# Infectious Media Attack

pentestlab.blog/category/social-engineering/page/6

April 8, 2012

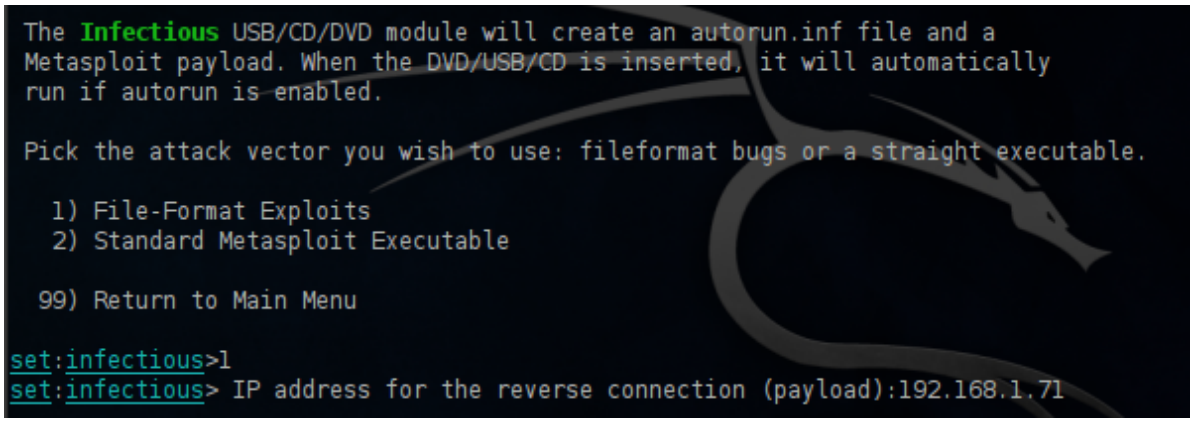

The majority of people have at least one USB stick in order to transfer files from work to their homes.Also a common characteristic of all humans is curiosity.These two things combined together can create a huge threat which can affect any organization.This article is an another example of why people are the weakest link in the security chain.

This type of attack allows the penetration tester to create a USB,DVD or a CD with malicious content.When the unsuspicious user will open the file the payload will executed and it will return a shell.In this article we will explore this type of attack.

We are opening the Social Engineering Toolkit and we are selecting the Infectious Media Generator option.

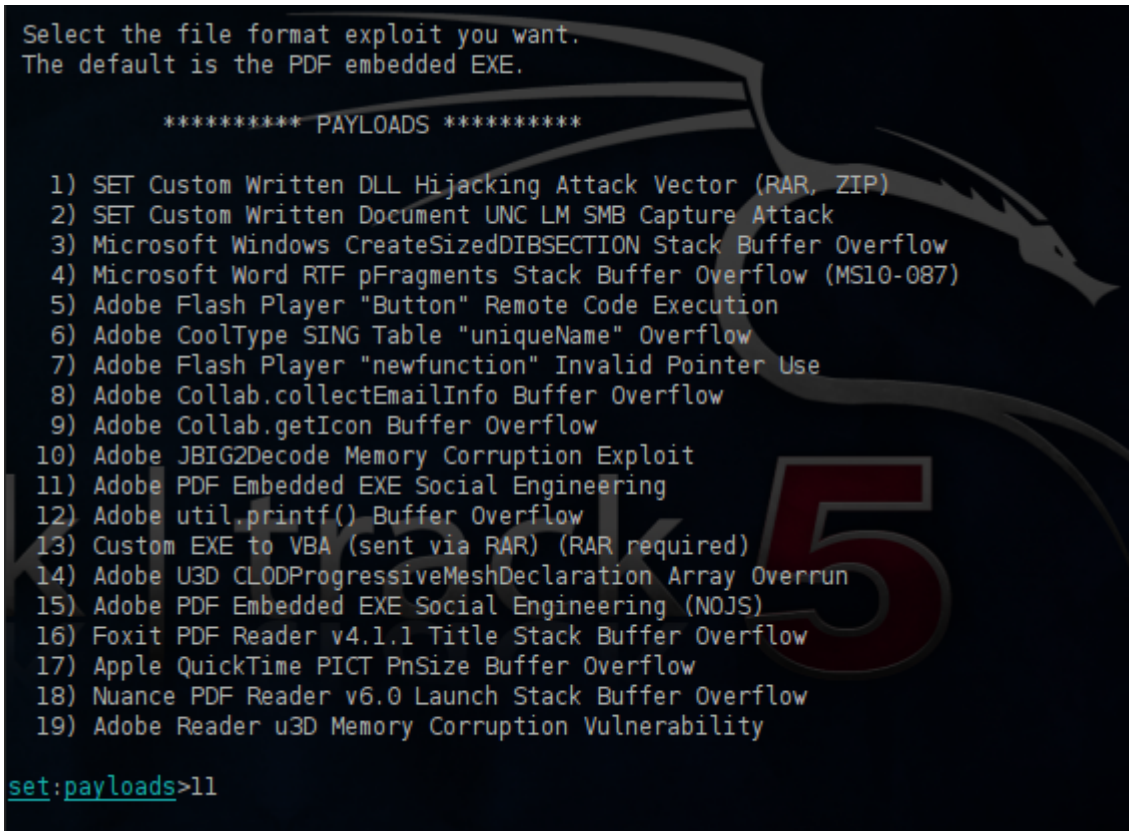

Infectious Media Generator

The implementation of this attack is very simple.SET will create automatically an **autorun.inf** file and a payload.For this scenario we will choose to use **File-Format Exploits** as an attack vector.



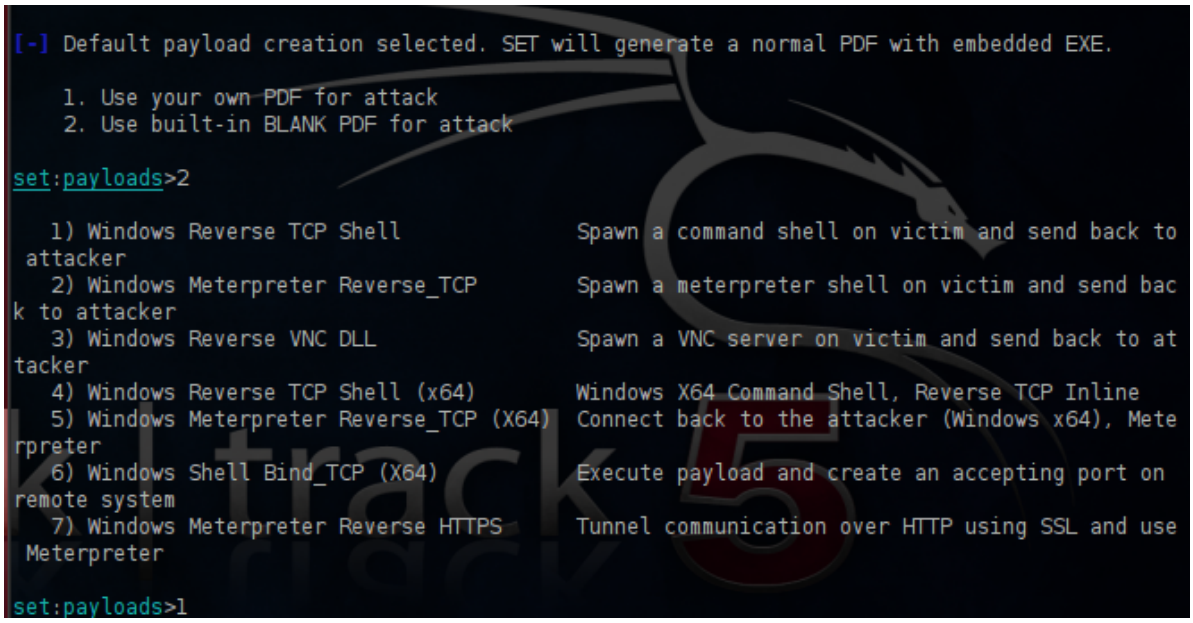

Selecting the Attack Vector

In the next image you can see the available payloads for this attack.We will use the default option which will embed an executable inside the PDF file.



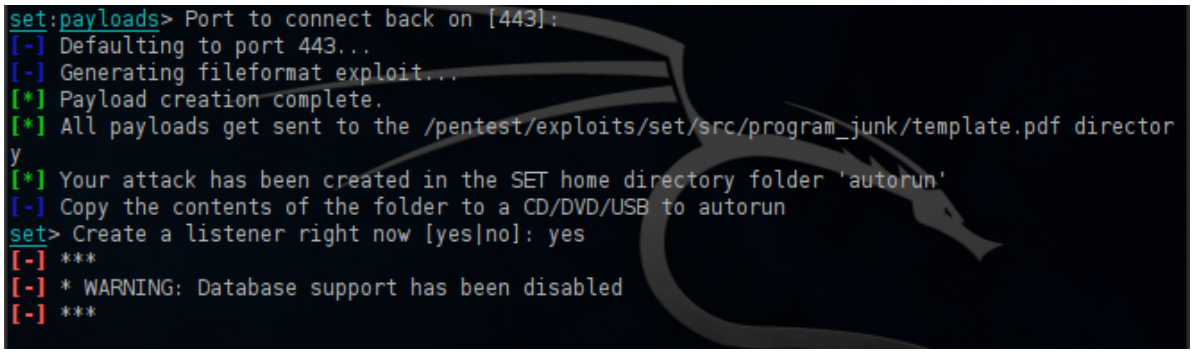

Available Payloads

Now it is time to choose the payload that the malicious pdf will carry.Our option will be to return to us a simple Windows Shell.



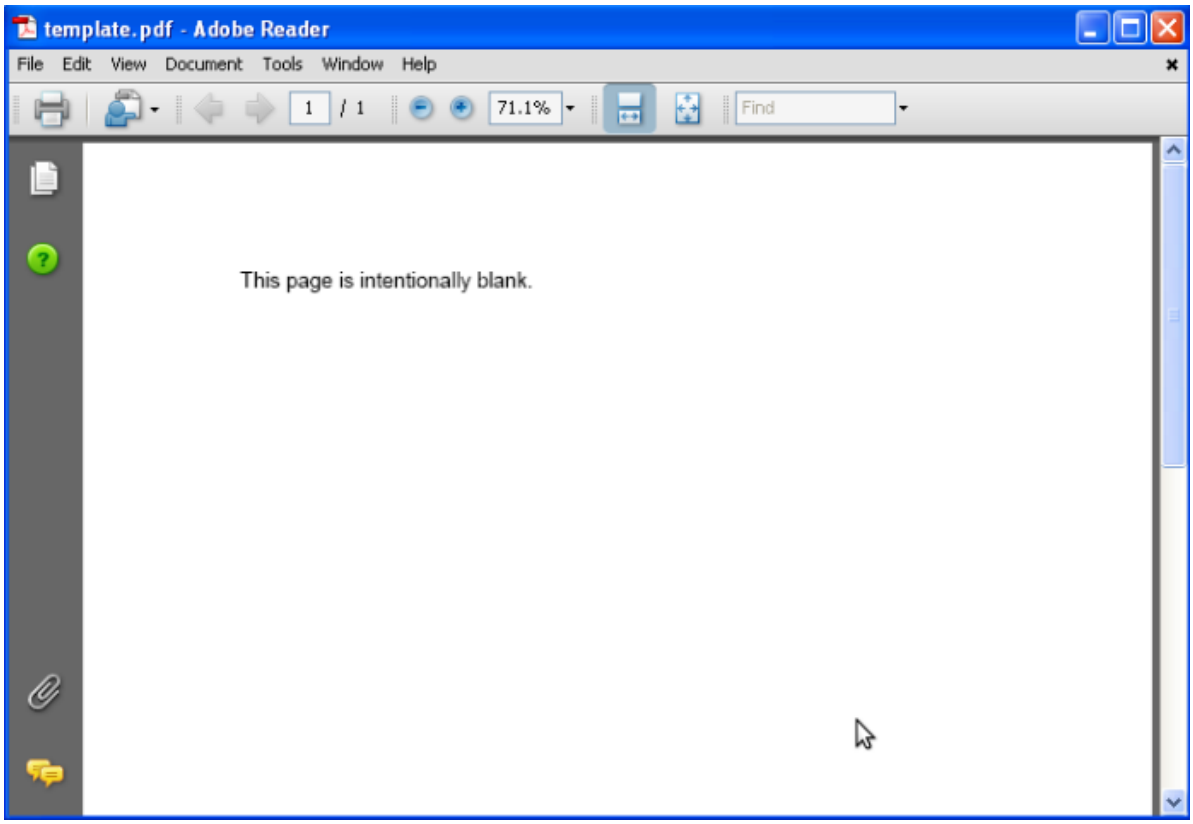

Choose the payload

We will set the port at 443 which is the default option and then the Social Engineering Toolkit will create the autorun file and the malicious PDF automatically.



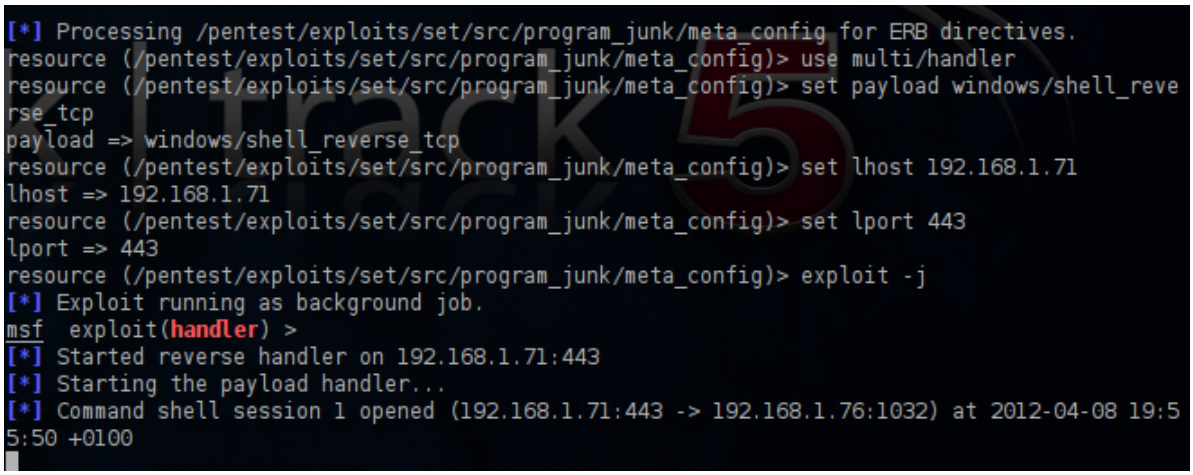

Generating the Exploit

Now lets say that during a penetration test we have plant the USB stick in a place that it will be too obvious for the employees to discover it.If someone takes that USB and connect this to his work computer then he will see a PDF file which is blank.




Malicious PDF

At that time the payload will executed to his machine and it will return to us a remote shell.




Obtain a Remote Shell

### Conclusion

This attack doesn't require any knowledge and it is very fast and easy to implemented by anyone.This means that anyone that can plant a malicious USB stick inside a company can be a potential threat.It also points out how a simple USB or DVD can bypass the network perimeter and can become a threat for any company if the employees are not following the security policies.For example companies should have a policy that would protect them against any mobile threats and the employees should follow that policy.

Companies must educate their users about the risks of such threats.Additionally this attack proves that it doesn’t matter how much money an organization will spend for securing their network perimeter with Firewalls,IDS and IPS when the biggest threat may come from inside and with no bad intention.