# PyRDP: RDP Proxy & Interception Tool

Olivier Bilodeau (@obilodeau) / Alexandre Beaulieu (@alxbl_sec)

GoSecure

# About Us

## Olivier Bilodeau

**Cybersecurity Research Lead at GoSecure**

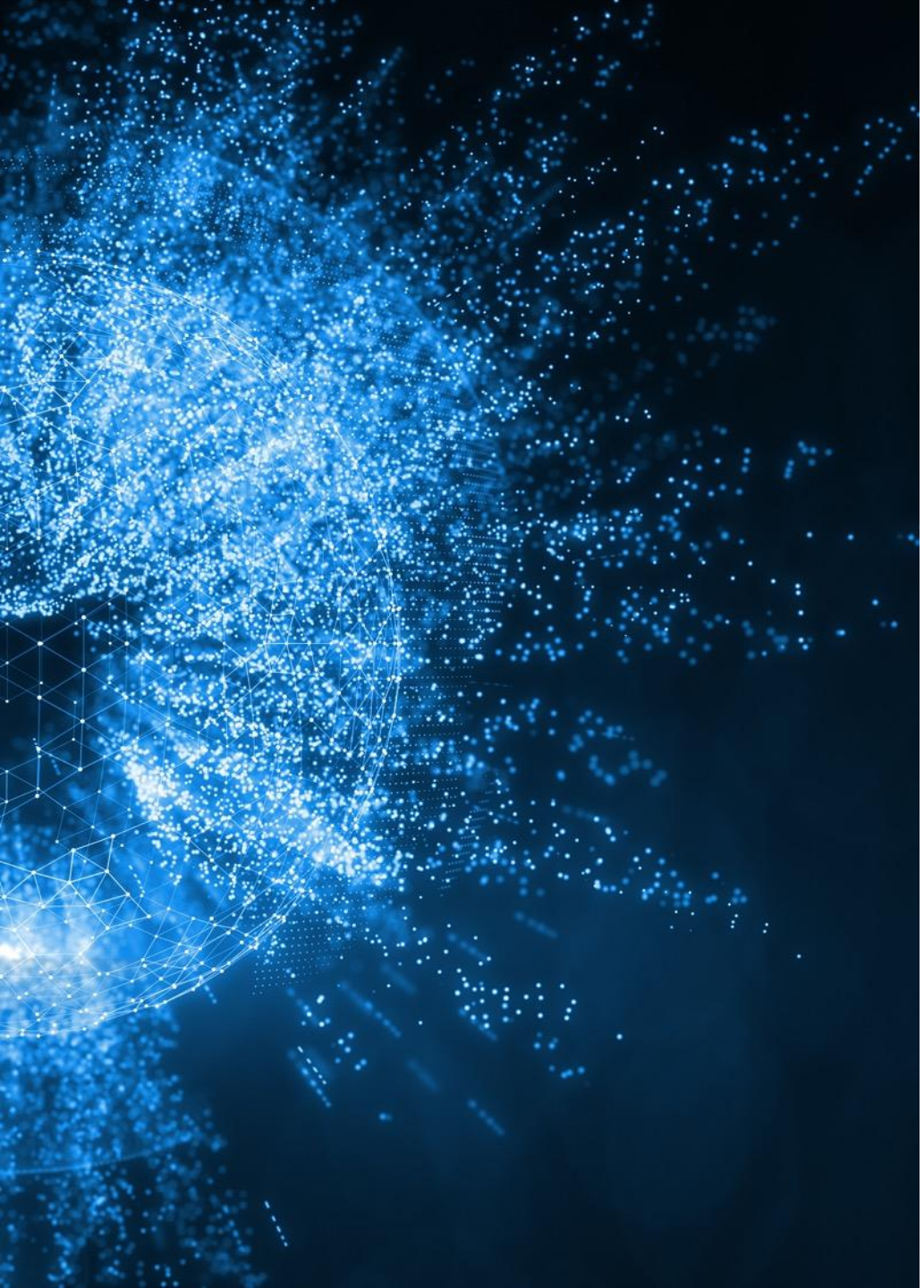
- Jack of all trades, master of none
- Co-founder MontréHack (hands-on security workshops)
- NorthSec VP Training / Hacker Jeopardy

## Alexandre Beaulieu

**Security Researcher at GoSecure**

- Software Developer
- Former Pentester
- Current PyRDP Maintainer / Developer
- Addicted to Running and Cycling

Twitter Web GitHub



# Contents



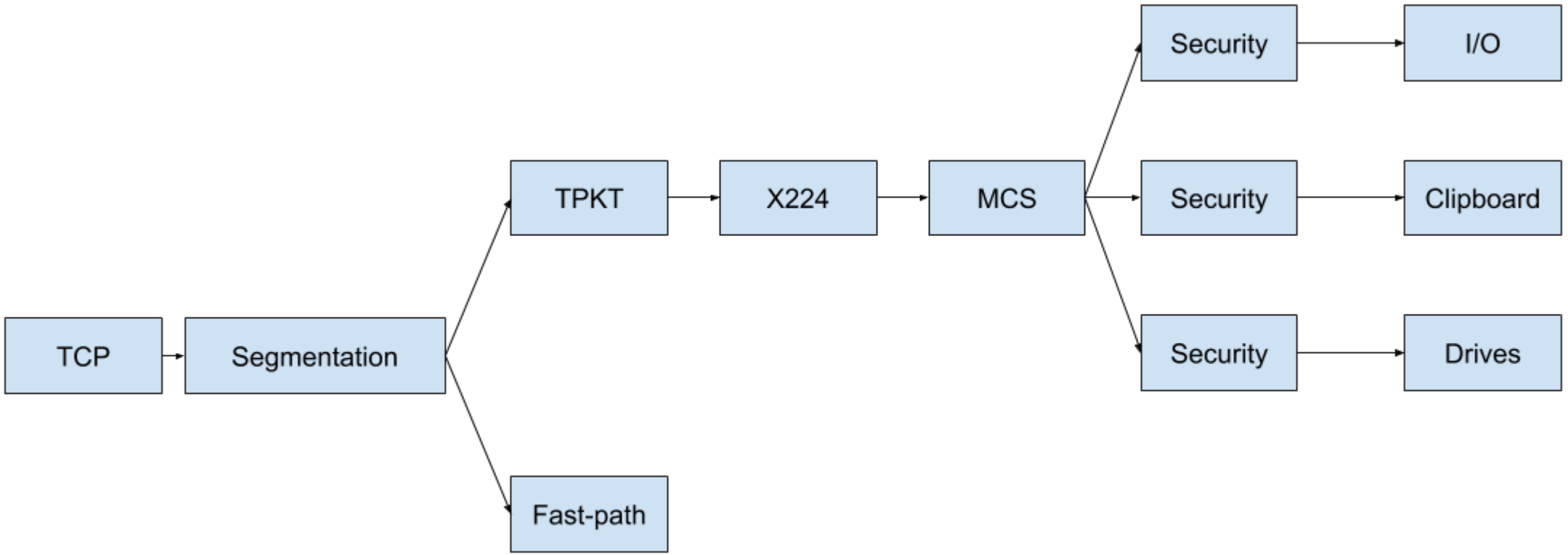
Questions? Ask on Discord channel #dl-bilodeau-pyrdp-text

# RDP at a Glance

GoSecure

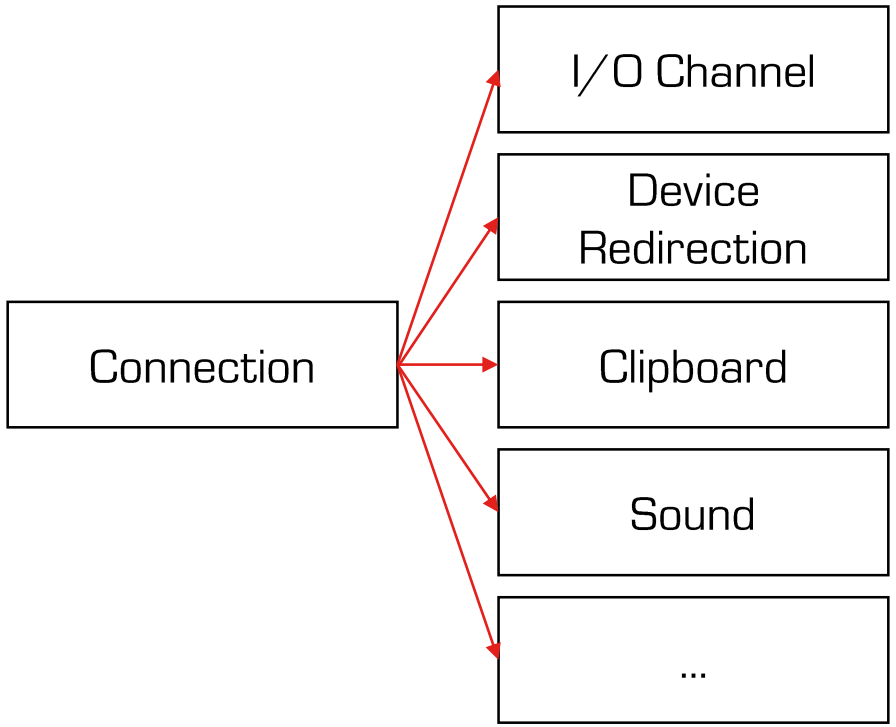
# RDP - A Layered Protocol

From TCP to Clipboard Management and I/O Channels



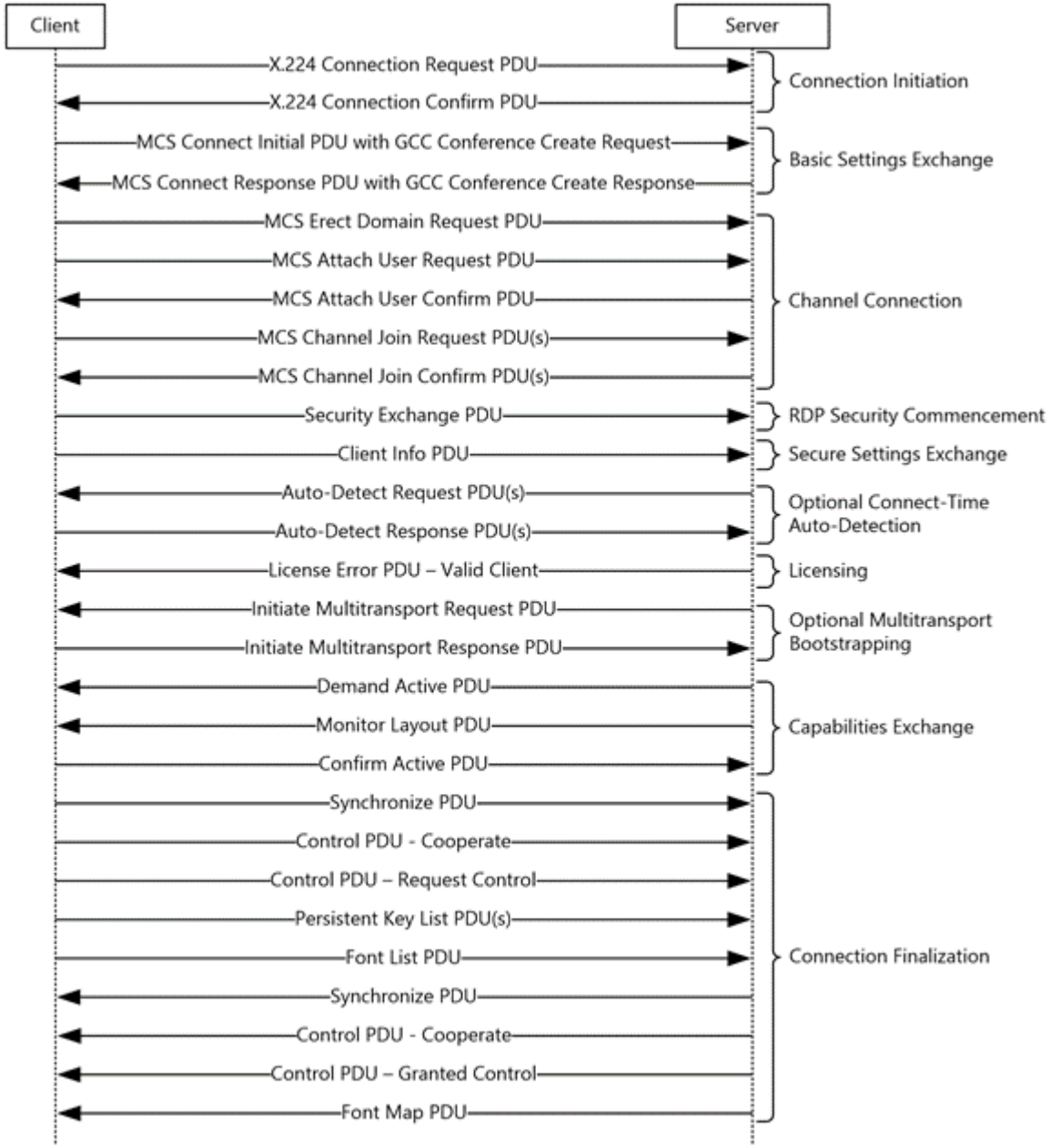
# RDP – Virtual Channels

Multiplexing data and extensions within a single connection




- Extra RDP features and extensions are implemented in virtual channels
- Server sends a list of available channels during connection phase
- Client chooses which channels to join

# RDP – The Connection Sequence



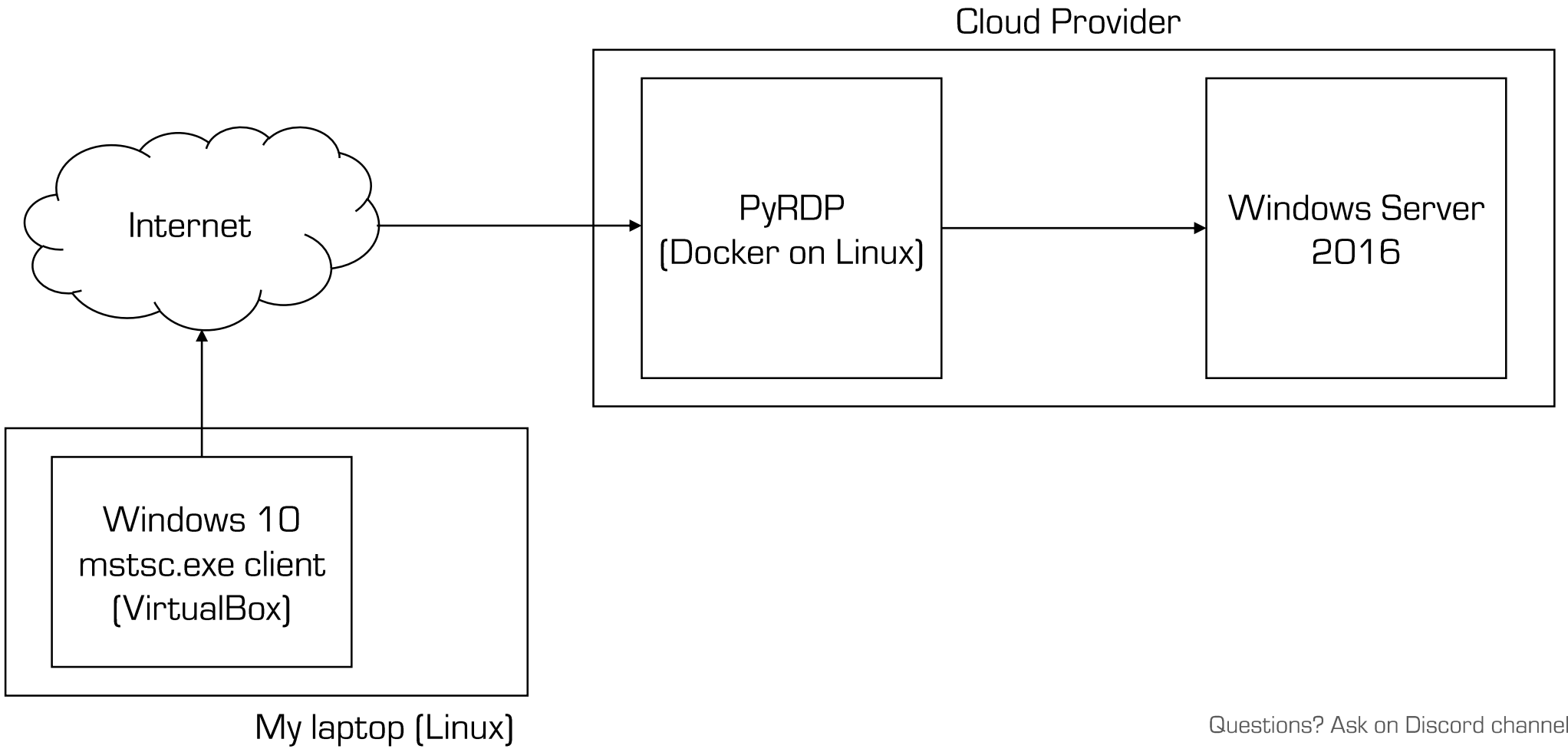

(Over-)Simplified

1. Connection Negotiation
2. Authentication
3. Channel Enrollment
4. Capability Exchange
5. Connection Established

Questions? Ask on Discord channel #dl-bilodeau-pyrdp-text

# PyRDP Core Features

# RDP Demo Environment




Questions? Ask on Discord channel #dl-bilodeau-pyrdp-text

# Core Features

## MITM

- Credentials collected
- Clipboard actively stolen
- File collector
- Extensive recording / logging

## Player

- Live replay of exact keystrokes and mouse movement
- Decoupled from MITM: sessions can be sent over the network
- After the fact replay of sessions recorded by the MITM

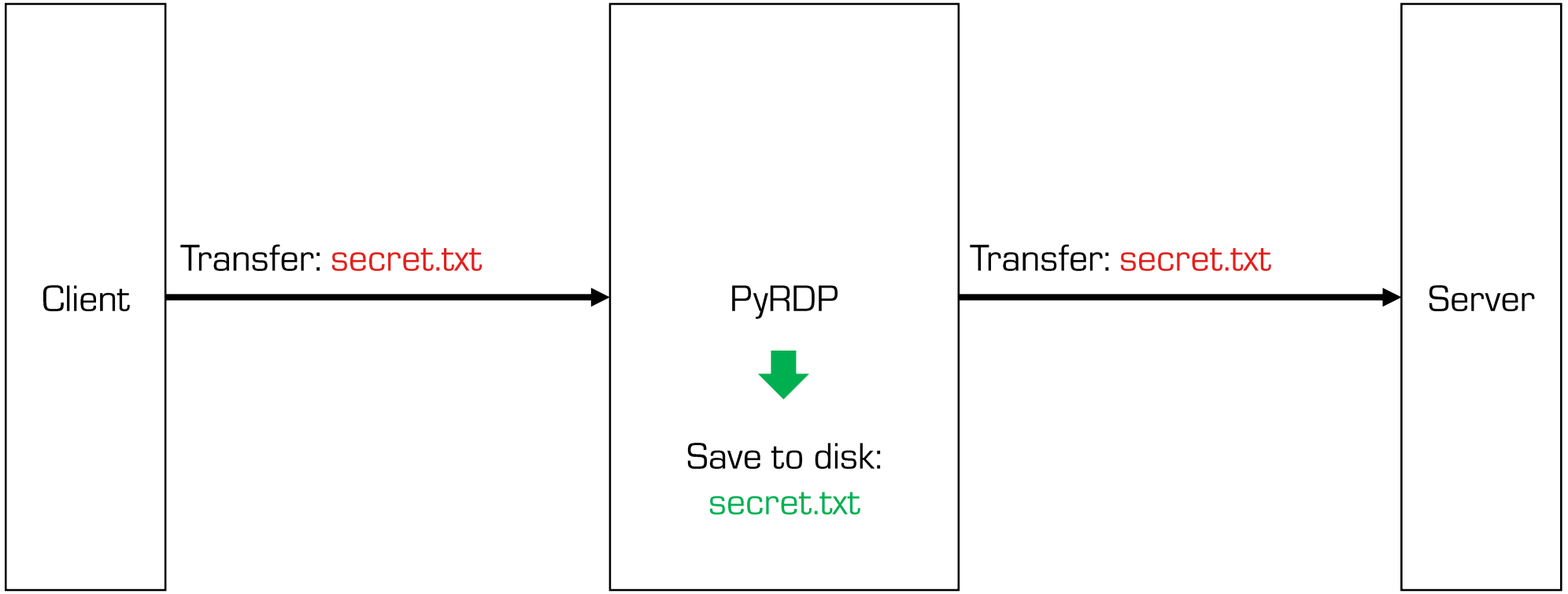
## Convert

- Recorded sessions can be converted to MP4
- Pcaps can also be converted to MP4 or PyRDP session files

Questions? Ask on Discord channel #dl-bilodeau-pyrdp-text

# PyRDP – File Carving

Transferred files are intercepted and stored to disk



# Core Features

## MITM

- Credentials collected
- Clipboard actively stolen
- File collector
- Extensive recording / logging

## Player

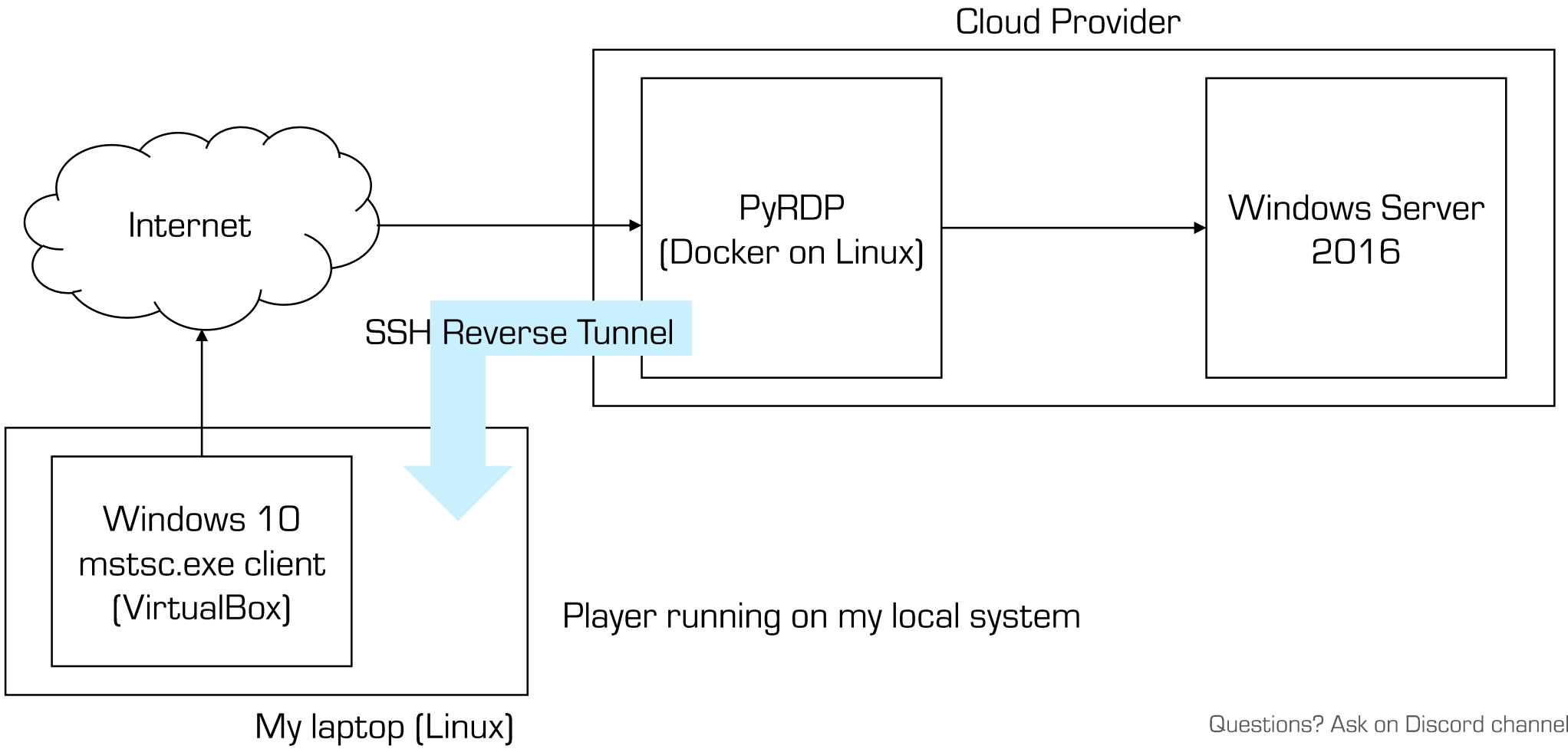
- Live replay of exact keystrokes and mouse movement
- Decoupled from MITM: sessions can be sent over the network
- After the fact replay of sessions recorded by the MITM

## Convert

- Recorded sessions can be converted to MP4
- Pcaps can also be converted to MP4 or PyRDP session files

Questions? Ask on Discord channel #dl-bilodeau-pyrdp-text

# PyRDP Player Tunneling



# Core Features

## MITM

- Credentials collected
- Clipboard actively stolen
- File collector
- Extensive recording / logging

## Player

- Live replay of exact keystrokes and mouse movement
- Decoupled from MITM: sessions can be sent over the network
- After the fact replay of sessions recorded by the MITM

## Convert

- Recorded sessions can be converted to MP4
- Pcaps can also be converted to MP4 or PyRDP session files

Questions? Ask on Discord channel #dl-bilodeau-pyrdp-text

# PyRDP as a Honeypot

GoSecure

# Honeypot Features

## Headless

- Reduced Image Size
- Architecture Independent
- Headless Player

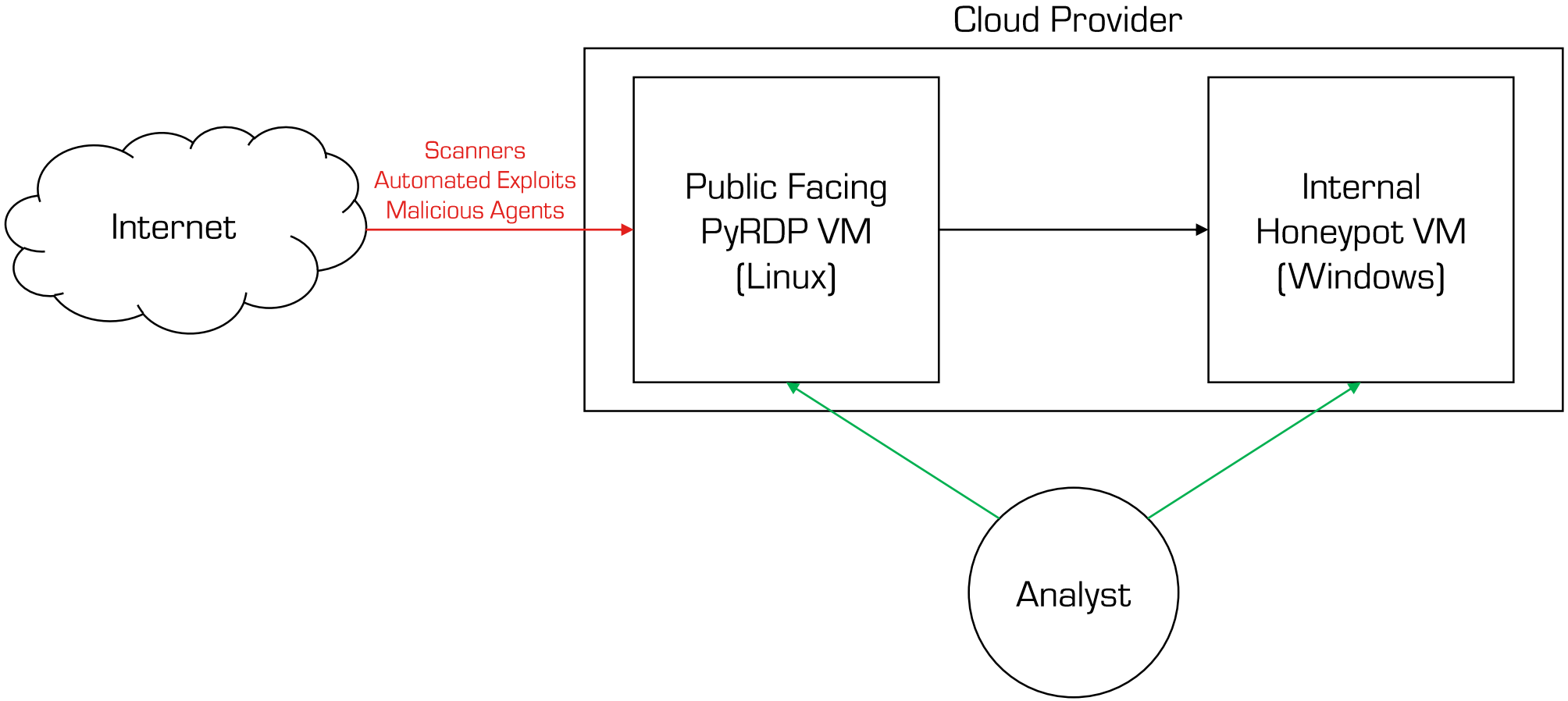
## Credentials replacement

- Any credentials will get a session
- Lure attackers

## File Harvester

- Actively steal files from client mapped drives

# RDP Honeypot - Overview




Questions? Ask on Discord channel #dl-bilodeau-pyrdp-text

# Honeypot Features

## Headless

- Reduced Image Size
- Architecture Independent
- Headless Player

## Credentials replacement

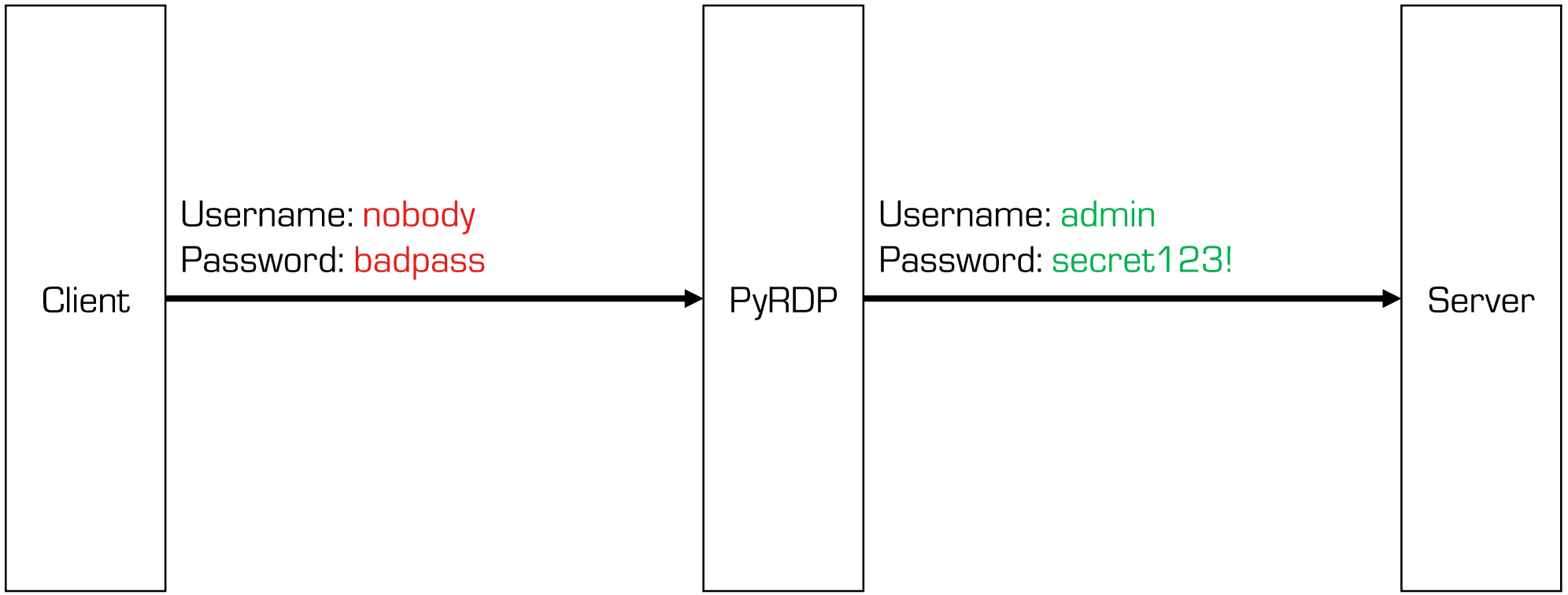
- Any credentials will get a session
- Lure attackers

## File Harvester

- Actively steal files from client mapped drives

# RDP Honeypot – Credential Stuffing

Force valid server credentials regardless of what the client requests




Questions? Ask on Discord channel #dl-bilodeau-pyrdp-text

# Honeypot Features

## Headless

- Reduced Image Size
- Architecture Independent
- Headless Player

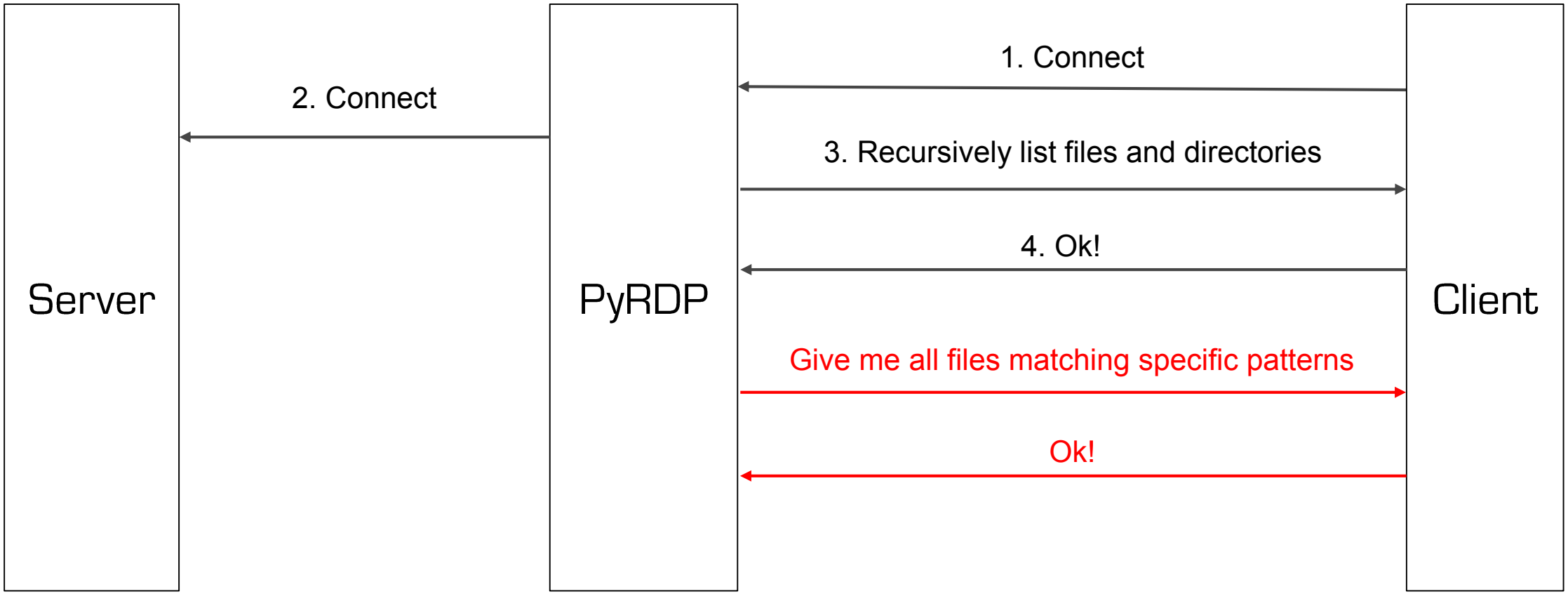
## Credentials replacement

- Any credentials will get a session
- Lure attackers

## File Harvester

- Actively steal files from client mapped drives

# RDP Honeypot – File Harvester



# Honeypot Features

## Headless

- Reduced Image Size
- Architecture Independent
- Headless Player

## Credentials replacement

- Any credentials will get a session
- Lure attackers

## File Harvester

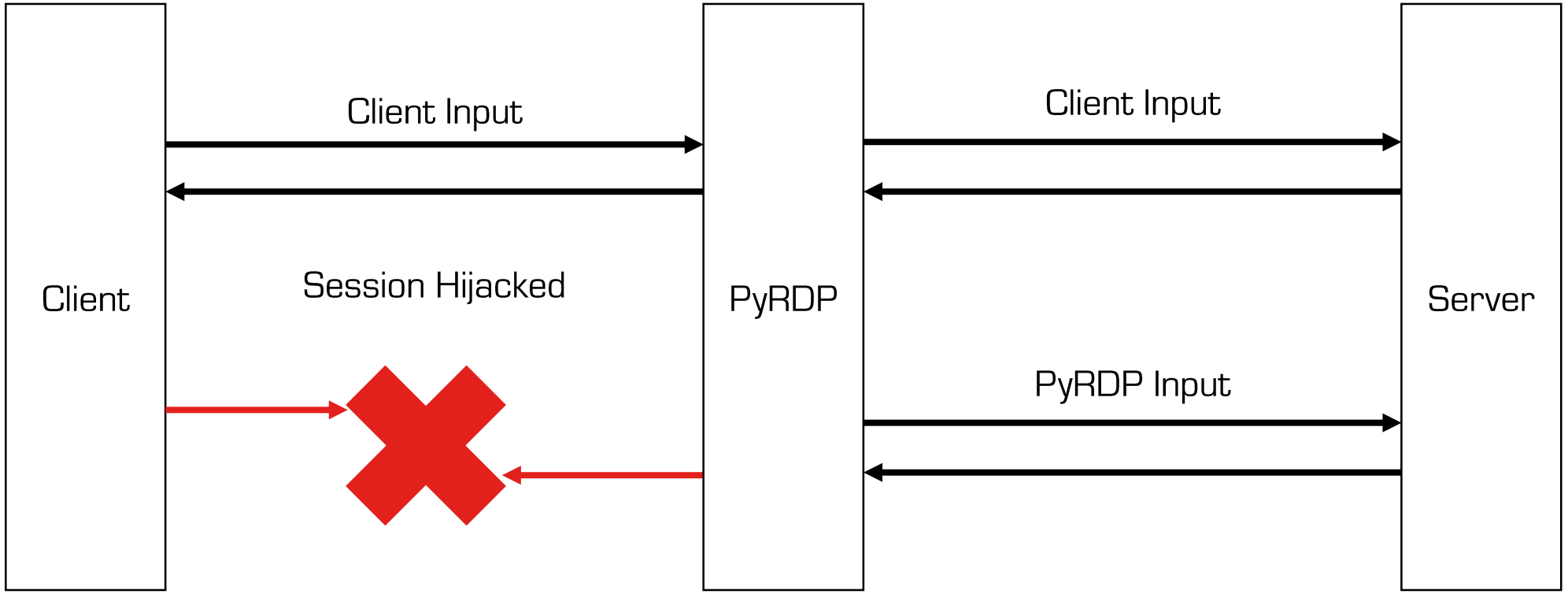
- Actively steal files from client mapped drives

# PyRDP as an Attack Tool

GoSecure

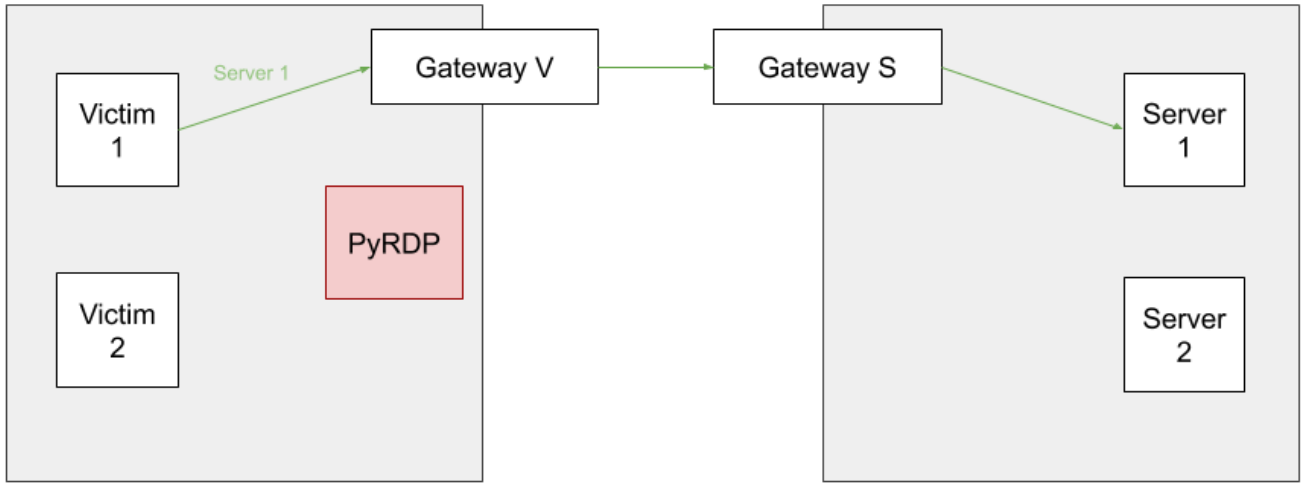
# RDP Attacks – Session Hijacking

Taking over an interception RDP connection with a single button



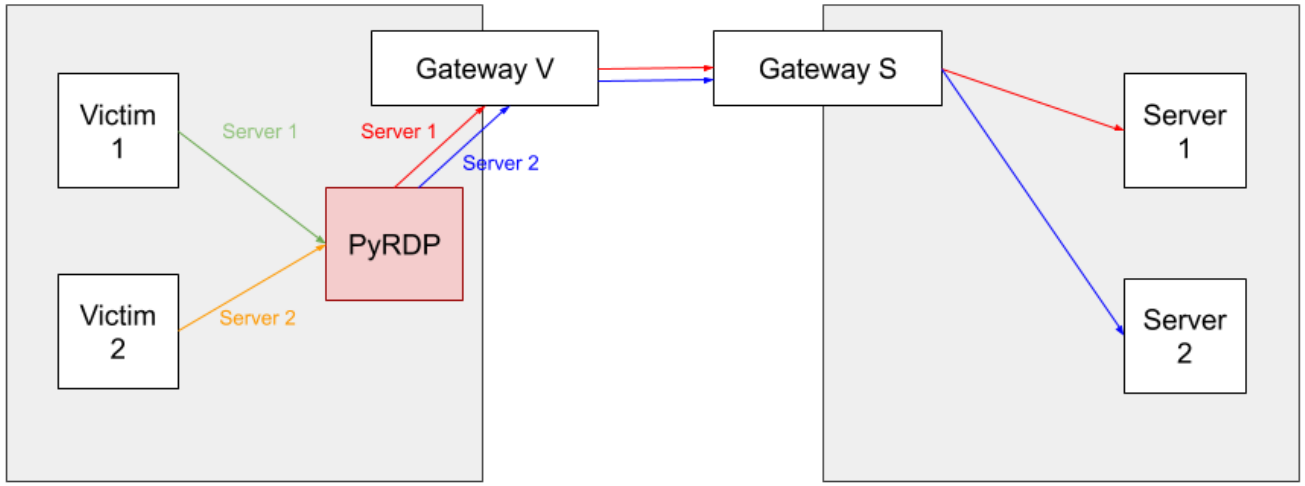
# RDP Attacks – Transparent Proxying

Transparently intercept subnets at scale with ARP spoofing




## No ARP Spoofing / TPROXY

**Clients must directly connect to PyRDP**



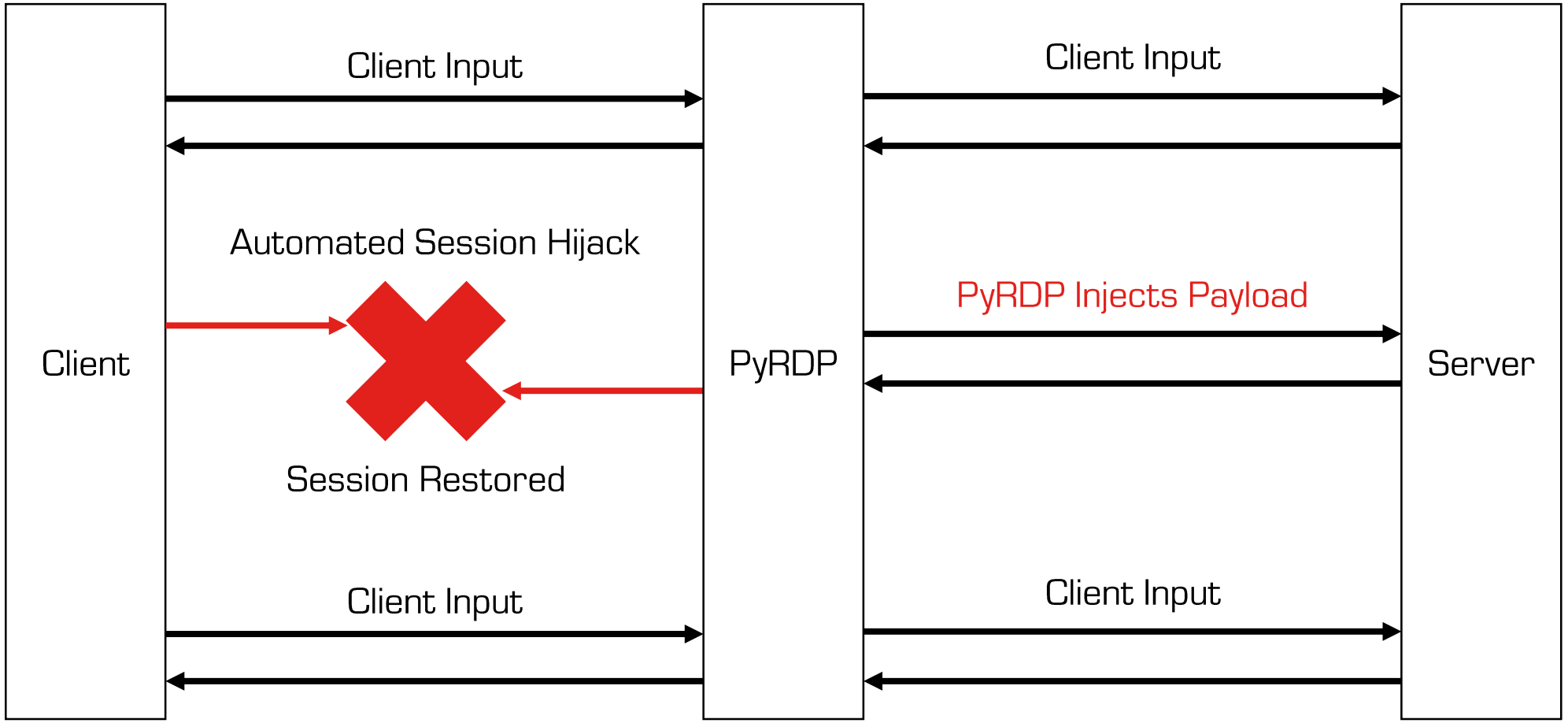

## ARP Spoofing + TPROXY

**Clients are intercepted and redirected to their intended server***

*Clients will fail to connect if the intended server enforces NLA or requires CredSSP

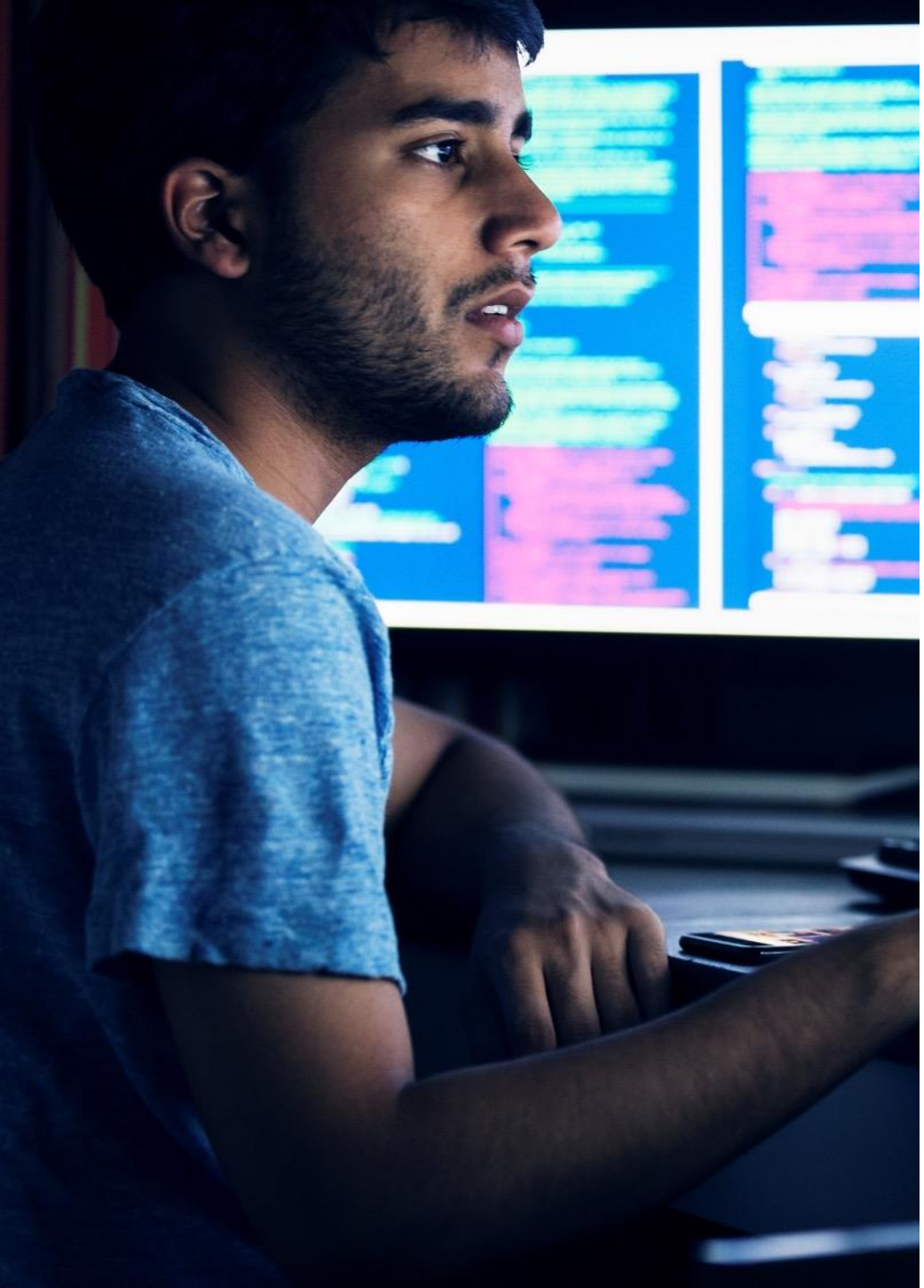
# RDP Attacks – Command Injection

Automatically run arbitrary code on any intercepted connection



# Resources

GoSecure



# Reminder on Attack Limitations

- **Certificate error upon connection**
  - Hostname (mitigate: pyrdp-clonecert.py)
  - Certs not CA signed
- **Mapped drives cause an additional warning dialog since Windows 10**
- **NLA (CredSSP) must not be enforced**
- **ARP poisoning is risky**

Questions? Ask on Discord channel #dl-bilodeau-pyrdp-text

# Learn More About PyRDP

Try it out, contribute, give us your feedback!

## Source Code / Documentation

- https://github.com/GoSecure/pyrdp
- PyRDP Transparent Proxying Guide

- RDP Connection Sequence
- RDP Basic Protocol Specification

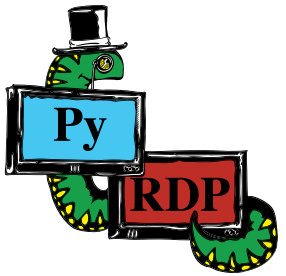
## Past Presentations & Blogs

- Introduction Blog Post
- NorthSec 2019 Talk
- BlackHat Arsenal 2019
- Blog: PyRDP on Autopilot
- DerbyCon 2019 (Video)


**Contact us on Twitter**

@obilodeau

@alxbl_sec


Questions? Ask on Discord channel #dl-bilodeau-pyrdp-text