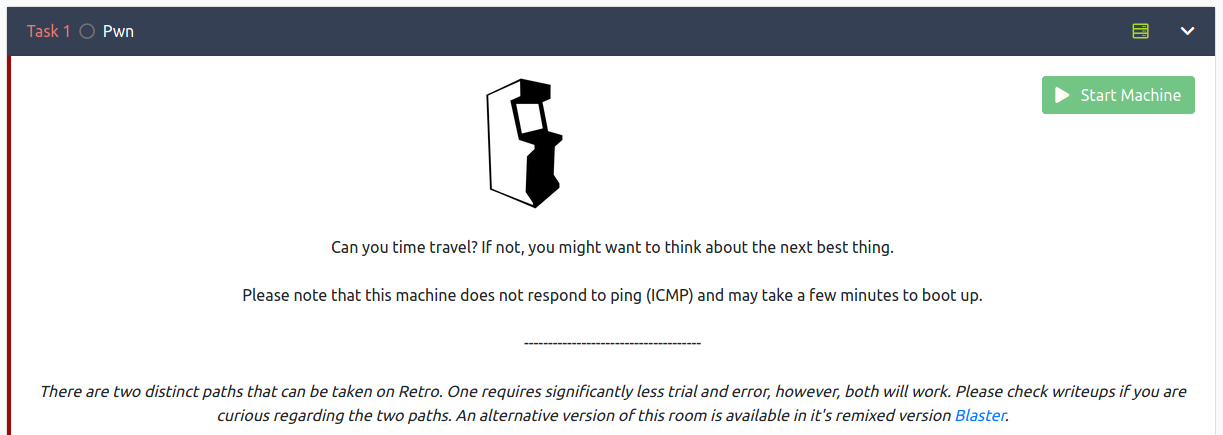
**Retro write-up**

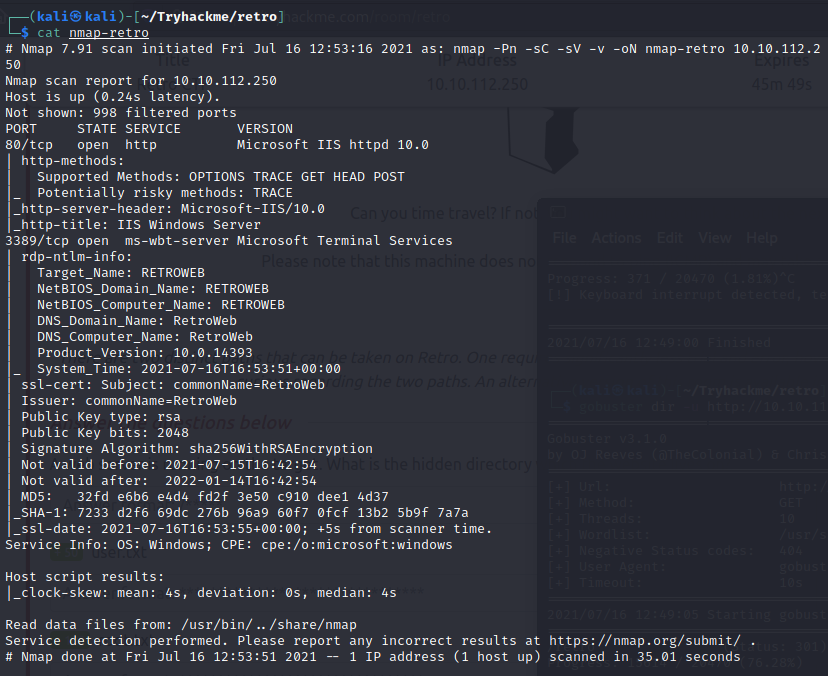
This is write-up for Retro which is Windows base CTF which have an alternative room Blaster that we have to search though website, find credential, connect to target machine via RDP and elevate our privilege to root this box

Site: <https://tryhackme.com/room/retro>

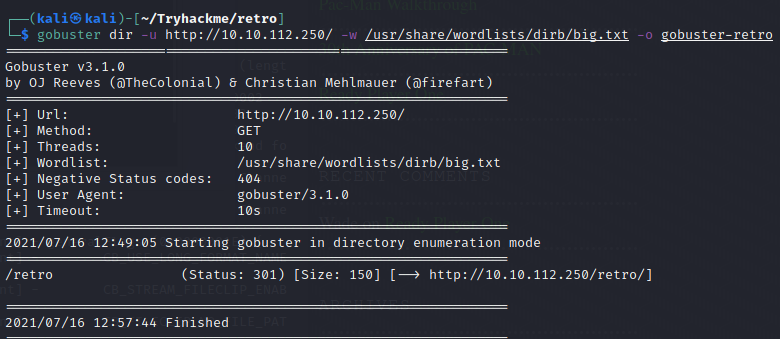


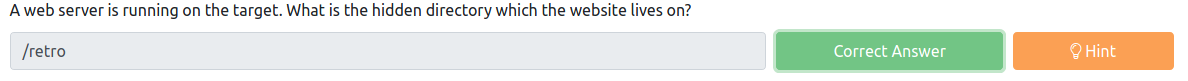


Always start with nmap port scanning and service enumerating, after finished we see that 2 ports are opened



Nothing much in website go it’s gobuster time and after let it run for a while /retro could be the one

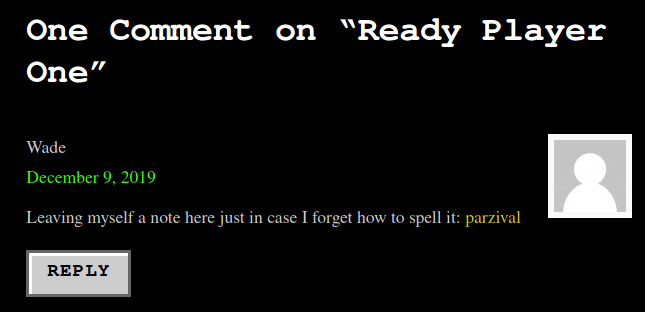




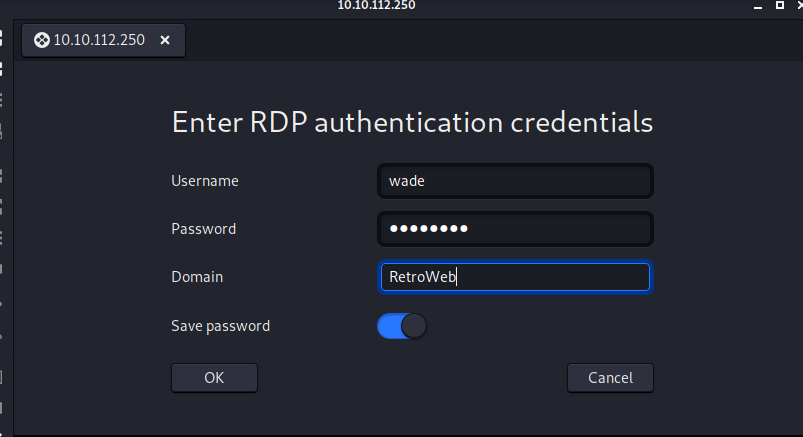
Visit and explore that hidden directory we can see that it’s a blog post and we got potential username there



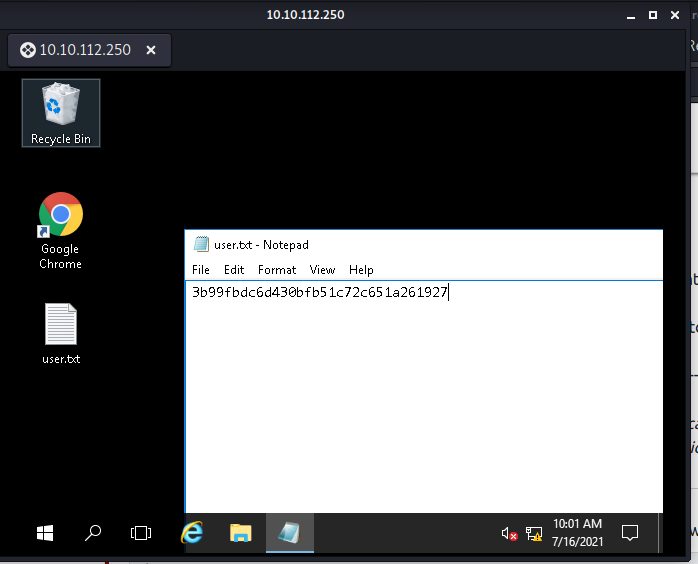
Also with potential password in comment



Now connect to target machine using RDP

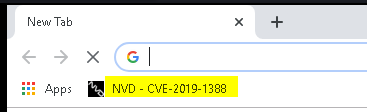


After connected we will see user flag in desktop



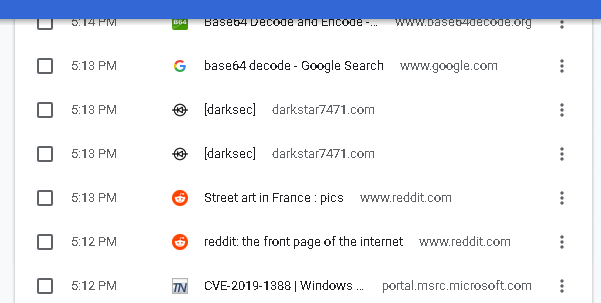


I guessed this user uses chrome regularly judging from a shortcut in desktop, after opened it we can see his bookmark



See more in History, this user visited CVE-2019-1338, Reddit, Darksec, base64decode

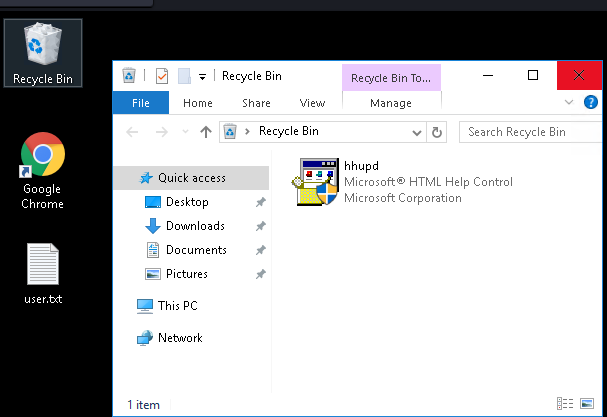
TryHackMe, Nintendo and update blog on WordPress localhost



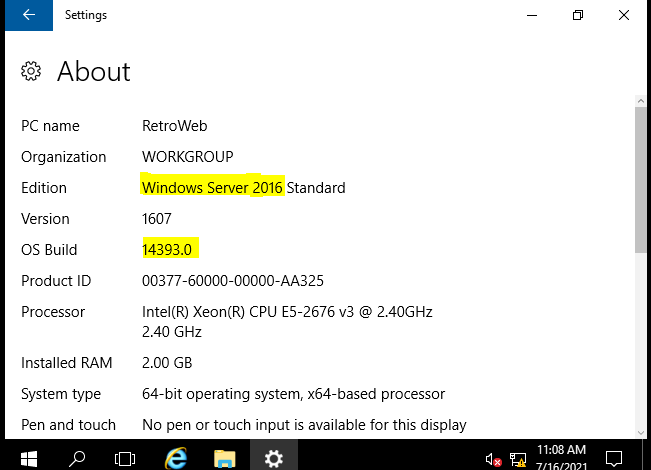
We can use this CVE to get SYSTEM shell in Blaster room but we can’t do that again in this room

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-1388>

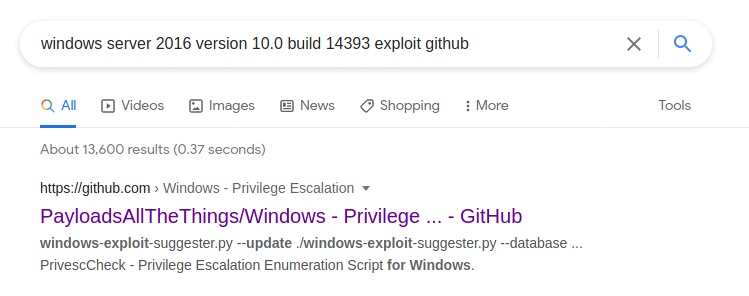
and in this Recycle Bin has a file that used to exploit



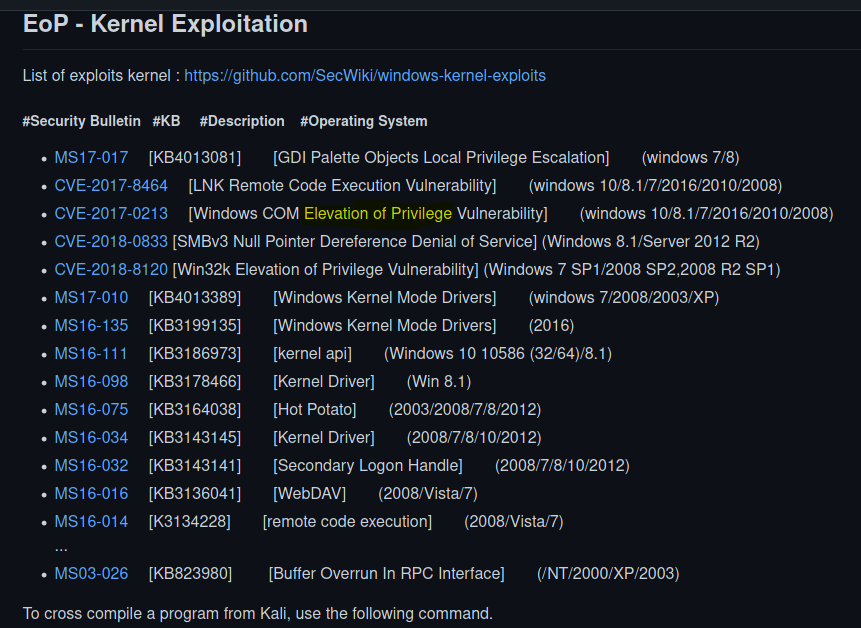
Now let’s find how to exploit this box, first let’s see system information first and we got that this is Windows Server 2016 build 14393.0 , architecture x64



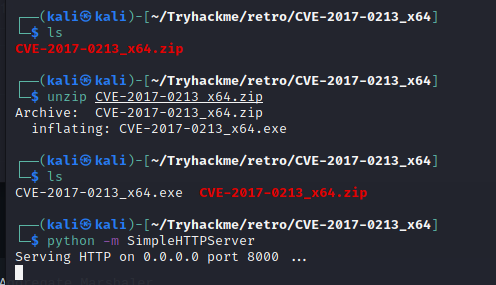
Search google and PayloadsAllTheThings could be really helpful for this

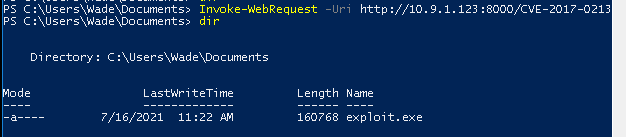


At kernel exploitation we will use this CVE to exploit this box

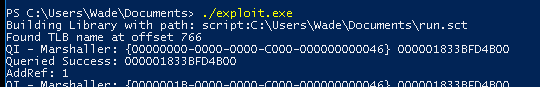


Git clone x64 zip (<https://github.com/SecWiki/windows-kernel-exploits/tree/master/CVE-2017-0213>) to our attacker box, unzip it and send it to target box

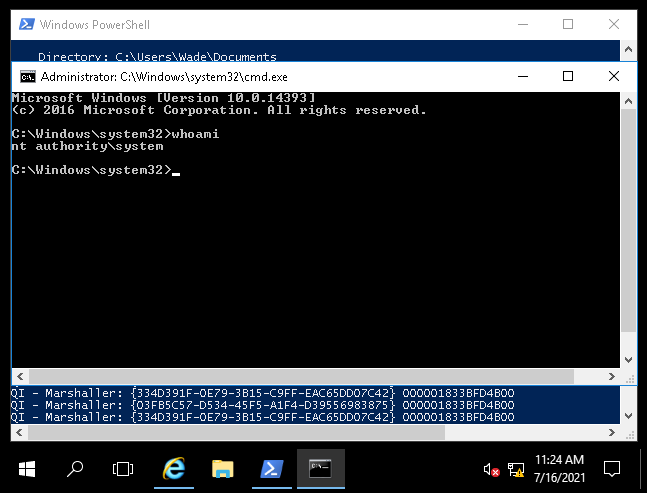




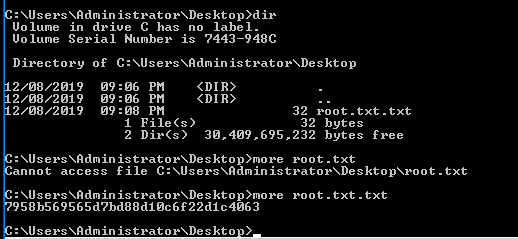
It’s time to exploit, run this executable file via powershell



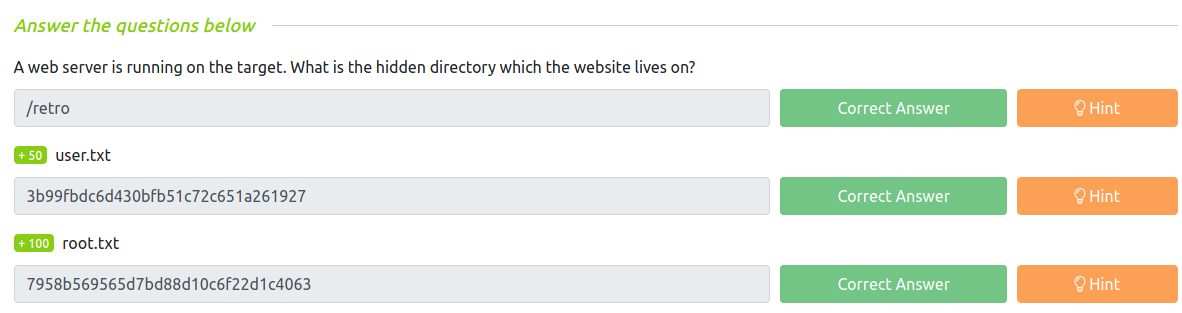
After executed we will get a SYSTEM shell now we can capture root flag in Administrator directory now



Root flag hide in Admin’s desktop, capture it we rocked this box!







We also can exploit with juicy potato in this GitHub: <https://github.com/ohpe/juicy-potato/releases>

And here 2 relevant write-ups using juicy potato to rock this box: <https://medium.com/azkrath/tryhackme-walkthrough-retro-273f8b35a20d>

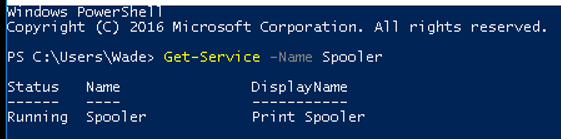
<https://infinitelogins.com/2020/12/09/windows-privilege-escalation-abusing-seimpersonateprivilege-juicy-potato/>

**Rock with PrintNightmare CVE-2021-1675**

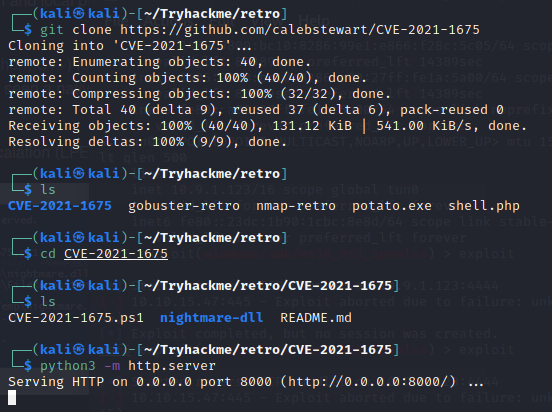
GitHub: <https://github.com/calebstewart/CVE-2021-1675>

More detail: <https://www.blumira.com/cve-2021-1675/>

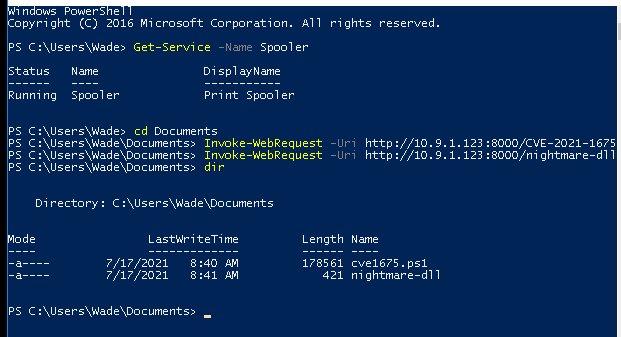
Windows already have Print Spooler service as default but we can make sure of it via PowerShell Get-Service



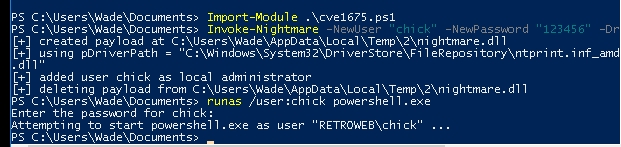
Clone that repository and send it to target box



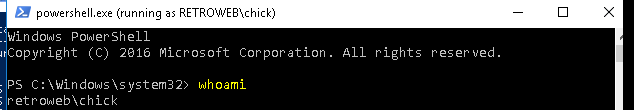
Get all we need here

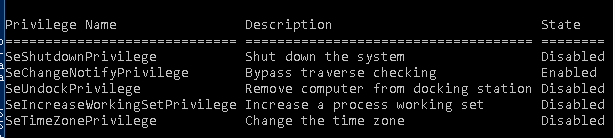


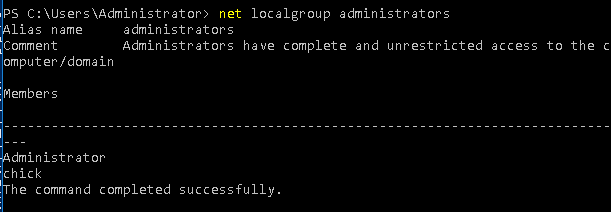
Import module and Add new user to local administrator privilege, once it successfully executed we can login as that user from here



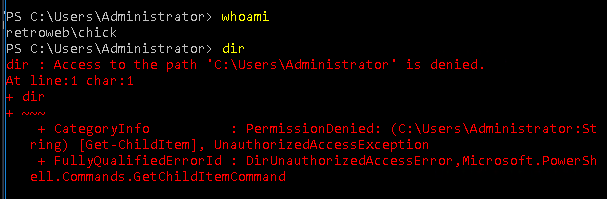
And this is how PrintNightmare on this repository works



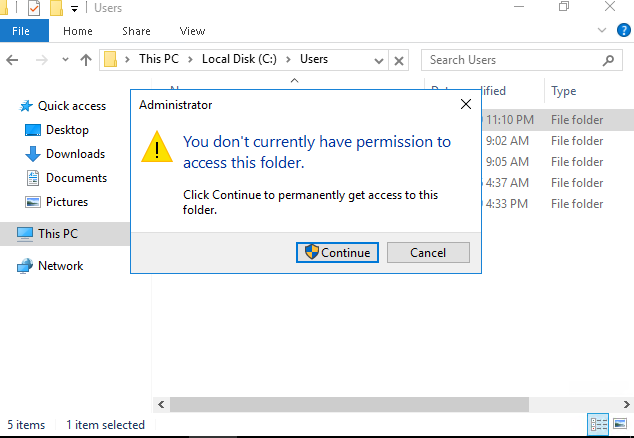


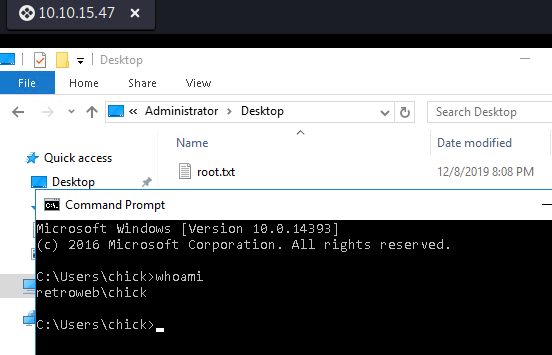


But there is a cut down of this way cause we need to use file explorer to catch our flag, not via cmd



Reconnect with new user and then go to administrator directory and force to continue and capture it





**PrintNightmare CVE-2021-34527**

GitHub: <https://github.com/JohnHammond/CVE-2021-34527>

