ClubHACK Mag

1st Indian "HACKING" Magazine

Security by luck, not possible!

Issue 31 | August 2012
www.clubhack.com

TechGyan Malware Memory Forensics | **Mom's Guide** Apple iOS vulnerabilities |

ToolGyan Tamper data | **Matriux Vibhag** Matriux Ec-Centric |

Hello Readers! Here we are with the 31st issue, which will be released at c0c0n 2012 - International Cyber Security Conference. Talking about the conferences, this year let's have a Hack Night in ClubHack2012 Conference. A night where actual hackers spend time not to "break" into someone but to "make" something interesting. For more details check :- http://www.clubhack.com/2012/

Pankit Thakkar

Coming back to this issue we have Malware Memory Forensics in TechGyan, Apple iOS vulnerablities in Mom's Guide, Tamper Data in ToolGyan and Matriux Ec-Centric which too will be released at c0c0n. The poster I designed would be very easy to understand for the Indian readers. Foreign readers, search for 7 chillies and 1 lemon on Google. You will understand what we are trying to say ;)

Keep your articles, feedbacks and suggestions flowing to info@chmag.in

Issue 31, August 2012.

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

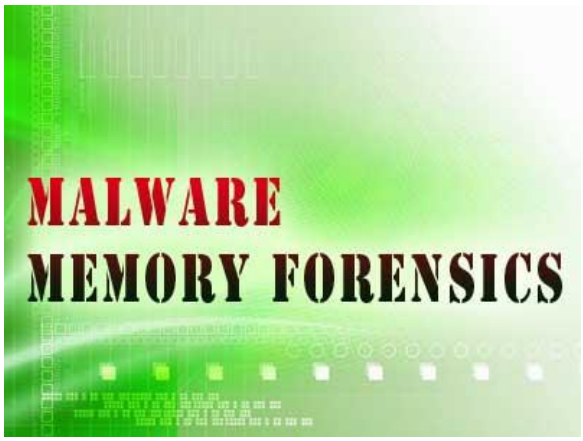
K.V.Prashant
good.best.guy@gmail.com

Sagar Nangare
sagar@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS



Malware Memory Forensics

Introduction

Memory Forensics is the analysis of the memory image taken from the running computer.

In this article, we will learn how to use Memory Forensic Toolkits such as Volatility to analyze the memory artifacts with practical real life forensics scenario.

Below are the list of steps involved in memory forensics:-

Why Memory Forensics?

Memory forensics can help in extracting forensics artifacts from a computer's memory like running process, network connections, loaded modules etc etc. It can also help in unpacking, rootkit detection and reverse engineering.

1. Memory Acquistion - This step involves dumping the memory of the target machine. on the physical machine you can use tools like Win32dd/Win64dd, Memoryze, DumpIt, FastDump on the virtual machine, acquiring the memory image is easy, you can do it by suspending the VM and grabbing the ".vmem" file.
2. Memory Analysis - once a memory image is acquired, the next step is analyze the grabbed memory dump for forensic artifacts. tools like Volatility and Memoryze can be used to analyze the memory.

Volatility - A Quick Overview

Volatility is an advanced memory forensic framework written in python. It can be installed on multiple operating systems (Windows, Linux, Mac OS X), Installation details of volatility can be found here - http://code.google.com/p/volatility.

Volatility Syntax & Usage

```
* using -h or --help option will display help options and list of a available plugins.
Example: python vol.py -h

* Use -f and --profile to indicate the memory dump you are analyzing.
Example: python vol.py -f mem.dmp --profile=WinXPSP3x86
```

* To know the --profile info use below command:
Example: python vol.py -f mem.dmp imageinfo

Demonstation - Memory Forensics

In order to understand memory forensics and the steps involved. I have created a scenario, our analysis and flow will be based on the below scenario.

Demo Scenario

Your security device alerts, show malicious http connection to ip address 208.91.197.54 from a source ip 192.168.1.100 on 8th june 2012 at around 13:30hrs...you are asked to investigate and do memory forensics on that machine 192.168.1.100

Preparation Steps

To start with, acquire the memory image from 192.168.1.100, using memory acquistion tools. for the sake of demo, the memory dump file is named as "infected.dmp".

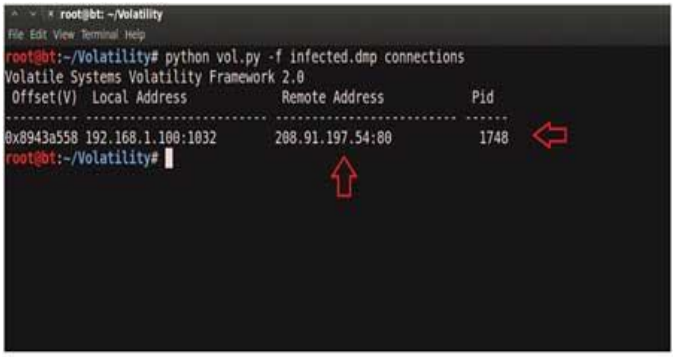
Demonstration - Memory Analysis

Now that we have acquired "infected.dmp", lets start our analysis.

Step 1: Start with what you know

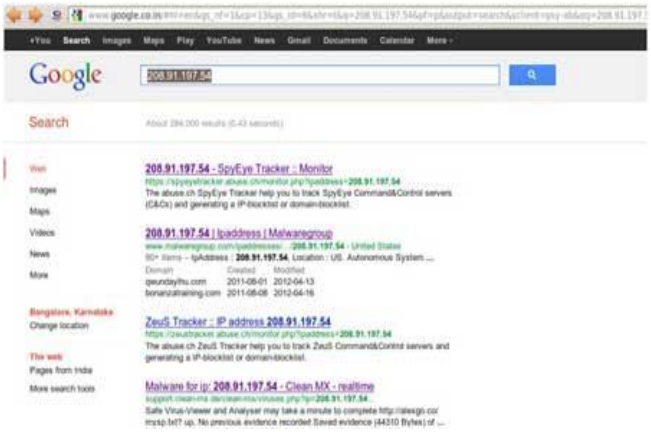
We know from the security device alert that the host was making an http connection to 208.91.197.54. So let's look at the network connections.

Volatility's connections module, shows connection to the malicious ip made by pid 1748.



Step 2: Info about 208.91.197.54

Google search shows this ip 208.91.197.54 to be associated with malware, probably "SpyEye", we need to confirm that yet.

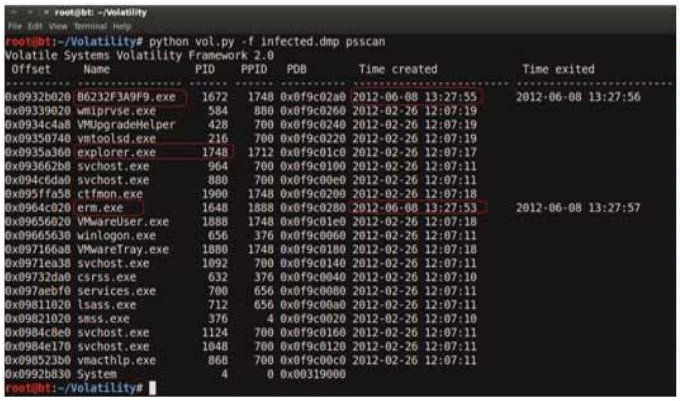


Step 3: Who is Pid 1748?

Since the network connection to the ip 208.91.197.54 was made by pid 1748, we need to determine which process is associated with pid 1748. "psscan" shows pid 1748 belongs to explorer.exe, also two process created during same time reported by security device (i.e. June 8th 2012).

dolor sit amet Lorem Ipsum Dolor sit Amet Loerm Ipsum dolor sit amet

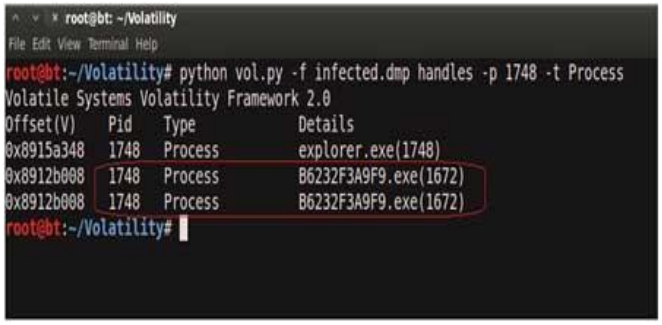
Loerm Ipsum dolor sit amet Loerm Ipsum dolor sit amet Loerm Ipsum dolor sit amet



Step 4: Process handles of explorer.exe

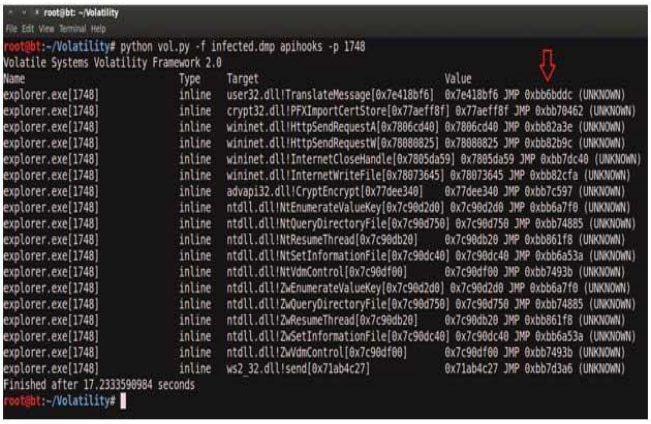
Now that we know explorer.exe (which is an operating system process) was making connections to the malicious ip, there is a possibility that explorer.exe is infected.

Lets looks at the process handles of explorer.exe. The below screenshot shows Explorer.exe opens a handle to the B6232F3A9F9.exe, indicating explorer.exe might have created that process, which might also be malicious...Lets focus on explorer.exe for now.



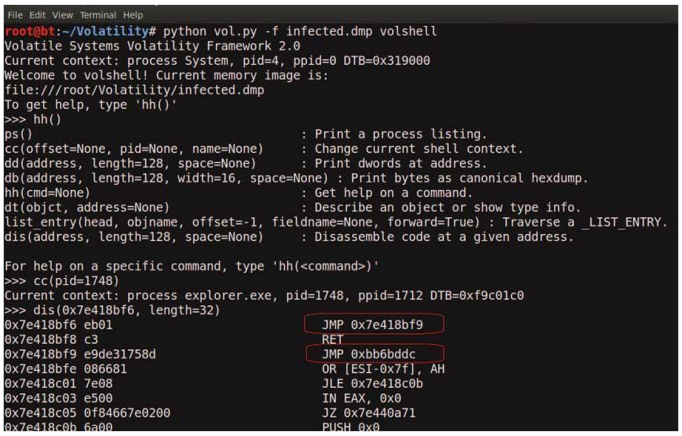
Step 5: API Hooks in explorer.exe

APIhooks module show, inline API hooks in explorer.exe and jump to an unknown location.



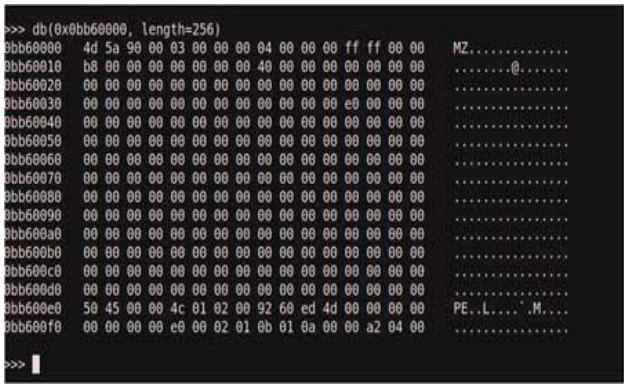
Step 6: Exploring the Hooks

Disassembled hooked function (TranslateMessage), shows a short jump and then a long jump to malware location.



Step 7: Embedded EXE in explorer.exe

Printing the bytes at the hooked location, show the presence of embedded executable in explorer.exe.

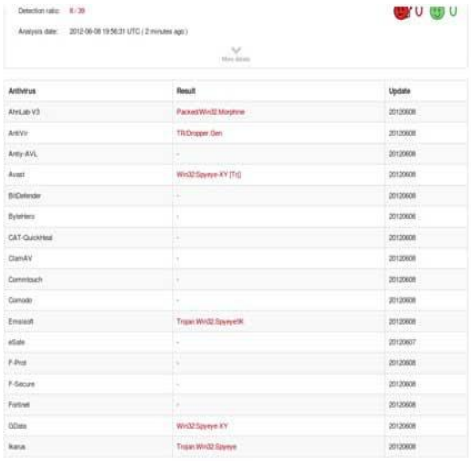


Step 8: Dumping the embedded EXE

VadDump tool dumps the embedded exe from explorer.exe.

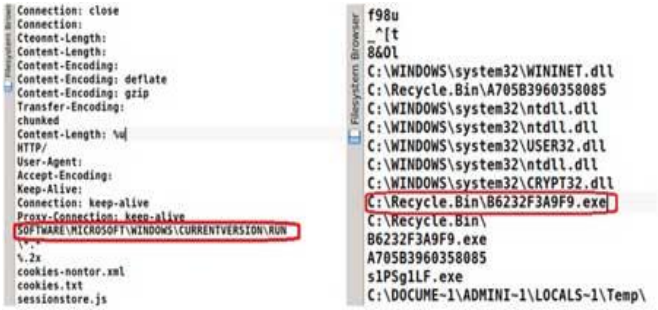
Step 9: VirusTotal Submission

Submission to VirusTotal, confirms the dumped executable as component of "SpyEye".



Step 10: Can we get more info?

Strings extracted from the dumped executable, show reference to interesting artifacts (executable and the registry key), it also shows the path to the suspicious executable B6232F3A9F9.exe.



Step 11: Printing the Registry Key

Printing the registry key determined from the above step (step 10) shows that, malware creates registry key to survive the reboot.

```
root@bt:~/Volatility# python vol.py -f infected.dmp printkey -K "SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN"
Volatile Systems Volatility Framework 2.0
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
Key name: Run (S)
Last updated: 2011-10-31 15:07:20

Subkeys:

Values:
----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: Run (S)
Last updated: 2011-10-31 20:28:57

Subkeys:

Values:
----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
Key name: Run (S)
Last updated: 2012-06-08 13:27:56

Subkeys:

Values:
REG_SZ        ctfmon.exe      : (S) C:\WINDOWS\system32\ctfmon.exe
REG_SZ        4Y3Y0C3A1F7XZHZWACQCUD : (S) C:\Recycle.Bin\B6232F3A9F9.exe
```

Step 12: Finding the Malicious EXE on Infected Machine

Now that we know the path to the suspicious executable, lets find it on the infected machine. Finding malicious sample from infected host and virustotal submission confirms SpyEye infection.

Conclusion

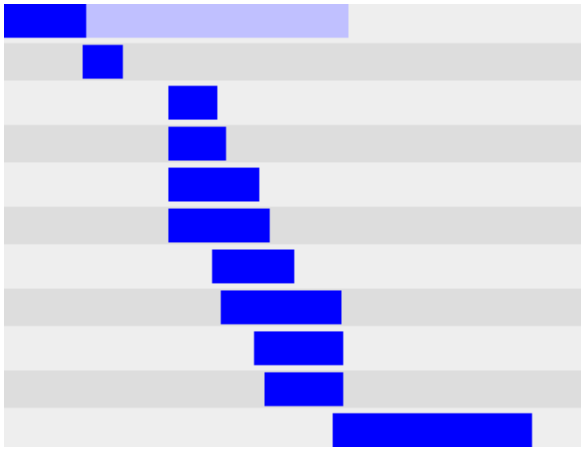
Memory forensics is a powerful technique and with a tool like Volatility it is possible to find and extract the forensic artifacts from the memory which helps in incident response, malware analysis and reverse engineering.

References

1. Reversing Training Session 6 – Malware Memory Forensics
2. Volatility - An advanced memory forensics framework
3. Volatility - Volatile memory analysis research
4. MoonSols Windows Memory Toolkit

Monappa

Monnappa one of the core members of management panel at SecurityXploded. He has rich experience of about 5 years in the security domain with core expertise in exploit development and malware analysis. In addition to publishing interesting research articles, he has also delivered training sessions on 'Reversing & Malware Analysis' at SecurityXploded. Currently he is working at Cisco Systems as Information Security Investigator.



Tamper data

What is Tamper Data?

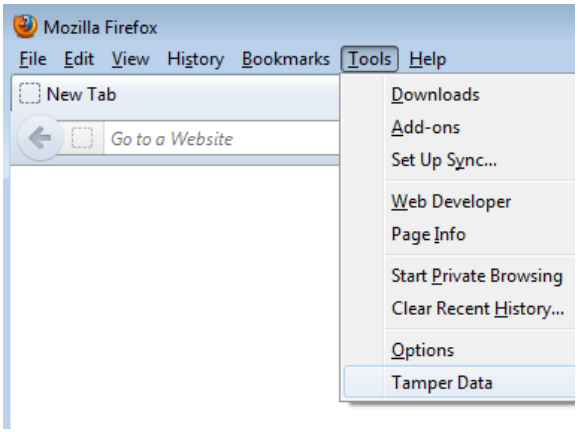
Tamper data, an add-on (extension) for Mozilla Firefox, is a fast, simple yet effective tool which can used to do penetration testing.

Tamper Data basically gives us the power to view, record and even modify outgoing HTTP requests. Since Tamper data is integrated into the browser, so it has no problems with the HTTPS connections, client authentication certificates or other features that the browser supports. We can trace and time the http/https connections, responses and parameters being sent.

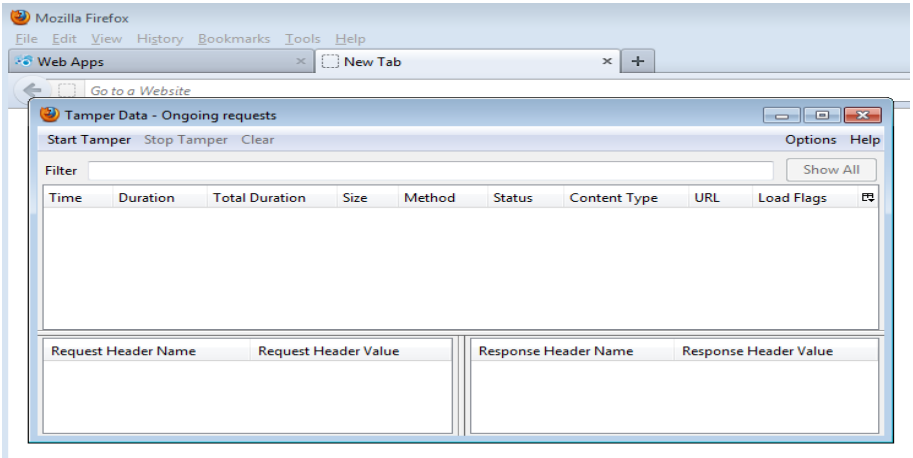
How to use Tamper Data?

Tamper Data is a plugin available for Firefox. We can easily download the xpi from Mozilla and install it. After installation of the add-on it would ask for restarting the Firefox.

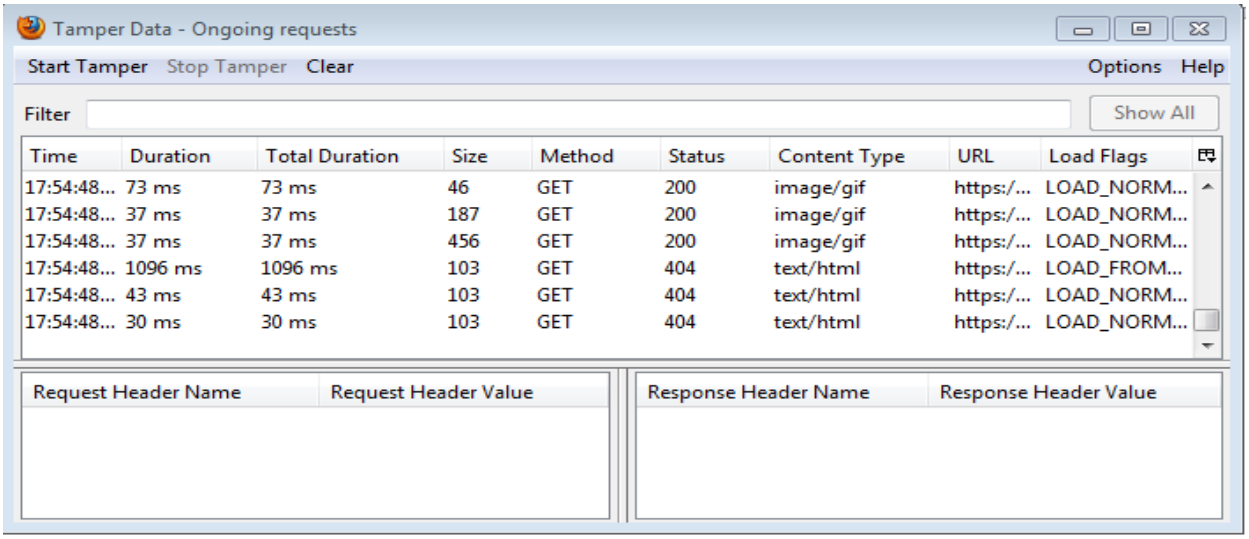
Now once we have restarted the Firefox we can visit the Tamper Data by going to TOOLS → Tamper Data



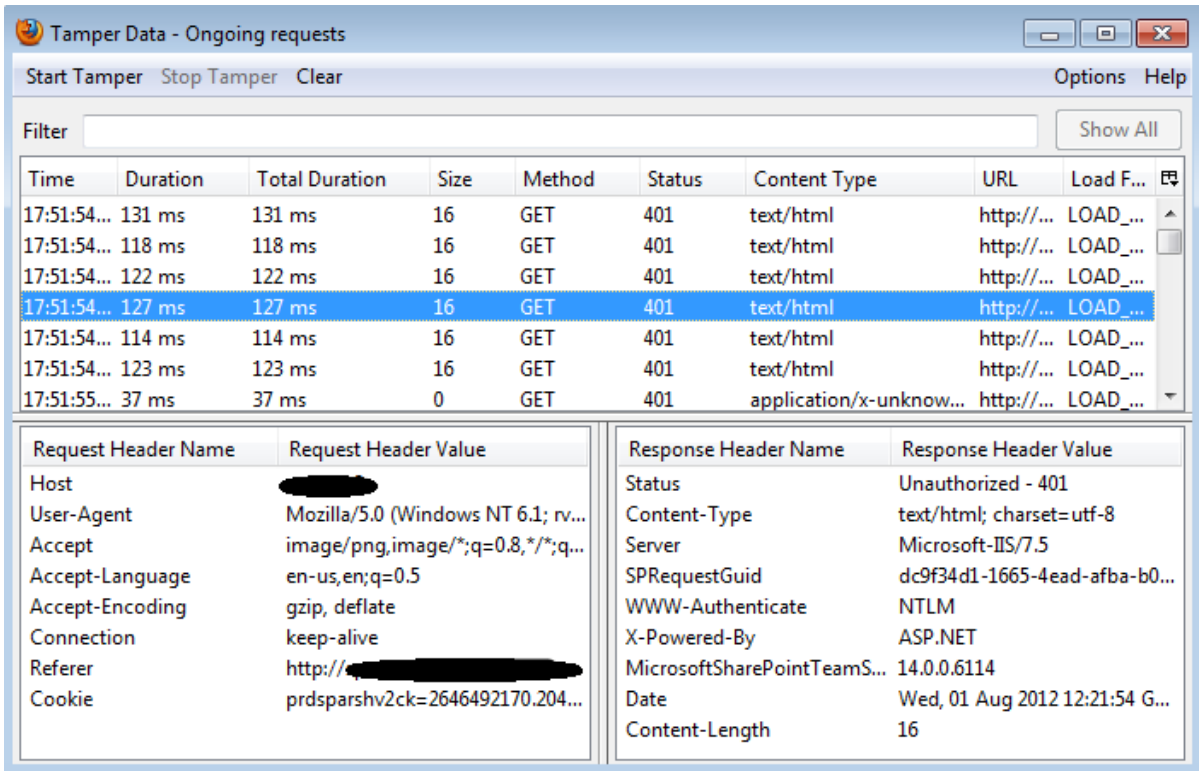
After clicking the Tamper Data the "Tamper Data - Ongoing Requests" window opens up.



As soon as this window is opened, Tamper data will start reading the HTTP requests. The window will look like this when it starts reading the requests.



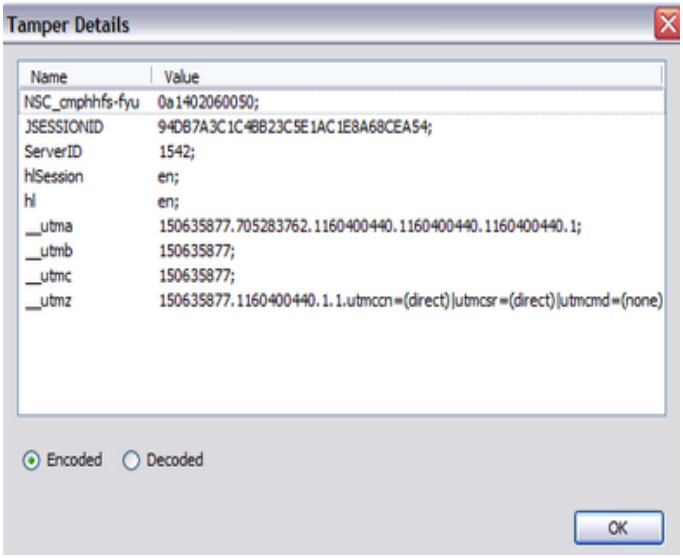
On selection of an item, its HTTP Request and Response information's are opened on the lower two left and right panes respectively.



Here we get a detailed view of what is going on in the request. If the selected request contains cookie information then we will see a cookie line in the left side pane or set cookie line in the right side pane or both.

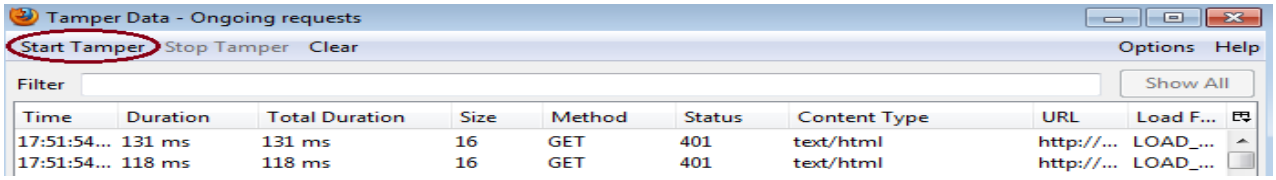
Now if we double click an entry then the "Tamper Details" window opens up, which provides us easy access to that request element's data.

Thus using the above process we can easily monitor what is going on during the browsing session.

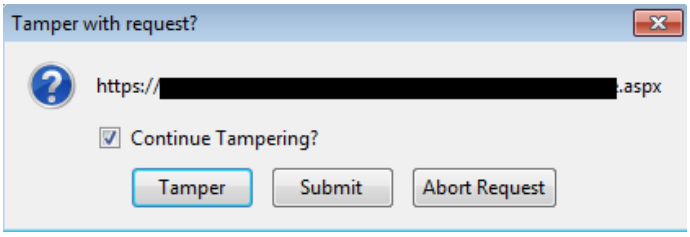


However till now we have just monitored the request. Tamper data can certainly do more than that. Now comes the sweet part of tampering the requests being made.

To begin we have to click on the option "Start Tamper".



From now on whenever the browser will make a request we will be prompted with three options...

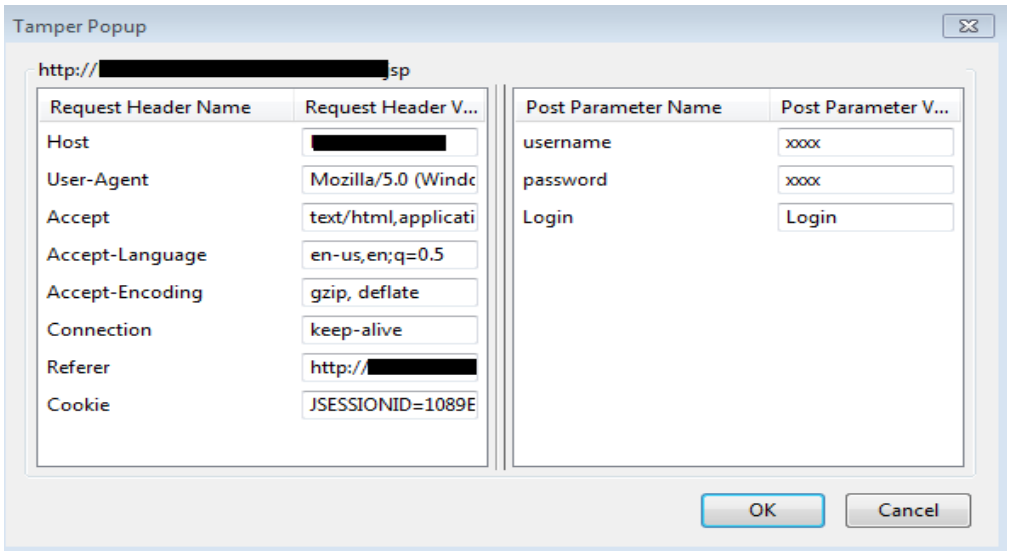


The three options are :

Submit → This just sends the request as it is without modifying it.

Abort Request → This, as the name suggests, will abort the request, i.e. will stop the request from being sent.

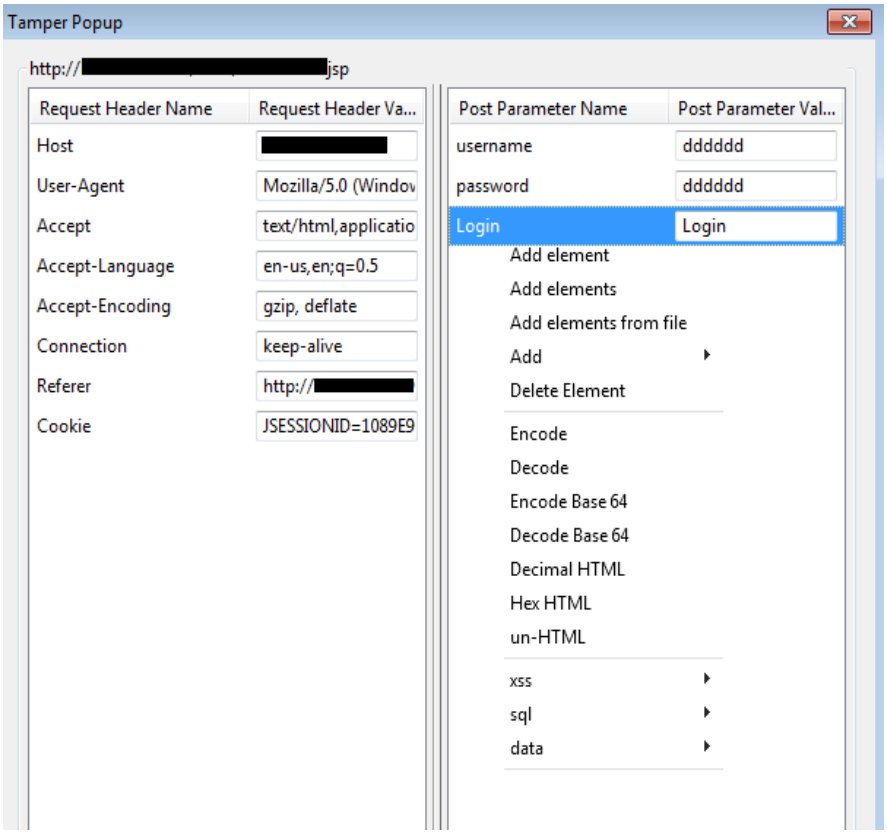
Tamper → This is the option which has made Tamper Data so famous and handy as well. When we click on this option, i.e. we want to tamper with the data, then a new window opens up.



On the top of the window (starting with the HTTP) is the URL the request is being sent to. On the left hand side pane we have the Request headers and their values. We can not only read them but also modify them as per our needs. On the right hand side pane we have the POST data of the request. Here we can see what POST fields are being sent and what are its values. We have a number of options here. On right clicking in the right hand pan we get the option to include our own elements which were not there earlier. Also on right clicking on the elements present we again get a handful number of options. These are very useful in manipulating the form in our own way and wish.

These numerous optionssaves us the effort of bypassing client side restrictions on what values may be sent or to submit an element not part of the form.

The only limitation of Tamper data is



that it can't modify http GET parameters. Otherwise Tamper Data is a neat tool by which we can easily see what our web application is doing, what are the parameters being passed etc.. With the help of this tool parameter manipulation has become literally a piece of cake.

Thus install this Firefox extension and enjoy the various offerings it has to offer.

Happy Hacking... ☺

Ramesh Chandra Bhattacharjee

Ramesh works for Infosys and is a beginner to information security domain.

Apple iOS vulnerabilities

Introduction

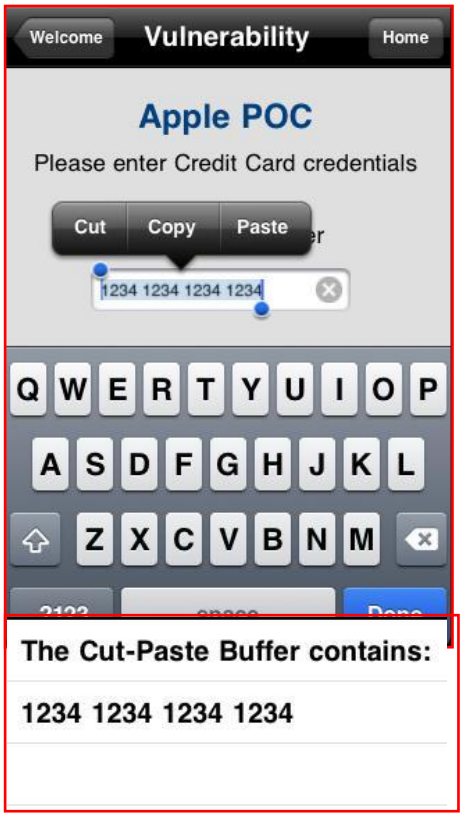
Apple iOS has successfully emerged as one of the most widely used Operating System today. It runs on Apple devices such as iPhone, iPad, iPod touch and Apple TV.

Apple AppStore has the highest number of applications (500,000) with 25 billion apps downloaded till date. However, the iOS developers aren't bothered about the secure aspect of the applications before they launch it on the AppStore. This huge number of apps and carelessness of developers has lured the hackers to steal data from the applications.

There has been numerous exploits exposed on the iOS platform. In this article, three such exploits will be discussed.Please note that these vulnerabilities can be only be exploited if the iPhone is jail broken and apps are installed out of Apple Store.

Cut & Paste Feature

Copy and Paste feature was introduced in iOS 3.0 which involves having a common buffer for all the applications in iOS. This feature can be exploited to steal sensitive data from an application into a malicious application.



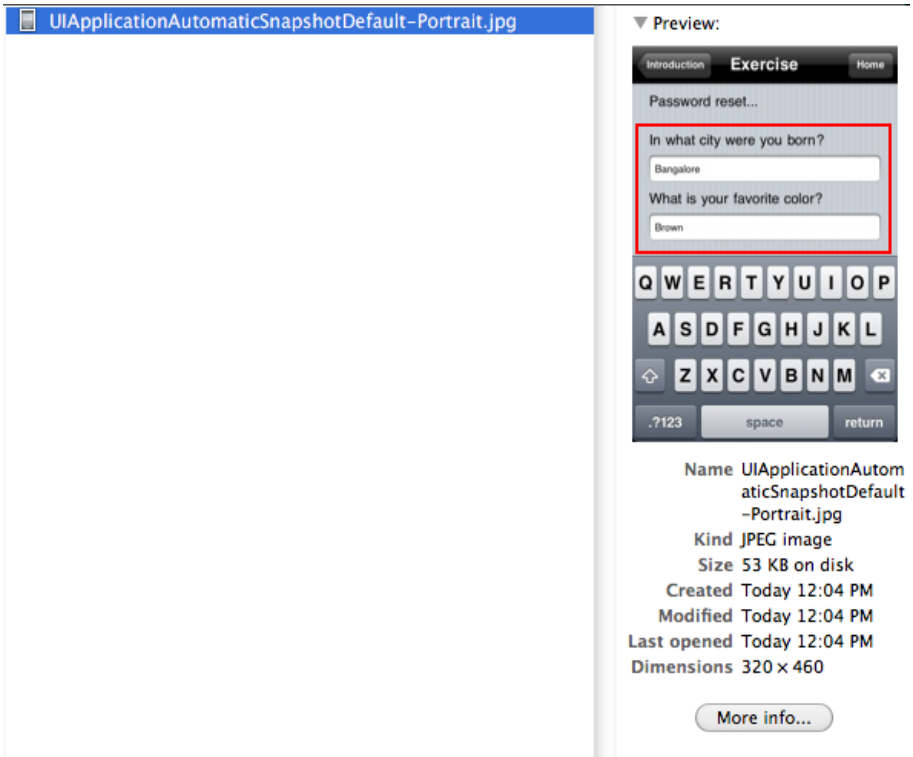
As shown in the above figure, at the top image, the credit card number is copied from the application, and it is stored in the common buffer within the iOS. Below, the malicious application is silently stealing data from the buffer and this applicationcan also remotely send the data to a remote server.

This issue can be remediated by the developer by either clearing the copy paste buffer every time the application exits, or disable the copy paste feature for applications which deal with sensitive data.

iOS Backgrounding

The Apple wanted to provide iOS device users an aesthetically pleasing effect when the application is entered or exited. Hence they introduced the concept of saving the last screenshot when the application goes into the background.

This feature can be exploited as the screenshot which is saved on the device may contain sensitive data like credit card details, Password recovery information etc.



The Fig. shows the user's password reset information stored in the screenshot. This screenshot is stored inside the iOS at the following location.

/private/var/mobile/Library/Caches/Snapshots

This issue can be remediated by the developer by writing a code snippet to clear the contents of the page on application exit.

Auto Correct Feature

Inside the iOS, there exist a file called dynamic-text.data , which is a binary keyboard cache containing ordered phrases of text entered by the user. This text is cached as part of the operating system's autocorrect feature, and may appear from entering text within an application on the device. Think of this as keyboard logger. Hence to avoid writing data to this cache, turn autocorrect off in text fields whose input should remain private, orconsider writing your own keyboard class for your application.

This file can be found on the device at the following location.

/private/var/mobile/Library/Keyboard/dynamic-text.dat

Sensitive data can appear in the autocorrect feature as a suggestion

As shown in the Fig-3, the username and passwords which are stored in dynamic text can appear on the screen asking for the user to choose that. The username and passwords will also be saved in the dynamic text file as it is being stored in a dictionary.

References:

1) OWASP Mobile Top 10 Risks.
2) Hacking & Securing iOS applications by Jonathan Zdziarski.

Anil Pai
anilpai@anilpai.com

Anil Pai is a Mobile App Security Analyst at Tata Consultancy Services with more than 2 years of experience. He is involved with security assessments of Apple iOS and Windows Phone 7 applications.

VARIOUS AUTHORITIES UNDER THE IT ACT

(1) Controller of Certifying Authorities (CCA)

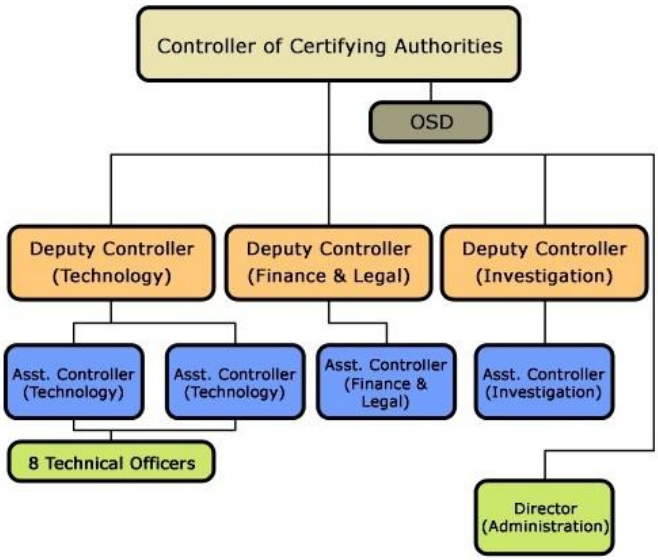
CCA is appointed by the Central Government under *section 17* of the IT Act.

Some of the functions of CCA are -

- Act. To exercise supervision over the activities of Certifying Authorities;
- To supervise public keys of the Certifying Authorities;
- To lay down the standards to be maintained by the Certifying Authorities;
- To specify the qualifications and experience which employees of the Certifying Authorities should possess;
- To specify the conditions subject to which the Certifying Authorities shall conduct their business;

Functions of the CCA are discussed in detail under *section 18* of the IT Act.

Organizational chart of the office of CCA



Controller's power to investigate the contraventions

Section 28 of the Act provides that, the Controller or any officer authorized by him shall have power to investigate contraventions as laid down in the provisions of this Act.

Important sections regarding CCA under the IT Act -

- **Section 17** - Appointment of Controller and other officers
- **Section 18** - Functions of Controller
- **Section 28** - Power to investigate contraventions

Website of the office of CCA - www.cca.gov.in

(2)Certifying Authority

Certifying Authorities (CA) has been granted a license to issue a digital signature certificate under *section 24* of the IT Act.

(3)Adjudicating officer (AO)

AO is appointed under section 46 of the IT Act to adjudicate offences under Chapter IX.

As per Rule 3 of the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003, it has been declared that the *Secretary of Department of Information Technology of every State and Union Territory shall serve as Adjudicating officer*.

Important sections regarding AO under the IT Act –

- **Section 46** - Power to adjudicate
- **Section 47** - Factors to be taken into account by the adjudicating officer

(4)Cyber Appellate Tribunal (CAT)

Cyber Appellate Tribunal has been established under the IT Act under the aegis of Controller of Certifying Authorities. It is established under Section 48(1) of the IT Act. Any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal.

Chapter X - Sections 48 to 64 of the IT Act has provisions regarding CAT.

Website of the office of CAT - http://www.catindia.gov.in

(5)Indian Computer Emergency Response Team (ICERT)

ICERT is the National Incident Response Centre for major computer security incidents in its constituency, i.e. Indian Cyber Community.

Under section 70B of the IT Act, ICERT has been empowered to serve as national agency for incident response.

Website of the office of CERT-In - http://www.cert-in.org.in/

(6)National Technical Research Organisation (NTRO)

NTRO is designated as the national nodal agency in respect of Critical Information Infrastructure Protection under Sec. 70A of the IT Act.

(7)Cyber Crime Cell

Cyber Crime Cell is a wing of law enforcement agencies like Police, CID, CBI, etc. established to expedite the investigation of Cyber Crimes.

Kindly note that, Cyber Crime Cell is not a Police station where one can go and register a complaint.

In India, Bangalore is the only city which has a Cyber Crime Police Station where one can register a complaint and can get a copy of the First Investigation Report (FIR).

Some of the duties of Cyber Crime Cell are –

- To assist law enforcement in investigating cyber crimes
- To spread awareness about cyber crimes and preventive measures in its territory
- To act as an expert in giving opinions on cyber crime related issues

Power to investigate offences under the IT Act is with the police officer not below the rank of Inspector as per Sec. 78 of the IT Act.

Sagar Rahurkar
contact@sagarrahurkar.com

Sagar Rahurkar is a Law graduate. He is a techno-legal consultant and a Senior Faculty at Asian School of Cyber Laws.

He specializes in Cyber Law, Cyber Crime Investigation, Computer Forensics and Intellectual Property Laws.

He teaches and provides consultancy to corporates, law enforcement agencies and education institutes across India.

He can be contacted at contact@sagarrahurkar.com.

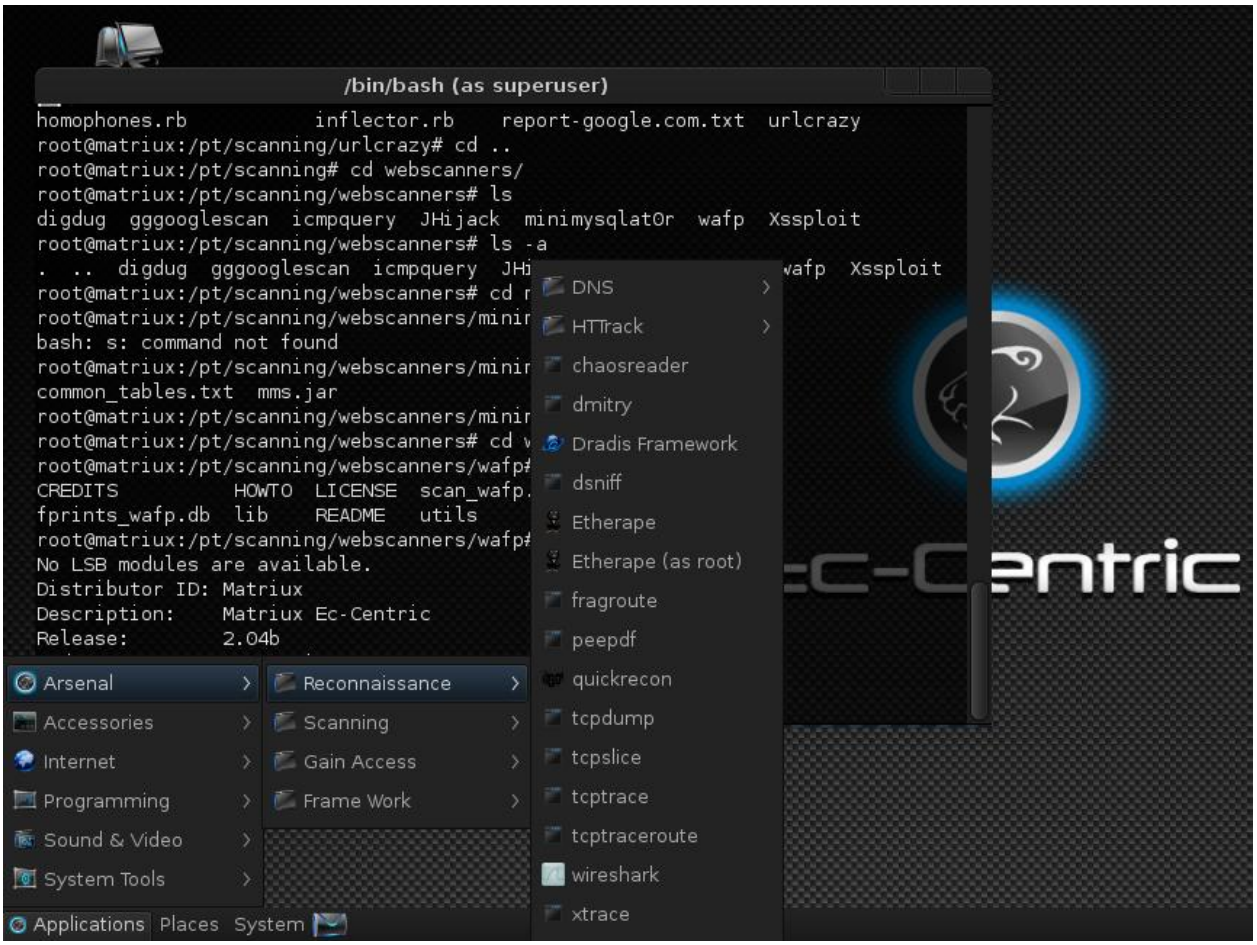
Matriux Ec-Centric

Hello every readers,

Matriux is been successfully running and getting a big support over the past 2 years and we have been working hard to provide the best security solutions and quality tools for all the penetration testing and forensic needs. On occasion this issue is to be released at c0con 2012, we are also proud to announce our upcoming release Matriux version 2.0 K0d3 name "Ec-Centric". We have been working hard over the release of the new version, so this month Matriux Vibhag will feature the Matriux Ec-Centric edition.

Features

- The "Arsenal" now includes around 325 powerful penetration testing and forensic tools and this time we included webshells making it the true arsenal for testing and cyber forensics.
- Also including the latest of tools and applications released at BlackHat 2012 US being the first distribution to include.
- Based on Debian Squeeze featuring the latest kernel 3.3.4.
- Custom compiled Kernel for high support for your hardware drivers along with squashfs and aufs modules.
- Lighter, Elegant and Faster UI with Gnome.
- Also making it more fast and easy to use.
- MID 0.3b to make the installation easier.
- Tools from Matriux Community.
- And the best part – runs easily on your 10 year old computer with p-IV and 256MB RAM with 6GB of HDD space.



Notable Updates

- More tools for VOIP and Forensics.
- Emphasis on Mobile forensics and malware analysis through security applications for Android and iPhone.
- Shell scripts.
- Build Update tool called “MUT”.
- And many more to check out at cocon 2012, be there as we will be there ;)

Happy Hacking and from next month we will continue with our regular tutorials on various security tools.

Team Matriux

http://matriux.com/

Get the best real-world Android training anywhere!

Attend AnDevCon IV

The Android Developer Conference

December 4-7, 2012

San Francisco Bay Area

Choose from more than 65 classes and workshops!

AnDevCon is the biggest, most info-packed, most practical Android conference in the world!

- Learn from the top Android experts, including speakers straight from Google!
- Attend sessions that cover app development, deployment, management, design and more
- Network and connect with hundreds of experienced developers and engineers like yourself

"AnDevCon is a fantastic conference! There is no better place to experience the latest and greatest technologies and techniques in the field of Android development. If you attend one conference this year, this one should be it!"

—Jay Dellinger, Senior Software Engineer, Manheim

Register Early and SAVE BIG!

www.AnDevCon.com

Follow us: twitter.com/AnDevCon

A BZ Media Event

ClubHACK

Security by luck, not possible!

Design : @pankit_thakkar