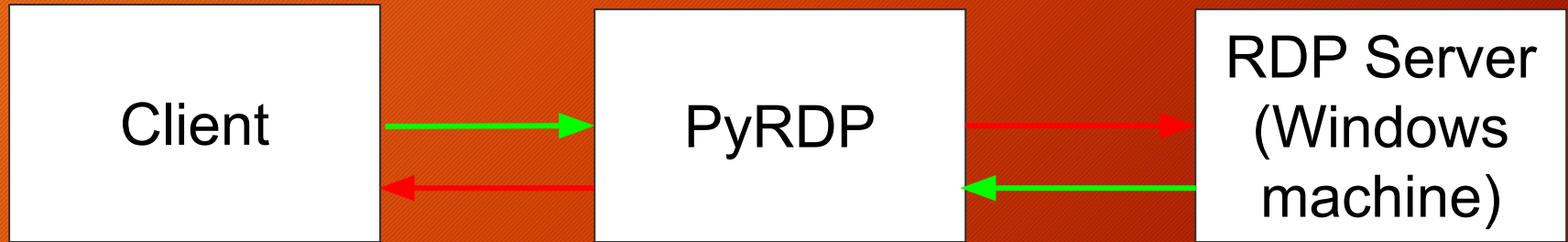


Starting Soon

PyRDP – Remote Desktop
Protocol Man-In-The-Middle

<https://github.com/GoSecure/PyRDP>

PyRDP – How it works



PyRDP – Features

- View RDP sessions live
- Record RDP sessions and replay them later
- Captures:
 - Credentials
 - Keyboard/mouse input
 - Graphical output
 - Files
 - Automatic PowerShell payloads on connection
- Enumerate the client's drive and download files from it
- Steal data copied on the client's clipboard, even if they don't paste it

PyRDP – Demo

PyRDP – Use cases

- Pentest

- Trick IT admins into connecting to PyRDP => **Become domain admin!**
- Combine with bettercap to ARP-spoof the network => **Gather creds of anyone using RDP!**

- Honeypot

- Put it on the internet and collect connection data
- Replay malicious sessions for analysis
- Files transferred through RDP are automatically saved

Try it out yourself!

- Give us a ★ on GitHub!
- <https://github.com/GoSecure/PyRDP>

Follow us on Twitter: [@GoSecure_inc](#) [@xshell](#)
[@Res260](#)