# ClubHACK Mag

1st Indian "HACKING" Magazine

## An attacker can hit you anytime

An attacker can hit you anytime

Issue 14 | Mar 2011
www.clubhack.com

**TechGyan** Remote Thread Execution in System Process | **ToolGyan** JS-Recon | **Mom's Guide** Choosing a Right Secure Mobile | **LegalGyan** Unauthorized Access | **Command Line** Backup & Bulk Copy | **Matriux Vibhag** Introduction – Part 1 |

Hello! I am the guy who manages the CHMag site. I keep these guys away from worrying about the magazine upload and the website! CHMag entered into its 2nd year with the last month's edition, february also witnessed nullcon's Second Edition where we all had a great time. It was last year nullcon where CHMag was launched. Also the Microsoft-Nokia deal leaved investors in cold with lot of rumors around.

***Abhishek Nagar***

Having said so much we present you the 14th Issue of CHMag with articles covering the latest HTML 5 based JS Network Reconnaissance Tool, Remote Thread Execution in System Process using NtCreateThreadEx, a guide on choosing the Right Secure Mobile and our regular Command Line by Rohit11and yes as a cherry on the cake we are also adding a new section named as Matriux Vibhag which would now provide you with a monthly dose of Matriux!!

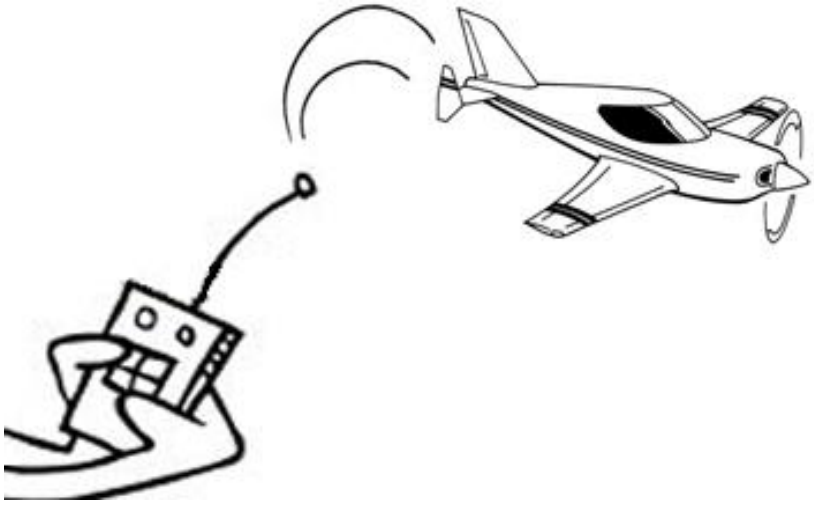
Feedbacks, Feedbacks and lots of them @ info@chmag.in are invited.

Have a Hacky month ahead.


Team CHMag
www.chmag.in
**Rohit** rohit@clubhack.com
**Abhijeet** abhijeet@chmag.in | **Abhishek** abhishek@chmag.in|
**Aarja** aarja@chmag.in| **Deepranjan** deepranjan@chmag.in|
**Pankit** pankit@chmag.in | **Varun** varun@chmag.in|

Issue 14, March 2011.
info@chmag.in

CONTENTS



# Remote Thread Execution in System Process using NtCreateThreadEx for Vista & Windows7

## Introduction

Windows provides API function called, CreateRemoteThread [Reference 2] which allows any process to execute thread in the context of remote process. This method has been mainly used to inject DLL into remote process, this technique is popularly known as 'DLL Injection'. Especially malware programs exploited this mechanism to evade their detection by injecting their DLL into legitimate processes such as Explorer.exe, Winlogon.exe etc.

## Vista & Session Separation

This DLL Injection technique using CreateRemoteThread technique has worked flawlessly till Vista without any limitations. However since Vista onwards things have changed with the introduction of 'Session Separation' [ Reference 3 ]. This was one of the many defenses introduced in Vista towards securing the system. 'Session Separation' ensured that core system processes including services always run in session 0 while all user process's run in different sessions. As a result any process running in user session failed to inject DLL into system process as CreateRemoteThread did not work across session boundaries.

This is clearly evident from the MSDN documentation of CreateRemoteThread [Reference 2] function...

"Terminal Services isolates each terminal session by design. Therefore, CreateRemoteThread fails if the target

process is in a different session than the calling process."

## About NtCreateThreadEx Function

With the failure of CreateRemoteThread, there was a need for universal solution for remote thread execution on Vista and Windows 7 platform. Then comes the function, NtCreateThreadEx [Reference 1], the undocumented function which provides complete solution for executing remote thread across session boundaries. It allows any process to inject DLL into any other process irrespective of the session in which it is running as long as it has sufficient privileges.

Here is the prototype of NtCreateThreadEx function [undocumented]

```
typedef NTSTATUS (WINAPI
*LPFUN_NtCreateThreadEx)
(
  OUT PHANDLE hThread,
  IN ACCESS_MASK DesiredAccess,
  IN LPVOID ObjectAttributes,
  IN HANDLE ProcessHandle,
  IN LPTHREAD_START_ROUTINE
lpStartAddress,
  IN LPVOID lpParameter,
  IN BOOL CreateSuspended,
  IN ULONG StackZeroBits,
  IN ULONG SizeOfStackCommit,
  IN ULONG SizeOfStackReserve,
  OUT LPVOID lpBytesBuffer
);
```

This function is almost similar to CreateRemoteThread function except the last parameter which takes unknown buffer structure. Here is the definition of that buffer structure parameter...

```
//Buffer argument passed to
NtCreateThreadEx function

struct NtCreateThreadExBuffer
{
  ULONG Size;
  ULONG Unknown1;
  ULONG Unknown2;
  PULONG Unknown3;
  ULONG Unknown4;
  ULONG Unknown5;
  ULONG Unknown6;
  PULONG Unknown7;
  ULONG Unknown8;
};
```

This information is derived based on reverse engineering work. Hence meanings and importance of internal fields of this buffer structure is not clear.

## Executing Remote Thread into System Process using NtCreateThreadEx

FunctionThe steps involved in the execution of the remote thread using NtCreateThreadEx is almost similar to that of CreateRemoteThread function. Hence the traditional steps such as allocating memory, copying the thread code into remote process are not repeated here. For detailed steps you can refer to article, "Three Ways to Inject Your Code into Another Process" [Reference 4].

Before we begin, we need to load NtCreateThreadEx function from Ntdll.dll as shown below.

```
HMODULE         modNtDll         =
GetModuleHandle("ntdll.dll");
if( !modNtDll )
```

```
{
      printf("\n failed to get
module handle for ntdll.dll,
Error=0x%.8x", GetLastError());
      return;
}
LPFUN_NtCreateThreadEx
funNtCreateThreadEx            =
(LPFUN_NtCreateThreadEx)
GetProcAddress(modNtDll,
"NtCreateThreadEx");
if( !funNtCreateThreadEx )
{
printf("\n failed to get funtion
address      from      ntdll.dll,
Error=0x%.8x",   GetLastError());
return;
}
```

Now setup the buffer structure which is passed as last parameter to NtCreateThreadEx function.

```
//setup and initialize the
buffer
NtCreateThreadExBuffer ntbuffer;

memset
(&ntbuffer,0,sizeof(NtCreateThre
adExBuffer));
DWORD temp1 = 0;
DWORD temp2 = 0;

ntbuffer.Size =
sizeof(NtCreateThreadExBuffer);
ntbuffer.Unknown1 = 0x10003;
ntbuffer.Unknown2 = 0x8;
ntbuffer.Unknown3 = &temp2;
ntbuffer.Unknown4 = 0;
ntbuffer.Unknown5 = 0x10004;
ntbuffer.Unknown6 = 4;
ntbuffer.Unknown7 = &temp1;
ntbuffer.Unknown8 = 0;
```

Finally execute remote thread 'pRemoteFunction' into remote process using NtCreateThreadEx function. Here one can use 'LoadLibrary' function address instead of 'pRemoteFunction' thread to implement 'DLL Injection' technique.

```
NTSTATUS status =
funNtCreateThreadEx(
        &hThread,
        0x1FFFFF,
        NULL,
        hProcess,
        (LPTHREAD_START_ROUTINE)
        pRemoteParameter,
        pRemoteParameter,

        FALSE, //start instantly
         NULL,
         NULL,
         NULL,
         &ntbuffer
         );
```

Now check for the result of NtCreateThreadEx function and then wait for it to execute completely.

```
if (hThread == NULL)
{
    printf("\n NtCreateThreadEx
failed, Error=0x%.8x",
GetLastError());
    return;
}

//Wait for thread to
complete....

WaitForSingleObject(hThread,
INFINITE);
```

Finally retrieve the return value from the remote thread function, 'pRemoteFunction' to verify the result of function execution.

```
//Check the return code from
remote thread function

int dwExitCode;
if(    GetExitCodeThread(hThread,
(DWORD*) &dwExitCode) )
{
     printf("\n Remote thread
returned with status = %d",
dwExitCode);
}

CloseHandle(hThread);
```

The steps illustrated above are almost similar except that here NtCreateThreadEx is used instead of CreateRemoteThread for creating thread in the context of remote process

## Limitations of NtCreateThreadEx Method

Though NtCreateThreadEx provides universal solution on Vista/Win 7 platform for remote thread execution, it is risky to use in the production code as it is an undocumented function. As things may change with new version and suppor packs, enough testing is necessary before putting it into production especially when injecting code into system critical process such as LSASS.EXE, CSRSS.EXE.

Another limitation is that it cannot be used in earlier platforms before Vista, such as Windows XP because NtCreateThreadEx function is available only Vista onwards. However developers can easily tune their code to dynamically use CreateRemoteThread function on XP and NtCreateThreadEx for Vista/Windows 7.

## Alternative Techniques

Another way to inject DLL into system process is to write the service process (which will run in session 0) and then issue the command from user process to that service to inject DLL into any system process using the CreateRemoteThread function.

This technique will work for any system process running in session 0. But it will fail to execute thread into any other process running in session other than 0.

Though it is a clumsy way of doing the work, it still holds good solution to inject thread into system process only.

## Conclusion

This article provides practical implementation of using NtCreateThreadEx function to execute remote thread into any process on Vista/Windows 7 platform. Though it is undocumented function, it provides universal solution for executing code in any process across session boundaries imposed by Vista/Windows 7.

## References

1. NtCreateThreadEx Function
2. MSDN Documentation of CreateRemoteThread Function
3. Impact of Session 0 Isolation on Services
4. Three ways to inject code into remote process

Nagareshwar is a security professional with the unbeaten passion towards Computer Security, 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.

# JS-Recon

# JS-Recon : JavaScript Network Reconnaissance Tool

## Introduction

When I say 'Network Reconnaissance' then most of you would immediately think Nmap! Some of the more hardcore geeks would also be thinking about Scapy. Both are awesome tools and are probably the best of their class but what happens when you want to do a quick network recon from a machine where:

1) No tools are installed

2) You do not have administrative rights

3) You cannot install or download any binaries or zip files due to proxy filtering

The above three points are a fair accurate representation of the status of the internal network of a lot of companies. Along with these restrictions if access to command prompt is blocked then you cannot use ping/telnet for your recon as well.

## JS-Recon

JS-Recon is a network reconnaissance tool written in JavaScript by making use of HTML5 features like Cross Origin Requests(CORs) and WebSockets.


**Figure 1: Port Scans**

JS-Recon can perform:

* Port Scans
* Network Scans
* Detecting private IP address

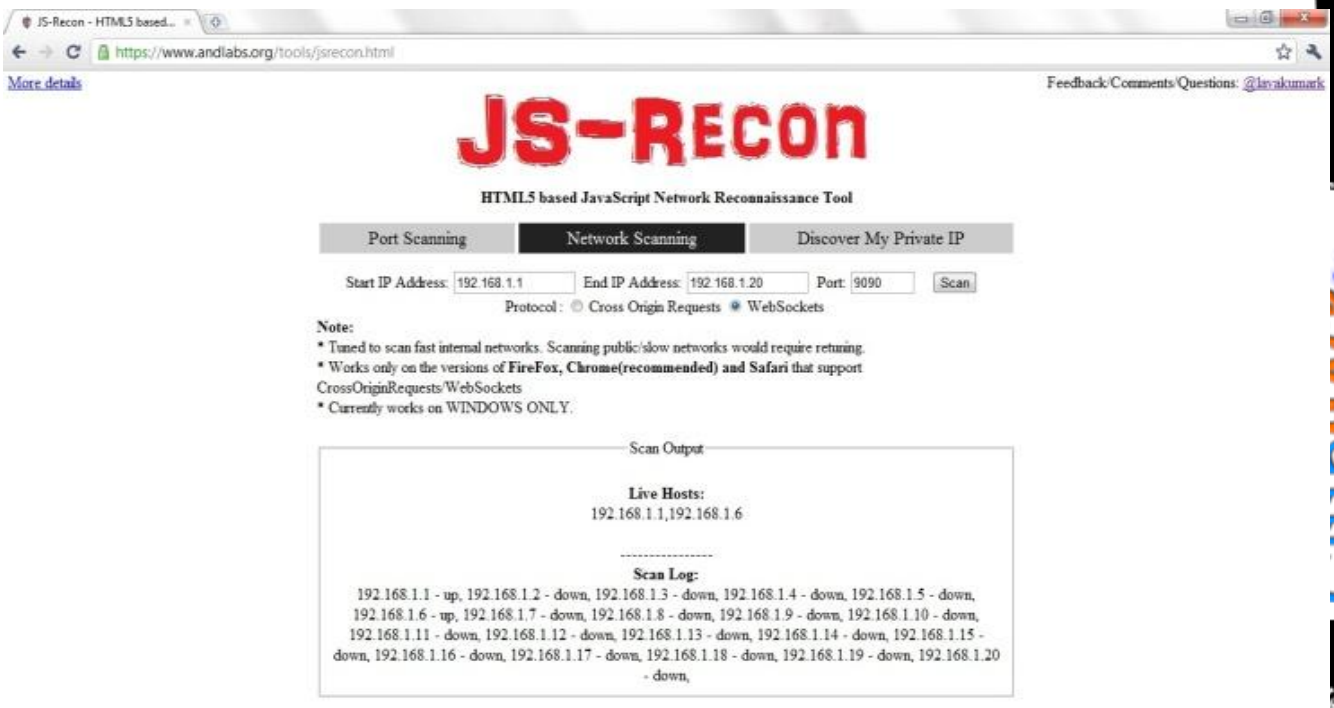



**Figure 2: Network Scans**

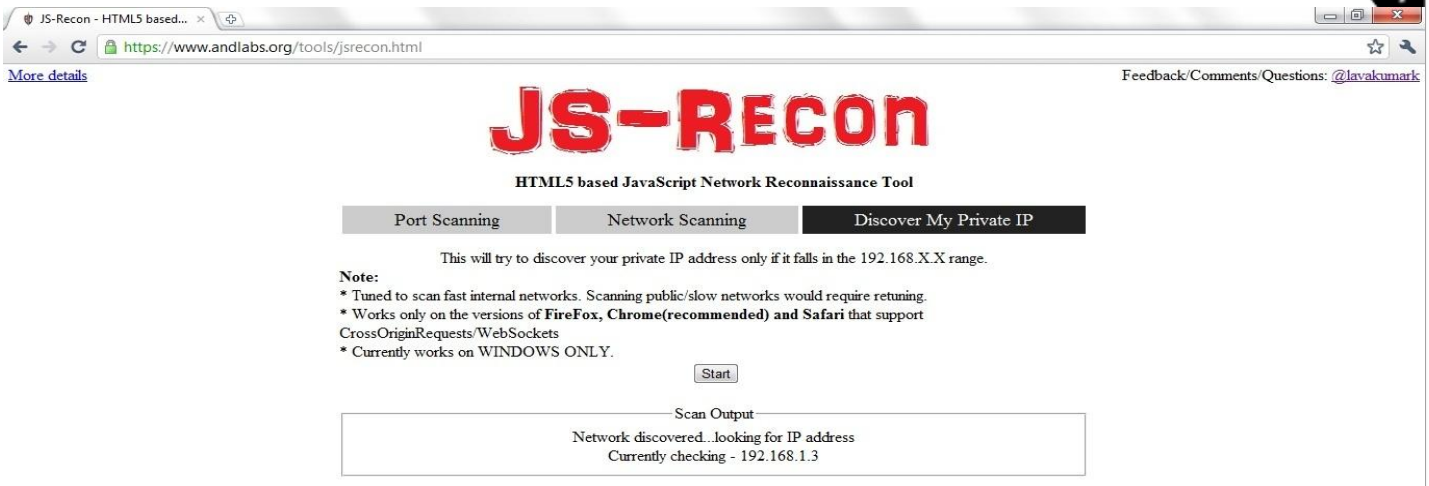



**Figure 3: Detecting Private IP address**

It is currently a windows only tool and works on modern browsers that support Cross Origin Requests or WebSockets. I have personally found Chrome to be the ideal browser to run this.

Using JS-Recon is very straight forward, it has a simple UI where the user selects the type of scan, enters the target IP addresses, port numbers and hits 'Start'.

The underlying base of any of thses scans is the ability to identify if a remote port is open or closed by using JavaScript. These are not socket-level scans like those done by Nmap but are application-level scans. To get the best out of the tool the user has to understand the underlying scanning technique employed by JS-Recon.

Cross domain XHR has five possible readystate statuses and WebSocket has four possible readystate statuses. When a new connection is made to any service the status of the readystate property changes based on the state of the connection. This transition between different states can be used to determine if the remote port to which the connection is being made is either open, closed or filtered.

When a WebSocket or COR connection is made to a specific port of an IP address in the internal network the initial state of WebSocket is readystate 0 and for COR its readystate 1. Depending on the status of the remote port, these initial readystate statuses change sooner or later. The below table shows the relation between the status of the remote port and the duration of the initial readystate status. By observing how soon the initial readystate status changes we can identify the status of the remote port.

Behavior based on port status:

| Port Status | WebSocket (ReadyState 0) | COR (ReadyState 1) |
|---|---|---|
| Open (application type 1&2) | < 100 ms | < 100 ms |
| Closed | ~1000 ms | ~1000 ms |
| Filtered | > 30000 ms | > 30000 ms |

**Figure 4: Port Status**

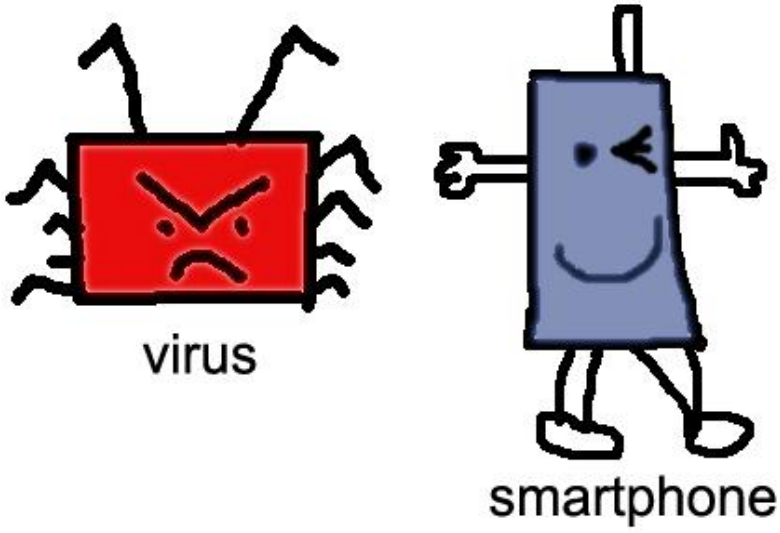
The port scanning technique can be applied to perform horizontal network scans of internal networks. Since both an open port and a closed port can be accurately identified, horizontal scans can be made for specific ports that would be allowed through the personal firewalls of most corporate systems.

As explained above the port status determination is majorly dependent on timing, therefore the location of the destination server is very important. JS-Recon is tuned for targets that are located in the internal network, if the user wishes to scan targets across the internet then he has to retune it.
A more detailed description of how Port scans, Network scans and Internal IP Detection work is mentioned in the JS-Recon Manual [http://www.andlabs.org/tools/jsrecon/jsrecon.html].

Happy Scanning! ☺

**Lavakumar Kuppan**
**http://andlabs.org/**

Lava is a Penetration tester and Security Researcher.




# Choosing a Right Secure Mobile for Yourself

## Introduction

Mobile phones have now become capable of performing much beyond than simply managing calls and messages. From just mobile phones initially they have evolved into smart-phones. From serving as a dedicated Camera, to solving almost all the purposes of a mini computer, mobile phones are everywhere. Powered with 3G services, "super-mobiles" will replace computers and laptops very soon.

This advancement in the mobile technology comes at a cost of a very important thing- Security. Mobile devices and the data stored on them are of critical nature for the owner, and if the device is lost then confidentiality of the user data can be at stake, if proper security mechanisms are not implemented. The purpose of this article is to create awareness about the security features, which a buyer/user should keep in mind before purchasing a mobile phone. I have tabulated these features below. Let's look at them one by one.

## Phone Lock and SIM Lock

Any device (a low-end or high-end) comes preloaded with some of the basic security features. Capability of locking a phone and/or SIM card is definitely one of them. The phone should be capable of getting locked all by itself, if it is kept idle for some time. Also, mechanisms should be in place to set/reset the pass code whenever user wants to do so. In case of a phone restart, the phone should prompt for the pass code and SIM code. The phone should get "bricked" after a definite number of unsuccessful attempts.

## Application Lock

The phone should provide basic mechanisms to restrict access to sensitive applications like Camera, Contacts, Messaging, Internet, Phone Settings etc. The phone should prompt for a pass code, every time someone wants to access those applications, even if the phone is in unlocked state.

## Mobile Tracker

The phone should come preloaded (or at least support) with a mobile tracking application. When turned on, the mobile tracker sends messages to designated numbers, whenever the SIM card is changed. So, in case of a theft, the mobile tracker can be used to locate the mobile phone.

## Encryption

The data stored in the mobile phone can be compromised if it is not encrypted. Proper encryption mechanisms should be put in place to make sure that the data residing in device memory and on memory card is encrypted. The access to memory card should be password protected. If taken out, the memory card should corrupt itself.

## Protection against Malware

With the increase in the usage of internet, threats from Malwares and Trojans have increased. A good built-in/downloadable anti-virus should be available for the device which you are going to buy. Also, the Anti-virus should be configured properly to make sure hourly/daily scans and updates.

## Bluejacking

Bluetooth is another entry point for the malwares. Malwares can be delivered by using the connectivity services supported by a device left in discoverable mode. The mobile should be configured to turn off Bluetooth, if it is left unused for a definite amount of time.

## Remote-Wipe

In case of a theft, the data residing on the mobile is in risk of being compromised. To circumvent this problem, provisions should be made to ensure a remote-lock and/or remote-wipe of the data present on the device.

## Certificate Check

In the present world of mobile apps, it is possible to download/install a Malware along with an app. To ensure safety against them, proper mechanisms should be put in place to check for the certificates/signed-unsigned status of the app which is currently being installed on the device. The phone setup should accommodate features to turn the certificate check ON. Also, any application which is doing unauthorized things like establishing an internet connection without user's permission should be removed from the mobile phone, even if it is signed.

## Safety for Online accounts

Smart phones are a good tool to remain connected to the world not only by means of the basic telephony services but also by using the internet connectivity which they readily provide. The phone should at least provide basic encryption mechanisms for such connections. The password, for ex, should never be sent in the clear text. Data like cookies and session variables should be stored in a location which is inaccessible to the user.

Although, the list provided above is not an exhaustive one, in this article I have tried to cover all the main security mechanisms which must be present in a smart phone in order to make it do smart things in a safer way. In order to get any clarifications, you can reach me at Shivendra.Saxena01@gmail.com.
Happy Smart-Phoning !!


## Shivendra Saxena

Shivendra Saxena is currently working with Infosys Technologies ltd as a Security Consultant. He has a hands-on experience on secure code analysis tools like Codesecure and AppScan. He latest area of research is Mobile security. He is a part of Infosys Mobile security solutions team.


# Law relating to Unauthorized Access

## Introduction

One of the most publicized risks to information systems is that of unauthorised access, often referred to as hacking. For some, hacking is seen as something that happens to other people typically large or high profile organisations. But this is not the case, as use of the Internet grows, so too does the number of attacks.

Generally, Unauthorized Access is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner.

## Unauthorized Access under IT Act

Law of Unauthorized access has been described under three sections, viz. Sec. 43, Sec. 66 and Sec. 70.

Before understanding meaning of **Unauthorized Access,** let's first understand the term "access".

Sec. 2 (1) (a) defines access as "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

Here, "gaining entry into" also applies to physical access, e.g. a massive supercomputer is located in a room. Rohit

breaks its door and entered into it. He has gained access to the computer.

**Section 43:- Penalty and compensation for damage to computer, computer system, etc.**

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,—

a) accesses or secures access to such a computer, computer system or computer network or computer resource;
b) downloads, copies or extracts any data, computer data base or information from such a computer, computer system or computer network including information or data held or stored in any removable storage medium;

*Explanation. — For the purpose of this section,—*

- *"computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;*

c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer network;

*Explanation. — For the purpose of this section,—*

- *"computer contaminant" means any set of computer instructions that are designed—*

*(1) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or*

*(2) by any means to usurp the normal operation of the computer, computer system, or computer network;*

- *"computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the*

*performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource; by any means.*

d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such a computer, computer system or computer network;

*Explanation. — For the purpose of this section,—*

- *"damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.*

e) disrupts or causes disruption of any computer, computer system or computer network;

f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

h) charges the services availed by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

j) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

*Explanation. — For the purposes of this section,—*

- *"Computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.*

Punishment for contravening provisions of this Section is *to pay damages by way of compensation to the person affected.*

**Sec. 66:- Computer related offences**

If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

*Explanation.—for the purpose of this section,—*

*(1) the word "dishonestly" as per section 24 of the Indian Penal Code means "Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".*

*(2) the word "fraudulently" as per section 25 of the Indian Penal Code means, "A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise".*

**Sec. 70:- Unauthorized access to protected systems**

1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

*Explanation.—For the purpose of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.'*

2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1).

3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

Appropriate Government is determined as per Schedule VII of the Constitution of India. Schedule VII contains three lists:-

- Union
- State
- Concurrent

Central Government (parliament) has exclusive rights to make laws on items mentioned in the Union list. E.g. Defence, banking, economy, foreign relations, atomic energy, etc.

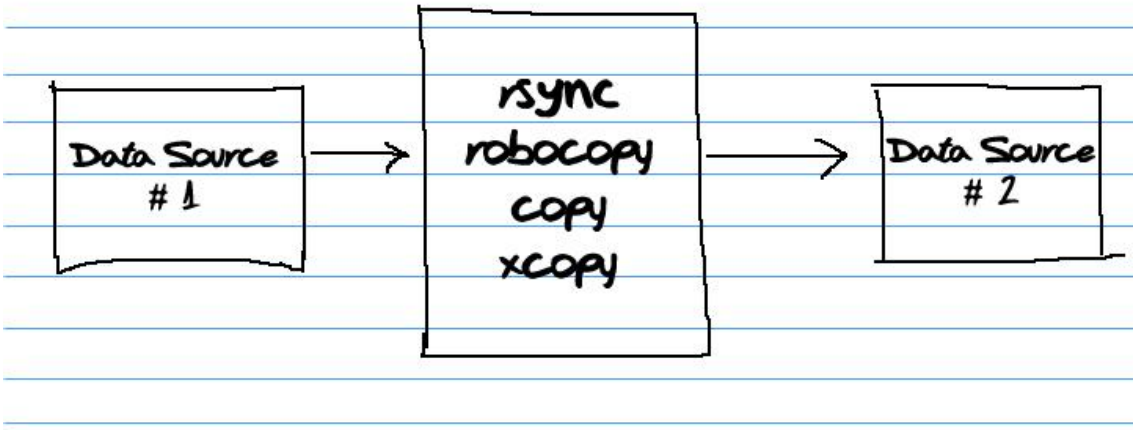
State Government has exclusive rights to make laws on the items mentioned in the State list. E.g. Police, law & order, local government, etc.

Central as well as state government has powers to make laws on the items mentioned in the concurrent list. E.g. electricity, forests, etc.

**Illustration: -** If the computer network of the RBI has been declared as a protected system, Central Government would be the responsible Government.

**Sagar Rahukar**
**sr@asianlaws.org**

Sagar Rahukar, 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.




# Backup & Bulk Copy

During academics, we have heard so many times about backups. In offices we have costly utilities to do such stuff too, but when it comes to personal data on laptops / desktops, we need something which can make our backup process better. After all we'll be backing up large files music & movies too ☺

In this issue of command line gyan, we'll see how we can use command line utilities to sync our folder locations and backup effectively. Although we talk about backup, this can be used for multiple activities as per user choice

## Linux

So far the best know utility in Linux to sync data is RSYNC
The best part with rsync is that it allows copy recursively within one machine and even remote machines as well.

As the name suggests, it's a sync utility which means will copy only the changes and not the whole file and it also maintains file ownership and permissions

The usage is pretty simple

$ rsync [options] source destination

For example

$ rsync –arH /home/clubhack/ /mnt/backup

I commonly use –arH options helps archiving the data (the a bit), does it recursively including subdirectories & maintains the hardlinks

Now if you want to use the same rsync to transfer file on remote machine, the best option would be

$ rsync -aH /my_dir/ remoteIP:/path/to/dir/

To preserve permissions, ownership, group & timestamp you can choose to use switches like -p, -o, -g, -t etc.

You can even choose which files to be included or excluded in your syncing.

I'd strongly urge you to go ahead and check the man page of rsync. If you are not using it, you are missing something very important.

## Windows

For windows environment till XP we haven't seen any such wonderful utility inbuilt.

Although commands like copy & xcopy are there but they are not as versatile & flexible as rsync.

To enjoy the features of rsync I'd recommend using it via cygwin or directly via the windows binary of rsync.

If you are one of those who hate linux binaries on windows, you can try using robocopy

Robocopy or "robust file copy" is a part of windows resource kit since NT4 and now it has been added as standard utility in windows vista, 7 & server flavors.

If you have moved to windows vista or above, then go ahead & fire

C:\>Robococpy /?

Robocopy an be used as extensively as rsync. Like if you want to copy a folder from one location to another, simply go ahead and type
C:\> robocopy C:\my_dir d:\my_dir /s

/s here copies the subdirectories too.

And similar to rsync when we need to transfer the file on remote machines, we can go ahead and use standard windows command method

C:\> robocopy my_dir \\remote_machine\backup_dir /s /z

/s for recursive copy
/z for maintaining filecopy even beyond network disconnections

If you want to make an exact copy & replicate deletion of file from to be matched at another, try /MIR which stands for mirror.

The main idea about using command line tools for file copy & backups, you can create your own scripts and use backup more efficiently

---

BTW, some people sent me mails that I don't cover the commands in depth. Dear readers, the idea is to point you to right tool, its your homework then to explore the features and use it to the best. And yes, if you explored nicely you can even submit your article for this section of the magazine ☺

**Rohit Srivastwa**
**rohit@clubhack.com**


# Matriux Vibhag Introduction – Part 1

## Introduction

Everybody wants to do something innovative and unique in life. This was the zeal behind Matriux. Matriux is a phenomenon that was waiting to happen.

Team Matriux is extremely honored to be associated with CHMag for starting an exclusive section for Project Matriux. Various articles and tutorials will be published through this section titled – "Matriux Vibhag".


## So what is Matriux?

Matriux is not just about a security distribution that can run from a CD / DVD / USB. It is something more than that. Project Matriux consist of the following.

- Security Distribution – Matriux Lithium and Matriux Xenon
- MSTF – Matriux Security Testing Framework
- DVM – Damn Vulnerable Matriux
- The k0d3 – (pronounced 'the code')

## Security Distribution

The first question that comes to mind when we talk about a new security distribution is – "why another distribution (when we have so many)? The answer is very simple – just following the spirit of Linux.

## MSTF - Matriux Security Testing Framework (under development)

MSTF is a security testing framework that will help you to carry out a penetration testing based on the workflow following the best practices and standards followed in the industry. The tool will guide

you through each step of the testing process and present the user with a comprehensive report covering every details of the test carried out. In simple words – MSTF is a tool with process oriented approach towards security testing with clear emphasis on the deliverables.


## DVM - Damn Vulnerable Matriux (under development)

The objective of Damn Vulnerable Matriux is to create a learning platform for creating and exploiting vulnerabilities. The project is currently under development and is lead by Prashant KV.

## The k0d3 - (pronounced 'the code')

The k0d3 is an initiative to promote secure coding practices targeted both at the academic and professional level. The project will have various activities that will help both students and professionals understand the concept and importance of coding securely. The project also aims at providing insight into coding security tools and applications.

Before we conclude with the first part of introduction let's have a glance at the existing scenario of the project, Matriux has released two flavors in its course. The first one being Matriux Lithium a Kubuntu based KDE distribution released in December 2009 and the other Ubuntu based Gnome Flavor Matriux Xenon both having their own significant features and advantages for the users.

## Conclusion

In the next edition, we will provide more information about how it all started and the future of Matriux Project and how individuals and organizations can contribute towards the project. After the introduction to Matriux is over, a series of tutorials based on various tools and projects are also planned exclusively for the CHMag.

*Happy Hacking and Happy Learning.*

**Matriux Team**
( http://matriux.com/ )


Photography: Nikhil Sharma
nikhilsh1@gmail.com
Design: @pankit_thakkar

Issue 14 | Mar 2011
www.clubhack.com