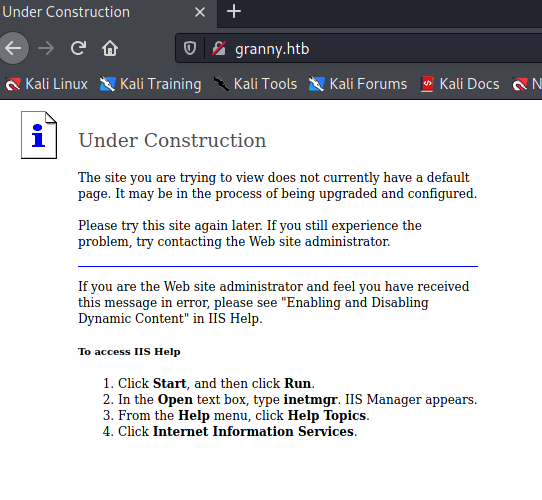
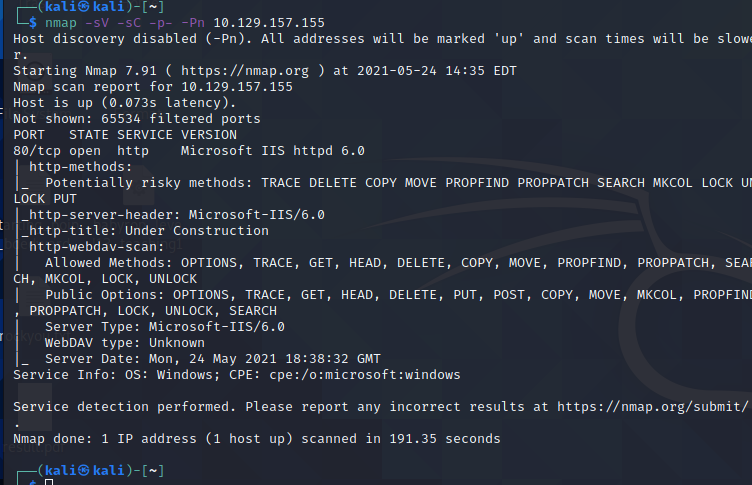
HTBGranny Windows Machine

Web:



Same webpage as “grandpa” htb machine

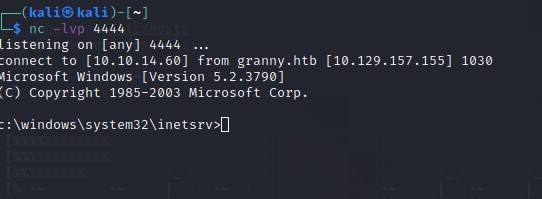
Nmap



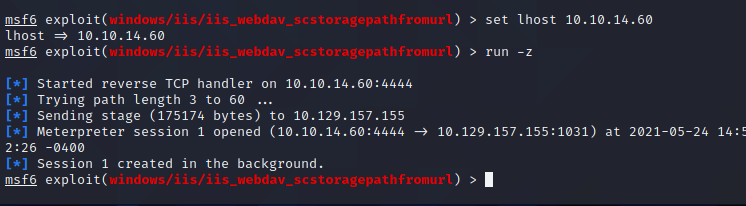
<https://github.com/g0rx/iis6-exploit-2017-CVE-2017-7269>

Same exploit as in grandpa gives us a shell:

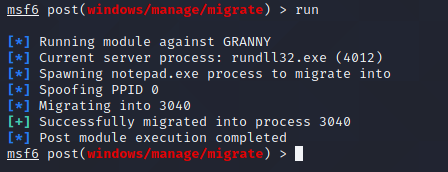




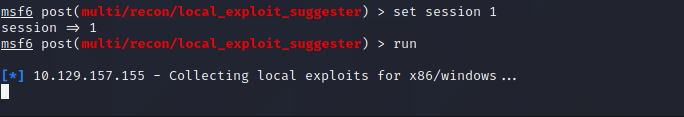
Using metasploit exploit “windows/iis/iis\_webdav\_scstoragepathfromurl

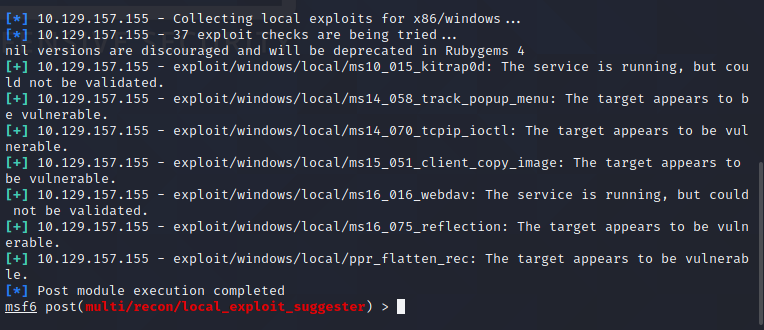


Migration:

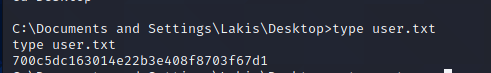


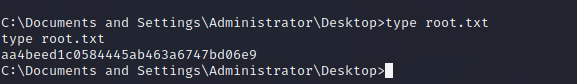
Local exploitation Suggester:





However, using ms14\_058\_track\_popup\_menu gave us a privileged shell:





Using ms16\_075\_reflection gives us a shell, but it is not a privileged shell

