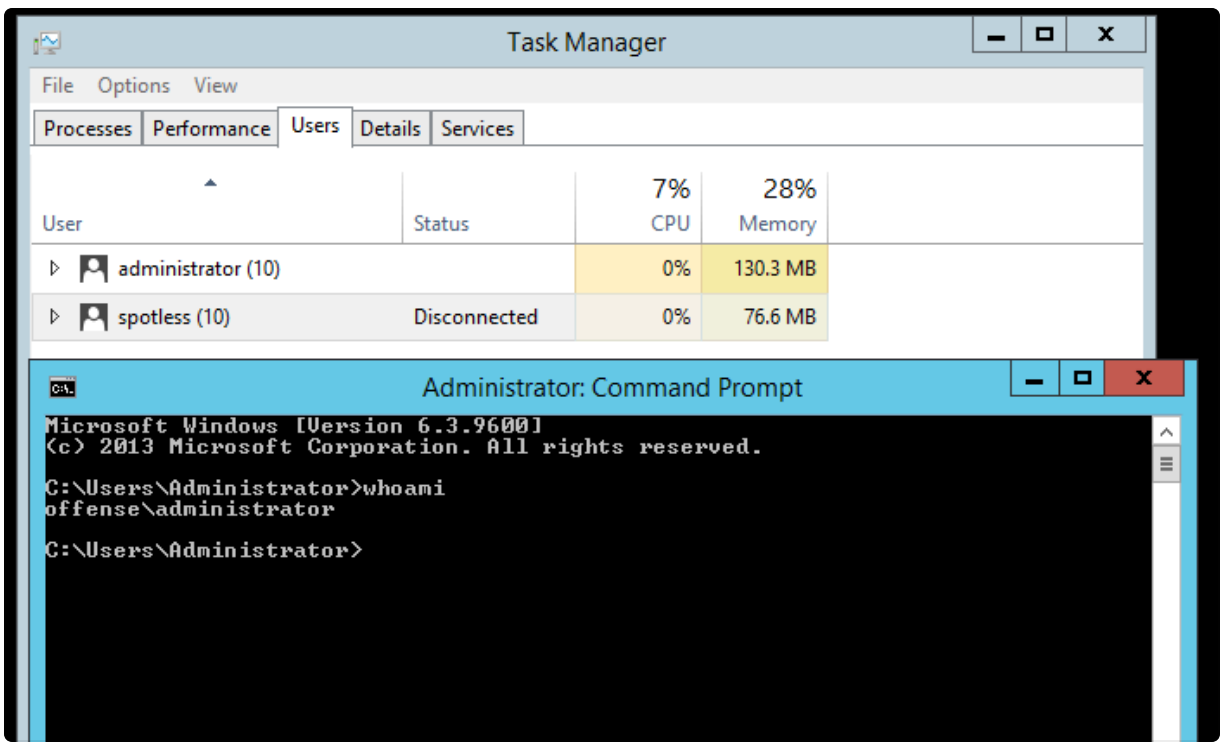
RDP Hijacking for Lateral Movement with tscon

This lab explores a technique that allows a SYSTEM account to move laterally through the network using RDP without the need for credentials.

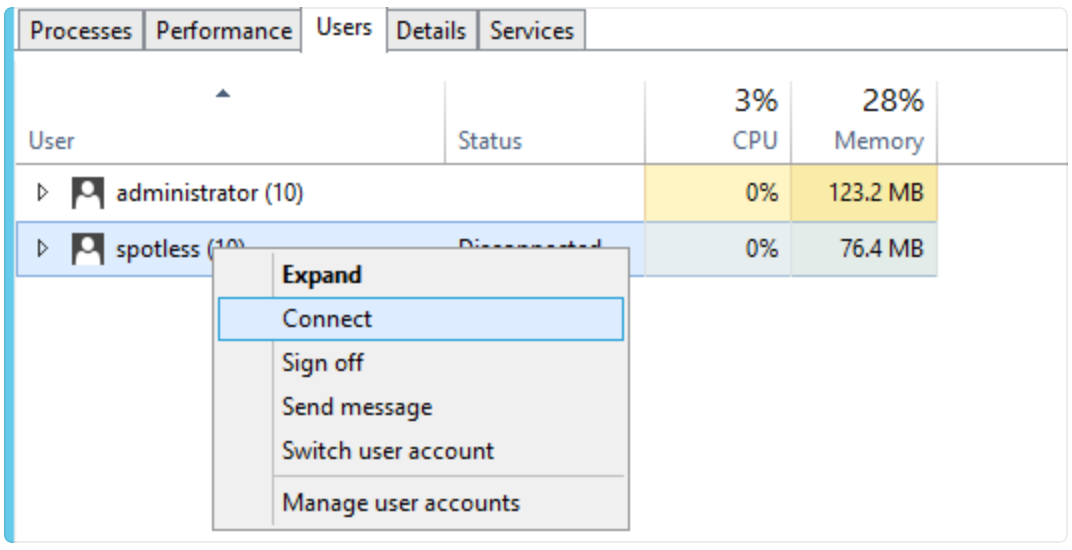
Execution

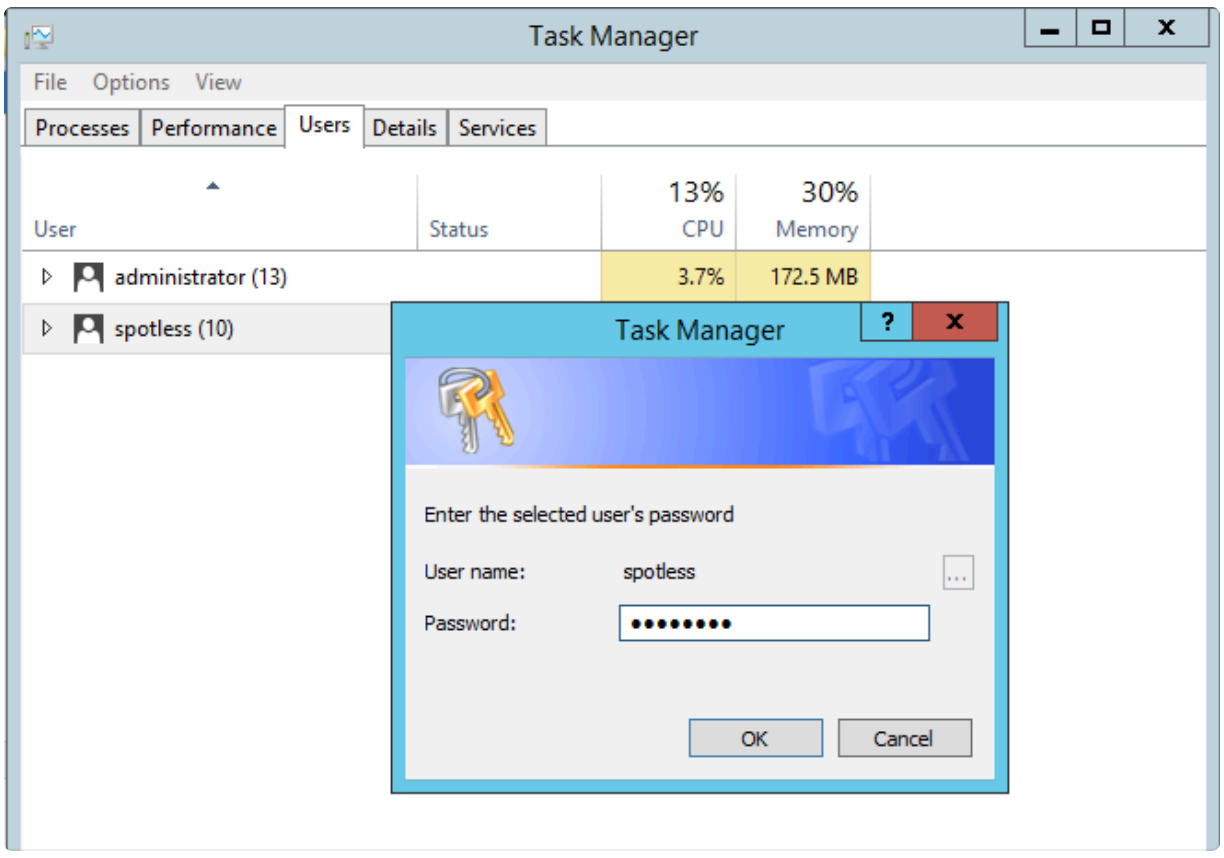
It is possible by design to switch from one user's desktop session to another through the Task Manager (one of the ways).

Below shows that there are two users on the system and currently the administrator session is in active:

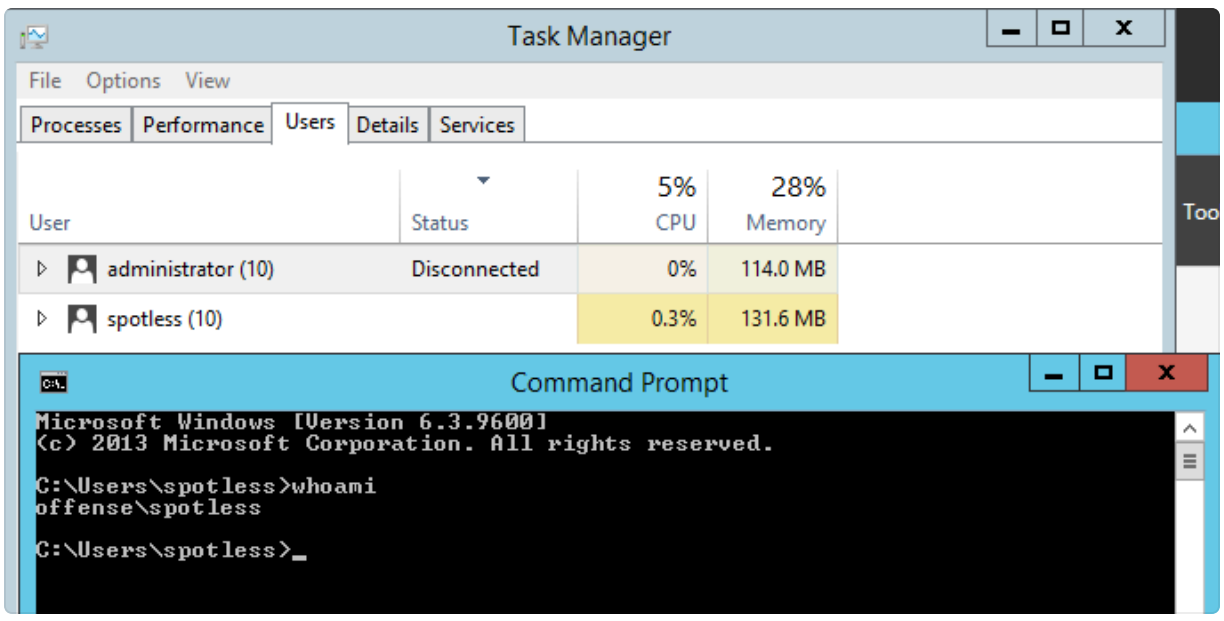


Let's switch to the `spotless` session - this requires knowing the user's password, which for this exercise is known, so lets enter it:



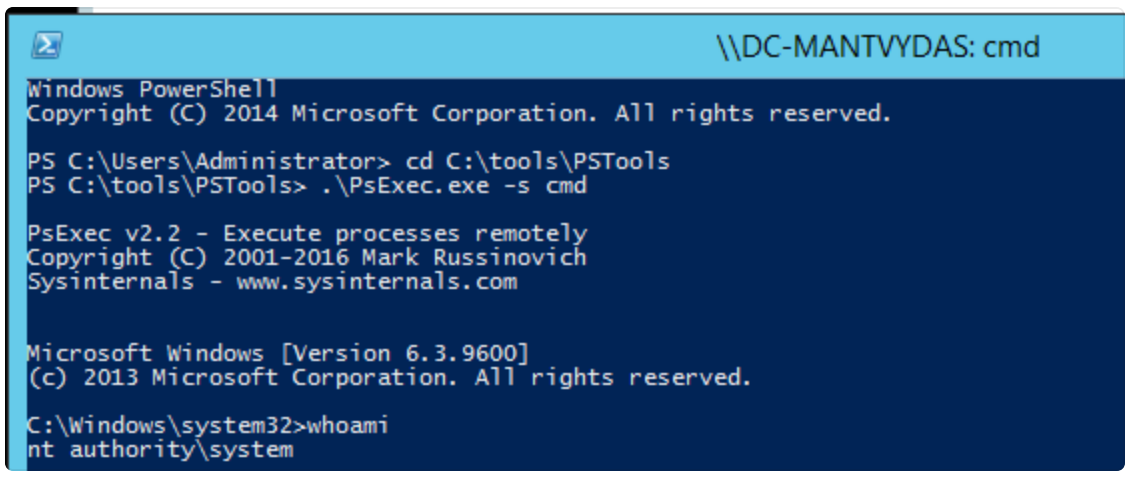


We are now reconnected to the `spotless` session:



Now this is where it gets interesting. It is possible to reconnect to a users session without knowing their password if you have `SYSTEM` level privileges on the system. Let's elevate to `SYSTEM` using psexec (privilege escalation exploits, service creation or any other technique will also do):

```
psexec -s cmd
```

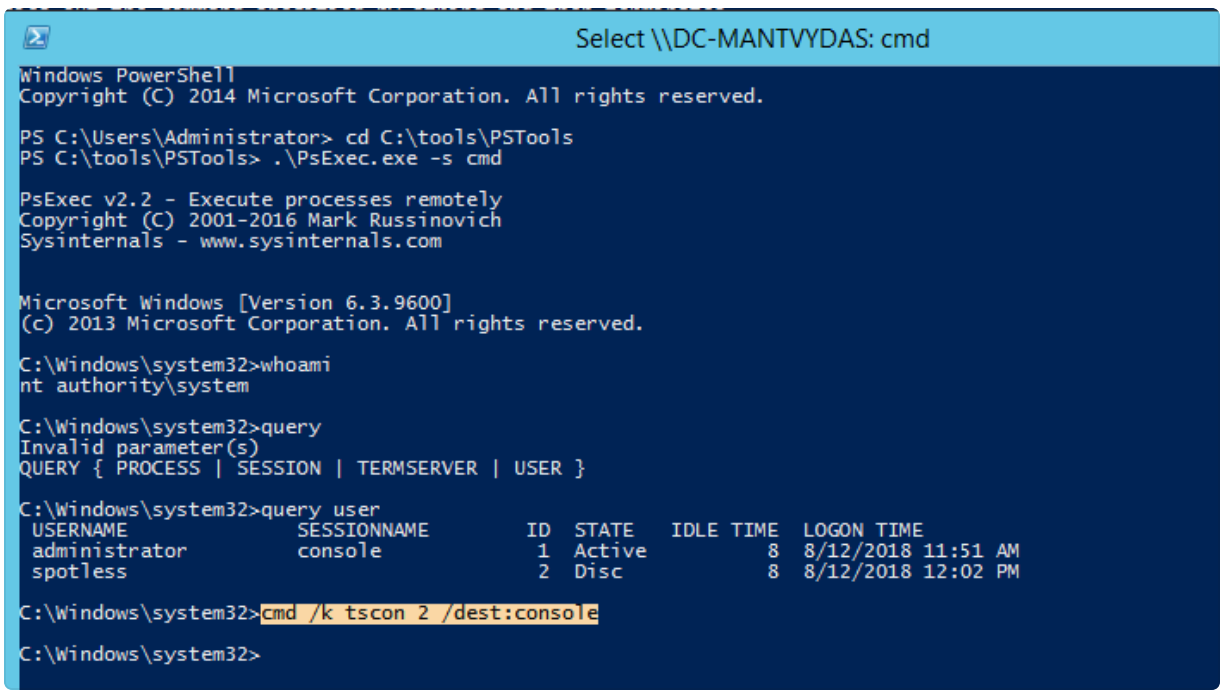


Enumerate available sessions on the host with `query user`:

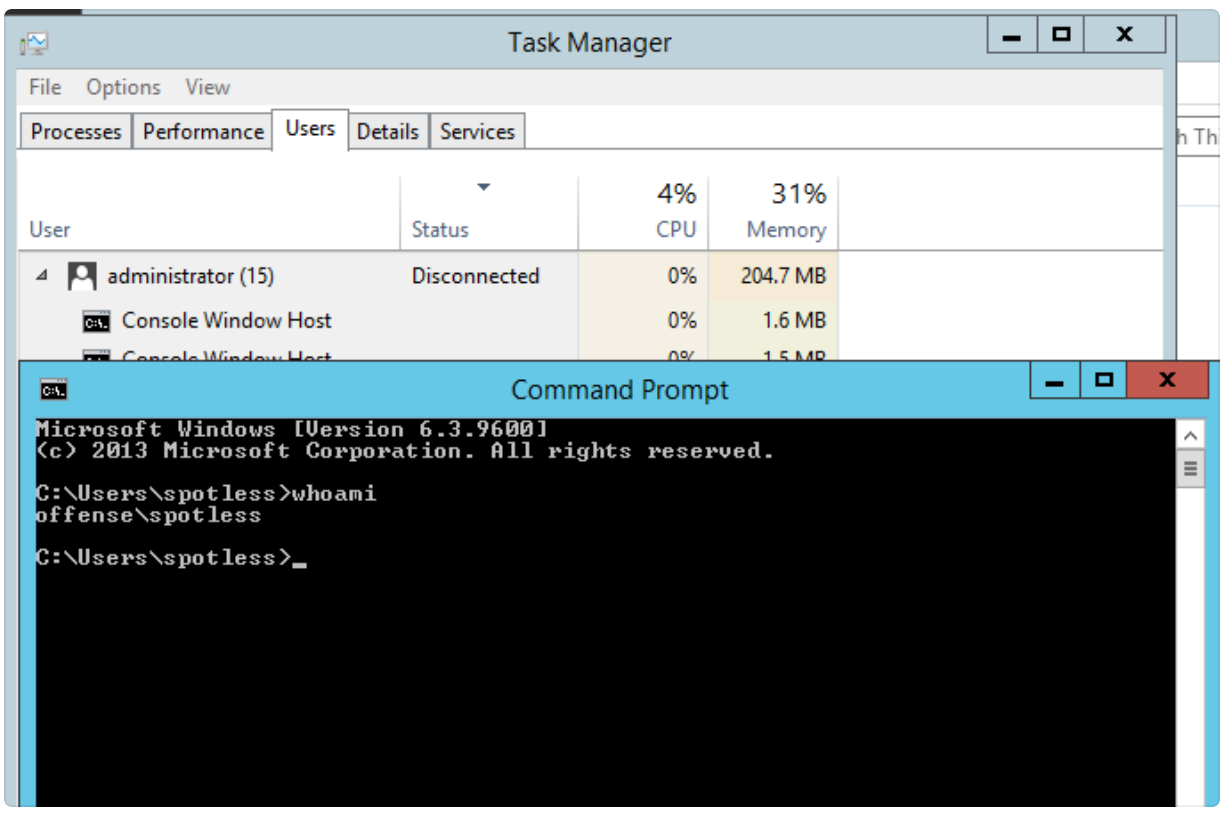
Switch to the `spotless` sessio
the native windows binary `tsc`

sessions by specifying which session ID (`2` in this case for the `spotless` session) should be connected to which session (`console` in this case, where the active `administator` session originates from):

```
cmd /k tscon 2 /dest:console
```

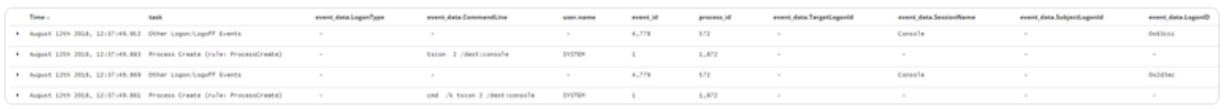


Immediately after that, we are presented with the desktop session for `spotless`:

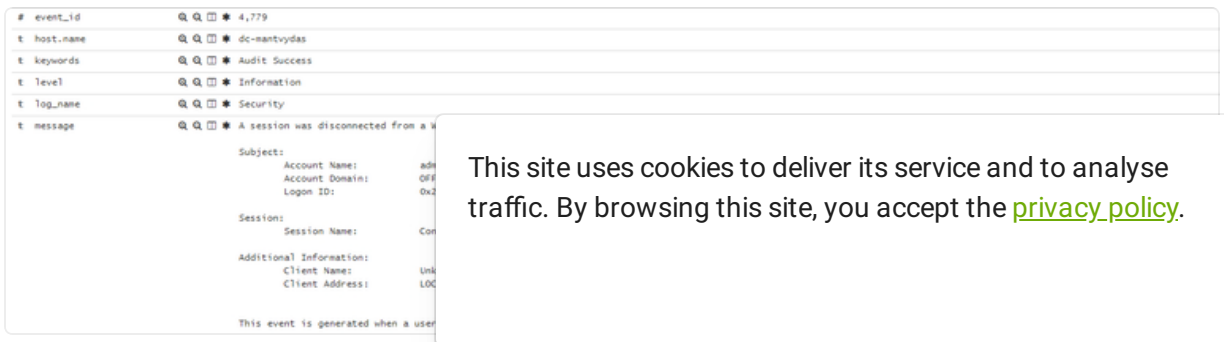


Observations

Looking at the logs, `tscon.exe` being executed as a `SYSTEM` user is something you may want to investigate further to make sure this is not a lateral movement attempt:



Also, note how `event_data.LogonID` and event_ids `4778` (logon) and `4779` (logoff) events can be used to figure out which desktop sessions got disconnected/reconnected:



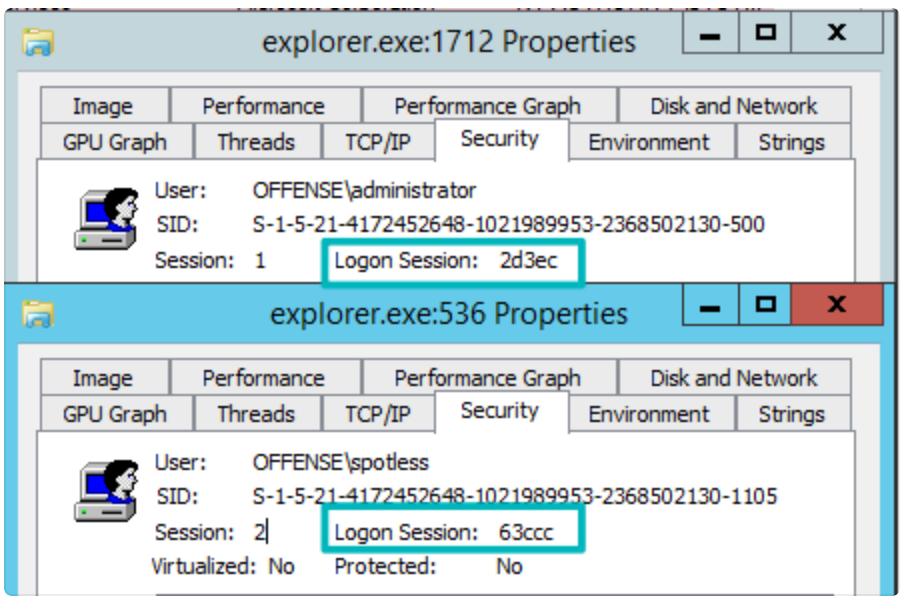
Administrator session disconnected

#	event_id	4,778
t	host.name	dc-mantvydas
t	keywords	Audit Success
t	level	Information
t	log_name	Security
t	message	A session was reconnected to a Window Station.

```
Subject:
        Account Name:           spotless
        Account Domain:         OFFENSE
        Logon ID:               0x63CCC

Session:
        Session Name:           Console

Additional Information:
        Client Name:            Unknown
        Client Address:         LOCAL

This event is generated when a user reconnects to an existing Terminal Services session, or when a user switches to an existing desktop using Fast User Switching.
```

Spotless session reconnected (hijacked)

Just reinforcing the above - note the usernames and logon session IDs:



References

- Vol de session RDP
  Blog de Gentil Kiwi
- Passwordless RDP Session Hijacking Feature All Windows versions
- Windows Security Log Event ID 4778 - A session was reconnected to a Window Station
- tscon
  docsmsft

Previous
WMI for Lateral Movement

Next
Shared Webroot

Last updated 6 years ago