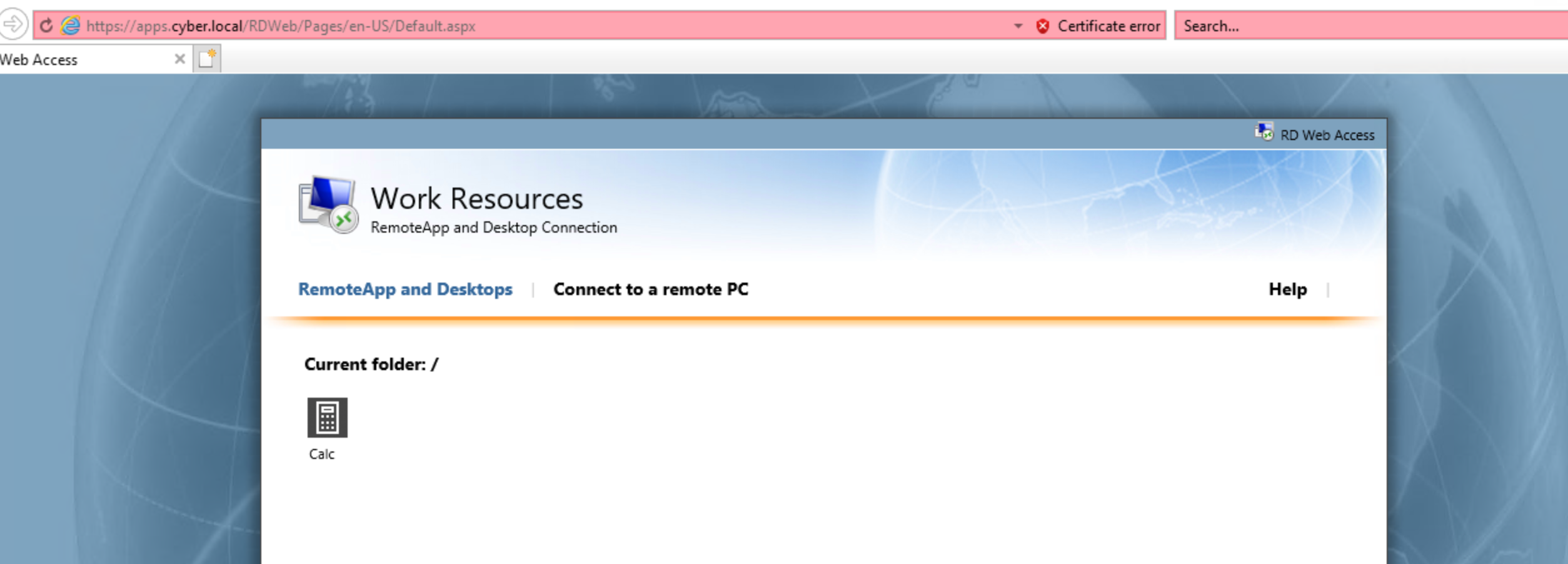
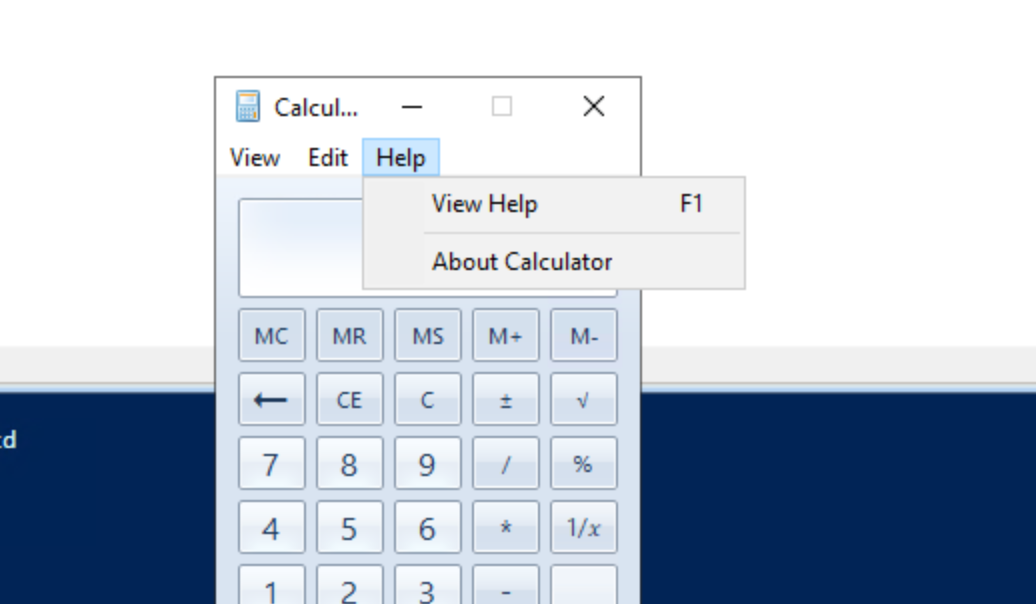
RDS Escape

In one CTF I was in front of a dockerrized RDP contained escape via via a published application(calc.exe) in a RDS had to be escaped.

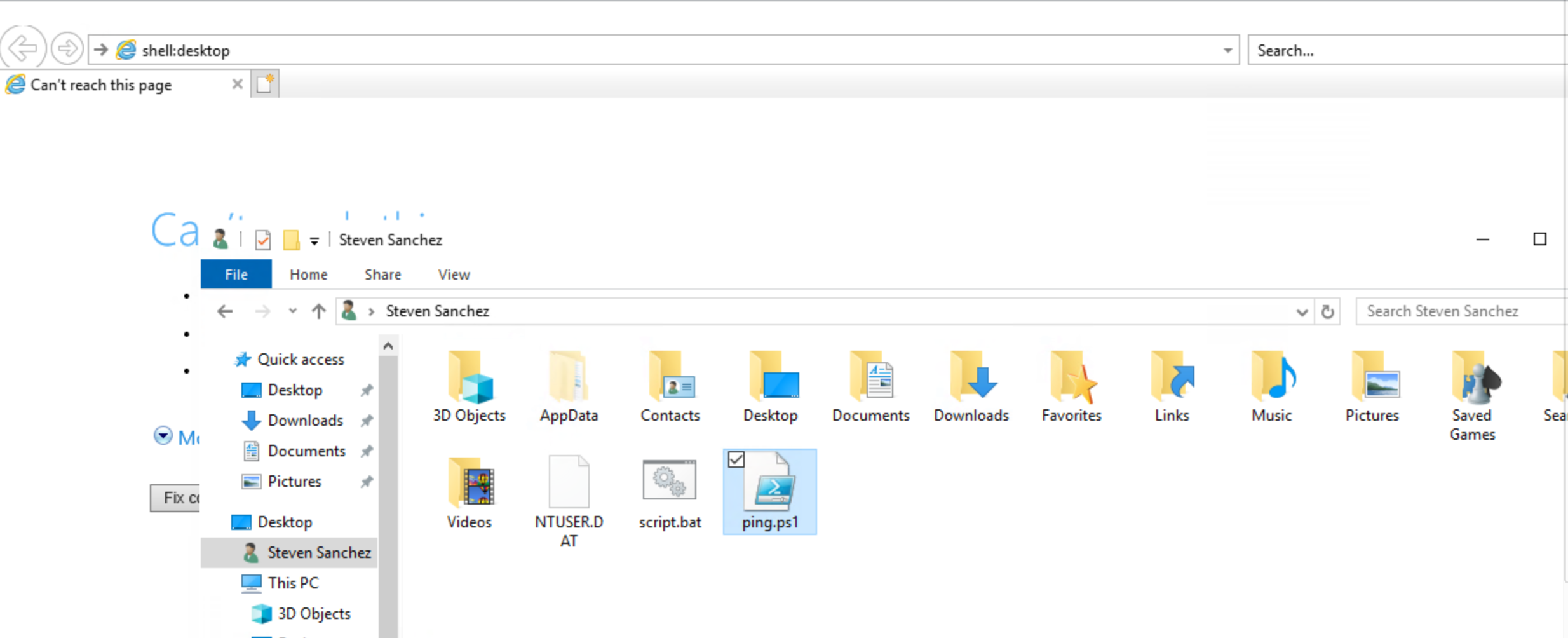


To escape I did:

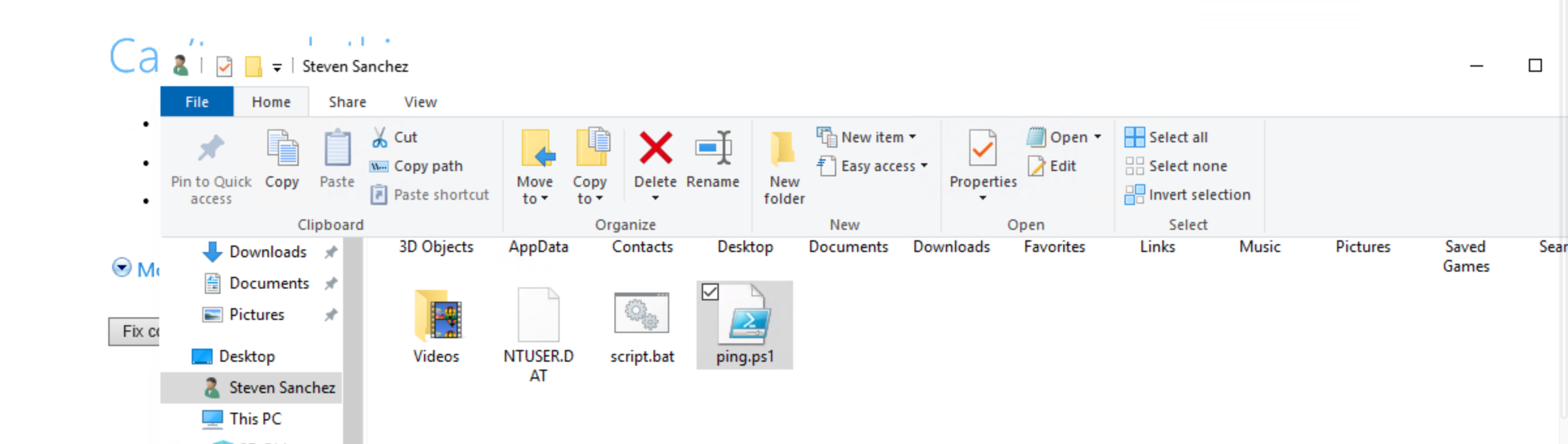
1. Spinned the application and clicked Help -> View Help



2. This opened IE.exe, where I could spawn the explorer.exe via the URL **shell:desktop**



3. From here I saved a dummy powershell script on the home folder(this was freely writable at the time). And upon clickin **Home -> Edit**



This opens the “Powershell ISE” which wasn’t blocked att all!

