



# 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](mailto:team@csnc.ch)  
[www.csnc.ch](http://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: 1110101010

Password:

[Login »](#)

Status: 9 october 2013

Anonymous User

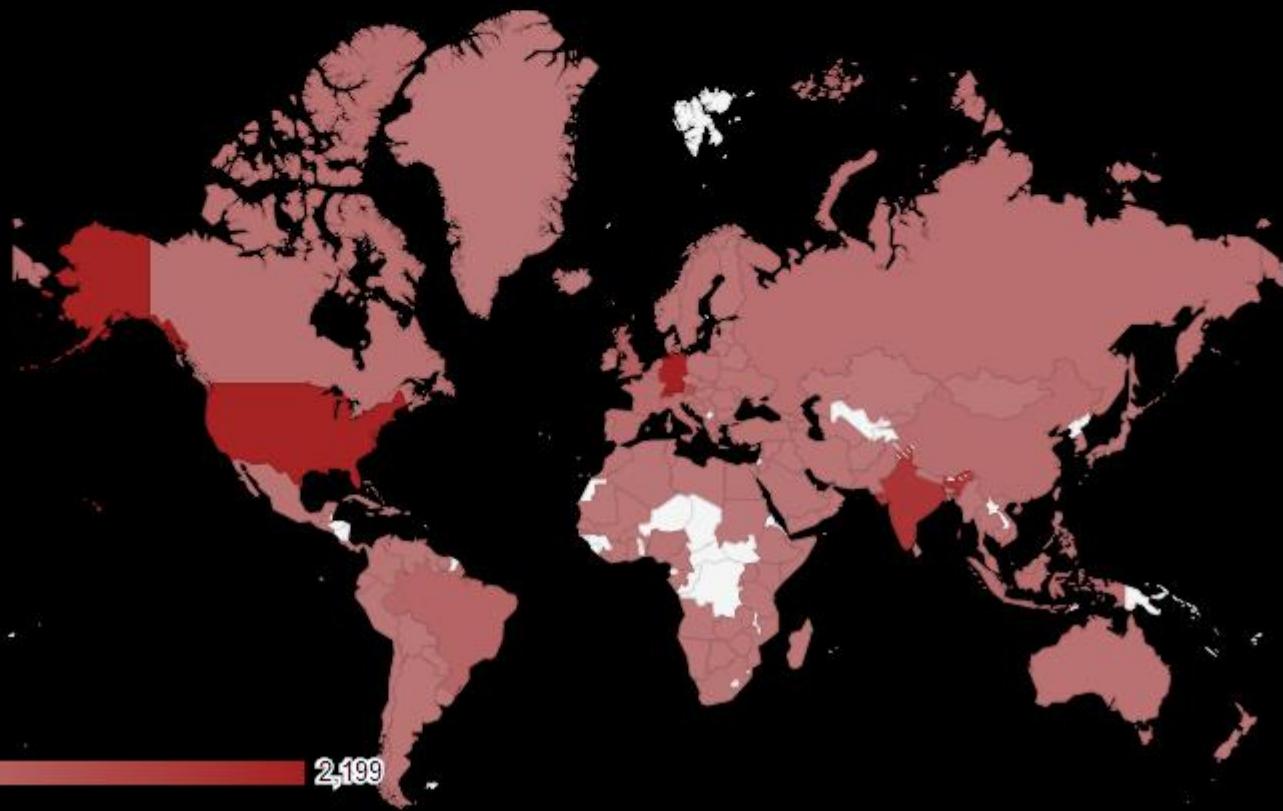
- [Home](#)
- [About](#)
- [Volunteer](#)
- [Partner & Sponsors](#)
- [Events](#)
- [Available Challenges](#)
- [Remote Security Lab](#)
- [Chat](#)
- [Wall of Fame](#)
- [Scoring System](#)
- [Avatar](#)
- [Mobile Services](#)
- [Video Tutorials](#)
- [Download](#)
- [FAQ](#)
- [Research](#)
- [Login / 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](mailto:team@csnc.ch)  
[www.csnc.ch](http://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>

2013.appsec-forum.ch/ateliers/

- Personal account on <http://www.hacking-lab.com>  
- Additionally, each participant should register, when possible before the conference, to 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 <a href="http://www.Hacking-Lab.com">www.Hacking-Lab.com</a>	Niveau			Prérequis en ordre?
	Débutant	Intermédiaire	Avancé	



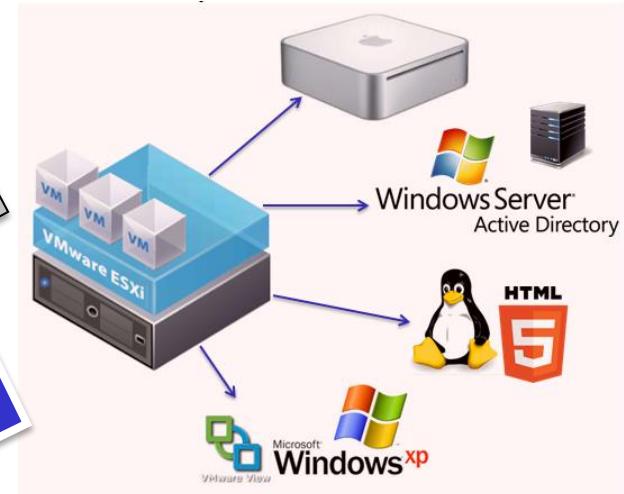
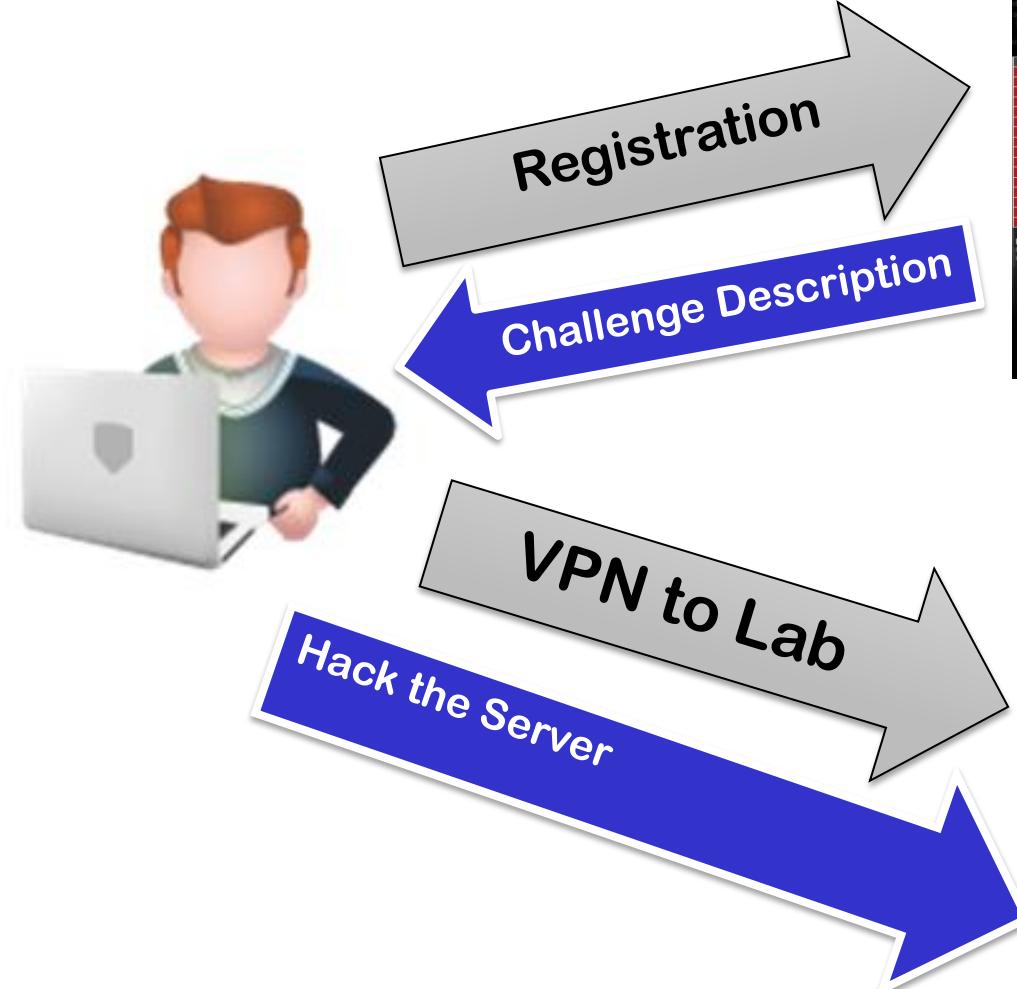
# HOW TO USE HACKING-LAB

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](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

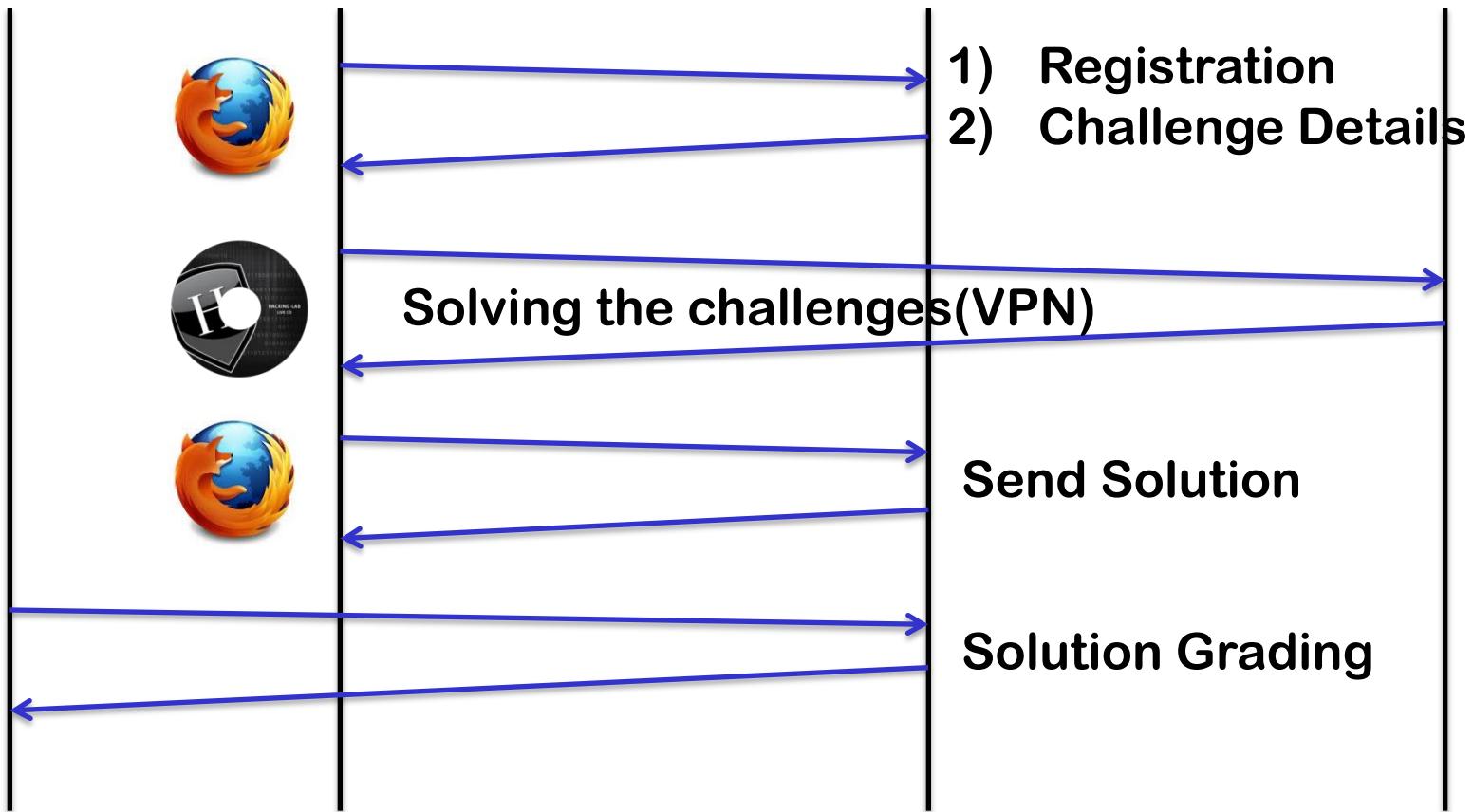
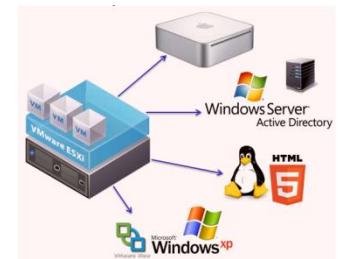
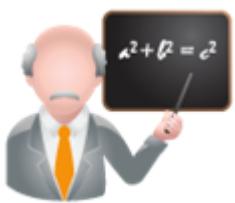


# WHAT IS «HACKING-LAB»????





# UNDERSTANDING HACKING-LAB





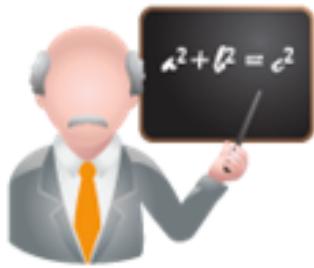
# HACKING-LAB ROLES

➤ 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) PARTIALLY 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](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)



# WHAT IS «HACKING-LAB»????



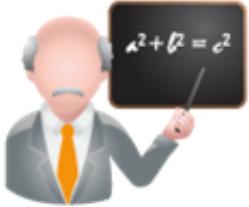
- (1) Vulnerable Servers and Applications  
(Web, Windows, Linux, iOS, Android)



- (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)



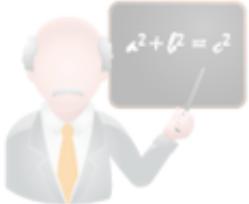
- (1) Vulnerable Servers and Applications  
(Web, Windows, Linux, iOS, Android)



- (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](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)



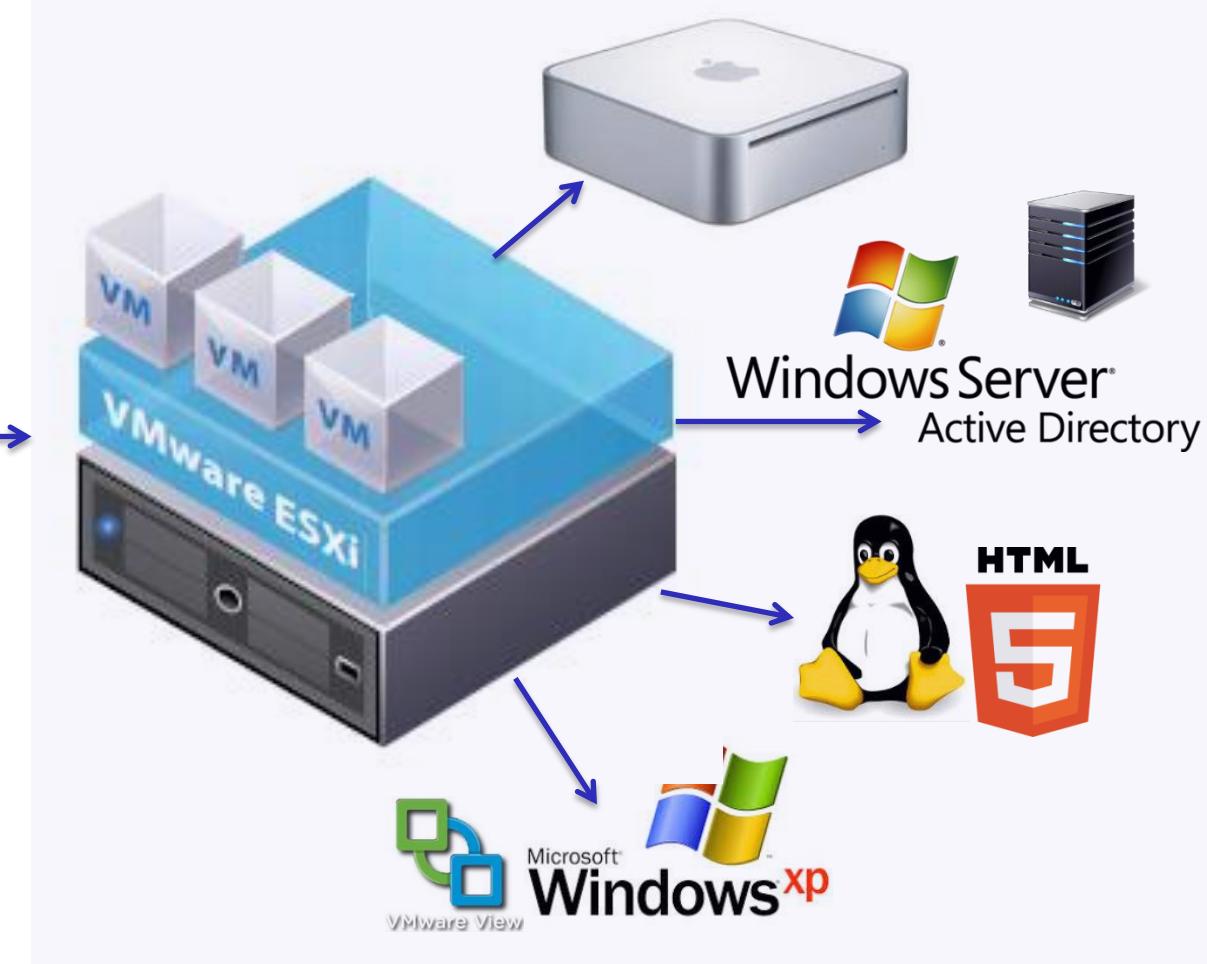
# DETAILS ABOUT HACKING-LAB

Vulnerable **Mobile**  
Apps



Vulnerable **Servers**  
Remote Security Lab

Automatic Revert to Snapshot





# MOVIE: INTRODUCTION ESXI

 Introduction\_ESXi.mp4

21.09.2013 22:57

MP4 File

52'220 KB

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)



## DETAILS ABOUT HACKING-LAB (2/4)



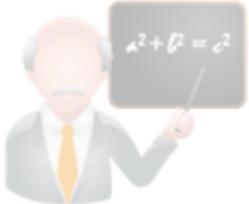
- (1) Vulnerable Servers and Applications  
(Web, Windows, Linux, iOS, Android)



- (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](http://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

[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](#)[Inbox](#)[Organisation Manager](#)[Question Manager](#)[Logout](#)

# 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	

[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](#)[Inbox](#)[Organisation Manager](#)[Question Manager](#)[Logout](#)

# 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



**Challenge Type**  
**WG** = Wargame  
**SBS** = Step by Step

## OWASP Top Ten

Ranking Event Channel Event Participants

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

[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](#)[Inbox](#)[Organisation Manager](#)[Question Manager](#)[Logout](#)

# OWASP

The Open Web Application Security Project

Link to the description (mission) of the challenge

## 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	

[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](#)[Inbox](#)[Organisation Manager](#)[Question Manager](#)[Logout](#)

# OWASP

The Open Web Application Security Project

**Level 1 = Easy**

**Level 2 = Medium**

**Level 3 = Advanced**



## OWASP Top Ten

Ranking Event Channel Event Participants

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

[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](#)[Inbox](#)[Organisation Manager](#)[Question Manager](#)[Logout](#)

# OWASP

The Open Web Application Security Project

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

[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](#)[Inbox](#)[Organisation Manager](#)[Question Manager](#)[Logout](#)

# OWASP

The Open Web Application Security Project

## OWASP Top Ten

Ranking Event Channel Event Participants

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

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



[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](#)[Inbox](#)[Organisation Manager](#)[Question Manager](#)[Logout](#)

# 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	



[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](#)[Inbox](#)[Organisation Manager](#)[Question Manager](#)[Logout](#)

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





# SOLUTION FORM (INCLUDING ATTACHMENTS)

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

## Manage Solution

Case: 6112 - OWASP 2010 - A2 - Cross-Site Scripting  
Points received: 0

This is my first solution.

1) Vulnerability = foo bar  
2) Exploit = 0xff, 0xff  
3) Mitigation = John Doe

Please grade my solution asap!

Regards  
super\_monster

1842

Attachment (Max: 10 files / Maxsize: 5MB )

 back



## DETAILS ABOUT HACKING-LAB (3/4)



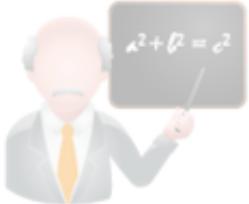
- (1) Vulnerable Servers and Applications  
(Web, Windows, Linux, iOS, Android)



- (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](http://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](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)



# TOOLS REQUIRED TO SOLVE THE CHALLENGES

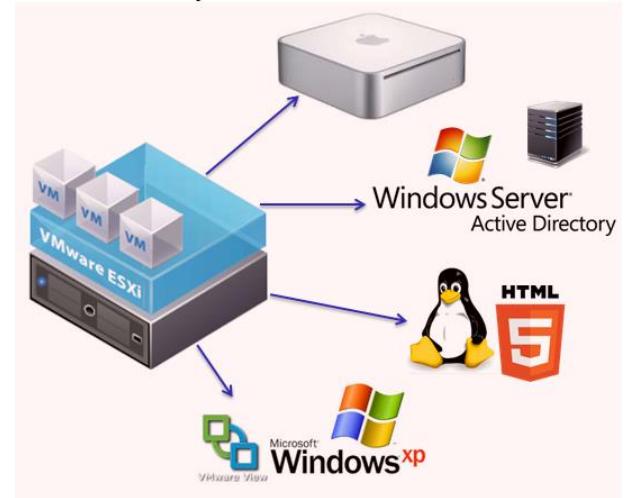


VPN to Lab



LiveCD

OpenVPN into ESX Server  
Infrastructure





# HACKING-LAB TOOL OVERVIEW



LiveCD



Windows XP VDI clients



iRAPPS 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](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)



# LIVECD FREE DOWNLOAD

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

Name	Last modified	Size	Description
Parent Directory		-	
<a href="#">create_release.sh</a>	19-Sep-2012 11:09	664	
<a href="#">openvpn-config/</a>	12-May-2012 08:51	-	
<a href="#">readme.txt</a>	12-May-2012 08:52	1.9K	
<a href="#">unstable/</a>	28-Nov-2012 14:46	-	
<a href="#">v5.63/</a>	15-Nov-2011 13:31	-	
<a href="#">v5.64/</a>	17-Nov-2011 14:41	-	



LiveCD  
VirtualBox OVA



LiveCD ISO



LiveCD  
Vmware OVA



## 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



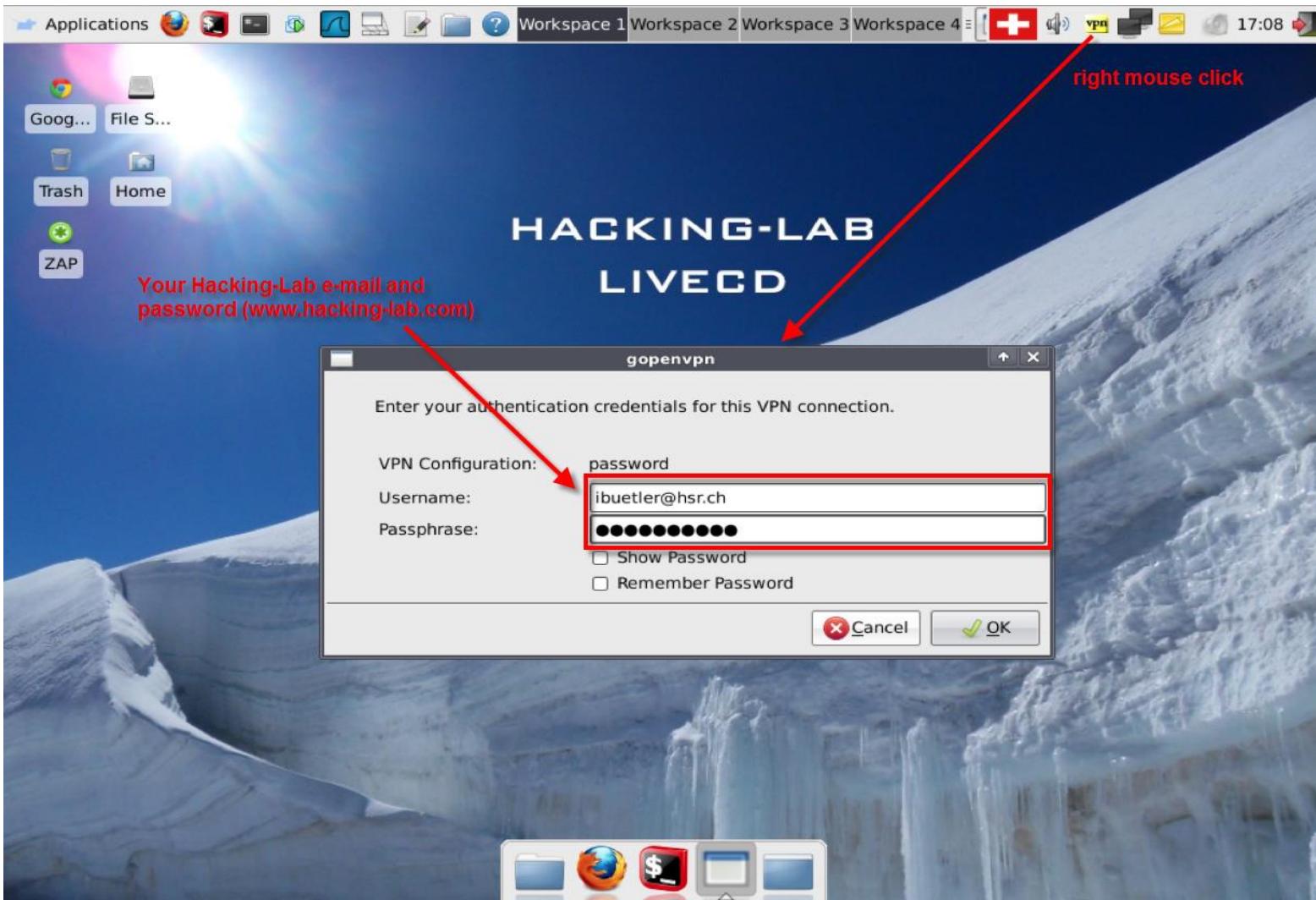


# LIVECD DESKTOP





# VPN ICON





# VPN GREEN = CONNECTED





# ROOT SHELL



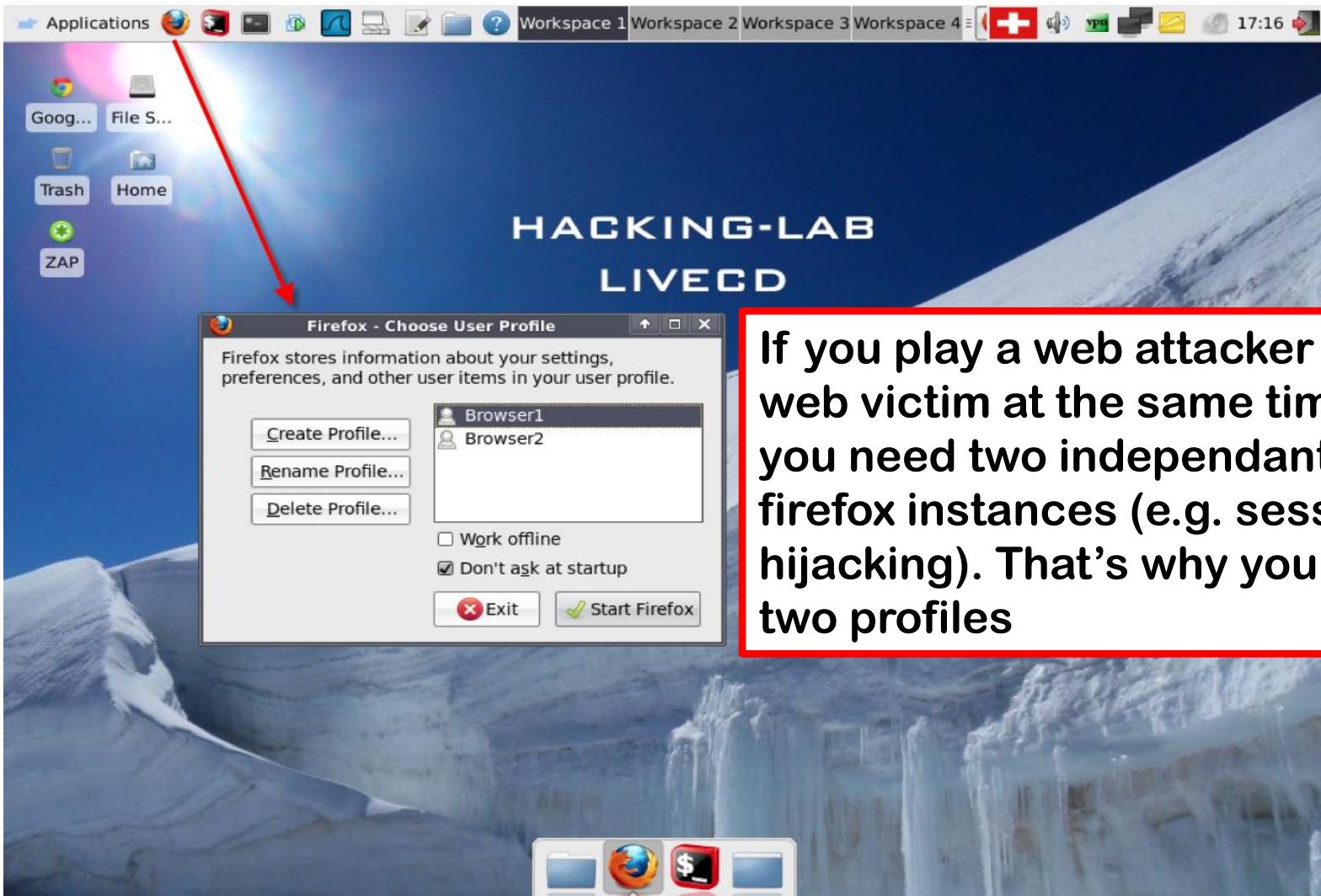


# START FIREFOX PROFILE MANAGER





# 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)

**FoxyProxy**  
default = ZAP is disabled  
proxy.hack.er = disabled  
only Default is active!

Enable "ZAP" if you want to use ZAP inspection proxy

File Help

Select Mode: Use proxies based on their pre-defined patterns and priorities

Proxies Proxy Subscriptions Pattern Subscriptions Global Settings QuickAdd AutoAdd Logging

Enabled	Color	Proxy Name	Proxy Notes
✓		ZAP Proxy (localhost:8080)	
✓		proxy.hack.er:3128	
✓		Default	These are the sett...

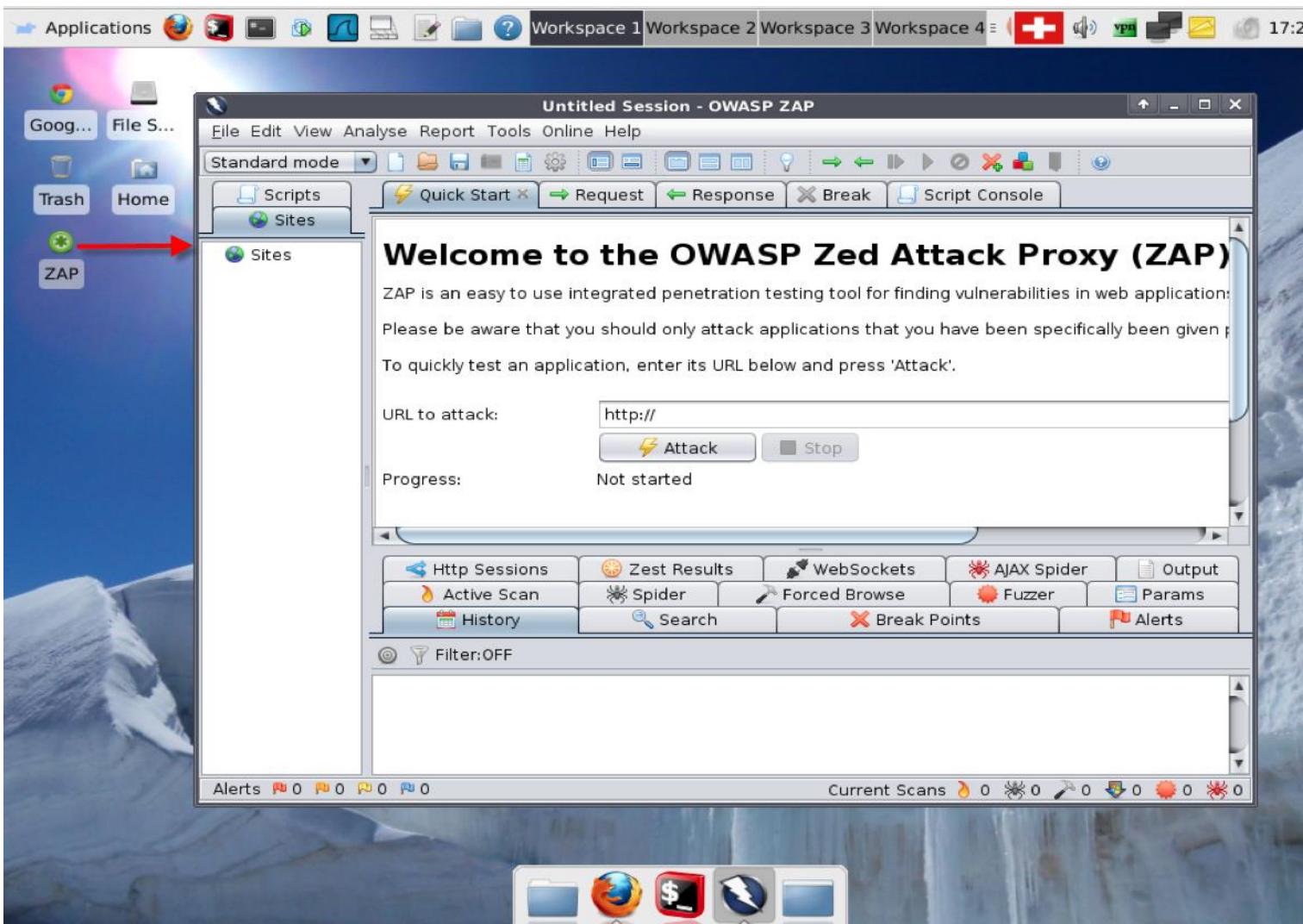
Move Up Move Down Add New Proxy Edit Selection Copy Selection Delete Selection

Please Donate Get FoxyProxy Plus Buy Proxy Service FoxyProxy for Chrome Close

max-age=2592000

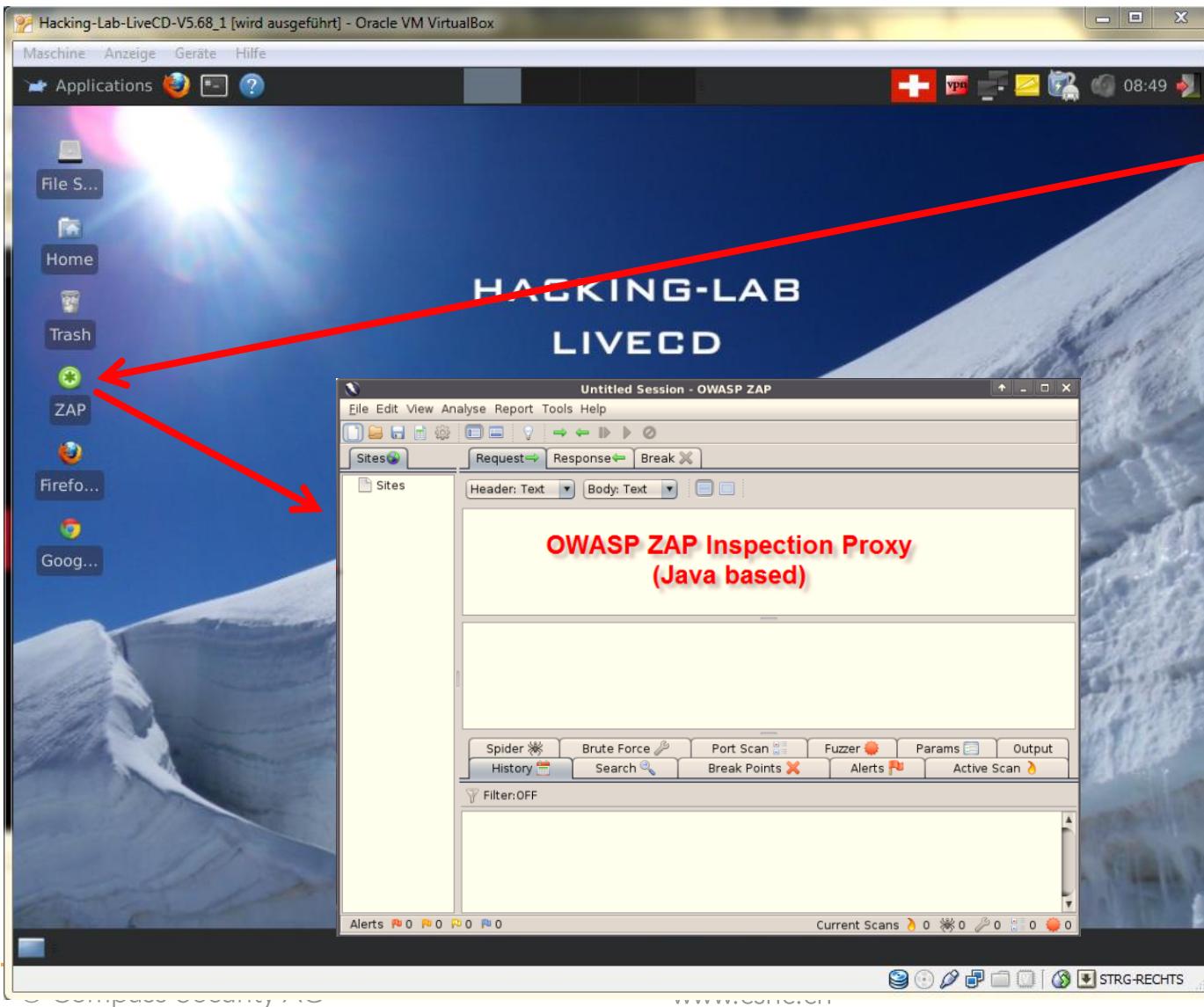


# ZAP INSPECTION PROXY (SLOW LOADING)





# 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

The screenshot shows the OWASP ZAP interface with several annotations:

- A red arrow points from the "Step Over" button in the toolbar to the "Step Into" button in the Request/Response tabs.
- A red box highlights the Request tab, and a red arrow points from the "Method" dropdown to the highlighted area.
- A red box highlights the "Trap Request (change request)" section in the main pane.

**Request Tab Content:**

```
GET http://wiki.hacking-lab.com/docs/doku.php?id=home HTTP/1.1
Host: wiki.hacking-lab.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
DNT: 1
Cookie: DokuWiki=86sv0cc8j2du7hcv8djj04iq13; __utma=138512565.2120051488.1360568983.1360568983.1360568983.1; __utmb=138512565.3.10.1360568983; __utmz=138512565.1360568983.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: keep-alive
```

**Toolbar Buttons:**

- Step Over (highlighted)
- Step Into

**Request/Response Tabs:**

- Sites
- Request (highlighted)
- Response
- Break

**Request Headers:**

- Method: GET
- Header: Text
- Body: Text

**Request Body:**

```
id=home
```

**Bottom Navigation:**

- Active Scan
- Spider
- Brute Force
- Port Scan
- Fuzzer
- Params
- Output

**History:**

Index	Type	URL	Status	Time	Notes
81	GET	http://wiki.hacking-lab.com/docs/doku.php?id=home	200 OK	199ms	Form, Hidden,...
82	GET	http://wiki.hacking-lab.com/docs/lib/plugins/indexmenu/jsmen...	200 OK	17ms	
83	GET	http://wiki.hacking-lab.com/docs/lib/plugins/indexmenu/index...	200 OK	7ms	
84	GET	http://wiki.hacking-lab.com/docs/lib/exe/css.php?s=all&t=arc...	200 OK	348ms	
87	GET	http://wiki.hacking-lab.com/docs/lib/exe/css.php?t=arctic_dark	200 OK	416ms	
86	GET	http://wiki.hacking-lab.com/docs/lib/exe/css.php?s=print&t=...	200 OK	413ms	
85	GET	http://wiki.hacking-lab.com/docs/lib/exe/js.php?edit=0&write=0	200 OK	376ms	
89	GET	http://www.google-analytics.com/ga.js	200 OK	83ms	
91	GET	https://versioncheck-bg.addons.mozilla.org/update/VersionC...	200 OK	986ms	
94	GET	http://www.google-analytics.com/ga.js	200 OK	1670ms	

**Bottom Status:**

- Alerts 0
- Current Scans 0



# MANIPULATE HTTP RESPONSES

The screenshot shows the OWASP ZAP interface with a manipulated HTTP response highlighted. The response is for the URL <http://wiki.hacking-lab.com>. The response code is HTTP/1.1 200 OK, and the date is Mon, 11 Feb 2013 08:12:29 GMT. The response body contains the HTML code for the Hacking-Lab Wiki homepage.

**Trap Response (http/s response)**

```
HTTP/1.1 200 OK
Date: Mon, 11 Feb 2013 08:12:29 GMT
Server: Apache/2.2.14 (Ubuntu)
X-Powered-By: PHP/5.3.2-1ubuntu4.18
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: DW7e884e68a840edf8b20756fc47fcf074=deleted; expires=Sun, 12-Feb-2012 08:12:28 GMT; path=/
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en"
lang="en" dir="ltr">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>
    home [Hacking-Lab LiveCD Wiki]

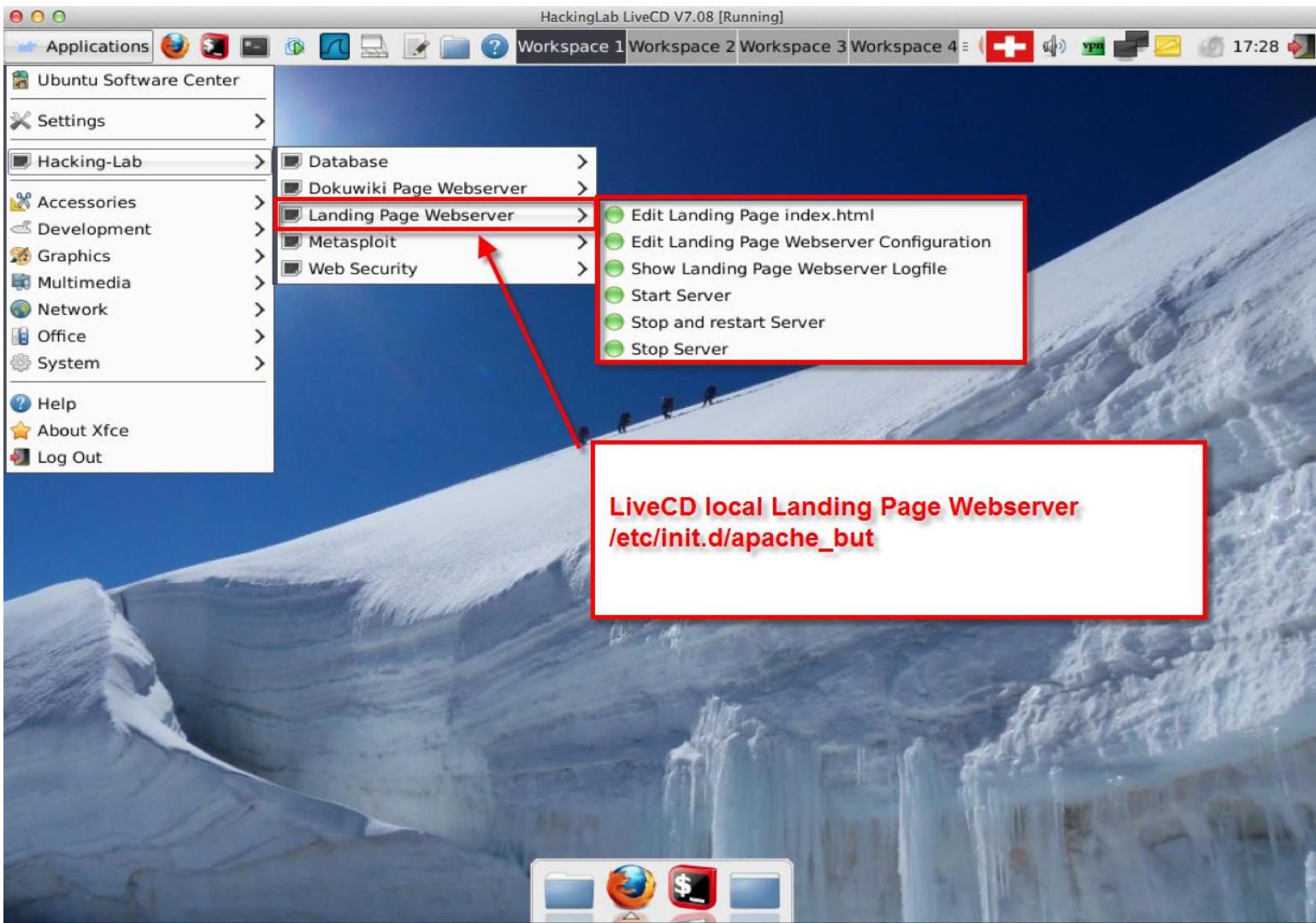
```

**Step Over** and **Step Into** buttons are highlighted with red arrows. The bottom pane shows a list of recent requests and responses.

Req ID	Type	URL	Status	Time	Notes
81	GET	http://wiki.hacking-lab.com/docs/doku.php?id=home	200 OK	199ms	Form, Hidden,...
82	GET	http://wiki.hacking-lab.com/docs/lib/plugins/indexmenu/jsmen...	200 OK	17ms	
83	GET	http://wiki.hacking-lab.com/docs/lib/plugins/indexmenu/index...	200 OK	7ms	
84	GET	http://wiki.hacking-lab.com/docs/lib/exe/css.php?s=all&t=arc...	200 OK	348ms	
87	GET	http://wiki.hacking-lab.com/docs/lib/exe/css.php?t=arctic_dark	200 OK	416ms	
86	GET	http://wiki.hacking-lab.com/docs/lib/exe/css.php?s=print&t=...	200 OK	413ms	
85	GET	http://wiki.hacking-lab.com/docs/lib/exe/js.php?edit=0&write=0	200 OK	376ms	
89	GET	http://www.google-analytics.com/ga.js	200 OK	83ms	
91	GET	https://versioncheck-bg.addons.mozilla.org/update/VersionC...	200 OK	986ms	
94	GET	http://www.csnc.ch	200 OK	1.770ms	



# LIVECD LANDING PAGE WEB SERVER





# WINDOWS XP VDI HOST

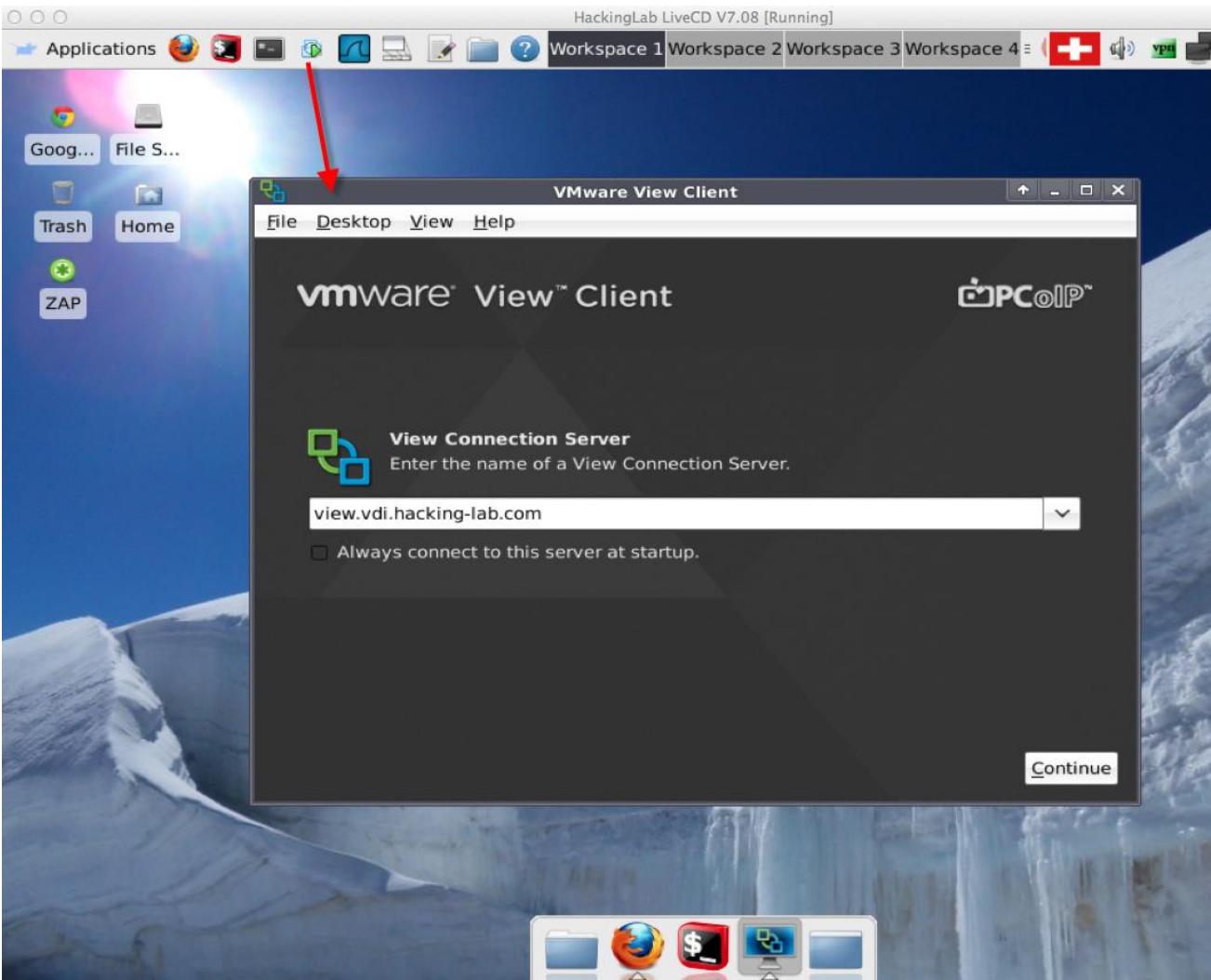


Compass Security AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

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

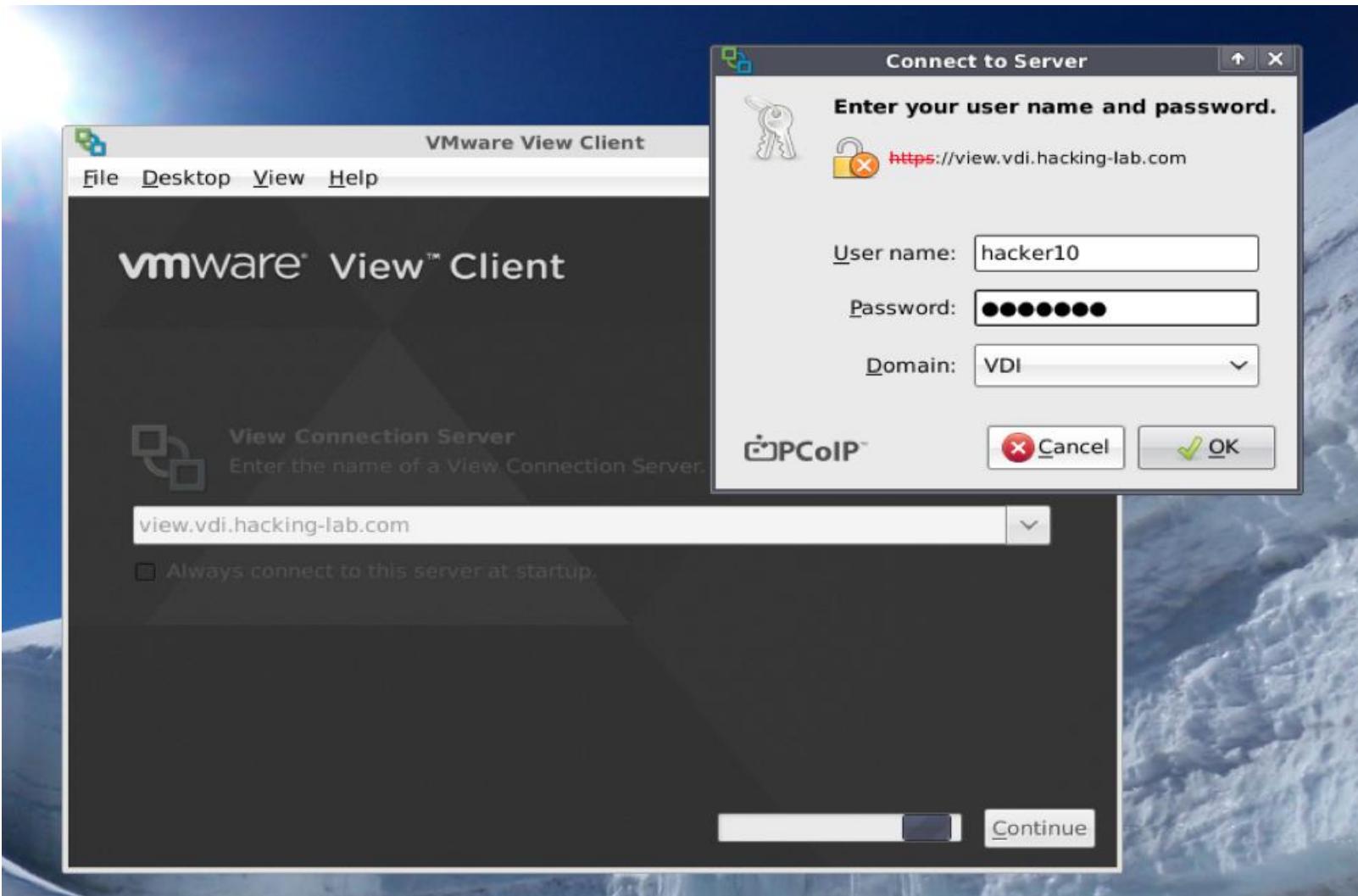


# WINDOWS XP VDI (VMWARE VIEW)



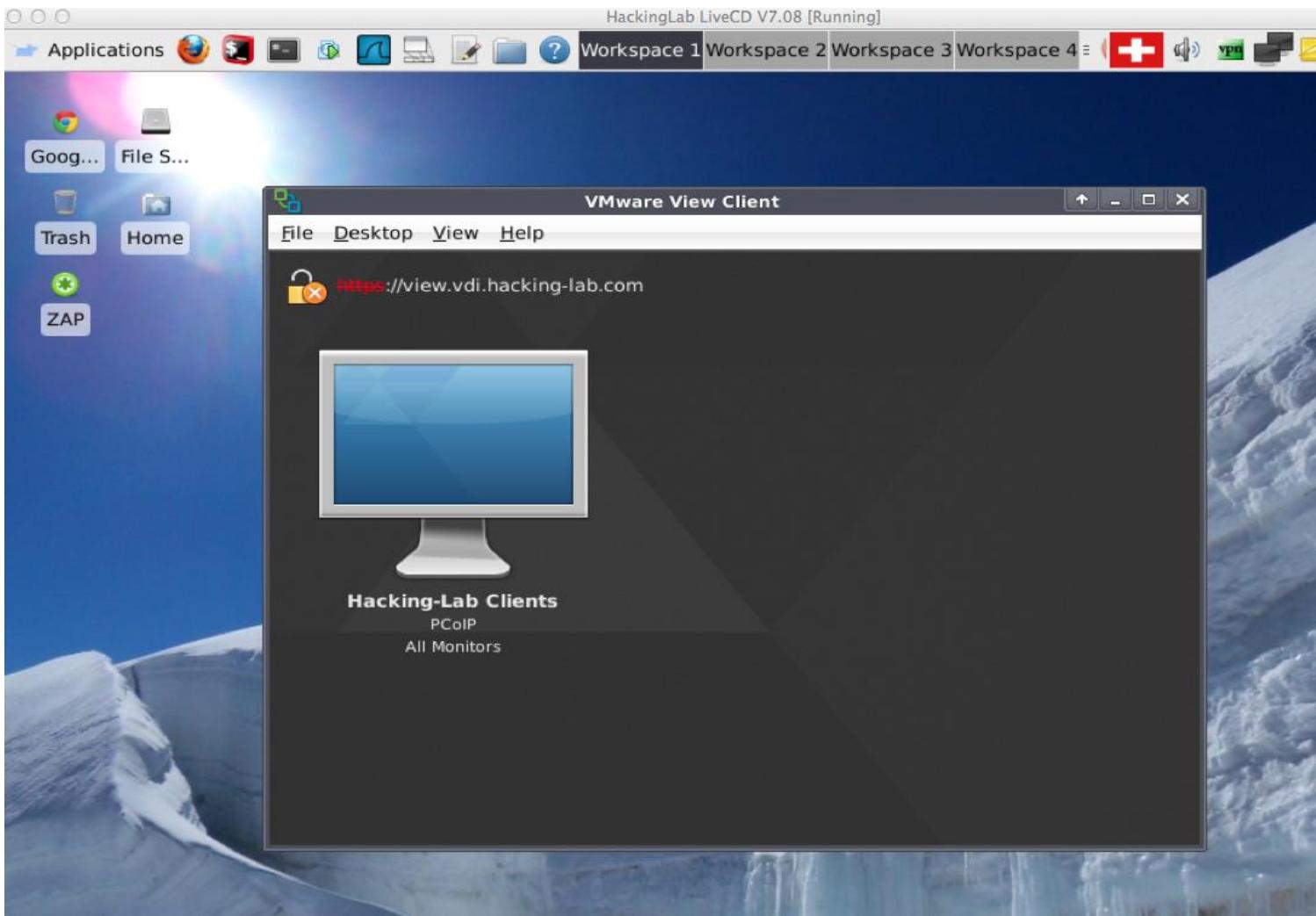


**USER = HACKER10, HACKER11,  
HACKER12,  
PASSWORD = COMPASS**



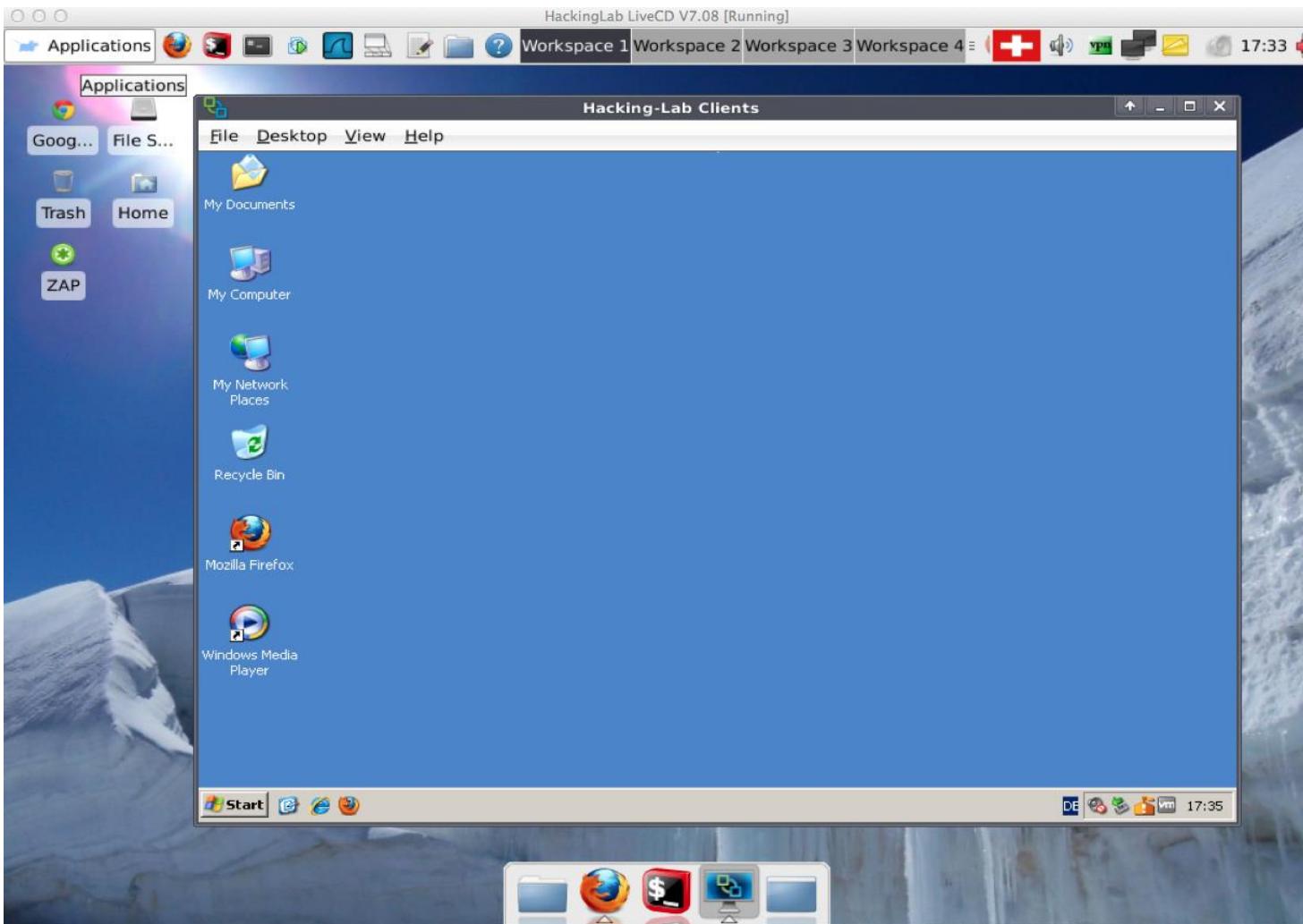


# WINDOWS XP VDI (VMWARE VIEW)





# WINDOWS XP VDI (VMWARE VIEW)





# OSX TERMINAL SERVER

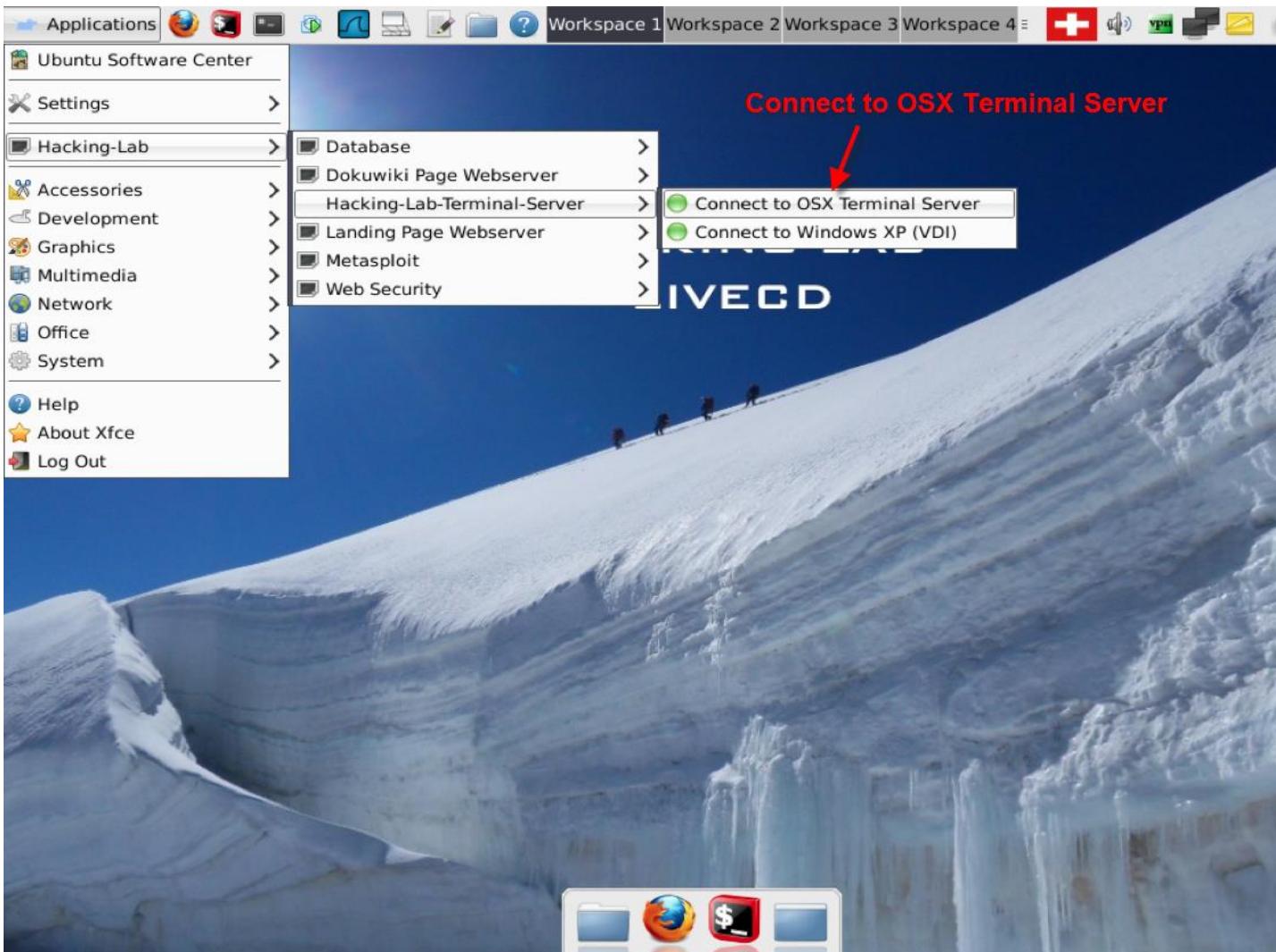


Compass Security AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

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

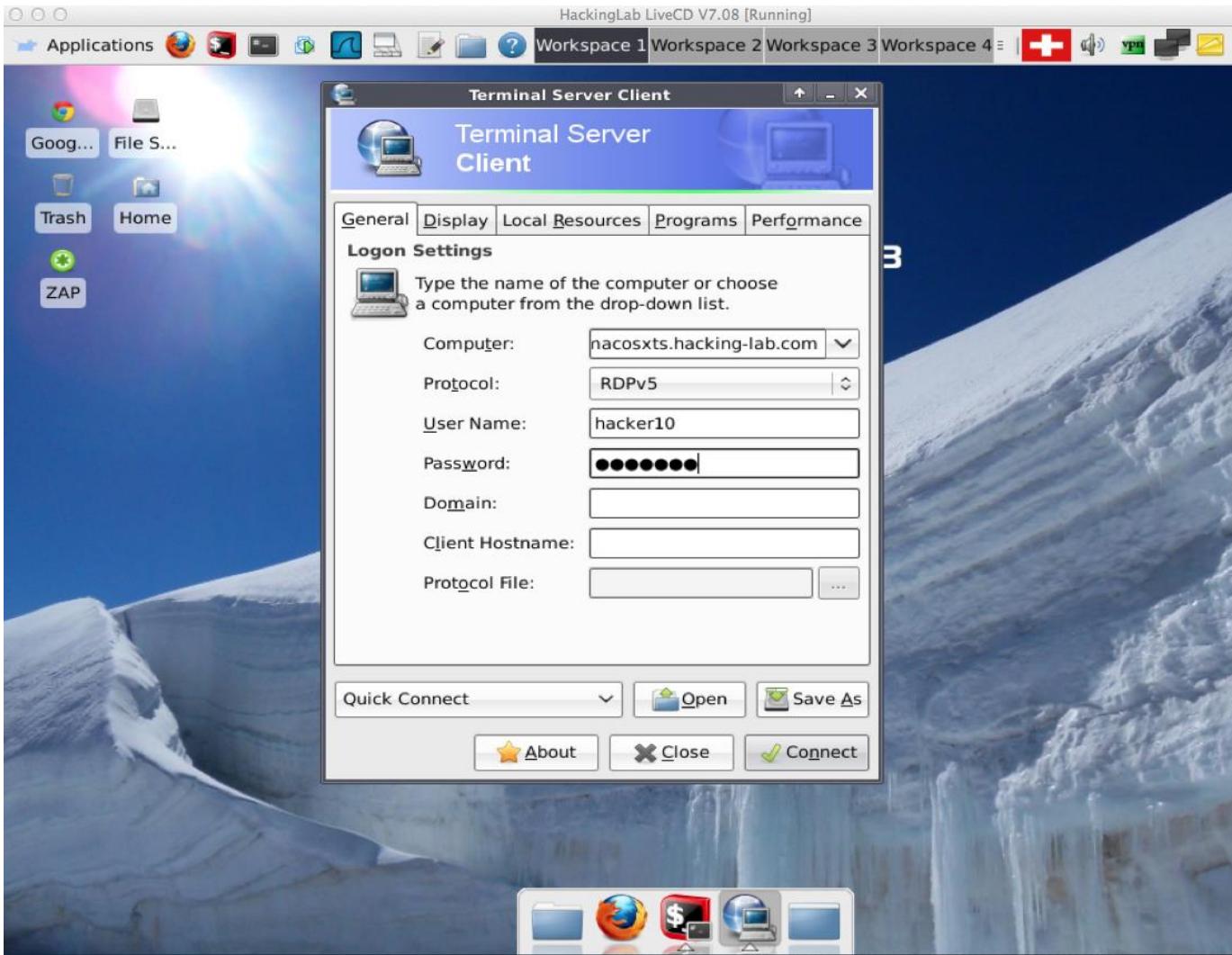


# OSX TERMINAL SERVER





# OSX TERMINAL SERVER





## DETAILS ABOUT HACKING-LAB (4/4)



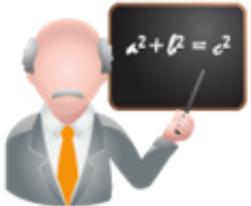
- (1) Vulnerable Servers and Applications (Web, Windows, Linux, iOS, Android)



- (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](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)



# SOLUTION GRADING AS «TEACHER»

H HACKING-LAB HOME NINA 16029 🔒 E1 📧 0 🚶 0 💬 0

**Solved Cases of Event: OWASP Top Ten**

Nick	Surname	Name	Email	Case	Status	Points	Date
super_monster	ivan	buetter	ibuetter@hsr.ch	6112 - OWASP 2010 - A2 - Cross-Site Scripting	⊕	0	2013-10-09 17:07:28
avantasia	null	null	david@adaformacion.es	6114 - OWASP 2010 - A4 – Insecure Direct Object References	⊕	0	2013-10-09 13:14:23
avantasia	null	null	david@adaformacion.es	6115 - OWASP 2010 - A5 – Cross Site Request Forgery	⊕	0	2013-10-09 12:15:00
avantasia	null	null	david@adaformacion.es	6111 - OWASP 2010 - A1 – Injection	⊕	0	2013-10-09 09:43:46
avantasia	null	null	david@adaformacion.es	6112 - OWASP 2010 - A2 - Cross-Site Scripting	⊕	0	2013-10-09 08:50:56
jagga	null	null	oxxjd@gmail.com	6119 - OWASP 2010 - A9 – Insufficient Transport Layer Protection	⊕	0	2013-10-07 17:04:02
sucounix			sucounix@gmail.com	6114 - OWASP 2010 - A4 – Insecure Direct Object References	⊕	0	2013-10-07 15:43:05
jagga	null	null	oxxjd@gmail.com	6115 - OWASP 2010 - A5 – Cross Site Request Forgery	⊕	0	2013-10-07 11:17:41
jagga	null	null	oxxjd@gmail.com	6118 - OWASP 2010 - A8 – Failure to	⊕	0	2013-10-03



**My Menu**  
Edit My Profile  
Inbox  
Organisation Manager



# SOLUTION GRADING AS «TEACHER»

The screenshot shows the 'Check Solution' page of the Hacking-Lab website. The left sidebar contains links like 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, and a My Menu section with Edit My Profile, Inbox, Organisation Manager, Question Manager, Admin, and Logout.

The main content area displays a student's solution for challenge 6112 - OWA BP 2010 - A2 - Cross-Site Scripting. The student is 'super\_monster' (ivan buettler, ibuettler@hsr.ch). The solution attachments are shown as three colored icons: green (checkmark), yellow (checkmark), and orange (info icon).

Grading options are listed:

- 1) Fully Accept (full points)
- 2) Partially Accept (partial points)
- 3) Reject (no points)

A red arrow points from the 'Attachments' section to these options. Another red arrow points from the 'Attachments' section to the 'Solution sent by the student' section, which contains the student's text message: "1) Vulnerability = foo bar  
2) Exploit = 0xff, 0xff  
3) Mitigation = John Doe  
  
Please grade my solution asap!  
  
Regards  
super\_monster".

To the right, a table shows other solutions rated by admins:

User	Rating
rt89	★★★★★
M.	★★★★★
Kori	★★★★★
johndo	★★★★★

A red arrow points from the 'Check Solution' title to the 'Rating' column in the table.



TEACHER HAS ACCESS TO «SOLUTION  
VIDEO»





# SOLUTION GRADING AS «TEACHER»

User: super\_monster  
Name: ivan buetler  
Email: ibuetler@hsr.ch  
Case: 6112 - OWASP 2010 - A2 - Cross-Site Scripting  
Teacher Solution:   
Points received: 0  
Rating

Dear super monster

Thank you for your solution. As a teacher, I will respond here to your Submission and that's how we communicate

Regards  
Your Teacher

1844  
Attachments:

### Solution History

back

Date	User	Text
2013-10-09 17:07:28	super_monster	This is my first solution.  1) Vulnerability = foo bar 2) Exploit = 0xff, 0xff 3) Mitigation = John Doe



# 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](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)



# GLOBAL CHAT

The screenshot shows the Hacking-Lab website with a focus on the Global Chat feature. On the left, there's a sidebar with links like Home, About, Volunteer, Partner & Sponsors, Events, Available Challenges, Remote Security Lab, Chat (which is selected), Wall of Fame, Scoring System, Avatar, Mobile Services, Video Tutorials, Download, FAQ, Research, and Login / Sign up. Below these links is a cartoon illustration of two stylized characters in red and blue. At the bottom of the sidebar are buttons for 'My Menu' and 'Edit My Profile'. The main area features a dark background with binary code patterns. A header bar includes the Hacking-Lab logo, the word 'HOME', a user profile for 'NINA', a user ID '16026', and a message from 'super\_monster'. A red box highlights the 'Global Chat' section. Below it, there's an 'Autoscroll' checkbox (checked). A message box contains a log of IRC chat messages:

```
[17:44:47] <sclientknight> how is everyone doing ?
[17:44:51] <sclientknight> 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> hmm 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> dfl,sdglspgk;
[06:07:14] <sagarkumar> scinent.n
[17:20:00] <pinkpather> hi
[18:42:52] <jayem1985> heelo
[18:42:57] <jayem1985> hello
[23:58:37] <ISentryll> Hi
[23:59:03] <ISentryll> anyone here?
[23:59:24] <ISentryll> 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/>

The screenshot shows the Hacking-Lab website's FAQ page. The background is a dark grey with a subtle binary code pattern. At the top left is the Hacking-Lab logo. The top right features a user profile with the name "super\_monster", 0 points, and a lock icon. Below the header, there's a navigation menu on the left and a main content area on the right.

**Hacking-Lab FAQ**

- General Hacking-Lab Questions
- OpenVPN Questions
- LiveCD Questions
- Chat Questions

**General Hacking-Lab Questions**

#	Question	Response
1	What is Hacking-Lab?	Remote Security Lab with more than 200 hands-on challenges
2	What is a challenge?	In our terminology, this is a security puzzle, a mission, a challenge
3	What is a challenge about?	Finding a vulnerability, followed by exploitation and suggesting remedy. Sending this information to the teachers of Hacking-Lab
4	What is a teacher?	This is a person evaluating the users solution. The teacher accepts or rejects a solution and gives points
5	Explain 'points' ?	Every user receives "knowledge" points. The more points you have, the better avatar you gain
6	What is an avatar?	Hacking-Lab scoring system. Beginners are 'hobos' and experts become 'root' level



# DESCRIPTION OF HACKING-LAB

- [Home](#)
- [About](#)
- [Volunteer](#)
- [Partner & Sponsors](#)
- [Events](#)
- [Available Challenges](#)
- [Remote Security Lab](#)
- [FREE OWASP TOP 10](#)
- [Topology](#)
- [Revert to Snapshot](#)
- [LiveCD](#)
- [OpenVPN](#)
- [Reference](#)
- [Vmware View VDI](#)
- [Chat](#)
- [Wall of Fame](#)
- [Scoring System](#)
- [Avatar](#)
- [Mobile Services](#)
- [Video Tutorials](#)
- [Download](#)
- [FAQ](#)
- [Research](#)
- [Login / Sign up](#)

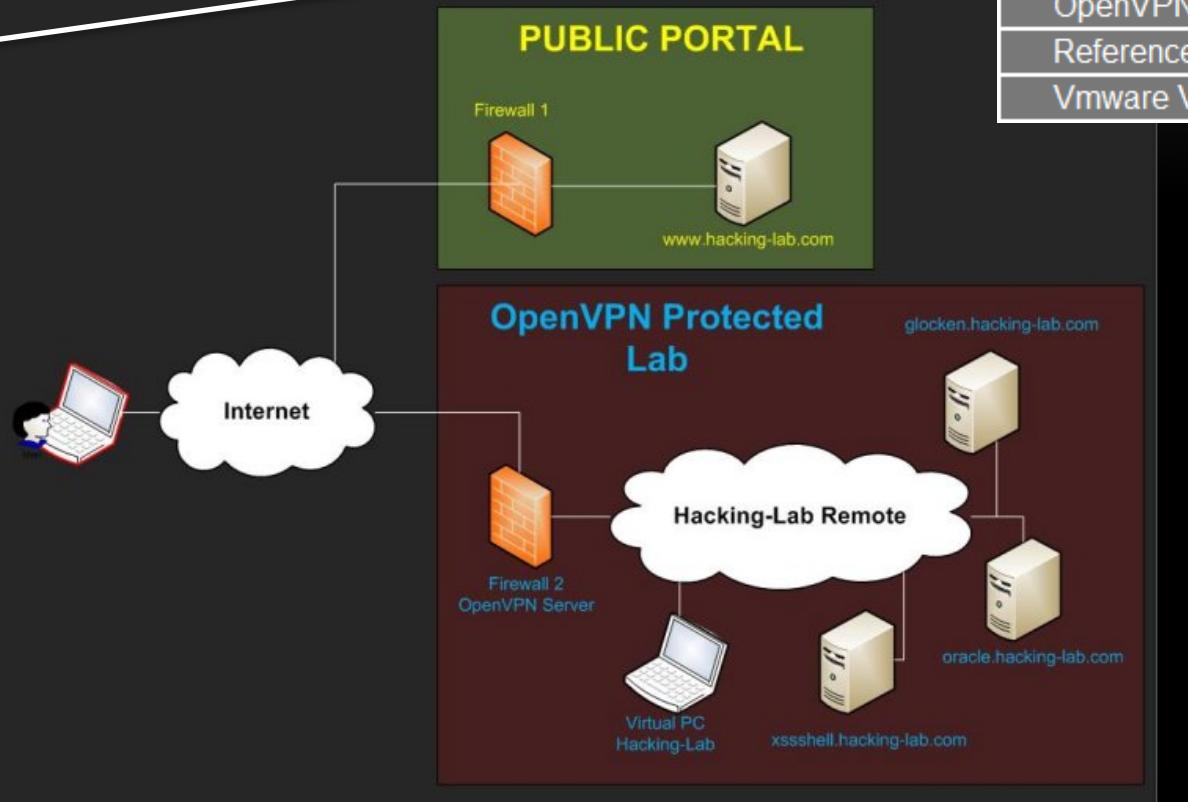


- [My Menu](#)
- [Edit My Profile](#)
- [Inbox](#)
- [Organisation Manager](#)
- [Question Manager](#)
- [Logout](#)

## Remote Security Lab

### Hacking-Lab Infrastructure / Topology

The picture below introduces our lab infrastructure. [www.hacking-lab.com](http://www.hacking-lab.com) is public! The lab is **OpenVPN protected**.



- [Remote Security Lab](#)
- [FREE OWASP TOP 10](#)
- [Topology](#)
- [Revert to Snapshot](#)
- [LiveCD](#)
- [OpenVPN](#)
- [Reference](#)
- [Vmware View VDI](#)



# 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!