

ON Hacking Demand

Vol.1 No.3
Issue 03/2012(3) ISSN: 1733-7186

PEN DRIVES SECURITY

THE GUIDE TO BACKTRACK

Special
Publication:
100
+pages

ANDROID EXPLOITATION WITH METASPLOIT
BACKTRACKING IN WIFI COUNTRY
DEFENDING LAYER 2 ATTACKS
HOW EXPOSED TO HACKERS IS THE
WORDPRESS WEBSITE YOU BUILT?

PLUS

BACKTRACK 5
TOOLKIT TUTORIAL



OFFENSIVE[®] security

www.offensive-security.com

**“If there’s no pain,
it’s probably not
Offensive Security”**

**For extreme live and online Penetration Testing Courses,
visit <http://www.offsec.com>**

THE LEADERS IN
INFORMATION SECURITY TRAINING



CRACK HACK FORUM

CHF is regarded as one of the best online hacking community with over 76k+ members.

CHF was created by a renowned hacker and web specialist named **ProVirus**.

-CHF-

- CHF has over 2k+ tutorials teaching you the very art of hacking from the very basic to the most advanced level.
- Has a special forum for cracked premium accounts worth thousands of dollars.
- The VIP section is filled with the tools and tutorials unseen elsewhere making the section unique.

Join CHF NOW!!!

www.CrackHackForum.com

**JOIN
NOW**

Greetings to: Srinuboy, Terrorbyte, Rain112, Hacker4life, Rynaldo, Mschoudhry, fakhr0

ON Hacking Demand team

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

Managing: Pawel Plocki
pawel.plocki@software.com.pl

Editorial Advisory Board: Board: Rebecca Wynn,
Mat Jonkman, Donald Iverson, Michael Munt, Gary S. Milefsky,
Julian Evans, Aby Rao

Proofreaders: Michael Munt, Patrik Gange, Jeffrey Smith,
Donald Iverson, Jonathan Edwards

Betatesters: Amit Chugh, Mohamed Alami,
Marouan BELLIOUM, mohamed ouamer, M.Younas Imran, Julio
Hernandez-Castro, Tom Updegrove, Jeff Smith,
Jonathan Ringler, Peter Hoinville, Antonio Domenico Saporita,
Keith D., Rissone Ruggero, Shayne Cardwell, Kiran Vangaveti,
Khaled Masmoudi, Tahir Saleem, Ivan Burke, Eduardo Montano,
Jake Sopher, Dan Walsh, Daniel Sligar, Kashif Aftab,
Tim Thorniley, Kyriakos Bitopoulos

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

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@hakin9.org

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


Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@hakin9.org

DTP: Ireneusz Pogroszewski

Marketing Director: Pawel Plocki
pawel.plocki@software.com.pl

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,

Our current edition takes up a subject of the most known IT security
program – BackTrack 5. This professional programme provides users
with easy access to a comprehensive and large collection of security-
related tools ranging from port scanners to password crackers. Thanks
to co-operation with BackTrack Creators and the group of professional
specialists, who decided to write specific articles for us, we were able
to close all the BT's toolkits and possibilities in one publication. This full
of security tools program, has been perfectly described from different
points of view and that gave us an excellent effect which is expanded
below.

Looking through the articles you'll find a few thematic sections
which present the author's work.

Metasploit Section includes three different attitudes to this area
of expertising. Aditya Gupta presents a practical BackTrack 5 usage
and shows us Android Exploitation through Metasploit. Johan Loos
presents some security vulnerabilities which, according to the author,
„can be used to exploit a system”.

Nayan Sanchania shows us how to protect a personal PC from
various kinds of exploits which can attack private data or even
security systems in the multinational corporations. Steve Myers
and Nicholas Popovich open for us a BackTrack Toolkit and show a
plenty of techniques which you can find during exploring this program.
WordPress, free and open source blogging tool and a dynamic
management system is precisely described by Alex Kah, a specialist
interested in Pentesting. The author presents the website framework
as a place for millions of people who should be prepared for new and
beyond attac from the Network.

Dusko Pijetlovis, an experienced IT security specialist, reveals a
Pentesting presentation about practical BT 5 usage. Moreover, one
can learn how to find the specific tools which help us making a perfect
scanning.

A huge tutorial about the most popular BackTrack tools was created
by Vikas Kumar. He shows us its possibilities via step by step articles
and he teaches how quickly and operationally work with them.

Dennis King shows the power hidden in BackTrack 5. Having
known what an experienced hacker can possibly do with this machine
of immeasurable possibilities, we can finally effectively take care of our
computer.

Pawel Plocki
and Hakin9 Team



[GEEKED AT BIRTH.]

PWR: 110%

[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 Game and Simulation
Strategic Technology Development
Technology Forensics
Technology Product Design
Technology Studies
Virtual Modeling and Design
Web and Social Media Technologies



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

www.uat.edu > 877.UAT.GEEK

METASPLOIT

Android Exploitation with Metasploit 08

by Aditya Gupta

In this article, we will be looking into the practical usage of Backtrack, and its tools. The article is divided into three sections – Android Exploitation through Metasploit, Nikto Vulnerability Scanner and w3af. The reader is expected to have basic knowledge of Backtrack and familiar with common web application vulnerabilities.

Use Metasploit in Backtrack 5 16

by Johan Loos

Metasploit comes in several flavors: Metasploit framework, Metasploit community edition, Metasploit pro. In Backtrack 5, Metasploit framework is installed by default. Metasploit framework provides you with information on security vulnerabilities which can be used to exploit a system. Penetration testers can also use this tool to launch manual or automated scans.

BACKTRACK5 TOOLKIT

TUTORIAL

BackTrack 5 Toolkit Tutorial 22

by Vikas Kumar

BackTrack is an operating system based on the Ubuntu GNU/Linux distribution aimed at digital forensics and penetration testing use. It is named after backtracking, a search algorithm. The current version is BackTrack 5, code name “Revolution.”

DEFENCE PATTERN

Defending Layer 2 Attacks 44

by Nayan Sanchania

Security has been a major concern in today’s computer networks. There has been various exploits of attacks against companies, many of the attacks cost companies their reputation and cost them millions of pounds. Many attacks are implemented using inside knowledge from previous and even current employees.

OPERATIVE BACKTRACK

BackTrack 5: The Ultimate Security Toolkit 60

by Steve Myers

In the security world today, a security professional relies heavily on knowing the right tools for the job, and knowing how to use these tools. There are hundreds of tools available and the list of tools is constantly changing and growing. For security assessments and penetration testing, there are very few toolkits as actively supported and all-encompassing as BackTrack 5.

Backtrack 5 Practical Applications And Use Cases 66

by Nicholas Popovich

This article breaks down what Backtrack Linux is, with a brief description and history. Then, we’ll explore a sampling of some of the many tools that are packaged within Backtrack Linux and provide use cases along with step-by-step tutorials to demonstrate some of the more common tasks that Backtrack is used to perform. Finally, we’ll see how most of the tools and techniques that Backtrack is designed to facilitate can be used by the many different roles in the IT security field.

EXPLORE YOUR PC How Exposed To Hackers Is the WordPress Website You Built? 76

by Alex Kah

WordPress is likely the most popular website framework used on the web today. With over 65 million downloads and a very active community you can accomplish many goals with ease using WordPress.

Become Quieter with a Little Help from BT 82

by Dusko Pijetlovic

When you are faced with a task of testing your production environment and strengthening your defenses, your choice of the tool is easy. Instead of concentrating on collecting penetration (pen) testing tools, just head to BackTrack website and download an image of one of the most popular white hat penetration testing and security auditing platforms. It’s #7 on the sectools.org Top 125 Security Tools list.

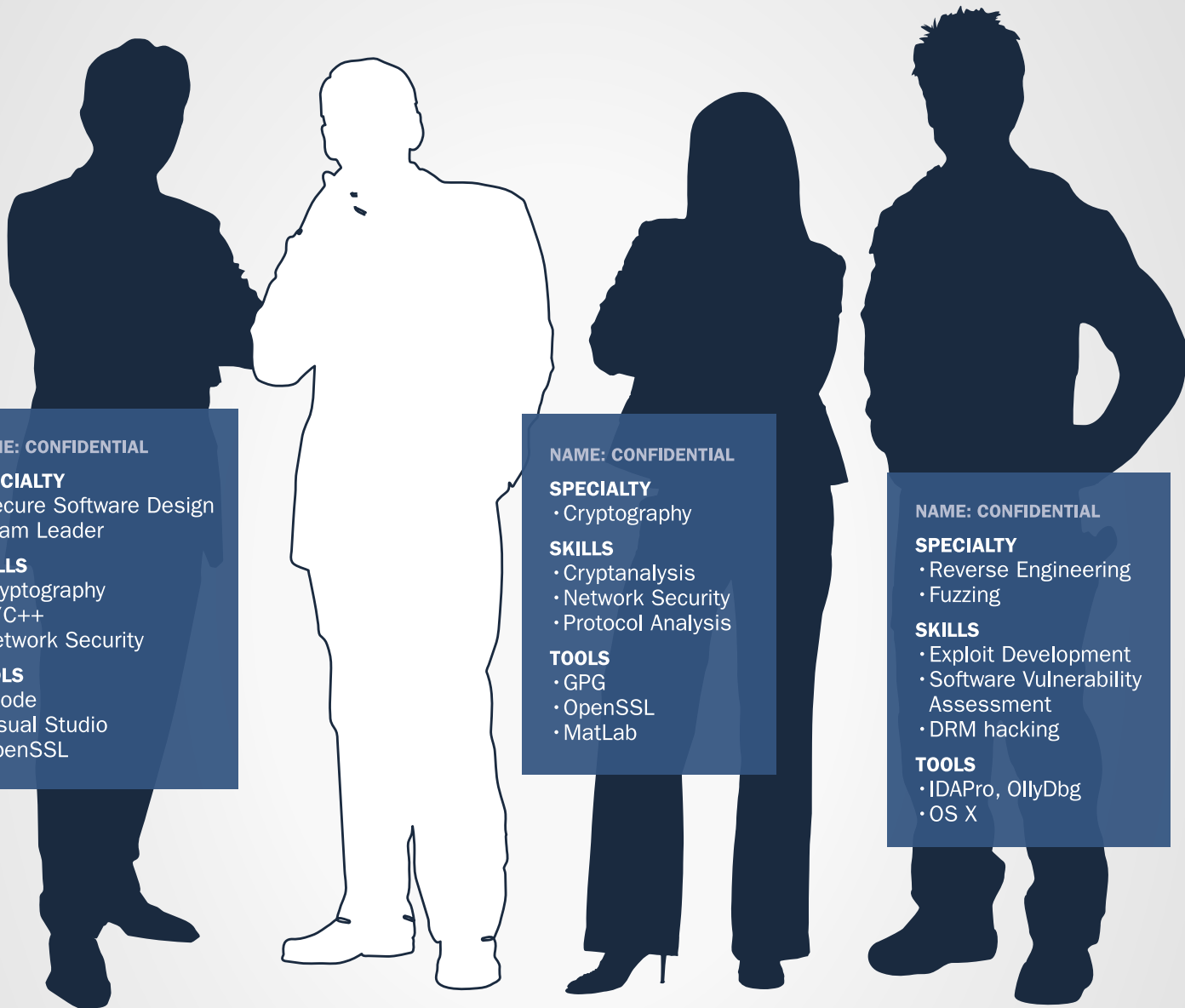
BackTracking in Wifi Country 92

by Dennis King

The BackTrack 5 distribution continues to be the “go to” tool in a security professional’s arsenal. With the latest release, “Revolution,” the Backtrack development team delivers a kit you can use anywhere on both light and heavy duty security tasks.

WE'RE BUILDING AN A-TEAM.

Have what it takes?



NAME: CONFIDENTIAL

SPECIALTY

- Secure Software Design
- Team Leader

SKILLS

- Cryptography
- C/C++
- Network Security

TOOLS

- Xcode
- Visual Studio
- OpenSSL

NAME: CONFIDENTIAL

SPECIALTY

- Cryptography

SKILLS

- Cryptanalysis
- Network Security
- Protocol Analysis

TOOLS

- GPG
- OpenSSL
- MatLab

NAME: CONFIDENTIAL

SPECIALTY

- Reverse Engineering
- Fuzzing

SKILLS

- Exploit Development
- Software Vulnerability Assessment
- DRM hacking

TOOLS

- IDAPro, OllyDbg
- OS X

NOW HIRING PREMIUM CYBER TALENT

4901 Springarden Drive | Suite 200 | Baltimore, MD 21209
www.securityevaluators.com | 443.270.2296

CAREERS@SECURITYEVALUATORS.COM



ISE is a white-hat security consulting firm that helps great companies protect their great customers.

Android Exploitation with Metasploit

In this article, we will be looking into the practical usage of Backtrack, and its tools. The article is divided into three sections – Android Exploitation through Metasploit, Nikto Vulnerability Scanner and w3af. The reader is expected to have basic knowledge of Backtrack and familiar with common web application vulnerabilities.

The Metasploit Framework is well known tool among Penetration Testers and InfoSec professionals. It could be used for a variety of purposes and against a variety of targets.

In this article, we will discuss a lesser known module in the Metasploit Framework, which could be used to steal any file from an Android phone, given; it navigates to the attacker's URL.

This vulnerability was discovered by Thomas Cannon in 2010, which leverage a Content:// URI multiple disclosure.

Now, let's go ahead and run the exploit in Metasploit.

Usage

The prerequisite to run this exploit is the victim phone must be running Android 2.3.4 or less, and should be

rooted, in case you want to get system files. Open up the Metasploit Framework, by typing in msfconsole (Figure 1).

```
root@bt:~# msfconsole
msf > search android
```

Right now, only two android modules are present in the Metasploit Framework (Listing 1).

We are here interested in the first module, which is android_htmlfileprovider. Let's have more information about this exploit (Listing 2).

To use this exploit:

```
msf > use auxiliary/gather/android_htmlfileprovider
```

```
msf > use auxiliary/gather/android_htmlfileprovider
msf auxiliary(android_htmlfileprovider) > set SRVHOST 10.0.53.75
SRVHOST => 10.0.53.75
msf auxiliary(android_htmlfileprovider) > set SRVPORT 80
SRVPORT => 80
msf auxiliary(android_htmlfileprovider) > set URIPATH /angrybirds
URIPATH => /angrybirds
msf auxiliary(android_htmlfileprovider) > █
```

```
msf > search android
Matching Modules
=====
Name                               Disclosure Date  Rank   Description
----
auxiliary/gather/android_htmlfileprovider  normal  Android Content Provider File Disclosure
auxiliary/scanner/sip/sipdroid_ext_enum    normal  SIPDroid Extension Grabber
msf >
```

Figure 1. Android modules in Metasploit

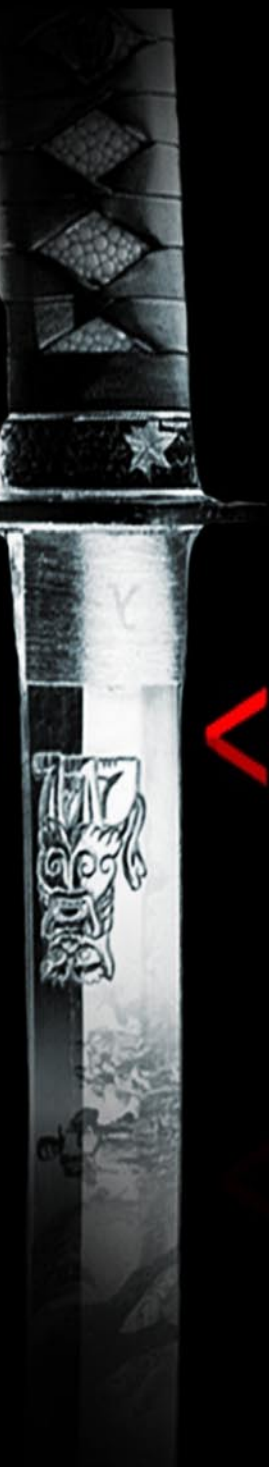
Figure 2. Setting up the options for Android exploit

Listing 1. Matching modules

```
Matching Modules
=====

Name                               Rank   Description
----
auxiliary/gather/android_htmlfileprovider  normal  Android Content Provider File Disclosure
auxiliary/scanner/sip/sipdroid_ext_enum    normal  SIPDroid Extension Grabber
```


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 , any where)
- Our Course is Totally Different from Other Courses (new Techniques)

We have Real World Hacking/Penetration Testing Lab with Over 20 Real Target

Use Metasploit in Backtrack 5

Metasploit comes in several flavors: Metasploit framework, Metasploit community edition, Metasploit pro. In Backtrack 5, Metasploit framework is installed by default. Metasploit framework provides you with information on security vulnerabilities which can be used to exploit a system. Penetration testers can also use this tool to launch manual or automated scans.

Before you actually could exploit a system, you need to know if the system is vulnerable for a certain type of attack.

What is a vulnerable system?

A vulnerability is a weakness in software, hardware that enables the attacker to compromise the confidentiality, integrity or availability of that system. A system can be but not limited to: a server running an operating system, router switch, firewall, mobile devices, TV, etc. For example: when an attacker launches a distributed denial of service attack, he enables the unavailability of a system. If data is intercepted and changed, he enables integrity.

An attacker can use a vulnerability to compromise a system. For example a weakness in a protocol allows the attacker to run arbitrary code.

The attacker launches the exploit on the vulnerable system. Based on the actual payload send together with the exploit, the attacker receives a (reverse) shell.

If you understand the vulnerability, it will help you to implement the appropriate security control. A security control can be a patch or a security device.

Important to know is that you understand the vulnerability context:

- Where do they exist?
- Where do they run?

So, what is the exploit context?

- Exploit runs where the vulnerability exists
- Where does it run, client side or server side?

Example 1

Let say, you have a server located into the DMZ. The vulnerability context is the server itself and the exploit context is the DMZ. If an attacker can compromise a vulnerable server in the DMZ, he has properly access to all servers in that DMZ. The attacker can use other techniques like pivoting to access servers in the internal network.

Example 2

If a client computer is placed on a client LAN, the vulnerability context is the client and the exploit context is the client LAN. If an attacker can compromise a vulnerable client in the LAN, he has properly access to all resources on the client LAN.

Client-side exploit

If a vulnerability exist on a client, it can be compromised by a client-side exploit. Client side vulnerabilities lives in Java, operating system, applications such as web browser, Office, Acrobat Reader. The attack is basically launched by tricking the user to click on a link embedded in an email, or send the user an attachment which contains the exploit. When the user clicks on the link, the user is redirected to a website which contains the actual code to launch the exploit. A traditional firewall does not help this attack from happening, since the user opens a connection over port 443 or port 80. These ports are usually allowed on the firewall. Before a system can be exploited, you can take the following steps:

- Choose and configure the module in Metasploit
- Select a payload, which provides the attacker a remote shell

BackTrack 5 Toolkit Tutorial

BackTrack is an operating system based on the Ubuntu GNU/Linux distribution aimed at digital forensics and penetration testing use. It is named after backtracking, a search algorithm. The current version is BackTrack 5, code name „Revolution.“

Support for Live CD and Live USB functionality allows users to boot BackTrack directly from portable media without requiring installation.

though permanent installation to hard disk is also an option. BackTrack includes many well known security tools including:



Figure 1. *Linux View*

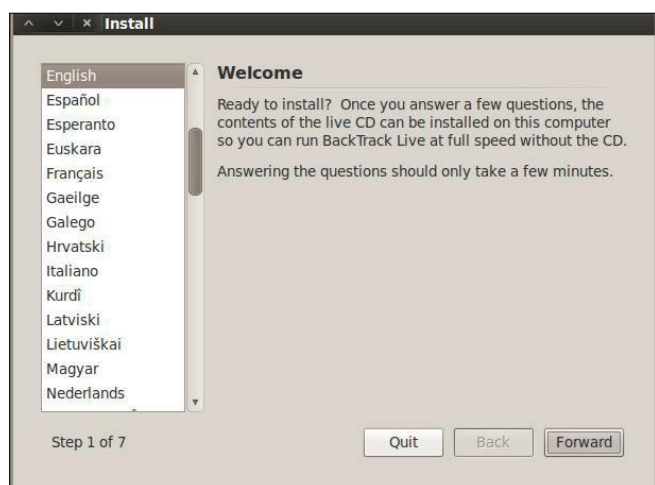


Figure 2. *BackTrack Installation I*

- Metasploit integration
- RFMON Injection capable wireless drivers
- Aircrack-NG
- Kismet
- Nmap
- Ophcrack
- Ettercap
- Wireshark (formerly known as Ethereal)
- BeEF (Browser Exploitation Framework)
- Hydra (Figure 1)

Table 1. *Releasing Dates Of BackTrack Versions*

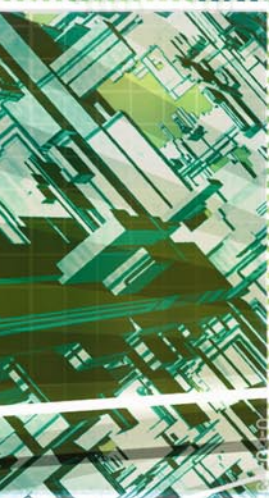
Date	Release
February 5, 2006	BackTrack v.1.0 Beta
May 26, 2006	The BackTrack project released its first non-beta version (1.0).
March 6, 2007	BackTrack 2 final released.
June 19, 2008	BackTrack 3 final released.
January 9, 2010	BackTrack 4 final release. (Now based on Ubuntu)
May 8, 2010	BackTrack 4 R1 release
November 22, 2010	BackTrack 4 R2 release
May 10, 2011	BackTrack 5 release (Based on Ubuntu 10.04 LTS, Linux kernel 2.6.38)
August 18, 2011	BackTrack 5 R1 release (Based on Ubuntu 10.04 LTS, Linux kernel 2.6.39.4)
March 1, 2012	BackTrack 5 R2 release (Linux kernel 3.2.6[8])

The Industry's First Commercial Pentesting Drop Box.

THE Pwn Plus.



Air Freshener?



Printer PSU?
...nope



FEATURES:

- ★ Covert tunneling
- ★ SSH access over 3G/GSM cell networks
- ★ NAC/802.1x bypass
- ★ and more!



PWNIE EXPRESS

@pwnieexpress.com

Discover the glory of
Universal Plug & Pwn

t) @pwnieexpress **e)** info@pwnieexpress.com **p)** 802.227.2PWN

Defending Layer 2 Attacks

Security has been a major concern in today's computer networks. There has been various exploits of attacks against companies, many of the attacks cost companies their reputation and cost them millions of pounds. Many attacks are implemented using inside knowledge from previous and even current employees.

The attacks are mainly due to poor network configurations which leave vulnerabilities on the network. This report will investigate common layer 2 attacks such as VLAN hopping, ping of death, password brute force, SYN attack and MAC spoofing. VLAN hopping, password brute force attacks and MAC spoofing are all used to gain unauthorized access on a network. Many of the attacks are due to default settings implemented on a network device.

Introduction

Problem Definition

The Information Technology Security sector contains vast amounts of different threats to a company's network. There are many possible potential threats that can be made within a network such as retrieving unencrypted and encrypted passwords across the network, and also retrieving vital company information. These threats are generally due to novice employees and weak network architecture. Most threats nowadays can be exploited due to un-patched servers, un-patched client/software, weak security settings, unsecure network devices, and even untrained employees.

The Information Technology security market demands for more secure networks are high. Businesses will spend more money securing their networks because this would control unauthorised access to vital information and also cut down the loss of money from an unsecure network. This project will evaluate network attacks and implement a new secure network design.

Rationale

The project values include finding different weaknesses that companies commonly suffer from. Whenever a

company suffers from security threats this would mean the company's confidential information are at risk. This increases the money lost from data losses or hacking, therefore companies must reduce this risk.

This project will involve implementing a network design and test to find different weaknesses. Once the weaknesses have been found, a new network design will need to be implemented by using the results from the previous test to countermeasure the security threats.

Aims and Objectives

Aims

The aim of this project is to conduct network security analysis using existing software with the purpose of discovering weaknesses within a network environment. By using results from tests, a new secure network design is to be implemented.

Objectives

The objectives in this project will determine how the project will be completed and how the aim will be achieved.

- Research and discussion into security issues: MAC spoofing, VLAN hopping and DoS attacks.
- Extensive research into Linux Backtrack 3 operating system.
- Use Linux Operating System Backtrack 3 to test vulnerabilities.
- Research into CEH (Certified Ethical Hacking) certification.
- Implement network design without security and test.

BackTrack 5:

The Ultimate Security Toolkit Part 1

In the security world today, a security professional relies heavily on knowing the right tools for the job, and knowing how to use these tools. There are hundreds of tools available and the list of tools is constantly changing and growing. For security assessments and penetration testing, there are very few toolkits as actively supported and all-encompassing as BackTrack 5.

BackTrack 5 (BT5) is a Linux security distribution that contains all of the tools necessary to perform a complete security assessment of systems, networks, and applications. This article will describe some basic practical uses of the tools within BackTrack 5 as they relate to a network-based penetration test or security assessment. BackTrack 5 was designed with penetration testing in mind. A pentest is a method of evaluating and testing the security of a system, network, or application by performing actions that are meant to simulate the actions of a malicious attacker.

The tools included in BackTrack 5 are very often the same tools an attacker might be using against a network, and understanding these tools and how effective they might be against your network is an important step of security in-depth. The tools covered in this two-part article and their usage will be outlined in the same order that a network assessment might take place, starting with host discovery and information gathering on discovered targets, moving onto identifying vulnerabilities within your targets, followed by attempting exploitation of the discovered vulnerabilities, and finally, what to do with your newly gained access, also known as post-exploitation. Web application assessment tools will be covered as well.

The first part of the article will cover the basics of BackTrack 5, simple host discovery and information gathering of an internal network, as well as a basic wireless assessment. Part two will cover the steps of discovery and information gathering for an external network assessment, as well as vulnerability assessment, exploitation, and post-exploitation. Some other useful tools will be covered as well. Keep in mind that there are many tools available in BT5 and many of

their functions can overlap, and the information in this article doesn't encompass all of the ways, nor the only way to perform these actions. Use this information as a starting point to discover the real capabilities of the toolkit. The version of BT5 used for in this article is BackTrack 5 R2 KDE 64-bit and there may be slight differences in commands and available applications if you are using a different version.

BackTrack 5 Basics

There are a few different ways BT5 can be setup and used. You can create a Live CD or bootable USB drive and run it in a live environment, install BT5 to *virtual machine* (VM), or install BT5 directly to a hard drive and boot to it as the main OS. Each method has its perks and drawbacks, but for the sake continually performing assessments and testing, creating a BT5 VM is recommended. If you are new to BT5, the in-depth details of setting up BT5 will not be covered in this article; however, the Official BackTrack 5 Wiki and Forums at <http://www.backtrack-linux.org/> contain all the information necessary for getting started.

Once you are up and running, before starting any information gathering, you should create a place to store the information you are collecting. Some of the tools in BT5 utilize databases to store information and one of the strengths of BT5 is that the databases should be preinstalled and configured to start using without much hassle. Since the context of this article covers pentesting of multiple clients, creating a separate folder for each client is recommended. For this assessment, everything will be stored in subfolders in the `~/PenTest` directory, created for this demonstration. Additionally, results that are stored within a database should be

Backtrack 5

Practical Applications And Use Cases

This article breaks down what Backtrack Linux is, with a brief description and history. Then, we'll explore a sampling of some of the many tools that are packaged within Backtrack Linux and provide use cases along with step-by-step tutorials to demonstrate some of the more common tasks that Backtrack is used to perform. Finally, we'll see how most of the tools and techniques that Backtrack is designed to facilitate can be used by the many different roles in the IT security field.

This article is by no means an all-inclusive tutorial on every tool within Backtrack, or every conceivable use one can find for Backtrack. I am not an expert per se, just an avid fan and user. I have experience on both sides of the Infosec spectrum.

I have been a security analyst/incident responder tasked with defending organizations' networks and info systems, and I have been a penetration tester tasked with trying to break into similar systems and networks. In either role (offensive or defensive) I have found Backtrack an invaluable tool in my tool box.

I plan to take some of the core functionality and tools in Backtrack 5, describe their use cases, and demo common tasks that security professionals use them for on a daily basis.

History

Backtrack Linux is a custom Linux distribution designed to aid security professionals with attack simulation, vulnerability identification and verification, and general penetration testing activities. Backtrack was the end result of a combination of two separate (competing) security distributions. WHAX (formerly Whoppix) a security distro developed by Mati Ahoroni and Auditors Security Collection, developed by Max Moser were combined to create Backtrack.

Backtrack version 4 and up are based on Ubuntu. The most recent release, as of this writing, is Backtrack 5 R2 which runs a customized 3.2.6 Linux Kernel. This release touts many new tools and improvements, some of those being better support for wireless attacks, the Metasploit Community Edition (4.2.0) and version 3.0 of the Social Engineering Toolkit. You can see more of

the tools and release info here: <http://www.backtrack-linux.org/backtrack/backtrack-5-r2-released/>.

You can download the latest (along with earlier releases) Backtrack release in ISO or VMware image formats from <http://www.backtrack-linux.org>.

It is true that most of the tools that come bundled within Backtrack can be downloaded separately and do not require Backtrack to run. What makes Backtrack an ideal tool is that its entire environment is setup with security testing in mind. From the tools, scripts, dependencies, libraries and system configurations, every aspect of the end user experience in Backtrack has been set up to enable the user to perform security testing quickly, with limited to no configurations having to be made, since Backtrack is set up in a "turn key" fashion.

I won't say that Backtrack is the only OS I run during penetration tests. I usually have several systems going. But, I always have at least a Backtrack VM running because if I need a tool, and I don't have Internet access to download it or I don't have the time to configure it on a machine, more often than not it's sitting on my Backtrack VM, ready to go with no configuration required. Similarly, when in a security analyst (defensive) role, having quick access to the pre-configured Backtrack environment reaps similar benefits when on a pen test and when needing to perform quick network analysis, or verify a vulnerability.

Mediums

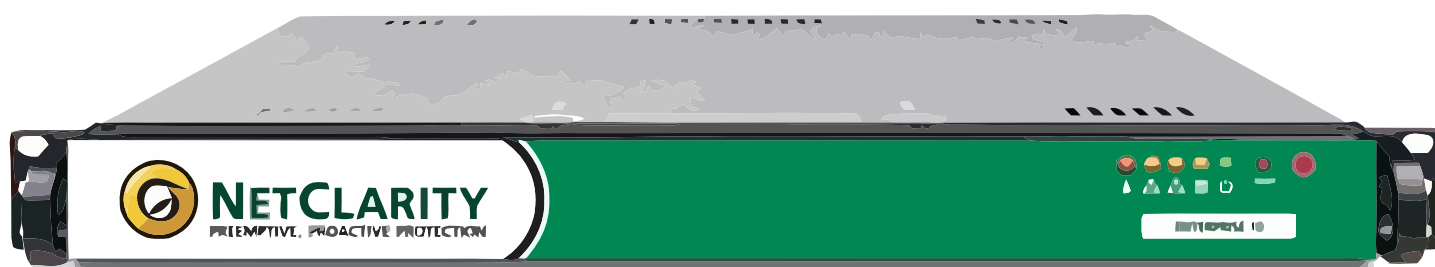
Backtrack 5 R2 can be installed or run in several different ways. It is designed to be portable and as such can easily be installed onto USB Hard Drives or "Pen Drives" as they're sometimes called. Also, you can burn



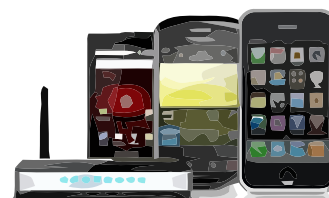
NETCLARITY
PREEMPTIVE, PROACTIVE PROTECTION



Harden your Network from the Inside Out



Network Access Control



Asset Vulnerability Management



Compliance Auditing and Reporting



www.netclarity.net

Available through Partners Worldwide

How Exposed

To Hackers Is the WordPress Website You Built?

WordPress is likely the most popular website framework used on the web today. With over 65 million downloads and a very active community you can accomplish many goals with ease using WordPress.

Not only does the standard WordPress package include many cool features but the number of easy to install WP plugins available continues to grow, which in turn continues to multiply the number of uses for WordPress. The problem with so many WordPress installations all with different variations of WordPress themes and WordPress plugins is the fact that many people will launch a WordPress site and think everything is safe and sound moving forward. That is not the case, however. As technologies evolve and hackers figure out new ways to generate money, new holes will be located within the core WordPress code, WordPress plugins, WordPress themes, and in sloppy system administration. The article below will provide you with a basic understanding of the types of attacks to which your WordPress site may be vulnerable, along with various methods to minimize your risk by using basic Linux commands and the tools within Backtrack Linux.

A Short Story About Incorrect WordPress File Permissions & The Possible Damage That Can Follow

You may be thinking that your WordPress site would never be a target for attackers, however, regardless of content, your WordPress blog is a target. (Many of the most effective WordPress exploits I have seen over time typically involve the quantity of breached websites versus the quality of the breach itself.)? One of the more tricky exploits I have seen with WordPress involved an attacker adding some simple PHP code to files on a WordPress server that had permissions set incorrectly which is a very common mistake among do it yourself web developers. The attacker adds the

malicious code to specific files within the WordPress file structure, which redirects traffic with a referrer of a set list of search engines. An example of the malicious code in action would be someone searching for XYZ on Google which happens to relate to an article you have written on your WordPress site, so they click the result that takes them to your article, but instead of displaying the article you posted about XYZ, they are instead redirected to another website that is full of ads or full of malicious code that could infect your browser and/or PC. The benefit to the attacker is that they are either making money from the ads, or they are exploiting your users' systems upon being redirected. Regardless of the scenario, the outcome is a horrible experience for the person visiting your website. The genius behind this type of attack is that it is extremely hard to track down and nearly impossible for inexperienced web developers or system administrators to locate. When this type of redirect issue is reported the person troubleshooting the problem typically visits the WordPress site in question and everything appears to be working as expected because they were not visiting the site through Google. Therefore they assume the issue was on the reporting users end. File permissions are extremely important and should be understood and followed when installing and/or managing a Wordpress installation. There are plenty of details on the WordPress Codex pages that can assist anyone not familiar with file permissions. The primary steps to take, however, include making sure files are not owned by the webserver process, setting directories permissions to 755, and setting file permissions to 644. Having the proper file permissions will keep the attacker's WordPress bots at bay.

Lisring 1. Enumerate WordPress Usernames Using WPScan In Backtrack Linux

```
#####
root@bt:/pentest/web/wpscan# ./wpscan.rb -e u[1-25] --url wordpress.example.com
```

```

  _ _ _ _ _
 / / _ _ \ / _ _ \
 \ \ / \ / / | | | | | ( _ _ _ _ _
 \ \ / \ / / | | | | | \ _ _ \ / _ _ \ ' ' \
 \ / \ / / | | | | | ( _ _ \ _ _ | | | | |
 \ / \ / / | | | | | \ _ _ \ _ _ | | | | | v1.1
```

WordPress Security Scanner by ethicalhack3r.co.uk
Sponsored by the RandomStorm Open Source Initiative

```
| URL: http://wordpress.example.com
| Started on Wed May 23 11:27:31 2012
[!] The WordPress theme in use is called 'drawar' v1.0
[+] We have identified 1 vulnerabilities for this theme :
| * Title: WooThemes WooFramework Remote Unauthenticated Shortcode Execution
| * Reference: https://gist.github.com/2523147
[!] The WordPress 'http://wordpress.example.com/readme.html' file exists
[!] WordPress version 3.3.2 identified from rss generator
[+] We have identified 1 vulnerabilities from the version number :

| * Title: Wordpress 3.3.1 Multiple CSRF Vulnerabilities
| * Reference: http://www.exploit-db.com/exploits/18791/

[+] Enumerating plugins from passive detection ... 2 found :

| Name: woo-tumblog
| Location: http://example.wordpress.com/wp-content/plugins/woo-tumblog/

| Name: jetpack
| Location: http://example.wordpress.com/wp-content/plugins/jetpack/
|
| [!] WordPress jetpack plugin SQL Injection Vulnerability
| * Reference: http://www.exploit-db.com/exploits/18126/

[+] Enumerating usernames ...

We found the following 5 username/s :
```

admin
superadmin
bob
wiwi

```
[+] Finished at Wed May 23 11:27:54 2012
root@bt:/pentest/web/wpscan#
#####
```

Below are two quick examples of what the file permissions should look like on the wp-content folder and the wp-cache-config.php file.

Changing File Permissions Example From WordPress Codex

```
*****
For Directories
find /path/to/your/wordpress/install/ -type d -exec chmod
    755 {} \;

For Files
find /path/to/your/wordpress/install/ -type f -exec chmod
    644 {} \;
*****
```

Use Backtrack Linux To Proactively Audit Your WordPress Installation

An exploit of sorts that was initially made public many years back is username enumeration which allows a would be attacker to easily obtain a real time list of users who likely have access to the /wp-admin or administration section of your WordPress site. This doesn't necessarily mean your WordPress site is immediately vulnerable but what it does mean is an attacker now has 50% of the necessary information to gain access to your entire website. There are numerous methods in Backtrack that provide some form of user enumeration including my personal favorite which is called WPScan and which has been specifically created for auditing WordPress sites. It will be a tool we will visit numerous times within this article. The wpscan.rb Ruby script written by Ryan Dewhurst (@ethicalhack3r) is classified as a WordPress vulnerability scanner which checks the security of WordPress installations taking a black box approach. Currently WPScan is the most comprehensive tool available on Backtrack Linux to test various security flaws within WordPress, including username enumeration, WordPress version info, and WordPress plugin info/vulnerabilities. WPScan also provides a method to brute-force WordPress logins once you have enumerated the usernames. To see basic information for WPScan including the list of command line switches available and a couple of example wpscan.rb commands, issue `./wpscan.rb -help` from the `/pentest/web/wpscan` directory. The first bit of information we will gather from a fake WordPress site will be a list of usernames using WPScan which by default will attempt to enumerate usernames with UID's or user id's 1 through 10. However, a new option in WPScan allows you to specify any range of UID's you prefer, as shown in the example below. Along with the username enumeration we will also get other default information output in our WPScan query which is also shown in the below example.

Enumerate WordPress Usernames Using WPScan In Backtrack Linux

See Listing 1.

Lets first analyze the command that was issued at the top of the above output to provide the results that were returned from WPScan. We issued two switches with the wpscan.rb command including `"-e u[1-25]"` which tells WPScan to enumerate usernames with UID's 1 thru 25 and `"--url wordpress.example.com"` which specifies the WordPress site URL. The WPScan output above is divided into four sections below, which include Wordpress theme information/vulnerabilities, basic WordPress information/vulnerabilities, WordPress plugin information/vulnerabilities, and WordPress username information.

WPScan WordPress Theme Information & Vulnerabilities

The wpscan.rb output was able to determine that the theme in use is the drawar theme provided by Woo Themes that it then notes has a vulnerability that allows remote code execution. When following the link in the drawar theme vulnerability output you can see that a would be attacker could execute remote code such as adding a Twitter follow me button on the remote site depending on the drawar theme version. You may or may not have a vulnerability or a list of vulnerabilities listed, depending on the theme name that is enumerated. WPScan is really accurate, however, in enumerating the theme name which provides a would be attacker more information than they had initially.

WPScan Basic WordPress Information & Vulnerabilities

Basic WordPress information is also output that shows a would be attacker the version of WordPress that is running along with any known vulnerabilities within that WordPress version. As you can see in the output above WordPress version 3.3.1 had a CSRF or Cross Site Request Forgery vulnerability that allows would-be attackers access to change data on the site such as Wordpress Post Title using CSRF and the WordPress Quick Edit Function.

WPScan WordPress Plugin Information & Vulnerabilities

Within the WPScan root directory, which is `/pentest/web/wpscan` on Backtrack Linux 5, there is a file in the data directory named `plugins.txt` which has a fairly large list of WordPress plugins that WPScan will query to see if they exist on the target site. Once a plugin has been verified not only will it be output, but the plugin and plugin version will be checked against a list of known vulnerabilities and will also output any matches

such as the JetPack plugin SQL Injection Vulnerability noted in the example output above.

WPScan WordPress Username Information:

One of the items that really impressed me when I first ran WPScan some time ago was the ability to enumerate usernames from a Wordpress site. While in my opinion this is a security flaw within Wordpress that should be resolved, it is still exciting to query a Wordpress site and have the primary admin users returned back to you. Notice that in this example we attempted to enumerate UID 1 through UID 25 and we were returned 25 results that include a user named admin and a user named superadmin. While the usernames themselves are not directly vulnerable, it does provide a would be attacker with 50% of the data necessary to brute force a login to your Wordpress site which, if accomplished, would be devastating to your Wordpress site. Below we discuss the Wordpress username enumeration security flaw in more detail including how to manually enumerate the usernames so you can better understand the basis of automated tools such as WPScan.

How To Manually Enumerate WordPress Login ID's And Usernames

Open the following URL but change the domain to the domain running your Wordpress site: URL: `http://www.wordpressexample.com/?author=1`.

If you have not deleted the default admin user created during your Wordpress install you will be redirected to a URL similar to the following: URL: `http://www.wordpressexample.com/authors/admin`.

So as you can see you now know that the default admin user still exists, its user id is 1, and the login is actually the default admin. Now if you received an error such as a 404 indicating that this user does not exist you could move right along to the next URL such as the following: URL: `http://www.wordpressexample.com/?author=2`.

If the above URL is successful in being redirected to something that means you will now know another user id and user name. It would obviously be easy to write a script that would walk through thousands of user ids in a short amount of time and in the end you would know all of the Wordpress user id's that are active and their corresponding Wordpress logins.

The WPScan application within Backtrack Linux is one of numerous tools available to assist in auditing your Wordpress installation. Other tools that are useful include wfuzz, w3af, nmap, and metasploit. These tools will be expanded on during a follow up article discussing auditing Wordpress with Backtrack Linux. Now that we see how easy it is to enumerate various data from Wordpress, lets look at a couple of methods to begin locking your Wordpress site down, so potential

attackers are discouraged and move on to another site that will be easier for them to exploit.

Begin Taking Steps To Lock Down Your WordPress Site

Now that you can see how easy it is to locate vulnerabilities within Wordpress and gather data about a specific Wordpress installation I will now discuss numerous security measures that can be put in place to minimize your Wordpress installation's exposure. Below it is discussed how to manually add an entry to .htaccess which will block username enumeration followed by various plugins that provide different security benefits which make exploitation of your Wordpress installation more difficult.

How To Defend Against WordPress User ID And Login Enumeration

I have not seen the below fix implemented previously and I am not sure if there are any hidden problems caused by utilizing such an .htaccess entry. For me, however, it is worth the risk, as any issues that may arise from blocking this query would likely be minimal. It would take me much longer to have to restore my entire site from scratch if it were hacked and defaced or destroyed after someone enumerated the Wordpress usernames and then brute-forced an administrator login to my Wordpress site. I have implemented the solution below on numerous Wordpress installations for months without any issues. To block user login enumeration we are going to add a couple lines to the .htaccess file located in the root web directory of your Wordpress web site as shown below. You will want to add this near the top of the .htaccess file because if it is added below the normal redirect, it is useless.

Code To Add To .htaccess File To Block WordPress User Enumeration

```
#####
RewriteCond %{REQUEST_URI} ^/$
RewriteCond %{QUERY_STRING} ^/?author=([0-9]*)
RewriteRule ^(.*)$ http://www.wordpressexample.com/
some-real-dir/ [L,R=301]
#####
```

The code above tells the web server that any request made to the Wordpress site matching the query string of `"/?author=` should be redirected to `http://www.wordpressexample.com/some-real-dir/`. I have this code right under "ServerSignature Off" which is at the top of the .htaccess file in the Wordpress root directory. Once you add these lines to the .htaccess file, user enumeration is now blocked. Continue below for discovering other security measures to take with

your WordPress site. Please note that `/some-real-dir/` could be any existing URL on your site or you could make a page that explains that user enumeration or viewing authors in this manner is not allowed for security reasons. It is always best practice to backup any file before making changes to do that and the `.htaccess` file is no exception.

Minimize WordPress Data Available Such As Block WordPress Version From Displaying

To accomplish the goal of minimizing the WordPress information that is exposed, I install a WordPress plugin called Secure WordPress. A quick search for Secure WordPress on the WordPress plugins site should return the Secure WordPress plugin at the top of the results. Just by installing and activating Secure WordPress you will resolve numerous security holes, including the hole allowing attackers to see your WordPress version. It also provides some protection against malicious URL requests, and removes the Really Simple Discovery link in `wp_head`. I also like to enable all checkboxes except for the Error Messages check box, and one option that is not checked by default but I do check is Windows Live Writer. I would also suggest signing up for WebSiteDefender as you will get a free scan of your web site which can be accomplished via the Secure WordPress settings page.

WordPress Plugin Secure Wordpress Admin View

See Figure 1.

Block Various SQL Injection Attempts To WordPress & Secure Other WP Areas

Another plugin I install is called BulletProof Security and it is also available on the WordPress site in the plugins directory. The WordPress plugin BulletProof Security is a bit more complex as you will first generate `.htaccess` files for various locations on your WordPress site, and then be required to merge them into existing `.htaccess` files. Make sure that when you merge the changes that the redirect for author that we previously added stays near the top of the `.htaccess` file located in the WordPress root directory. BulletProof Security provides a bunch of rules that minimize your exposure to SQL Injection and other nasty attacks. Make sure to backup the current `.htaccess` files before merging any new changes into them.

Example BulletProof Security Plugin .htaccess Entry

```
#####
RewriteCond %{QUERY_STRING} (;<|>|'|"|\)|%0A|%0D|%22|%27|%3C|%3E|%00).*(/|*|union|select|insert|drop|delete|
```

```
update|cast|create|char|convert|alter|declare|order|
script|set|md5|benchmark|encode) [NC,OR]
#####
```

There are dozens of `.htaccess` entries similar to the above example entry. As you can see in the provided example BulletProof security will simply block malicious requests made to your WordPress site such as possible SQL Injection attempts. Keep in mind that implementing any plugin such as BulletProof Security that modifies web requests to your server could cause potential issues on your site so any changes made should be thoroughly tested.

Remove readme.html File In WordPress Root Directory

This one is self-explanatory. During the installation of WordPress a `readme.html` file is generated in the root WordPress directory so make sure to remove it. You can remove this file via FTP or using “rm” from the command line as shown in the below example.

```
####
[root@dev ~]# rm /path/to/wordpress/root/dir/readme.html
rm: remove regular file `/path/to/wordpress/root/dir/
      readme.html'? y
[root@dev ~]
#####
```

Other WordPress Security Plugins To Consider

Depending on the WordPress installation, I also install several other plugins related to security, including the Login Lockdown WordPress plugin, the AntiVirus WordPress plugin, the Login Logger WordPress plugin,

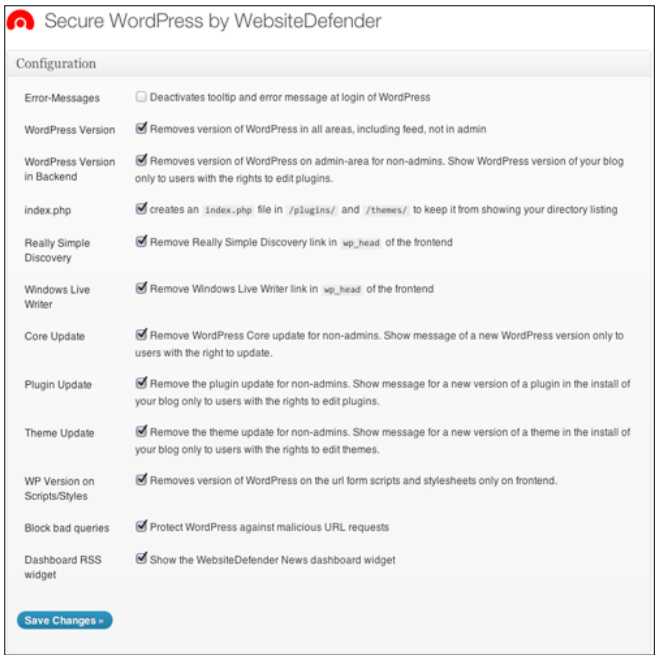



Figure 1. WordPress Plugin Secure Wordpress Admin View

Leave a Reply

Name (required)

E-mail (will not be published) (required)

Great article. Ohh I need to also fill in the **captcha** below so if I am a SPAM bot my comment will not be posted successfully.



CAPTCHA Code *

*Type the letter/number combination in the above field before clicking submit.

Figure 2. WordPress Comment Form Captcha

and The WP Block Admin WordPress plugin. You should also consider utilizing something like Really Simple Captcha and you should make sure to include a Captcha on any contact form installed on your site, which will also cut down on SPAM. Another item that can become a hassle quickly with WordPress is the amount of SPAM received via comments attached to each WordPress post. To combat this you can install a WordPress plugin such as SI CAPTCHA Anti-Spam which will add a captcha to comments attached to WordPress posts and or WordPress pages as shown in the below example image.

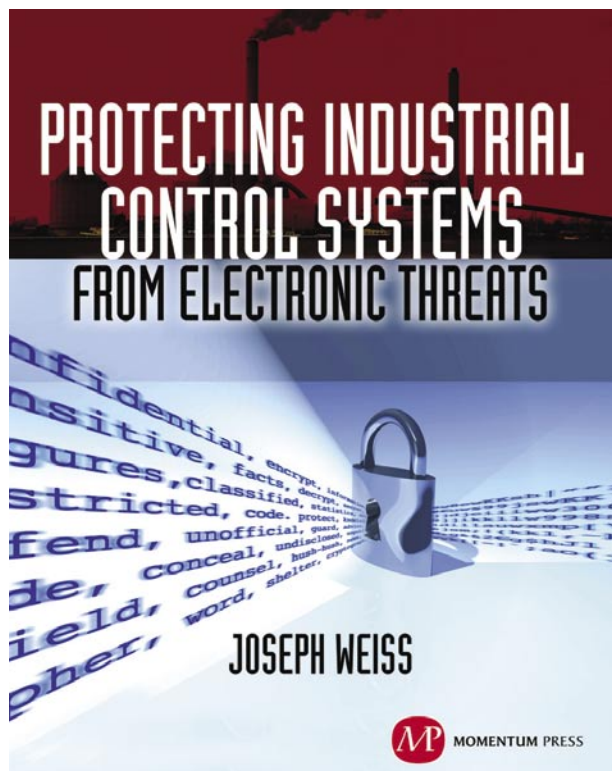
WordPress Comment Form Captcha

Last but not least, make sure permissions are correct throughout the entire WordPress directory. If you provide the incorrect write permissions for vulnerable WordPress files, you are guaranteed to be hacked in a short amount of time (Figure 2).

Keeping Your WordPress Installation Secure Moving Forward

Once the above security measures are firmly in place, the task of defending your WordPress site against potential attackers is still not complete. If you want your WordPress site to be secure on a long term basis, you will need to employ a proactive approach. You will need to continue using tools such as WPScan combined with other relevant tools in Backtrack Linux.. You will also need to update WordPress itself, to update your WordPress plugins, and possibly to use a third party service that runs automated scans against your WordPress site, all performed on a regular basis.

ALEX KAH



For many years, Joe Weiss has been sounding the alarm regarding the potential adverse impact of the 'law of unintended consequences' on the evolving convergence between industrial control systems technology and information technology. In this informative book, he makes a strong case regarding the need for situational awareness, analytical thinking, dedicated personnel resources with appropriate training, and technical excellence when attempting to protect industrial process controls and SCADA systems from potential malicious or inadvertent cyber incidents."

—**DAVE RAHN**, *Registered Professional Engineer, with 35 years experience.*



MOMENTUM PRESS

FOR US ORDERS:
www.momentumpress.net
PHONE 800.689.2432

FOR INTERNATIONAL ORDERS:
McGraw-Hill Professional
www.mcgraw-hill.co.uk
PHONE: 44 (0)1628 502700

Become Quieter

with a Little Help from BT

"The quieter you become, the more you are able to hear."

-BackTrack

BackTrack Live Security Linux Distribution Overview/Tutorial

When you are faced with a task of testing your production environment and strengthening your defenses, your choice of the tool is easy. Instead of concentrating on collecting penetration (pen) testing tools, just head to BackTrack website and download an image of one of the most popular white hat penetration testing and security auditing platforms. It's #7 on the sectools.org Top 125 Security Tools list.

BackTrack is a merger between three different live Linux penetration testing distributions: Whoppix, IWHAX and Auditor. The current version BackTrack version 5 R2 (Code Name Revolution) is based on Ubuntu Linux distribution version 10.04.3 LTS (Lucid Lynx), which means good stability, hardware detection and a lot of easily obtainable software. It's available in GNOME and KDE window managers (you can also configure FluxBox window manager), and for 32-bit, 64-bit and ARM architecture. It comes with over 300 PenTesting tools.

First Steps

You can run the distribution as a Live DVD or install it as a regular operating system on a hard disk or USB flash drive. The Live DVD offers these different boot options:

- Default text mode – boots into a customized Linux shell. You can work on the command-line or boot into the desktop environment by using the `startx` command.
- Stealth mode – boots the OS with networking disabled.
- Forensics mode – boots without automatically mounting drives or swap space.

- `noDRM` – boots without DRM (*Direct Rendering Manager*) drivers. DRM are Linux kernel modules that enable certain applications to use a GPU more efficiently, especially 3D rendering. Use this option if the boot halts or if you have screen problems.
- Debug – boots into Safe Mode. Choose this option if you have problems getting BackTrack to boot. For example, if you are having screen problem and the `noDRM` option doesn't fix it, boot into *Debug* mode and try adding the `nomodeset` parameter. It instructs the kernel to not load video drivers and use BIOS modes instead until X Window System is loaded. To do that: while in the boot menu, highlight the BackTrack Debug – Safe Mode, press Tab in order to edit the boot option and add `nomodeset` to the end of the list.
- Memtest – starts `memtest` memory diagnostic utility.
- Hard Drive Boot – boots the first hard disk.

Even though BackTrack is primarily intended to work as a live DVD, for my test environment I installed it as a virtual machine in VirtualBox because I like the convenience of switching between BT and Mac OS X on the fly. It's also useful to configure BackTrack this way if you plan to use it regularly or customize it. The full install requires about 12 GB.

When you are running BT5 in the virtual machine, you can't use a wireless card because the virtual machine software blocks access to the hardware except for USB devices. To be able to use wireless portion of the tools in the virtual machine, you can install a USB wireless card. BackTrack site has a list of compatible cards called Tested and Working Cards List (*Note that this list needs*

BackTracking in Wifi Country

The BackTrack 5 distribution continues to be the “go to” tool in a security professional’s arsenal. With the latest release, “Revolution,” the Backtrack development team delivers a kit you can use anywhere on both light and heavy duty security tasks.

In this practical guide, we’ll cover auditing Windows passwords and wireless keys, as well as forensic recovery using BackTrack on a USB, in a persistent hard drive installation and running in a virtual machine.

BackTrack Everywhere

The key to a useful tool is not only the function of the tool; it’s having it available where you want it when you need it. The best tools in the world won’t do you much good if they’re not with you when you need them. That’s where BackTrack comes in.

BackTrack 5 provides over three hundred individual tools built on an Ubuntu base. More than just a collection of tools, BackTrack aligns with familiar security testing methodologies:

- Information Gathering
- Vulnerability Assessment
- Exploitation
- Privilege Escalation
- Maintaining Access

The current release is available for 32-bit and 64-bit platforms and earlier releases include ARM support. It can be downloaded in Gnome or KDE variations, as an ISO image to run as a Live distribution, or installed on a USB flash drive or a hard drive. Earlier 32-bit releases are prepackaged to run in VMware.

With so many tools and the ability to run it in so many ways, a security professional can be assured of immediate access to a tool that’s ready to go when and where it’s needed. As we move from one installation of BackTrack to the next, we gain familiarity with a

common interface and a complete set of tools that line up with common security methodologies.

Choosing a Path

In this article we’ll use BackTrack to perform three common tasks for a security professional: auditing Windows and Wifi keys, capturing a drive image, and recovering deleted files.

In performing these tasks, we’ll bounce between installations of BackTrack on USB flash drives, in virtual machines and installed directly to a hard drive. In each case, choosing the right platform for the task at hand.

Due to sheer size of BackTrack and time and space limitations of this article, we only scratch the surface of what you can do with BackTrack. However, we hope you’ll get a solid grasp for how to use a few key tools included with BackTrack, and more importantly, see how various installation approaches allow you to tackle different parts of a job and make your task easier.

Throughout this article, we’ll refer to the BackTrack website (<http://www.BackTrack-linux.org>). Not only will you download the distributions we’ll be using there, but you will also find many detailed HOWTO’s and guides on taking BackTrack to the next level.

The best tools for any job are available immediately and conveniently and lack a steep learning curve. Simply put, when you need BackTrack it can be just about anywhere, and it will be the same every time you boot it.

Getting Started with BackTrack

Before beginning, we should understand the effect persistence has on our installation of BackTrack. Just like other Live CD/DVDs, booting and running BackTrack

Atola Insight

That's all you need for data recovery.

Atola Technology offers *Atola Insight* – the only data recovery device that covers the entire data recovery process: *in-depth* **HDD diagnostics**, **firmware recovery**, **HDD duplication**, and **file recovery**. It is like a whole data recovery Lab in one Tool.

This product is the best choice for seasoned professionals as well as start-up data recovery companies.

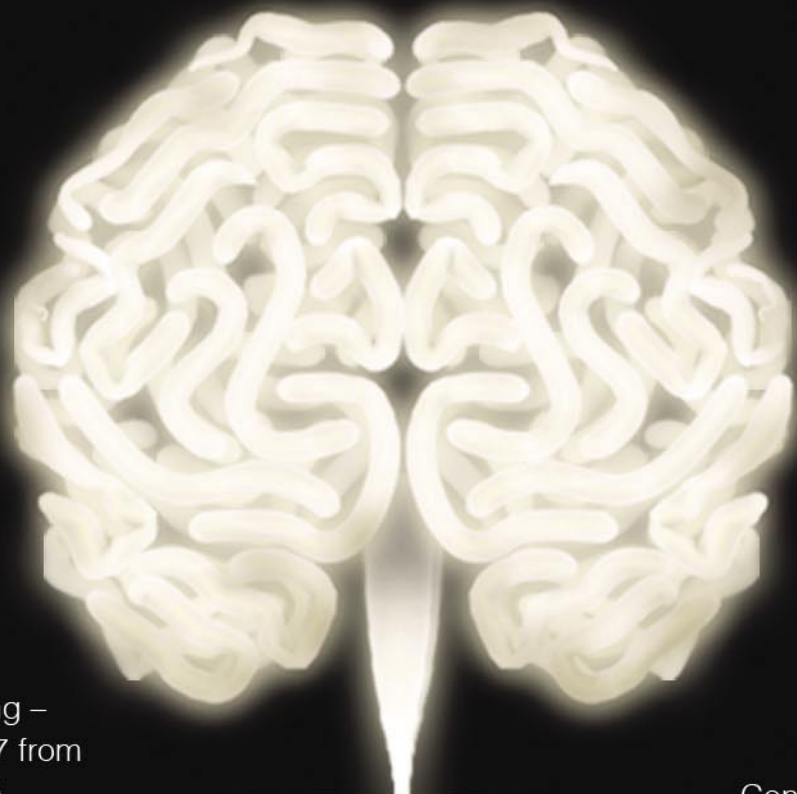
Emphasized features at a glance:

- Automatic in-depth diagnostic of all hard drive components
- Automatic firmware recovery and ATA password removal
- Very fast imaging of damaged drives
- Imaging by heads
- Case management
- Real time current monitor
- Firmware area backup system
- Serial port and power control
- Write protection switch



Visit atola.com for details





Cloud-based training –
access content 24/7 from
anywhere with ease.

Hands-on labs – gain
practical experience from
a "hacker's" perspective.

Constantly updated
curriculum – new
modules added monthly.

Direct mentoring and 1
on 1 instructor interaction.

Content covers:

- Hacking fundamentals
- Recon, network, server,
client, and web pentesting
- Pentest structure
- Reverse engineering
- Digital forensics & more!

Teaches the latest
offensive security
techniques from beginner
through cutting edge.

Are you thinking like a
HACKER yet?
www.thehackeracademy.com

