Capture NTLM Hashes using PDF (Bad-Pdf)

posted in[**Hacking Tools**](https://www.hackingarticles.in/category/collection-of-hacking-tools/), [**Penetration Testing**](https://www.hackingarticles.in/category/penetration-testing/) on [**May 12, 2018**](https://www.hackingarticles.in/capture-ntlm-hashes-using-pdf-bad-pdf/) by [**Raj Chandel**](https://www.hackingarticles.in/author/raaz/)

SHARE

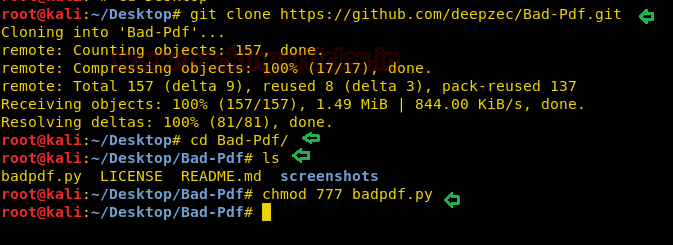
Today we are demonstrating stealing NTLM hashes through a pdf file. We have already discussed the various methods to Capture NTLM Hashes in a Network in our [previous](https://www.hackingarticles.in/4-ways-capture-ntlm-hashes-network/) article. Recently a new tool has launched “Bad-PDF” and in this article, we are sharing our experience.

Bad-PDF creates malicious PDF to steal NTLM(NTLMv1/NTLMv2) Hashes from windows machines, it utilizes vulnerability disclosed by checkpoint team to create the malicious PDF file. Bad-Pdf reads the NTLM hashes using Responder listener.

This method works for all PDF readers(Any version) and java scripts are not required for this attack, most of the EDR/Endpoint solution fail to detect this attack.



|  |  |
| --- | --- |
| 1  2  3  4 | git clone https://github.com/deepzec/Bad-Pdf.git  cd Bad.Pdf  ls  chmod 777 badpadf.py |

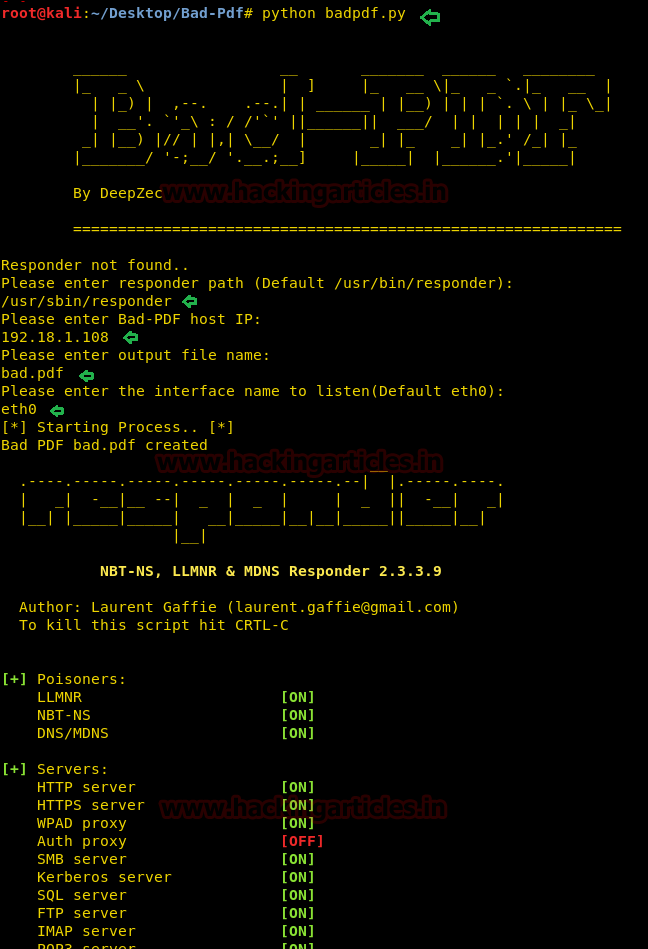


Now run the python file with the help of following command given below:

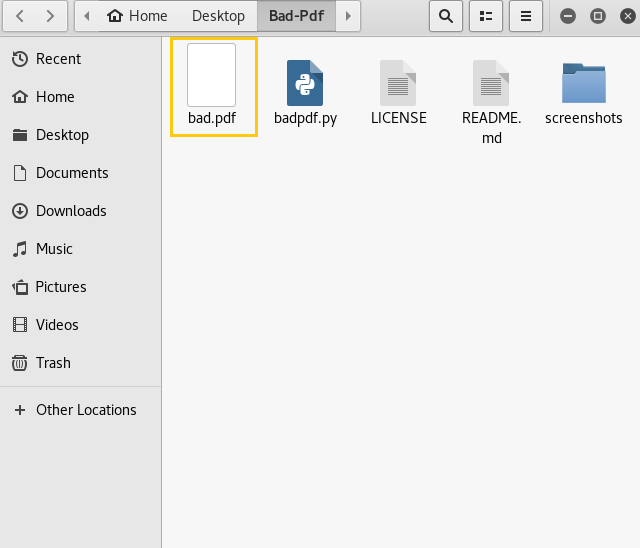


|  |  |
| --- | --- |
| 1 | python badpdf.py |

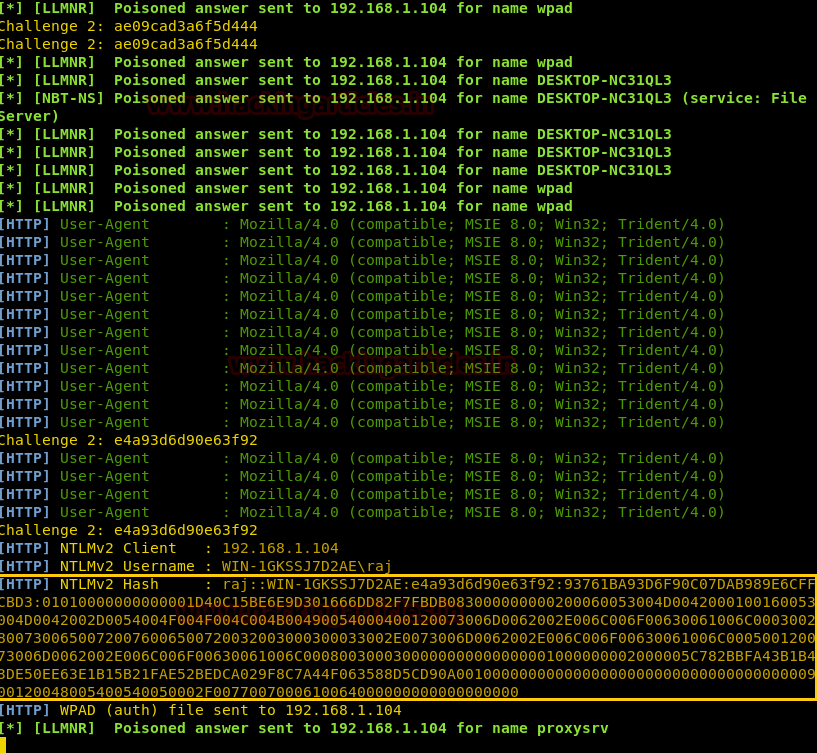
Then it will try to connect with Responder through its default path i.e. /user/bin /responder but in our case, the location of the responder is user/sbin/responder. After then it will ask your network IP, the name of the output file and interface name, submit this information as per your network.



Then it will create a malicious pdf file with name bad.pdf, now transfer this pdf file to your target.



So, when the victim will click our malicious file, his NTLM hash will be captured as shown in below image. Here you can observe username ‘raj’ along with its hash password. Now copy the hash value in a text document so that you can crack this hash value for retrieving the password.



We have pasted the hash value in a text file and save it as “hash” on the desktop. Later we had used John the ripper for cracking the hash.



|  |  |
| --- | --- |
| 1 | john hash |

Awesome!!! We have retrieved **password: 133** for user: raj.

