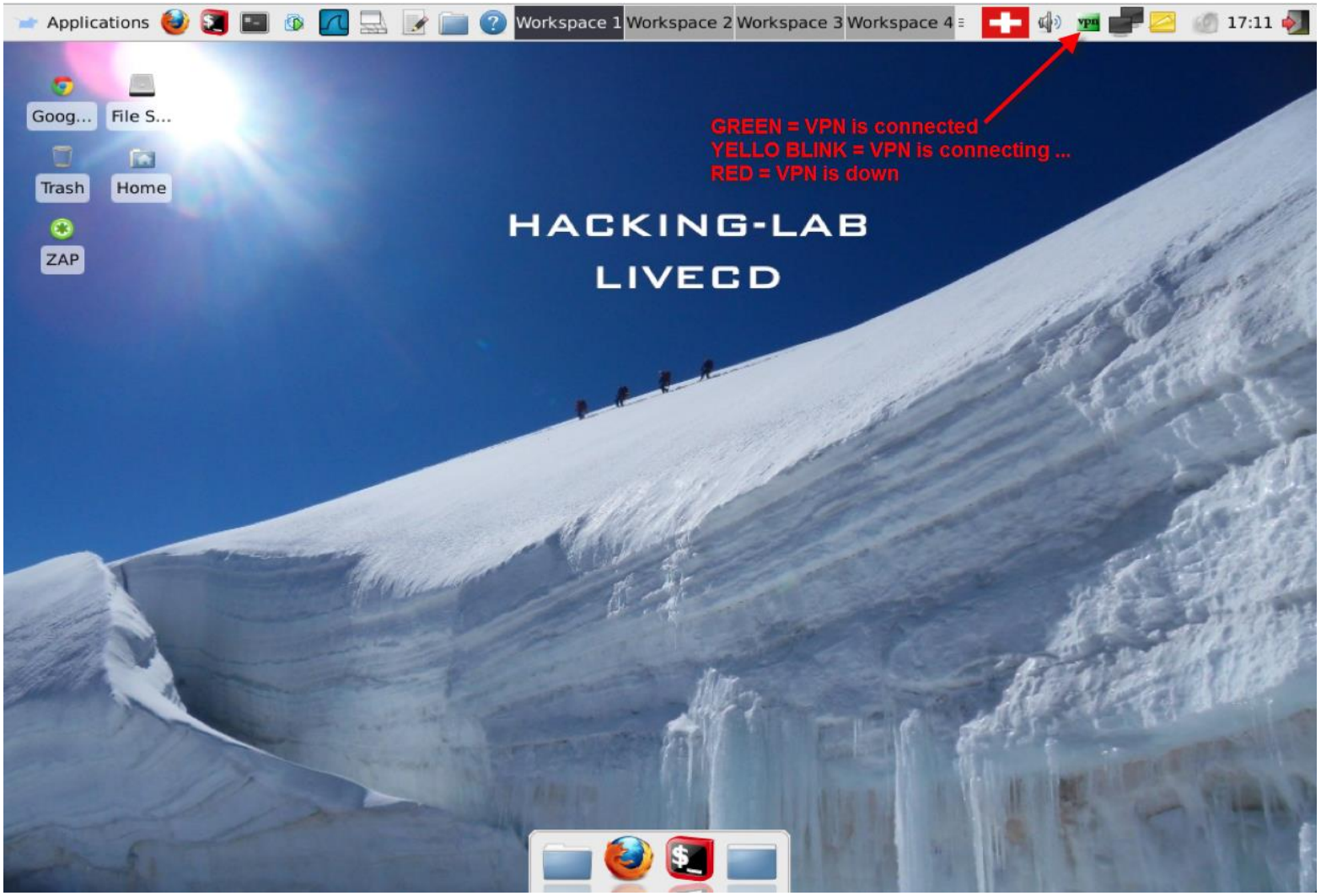
2. Root Shell
3. ZAP Inspection Proxy
4. Firefox Profiles
5. Firefox Switch Proxy
6. Landing Page Web Server
7. Local Doku Wiki Web Server

LIVECD DESKTOP

VPN ICON


Applications
Workspace 1
Workspace 2
Workspace 3
Workspace 4
17:08
Goog...
File S...
Trash
Home
ZAP
HACKING-LAB
LIVECD
right mouse click
Your Hacking-Lab e-mail and password (www.hacking-lab.com)
gopenvpn
Enter your authentication credentials for this VPN connection.
VPN Configuration:
password
Username:
ibuetler@hsr.ch
Passphrase:
Show Password
Remember Password
Cancel
OK

VPN GREEN = CONNECTED

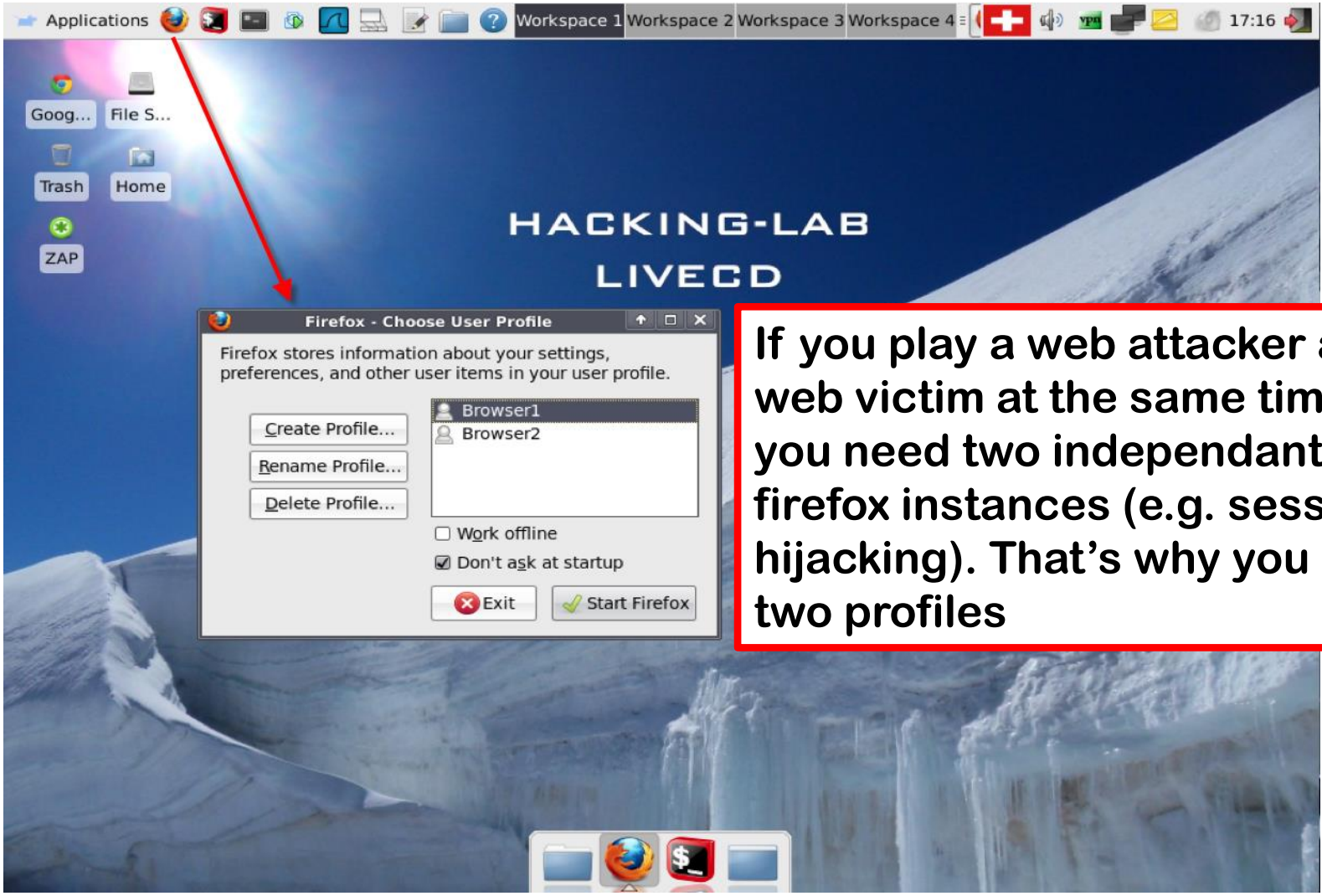


ROOT SHELL


HackingLab LiveCD V7.08 [Running]
Applications
Workspace 1
Workspace 2
Workspace 3
Workspace 4
17:01
Goog...
File S...
Trash
Home
ZAP
Open a ROOT shell
HACKING-LAB
LIVECD

START FIREFOX PROFILE MANAGER

FIREFOX PROFILE MANAGER



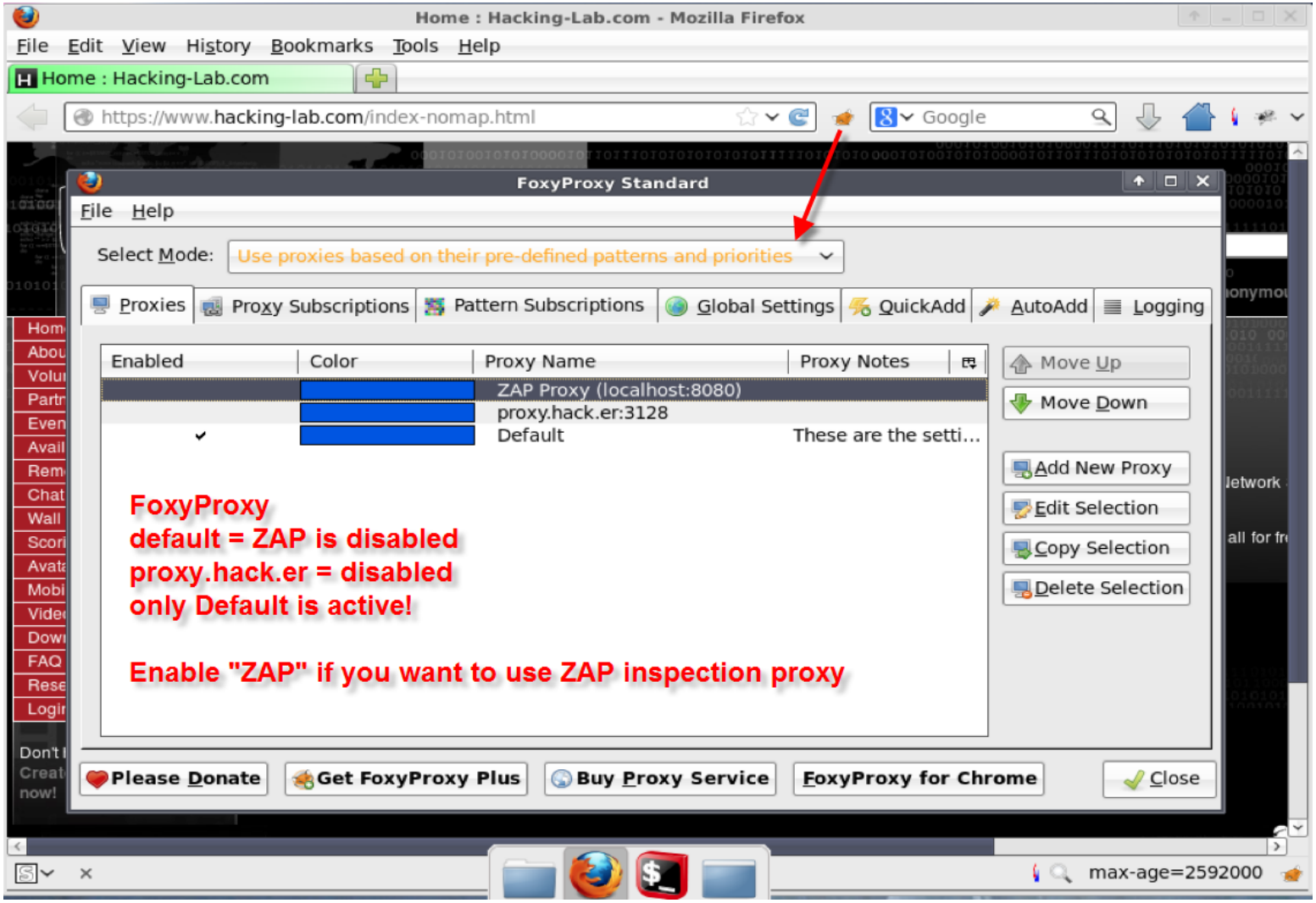
If you play a web attacker and web victim at the same time, you need two independant firefox instances (e.g. session hijacking). That's why you have two profiles

FIREFOX TESTING PROFILES

FIREFOX TESTING PROFILES

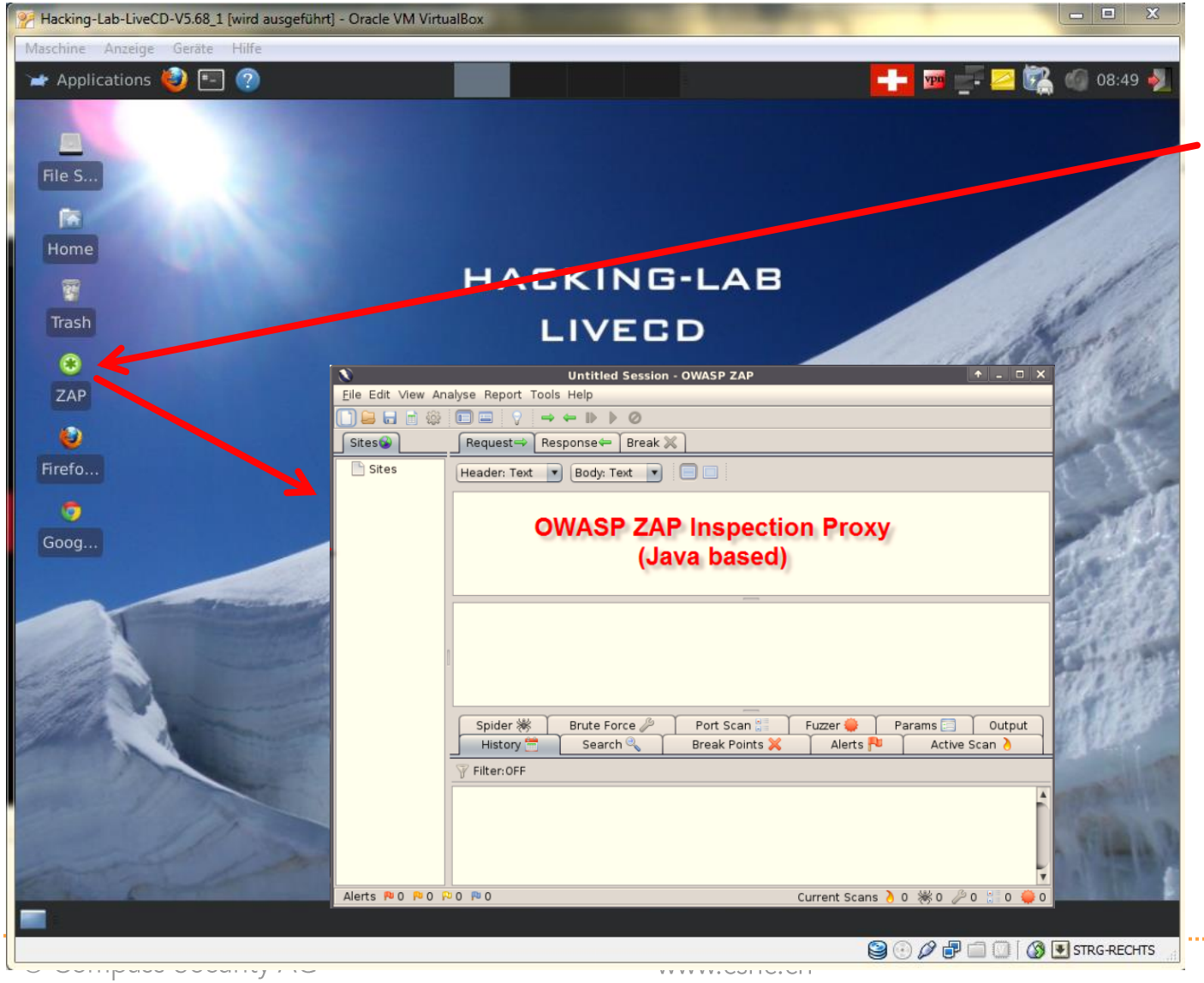
1. Firebug
2. FoxyProxy Switch Proxy Tool
3. LiveHttpHeader Plugin
4. Cookie Manager (change your cookie values)

FIREFOX – FOXYPROXY PLUGIN (ZAP)



ZAP INSPECTION PROXY (SLOW LOADING)

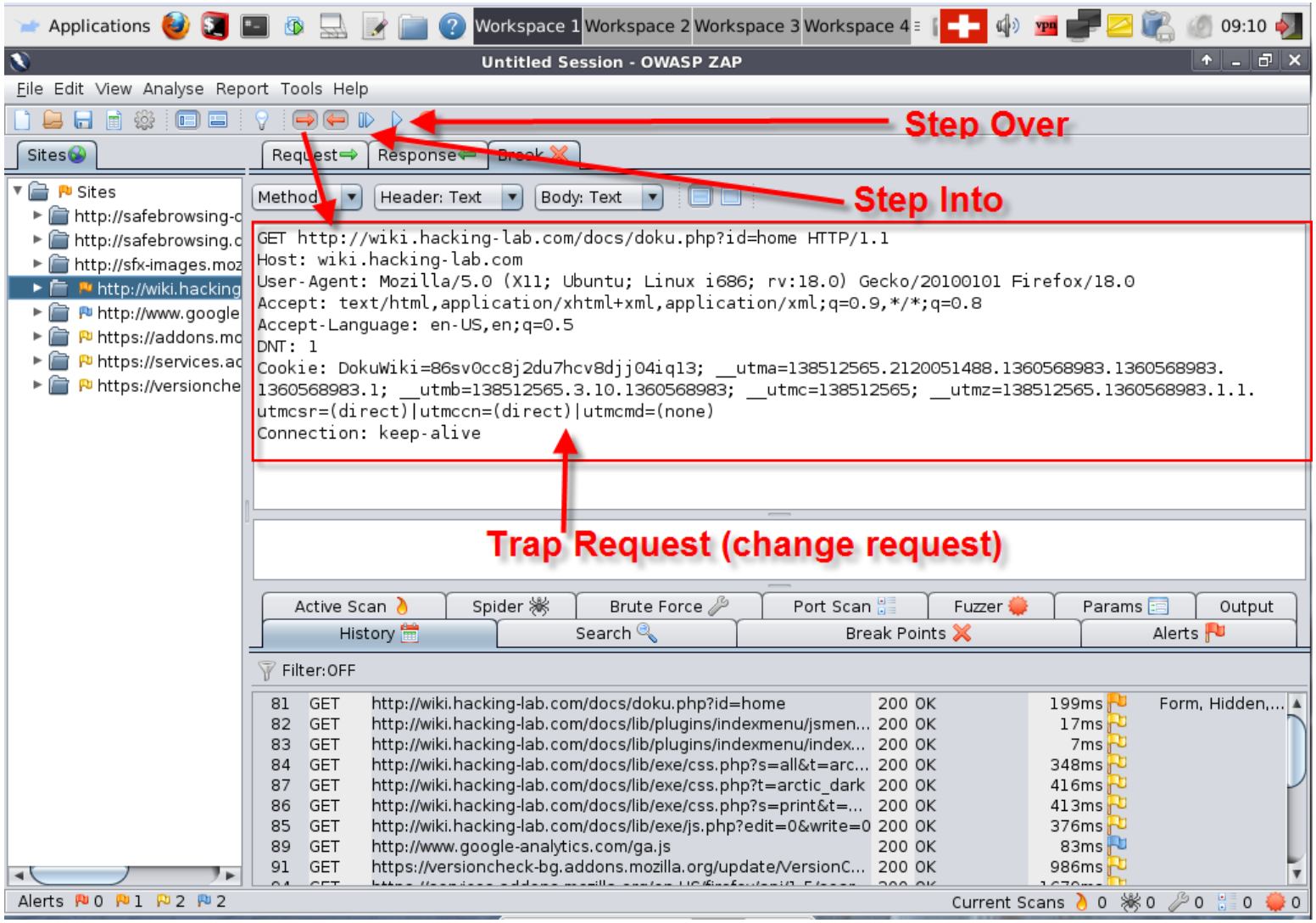
WEB MAN IN THE MIDDLE INSPECTION PROXY



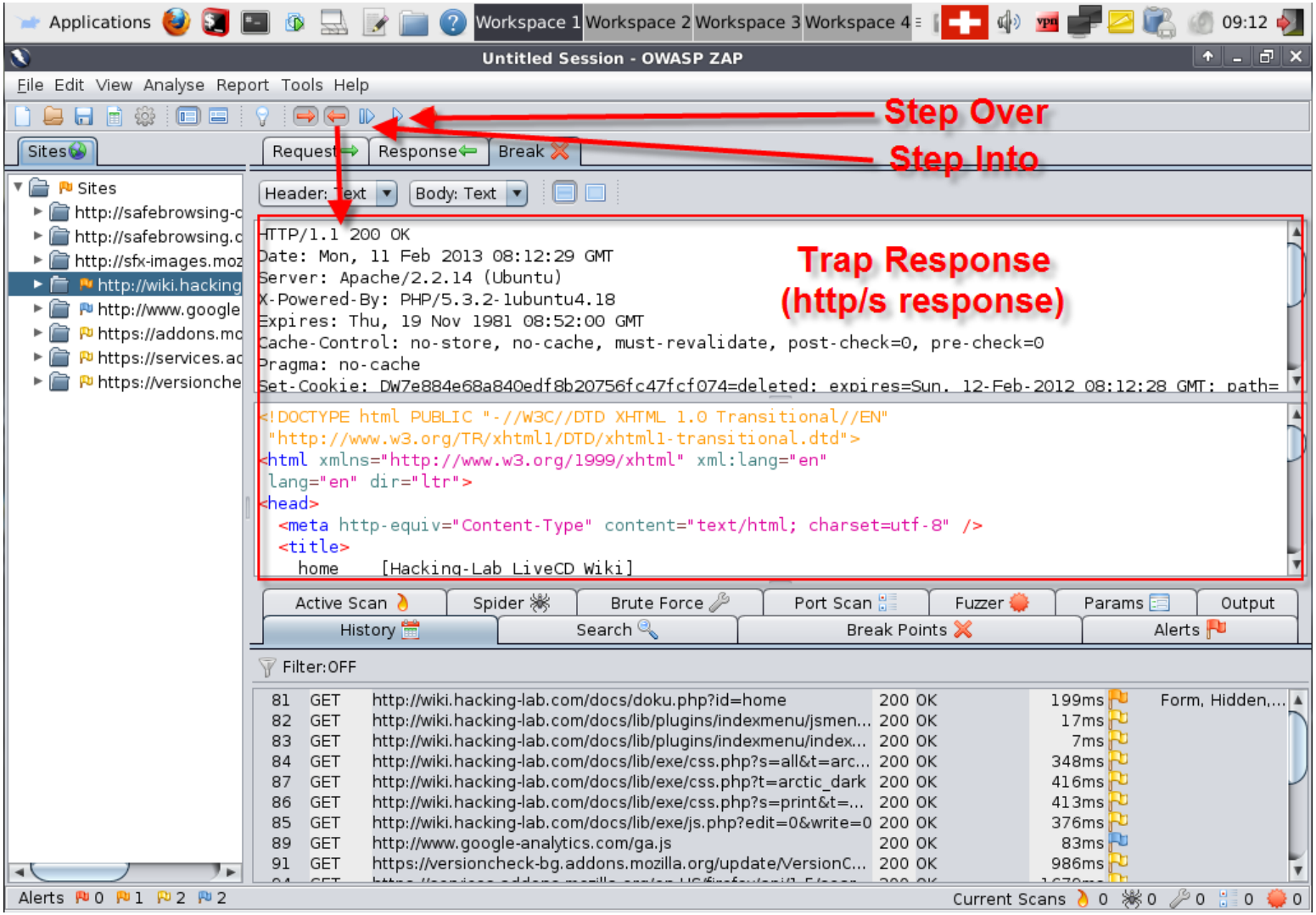
ZAP Inspection Proxy

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

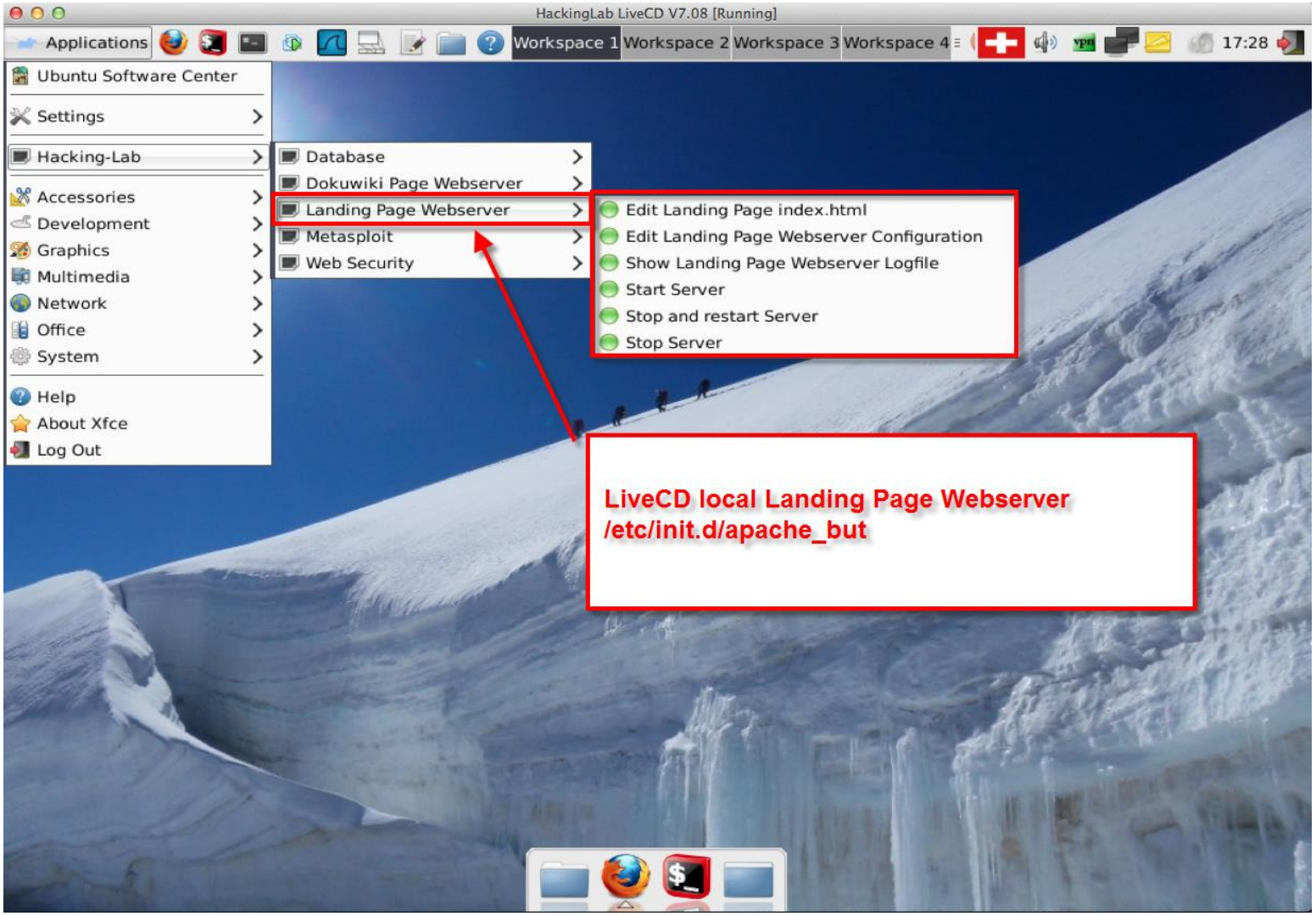
MANIPULATE HTTP REQUESTS



MANIPULATE HTTP RESPONSES



LIVECD LANDING PAGE WEBSERVER

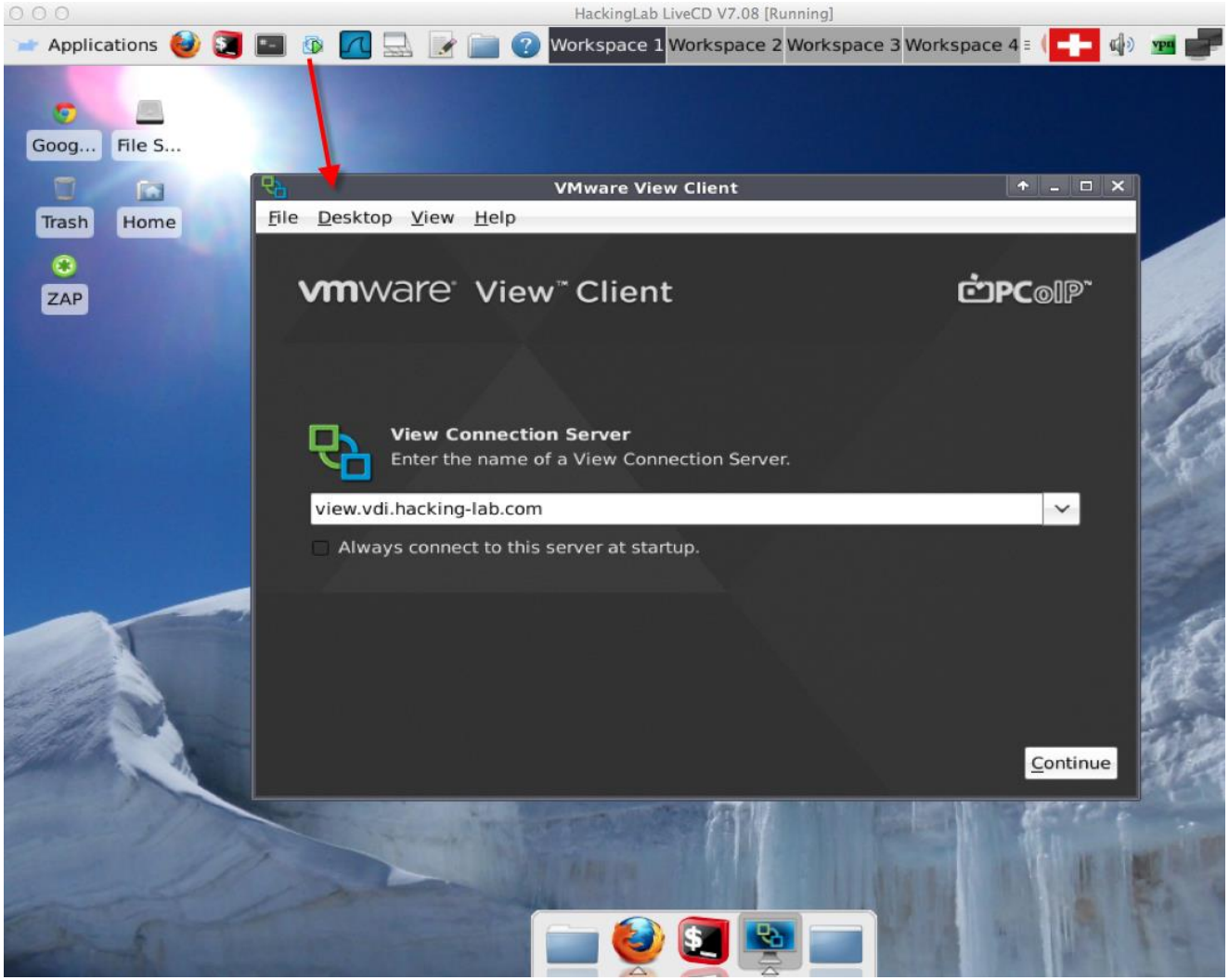


WINDOWS XP VDI HOST

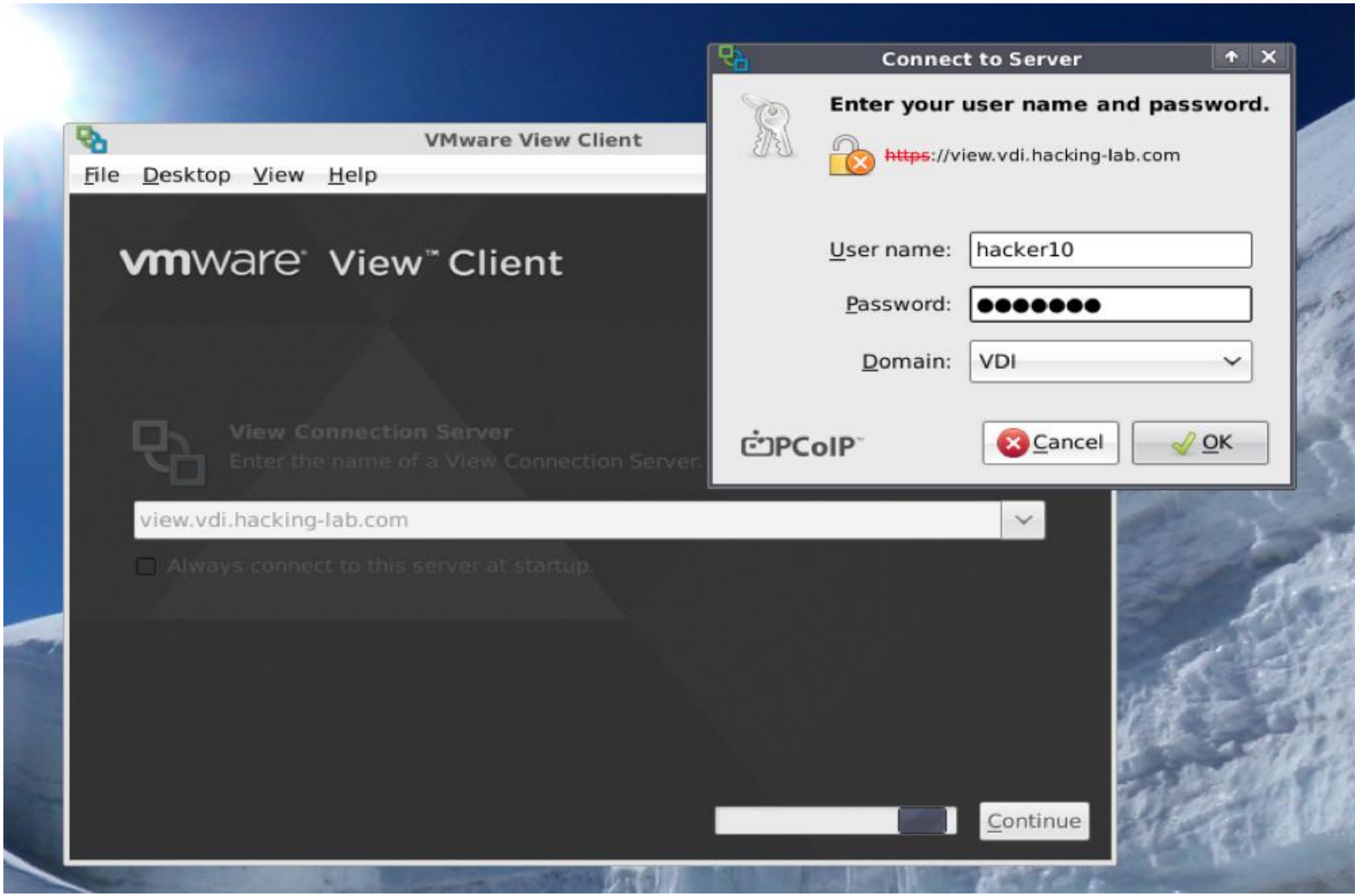
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

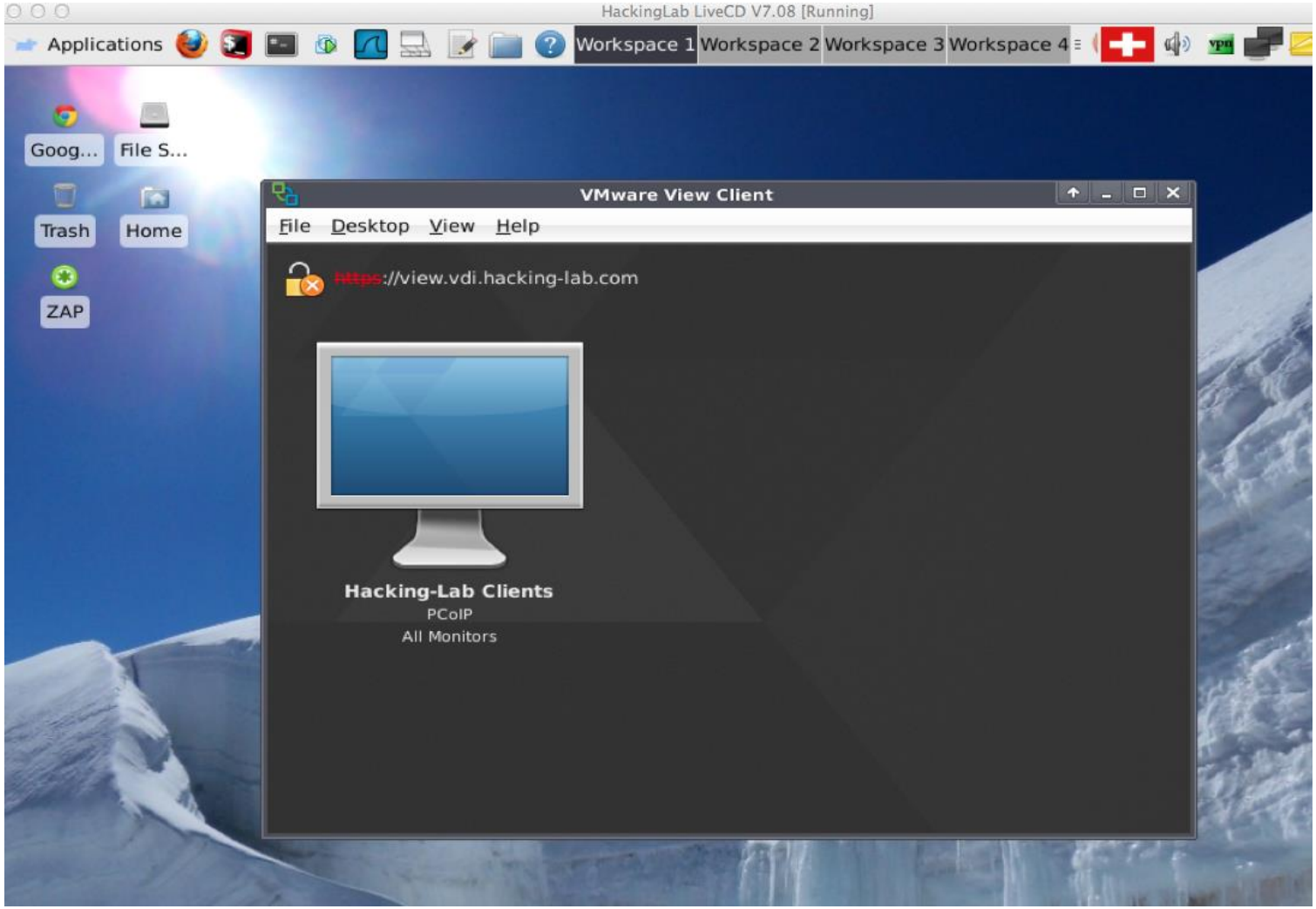
WINDOWS XP VDI (VMWARE VIEW)



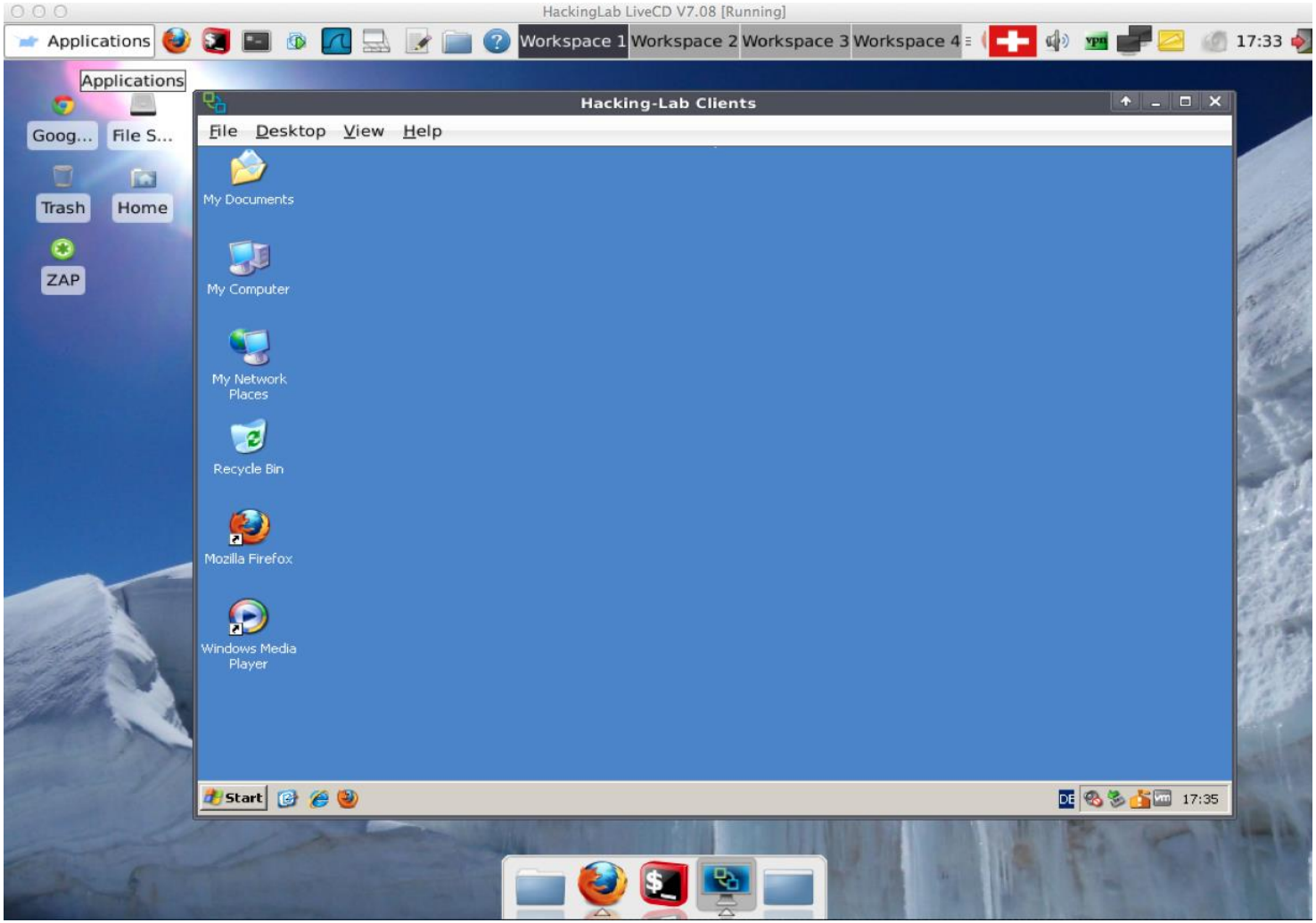
USER = HACKER10, HACKER11, HACKER12,
PASSWORD = COMPASS



WINDOWS XP VDI (VMWARE VIEW)



WINDOWS XP VDI (VMWARE VIEW)

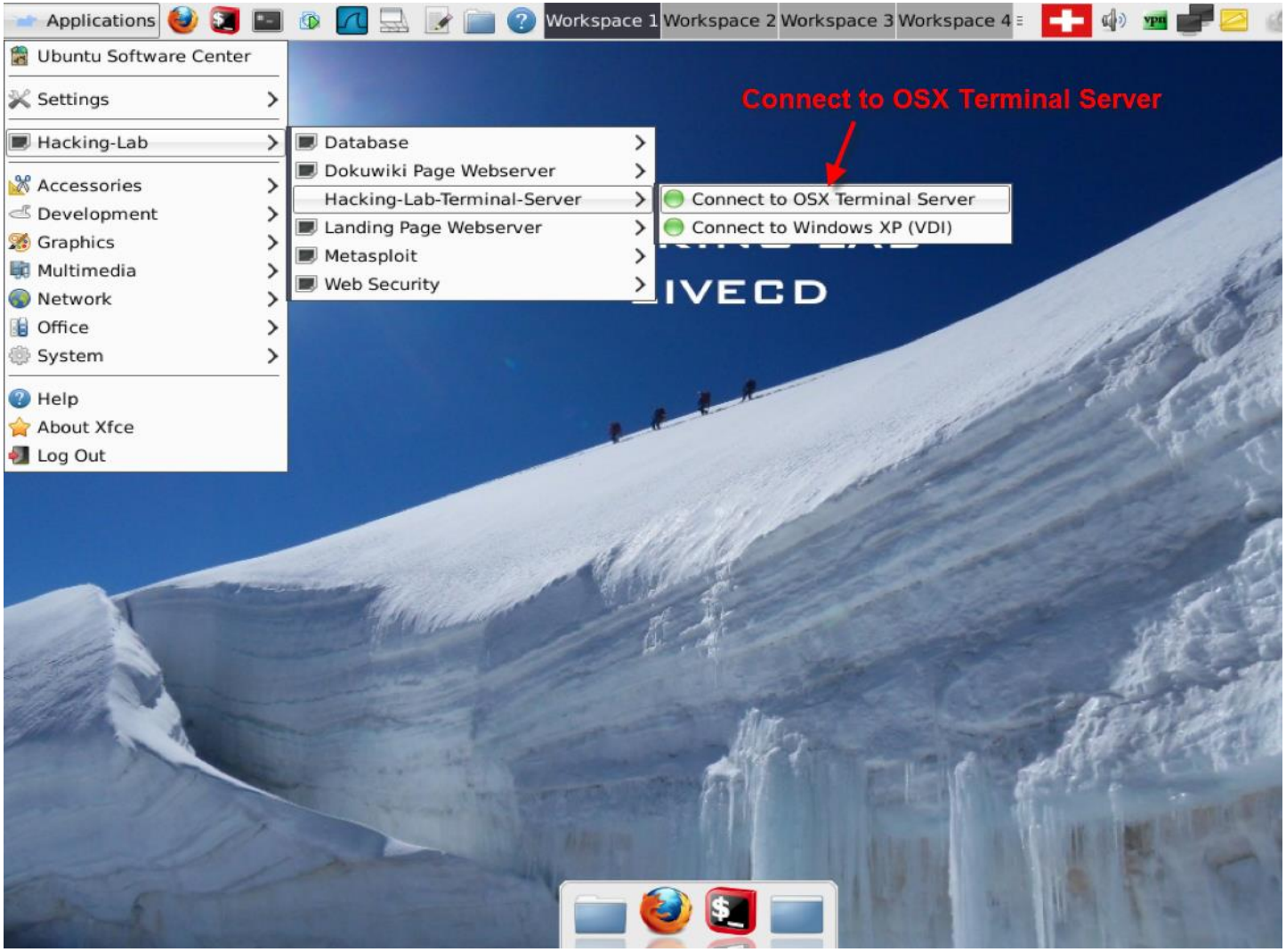


OSX TERMINAL SERVER

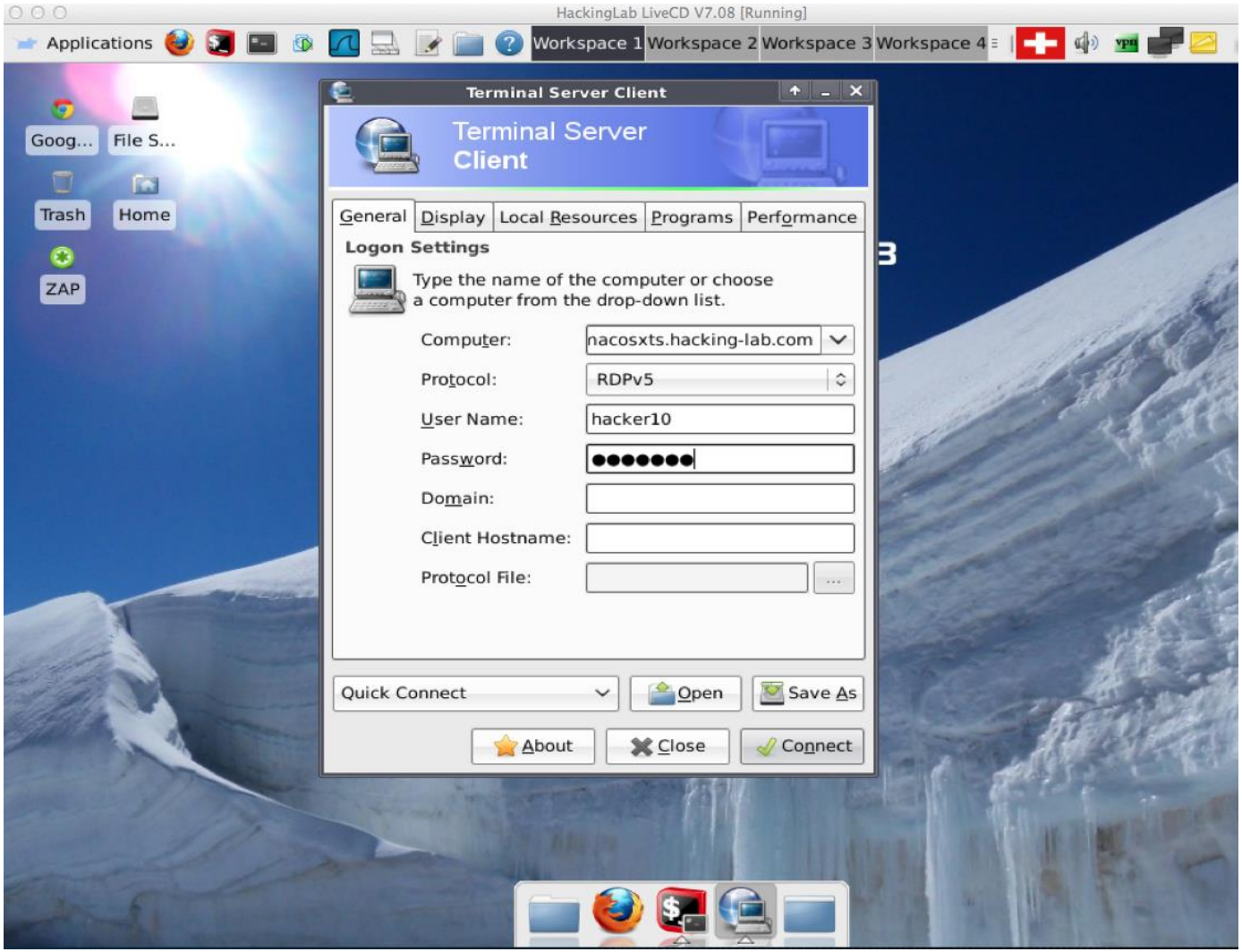
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

OSX TERMINAL SERVER



OSX TERMINAL SERVER



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

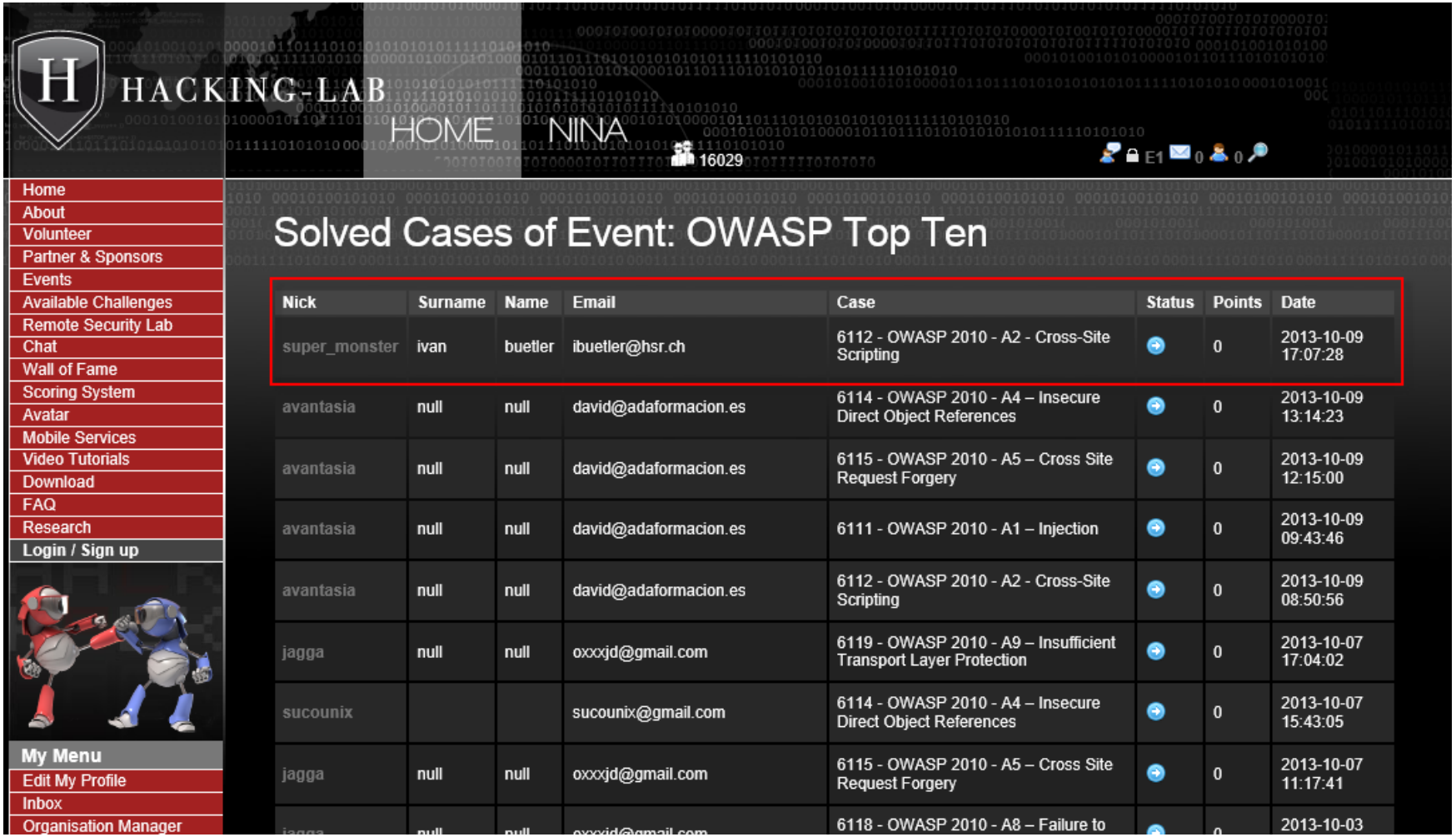
- (4) Teacher function (accept/reject solutions)

HACKING-LAB TEACHER TASKS

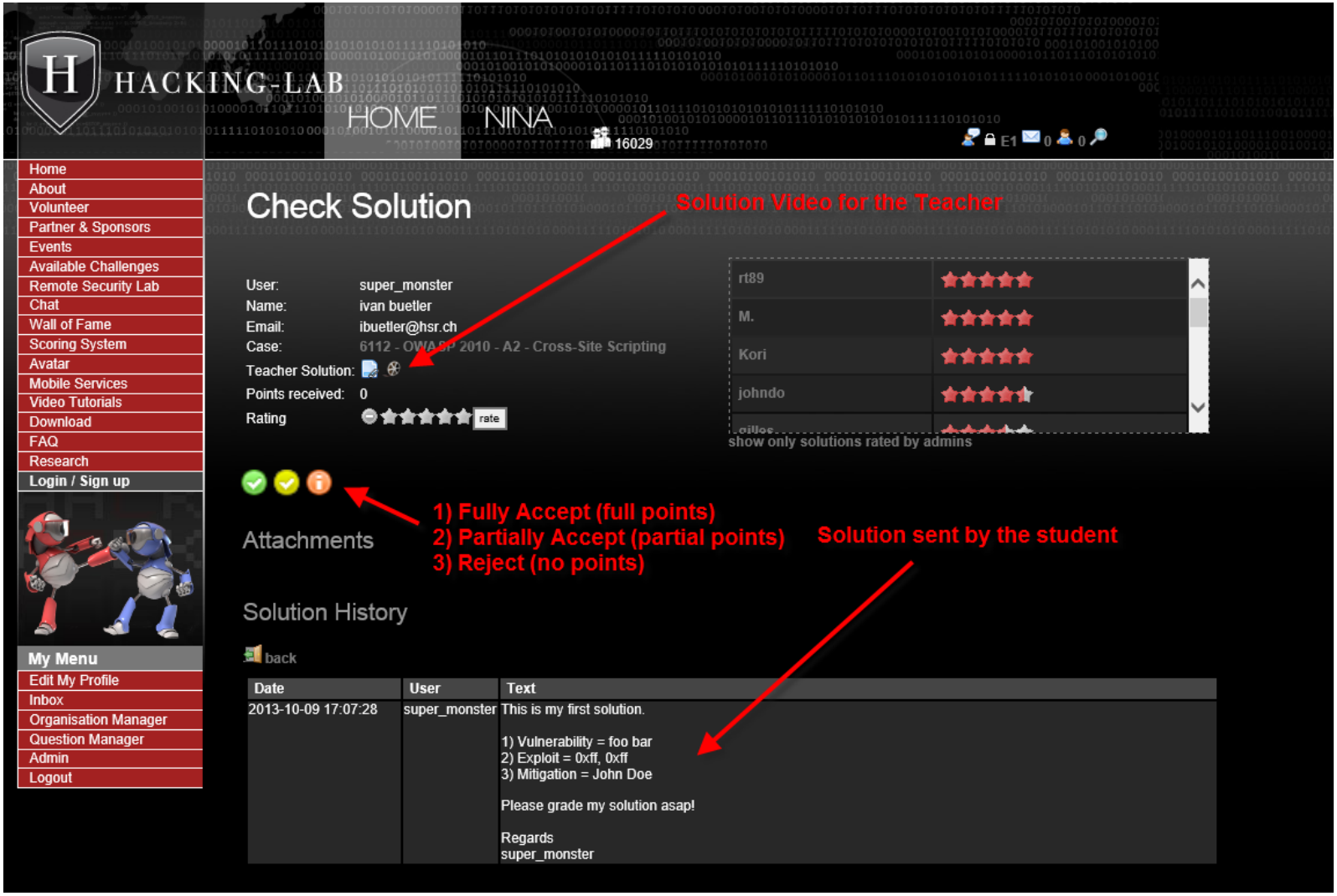
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

SOLUTION GRADING AS «TEACHER»

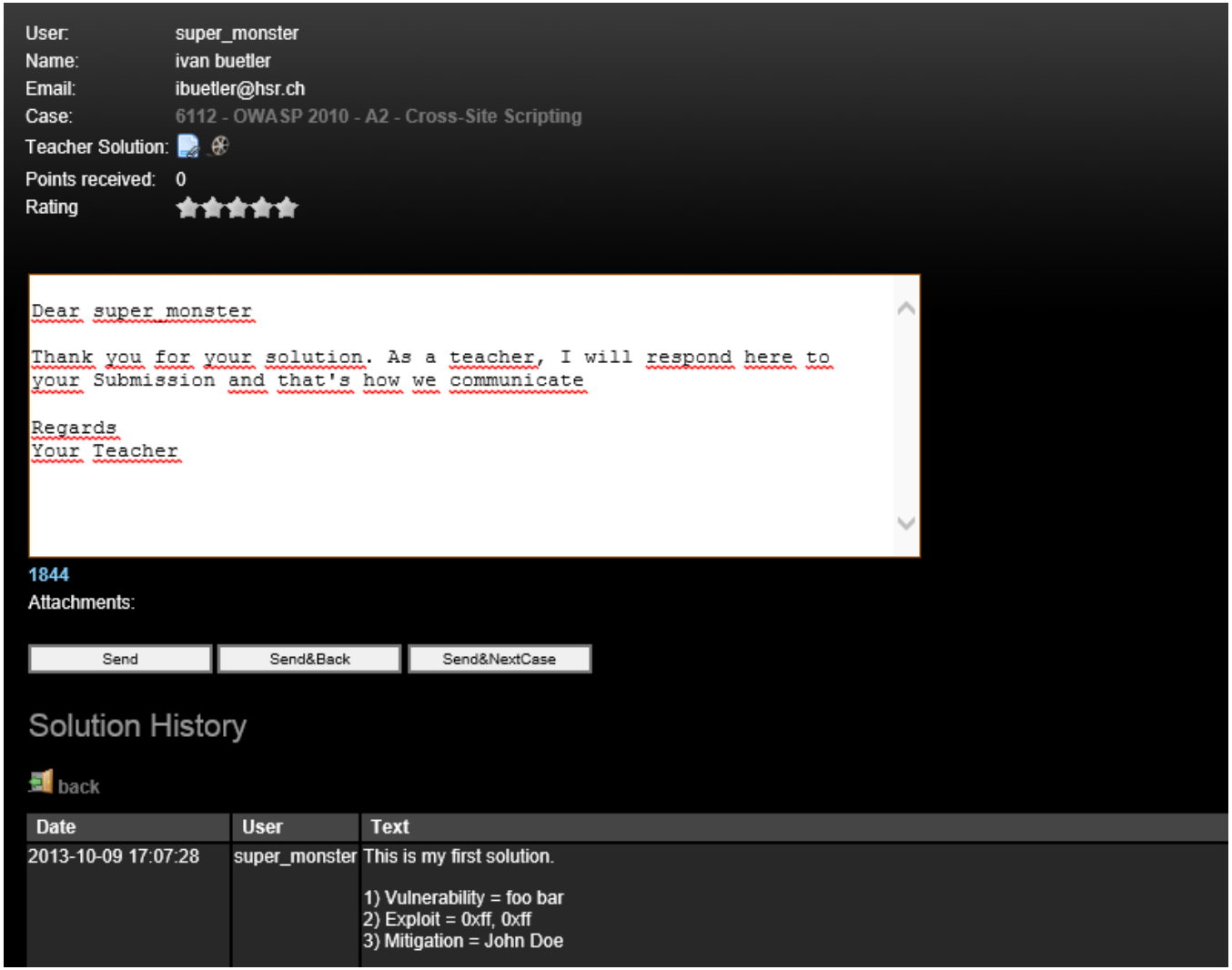


SOLUTION GRADING AS «TEACHER»



TEACHER HAS ACCESS TO «SOLUTION VIDEO»

SOLUTION GRADING AS «TEACHER»

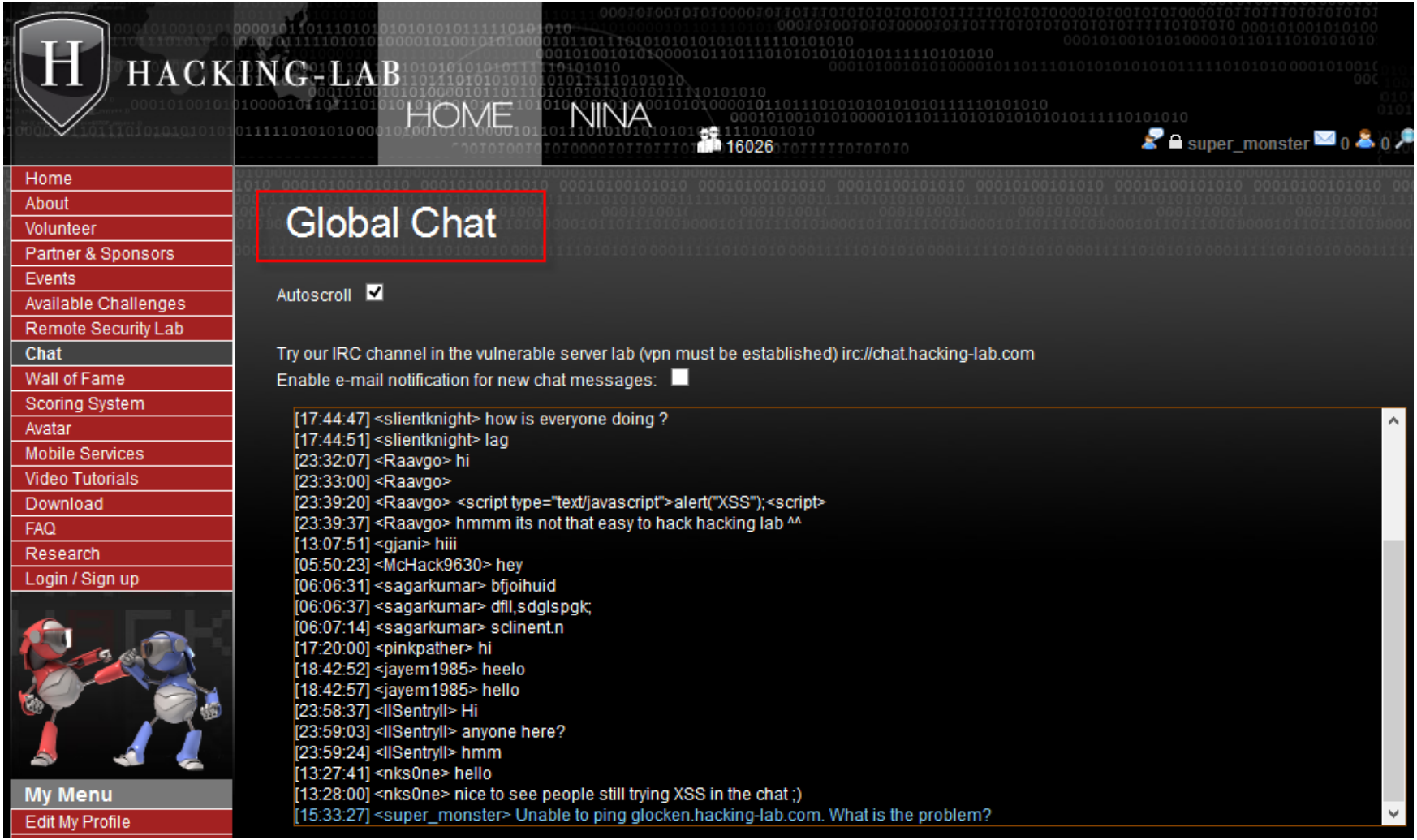


HACKING-LAB SUPPORT

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

GLOBAL CHAT


HACKING-LAB
HOME
NINA
16026
super_monster 0 0
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
My Menu
Edit My Profile
Global Chat
Autoscroll
Try our IRC channel in the vulnerable server lab (vpn must be established) irc://chat.hacking-lab.com
Enable e-mail notification for new chat messages:
[17:44:47] <slientknight> how is everyone doing ?
[17:44:51] <slientknight> lag
[23:32:07] <Raavgo> hi
[23:33:00] <Raavgo>
[23:39:20] <Raavgo> <script type="text/javascript">alert("XSS");<script>
[23:39:37] <Raavgo> hmmm its not that easy to hack hacking lab ^^
[13:07:51] <gjani> hiii
[05:50:23] <McHack9630> hey
[06:06:31] <sagarkumar> bfjoihuid
[06:06:37] <sagarkumar> dfll,sdglspgk;
[06:07:14] <sagarkumar> sclinent.n
[17:20:00] <pinkpather> hi
[18:42:52] <jayem1985> heelo
[18:42:57] <jayem1985> hello
[23:58:37] <IISentryII> Hi
[23:59:03] <IISentryII> anyone here?
[23:59:24] <IISentryII> hmm
[13:27:41] <nks0ne> hello
[13:28:00] <nks0ne> nice to see people still trying XSS in the chat ;)
[15:33:27] <super_monster> Unable to ping glocken.hacking-lab.com. What is the problem?

VIDEO TUTORIALS AND HELP

- LiveCD usage with VirtualBox Appliance

- LiveCD usage with Vmware8 workstation

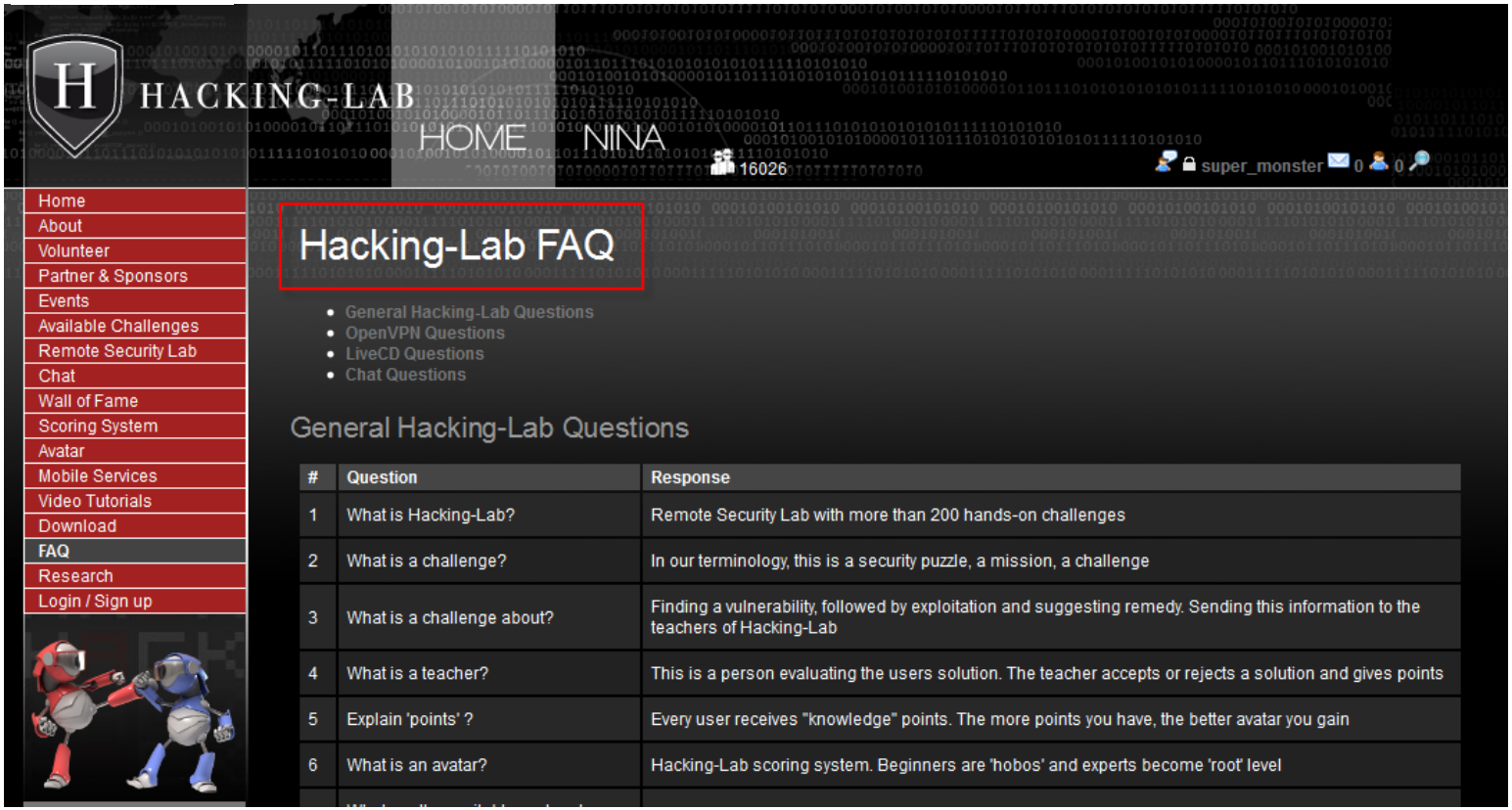
- How to connect in HL with OpenVPN

VIDEO TUTORIALS

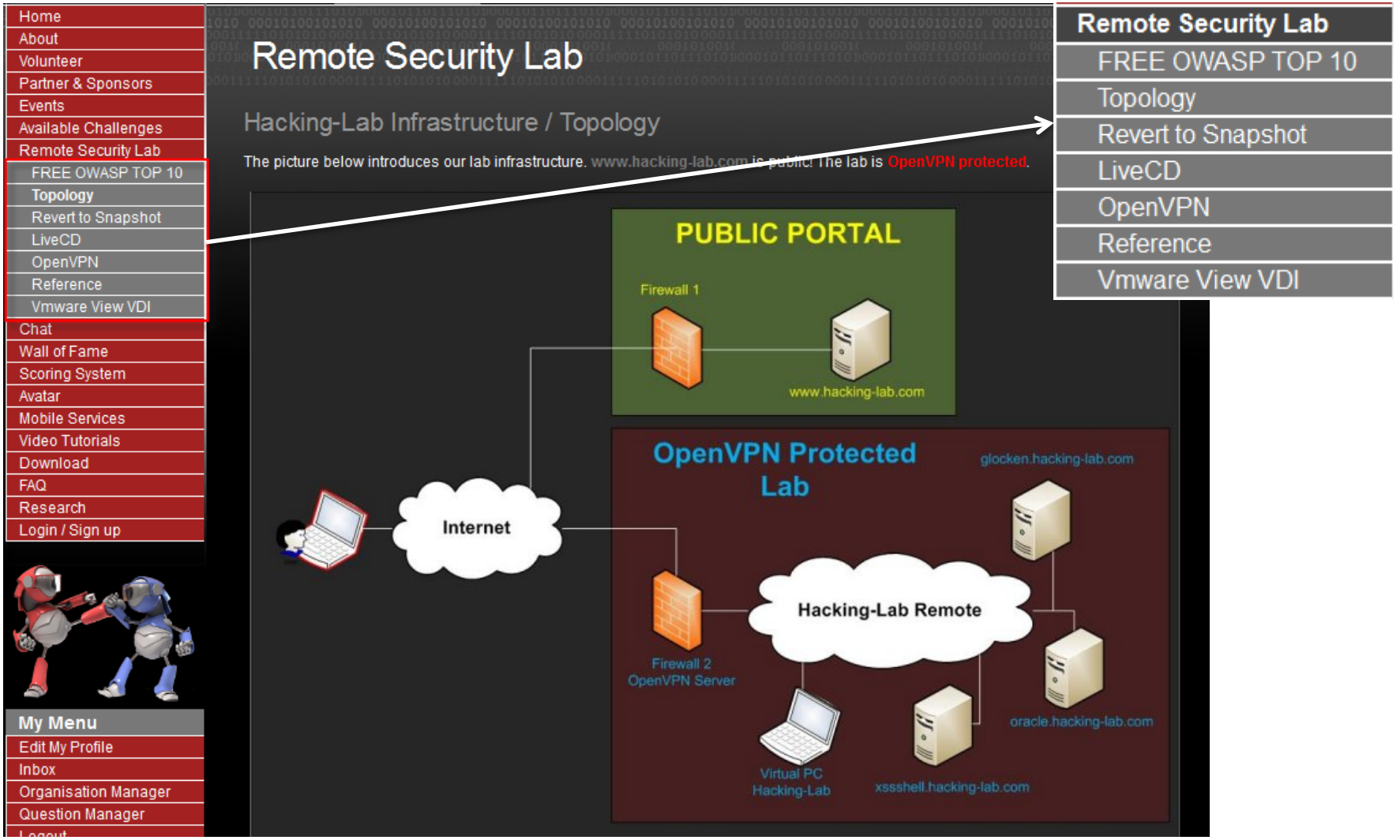
https://www.hacking-lab.com/tutorial/

HACKING-LAB FAQ

https://www.hacking-lab.com/FAQ/



DESCRIPTION OF HACKING-LAB



HACKING-LAB ARCHITECTURE FOR THIS LAB

For today, the following WLAN connects you straight into the lab

- SSID: Hacking-lab
- Passphrase: hacking-lab
- IP address is assigned automatically (DHCP)

I recommend the following challenges to start with:

- For beginners
  - 6111 - OWASP 2010 - A1 – Injection Step-by-Step (SBS)
- For intermediates
  - 6111 - OWASP 2010 - A1 – Injection War Game (WG)
- For advanced
  - 7041 Struts2 Vulnerability War Game (WG)

Pascal and I will evaluate the answers submitted this morning

- The event will remain open until end of 2013
- Feel free to continue solving challenges until then – correction will also occur, but probably with some delay

CONTACT DETAILS

Do not hesitate to ask!