Starting of with a nmap scan to determine open ports, thus attack vector !

It seems that I have port 21 & 80 open and FTP allows anonymous access. From the output of nmap I am pretty sure that the files which I can see in the FTP server are the default files for the Microsoft IIS Server ! By going to the web page and checking the source of the page I was able to determine that the files for the webserver are accessible from the ftp folder. That gives me an idea of uploading a webshell and from there to get a reverse shell on the system and enumerate to escalate to NT\_Authority.

I now have the webshell uploaded and I can access it from the browser. It turned out that I with numerous tries to get a reverse shell through the asp webshell, so I searched in google and found that Windows server IIS 7.5 - present is able to execute aspx files. That means I can generate a .aspx reverse shell with msfvenom and this will give me a reverse shell.

Alright, now I only need to upload it and execute it !

Now I have reverse shell and I can start enumerating the system to get System/NT\_AUTHORITY. I can now use the post exploit from metasploit to show me what exploits I can possibly use to get system !

Alright, the ms10\_015\_kitrap0d seems more interesting than the bypassuac\_eventvwr so I will try it.

Here I have forgot to change the session number and I got an error so I quickly changed it and the exploit worked !

I am now NT\_AUTHORITY\SYSTEM ! That is how you do Devel from HackTheBox !