

# Forum:[Hack Forums](#)

Thread: [???? \[TUT\]Hack Windows XP with Metasploit\[TUT\] - HD Pictures ????](#)

**Numinous** - *October 26, 2012, 11:28 am*

[TUT]Hack Windows XP with Metasploit[TUT] - HD Pictures

Step 1-

Spoiler [\(Click to View\)](#)

Step 2-

Spoiler [\(Click to View\)](#)

Step 3-

Spoiler [\(Click to View\)](#)

Step 4-

Spoiler [\(Click to View\)](#)

Step 5-

Spoiler [\(Click to View\)](#)

Step 6-

Spoiler [\(Click to View\)](#)

Step 7-

Spoiler [\(Click to View\)](#)

Step 8-

Spoiler [\(Click to View\)](#)

Step 9-

Spoiler [\(Click to View\)](#)

Step 10-

Spoiler [\(Click to View\)](#)

Step 11-

Spoiler [\(Click to View\)](#)

[Hack Windows 2000](#)

[Hack Windows XP](#)

[Hack Windows Seven](#)

To Get Fully Detailed E-Book - Please POST Here (Don't PM Me)

**pashabiceps** - *October 26, 2012, 2:11 pm*

Windows XP is the most vulnerable windows OS via LAN attacks

**Nasrat597** - October 26, 2012, 2:14 pm

may i get this ebook ?

thanks

Eid-Mubarak

**fred goffa** - October 26, 2012, 2:49 pm

anyone can hack a windows xp system or 2003, ms08 or ms03. But the question is from a external point of view , if ur attacking a home machine, port 445 or the netbios ports required to hack it wount be open in most case, because of router or firewall, and most servers that are hosted never use windows xp so u wount see this type of vulnerability occuring anywere, i havent seen this vulnerability since the year 2006

**Silent1ntruder** - November 2, 2012, 8:13 pm

Another great tutorial, good job. Can I get the ebook pls? Would be much appreciated.

**Sonic Boom** - November 3, 2012, 1:07 am

Hey this tutorial was awesome! The Windows 7 one too. May I get the ebooks for both hacking XP & 7 ? I would like to see if I can do this outside a LAN. Thanks!

**GosthShadow** - November 4, 2012, 4:23 am

Great job, looks very informative.

Can I have the eBook? Thanks :)

**gizmodo** - November 5, 2012, 9:59 pm

(Oct 26, 2012 02:49 PM)fred goffa Wrote: [\[CITE\]](#) anyone can hack a windows xp system or 2003, ms08 or ms03. But the question is from a external point of view , if ur attacking a home machine, port 445 or the netbios ports required to hack it wount be open in most case, because of router or firewall, and most servers that are hosted never use windows xp so u wount see this type of vulnerability occuring anywere, i havent seen this vulnerability since the year 2006Agreed, this exploit is been more than 6 years old, and it looks like it came from SecurityTube Metasploit Framework Expert tutorials. they use old system to exploit.

**sharkworm2501** - November 5, 2012, 11:13 pm

love this tut man very nice and detailed thanks :D

**iSevere** - November 6, 2012, 9:15 am

Can i have this please?? Thanks. Good work.

**jigarladhava** - November 6, 2012, 11:57 pm

Can i have one plz ? Nice Job Dude

**The Fifth Of November** - November 7, 2012, 12:32 am

I want this man,  
thanks in advance.

**NiGGA CODING** - November 7, 2012, 1:36 am

Every time I try this exploit it just says no target found... (on armitage) is this antivirus or did I do it wrong?

**\_Baphomet\_** - November 9, 2012, 1:55 pm

I've heard of this. Apparently, it's only SP2 and up (Tested XP SP2/3) but fails on SP1.

**fristpharaoh** - November 9, 2012, 1:58 pm

Impressive tutorial , I'd love to have eBook , Please send me the link , Thanks In Advanced for Sharing this mate  
Cheers ;)

**MitchellHax** - November 9, 2012, 2:22 pm

Can i have one plz ? Nice Job mate seems cool

**RepairMe** - November 11, 2012, 2:11 am

Very Impressive. I'm on XP and that scared me a little bit considering I have test lab on that OS also. May I please have the ebook for such a feat? I'm new here and didn't realize, I came looking for commview help with my Proxim. Thanks again!

**lalo** - November 11, 2012, 1:25 pm

Can i have this please?? Thanks. Good work.

**back3n** - November 21, 2012, 7:09 am

nyc job.. wil you pls send me ebook link thanks

**Shagrath** - November 21, 2012, 7:18 am

can i get this e book

thanks in advance

**hacksaw24** - November 30, 2012, 4:35 am

may i get this ebook sir? thanks in advance! :)

**Mackful** - December 2, 2012, 1:03 pm

Looks like a great couple guides you put together, looking forward to reading them. :)

**koyd** - December 2, 2012, 1:26 pm

i would love to read your e-book  
would love to have it  
thanks in advance

**Polite** - December 4, 2012, 1:46 am

Thanks for this. I really got one, with Kaspersky enabled.

**Mingle** - December 4, 2012, 7:26 am

Great tutorial.

Can I have the e-book?

Thanks in advance.

**T34bagm** - December 4, 2012, 12:31 pm

Hey man! I would very much love to have this E-book! Could I please get a link! Thanks in advance man!

**chawk** - December 4, 2012, 12:44 pm

(Oct 26, 2012 02:11 PM)pashabiceps Wrote: [\[CITE\]](#) Windows XP is the most vulnerable windows OS via LAN attacks

True dat....Im trying to resolve those issues now.

**aymi68** - December 6, 2012, 1:46 pm

Can i get the e-book please? Thank you !

**chronical\_damage** - December 7, 2012, 5:15 pm

Could I please please have it??? Thank you :)

**brightrollwtf** - December 9, 2012, 3:31 pm

This tut really gives an easy to follow guide. Are there any good exploitable XP ISOs out there to download?

**troyyashverma** - December 15, 2012, 9:21 am

looks very informative.

Can I have the eBook?

**psycho001011** - December 16, 2012, 9:22 am

Great tutorial. Can i get this ebook ?

**D4yZ\_** - December 17, 2012, 12:21 pm

Can i have this please?? Thanks. Good work.

**clapashiya** - December 22, 2012, 8:45 pm

can i get the book ???

thanks in advance man

**TheMaTriX32** - December 23, 2012, 6:11 am

Look Like A Very Good Tutorial

Thank You.

**rix007** - January 9, 2013, 12:49 pm

Thanks for the info.

Can I have the ebook?

**SIM-553562** - January 10, 2013, 2:01 pm

just another very good tutorial from you! Keep up the excellent work and stay HQ ;)

-Manolis

**Scrat** - January 11, 2013, 1:00 pm

Hmm it'd be very nice if you gave me this ebook mate :P

**illi L???Y illi** - January 28, 2013, 1:00 pm

Nice share bro. I'd like to have your e-book. Let me get a link in PM please.

Thanks for the share.

**nick\_bachelor** - January 31, 2013, 11:45 am

can i have the ebook thanks in advance :)

**Emyli** - January 31, 2013, 3:03 pm

Looks good. However, I agree with anyone and everyone who says winxp is so easily hackable. agreed. I'm more interested in Windows 7/Windows 8. ....I hate windows 8 so much, and it refuses to leave willingly.

**umeysh** - February 4, 2013, 2:48 am

hey dude plz gv me link of book thnx

**BlackTrojan** - February 10, 2013, 2:44 am

Thank you so much friend. Can i have the link of book please ? I want to know if i can do this outside the LAN.

**420united** - February 10, 2013, 8:48 am

Thank you a lot for this very dedicated and delightful tutorial at least some people are still taking time to write something useful

**Head16** - February 10, 2013, 12:27 pm

Can i get a E-Book , THank you in advance.

**genius617** - February 10, 2013, 2:18 pm

Great job, looks very informative.

Can I have the eBook? Thanks :)

**chotzo** - April 15, 2013, 1:16 am

Good work ! Thanks.. Can I have the ebook ?

**Changement** - April 16, 2013, 1:18 am

Nice tutorial, this was well explained!

**Krueger** - September 17, 2013, 11:47 am

Could you PM this one as well ? Thanks Sir.

**netwise** - September 23, 2013, 1:11 pm

Thank you for your work.

I'm just starting to use metasploit  
in practice very well.

**warl0ck08** - October 7, 2013, 1:37 am

I just want to take a look on your ebook can you share it to us.?

**AcidRainCM** - October 7, 2013, 4:06 am

I'd like to get this ebook aswell please :)

thank you  
greetings :)

**bankbouy** - October 8, 2013, 5:48 am

Good job i will try hope work Thanks

**ClaudineMar** - October 26, 2013, 5:24 am

THanks.

It does not work for me it gets stuck on

"Attempting to trigger the vulnerability".

Any suggestions?

THANK you masters

**ani\_1** - October 30, 2013, 4:27 am

Thank You... will surely follow it someday

**TheNeutron** - October 31, 2013, 11:35 pm

I'd like the PDF please, And Nice tutorial :)

**?O?AL€™** - November 2, 2013, 9:31 pm

can I have Fully Detailed E-Book please ? :)

Thanks

**anonymousram** - November 3, 2013, 9:22 am

can i get this Ebook. .please. Thanks in advance

**imakehitz** - December 1, 2013, 10:51 am

thank you sir, Great tutorial && share...

**levieux100** - December 1, 2013, 11:56 pm

good tutorial bro, can i get the ebook pls ?

**?lex** - December 2, 2013, 1:12 am

Exploiting Windows XP is kinda easy since it's the most vulnerable OS.

Not many guys use it today.

Thank you for sharing.

**fr332play** - December 3, 2013, 10:30 pm

may i get this ebook ?

thanks in advance

**warlock994007** - December 4, 2013, 9:34 am

Woow !!! Good tutoial, Thanks for providing this, Gona try this soon.

Ple\z post for Linux.

**PTPT123** - December 5, 2013, 12:02 am

good.. one... can you send the link for ebook...

**XBatt** - December 5, 2013, 1:35 pm

I just installed a fresh install of XP and it doesn't seem to be vulnerable to the netapi exploit? What's the issue here, how does this exploit work and what does it exploit exactly?

**Aoss** - December 5, 2013, 5:33 pm

(Dec 5, 2013 02:35 PM)XBatt Wrote: [\[CITE\]](#) I just installed a fresh install of XP and it doesn't seem to be vulnerable to the netapi exploit? What's the issue here, how does this exploit work and what does it exploit exactly?

What service pack are you using? I dont see why it wouldn't work, are you sure you're putting the right IP in for the RHOST and LHOST, along with the correct port?

The exploit is a path stack corruption, basically any user can remotely bypass any security (being nX which stands for no execute, this security measure secludes memory so that it cannot be executed) via RCE using a special RPC request, which will allow you to shell the system, from then you can migrate to processes, escalate privs using UAC bypass if possible, cd into directories etc.

**DrDinosaur** - December 5, 2013, 5:58 pm

What service pack are you using? I dont see why it wouldn't work, are you sure you're putting the right IP in for the RHOST and LHOST, along with the correct port?

The exploit is a path stack corruption, basically any user can remotely bypass any security (being nX which stands for no execute, this security measure secludes memory so that it cannot be executed) via RCE using a special RPC request, which will allow you to shell the system, from then you can migrate to processes, escalate privs using UAC bypass if possible, cd into directories etc.

UAC bypass in Windows XP? Oh boy.

**XBatt** - December 5, 2013, 11:48 pm

I installed it with service pack 2, that might be the issue. If not I'm provable doing something wrong in metasploit and will show you the error later.

**DrDinosaur** - December 5, 2013, 11:56 pm

(Dec 6, 2013 12:48 AM)XBatt Wrote: [\[CITE\]](#) I installed it with service pack 2, that might be the issue. If not I'm provable doing something wrong in metasploit and will show you the error later.

Ok that would be helpful. I can get it working on XP SP2. Just to be sure, you turned on file and printer share right?

**XBatt** - December 6, 2013, 9:08 am

(Dec 6, 2013 12:56 AM)DrDinosaur Wrote: [\[CITE\]](#) Ok that would be helpful. I can get it working on XP SP2. Just to be sure, you turned on file and printer share right? Nope, how would you do that? Haven't used XP in years :/

**Aoss** - December 6, 2013, 12:12 pm

(Dec 5, 2013 06:58 PM)DrDinosaur Wrote: [\[CITE\]](#) What service pack are you using? I dont see why it wouldn't work, are you sure you're putting the right IP in for the RHOST and LHOST, along with the correct port?

The exploit is a path stack corruption, basically any user can remotely bypass any security (being nX which stands for no execute, this security measure secludes memory so that it cannot be executed) via RCE using a special RPC request, which will allow you to shell the system, from then you can migrate to processes, escalate privs using UAC bypass if possible, cd into directories etc.

UAC bypass in Windows XP? Oh boy.

I apologize, I shouldn't have said UAC Bypass on windows XP. Seeing as how there is no UAC.

**HarveySpecter** - December 8, 2013, 5:35 pm

thank you for this thread it was really helpful.

**ipdragon666** - December 8, 2013, 11:07 pm

this is a cool tut can you do 1 on windows vista its on my network connected wirelessly..

**Numinous** - December 9, 2013, 4:38 am

Yes, there are so many exploits are available for Windows VISTA too.

**kzx2050** - December 23, 2013, 1:14 am

Can I please have this ? Thanks in Advance.

**warlock994007** - December 24, 2013, 3:06 am

Windows XP is more vulnerable for this kind of attacks, can you please send a tutorial for linux and mac....please

**anonymousram** - January 12, 2014, 10:16 pm

please send me the full detailed ebook

**egyptghost** - January 13, 2014, 3:47 pm

Another great tutorial, good job keep it up pro

**super\_haker2002** - February 25, 2014, 5:36 pm

Need open Port in router and firewall or no ???

**Letoll** - February 25, 2014, 7:16 pm

So to mention something Ive only barely seen brought up here is the fact that XP is already super vulnerable. Even more so if you are user the metasploitable version of it which you clearly were given the fact the tutorial is an exact copy of the first little test run they have you do in Offensive Security's pentesters guide. Not only that, but the exploit you use is patched in SP3, which is also stated in that very same guide because it was the major hole found in the operating system that was exploited by the Conficker worm.

So really all you have successfully done here is copy the equivalent of a "Hello World" out of a book written about the basics of pentesting.

I just felt obligated to point this out since there is 8 pages of rands saying "hey great tutorial" when all they are doing is posting in here to up there count.

Should any of you actually want to learn something instead of using this very basic junk that will not get you anywhere in any real world scenario, you can start by reading the FREE ebook by Rapid7: Metasploit Unleashed. [http://www.offensive-security.com/metasploit-unleashed/Using\\_Exploits](http://www.offensive-security.com/metasploit-unleashed/Using_Exploits)

You're welcome.

>\_>

**TheUzuki.'** - February 26, 2014, 9:47 am

Quick notice to all beginners:

It is just working if you are on the same Network as the victim.  
However, when you can crack the WLAN it does not matter.

**Hassan Khan** - February 26, 2014, 10:38 am

Nice Tutorial sir, Thanks a lot for this :)

**Tajmonekus** - March 30, 2014, 11:44 am

Yeah, the old good ms08\_067\_netapi :)

**LAKHDAR** - April 2, 2014, 4:45 pm

Very nice tutorial men ! I love your job :). PLease, drop me the Ebook.

Have a good day, and sorry for my bad English !

@LAKHDAR

**himanshu raj** - January 17, 2015, 7:29 am

fulll of knowledge thanks for this]

**Blahh420** - January 19, 2015, 11:21 pm

Nice Tutorial , Thanks for this im gunna try this tonight

**Obelixus** - January 24, 2015, 2:20 am

Love this tut man very nice and detailed thanks :D

**JOhhhhhww** - January 25, 2015, 1:23 pm

I LOVE THIS TUT SO MUCH THANKS SO MUCHCCC

**Mathew425** - February 2, 2015, 3:27 pm

Ok, this is a noob question, but what exactly does this do? Will it grant you access to their files or what?