Bastion

```
└─$ nmap -sC -sV -oN nmap/init.nmap 10.10.10.134
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 00:56 EDT
Nmap scan report for 10.10.10.134
Host is up (0.084s latency).
Not shown: 997 closed tcp ports (conn-refused)
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
445/tcp open          Windows Server 2016 Standard 14393 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| 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: 2023-09-22T06:56:32+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: -39m57s, deviation: 1h09m15s, median: 0s
| smb2-time:
|   date: 2023-09-22T04:56:34
|_  start_date: 2023-09-22T04:55:41

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.16 seconds
```

Foothold

There is an smb share called “Backups" with some interesting files.

We find 2 vhd files which are virtual hard disk backups which might have something interesting

These files were found in L4mpje-PC/
so we know a username of interest is L4mpje

We can mount one of the vhd files to view all files of the backup's file system

We can view some system hashes by doing the following:

- From Windows\System32\config, grab SAM and SYSTEM
- Use `impacket-secretsdump -sam SAM -system SYSTEM local` to get hashes

We see that the Administrator's hash starts with 31d6, which is a blank password. This probably means that the account is disabled

There is a hash, however, for the user of interest. We can easily crack this password using crackstation

L4mpje:bureaulampje

This password allows us to ssh into the box

Priv Esc

Turns out Administrator account is now enabled (it wasn't in the backup file we examined) so our goal is to escalate to it

In Program Files (x86), we see a program called mRemoteNG.

Doing some research, we find out that we can find password hashes in:
C:\User\L4mpje\AppData\Roaming\mRemoteNG

Using a python script from github, we can decrypt this hash
https://github.com/haseebT/mRemoteNG-Decrypt

Administrator:thXLHM96BeKL0ER2