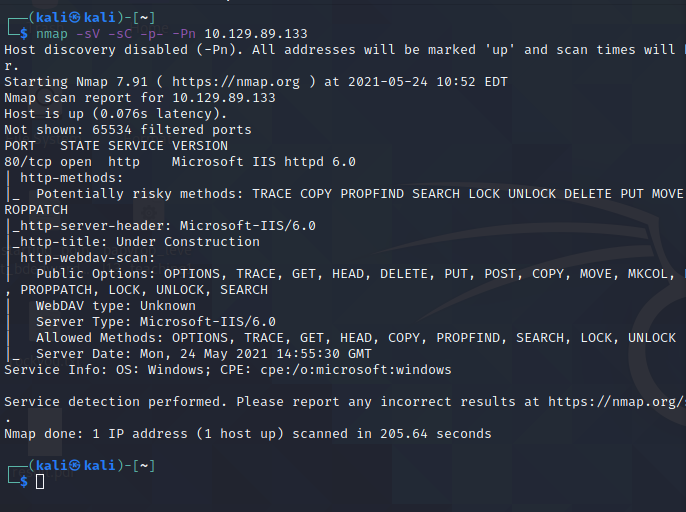
HTB - Grandpa Windows Machine

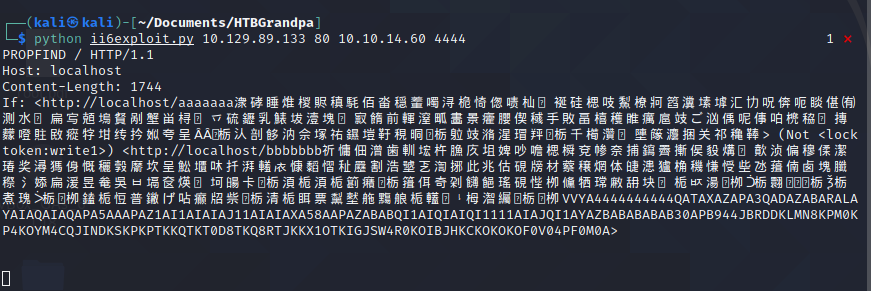
Nmap

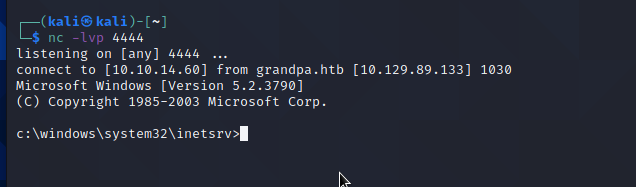


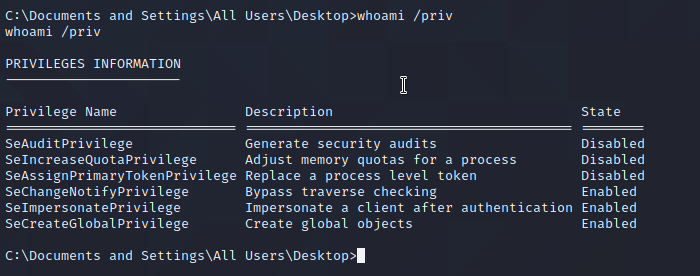
IIS 6.0 exploit:

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

This payload got us a shell:







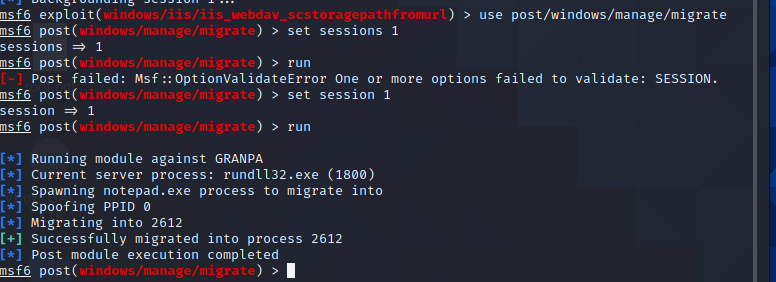
[ohpe/juicy-potato: A sugared version of RottenPotatoNG, with a bit of juice, i.e. another Local Privilege Escalation tool, from a Windows Service Accounts to NT AUTHORITY\SYSTEM. (github.com)](https://github.com/ohpe/juicy-potato)

[Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow - Windows remote Exploit (exploit-db.com)](https://www.exploit-db.com/exploits/41738)

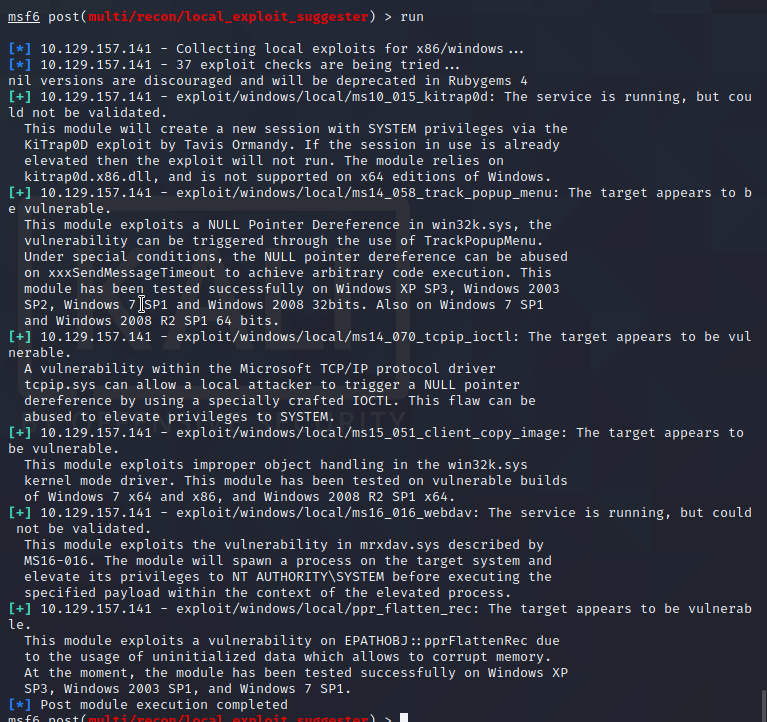


Using msfconsole to run this exploit and then running a local escalation gave:

Then post exploitation migration:



Then



Trying these different exploits, ms14\_070\_tcpip\_ioctl worked to get root shell:

