

HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

SQL INJECTION

http://www

CYBERWAR: DEFENDING A COUNTRY

PRACTICAL CLIENT SIDE ATTACKS

INTERVIEW WITH GORD BOYCE

Vol.7 No.01
Issue 01/2012(49) ISSN: 1733-7186

PLUS

**TOOL TIME: SECURE YOUR DNS
(IL)LEGAL: WHY CAN'T ONLINE BANKING
BE LIKE FACEBOOK?**





It's here! Penetration testing for Students



Click here
To enter the
early bird list



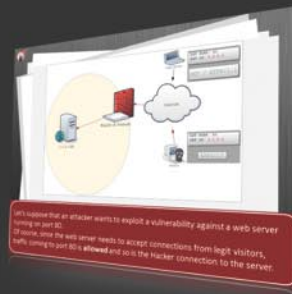
80% of beginners remain beginners or give up completely

We know the pain of being a beginner.

You either don't have the foundational skills or you don't have a clear path to follow. Don't give up. There is a better way. Our course will teach you basics of networks and web apps.

It's not just about 1337 instructors

Expert teachers hardly remember what took them to the expert status. It's a fact. There is no way to effectively teach beginners other than help them building strong foundations and showing them the correct path.



You can do it

If you keep studying without a clear learning path you are probably wasting time. Secret is path and perseverance. Better a single step in the correct direction than 10 random steps. Our course will save you months of struggling and frustrations.

You gotta see this.

www.elearnsecurity.com



Still hacking virtual machines?



Coliseum Lab is here!

The most epic web app hacking lab
you have ever seen

CLICK HERE

14 educational challenges
in a multi-platform
environment.

Epic!

www.coliseumlab.com



HAKIN9 team

Editor in Chief: Grzegorz Tabaka
grzegorz.tabaka@hakin9.org

Managing Editor: Marta Jabłońska
marta.jablonska@hakin9.org

Editorial Advisory Board: Julian Evans, Aby Rao, Julio Gómez Ortega, Leonardo Neves Bernardo, Gautam, Roland Koch and Steffen Wendzel

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Proofreaders: Bob Folden, Nick Malecky

Top Betatesters: Nick Baronian, John Webb, Ivan Burke

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.


Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@software.com.pl

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.
All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them.
To create graphs and diagrams we used smartdraw.com program by  SmartDraw

Mathematical formulas created by Design Science MathType™

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Readers,

Welcome in 2012! I hope you are well and you had great time. It's the first issue this year I hope you will like it. First article „Practical Client Side Attacks” is written by Julio Gómez Ortega.

In a penetration test, it is common not to pay attention to web vulnerabilities like XSS or XSRF. This is because people usually think about an alert message when speaking about XSS. The reality is that the client side web vulnerabilities can be a powerful way to access forbidden resources and information. You will learn how to take advantage of a XSS in a penetration test, different client side attack vectors and solutions to these vulnerabilities.

Next article is written by our long contributor Leonardo Neves Bernardo.

This article will discuss how to install OpenSSH and increase the level of security using asymmetric key authentication. We will see how to centralize user authentication by using an LDAP server for retrieving public keys instead of `~/.ssh/authorized_keys`. Finally, there are some security tips that are very important to obtain a good level of security using OpenSSH.

Since the mid-twentieth century to our time, information technology has rapidly evolved. From ENIAC-1, with its' huge size by today's standards to the desktop with next-generation quad-core processors, only fifty years have passed. More information you will find in „Cyberwar: Defending a Country”.

Read also two parts of Social Network Security article by Roland Koch and Steffen Wendzel. Social networking platforms such as Facebook or XING aim on collecting huge amounts of personal information about their users. In this first of two articles, we will highlight the risks linked to such social networking sites while the next article will focus on the protection methods which can be applied for enterprises and private users.

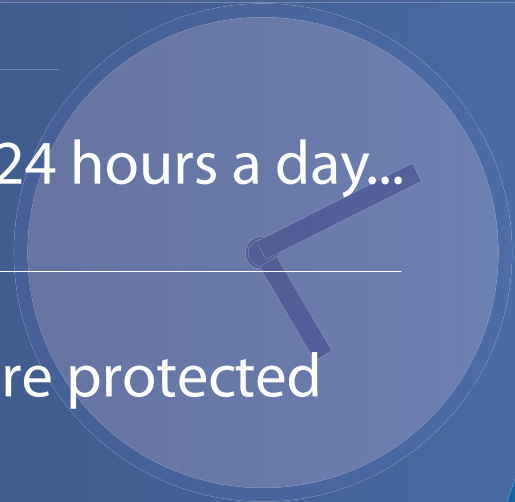
Want to learn what is SQL Injection, different types of SQL Injection and how to protect from SQL Injection? Have a look at “The Most Dangerous Attack Of Them All” by Gautam.

We also recommend our columns, (IL)Legal and Tool Time.
At the end you can find an interview with Gord Boyce.

We wish you good reading!
Marta & Hakin9 Team

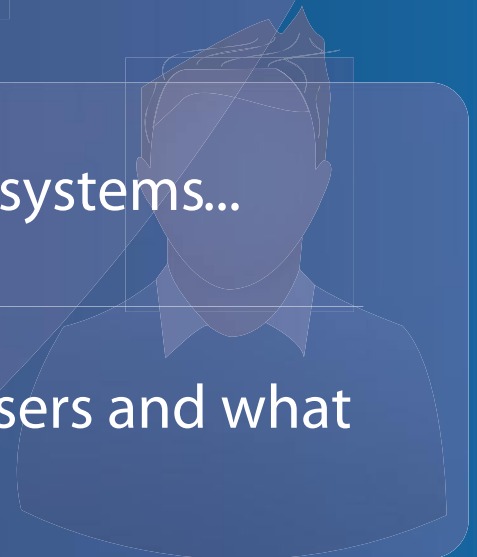
Be reactive...

- Your systems are being attacked 24 hours a day...
- You understand the threats and are protected against them...



Be proactive...

- My users' behaviour threatens our systems...
- I understand what motivates my users and what threats are coming my way...



ID Theft Protect provides information on threats from a user perspective.

IN BRIEF

08 Latest News From IT Security World

By Schuyler Dorsey, eLearnSecurity and ID Theft Protect

As usual specialists from companies eLearn Security and ID Theft protect will share with us latest news from IT security world. Read it to up-date yourself.

BASICS

10 Practical Client Side Attacks

By Julio Gómez Ortega

In a penetration test, it is common not to pay attention to web vulnerabilities like XSS or XSRF. This is because people usually think about an alert message when speaking about XSS. The reality is that the client side web vulnerabilities can be a powerful way to access forbidden resources and information. You will learn how to take advantage of a XSS in a penetration test, different client side attack vectors and solutions to these vulnerabilities. One of the most interesting attacks which is possible to do through a XSS is Session Hijacking. It allows to impersonate a user by stealing his cookie session. After that, the attacker will have to change his own cookie for the stolen one.

The tool Shell of the Future (sof) makes all these steps easy once you have successfully exploited a Cross Site Scripting. That is, when you have infected the web page the user is browsing with the sof Javascript code.

16 OpenSSH Good Practices

By Leonardo Neves Bernardo

This article will discuss how to install OpenSSH and increase the level of security using asymmetric key authentication. We will see how to centralize user authentication by using an LDAP server for retrieving public keys instead of `~/.ssh/authorized_keys`. Finally, there are some security tips that are very important to obtain a good level of security using OpenSSH.

24 Cyberwar: Defending a Country

By D. David Montero Abuja

Since the mid-twentieth century to our time, information technology has rapidly evolved. From ENIAC-1, with its' huge size by today's standards to the desktop with next-generation quad-core processors, only fifty years have passed. How can we defend computer attacks a country with millions of connections in and out every minute, with thousands of critical applications and servers between your critical infrastructure? This is the question asked all government security officials, seeking a solution that minimizes the risks to national critical assets. The airspace

is controlled countries both civilian and military control towers. Everyone wants to know who passes through its borders, who flies over its territory, knowing the vehicles, meet the crew. Why not cyberspace? Cyberspace can be reduced to After a series of IP address ranges and communication nodes managed by different national operators. Through communication nodes passing packets on TCP / IP with an IP source address, destination IP address and additional information. Packets that are routed from source to destination through different communications equipment.

28 Social Network Security part 1 &2

By Roland Koch and Steffen Wendzel

Social networking platforms such as Facebook or XING aim on collecting huge amounts of personal information about their users. In this first of two articles, we will highlight the risks linked to such social networking sites while the next article will focus on the protection methods which can be applied for enterprises and private users.

ATTACK

36 The Most Dangerous Attack Of Them All

By Gautam

Want to learn what is SQL Injection, different types of SQL Injection and how to protect from SQL Injection? All the attacks above use a very simple technique known as SQL Injection. SQL injection is an attack in which a website's security is compromised by inserting a SQL Query in the website which performs operations on the underlying database. These operations are unintended by the website's designer and are usually malicious in nature. Attackers take advantage of the fact that designers usually take SQL commands having parameters which are user supplied. The attacker instead of providing the normal user parameter inputs his SQL query which runs against the backend database. Let us go through an example. Consider a website which has a login page. The user enters his username and password on the login page. The underlying database query might look like this.

(IL)LEGAL

42 Why Can't Online Banking Be Like Facebook?

By Drake

In my last column, we talked about some of the problems of pricing information security. This month, we look at a practical application of some of the challenges – specifically around online banking.

TOOL TIME

44 Secure your DNS

By Mervyn Heng

Do you trust your ISP's DNS setup? I don't! DNS is susceptible to attack by malicious entities to target innocent victims just like any other protocol. The solution is to engage OpenDNS as your trusted DNS service which is harnessed by home and enterprise networks globally.

INTERVIEW

46 Interview with Gord Boyce

By Aby Rao



HAKIN9

Subscribe to our newsletter and stay up to date with all news from Hakin9 magazine!

<http://hakin9.org/newsletter>

Learn
Web Application Security
with...



Coliseum

Virtual labs
100% practical hands on
training
by eLearnSecurity

FIND OUT

14 educational challenges

- ✓ Real world scenarios
- ✓ No set-up time
- ✓ Play on MS SQL Server
- ✓ Got stuck? We support!

ADOBE READER EXPLOIT

Adobe products have consistently been the victim to several different hacks and their Adobe Reader product has been exploited yet again. A new vulnerability was reported to Adobe by Lockheed Martin Computer Incident Response Team and the Defense Security Information Exchange. Adobe confirmed the vulnerability and released a security advisory. *This U3D memory corruption vulnerability (CVE-2011-2462) could cause a crash and potentially allow an attacker to take control of the affected system... There are reports that the vulnerability is being actively exploited in the wild in limited, targeted attacks against Adobe Reader 9.x on Windows. Adobe Reader X Protected Mode and Acrobat X Protected View mitigations would prevent an exploit of this kind from executing.* Adobe plans on releasing updates for Adobe Reader 9.4.6 for Windows first as it is the main product being exploited in the wild. Updates for Adobe Reader and Acrobat X for all platforms are slated to be released in January.

by Schuyler Dorsey

BROWSER HISTORY EXPLOIT

Google researcher Michal Zalewski has released a new proof of concept exploit that allows a web server to see recent browsing history of the victim client computer. It has been confirmed to work against full patched Internet Explorer, Firefox and Chrome on both Windows and OS X platforms. Zalewski said *My proof of concept is fairly crude, and will fail for a minority of readers... but in my testing, it offers reliable, high-performance, non-destructive cache inspection that blurs the boundary between visited and all the 'less interesting' techniques.* Dan Goodin of The Register explains the exploit *It starts by loading an iframe tag containing a list of website into the page accessed by the visitor. It then calculates how quickly the websites are rendered. Those that load more quickly must be stored on the browser cache, an indication they have been visited recently.*

by Schuyler Dorsey

PUBLIC JAVA EXPLOIT

A previously commercial-only Java exploit for the vulnerability CVE-2011-3544 has been publicly released and added to many exploit frameworks. The National Institute of Standards and Technology states *Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7 and 6 Update 27 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality, integrity, and*

availability via unknown vectors related to Scripting. The Metasploit team tested the exploit and found it to affect all of the major browsers across Windows, OS X and Linux. Oracle states that there are currently over three billion devices running Java so users are urged to upgrade their Java software immediately to avoid any widespread exploitation. Users running JRE 7 update 1 and 6 update 29 are safe.

by Schuyler Dorsey

U.S. DRONES HACKED

Iranian electronic warfare specialists successfully exploited a weakness in U.S. drones and were able to guide a drone to land safely in hostile territory. The specialists used a navigational weakness already known by the U.S. military; they jammed the communication to the drone and forced it into autopilot. At this point, they were able to have the drone land at the exact location they desired by spoofing GPS coordinates; this circumvents having to crack the communication altogether. In the past, they were able to capture video feeds from the drones using off the shelf software but the ability to essentially control the drones and capture them proves a much greater danger.

by Schuyler Dorsey

HP LASERJET VULNERABILITY

Researchers at Columbia University have discovered a vulnerability in HP Laserjet printers made in and before 2009. Through a modified print request, attackers could change the firmware of the printer entirely. Possibilities of the modified firmware range from compromising the network to overheating the printer. The weakness stems from the HP printers' lack of authenticating the software updates. In HP's statement, they said *The specific vulnerability exists for some HP LaserJet devices if placed on a public Internet without a firewall... In a private network, some printers may be vulnerable if a malicious effort is made to modify the firmware of the device by a trusted party on the network. In some Linux or Mac environments, it may be possible for a specially formatted corrupt print job to trigger a firmware upgrade.* There are currently no reports of this exploit being used to gain unauthorized access to any systems but HP is quickly working to resolve the issue.

by Schuyler Dorsey

RUSSIAN HACKERS HIT TWITTER WITH AUTOMATED HASHTAG TWEETS

Russian hackers hit Twitter with automated hashtag tweets Russian hackers have taken aim at Twitter in recent days to hamper communication between

opposition activists as outrage against the conduct of last week's general elections grows. The pro-government messages were generated by thousands of Twitter accounts that had little activity beforehand. The hashtag is #???????????? (Triumfalnaya), the name of the square where many protestors gathered. Maxim Goncharov, a senior threat researcher at Trend Micro, observed that *if you currently check this hash tag on twitter you'll see a flood of 5-7 identical tweets from accounts that have been inactive for month and that only had 10-20 tweets before this day. To this point those hacked accounts have already posted 10-20 more tweets in just one hour.*

Source: ID Theft Protect

ROOTED ANDROID NFC PHONE DECRYPTS GOOGLE WALLET DATA

Security researchers rooted an Android NFC Google wallet device and established that a large amount of data was left unencrypted. However worth pointing out that no access to the secure element was gained. Credit cards numbers and PIN are stored securely) however it appears Google Wallet stores unencrypted data on the device i.e. last four digits of your credit card, credit card balance and limits. The security researchers only conducted a high level analysis but are sure other vulnerabilities are present. The secure element wasn't accessed in this test – the secure element is the layer that stores and protects payment instructions and data including credit card and CVV numbers.

Source: ID Theft Protect

GOOGLE CODE PLAYGROUND XSS VULNERABILITY POC IDENTIFIED

Two security researchers have identified an XSS in Google Code. Proof Of Concept: Just go to <http://code.google.com/apis/ajax/playground/> and then click on edit HTML after that remove all the codes and type this script: `onerror=alert(„XSS“)/>` and click on DEBUG CODE, and then first it will show you `sample must have <head> element` click OK and wait for the window to load if nothing happen then try the same thing again or simply you can click on RUN CODE, and you will get a popup which is XSS. Thanks to our friends @THN.

Source: ID Theft Protect

FAKE VERIZON ZIP FILE ATTACHMENT TROJAN IN CIRCULATION

Microsoft is warning users about a fake Verizon notification which is carrying a Trojan. The email appears to come from Verizon and attempts to make

the customer feel a sense of urgency by claiming it contains crucial account information from Verizon Wireless. The fake email has a ZIP file attached named *Verizon-Wireless-Account-StatusNotification_#####.zip* (random numbers are used in the name). This same malware attack vector is being used in fake critical updates for Adobe Acrobat Reader and Adobe X Suite.

Source: ID Theft Protect

FACEBOOK FIXES PHOTO PRIVACY SECURITY FLAW

Facebook has this week (w/c 5th Dec) patched a vulnerability that allowed any user to view any other user's private photos. Mark Zuckerberg's Facebook account was compromised and a total of thirteen photos were downloaded and posted on a website called *imgur.com*. Facebook responded very quickly after Zuck had his account compromised after a post in a discussion forum on bodybuilding, detailed a method for using a feature to report suspicious content to bypass privacy protections on other Facebook users' accounts. The code flaw was actually created in a recent code push and Facebook confirmed that the flaw was only available for a *short period of time* before it was patched.

Source: ID Theft Protect

BRAZILIAN BANKING TROJAN DISGUISED AS MICROSOFT ANTI-VIRUS SOFTWARE

A Trojan (identified as Trojan-Downloader.Win32.VB.aoff) is targeting Windows-based systems by removing built-in AV software and clearing a path for cybercriminals to silently steal online banking credentials. The Trojan affects *ntldr* the default boot loader in Windows. The Trojan is propagating as an attachment on an email. This attack vector relies on the victim clicking on the malicious link which then downloads two malicious files from AWS. The malicious files are *xp-msantivirus* and *xp-masclean* which worm their way to the bootloader (ntldr). The malicious files replace the bootloader file with a malicious version of GRUB and ntldr then boots into Linux or UNIX to remove a common Brazilian banking plug-in while at the same time removing the in-built Microsoft security software. This action occurs as the computer starts up and automatically erases itself so the victim has no idea their Windows PC is infected.

Source: ID Theft Protect

Practical Client Side Attacks

In a penetration test, it is common not to pay attention to web vulnerabilities like XSS or XSRF. This is because people usually think about an alert message when speaking about XSS. The reality is that the client side web vulnerabilities can be a powerful way to access forbidden resources and information.

What you will learn...

- To take advantage of a XSS in a penetration test.
- Different client side attack vectors.
- Solutions to these vulnerabilities.

What you should know...

- What is a XSS and a XSRF.
- Knowledge about HTML and Javascript

When people think about Client Side Attacks, the first one in which they think of is *Cross Site Scripting* (XSS). OWASP Top 10 classifies it like the second most frequently vulnerability in Web applications. Nevertheless, the image usually comes to our minds when we are speaking about XSS as an alert message showing the word XSS or the user cookie (Figure 1).

In that, many webmasters and business security managers believe that Cross Site Scripting is not a risky vulnerability. Another reason is that XSS does not affect their system, it affects the user browsers.

Reality is that Cross Site Scripting allows many different kinds of attacks and it is actually easy to spread to many users in little time.

One of the most interesting attacks which is possible to do through a XSS is *Session Hijacking*. It allows to impersonate a user by stealing his cookie session. After that, the attacker will have to change his own cookie for the stolen one.

The tool *Shell of the Future* (soft) makes all these steps easy once you have successfully exploited a Cross Site Scripting. That is, when you have infected the web page the user is browsing with the *soft* Javascript code.

The main idea of *soft* is to send information about the web page that the victim is browsing (the page affected by the XSS) to a controlled server which exchanges this information with a proxy. The attacker uses the

proxy to access the same domain with the cookie of the user (which is set up by the proxy). The result is that the attacker has a list of every hijacked sessions and can choose amongst them in an effortless way.

The information sent to the controlled server is the cookie the victim is using, the URL and the HTML code of the page (that allows to see the current page the user is visiting) and all HTTP headers.

Shell of the Future is a proof of concept and it has several deficiencies. Nevertheless, it can be really useful to create a testing environment where to show the potential of Cross Site Scripting in a presentation.

One of the problems of *soft* is that the control only lasts while the user is in the infected page. After that, the attacker can continue using the user cookie but if it changes, he will not be able to know it. The solution *soft* suggests, is to open a new tab in the browser and



Figure 1. Cross Site Scripting – Typical alert message

redirect user interaction to this tab while the infected one remains unchanged. Maybe this is a too visible solution and users would be able to see that something strange is happening.

Other frequent attack which is possible to do through a Cross Site Scripting is *Website Defacement*. It is usually used to damage the image of a company or an institution by the publication of a link which exploits the XSS modifying the original content of the website.

These are just some basic examples of what kind of attacks are possible to carry out through a Cross Site Scripting.

Advanced Client Side Attacks

If we are performing a penetration test and we need to take advantage of a Cross Site Scripting, the biggest difficulty we have to overcome is to program the Javascript exploit which we will use to infect the browser victims.

The *Browser Exploitation Framework* (BeEF) can help in this task offering us the swissknife of XSS attacks.

BeEF allows to manage a *botnet* composed of XSS infected browsers. It offers different possibilities depending on the browser and operative system being used by the victim. Some of the most important are:

- to get information about the operative system and browser version, installed plugins and other third party software,
- partial or complete website defacement of the page that the victim is visiting,
- different ways to attack the infected website looking for vulnerabilities like SQL injection or *Cross Site Request Forgery* (XSRF),
- to scan victim network looking for other web servers and alive hosts,

- to use the controlled browser like proxy to navigate inside the infected domain,
- exploitation of known vulnerabilities in JBoss, vTiger CRM, Linksys systems, etc.,
- Metasploit integration.

Infecting browsers

BeEF is a framework with different possibilities about how to take advantage of a Cross Site Scripting. But before using it, it is necessary to infect the victims browsers with the Javascript exploit of BeEF.

To do that, the user needs to enter in a controlled domain in which the attacker had previously put the BeEF code, or needs to be deceived to exploit a XSS following a malicious link.

In both cases, we have the same problem with *Shell of the Future*: the user has to stay in the controlled domain, or exactly on the web page with the XSS to use BeEF against him. This is a big problem we need to solve.

One possible solution is to find a domain which the user frequently visits, in which the penetration tester has enough time to perform the attack and inject the BeEF code inside it. Some examples of interesting websites are:

- companies internal websites like intranet portals or other sites with internal resources,
- social networks,
- usual home pages like search engines, web desktops...

In some penetration tests, it is possible to have access to internal resources like intranet websites or other internal web servers. These are good targets because employees usually have these kinds of sites as home pages in their browsers and waste enough time in them to perform the attack.

Listing 1. iGoogle gadget definition example

```
<?xml version="1.0" encoding="UTF-8" ?>
<Module>
  <ModulePrefs
    author="Attacker"
    author_email="fakemail@gmail.com"
    author_location="123 Fake Street"
    description="This gadget is a PoC for Hakin9 Magazine"
    title="My Hakin9 Gadget!!"
    directory_title="My Hakin9 Gadget!!"
    thumbnail="http://hakin9.org/wp-content/uploads/2011/03/hakin9_EN.png">
    <Require feature="views" />
  </ModulePrefs>
  <Content type="url" view="home" href="http://www.example.com/Hakin9/index.html" />
</Module>
```

On the other hand, if we do not have direct access to these resources, it is difficult to achieve enough knowledge of them to find some vulnerability to take advantage of it and use it against network users. Moreover, maybe the target of the penetration test is to obtain access to these resources, so we would be in a Catch-22 situation.

Social networks allow to infect many users in a short period of time, but they are usually filtered from business networks. Therefore, they are not really useful in penetration tests.

Typical home pages have the same advantages of internal websites resources: users use them many times per day and usually have them opened for long periods. However, these sites are very secure and it is not easy to find a stored XSS, which is the most interesting kind of XSS for these attacks.

One solution we can use with web desktops and social networks is to use the functionalities they offer to developers and program a malicious third party application like a game or a gadget.

Because of all the above reasons, a good way to control a high number of browsers is using an iGoogle gadget which contains the BeEF Javascript code.

iGoogle uses OpenSocial API to define metadata information about the gadget like the author, the name of the gadget, the description, a thumbnail, the final URL, etc.

When the iGoogle gadget is finished, the way of spreading it is sharing it amongst users with one link like the following: http://www.google.com/ig/directory?dpos=top&root=/ig&url=www.example.com/Hakin9/ig_gadget.xml.

If the target is to infect as many browsers as possible, the link can be published in social networks, blogs, forums, sent in e-mails or use other social engineering strategies. The easier way is that the content of the gadget would be attractive to users because they will share it amongst themselves.

This is a basic example of how to include the malicious code of BeEF in a frequently visited website, and being totally invisible for users. Moreover, it is really easy to

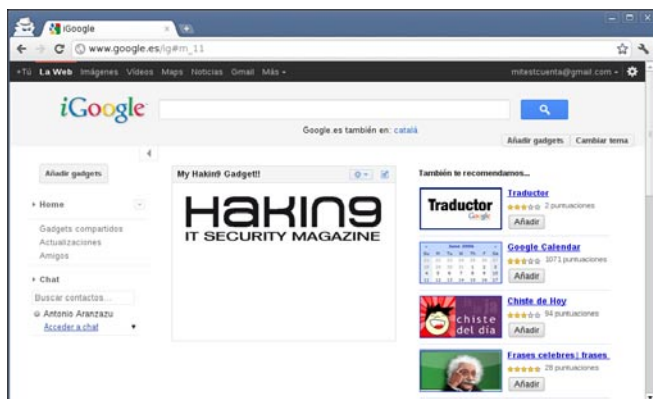


Figure 2. iGoogle Desktop with a malicious Hakin9 gadget

spread because the link which infects iGoogle desktops belong to www.google.com domain.

Cross Domain and Cross Site Request Forgery

Modern web browsers implement same origin policy. This policy forbids access across pages on different domains using browser-side programming languages such as Javascript or Flash.

In the practice, when you try to make a request to other domain using, for example, the AJAX object `XMLHttpRequest`, the browser actually makes the request and when the response is received, an exception is thrown, which does not allow to process the response.

Knowing that, if we have controlled a browser from the domain www.attacker.com, we can use BeEF to make requests to www.intranet.com but we will not be able to process the response. The requests we send from BeEF using `XMLHttpRequest` will have the session cookie which the browser would have stored. So, if we have infected the browser of a network administrator, we will be able to access management sites where he would have a session opened, and send requests such as:

```
www.intranet.com/admin/createUser?username=attacker&password=5f4dcc3b5aa765d61d8327deb882cf99
```

This request may create a new user `attacker` with password `password` in the application hosted in www.intranet.com.

The only restriction here is protection against *Cross Site Request Forgery* (XSRF) which could be implemented in the management site. Some tasks which are possible to do are: create or delete users, upload files to the server, deploy applications, etc.

Other BeEF uses

If the penetration test is being performed from outside of the company, BeEF allows to scan the internal network looking for alive hosts and other web servers or performing port scans. This information could give

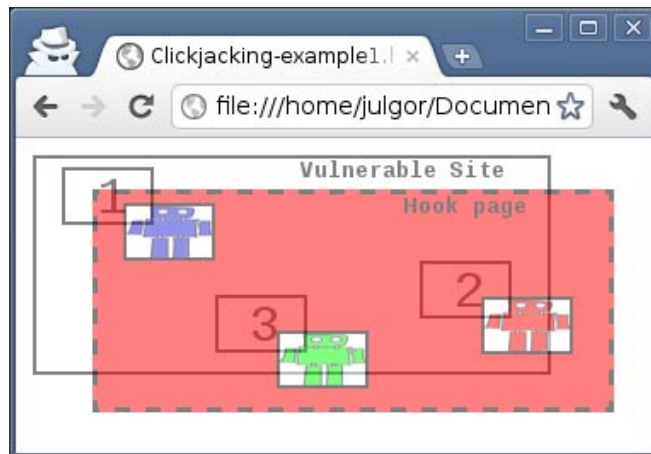


Figure 3. Clickjacking example

a general idea about the company network before to perform other kinds of attacks.

In fact, in this case, it can be interesting to use Metasploit through BeEF to take control of the victim system. Metasploit has a big set of exploits which can be used to jump from the browser to the operative system. By this, the computer of the victim could be used as a bridge to get access to the company network and the internal resources.

Another BeEF use is Website Defacement. As I have explained above in this article, this attack can be very useful if it is well performed.

One of the most typical defacements is to replace the login form with another one, which sends user credentials to a controlled server. Here the attacker can store all the stolen credentials. To be detected by the user could be avoided by sending the user credentials to the correct server at the same time. Another valid option is to replace the login form of the first login attempt of the user, and restore the correct form in the second one. In this case, the user will usually think that he has been wrong the first time.

Those are some of the functions BeEF offers which allows to take advantage of a Cross Site Scripting. The set of all possibilities depends on the imagination of the penetration tester.

Clickjacking

In 2008, Robert Hansen and Jeremiah Grossman presented a new kind of attack which they called Clickjacking.

Clickjacking is a way of tricking users into doing some tasks they do not know they are doing while clicking on a seemingly harmless web page (hook page).

The main idea is to put the hook page over the page where the user is actually performing the action. The user, who only can see the hook page, will interact with the real one while clicking on the links showed.

Figure 3 shows a possible scene where the objective is that the user clicks over the boxes 1, 2 and 3. The red frame is put over the boxes to hide them and presenting a challenge (like a captcha) to the user, where the user has to click over three different objects in a certain



Figure 4. Fake game with a hidden iframe

order. In this case, the challenge is to click over the blue, the red and the green robot.

This is only a theoretical example to understand the Clickjacking concept. One practical example which allows seeing it in a real situation is how to turn on the webcam of a remote user through iGoogle.

Figure 4 shows a simple game where the user has to destroy alien spaceships clicking over them. The game seems to be innocuous, but actually the iGoogle main page is placed below the game frame (Figure 5).

When the user starts to play, some of the spaceships appear strategically placed where the user has to click performing different tasks:

- enable the chat function,
- add the attacker as a new contact,
- start a conversation with the attacker
- and ask him for a video conference.

If the user clicks on all the spaceships, the attacker only needs to pick up the video conference to turn on the user webcam.

Clickjacking is not really used to perform complex attacks. At present it is used in more common uses like tricking users into clicking over advertisements or *Like* buttons, which is also known as Likejacking.

Likejacking uses the same idea of Clickjacking, but in this case, the hidden panel is a *Facebook Like button* or a *Google +1 button*. When the user clicks over that, he is publishing on his wall that he likes what the attacker wants. That is an easy way of do free marketing.

As we can see, a website is vulnerable to Clickjacking, if it can be inside of a frame different from the *Window* object of the DOM model. That means, if the website does not force to use the full window.

Mixing this concept with some phishing techniques like similar domain names (*hakin9.org* vs *hackin9.org*), DNS Poisoning... it is possible to program a Java applet which simulates the activity of some bank trojans, taking screenshots of user activities.

Imagine we need to do an exhibition about a bank website, in which we have to study if the bank



Figure 5. Fake game showing the iGoogle frame

website (www.fakebank.com) is or is not vulnerable to Clickjacking. Depending on the accuracy we want to give, we can buy the domain (www.myfakebank.com) and set it up with a main page which has an iframe with the real website bank.

Moreover, the main page would try to execute a malicious Java applet which takes screenshots of user activities every few seconds and send them to a controlled server. To avoid being detected because of the bandwidth used, the images could have low resolution and send them all together every several minutes or one by one, depending on the network congestion.

With this kind of client side malware it is possible to steal credit card and bank account numbers, personal information, e-mail addresses, etc.

Figure 6 and 7 show two vulnerable actual websites. The first one is a page from an American bank where the customers fill out a form with some personal information and their debit card number.

The second figure is the login page of a Spanish bank where the PIN is introduced using a virtual keyboard. Looking at the position of the mouse when each dot is written, it is possible to know the PIN number. Using this technique TANs (*Transaction Authentication Numbers*) can be recovered too.

At present, most websites are not protected against Clickjacking. That is most banks and electronic commerce websites are not protected, and using this technique is an easy way to steal credit card numbers and other sensitive information. A lot of management portals are not protected too, so deceiving users to do some privileged tasks is possible.

Identification and Prevention

Cross Site Scripting and other Javascript Attacks

Identification of Cross Site Scripting is not an easy task. It needs to identify all application input variables which are returned as a part of the HTML or Javascript code in the response.

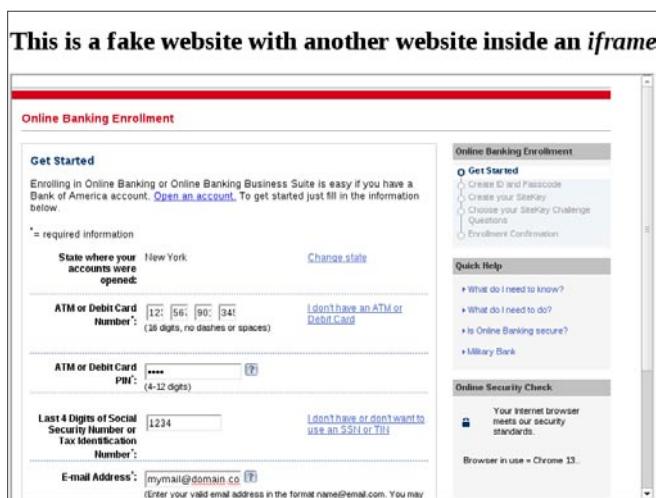


Figure 6. An American Bank enrollment form

That includes inputs which are stored in any database and could be returned in any moment (Stored XSS) and those inputs which are threats and immediately returned (Reflected XSS). The adoptive measures to solve Cross Site Scripting start validating all inputs by the most restrictive way. Regular expressions which allow only expected values can be used to do that.

In the second step, all output variables must be encoded using HTML entities. That means, changing HTML characters for its HTML encoded version: `<` is `<`, `>` is `>`, etc. In this case, it does not matter the origin of the output variable (a database, a configuration file, a user input...), all of them must be encoded.

That is not enough to avoid attacks like the ones showed using BeEF, because its code does not need to be injected through a Cross Site Scripting. It can be inside a controlled domain.

The most effective way to avoid these kinds of attacks is to disable Javascript in browsers or to use some extension like NoScript. The problem with both solutions is that too many web applications will not work correctly, and because of that most users will change the configuration to allow Javascript again, becoming vulnerable to Javascript attacks.

Another solution could be to enforce the control of allowed websites through the company proxy. Nevertheless, this practice is not very effective as well because employees' work could be affected.

In other words, users access to dangerous content have to be assumed. So they will be able to be infected with Javascript malware or worse, their computers will be able to be controlled through browser exploits. To try to reduce the risk, browsers have to be always patched up to latest stable version.

Clickjacking

Clickjacking can be easily identified creating a web page with a HTML iframe which contains the domain we need to check:

```
<html><body>
  <iframe src="http://www.example.com">
</body></html>
```

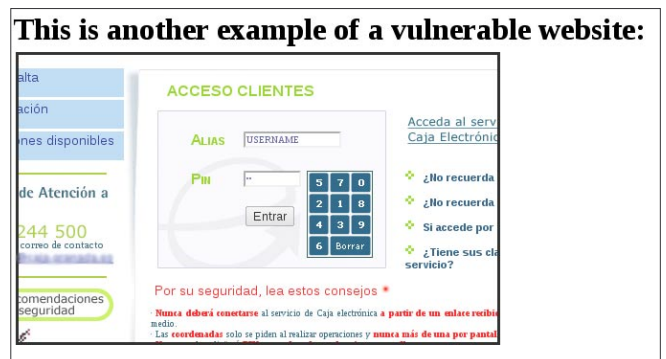


Figure 7. A Spanish bank login page

Table 1. X-Frame-Options values

Value	Meaning
DENY	The page cannot be displayed in any frame, no matter the domain.
SAMEORIGIN	The page can only be displayed in frames from the same top-level domain (TLD).
ALLOW-FROM origin	The page can be displayed in frames from the specified domain. Several domain definitions are not supported.

On the 'Net

- <http://www.andlabs.org/tools.html> – Shell of the Future
- <http://beefproject.com/> – Browser Exploitation Framework (BeEF)
- <http://www.sectheory.com/clickjacking.htm> – Original Clickjacking paper
- <http://metasploit.com/> – Metasploit
- <http://code.google.com/intl/en/apis/igoogle/docs/igoogledevguide.html> – iGoogle Developer's Guide
- <http://en.wikipedia.org/wiki/Framekiller> – Framekillers
- <https://addons.mozilla.org/en-US/firefox/addon/noscript/> – NoScript Firefox Add-on

If the domain is shown inside the iframe when the test page is open in the browser, then the domain is vulnerable to Clickjacking.

One way to avoid it is using a *Framekiller*. A framekiller is a piece of Javascript code which checks if the father frame of a web page is the DOM object *Window*.

```
<script type="text/javascript">
  if (top != self) top.location.replace(location);
</script>
```

There are several ways to bypass framekillers using Javascript code. Moreover, if NoScript is installed in browsers, this solution cannot work.

The most effective solution is to add the HTTP Header named X-Frame-Options using one the possible values shown in Table 1. Like in every validation process, it is always recommended to use the most restrictive value which, in this case, is deny. That forbids to use the web page inside any frame.

The value *sameorigin* is not recommended due to every domain with the same TLD (Top-Level Domain), can include the web page which has the HTTP Header X-Frame-Options. That means, if the web page we need to protect is <http://www.example.com/login.php>, every .com domain can include it inside a frame.

The third value, *allow-from*, allows to specify the domain which can include the protected web page. This option cannot be used to specify more than one domain at the same time. When a web page needs to be accessed from different domains, one possible solution is to send some owner domain information in the query string parameter. The server will check if the passed information matches with the expected one according to the actual domain and if it does, the server will return the web page with the corrected *allow-from* header value.

It is important to note that this header cannot be replaced with a HTML META Tag because many

browsers ignore this tag. Moreover, older versions of browsers do not support X-Frame-Options header. Browsers supporting it are:

- IE8+
- Firefox 3.6.9+ (older versions support it with NoScript)
- Chrome 4.1.249.1042+
- Opera 10.50+
- Safari 4+

Summary

Client Side Attacks can be used in several phases of a penetration test. In the reconnaissance and scanning phases, they can be used to achieve information like what software versions are installed, take a first look of the user network, locate other web servers, etc.

In the exploitation phase, Client Side Attacks can help take control of user systems through web browser vulnerabilities. Making a bridge between the penetration tester and the user network.

Moreover, combined with social engineering or phishing techniques they can be used to achieve sensitive information or to deceive users to perform some privileged tasks.

In conclusion, Client Side Attacks are a powerful tool which should be more used in penetration tests because of their possibilities.

JULIO GÓMEZ ORTEGA

The author has been working in the Security IT Industry for more than four years. He works like Security Engineer at S21sec. He collaborates actively in the sector researching and developing new open software security tools. He is the founder of a security blog where, in collaboration with other colleges, publish the results of their researches.

OpenSSH Good Practices

This article will discuss how to install OpenSSH and increase the level of security using asymmetric key authentication. We will see how to centralize user authentication by using an LDAP server for retrieving public keys instead of `~/.ssh/authorized_keys`. Finally, there are some security tips that are very important to obtain a good level of security using OpenSSH.

What you will learn...

- Why SSH is important for security;
- How to secure OpenSSH using keys and agents;
- How to use the LDAP Public Keys (LPK) patch.

What you should know...

- A basic understanding of the SSH protocol;
- Basics of the Linux shell.

SSH is a protocol which started as a replacement to (very) insecure protocols like telnet, rsh and rlogin. These insecure protocols did not protect the confidentiality of data, and did not provide strong authentication. In 1995 Tatu Ylönen, from Finland, designed the first version of the SSH protocol (SSH-1) which quickly became widely used. At first SSH was free software, but in December 1995 Ylönen founded the SSH Communications Security company, and later versions of SSH were proprietary software. In 1999 some people, in particular some from the OpenBSD project, who were concerned with the importance of SSH continuing to be available as free software, started the OpenSSH project. Today OpenSSH is the most widely used version of SSH, and SSH has become the primary protocol used for remote administration of Unix systems, used by millions of users.

At first SSH was used only for remote administration, but other functionality was added over time, such as secure file transfer and forwarding of the X window system.

Due to the importance of the protocol, the *Internet Engineering Task Force* (IETF) formalized a number of Requests for Comments. There are currently many RFCs related to SSH in the process of being evaluated.

Although the SSH protocol is widely used for confidentiality, integrity and authentication, some other features such as strong authentication using

asymmetric keys are supported but not often used. Some SSH installations are not secure using the default configuration, and the majority of system administrators use default parameters when they install new systems. We will see below how to avoid some insecure configurations, and how to implement centralized strong authentication using LDAP and the *LDAP Public Keys* (LPK) patch for OpenSSH.

OpenSSH Software

OpenSSH is developed by two teams in the OpenBSD project. One team does strictly OpenBSD-based development, aiming to produce code that is as clean, simple, and secure as possible. The other team takes the clean version and makes it portable to enable it to run on many other operating systems, including linux. The portable version has *p* included in the name. For example, *openssh-5.0.tar.gz* and *openssh-5.0p1.tar.gz* have the same functionality.

Over time, a number of vulnerabilities have been discovered in both the SSH protocol and in OpenSSH, which have been corrected in subsequent versions. As SSH and OpenSSH continue to be a security target, it is likely that additional vulnerabilities will be discovered in the future. In general, you should avoid the obsolete SSH-1 protocol (SSH-2 was launched around 2006). In the case of OpenSSH it is best to use the most recent version, but versions 5.0 and above have a reasonable level of security.

The two main components of OpenSSH are the SSH server (sshd) and the SSH client (ssh). Some additional components like secure file copy (scp) and SSH agent (ssh-agent) are also distributed in the SSH package. OpenSSH is distributed under the BSD licence and uses the OpenSSL libraries to implement SSL functionality. Some security functionality such as chroot support started as a patch and subsequently became part of the core development of OpenSSH. Other functionality such as LPK and sftp-server audit logging continue as patches, but are very useful to increase the level of security.

Installing OpenSSH

Unless your system is BSD like, to install OpenSSH you should download the latest version from <http://www.openssh.com/portable.html>. At the time this article was written, the latest version was *openssh-5.9p1.tar.gz*. You also need the openssl development package to install OpenSSH.

Install OpenSSH using the following commands:

```
# tar -zxvf openssh-5.9p1.tar.gz
# cd openssh-5.9p1
# ./configure && make && make install
```

To use TCP Wrappers, you can compile with the following command:

```
# ./configure --with-tcp-wrappers && make && make install
```

The above instructions will be sufficient for most users, however we intend to store SSH public keys using LDAP. To achieve this we need to install OpenSSH with the LPK patch. The LPK patch is not updated frequently, in fact the last OpenSSH version *officially* supported is openssh-4.6p1. Fortunately there are patches inside the contrib directory that run in newer versions of OpenSSH. The last version for which it is possible to use the LPK patch is openssh-5.4p1. Although version 5.4 is not the latest and most secure version of OpenSSH, it has a good level of security.

First of all, download version 5.4 of OpenSSH and uncompress it:

```
# tar -zxvf openssh-5.4p1.tar.gz
```

Download the LPK patch, from the subversion repository:

```
# svn checkout http://openssh-lpk.googlecode.com/svn/trunk/openssh-lpk-read-only
```

The LPK patch was designed to use the openssh-5.4p1.orig directory instead of openssh-5.4p1. Because

of this, we need to change the patch with the following command:

```
# sed -i 's/.orig//g' openssh-lpk-read-only/patch/contrib/contrib-openssh-lpk-5.4p1-0.3.13.patch
```

Now, we run the patch command:

```
# cd openssh-5.4p1
# patch -p 1 < ../openssh-lpk-read-only/patch/contrib/contrib-openssh-lpk-5.4p1-0.3.13.patch
```

And install, using the `--with-ldap` argument:

```
# ./configure --with-tcp-wrappers --with-ldap
# make
# make install
```

Configuring OpenSSH

The first action to carry out to secure an installation of OpenSSH is to disable unused features. Many vulnerabilities that have been discovered are related only to some part of the SSH daemon, and do not affect the whole daemon. It is very common, for example, for vulnerabilities to be discovered related to X windows forwarding. If you start X windows forwarding unnecessarily, you are vulnerable to all the problems related to that feature. Let's look at some relevant configuration changes to make sure that the SSH daemon has a minimal level of security issues:

X11Forwarding

Unless this host is an X terminal server or has some software which runs only under X such as IBM installers, use *X11Forwarding no*. Sometimes it is recommended to enable X11Forwarding only to install some software, and afterwards to disable this feature again. The X11Forwarding default configuration is *no*.

Protocol

The SSH-1 protocol is now obsolete, with some security issues being corrected in the SSH-2 protocol. It is very important to configure *Protocol 2* in *sshd_config*. It is possible to use the protocol directive to support multiple protocols using comma separated values such as *Protocol 2,1*, but this does not ensure the precedence order of different protocol versions, because the SSH protocol version is negotiated between the client and the server. Because of this, the only configuration that ensures that only protocol 2 is used is *Protocol 2*. This is now the default configuration.

Subsystem

Subsystem configures an external subsystem (e.g. a file transfer daemon). Even though sftp has SSH

protection related to authentication and confidentiality, it lacks auditing. You have some different alternatives here, depending on your situation. When confidentiality is not a concern, you can use the rsync daemon. If confidentiality is a concern, sometimes the best solution is to use FTPS (FTP with TLS support). If you use sftp, consider the sftp-server *audit* logging patch, although unfortunately this patch is supported only by OpenSSH version 4. We will discuss how to restrict subsystem sftp to only certain hosts or users. Independently of configuration, scp and rsync + ssh would permit the transfer of files from and to your server.

StrictModes

StrictModes ensures that sshd will check file modes and ownership of the user's files and home directory before accepting a login. *StrictModes yes* is the default and recommended configuration.

Port

The default TCP port of the SSH service is 22. Some people change this default port to another, aiming for security through obscurity. I consider that security by obscurity is no security at all. If you think differently, please consider the recommendation of The *United States National Institute of Standards and Technology* (NIST) against this approach. NIST states that *system security should not depend on the secrecy of the implementation or its components*. If you want to change the SSH port anyway, no problem, your SSH daemon will have the same security level with either port 22 or a different one.

ListenAddress

If your host has multiple network interfaces, it is important to restrict access only from the most secure network. We can improve security further using more detailed firewall rules (router firewalls, iptables, ipfw, etc.) or TCP Wrappers, but the first step is to restrict access using ListenAddress.

AllowTcpForwarding

The `sshd_config` man page states the following regarding AllowTcpForwarding:

Specifies whether TCP forwarding is permitted. The default is *yes*. Note that disabling TCP forwarding does not improve security unless users are also denied shell access, as they can always install their own forwarders.

Although the man page states that disabling TCP forwarding is not a security improvement, if your host has good hardening, where common users don't have permissions to install or run external software, and there is no software available to them that can be used

to create tunnels, this configuration could be effective. I recommend you use *AllowTcpForwarding no*.

AllowAgentForwarding

Like AllowTcpForwarding, the `sshd_config` man page advises that disabling agent forwarding does not improve security because users can install their own agent forwarders. I disagree again, because in hosts with good hardening and with all servers configured to accept connections only with keys, you can prevent users (or intruders) from accessing one server from another server. I recommend you use *AllowAgentForwarding no*. There is one situation where *AllowAgentForwarding yes* is necessary: on an SSH proxy which SSH communications need to pass through.

UsePrivilegeSeparation

This configuration is very important to security. With *UsePrivilegeSeparation yes*, sshd will fork another process with user privileges after login, and any security problem will exploit the system only with common user privileges. The default and recommended configuration is *UsePrivilegeSeparation yes*.

AllowUsers, AllowGroups, DenyUsers, DenyGroups

If on the system some users need SSH access and others don't, you can use these directives to control access. In general, recommendations are:

- Use an invalid shell for users if they don't use another daemon that needs a valid shell;
- Use TCP Wrappers where it is not necessary to reload the daemon to change configurations;
- Use **groups* directives instead of **users* directives, it is simpler and therefore more secure to administer;
- Use *Allow** directives instead of *Deny** directives, as *Allow** directives follow the least privilege principle. I recommend you use *AllowGroups* if you have an LDAP-aware environment.

PasswordAuthentication, PubkeyAuthentication, ChallengeResponseAuthentication

The most secure authentication method is Pubkey Authentication. Because of this, it is recommended to use *no* in all directives related to authentication, except PubkeyAuthentication. Use *PubkeyAuthentication yes*.

PermitRootLogin

There are four possibilities for PermitRootLogin, but the most secure is *PermitRootLogin no*, because it is not recommended for the root account to login directly to

the system. Use the `sudo` command when necessary following login instead of configuring `PermitRootLogin` to be a different option from `no`.

Configuring a Minimal SSH Install With PubkeyAuthentication Only

Before the instructions on configuration, we need to remember a little about asymmetric cryptography. Public key authentication uses a pair of computer generated keys – one public and one private – to authenticate between a host and a client. The public key and the private key are related. When authenticating a client,

Listing 1. Minimal `sshd_config` file

```
Protocol 2
Port 22
AllowTcpForwarding no
AllowAgentForwarding no
X11Forwarding no
UsePrivilegeSeparation yes
StrictModes yes
PubkeyAuthentication yes
PasswordAuthentication no
ChallengeResponseAuthentication no
PermitRootLogin no
```

Listing 2. Detailed attempt to authenticate

```
# ssh -v test@localhost
OpenSSH_5.4p1lpk, OpenSSL 0.9.8k 25 Mar 2009
debug1: Reading configuration data /usr/local/etc/
        ssh_config
debug1: Connecting to localhost (::1) port 22.
debug1: Connection established.
debug1: permanently_set_uid: 0/0
debug1: identity file /root/.ssh/id_rsa type -1
debug1: identity file /root/.ssh/id_rsa-cert type -1
debug1: identity file /root/.ssh/id_dsa type -1
debug1: identity file /root/.ssh/id_dsa-cert type -1
debug1: Remote protocol version 2.0, remote software
        version OpenSSH_5.4
debug1: match: OpenSSH_5.4 pat OpenSSH*
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_5.4
... Lot of messages about key exchange ...
debug1: Authentications that can continue: publickey
debug1: Next authentication method: publickey
debug1: Trying private key: /root/.ssh/id_rsa
debug1: Trying private key: /root/.ssh/id_dsa
debug1: No more authentication methods to try.
Permission denied (publickey).
#
```

the host machine verifies data that has been encrypted using the client's private key, using the client's public key. If the verification succeeds, this confirms the client as the owner of the key pair, and access is granted. The security of the system is predicated on the security of the private key.

Now, let's create a minimal `/usr/local/etc/sshd_config` using Listing 1 as an example.

Remember that `/usr/local/etc/sshd_config` should be writable by root only. Start the SSH daemon with the following command:

```
/usr/local/sbin/sshd -f /usr/local/etc/sshd_config
```

And now, let's create a user named `test` and set the password to `tests`:

```
# useradd test
# passwd test
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Now, we try to connect using password authentication. We will use the `-v` flag to show more details of the

Listing 3. Using `ssh-agent`

```
# ssh-agent
SSH_AUTH_SOCK=/tmp/ssh-jrSKZC3330/agent.3330; export
        SSH_AUTH_SOCK;
SSH_AGENT_PID=3331; export SSH_AGENT_PID;
echo Agent pid 3331;
# SSH_AUTH_SOCK=/tmp/ssh-jrSKZC3330/agent.3330;
        export SSH_AUTH_SOCK;
# SSH_AGENT_PID=3331; export SSH_AGENT_PID;
# ssh-add
Enter passphrase for /root/.ssh/id_rsa:
Identity added: /root/.ssh/id_rsa (/root/.ssh/id_
        rsa)
# ssh test@localhost
Last login: Mon Dec 12 20:48:12 2011 from localhost

uid=1003(test) gid=1003(test) groups=1003(test)
```

Listing 4. header of `slapd.conf`

```
include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/
        inetorgperson.schema
include /usr/local/etc/openldap/schema/nis.schema
include /usr/local/etc/openldap/schema/lpk.schema
```

attempt. Listing 2 shows that the ssh client attempts to authenticate using keys located in `/root/.ssh/id_rsa` and `/root/.ssh/id_dsa`. As there are no private keys in these locations, authentication fails. We can see some other details about the SSH version and protocol and the SSL version.

Now, we will create a pair of keys to use for authentication:

```
# ssh-keygen -q
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase): passphrase
Enter same passphrase again: passphrase
#
```

Well, here we have a problem. Many users and even system administrators like to create keys without passwords. All the advantages of two-factor authentication using public key + passphrase are lost. If you need three-factor authentication, you can consider buying some biometric tokens to store your private keys.

Let's authorize our user (root) to access the `test` account using keys. Copy the content of `~/.ssh/id_rsa.pub` to `~test/.ssh/authorized_keys`.

Now, try to access the `test` account using keys:

```
# ssh test@localhost
Enter passphrase for key '/root/.ssh/id_rsa':
Last login: Mon Dec 12 20:47:13 2011 from localhost
$ id
uid=1003(test) gid=1003(test) groups=1003(test)
$
```

As you can see, now authentication is working fine but we still have some problems. First of all we have a problem that we have to type the passphrase all the time, consequently leaving the passphrase more susceptible to key loggers. We can solve this problem using `ssh-agent`, as is shown in Listing 3.

Using `ssh-agent` permits SSH access to SSH servers without the repetitive typing of passphrases. It's important to note that the socket file is a critical point and any user with read access to it can use a key loaded in memory. In particular, root has access to any key loaded in the system.

On the server side we have another problem: control of `authorized_keys` files. As any user can create their own `authorized_key` file, reasonable control is almost impossible. We can control easily only the root user, because it is possible to configure `PermitRootLogin no` in `sshd_config`.

Even though public key authentication is not perfect, by using keys we are protected from brute-force attacks, we are a little more protected from key

loggers using `ssh-agent` and we can use two-factor or three-factor authentication with biometric tokens. On the other hand, we have no centralized control and we have a potential security point of failure in the `ssh-agent` socket file.

Configuring an SSH Public Key Repository with LDAP

If you, like me, are a little paranoid about security and are convinced that the security level is not yet sufficient, you can store public keys inside an LDAP service. I imagine that it is not necessary to tell you about the importance of a good level of security in your LDAP service. You could read my article *Secure OpenLDAP Infrastructure* in Hakin9 Magazine Vol.6 No. 12 (December 2011), for some information about how to start installing and configuring a secure LDAP service.

Note that in this article I will use insecure LDAP, because this is the simplest way to focus only on the LPK patch. My example LDAP server is running on localhost listening on port 389, and the configuration files are located in `/usr/local/etc/openldap`.

First of all, you need to extend LDAP to accept the LPK attributes by copying the schema file from the LPK patch directory to the schema directory of OpenLDAP. In my case, the following command will copy and rename the schema file to the correct place:

```
# cp /usr/src/openssh-5.4p1/openssh-lpk_openldap.schema \
/usr/local/etc/openldap/schema/lpk.schema
```

It is necessary to include the schema in the `slapd.conf` configuration file. Some other schemas are also necessary like `inetorgperson.schema`. An example `slapd.conf` can be started with the content of Listing 4.

We can see that our `lpk.schema` is very simple. Listing 5 shows it.

First, we need to create an `ldif` file with user definitions. Listing 6 shows the definition of user `test2`, with public key stored.

Insert `test2` user in your directory, using `ldapadd`:

```
# ldapadd -D"cn=admin,dc=example,dc=com" -W -f test2.ldif
Enter LDAP Password:
adding new entry „uid=test2,ou=people,dc=example,dc=com“
#
```

Our system needs to know about users stored in LDAP. To achieve this, you need to configure `nss` (name service switch). The following example is a minimal `/etc/ldap.conf`:

Listing 5. *lpk.schema*

```

#
# LDAP Public Key Patch schema for use with openssh-ldappubkey
# Author: Eric AUGE <eau@phear.org>
#
# Based on the proposal of : Mark Ruijter
#

# octetString SYNTAX
attributetype ( 1.3.6.1.4.1.24552.500.1.1.1.13 NAME 'sshPublicKey'
  DESC 'MANDATORY: OpenSSH Public key'
  EQUALITY octetStringMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )

# printableString SYNTAX yes|no
objectclass ( 1.3.6.1.4.1.24552.500.1.1.2.0 NAME 'ldapPublicKey' SUP top AUXILIARY
  DESC 'MANDATORY: OpenSSH LPK objectclass'
  MUST ( sshPublicKey $ uid )
  )

```

Listing 6. *test2.ldif* file

```

dn: uid=test2,ou=people,dc=example,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: posixAccount
objectclass: ldapPublicKey

cn: test2
sn: test2
uid: test2
uidNumber: 200
gidNumber: 200
homeDirectory: /home/test2
sshPublicKey: ssh-rsa AAAAB3NzaC ...public key content... root@localhost

```

Listing 7. *Public Key Authentication test*

```

# ssh test@localhost

# ssh test2@localhost
Last login: Mon Dec 12 23:06:48 2011 from localhost
Could not chdir to home directory /home/test2: No such file or directory
$ id
uid=200(test2) gid=200 groups=200
$

```

```
base dc=example,dc=com
uri ldap://localhost/
nss_base_passwd ou=people,dc=example,dc=com
nss_base_shadow ou=people,dc=example,dc=com
```

Modify `/etc/nsswitch.conf` to include LDAP backends:

```
passwd: compat ldap
shadow: compat ldap
```

To verify that the system is now aware of LDAP users, you can use the `getent` command, like this:

```
# getent passwd test2
test2:*:200:200:test2 :/home/test2:
```

We then need to modify the SSH daemon to look up LDAP keys in the LDAP directory. In `/usr/local/etc/sshd_config`, include the following attributes at the bottom of the file:

```
UseLPK yes
LpkLdapConf /etc/ldap.conf
LpkForceTLS no
```

Restart the SSH daemon for the changes to take effect. Now, test the access:

```
# ssh test2@localhost
Could not chdir to home directory /home/test2:
No such file or directory
$ id
uid=200(test2) gid=200 groups=200
$
```

As you can see, authentication with public keys inside LDAP works. It is also possible to use multiple public keys for the same user. In the way that we configured our system, LDAP is the first source of public keys, but the traditional `authorized_keys` file also works as a fallback. The most secure configuration is to disable `authorized_keys` to make sure that all keys are stored in the LDAP directory.

The SSH daemon has the keyword `AuthorizedKeysFile` pointing to `~/.ssh/authorized_keys` even if this is not explicitly configured, and there is another undocumented keyword named `AuthorizedKeysFile2` pointing to `~/.ssh/authorized_keys2`, used only in protocol version 2.

To make sure that only LDAP is used, we can point these keywords to the `/dev/null` file. Include in `/usr/local/etc/sshd_config` the following lines:

```
AuthorizedKeysFile /dev/null
AuthorizedKeysFile2 /dev/null
```

References

- <http://www.openssh.org>
- <http://www.openldap.org>
- <http://code.google.com/p/openssh-lpk/>

Now, we can verify that authentication runs only when the key is inside LDAP and not with the `authorized_keys` file. Listing 7 shows authentication working only with the LDAP backend.

Conclusions and other possibilities

OpenSSH is very powerful and customizable software. The LPK patch extends OpenSSH in a very important way, enabling OpenSSH authorization to be managed like a service, using LDAP as a backend. Even though in this article we used some insecure configuration, like unencrypted communication with LDAP, it is possible to create a very secure system.

Some other interesting SSH and LPK configurations that I didn't cover in this article, but that I recommend you look at are:

- `ChrootDirectory` – To force users inside specific directories;
- `ForceCommand` – To limit the commands that users can run;
- `Match` – To create blocks of specific definitions (User, Group, Host or Address);
- `LpkFilter` – LPK LDAP filter. You can use this to permit users to access only certain hosts.

Other important configuration options are `LpkBindDN`, `LpkBindPw` and `LpkForceTLS`. These options ensure a minimum level of security when LDAP is accessed.

LPK is a very powerful patch; I hope that the people from the OpenSSH project include this patch in the main distribution soon and more and more people start to use it.

LEONARDO NEVES BERNARDO

Leonardo Neves Bernardo got started with Unix in 1996 when he found this operating system more interesting than any other. For more than fifteen years he worked in several areas of IT, but now is focused on IT security. Leonardo is LPIC-3, LPIC-302 and LPIC-303 certified and holds a Bachelor's degree in Computer Science from Universidade Federal de Santa Catarina, Florianópolis, Santa Catarina, Brazil, as well as RHCT and ITILv3 Foundation certifications. Visit his linkedin profile at: <http://br.linkedin.com/in/leonardoneves>.

CODENAME: SAMURAI SKILLS COURSE



<< Penetration Test Training Samurai Skills >>

- You will learn Real World Hacking Techniques for Targeting , Attacking , Penetrating your target
- Real Live Targets (Websites , Networks , Servers) and some vmware images
- Course Instructors are Real Ethical Hackers With more than 7
- years Experience in Penetration Testing
- ONE Year Support in Forums and Tickets
- Every Month New Videos (Course Updated Regularly)
- Suitable Course Price for ONE Year Support
- Take Our course at your own pace (any time , anywhere)
- Our Course is Totally Different from Other Courses (new Techniques)

20% discount!

Remember the code: NinjaSec007 and save 20% instantly

Cyberwar: Defending a Country

Since the mid-twentieth century to our time, information technology has rapidly evolved. From ENIAC-1, with its' huge size by today's standards to the desktop with next-generation quad-core processors, only fifty years have passed.

What you will learn...

- In this article we will make a brief review of the circumstances of cyberwar, the evolution and impact on national critical infrastructure, and to analyze an idea for improving national security against cyberactions in the field of national critical infrastructure.

What you should know...

- The article is aimed at all audiences, with minimal knowledge of information technology and communications.
-

During this time, with the advent of communication technology like the Internet, information has come to the homes of many people, at the offices of many businesses and offices of many leaders.

The computer has become an indispensable ally in any environment: family, business, social, military, etc, an ally that has allowed the improvement of productivity and potential to levels undreamt of fifty years ago.

In countries with some degree of technological development, information technology and communications may have been transformed into an ally, but also has another reading finer, more subtle, is that we have become dependent, and dependence leads risks.

Cyberwar

One of the tasks of any country is to defend critical infrastructure against internal or external attacks. For this, there are different forces and security forces, both military and civilian related. Civilian security forces are responsible, among other things for the citizen oversight. Cyberwar or war in cyberspace is about hostile actions between countries and stakeholders.

We just have to remember, the attacks carried out from Chinese attackers to Google during its inflexible hostility to the company about the requirements of the Asian country in the search. We might also point out the attacks produced by the group Anonymous against various government web sites, including several

government websites in Spain, and others in Europe and America.

This form of warfare is changing many of the concepts associated with traditional warfare: strategy, tactics, attacks and defenses, some of the issues are being discussed widely in the scenarios designed by countries under such circumstances. Countries are being forced to take action on the issue of protection against hacking, which has been translated in recent years in initiatives aimed at national security.

Current Situation

Virtually all countries have some dependence on technology infrastructure plans or have created plan to act in cases of cyber warfare. Far in the year 2009, Spain created the CNPIC (*National Center for Critical Infrastructure Protection*), whose objective is the response and protection of critical national assets related to cyber attacks, power grids, telecommunications, financial system, etc.

Also during 2010, there was a simulated cyber-attack on the United States, under the premise of the deactivation of the country's electricity networks. It remains curious that one of the world's leading countries in the economic and military, considers that the response to this attack simulation was insufficient, if not a failure. Plans made for contingencies, disaster recovery, detection and prevention of cyber attacks was considered worthless during the simulation.

All this was compounded by the fact that the United States was the first world power to create a fourth army to protect its nation.

The troops are trained in cyber-war tactics and are prepared for battle in cyberspace, and in turn, appoint a military commander as responsible for the fourth army, a cyber-zar, General John Andrews.

National Defense

How can we defend against computer attacks in a country where millions of connections come in and out every minute, with thousands of critical applications and servers throughout its critical infrastructure?

This is the question asked by all government security officials, seeking a solution that minimizes the risks to national critical assets.

The airspace is controlled in countries both by civilian and military control towers. Everyone wants to know who passes through its borders, who flies over its territory, knowing the vehicles and meet the crew.

Why not cyberspace? Cyberspace can be reduced to a series of IP address ranges and communication nodes managed by different national operators.

Through communication nodes, passing packets on TCP/IP with a source IP address, destination IP address and additional information. Packets are routed from source to destination through different communications equipment.

Actually, all the information a country needs to protect their critical infrastructure is there, in the communication nodes of the operators.

At this point is born the idea for the CESEIP, Strategic Center for Monitoring of the IP space. The mission of these centers is monitoring national cyberspace through technological coordination with the various national telecommunications operators and civilian and military agencies.

Building your CESEIP

Strategic Centres for IP Space Monitoring (CESEIP) are configured as an effective solution to the huge amount of cyber attacks against information systems of national critical infrastructures of certain countries.

The first step in establishing a CESEIP is the legal adequacy of the future CESEIP to the law of each country.

It is important that the activities have a place CESEIP within the legislative framework of each nation, a framework that strikes a balance between protection of the fundamental rights of citizens and the need to protect the critical national infrastructure.

This legal adjustment would reduce the pressure of certain social, economic and political agents which may interfere with performance on the premise CESEIP for the protection of fundamental rights.

The second step is to create a confidential list of public IP addresses for critical national infrastructure, which we call Alpha List. This list must be secret, being accessible only to appropriate institutions and individuals. A public Alpha List would be the prelude to an increase in acts of cyber war against that country.

The third step is to configure national communications operators corresponding deviations IP packets whose destination is some of the IP addresses of the Alpha List. All IP packets that manage the communications operator will be duplicated and sent to CESEIP, for monitoring.

Additionally, communications operators should enable a locking through firewall configurations that can allow a particular cut CESEIP transmission of IP packets that may involve an attack on critical infrastructure. Such closures could reduce the effectiveness of certain distributed denial of service attacks.

One of the determining factors to calculate CESEIP infrastructure is often the rate of transmission of IP packets from operators to CESEIP. Are we going to pass each and every one of the packets arriving at Alpha List? Is it only going to take *pictures* every x seconds?

IP packets received by communications operators would be stored in databases CESEIP and interpreted in real-time displays of maps and resources located in a room within the CESEIP 24x7 monitoring.

Attack Detection

The detection of attacks is the main function of CESEIP, in turn, the main difficulty. How to detect a real attack or a false positive?

Detect denial of service attacks or distributed is simple because they would be on the maps of critical infrastructure resources such as hundreds or thousands of connections hit a specific IP address. In this case, it would generate an immediate freezing order to the various operators managing incoming connections.

The problem is to detect possible silent attacks or penetration testing against information systems. One possible solution is to take a preventive screening policy. Before any attack occurs, there is a vulnerability scan to detect faults in the information system that could be used by the attacker. These scans are usually done with popular tools, which usually follow a set pattern in the automation of their actions.

Therefore, the goal is to use scanners to detect background in IP packets arriving at CESEIP, certain strings that use vulnerability scanning tools in their actions.

In this way, we create a blacklist of potential attackers are going to be blocking the communication operators

before running any shares of cyberwar. An interesting formula for a preventive defense.

Infrastructure

The CESEIP must have the necessary infrastructure that can ensure continuity of service, supportive supervision facilities, duplication of communications, support staff, etc..

Regarding human resources, they should be established as an additional public organization, with the limitations of this type of organization, dependent on a higher body related to national intelligence.

A particularly sensitive area within the organization would be the area of institutional relations, responsible for liaising and coordinating with civilian and military agencies. Do not forget that the mission of the CESEIP is the supervision and coordination of the national IP space in relation to national critical infrastructure. This applies to civilian and military alike.

Legal Aspects

One of the most important points to consider in creating the CESEIP is to adapt its activities to the laws and regulations of each country. IP packet interception by the CESEIP can be considered a violation of fundamental rights of citizens, in particular, the right to privacy of information. There are no universal solutions to this problem, which puts us in measuring the balance of national security with respect to the rights of citizenship. It is true that certain countries have made legislative progress in this regard, establishing legal guidelines for the protection of critical infrastructures such as Spain by Law 8/2011, Critical Infrastructure Protection.

One possible formula for limiting access to confidential information from the IP packets, and consequently, to guarantee the fundamental rights of citizenship, is to generate legislative Annexes for that information can not be accessed unless evidenced an attempt to attack national critical infrastructure.

Thus, the CESEIP will at first try the source IP address, destination IP address and other non-confidential information packets. The remaining information will be stored without being accessed.

Finally, we can not forget that much of the information captured by the CESEIP connections will come from outside the country, so in most cases do not apply the fundamental rights of the citizens of the country. For systems using anonymizers like TOR network, this should be explored for each country to legally determine if communication really belongs to the citizen, or the owner of the IP you are using.

Advantages

The advantages of mounting a national CESEIP are diverse, starting with improved monitoring and near real-

time monitoring of cyberspace in relation to information systems of critical national infrastructure.

The storage of IP packets in CESEIP databases also facilitate incident forensics that may occur, including the early detection of attacks by the study of related IP packets and perimeter vulnerability scans.

The CESEIP link with telecommunications operators would avoid undetermined percentage of distributed denial of service, with the option of closing the communications.

Finally, CESEIP infrastructure could be used to incorporate cyber operational units, which act as a counter-measure against potential external threats.

Conclusions

The establishment of a CESEIP can be a decisive step in the protection of information systems related to national critical infrastructure, saving the legal aspects related to the right to privacy and other fundamental rights of citizenship.

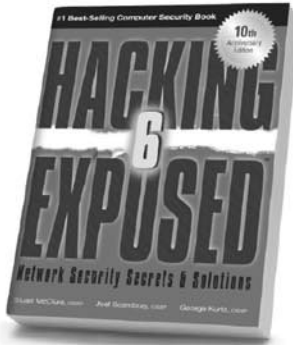
On the other hand, we must not forget that a CESEIP is a need that arises as a consequence of increased stock cyberwar on countries, actions that tend to be aimed at unauthorized access to secret information of the States.

D. DAVID MONTERO ABUJA

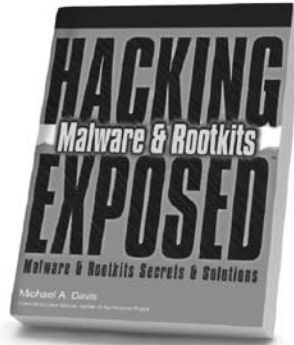
D. David Montero Abuja (1976), aka „Raistlin“ is CISA, CISM and CRISC by ISACA, besides having the only degree awarded ISMS Lead Auditor IRCA in Spain. Andalucía OWASP Chapter Leader and member of the ISO subcommittee JTC1/SC27/WG1 of Spain.

In 2006 he founded the iSoluciones Group, a group of companies specialized in information security, and in 2009 the IP Intrusion company, specializing in ethical hacking, based in Spain, Germany and Uruguay. He can be contacted david.montero@ipintrusion.com.

Stop Hackers in Their Tracks



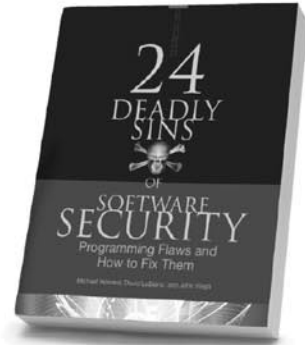
Hacking Exposed,
6th Edition



Hacking Exposed
Malware & Rootkits



Hacking Exposed Computer
Forensics, 2nd Edition



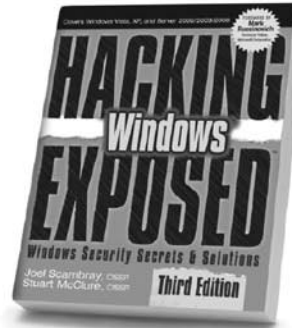
24 Deadly Sins of
Software Security



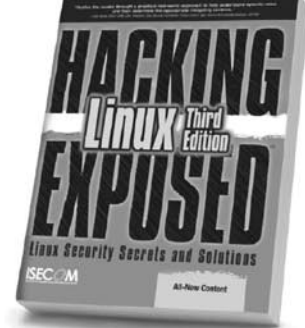
Hacking Exposed Wireless,
2nd Edition



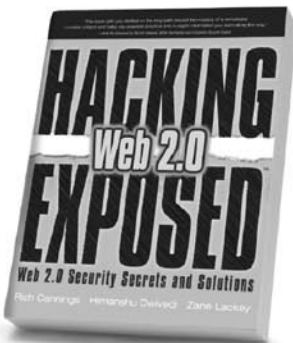
Hacking Exposed:
Web Applications, 3rd Edition



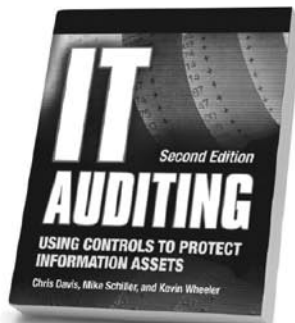
Hacking Exposed Windows,
3rd Edition



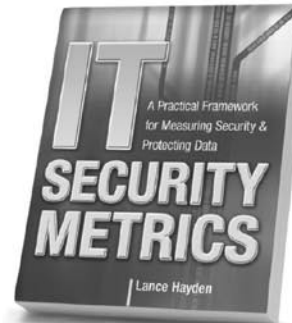
Hacking Exposed Linux,
3rd Edition



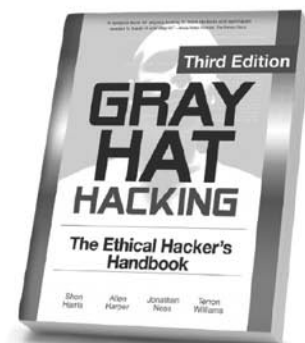
Hacking Exposed Web 2.0



IT Auditing,
2nd Edition



IT Security Metrics



Gray Hat Hacking,
3rd Edition

Available in print and ebook formats

Follow us on Twitter @MHComputing

Learn more.  Do more.
MHPROFESSIONAL.COM

Social Network Security

Part 1 – A Summary of Risks

Social networking platforms such as Facebook or XING aim on collecting huge amounts of personal information about their users. In this first of two articles, we will highlight the risks linked to such social networking sites while the next article will focus on the protection methods which can be applied for enterprises and private users.

What you will learn...

- The risk linked to social networking sites

What you should know...

- No skills required; for beginners
-

In the past, Internet-based attacks on individuals and enterprises were usually accomplished via technical attacks such as those on network communication protocols or on operating system exploits or flaws. Within the past few years, the security community again had to deal with an old type of security threat, namely social engineering. Social engineering is a technique that coerces a user into doing something useful for the attacker (e.g. clicking on a web-link to execute malicious code). Typically, a user is not aware they are acting in favor of the attacker. Social engineering is well known through phishing/online banking attacks but also occurs within social network platforms. Social engineering is a well known problem throughout the ages but problems regarding the privacy protection of Web 2.0, and with it: social networks, led to a renaissance of these social engineering attacks. Besides the purely social engineering aspect of social networking platforms, we will also describe other problems of these social networks. Recently many news and publications came out focusing on the problem of privacy protection, data leakage and other problems associated to the use of social networks. In this article, we provide a summary of these known problems, too.

Reducing an Enterprise's Footprint

Companies can create profile pages within social networks that can usually be *liked* (Facebook) or

followed (Twitter) by the social network's users. However, users are in several cases able (such as on Facebook) to put content in a company's profile and therefore can talk about a company's products and are – in some cases – able to rate these products. Competitors can place bad product evaluations on such profiles and angry users can do the same. However, profile pages are not required to blame a company as shown in the case of *Kentucky Fried Chicken*: A video uploaded to *Youtube.com* showing rats running through a subsidiary of KFC was distributed in a social networking platform and thus resulted in a loss of reputation for some users [1]. On the other hand, angry employees of a company can harm the standing of their employer by posting *status updates*, such as *Oh my god, my boss wants us to put an unfinished software release on our website to satisfy the customers with the stupid new feature*. Other variants of web 2.0-based content contributions are also harmful for enterprises, as shown in a case of the boss of an advertising agency in Stuttgart who posted his political opinion in a social network [2]. Similar problems occur if employees *like* politically incorrect content [3]. Regardless, each company has to take intensive care of their profiles to remove harmful content.

Loss of Confidential Information

A similar problem is the loss of confidential information via social networks. For instance, a user can post *We*

plan to add the new feature for XY support, however, it will still take six months of hard work and I am already damn busy right now to a social networking platform. This message contains potentially confidential information about the planned support. A competitor can then use this information to advance the development of a comparable feature in their product. Of course, the information leakage can be intentional or non-intentional, dependent upon the user's goals. However, it is worth mentioning that the publication of such confidential information due to overt channels such as Facebook is not comparable to covert information transfer using steganographic channels or covert channels [7].

Cyber Mobbing and Loss of Time

In online networks, the inhibition threshold of users is low in comparison to their behavior outside of a social network [5]. This lower threshold can result in cyber mobbing using social networks. Due to the typical linkage of personal friends as well as friends from work, a new problem is envisioned: If the social network's user is mobbed at work, the mobbing can continue within the social networking platform and thus can be adopted by other friends which are actually not colleagues of the person. However, such a scenario is only valid if and as long as the friendships are established.

The loss of work time of employees related to the usage of social networking platforms (be it for cyber mobbing or – what is more likely – for typical social interactions) also results in a loss of money for the employer (approximately one hour per day and employee [4]).

Monitoring

A well-discussed problem is the monitoring of social network users. Besides the fact, that social networking providers know when a user is online, they also know, how long a given user is online and, depending on the IP address, they also know from which location the user accesses the social networking platform or can at least get significant information about the current global area of a user if no anti-trace proxy is used. However, third party applications can obtain the same information by monitoring whether a user is marked as online or not. In case a user publishes his location (e.g. using services such as Facebook places), a third

Acknowledgements

This work is a partial summary of work done by the HSASec security research group (www.hsasec.de) at the University of Applied Sciences in Augsburg. We would like to thank all other contributors for their information retrieval work within the summer school.



[GEEKED AT BIRTH]



You can talk the talk.
Can you walk the walk?

[IT'S IN YOUR DNA]

LEARN:

- | | |
|---------------------------------|-----------------------------------|
| Advancing Computer Science | Network Security |
| Artificial Life Programming | Open Source Technologies |
| Digital Media | Robotics and Embedded Systems |
| Digital Video | Serious Games and Simulation |
| Enterprise Software Development | Strategic Technology Development |
| Game Art and Animation | Technology Forensics |
| Game Design | Technology Product Design |
| Game Programming | Technology Studies |
| Human-Computer Interaction | Virtual Modeling and Design |
| Network Engineering | Web and Social Media Technologies |

www.uat.edu > 877.UAT.GEEK

Please see www.uat.edu/fastfacts for the latest information about degree program performance, placement and costs.

References

- John H. Bell: Corporate Reputation in the Social Age, http://www.yoursocialmediascore.com/downloads/b_repmanagement.pdf [1]
- Politik Digital: Der bezahlbare Ruf, <http://politik-digital.de/der-bezahlbare-ruf> [2]
- Legal Tribune Online: Illoyale Arbeitnehmer – Gefährliches Netzwerken bei Daimler, http://www.lto.de/de/html/nachrichten/3386/illoyale_arbeitnehmer_gefaehrliches_netzwerken_bei_daimler/ [3]
- Marzena Sicking: Facebook & Co verursachen Millionen-Schäden in Unternehmen, <http://www.heise.de/resale/artikel/Facebook-Co-verursachen-Millionen-Schaeden-in-Unternehmen-1251956.html> [4]
- paradisi.de: Online-Kriminalität: Hemmschwelle bei Jugendlichen sehr niedrig, http://www.paradisi.de/Freizeit_und_Erholung/Gesellschaft/Jugendkriminalitaet/News/15987.php [5]
- Andrea König, Chris Nemey: 5 Bedrohungen bei Social Media, <http://www.cio.de/knowledgecenter/security/2277766/index.html> [6]
- Steffen Wendzel, Jörg Keller: Low-attention forwarding for mobile network covert channels, 12th IFIP Communications and Multimedia Security Conference (CMS), Ghent, pp. 122-133, Springer, 2001 [7]
- Saafan: fbpwn – A cross-platform Java based Facebook social engineering framework, <http://code.google.com/p/fbpwn/> [8]

party is able to access this information, too. Thiefs can use this information to detect the absence of users from their home to steal personal objects.

Malware and SPAM

The distribution of malware (viruses etc.) and SPAM is possible through social networking platforms as well. The capability to *like* content eases the content's distribution. For instance, a website containing a funny video but also some malware, can be *liked* by a user. The *like* and the website's abstract is then presented to the user's *friends* who can also click on that link and visit the harmful website. Besides the distribution of malware, phishing attacks and SPAM distribution are possible by weaponizing *likes*. Similar problems are related to the well-established short links (Link shorteners such as *bit.ly* can be used to by attackers to hide the destination of a link [6]).

Identity theft

Identity theft is the discipline of taking over another person's identity. Such a takeover requires as much personal information as possible and thus acquiring this information can be eased by using social networking platforms. Using available personal information, friendships can be established to other persons by spoofing an identity. A thinkable attack in that case is to scan social networking platforms for friends of a person. In this case, one person X

is a friend of person Y in social network A but not in social network B, the attacker can use the information obtained about person X in network A to create a profile for person X in network B. Afterwards, the attacker can use the new profile of X in network B to establish a friendship with person Y. Such a friendship can be used to gain additional personal or even confidential business information. Tools such as *Facebook Pwn* help to establish such fake contacts. Facebook Pwn is a Java framework that automatically sends friend requests and dumps all personal information of a user to the attackers system after a friendship was established [8].

STEFFEN WENZEL

Steffen Wendzel is a Ph.D. student at the University of Hagen as well as a member of the security research group at the University of Applied Sciences (UAS) in Augsburg (HSASec). He received his Diploma (FH) degree from the UAS in Kempten in 2009 and his M.Sc. degree from the UAS in Augsburg in 2011. He is author of a number of books, articles and other publications. His website is <http://www.wendzel.de>.

ROLAND KOCH

Roland Koch is a member of the security research group at the UAS Augsburg. He received his Diploma (FH) degree from the UAS in Kempten in 2009 and currently finishes his Master's degree in computer science at the UAS in Augsburg. His website is <http://www.devko.de>.

Co-Authors of the original document: Gordon T. Rohrmair, Franziska Krün, Benjamin Kahler, Florian Forster, Dominik Heimstädt, Sebastian W. Kraemer, and Patrick Branner

E DETECTIVE



E - Detective®

**Lawful Interception
Network Forensic Analysis
Internet Surveillance
Enterprise Information Security**



Email



Chat



Web



FTP



P2P



VOIP



WebCam



HTTPS/SSL



TELNET



DECISION GROUP INC.

Address : 4/F No.31, Alley 4, Lane 36, Sec. 5, Ming-Shan East Rd, Taipei, Taiwan

Phone : +886 227665753 Fax : +886 227665702

Email : decision@decision.com.tw

Website : www.edecision4u.com

Social Network Security

Part 2 – Fencing the Risks

This article provides a summary of how to deal with the security aspects of social networks.

What you will learn...

- How to deal with the security aspects of social networks

What you should know...

- No skills required; for beginners
-

Social networking platforms such as Facebook or XING aim at collecting huge amounts of personal information about their users. In this second of two articles, we will highlight the risks linked to such social networking sites while the first article focused on the protection means which can be applied for enterprises and private users.

Introduction

To deal with problems caused by social networks, the first idea of enterprises for handling these risks is to simply block social networking sites. However, blocking such sites is linked to disadvantages. Blocking will not only cause morale issues, but also prevent employees from participating in discussions outside of the companies' walls. In your private life, blocking these sites may help you to stay productive and prevent your children from registering under the required age of 13 at Facebook. However, the appropriate way to handle issues with social networks in corporate environments is to increase the awareness of employees. Porsche blocks Facebook to prevent the company from data loss porschefb [1]. This might sound paranoid, but just these days there are reports about the CIA watching Twitter tweets as well as Facebook status updates ciatwitter [2].

Your Personal Security Aspect

If you use a social network, you should always consider which information you share and with whom

you share them. The main principle should always be that less sharing of private information is better. You cannot see where your data is stored and who will be able to read it in the end. Therefore it is not recommended to trust any social network provider. If you get private messages or contact requests, the most critical task is to verify these in the real life. By simply viewing a photo and a description you cannot verify that the virtual person is actually your friend. If messages contain critical topics, consider contacting the person by telephone.

On Facebook, there are a lot of so-called *apps* which request access to your profile. This also happens on websites that use Facebook for their authentication. You should always read the permissions the application requests and consider if the application really needs them. Just accepting these permissions can lead to full access to your and your friends' private information, whether you are using this application right now or not. For your account security you should use (as for every other service) a strong password that includes letters, numbers and special characters. You should also use a unique password for each social network, to prevent that if an attacker knows one, he cannot use it for your other accounts. Of course you should also never share your password or use your account information to log into other sites. If other sites request this information, it will most certainly be an attempt to steal it.

One of the latest attacks on user privacy was based on the fact, that most people use the same email addresses on all social networks attackprivacy [3]. To prevent to be hit by this, try to use a unique email for each network.

Handling Social Networks in Enterprise Environments

Blocking social network sites in a company environment is quite simple to apply by using adequate proxy or firewall settings. However in most cases, this doesn't make sense because there is always a way around these means and the employees will use the platforms also in their spare time. This private usage can affect your company but you cannot forbid it.

It is very important to teach employees the risks of social networks. Moreover not only the employees but also their families have to be made aware of the risks. If the wife of a security manager writes on Facebook that next month she is on holiday with her husband, this could be useful information for attackers.

There are companies around that provide training, but it can mostly be performed internally in the company. The required information is available on the Internet for free. We recommend interactive training, not just providing some information material because this is likely to be ignored. Interactive training (e.g. securing your personal profile in Facebook by modifying the settings) is a much more effective way to teach your employees. It is always important not to focus on personal security issues only, but also to explain potential risks for the company (cf. Article 1: S. Wendzel, R. Koch: *Social Network Security, Part 1 – A Summary of Risks*).

Policies

For every company, a social network policy must be created. A policy helps to explain the risks that can arise by interacting with social networks. A policy should not be a list of forbidden things, but an explanation why some actions can cause serious damage for the company. You can find sample policies on smpol [5], a database with 178 policies of known companies. Because the Internet is a fast changing world, these policies have to be updated regularly. Therefore, the awareness training must be done regularly (e.g. annually).

An example for a company with a recommendable policy is IBM. This policy not only includes guidance

Acknowledgements

This work is a partial summary of work done by the HSASec security research group (www.hsasec.de) at the University of Applied Sciences in Augsburg. We would like to thank all other contributors for their information retrieval work within the summer school.



[GEEKED AT BIRTH]



You can talk the talk.
Can you walk the walk?
Here's a chance to prove it.

[IT'S IN YOUR PULSE]

LEARN:

Advancing Computer Science
Artificial Life Programming
Digital Media
Digital Video
Enterprise Software Development
Game Art and Animation
Game Design
Game Programming
Human-Computer Interaction
Network Engineering

Network Security
Open Source Technologies
Robotics and Embedded Systems
Serious Games and Simulation
Strategic Technology Development
Technology Forensics
Technology Product Design
Technology Studies
Virtual Modeling and Design
Web and Social Media Technologies

www.uat.edu > 877.UAT.GEEK

References

- [Porscheffb] Porsche Curbs Facebook `Threat,' Shields Itself Against Spying, <http://www.bloomberg.com/news/2010-10-11/porsche-curbs-facebook-threat-shields-itself-against-spying.html> [1]
- [ciatwitter] AP Exclusive: CIA following Twitter, Facebook, <http://news.yahoo.com/ap-exclusive-cia-following-twitter-facebook-081055316.html> [2]
- [attackprivacy] Attacking the Privacy of Social Network Users, Marco Balduzzi, HITB SecConf 2011, Kuala Lumpur, Malaysia – 11-13/10/11 [3]
- [ibmguidel] IBM Social Computing Guidelines, <http://www.ibm.com/blogs/zz/en/guidelines.html> [4]
- [smpol] Social Media Policy Database, <http://socialmediagovernance.com/policies.php> [5]
- [bbcpol] Social Networking, Microblogs and other Third Party Websites: Personal Use, <http://www.bbc.co.uk/guidelines/editorialguidelines/page/guidance-blogs-personal-summary> [6]
- [intelpol] Intel Social Media Guidelines, <http://www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html> [7]

for the company but also for the employees ibmguidel [4]. The authors advise the employees to take part in social networks to find new ideas, but also show the legal aspects and risks in company and private usage. This guideline is updated regularly, to include new trends in technology. The IBM policy also includes notice that all information that is put on the Internet will be visible for a long time and is nearly impossible to get deleted. It also informs SN users that sharing material should cover with legal rights and copyright. If employees discuss topics that are directly related to IBM, they should declare that they are employees of IBM, if needed also with the position in the company. However, the employees should also declare that they are posting their own opinion, i.e. they are not speaking for the whole company. Of course, the policy forbids the sharing of confidential information and the quotation of business partners without their acceptance. The policy moreover covers that you should not publish emotional or even insulting messages on the Internet. Employees should also not talk about political topics. The policy of the BBC for example includes the point: *The personal use of the internet by BBC staff must be tempered by an awareness of the potential conflicts that may arise* bbcpol [6]. Last, but not least, there is one important aspect included in Intel's: *Always pause and think before posting* intelpol [7].

There are no standards available for handling the social networks in cooperate environments. But the

availability of the mentioned guidelines of well-known companies shows that they are already aware of social networking security aspects.

STEFFEN WENZEL

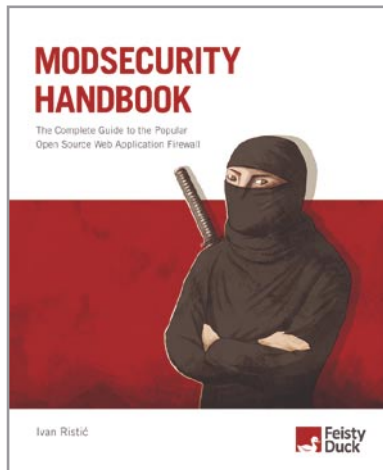
Steffen Wendzel is a Ph.D. student at the University of Hagen as well as a member of the security research group at the University of Applied Sciences (UAS) in Augsburg (HSASec). He received his Diploma (FH) degree from the UAS in Kempten in 2009 and his M.Sc. degree from the UAS in Augsburg in 2011. He is author of a number of books, articles and other publications. His website is <http://www.wendzel.de>.

ROLAND KOCH

Roland Koch is a member of the security research group at the UAS Augsburg. He received his Diploma (FH) degree from the UAS in Kempten in 2009 and currently finishes his Master's degree in computer science at the UAS in Augsburg. His website is <http://www.devko.de>.

Co-Authors of the original document: Gordon T. Rohrmair, Franziska Krün, Benjamin Kahler, Florian Forster, Dominik Heimstädt, Sebastian W. Kraemer, and Patrick Branner

Special Promotion on Selected Security Titles from Feisty Duck!



45% off
code **HAKIN9MS**

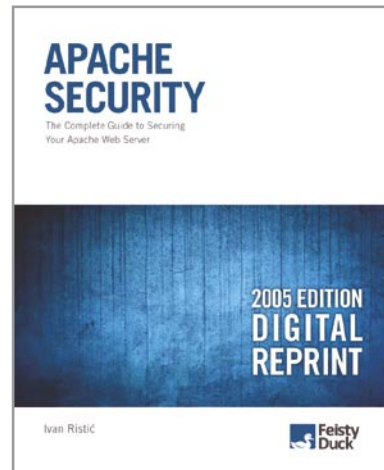


“A book that will provide answers to security issues you may not have realized exist.”

Mike Weber, Beginlinux.com

“All you need to harden your web presence with ModSecurity is at your fingertips.”

Russ McRee, holisticinfosec.org



60% off
code **HAKIN9AS**



“The single best Apache security book in print.”

Richard Bejtlich, author of *The Tao of Network Security Monitoring* and *Extrusion Detection*

“Everyone running Apache needs this book.”

Rich Bowen, author of *Apache Administrator's Handbook* and coauthor of *Apache Cookbook*

www.feistyduck.com

Our books are available in paperback and a variety of digital formats: **PDF, Mobi, EPUB, and online. No DRM.** The above discount codes will provide you with additional 20% off our current prices. The total discount will be approximately 45% for purchases of *ModSecurity Handbook* and 60% for purchases of *Apache Security*.



The Most Dangerous Attack Of Them All

Sep 2011 – Turkish hackers attacked NetNames DNS records and changed entries redirecting users of The Telegraph, NGC and Acer to a site set up by them.

Aug 2011 – Hacker steals records from Nokia Developer Site.

Jun 2011 – PBS was hacked.

Jun 2011 – Hactivist Lulzsec were accused of stealing coupons, downloading keys and passwords that were stored in plaintext on Sony's website.

Apr 2011 – Barracuda Networks were compromised.

Mar 2011 – Official homepage of MySQL was compromised.

Nov 2010 – The British Royal Navy was compromised.

The above attacks look as if they were very sophisticated in nature. After all the Royal Navy, MySQL, Sony, Barracuda all of these are government/ corporate websites with extensive security measures built in them. It would require a very high level of expertise to get around their firewall/IDS etc. It would require extensive knowledge of the various tools involved in the different phases of the attack. But what if I were to tell you that all it requires is simple knowledge of SQL and a web browser. How is it possible? Read on.

What you will learn...

- What is SQL Injection
- Different types of SQL Injection
- How to protect from SQL Injection
- Real Time Examples

What you should know...

- Basics of SQL
- Basics of Internet
- That's it

All the attacks above use a very simple technique known as SQL Injection. SQL injection is an attack in which a website's security is compromised by inserting a SQL Query in the website which performs operations on the underlying database.

These operations are unintended by the website's designer and are usually malicious in nature. Attackers take advantage of the fact that designers usually take SQL commands having parameters which are user supplied. The attacker instead of providing the normal

user parameter inputs his SQL query which runs against the backend database. Let us go through an example. Consider a website which has a login page. The user enters his username and password on the login page. The underlying database query might look like this

```
$sql_query = „select * from users where user='$user' and password='$pass'”
```

Now if the attacker enters admin' or '1'='1' the query will change to

```
$sql_query = „select * from users where user='admin' or '1'='1' and password='$pass'”
```

The attacker will now bypass the login page. This is due to the fact that the query will always return true because of the OR condition. This is a very basic SQL injection. Another type of SQL injection can be performed on the URL of the website itself. Suppose the URL of the website is like this.

```
www.baddeveloper.com/index.php?id=17
```

The underlying SQL statement might be something like

```
Select something from table where id = 17
```

Now if we add OR 1 = 1 the query will convert to

```
Select something from table where id = 17 or 1 = 1
```

which will display all that is present in the something column. Sometimes we deliberately insert a dummy character so as to create a syntax error. If the website doesn't have proper error handling measures then it will display an error message which will give out information on the type of database running, the table present, the column name etc. This information can be leveraged to launch successful attacks.

Types Of SQL Injection

Poorly Filtered Strings

This type of SQL injection occurs when the user input is not filtered for any escape characters. For example in the below code:

```
$pass = $_GET['pass'];  
$password = mysql_query(„SELECT password FROM users  
WHERE password = '$pass'”);
```

Now if the attacker enters ' OR 1 = 1 /*. The query changes to

```
SELECT password FROM users WHERE password = '  
OR 1 = 1 /*
```

The query will return true every time thus allowing a user to bypass the authentication. It's similar to the example we saw earlier.

Incorrect Type Handling

This type of SQL injection occurs when a user supplied field is not checked for any type constraint. This could happen when there is a field which should have been an integer but the developer has not enforced it. For example:

```
statement := „SELECT * FROM userinfo WHERE id = „ +  
a_variable + „”
```

In the above example id is of type integer. The user enters 1;DROP TABLE users. The query then changes to

```
SELECT * FROM userinfo WHERE id=1;DROP TABLE users;
```

Signature Evasion

Many SQL injections will be blocked to some extent by intrusion detection and intrusion prevention systems. These systems are not fool proof and their signatures can be bypassed. One method in which we can do this is to encode the input differently. Consider once again the URL

```
www.baddeveloper.com/index.php?id=17
```

An IDS/IPS might be able to detect or 1 = 1. But if we encode it like OR+1%3D1 the signatures of IDS/IPS might be thwarted.

Blind SQL Injection

Most of the websites which have good defences set up will not allow error messages to be displayed. If there is any error it will be redirected to a standard error page. In such cases when we cannot glean any information from the error message we have to fallback to blind SQL injection. In some cases there will be slight changes. An unsuccessful injection might redirect the attacker to the standard error page. A successful injection might display a blank page. Usually it's a matter of patience and skill before you can successfully blind inject a website.

Mitigation

The mitigation for SQL injection is fairly simple. Makes you wonder why it's not followed. Well that's life. The main techniques by which you can protect from it is by using Parameterized queries or by Escaping.

Parameterized Queries

In most cases instead of accepting the user input directly we can force the user input to be entered as

parameters. For example in the below query:

```
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'x' OR full_name LIKE '%Bob%';
```

The above code is already injected. But if we code it like below.

```
SqlConnection conn = new SqlConnection(_connectionString);
conn.Open();
string s = „SELECT email, passwd, login_id, full_name „ +
„FROM members WHERE email = @email“;
SqlCommand cmd = new SqlCommand(s);
cmd.Parameters.Add(„@email“, email);
SqlDataReader reader = cmd.ExecuteReader();
```

Now if you put try to inject code in this by typing OR full_name LIKE %Bob%, it will be treated as a string in the parameter @email. There will be no query executed with injected SQL. By using parameterized

query the query will actually search in the table for a string which has OR full_name LIKE '%Bob%!

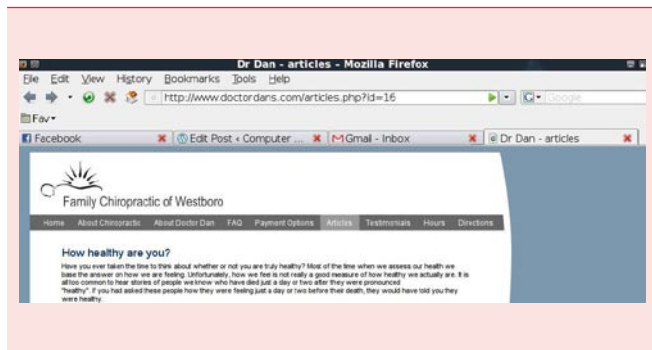
Escaping

Another technique is by escaping the characters which have a special meaning. For example the occurrence of a single quote ' can be escaped by placing another quote before it " to form a valid string. In PHP, we can use the function mysql_real_escape_string() which escapes all special characters.

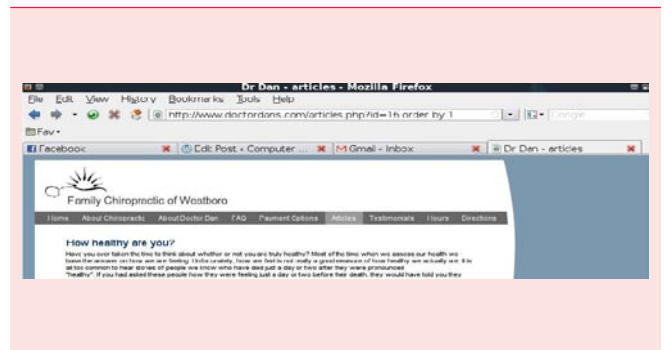
```
$query = sprintf(„SELECT * FROM `Users` WHERE
UserName='%s' AND Password='%s'“,
mysql_real_escape_string($Username),
mysql_real_escape_string($Password));
mysql_query($query);
```

The function sanitizes the data before sending it to the database.

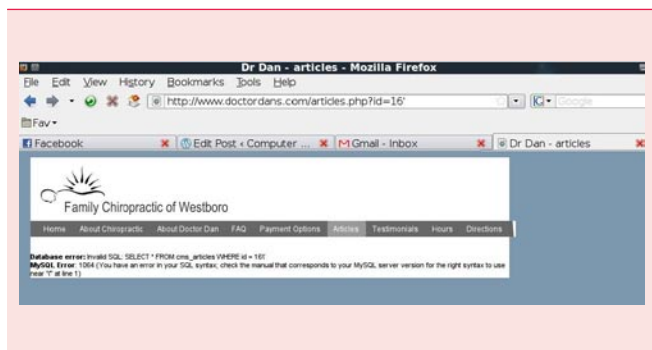
And Now For Some Real Time Examples !!!



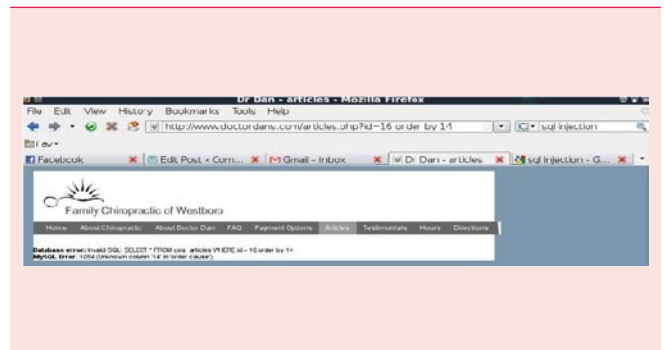
01 First we identify a vulnerable website.



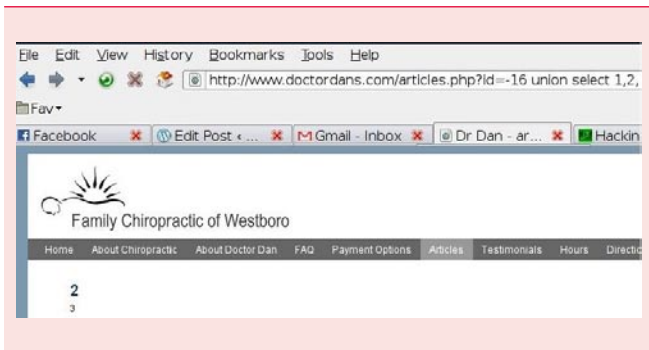
03 Next we try to get the number of columns in the table by giving an order by followed by 1 then 2 and so on...



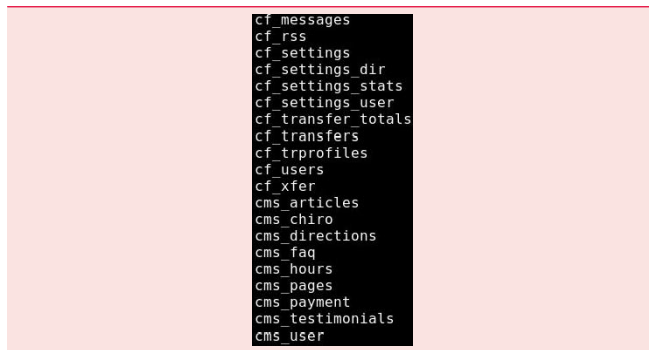
02 The we get information about the database and tables by forcing an error



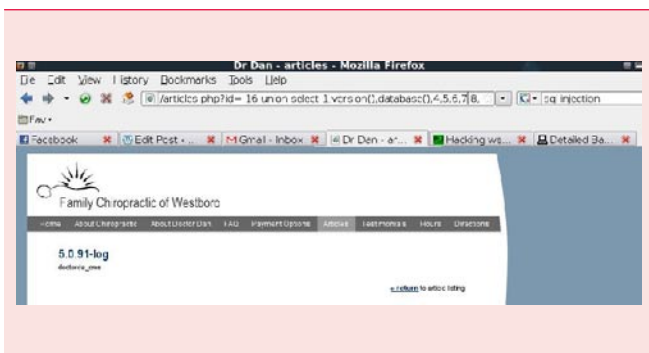
04 Since there are no errors, we keep on increasing the number in the order by statement till we get an error. We got an error when did an order by 14. That means we are trying to order column number 14 but there is no column 14. So that means we have a total of 13 columns.



05 Next we try to find out which columns can be displayed in the website by giving all the column numbers in the URL.



08 The tables



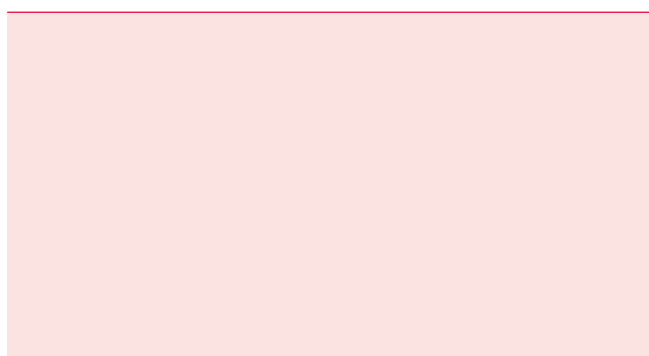
06 Now in place of those column numbers we add `database(), version()` we enter the below info.



09 Next we dump the data in the cms_user table by giving the `--dumps` parameter.



07 Then we use a tool called sqlmap to get all the tables in the database. Below is the command.



10 Viola we have email, username and a hashed version of the password which can be cracked to give the real password.

Let's Go Through Another Example



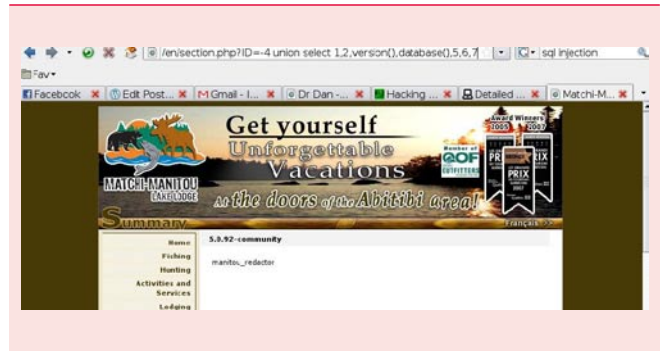
01 Another website



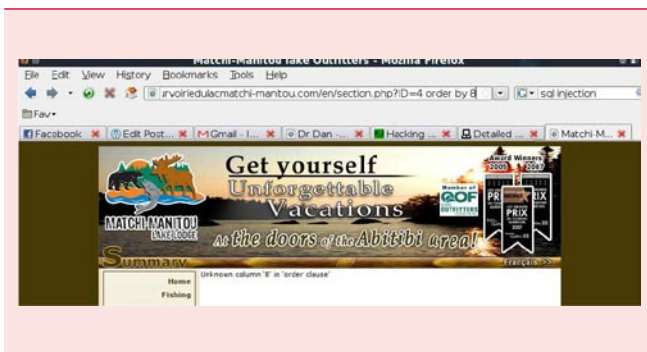
04 Get the viewable columns



02 The error



05 Database name and version



03 Get the number of columns



06 Get the tables

References

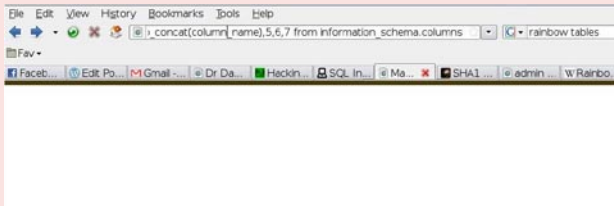
- http://www.imperva.com/resources/glossary/sql_injection.html
- http://en.wikipedia.org/wiki/SQL_injection
- <http://www.greensql.com/articles/backdoor-webserver-using-mysql-sql-injection>
- http://hakistan.com/index.php/SQL_Injection#SQL_Injection_Types
- <http://www.codinghorror.com/blog/2005/04/give-me-parameterized-sql-or-give-me-death.html>

Join

hakin9 team!



07 Get the columns in the table



08 Get the login and password



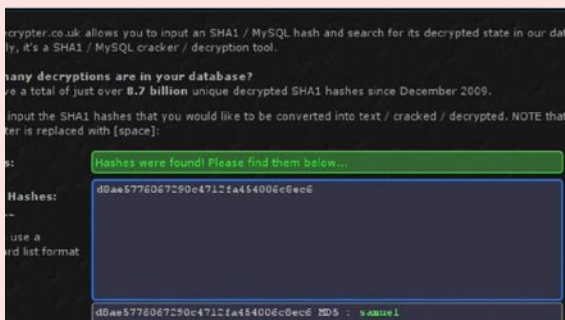
If you would like to help our team in creating hakin9 magazine you can join our authors or betatesters today!

All you need to do, is to send an email to:

editors@hakin9.org

and give us a brief description of your field of interest.

09 Run the hash through a hash cracker and you have the password



GAUTAM

My name is Gautam. I work as a Software Engineer. While I'm not writing SQL queries, I keep myself busy in the world of computer and network security. You can catch me on facebook at www.facebook.com/companynetsec or at my blog <http://computerandnetworksecurity.wordpress.com>



We look forward to hearing from you!

Why

Can't Online Banking Be Like Facebook?

In my last column, we talked about some of the problems of pricing information security. This month, we look at a practical application of some of the challenges – specifically around online banking.

What you will learn...

- How badly designed legislation can affect consumers
- Why online banking, and the approaches to security around it, can evolve only slowly
- Why online banking can never have the same look and feel as social media

What you should know...

- A little bit of economics

The *digital native* is a concept that has been talked about in education circles for a number of years now, meaning a person who is used to interacting with institutions and other key parts of life mainly online. The concept is very much a reality, and is here to stay. These individuals are likely to be relatively highly educated, with a higher-than average earnings potential. One recently-graduated Harvard MBA of my acquaintance had pictures of his first born child on his Facebook page less than an hour after delivery. It is very easy to keep track of the activities of my brother-in-law, a respected professional in his innovative employer. The more-or-less unexpurgated set of his exploits can be found on not only, of course, Facebook, Linked-In, and a professional blog or two, but also on Vimeo, Flickr, the music press, and naturally, his own web pages. A recent study by an online advertising provider indicated that something in the order of 26.2% of time online at work is spent on things on personal activities, that the youngest age segment (18-34) spent the highest proportion of time online (c.34.4%), and that only 28.5% of employees of any age feel guilty about personal use of the internet at work. The key points here are that, firstly, where these early adopters lead, others are likely to follow, and secondly, the line between personal and business online presence are increasingly indistinct.

The first generation of true *digital natives* are starting to enter the workplace – individuals who manage and showcase their lives on line. Not only are these technology-

literate individuals used to, even dependent on, portals such as Facebook, Orkut, Tumblr, and their ilk, they are both drawn to novelty and intolerant of homogenizing, externally imposed modes of organising their affairs. This potentially poses consumer financial services businesses with an interesting conundrum: the user experience of online banking and related services are, in large part, dictated by the concerns of the business and their regulators, rather than those of the consumer. Layer on this a more richly populated, diverse financial services market, and an interesting picture begins to emerge. The basic premise of this essay is that the market for online banking is severely distorted by a range of uncostered externalities, creating perverse incentives. The opportunities include the effective pricing of these externalities, and changing the value proposition of the service offering. Revised regulation could act as a critical enabler. Taking the Facebook model, this is suggestive of a certain core set of characteristics that one might expect to see in online customer interaction with financial services optimised for the digital native customer. This list might include:

- Flexibility – ready accessibility, with minimal barriers to the consumer experience
- Extensible functionality – can be expanded beyond the initial offering
- A *viral* element to the offering's growth model
- Strong branding- the consumer experience includes feeling part of the brand, rather than simply

- Consumer ability to publicise private achievement, if so desired (e.g. the ability to flex the privacy settings of one's Facebook account).

It is true that a number of retail banks have considered, at various points, account aggregation portals – i.e. a one-stop online shop for an individual's interaction with multiple accounts and other financial products spread across a number of banks. It is also true that various flexible, scalable, micro-finance providers exist – notably Zopa (<http://uk.zopa.com/ZopaWeb>), and also Prosper and Smava. Yet, none of these fully embody all the five characteristics laid out above. So, why doesn't online banking look like Facebook? It could be argued that the rollout of online banking is a very good exposition of an economic model known as Selten's Chainstore Paradox, albeit with the strength of deterrence to new entrants evaporating over time. One could also argue that the introduction of various sorts of service enhancement, such as Two Factor Authentication, conform to a similar model. However, there is also an argument that this throws into sharp relief the number of market failures around online banking. The customer can more readily switch allegiances than ever before (viz rate-driven credit card switching, an very common phenomenon in the UK). Customers place little value on security per se, which they see as the responsibility of the financial service provider – however, they expect their funds to be secure. In other words, lack of appropriately tangible costing of information security is a cause of market failure. The nature of the security measures around online banking are dictated in part by regulation, and in part by the deterrence value of externalities such as negative press coverage. In the UK, at least, the legal responsibility for maintaining their online facility securely resides ultimately with the customer.

Other developments loom on the horizon – the EU is currently considering new legislation for use against organisations which lose customer data, for example. This could see fines levied against them of up to 5% of global turnover. This is clearly a serious potential problem if you are in a sector which is operating in a troubled market, and have a history of data loss (as many banks do). The legislation is still in draft, and may be subject to change; however, if you were a bank's chief executive, would it make you want to hand more control to your customers, or less? Therefore the customer is forced to conform to a user experience model which they did not choose, which does not speak to the characteristics they value, and which holds the possibility of punishing them should the service delivery model fail. This, one could argue, is not rational. So, given a raft of challenges, what opportunities might spring from them? Laying aside the possibility of radical regulatory change, these might fall into two main streams, which may be complementary: Market segmentation and Changing the value proposition.

Dealing briefly with the first of these, at present, a UK online banking customer can be held responsible if, through lack of care on their part their account details are compromised. To restate this, if I, as a customer, do not have a personal firewall or up-to-date anti-virus software on my home PC, that PC is infected by one of a number of types of virus or related malware, and the contents of my accounts are siphoned off to a criminal party, then liability is mine. Yet, making sure that the security on my PC is appropriate is not entirely incentivised. At the same time, the provider of my online banking will bear costs associated with my behaviour. So, why not reward me for behaving appropriately, by providing different levels of security, which the customer can consciously choose and be charged for? In terms of the factors behind the success of social networking site uptake, are there not some elements that could be incorporated? Would an online banking service have higher cachet if it was invitation only, for example? Might there not be a market for some sort of comparative status rating in such a community – some sort of financial health monitor, perhaps, in a crude form based on the relative proportions of income and outgoings? Could this not be used to increase the number of user interactions in a day, for example, in much the same way that status updates, new pictures, and so on drive user interaction with social networking sites? However, returning once again to the Chainstore Paradox, in this scenario there is a massive deterrent effect – failure would be the source of considerable opprobrium.

In conclusion, there are a number of reasons why, historically, online banking has not mirrored the growth model and user experience of the more popular social networking sites, but this represents a set of incompletely explored possibilities. An essential precondition for the successful exploitation of these possibilities is the internalisation of a key externality (information security). This in turn could be facilitated by a concerted effort to accurately price information security – current pricing models, such as the Information Security Forum's ROSI may not be adequately robust for this task. Given the dynamics of the market, this could be a powerful tool in influencing an overhaul of the pertinent regulatory regimes, in order to more closely align the service provider and customers' incentives. In other words, it's pretty clear that the profession of information security needs to do some serious thinking if it is to do what it has long said it was capable of – acting as a business enabler, rather than the people who like to say *No*.

DRAKE

Drake has worked on information security and strategy with government agencies, the military, financial institutions and other blue chip organisations in Europe, the Middle East, and Africa since Boris Yeltsin was President.

Secure your DNS

Do you trust your ISP's DNS setup? I don't! DNS is susceptible to attack by malicious entities to target innocent victims just like any other protocol. The solution is to engage OpenDNS as your trusted DNS service which is harnessed by home and enterprise networks globally.

Configure your home network to utilise *OpenDNS* by entering both `208.67.222.222` and `208.67.220.220` into your home router configuration menu. You are now routing all your *DNS* queries to *OpenDNS*.

OpenDNS also offers security protection to its users. Register for an account with *OpenDNS*. Login and click on *Settings* then click on *ADD THIS NETWORK*.

Give your network a name and click on the existing IP to access the *Web Content Filtering* section. Customise your filtering by selecting the categories that you wish to block and clicking on *Apply*. One unique feature that *OpenDNS* offers is correction of incorrectly typed Domain names. *Enable dynamic IP update* to ensure your address is always mapped with your profile. Their website offers *Windows* and *Mac OS X* clients for download to support this. I installed an open source *Linux IP updater* software called *ddclient* on *Ubuntu 10.04 LTS* using the following command.

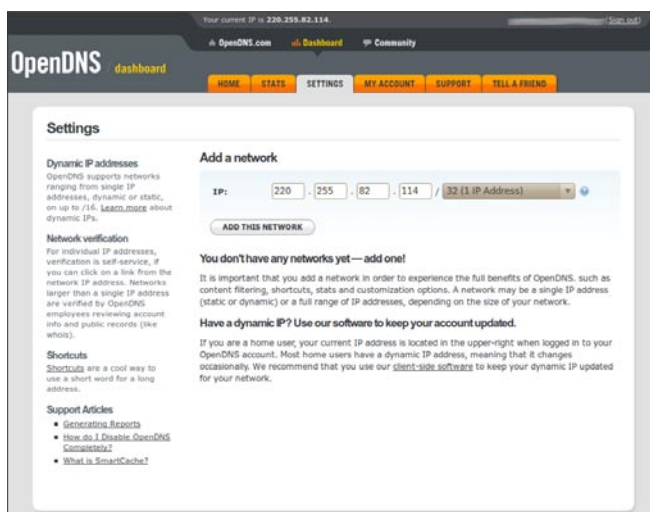


Figure 1. Add network

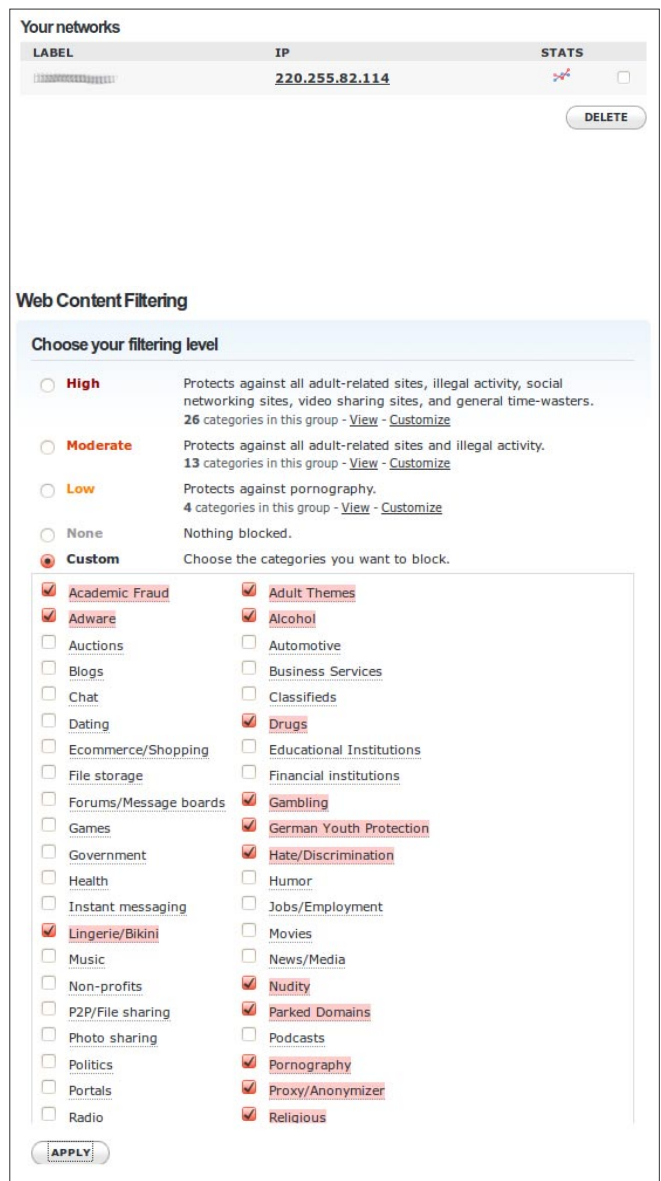


Figure 2. Web Content Filtering

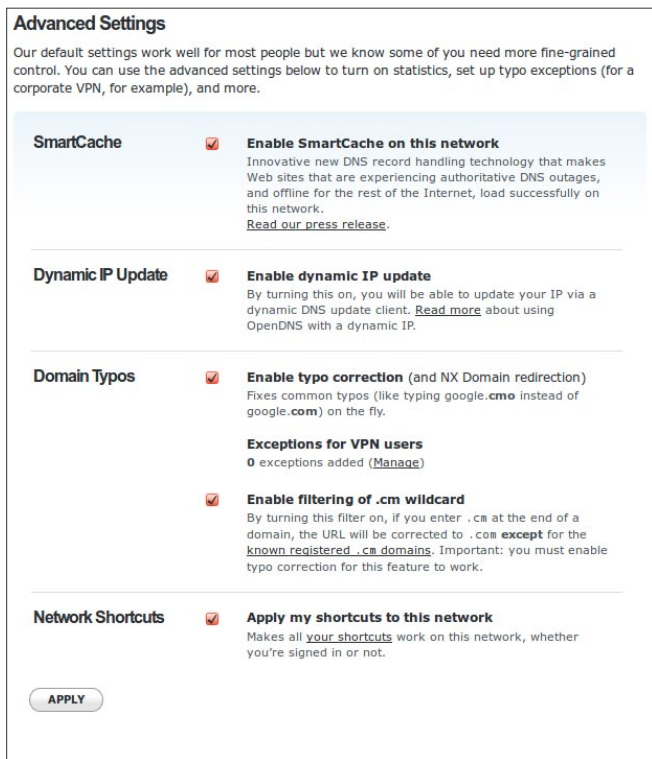


Figure 3. Advanced Settings

```
commandrine@bridge:~$ sudo apt-get install ddclient
```

Edit `/etc/ddclient.conf` to include your *OpenDNS* account name, password and network label highlighted by the square brackets.

```
# Configuration file for ddclient generated by debconf
#
# /etc/ddclient.conf
use=web, web=myip.dnsomatic.com
ssl=yes
server=updates.opendns.com
```

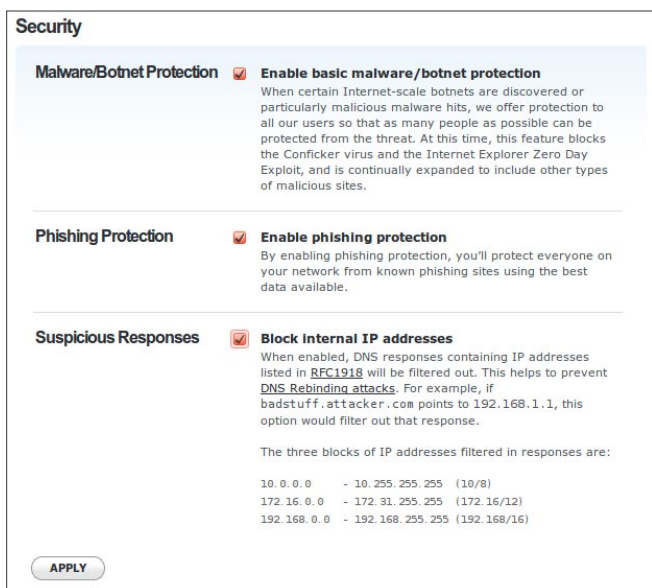


Figure 4. Security

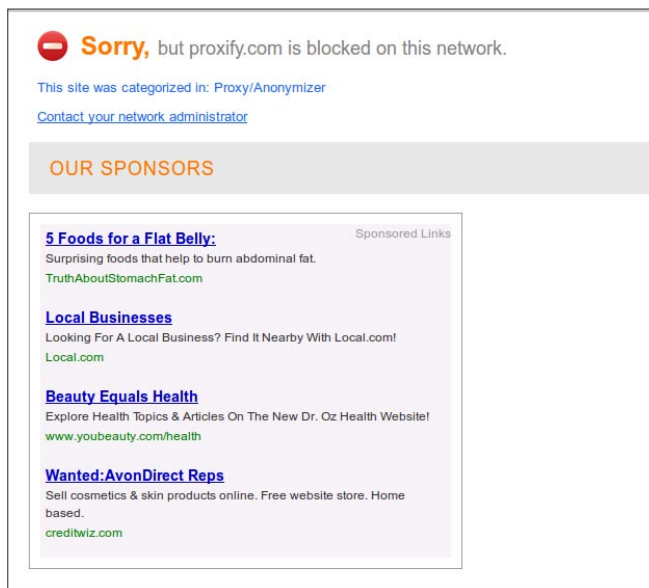


Figure 5. Block page

```
protocol=dyndns2
login=[USERID]
password=' [PASSWORD] '
[OPENDNS_NETWORK_LABEL]
```

Restart the client to ensure that the software is running and that your *IP* address is updated to *OpenDNS*.

```
commandrine@bridge:~$ ./ddclientrestart.sh

ddclient restarting

* Restarting Dynamic DNS service update utility
                               ddclient                               [ OK ]

SUCCESS: updating opendns_network_label: good: IP
                               address set to xx.xx.xx.xx
```

Access the *Security* section. Enable all features for your own protection.

Test your new settings by accessing an *Anonymous Proxy* site for example. Undesirable and malicious sites are now blocked by *OpenDNS* as defined in your settings.

Utilising this service does not require you to install a server or modify your existing infrastructure. The only caveat is that it takes time for new configurations or changes applied to take effect. *OpenDNS* is free for home use and worth considering for your enterprise. What are you waiting for?

MERVYN HENG

Mervyn Heng is into Ubuntu, Comic Universe characters, Pop culture and Art outside of Information Security. If you have any comments or queries, please contact him at commandrine@gmail.com.

Interview With

Gord Boyce

CEO at ForeScout Technologies



Gord, your company survived the early NAC vendor shakeup and NAC is more mainstream with demand in the last couple of years accelerating. To what do you attribute the increased market demand?

The early *Network Access Control* (NAC) market did see a lot of consolidation and failures. Early vendors promised more than they delivered in terms of functionality and deployment ease. Many of those products required managing different components and replacing infrastructure, with results sometimes disrupting users from doing work. So the cost and impact was greater than the expected benefits. Network Access Control has definitely matured since then, but so have the reasons for why organizations are buying.

Enforcing authenticated access and facilitating guest networking are still common NAC drivers. But companies are now looking at ways to manage the risks of personal and mobile devices on their network – the IT consumerization issue is a challenge that is finding most customers playing catch up. Given increased network dynamics and connectivity, and the velocity of new attacks, companies are also seeking ways to converge endpoint, network and identity intelligence so that they can improve how quickly and efficiently teams can respond to security issues, if not prevent threats in the first place. NAC can support these initiatives.

What do you attribute your company's ability to take advantage of these NAC trends?

Early on, ForeScout was an *Intrusion Prevention Systems* (IPS) company who had developed some very innovative technologies that identified malicious network and application behavior to stop threats without relying on signatures. This product, CounterACT Edge, still prevents a good majority of today's zero day attacks and targeted threats – the product has a great following. But soon after, we entered the NAC market with our IPS heritage and evolved our CounterACT platform to meet various NAC customer requirements and environments, leveraging our IPS technology and networking expertise.

We incorporate network-based infrastructure discovery, traffic monitoring and endpoint fingerprinting teamed with a strong policy engine and flexible means to take actions. As a result, we have an agentless, non-disruptive and highly interoperable approach that really gives us a competitive advantage in our space. More importantly, CounterACT solves a variety of security problems and enables real business benefits for our customers. That said, I feel our biggest asset is the zeal at which our developers and employees work with customers to get things right and meet requirements.

What is CounterACT and what can organizations benefit from that platform?

CounterACT is our flagship product that, as an automated security control platform, serves four major security categories. Obviously, we are a leader in Network Access Control, but we also provide mobile security, endpoint compliance and threat prevention. When our appliance is placed in a corporate network, CounterACT enables real-time visibility and control capabilities for medium and large organizations.

Our customers are using CounterACT to apply uniform rules across their enterprise to limit or block access to network resources based on user, device, time and location attributes; to enable guest networking; to identify and classify known and unknown devices; to find and even fix endpoint security violations; and to stop malicious actions and attacks. And it does so working with our customers' existing infrastructure.

The value of automating these controls is bottom line cost savings and operational efficiency. For example, many of our customers start off with processes around access, endpoint compliance and guest networking. They can use 802.1x, non-802.1x or both as methods for controlling network access. They often first build out policies around required endpoint configuration and security client software. Policies can start in monitoring mode and then move to stronger enforcement – this way a set of policies can be phased in and exceptions can be managed proactively. The same is true for guest networking where our system provides the mechanisms to register and limit guest access.

Often we are brought in to address one or two critical problems or initiatives. Soon after, organizations see broader application and value. Many of our more progressive customers take advantage of our real-time monitoring, enforcement and remediation capabilities – essentially lowering helpdesk calls and more manual security incident response.

What are some of the advantages and disadvantages of automating solutions over an experienced security team supervising the function?

That's a great question, as companies aren't searching on Google for an automated security control platform – though they would find us. From a tactical viewpoint, they want to solve a security issue or meet compliance requisites. But our platform's capabilities does lend itself to allow network and security operations to do more. It's a powerful platform. There are some that shudder when they hear the words *security automation*. But organizations are already doing this – when they apply firewall rules, activate anti-virus, invoke encryption gateways or set VM zoning, for example.

It's not about putting a tool ahead of experienced security teams, but it is about how to optimize security

operations, which is a valued and expensive resource. It is also about coping with the sheer number and volume of threats that exceed human processing capacity. There are certain security scenarios that are black and white – you don't want the attack or violation to occur. So you are relying on your security team's experience to define policies in order to enable defenses to react faster and fix problems with little helpdesk and IT intervention where possible.

The disadvantages of automation could be working through policy exceptions, interfacing with different operations, tracking activity, and potential business disruption – but these are manageable. It is a matter of building out the controls and responses. What is not simple is being able to actually extend more dynamic and granular controls across the entire enterprise. For what we provide, our platform approach is proven and I believe there is more that ForeScout can offer.

The advantage, by operationalizing security, is risk reduction and increased savings. In some respects, CounterACT offers job enrichment because we free up the experienced security team to focus on more interesting initiatives, processes and issues.

With Bring Your Own Device (BYOD) commonplace in various organizations, what are some of the major security threats that are introduced to the work culture and how can organizations respond?

BYOD and mobile security are two huge issues that our clients and prospects are working on. Organizations need to embrace the fact that their employees are using personal mobile devices at work – these devices are already on the corporate network, possibly taking advantage of existing credentials. Companies want to realize productivity and connectivity gains of such devices but not at the expense of security. The threats right now are less about mobile malware (although there is certainly potential), but more about data leakage, phishing and privacy.

Organizations need to assess technologies that will allow them to segregate personal from corporate information and network access – but that's more likely for corporate-managed devices. On unmanaged devices, companies need to be able to identify these smartphones, netbooks and tablets, and have a roles-based, non-intrusive way to enable appropriate access to either the Internet or specific network resources. ForeScout offers many of these capabilities today where we can enforce policy for managed and unmanaged, wired and wireless devices, as well as monitoring for post connect threats. With regards to BYOD and securing personal devices, this has to be handled in a manner that is legal and acceptable to end users.

Since ForeScout is a global company, what are some of the regulatory and compliance laws that you have to deal with outside USA?

Our customers know that any product by itself does not let an organization be compliant, but, instead, it is the combination of policies, processes and technologies which help support meeting privacy and other compliance mandates. For example, one of our customers was looking at how to assure wireless network scanning and elimination of rogue wireless access points across multiple sites to support PCI. Another customer wanted to add a layer of protection to segregate and monitor user access to cardholder data. We were able to quickly support these requirements with controls and reports. These customers were able to use our built-in policies and implement enforcement with no change to their environment; even if the network between multiple sites is different.

Other regulatory requirements can involve how ForeScout complies to security standards. For example, our appliance needed to be FIPS certified to support many financial institutions. On the government side, CounterACT recently achieved Common Criteria EAL 4+ status, the highest level for a NAC solution, which was required by ForeScout to support government and military installations seeking to satisfy a variety of endpoint and access control mandates.

As a CEO, what kind of questions do you face when you interact with new clients? What are some of the top areas they need help with?

When I meet customers, it is often with more senior IT and security executives, and not always the staff actually operating our product. Senior IT members are more involved with establishing a more strategic dialogue beyond what might be the specific project. They inquire about our support, corporate stability, futures and how to design policies to enable proactive defenses. Discussions seem to be more about operations rather than just compliance. The majority of clients are extremely focused on lowering costs and managing risk so they ask about product usability and how well you will be able to support new devices, or ways to manage new types of threats. We have gained a great deal of product insight by listening to our customers.

So as a pure-play NAC vendor, how do you contend with larger vendors that offer broader suites of product?

NAC products must be usable out of the box, easily managed, flexible to meet different security scenarios, and scalable – not all are. To be competitive, our products must be highly extensible, have a lower overall cost of ownership, and offer more assured

implementation versus that of larger incumbents. As a pure-play vendor, you are also forced to support a broader range of infrastructure products and to be vendor agnostic.

We have to fully leverage our customer's existing network, security and process investments. Every customer has at least something with a vendor that we compete with. As you can imagine, while we compete with Cisco and Juniper for NAC, we need to support their network and security devices so our deployment is seamless.

When you're a broad-based vendor, you typically focus on roadmaps that support selling more product and assume a more homogenous customer environment. You also have significant legacy product support that can affect the speed at which you can deliver new and customer-requested features. We've gained decent industry visibility, but we are not yet a household name in the data center. However, when prospects compare us to the larger vendors in terms of architecture, technical merit and our means to be responsive, and to support a customer's evolving requirements – we compete quite effectively.

You mention infrastructure interoperability. In terms of the security eco-system, what are the more interesting industry partnerships that provide customer's more value than either product alone?

I have two answers. First, is how we can protect a customer's security investments. CounterACT identifies and assesses devices in real-time and we support the majority of popular endpoint protection products such as anti-virus. We have found that as much as 30% of client security tools have conflicts, are out-of-date, removed or deactivated – and incorrectly reported. We have the means to fix many of these issues as background processes.

More recently, we have been extending the value of CounterACT by integrating with other vendors' offerings, such as helpdesk, systems management and security management. Our product supports the SIEM (*Security Information Event Management*) and *Common Event Format* (CEF), for example. We can send our security event data to products such as HP ArcSight and Nitro Security (now McAfee). With ArcSight, we offer added capabilities where we can send real-time endpoint configuration details to ArcSight. ArcSight can also use their correlation engine to send commands to ForeScout CounterACT to take action such as to block an attacker, quarantine malicious systems or re-activate a security agent. We anticipate opening up our platform to enable other products to obtain CounterACT's real-time visibility and control functions.

Does ForeScout offer any solutions in the virtualization and Cloud computing space?

Our family of appliances is also available as virtual appliances. You might think that as soon as we announced the availability of a virtual appliance that it would immediately outsell physical appliances. There certainly are datacenter consolidation advantages, but at the same time, many IT organizations remain more comfortable with the plug-and-play physical appliance.

Both our physical and virtual models are identical and even our management appliance can support a mixed physical and virtual environment. Our virtual appliance models offer more deployment flexibility since customers can more readily obtain and provision VM images and licenses using their own hardware. And we offer the means for virtual appliance licenses to be upgraded, which you can't do with a fixed physical model.

More recently, we announced packaging of our virtual appliances to support cloud computing in terms of a NAC as a Service platform. We needed to satisfy customers seeking to offset capital expenditures and outsource security expertise. If you take a look at our platform being integrated, interoperable, vendor agnostic, non-disruptive, scalable – and virtual – that really offers a service provider a solid means to deliver NAC as a hosted or managed service. We had received quite a few inquiries to support managed service providers and actually had a few large accounts in North America already using CounterACT through a managed service delivered by a few partners.

We had a proven implementation, but we really didn't fully package NAC for the services market. We now offer our authorized service provider partners a subscription license and the means to quickly adjust licenses to better serve their clients. This provides for rapid deployment, monthly billing, on-demand scaling and marketing support for our partners to offer our solution as a hosted or managed service for customers that want a service option.

Having started in sales, then moving into a chief operating officer position – and ultimately a CEO position – for our entrepreneurial readers who want to take the helm of their own security business, what advice would you offer them in this economy?

Be sure you have a solution that provides demonstrable results in terms of not only risk reduction, but also operational savings. In a tough economy, people buy aspirin, and hold off on vitamins. As a start up, outstanding support is as equally important as outstanding product. Ultimately, you want to forge a relationship with every strategic customer and partner so you can learn how to improve your product or

service, understand where the market is heading, and gain referrals to grow your business in conjunction with conventional selling and marketing.

ForeScout has made visible strides in the Network Access Control space. Tell us a little about what the future holds for ForeScout?

It is exciting times for ForeScout and we are growing. We are very mindful to continue to invest in our platform to assure our customers, partners and prospects that they will continue to receive best-in-class functionality, support and services. Beyond NAC, which is core to our business, we also have identified ways to bring our value to mobile and cloud environments. Our platform closes operational gaps by bridging what are often blind or silo'd management areas that affect security. We see an opportunity to empower security operations to gain visibility and control over what is surely an extended, borderless network for both managed and unmanaged devices with greater user, network, security posture and application context.

About ForeScout Technologies, Inc.

ForeScout enables its customers to unleash the full power of their network through enterprise-class security and control. ForeScout's automated solutions for network access control, mobile security, threat prevention and endpoint compliance empower organizations to gain access agility while preempting risks and eliminating remediation costs. Because security solutions are easy to deploy, unobtrusive, intelligent and scalable, they have been chosen by more than 1,000 of the world's most secure enterprises and military installations for global deployments spanning 37 countries. Headquartered in Cupertino, California, ForeScout delivers its solutions through its network of authorized partners worldwide. Learn more at www.forescout.com.



Taking On Mobile & Wireless **Security**

TAKEDOWNCON

LAS VEGAS | 2011

Training: Dec 2 - 5

Conference: Dec 6 - 7

Las Vegas, M Resort



www.takedowncon.com

Is your
MISSION-CRITICAL
security strong enough
to stop a
SKILLED ATTACKER?

Don't guess
Don't believe
Don't hope

KNOW!



An ACROS Penetration Test is **conducted exactly like a real attack by a skilled, motivated adversary** – only without the damage. We will find the weakest links in your security and use all our knowledge, skills and capabilities to try to achieve exactly what your security measures and policies are there to prevent. If it sounds difficult, we're interested.

Experience **the ultimate test of your security.**
(After all, the only alternative is to wait for an actual attack.)