HACKING-LAB

Hacking-Lab Magazine
Issue 01-2012

Remote Security Lab - Hack & Learn - Train your Brain

Hacking-Lab
Remote Security Lab
Hack & Learn
www.hacking-lab.com

Editorial

National Cyber Defense Strategies around the world consider well trained employees as an important key factor. In-depth knowledge derives from theory and practical skills. This is the core competence of Hacking-Lab - bringing talents and tutors around the globe together! Hack&Learn!

From: Ivan Bütler / E1

Back in 2006, while preparing the first Swiss Cyber Storm Security conference, the idea of a remote security lab was born. An idea that wasn't a success from the beginning - because the lab was purely focussed in providing a large set of vulnerable applications without having interaction with the trainee.

How do you train your staff without communication? This is a weird question, but we have learned just downloading a vulnerable Vmware image providing security challenges is not sufficient.

Back in 2009, we have decided to glue the already existing comprehensive lab together with a student and teacher interface. Hacking-Lab was born!

Eventually in 2011, Hacking-Lab was enriched with more features for students, teachers and organizations. Today several entities (Industry, OWASP, Universities) are using Hacking-Lab as a platform to teach their members or staff and to improve resistance against cyber threats. Today, the Hacking-Lab community is growing, because of its unique approach of providing its remote security lab. Luck we have with our volunteers, the number of challenges, the quality of puzzles is being increased day by day.

Future Development

In March 2012, we have bought a nice (but expensive) ESXi virtualization hardware that is currently setup and planned to become our new Vmware View VDI host. One of the drawbacks of Hacking-Lab, most cases are Linux and Open Source based. But in the real world, Microsoft Windows plays a major role. Using Vmware VDI solution will fill the gap, especially when it comes to client security aspects (Virus, Trojan, Malware, OllyDbg).

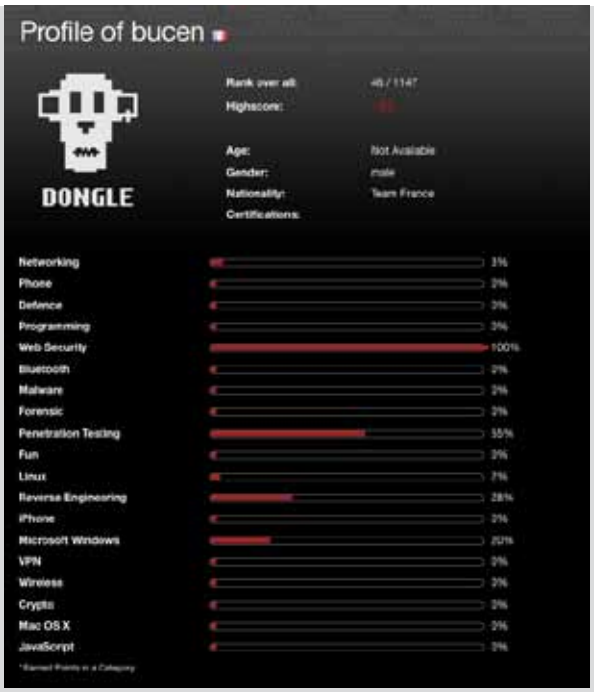
Thank you for your great support and feedback.

Have a safe day!
E1

Ivan Bütler, E1, CTO Hacking-Lab

After his studies in 1996, Ivan used to work for a Swiss bank as Unix and VMS administrator. At this time, the tool „SATAN - System Administration Tool for Analyzing Network" and PGP from Phil Zimmermann was released. As security became his major interest, he decided to move to r3 security engineering AG, a Swiss crypto firm rewarded for their 128 bit encryption software. This was at a time when 128 bit encryption was banned by the US export restrictions and only 56 bit encryption was availble in Europe. Later, when r3 security engineering was bought by Entrust Technologies, Ivan open his own business, together with his fellow Walter Sprenger.

Ivan is still working for Compass Security AG, a Swiss ethical hacking and penetration testing firm. He talked at Blackhat Las Vegas, IT Underground Warsaw, OWASP AppSec US in Washington and several other international conferences.



Nicolas Hochart / Volunteer

From: Nicolas Hochart

I'm French, 37 and I have around 12 years of experience in networks and IT security. I worked until last June in an IT infrastructure team for an international company in France. Our team defined, managed and supported some global network, system and security solutions (LAN/WAN, VPN, AD, mail, IPS, WAF, DMZ ...) I moved last summer for personal reasons to Helsinki (Finland).

How I met Hacking-Lab?

I remember that a year ago I searched for websites with hacking challenges. I think it's a good way to practice pentest in an ethical manner.

When I found hacking-lab.com website, I was impressed by the quality of events, specially the „Swiss Cyber Storm 3 CarGame Challenge" where I waited impatiently the beginning of the month that a new challenge was online for 30 days.

Today, I continue to enjoy trying to pass the different HL events (owasp top ten, xmas hacking...)

Why I work as Volunteer

In the 2011 HL October newsletter I saw that hacking-lab.com was searching for volunteers. I got interested right away, replied to the call and now I've worked as a volunteer since then. This way I have the chance to discover new challenges that are not public on HL website and earn CPEs for my CISSP certification.

I'm sure that the work I'm doing at the moment is an experience that companies could find interesting for a future job. But the most important thing is that I'm able to expand my skills in IT security and learn something new every day.

I'm relatively new in penetration testing and joining as a volunteer an organization focusing on information system security like hacking-lab.com is a very good thing.

I WANT TO EXPAND MY SKILLS IN IT SECURITY

What projects I did

I started to produce Hackademics Videos in Hacking-Lab with Camtasia software. It's a tool easy to use, but doing video solutions very clear and understandable is another thing. Since the beginning of the year, I started Hacking-Lab challenge development. I adapt webgoat project for hacking lab platform. With this project, I put hands on java and tomcat j2ee server. I've done as well HL challenge descriptions (html pages) and HL solution documentation (html pages).

Nicolas (CISSP, OSCP)

Free OWASP TOP 10 Challenges

Since 2011, Hacking-Lab provides free OWASP TOP 10 challenges. Profit from both, OWASP and Hacking-Lab and increase your skill level.

From: Martin Knobloch

Since AppSec USA 2011, OWASP and Hacking-Lab have a joint educational project. Lower levels of performance can normally be taught using the more passive learning methods where higher levels of performance usually require some sort of action or involvement by the learners . Real hands-on experience makes the difference, that's why OWASP has decided to go this route.

OWASP Academy Portal

Since its start with AppSec US in Minneapolis 2011, more than 1072 individuals have assigned to the free OWASP TOP 10 challenges. In the mean time, the portal has more than 6000 active users.

OWASP Scoring

Currently, the user with the nickname „bashrc" is leading the scoring of the OWASP TOP 10 event. Within the last couple of months, 167 users have successfully solved the OWASP challenges.

OWASP GEC team is checking submitted solutions day and night. Luck we have with Martin Knobloch, Cecil Su, Steven van der Baan and Zaki Akhmad, the community derives great support from these OWASP members.

XXE and Apache Struts2

OWASP and Hacking-Lab are working close together for providing best and latest security challenges. In March 2012, the Apache Struts2 challenge was release, where the XML external entity attack challenges will be release soon.

Rank	Score	Type	Name
1.	140		bashrc
2.	130		Zy0d0x
3.	130		PS
4.	130		kamil
5.	130		gold50china
6.	130		nsiskov
7.	130		Spassbremse
8.	125		SgtDDog
9.	120		hackingmtl
10.	120		scegliau
11.	120		jorang
12.	120		solozero
13.	120		seimen
14.	110		tht
15.	110		pgn
16.	103		analfa
17.	100		dreadknight
18.	90		bucen
19.	90		_dev_null
20.	80		nu11_nu11
21.	80		0xquad
22.	80		paulo
23.	70		dishix
24.	63		n00b0rc
25.	60		aimfeld

Martin - OWASP GEC chair

OWASP SUMMIT 2011 LISBON PORTUGAL FEB 8-11

The Hacking-Lab project was presented at the OWASP Summit 2011 in Lisbon. Since then, Hacking-Lab provides the free OWASP TOP 10 training.

Martin Knobloch, OWASP Global Education Committee Leader

OWASP Online Competition

Moreover, OWASP is planning to add more additional challenges into the Hacking-Lab infrastructure. Thanks to the Greece Hackademics project, additional challenges are now ready to be used for the planned OWASP online security competition 2012. The winner will receive a free ticket to one of the OWASP international conferences.

WebGoat Integration

Luck we have with our volunteers, WebGoat has been integrated into the Hacking-Lab framework during the last couple of weeks. Thanks to Nicolas Hochart from Helsinki, the major work is done and we are in the quality assurance process before making them public. Thus, with the Hackademics and the WebGoat project, we will have more than 20 new and free challenges available for your hands-on experience.

SAML Security Analysis (Page1/4)

Security Assertion Markup Language (SAML) is an XML-based open standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee.

From: Thomas Risch

This article gives a short introduction into a typical use case of SAML in a corporate environment. It shows how such a setup could be attacked and how it can be security reviewed to ensure a certain minimal level of security on the service provider side.

The tool „Samlsnort" is introduced that provides an easy-to-use interface for testing SAML.

The article is not a complete write-up. It describes one attack vector. Many details of the SAML protocol are not mentioned and many security relevant considerations around SAML are not within scope.

Signature

Within the Signature attribute, the SignatureValue attribute contains the value of the signature of the assertion, eg:

```
<SignatureValue>QGLnrnn4O+xtF1SQQDksI065yOb1GZ0Tl3OVO9TTxR+vsK5HNjR3Ot+z9jB9HagvxuXqixFr6Ay
TpGHP3zcM12PEOmAKgxpZrBQlu3fKYOryTIiiS8hFezVbjyoCLvhcdpqUp+ts7fCkDqbNMBK+V4mwtFR8veG7Hg/ZXa
DiMdg62n7oe5LiUlmf/TM02dnPZyqYzcYjycFWKKIjnRi4KrJiuIXA8/qMlcRCbXvP6i6ew1wbkH13s3Cy6yMhaSVC7
6hYf8fT+nqwZHAdBXAoJxr0hJZ/2Hp2zRBzxowco462XW9967FCuOTktO7JxtL+A2n+m2cXAmSUmYLQMHewg==
</SignatureValue>
```

The signature is produced by the IdP that generates the assertion with use of the IdP's private key. The signature can be verified by any service provider with the public key of the IdP.

Attacking SAML2 Serv. Provider

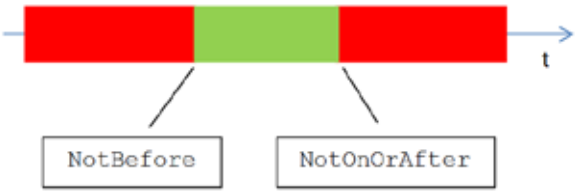
SAML is a protocol that can be used to set up Single Sign-on (SSO) between corporations. See the picture below how SAML is commonly used.

NotBefore and NotOnOrAfter

The NotBefore and the NotOnOrAfter attributes are used to determine the validity period of the assertion. They are set by the IdP when the assertion is generated.

Trust Establishment

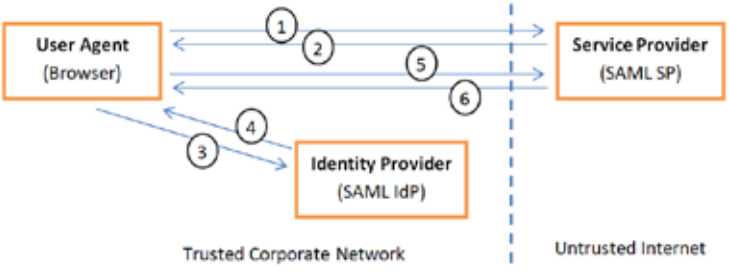
Nevertheless the SP has to complete certain validations in order to proof that the assertion is valid and trustworthy. These validations are based on certain attributes of an assertion. The following specific attributes are of interest in this security write-up



Standard Use-Case with SAML2 Service Provider

1. User requests URL at SP
2. SP requires a valid SAML Assertion
3. User requests SAML Assertion at IdP
4. IdP provides user with Assertion
5. User presents Assertion to SP
6. SP returns URL

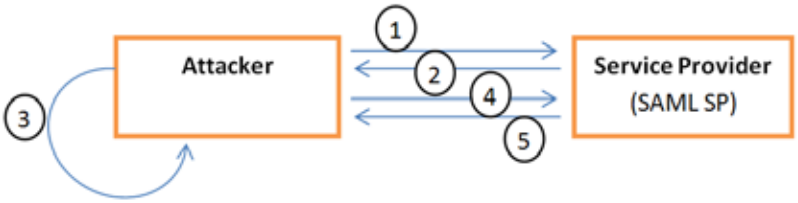
standard use case for SAML



SAML Security Analysis (Page 2/4)

Attack Scenario 1: Fake Assertion

1. Attacker requests URL at SP
2. SP requires a valid SAML Assertion
3. Attacker generates its own, fake SAML Assertion
4. Attacker presents Assertion to SP
5. SP returns URL

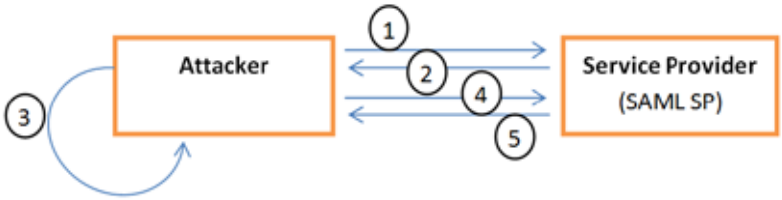


The vulnerability that leads to this scenario is between step 4 and step 5. The service provider should determine the integrity of the assertion by validating the signature of the assertion. He does so with the public key of the IdP he expects assertions from. The attacker can only provide assertions that are signed with the wrong key or assertions that are not signed at all .

Attack Scenario 2: Replay Assertion

1. Attacker requests URL at SP
2. SP requires a valid SAML Assertion
3. Attacker takes a SAML Assertion he has gotten in advance
4. Attacker presents Assertion to SP
5. SP returns URL

Prerequisite to this scenario is that the attacker has a assertion that was valid at a certain point in time. He could get it either by network sniffing, by analyzing traffic on the victim's end user system or by saving it off while he is allowed to access the SP (eg. shortly before he is leaving the company).
Again between step 4 and 5, an important step is missing. The service provider this time validates the integrity of the assertion and detects that it is correct. But the SP does not analyze the timing attributes (NotBefore and more important NotOnOrAfter). Therefore, even though the IdP has specified a short lifespan for the assertion (typically some minutes) the SP accepts them regardless of age .



About Thomas Risch

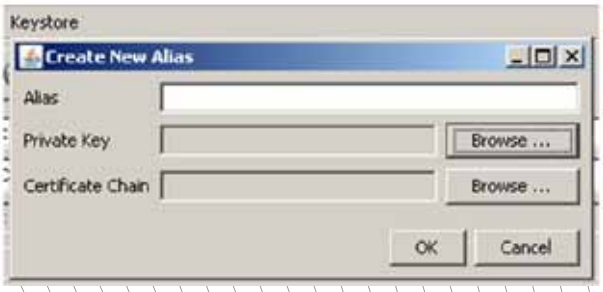
Thomas went into the callenges of Information Security in 1998 at a Swiss Bank, after working some years as software developer. In his current position within Swiss Re, he is responsible for conducting risk assessments and security reviews. He has a broad range of topics on his plate, ranging from web applications to ERP systems.

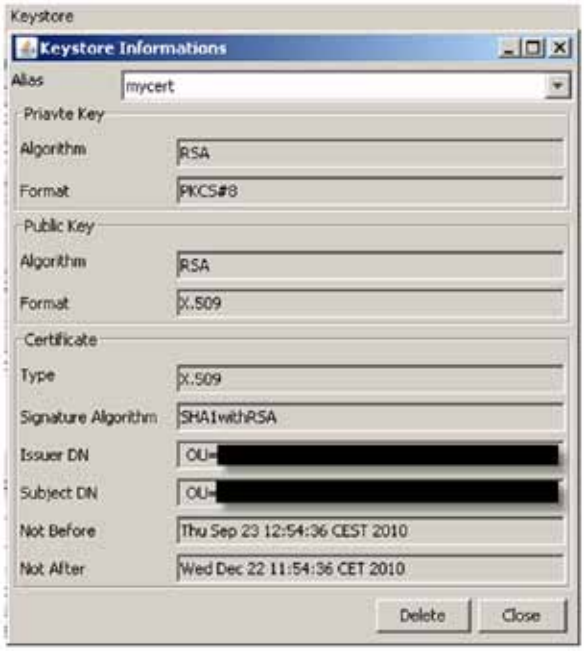
SAML Security Analysis (Page 3/4)

Testing Tutorial

In all the above scenarios, a company outsources data to an application outside of its control. Nevertheless it does not outsource the responsibility for keeping the data secure. Therefore, at least some basic checks should be performed in advance to the outsourcing. During a pentest, SAML assertions could be recorded and replayed manually, eg. using a locally installed proxy like OWASP's ZAP or Portswigger's Burp.

Furthermore, the Samlsnort tool provides a simple GUI for this kind of testing. The following part of the document describes how to test for the attack scenarios mentioned.





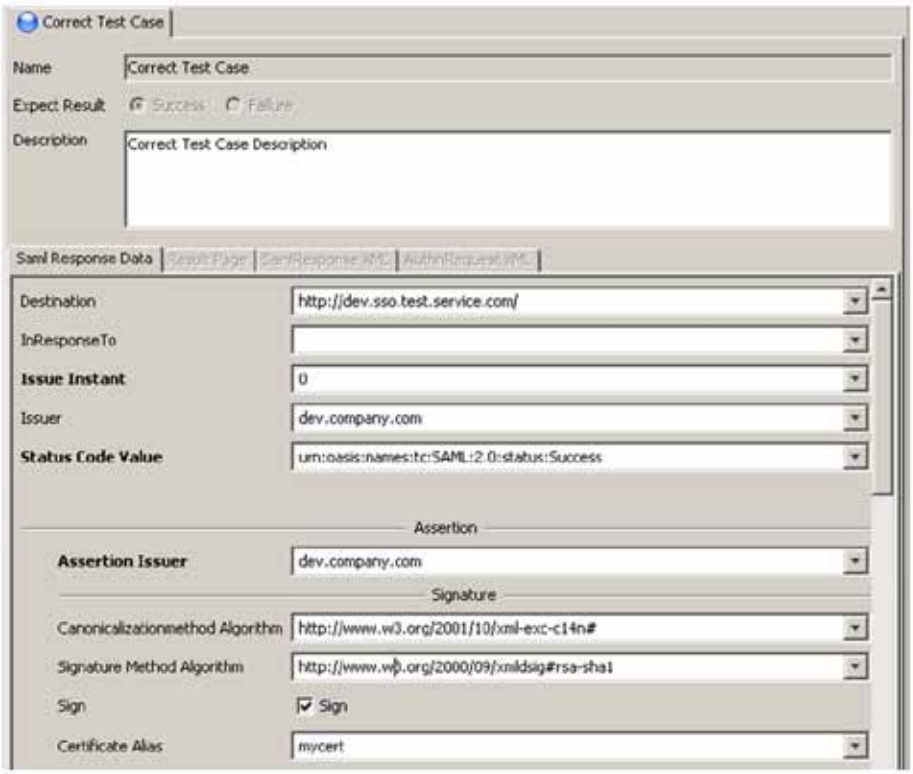
Step1: Preparation

In order to test for SAML assertion that should not be consumed by the SP, we first need to craft an assertion that is properly accepted. In order to sign the assertion, Samlsnort must be aware of the private key of the IdP. It can be imported from a given DER file.

Always use the key of your test infrastructure when playing around with this, never use the productive key! From this point on, the Samlsnort tool is able to act as an IdP and creates valid assertions if provided with correct parameters.

Step2: Generate a valid assertion „Correct Test Case“

This step is the most challenging while testing saml security. Usually if you set up the connection from the IdP to the SP, you are aware of the required attributes. The tool provides you with some options to choose from.



Save the test suite and run it. After a successful run, the bullet on the tab turn green, and the result page tab will show the expected web site.

SAML Security Analysis (Page 4/4)

Step 3: Generate invalid assertions

You can copy the valid test case with Ctrl-T (Test Case – Add Test Case), so all relevant attributes are preserved. Then start manipulate the attributes.

Suggested manipulations to test the attack scenarios outlined above:

- Remove signature
- Sign with wrong certificate
- Change NotBefore and NotOnOrAfter attributes

For example generating an assertion that is not valid anymore can be achieved by setting both NotBefore and NotOnOrAfter to a value in the past.

This will generate the following assertion, it can be seein tn the SamlResponse XML tab:

```
<saml2:Subject>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">Testuser_002@company.com</saml2:NameID>
  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml2:SubjectConfirmationData NotBefore="2011-12-28T14:21:48.390Z" NotOnOrAfter="2011-12-28T14:31:48.390Z" Recipie
  </saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2011-12-28T14:21:48.390Z" NotOnOrAfter="2011-12-28T14:31:48.390Z">
  <saml2:AudienceRestriction>
    <saml2:Audience>http://dev.sso.test.service.com/</saml2:Audience>
  </saml2:AudienceRestriction>
</saml2:Conditions>
<saml2:AuthnStatement AuthnInstant="2011-12-28T14:41:48.390Z" SessionIndex="_53dc6643e41b6dfbadb6e2f73c06bffd">
  <saml2:AuthnContext>
    <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
```

Note that the timestamps for NotBefore and NotOnOrAfter are in the past, relatively to the time the assertion has been generated and sent (see AuthnInstant). Such an assertion should not be accepted by the SP.

Summary and Outlook

Some specific attacks to SAML setups in a corporate environment were introduced. The attacks are based on configuration mistakes or extremely sloppy programming style on the SP's side. Experience shows that with relatively low effort and skills on SP side, but a good SP software, these mistakes are easy to circumvent and correct SP configuration is possible. Nevertheless surprisingly many companies reinvent the wheel and build their own SP software. Such setups are prone to programming errors, configuration mistakes or developers misinterpreting the SAML standard.

The introduced attack scenarios and testing procedures could be enhanced, e.g. with fuzzing techniques, to find vulnerabilities in commercial SAML SP's or the used XML parsers therein. This exceeds the normal corporate scope, since it is rather unlikely that the IdP used by the company generates malformed SAML assertions.
The security of the corporate setup finally depends on the protection of the IdP's private key. If an attacker gets access to the private key, the whole system must be seen as compromised.

References

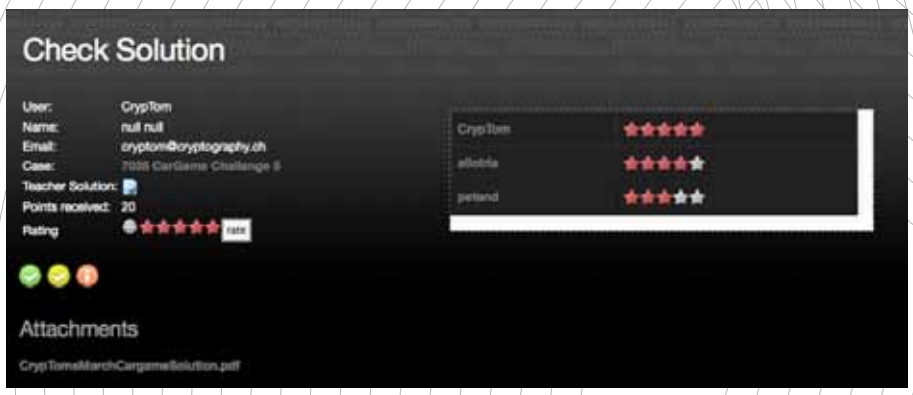
1. SAML 2.0. Wikipedia. [Online] [Zitat vom: 27. 12 2011.] http://en.wikipedia.org/wiki/SAML_2.0.
2. Security Assertion Markup Language (SAML) 2.0. OASIS Open Standards. [Online] [Zitat vom: 27. December 2011.] http://www.oasis-open.org/standards#samlv2.0.
3. OWASP Zed Attack Proxy Project. OWASP - The Open Web Application Security Project. [Online] [Zitat vom: 28. 12 2011.] https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project.
4. Burp Proxy. Portswigger Web Security. [Online] [Zitat vom: 28. 12 2011.] http://portswigger.net/burp/proxy.html.
5. Samlsnort Wiki Home. Sourceforge. [Online] [Zitat vom: 28. 12 2011.] http://sourceforge.net/p/samlsnort/wiki/Home/.

Outlook Features

What is planned for the future?

Solution Rating

Teachers will be able to rate the user solutions. It is the idea that we will disclose these solutions to users who have successfully solved the same challenge. This way, you can learn alterantive routes how to solve a puzzle and increase your skill.



Online Certification

We are working on a certification program in Hacking-Lab. The exam will be a combination of multiple-choice questions and online hands-on challenges. Every user will get a certificate if he or she passes the exam. Passing a remote exam will result in a SILVER CERTIFICATE

If you are attending an on-site exam (Partner University), you can then get your GOLD CERTIFICATE.

Vmware View Infrastructure

Hacking-Lab is setup a Vmware View based VDI solution. Using the vmware view client which is already preinstalled on our latest LiveCD, you will connect to the next free Microsoft Windows RDP host for the sake of Microsoft challenges. We are planning to have 20 workstations up and running.

The VDI solution shall spice up Hacking-Lab with

1) CryptTool usage
2) Cain&Abel
3) Windows Forensics
4) Alternative Data Streams
5) Shatter Attack

We are sure, this will level up the power of Hacking-Lab.

Outlook Events

What is planned for the future?

OWASP AppSec EU 2012

Hacking-Lab is futher collaborating with OWASP! We will provide the educational lab environment for the University Challenges in Athen.

Swiss Cyber Storm 4 - 2013

Swiss Cyber Storm is an awesome international IT security conference with all, lecturing and tutorial lessons including geek style CTF challenges. Speakers from all around the globe have been talking about new attack methods and defense strategies. SCS4 will be held in Zürich, downtown Switzerland.

We are proud to provide the CTF and hacking challenge infrastructure.