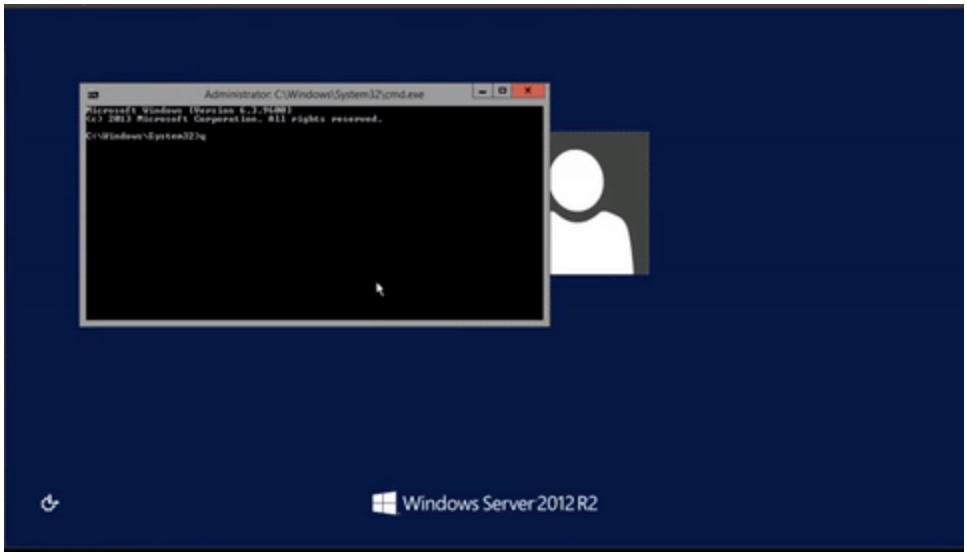
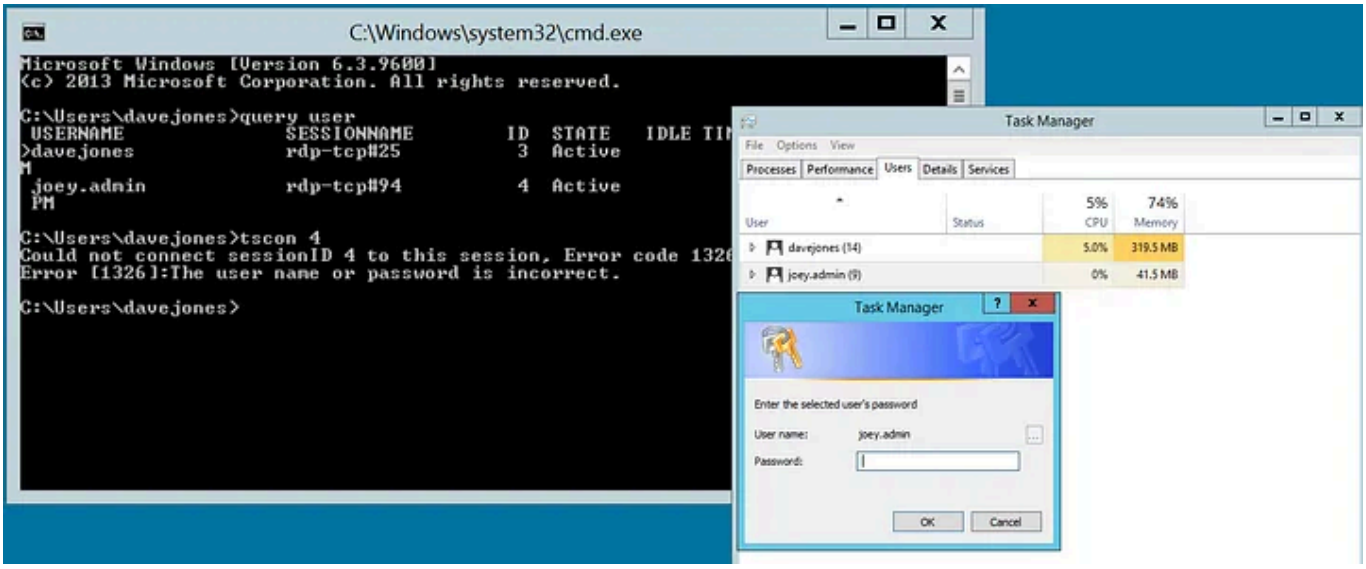
RDP hijacking — how to hijack RDS and RemoteApp sessions transparently to move through an



Alexander Korznikov demonstrates using Sticky Keys and tscon to access an administrator RDP session —



So, you have full blown RDP session hijacking, with a single command.

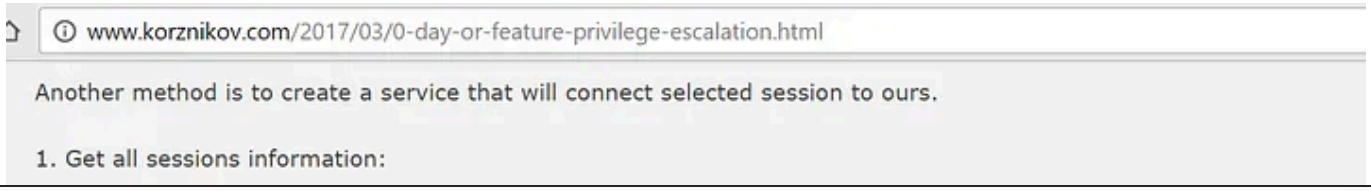
Some parameters about how far this reaches

- You can connect to disconnected sessions. So if somebody logged out 3 days ago, you can just connect straight to their session and start using it.
- It unlocks locked sessions. So if a user is away from their desk, you steal their session AND it unlocks the 'workstation' without needing any credentials.
- It works for the physical console. So you can hijack the screen remotely. It

- It works remotely. You can take over sessions on remote computers, even if you're not logged into that server.

Gaining SYSTEM for tscon.exe

If you're an administrator, you can use a service as Alexander demonstrates:



https://www.youtube.com/watch?v=OgsoloWmhWw

Other methods:

- You can use Scheduled Tasks to gain SYSTEM and run the command. Just schedule the command to run immediately as SYSTEM with interactive privileges.
- Use can use a variety of methods like Sticky Keys to get SYSTEM, without even needing to log in (in the future). See below.

From research, over 1 in 200 scanned Remote Desktop servers online are already backdoored using these methods. This means that you can session hijack with them right now, without even needing to try to log in or authenticate in any way. That's bad. Consider Shodan shows there are millions of RDP servers online right now, and the number grows constantly with cloud services etc, this is going to generate... issues.

RDP backdoor method one — Sticky Keys

The concept here is pretty simple — Windows supports a feature called Sticky Keys, which is an Accessibility feature built into the OS and available

It's exactly the same as before, just trojan utilman.exe instead. At the login screen, press Windows Key+U, and you get a cmd.exe window as SYSTEM.

```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe" /t REG_SZ /v Debugger /d "C:\windows\system32\cmd.exe" /f
```

Scanning for backdoor'd RDP servers

There is a prebuilt tool here, which works wonders — just spin it up and find

Don't expose RDS/RDP to the internet — if you do, I ***strongly suggest*** you implement multi-factor authentication. You can use things like Microsoft RD Gateway or Azure Multi-Factor Authentication Server to get very low cost multi-factor authentication. If you're exposing RDP directly to the internet and somebody creates a local user or your domain users have easy to guess or reused credentials, things will go downhill fast. Trust me — I've seen hospitals and others be ransomware'd by RDS servers.

Monitoring

It is surprisingly very difficult to record session hijacking — there is one event

Q: This isn't new or a vulnerability.

A: Java applets and macros aren't new. If the technique works, it will get used. This one has flown under the radar — that doesn't mean it is not valid.

Q: If you have SYSTEM you already own the box.

A: Correct. Can you type one command and get the unlocked desktop of a user, even if they went on holiday a week ago, without a log of it? Now you can.