What is RDP session hijacking?

RDP session hijacking is taking over another user's existing Remote Desktop session without knowing their password. With SYSTEM privileges on a machine, an attacker can use the built-in `tscon` command to connect a target's disconnected or active session to their own, instantly acting as that user. If a Domain Admin has a lingering session on the host, this is a direct path to their privileges. It abuses a legitimate Windows feature, so the defence is operational: avoid leaving privileged sessions on shared hosts.

HOW IT WORKS

01 The abuse and payload

With SYSTEM on the host, the attacker lists sessions and hijacks one:

- List sessions: `query user` or `query session` (shows session IDs and users).
- As SYSTEM, attach a target session to the current one: `tscon <target-session-id> /dest:<your-session-name>`
- A common path runs it via a SYSTEM service: `sc create hijack binpath= "cmd /k tscon <id> /dest:rdp-tcp#<n>" && sc start hijack`

The attacker now controls the victim's desktop session as that user. Documented technique shown for defenders.

> NO PASSWORD NEEDED
>
> *The danger is that as SYSTEM, tscon needs no password. A disconnected admin session left on a server is a credential the attacker can simply resume.*

HOW TO DEFEND

- Log off, do not just disconnect, privileged RDP sessions, and set policies to end disconnected sessions quickly.
- Keep Domain Admins off shared or member servers so their sessions are never sitting there to hijack.
- Limit who can gain SYSTEM on hosts (the prerequisite for the attack).
- Apply tiered administration so high-value sessions only exist on protected admin workstations.
- Monitor for tscon usage and session-connect events from service or SYSTEM contexts.

SOURCES

[1] MITRE ATT&CK: Lateral Movement (TA0008)

[2] Microsoft: Remote Desktop Services

[3] NIST SP 800-115 Technical Guide to Security Testing

Find the lateral-movement paths before an attacker does.

securelayer7.net/learn/lateral-movement/what-is-rdp-hijacking

Open online