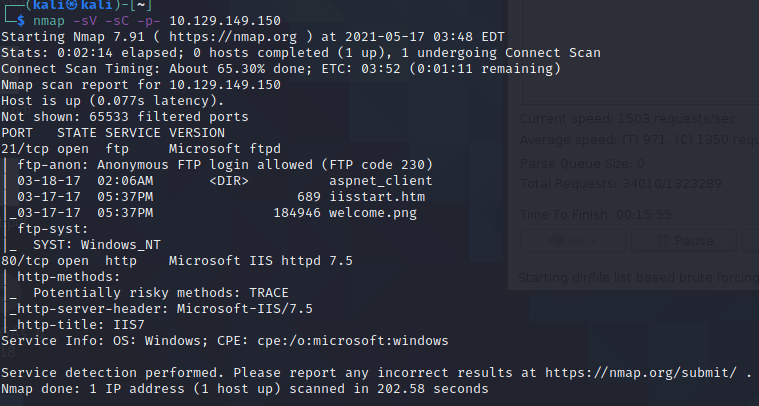
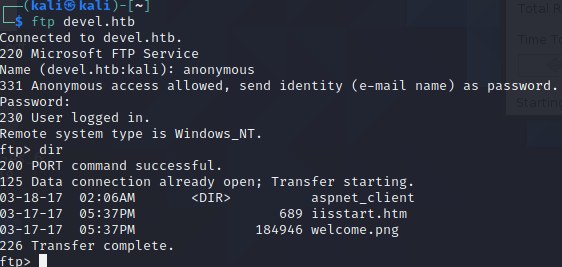
HTB Devel - Windows Machine

10.129.149.150

Nmap



First observation that FTP anon login is allowed.

FTP:  


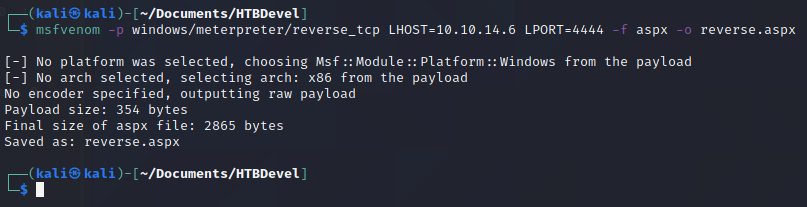
With FTP anonymous user I am able to manipulate the home directory. I can rewrite the iisstart.htm file to be anything I want. I should be able to upload a script to get a shell.

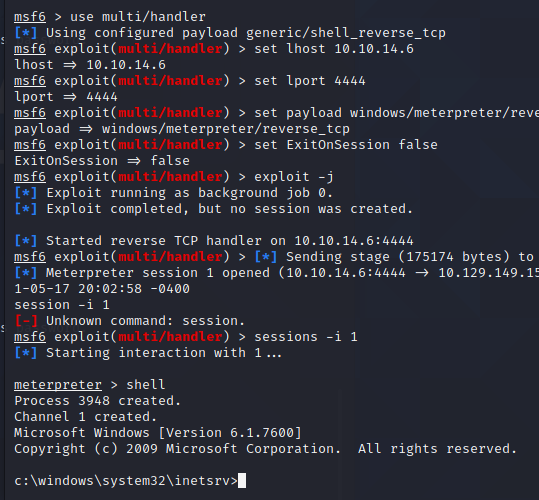
Microsoft IIS HTTPD7.5

Since there is an aspnet client directory this leads me to think there is an asp authentication bypass vulnerability

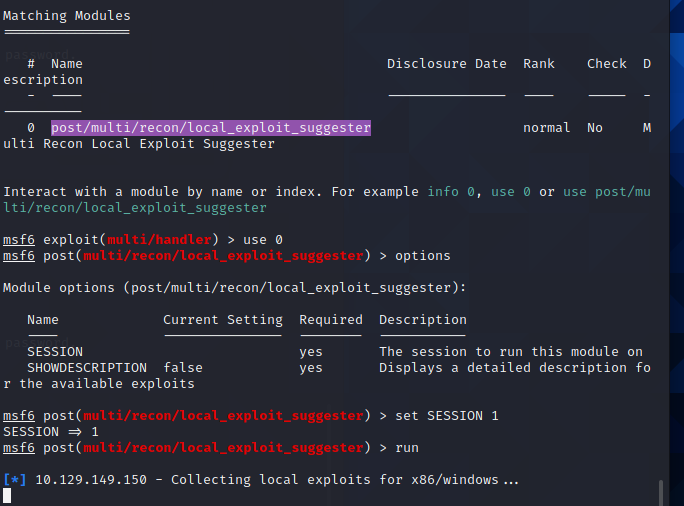
<https://www.exploit-db.com/exploits/19033>

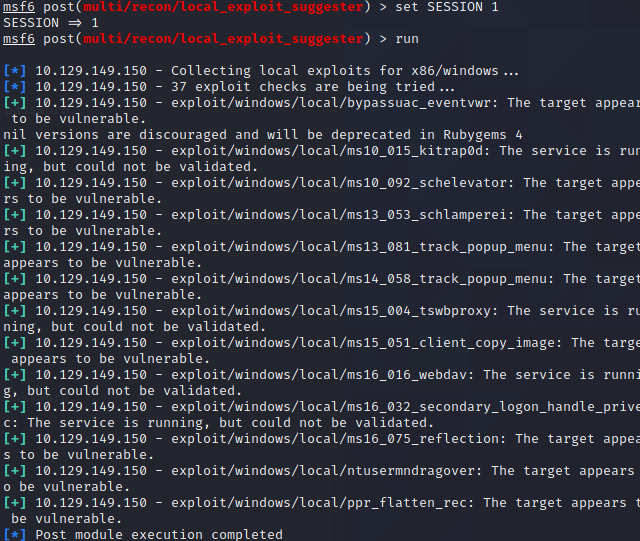
I was able to use FTP to upload a msfvenom aspx payload to get a reverse session.





Something new I learned about msfconsole is a an exploit suggester





Using “kitrap0d” gave a new meterpreter session “2” with elevated privileges. NT Authority gave us access to admin and user flags.