Granny+Grandpa

Granny

port 80 shows an IIS 6.0 website under construction

IIS 6.0 is vulnerable to CVE-2017-7269
-> metasploit's windows/iis/iis_webdav_upload_asp get's us a shell as "NT Authority\Network Service"

We can migrate to a process owned by us for more stability
-> ps to show processes then migrate <PID>

Using metasploit's local exploit suggestor, we can script kiddie our way to root :D

Grandpa

port 80 shows an IIS 6.0 website under construction

IIS 6.0 is vulnerable to CVE-2017-7269
-> metasploit's windows/iis/iis_webdav_scstoragepathfromurl get's us a shell as "NT Authority\Network Service"

We can migrate to a process owned by us for more stability
-> ps to show processes then migrate <PID>

Using metasploit's local exploit suggestor, we can script kiddie our way to root :D