



PyRDP: RDP Proxy & Interception Tool

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



About Us



Olivier Bilodeau

Cybersecurity Research Lead at GoSecure

- Jack of all trades, master of none
- Co-founder MontréalHack (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

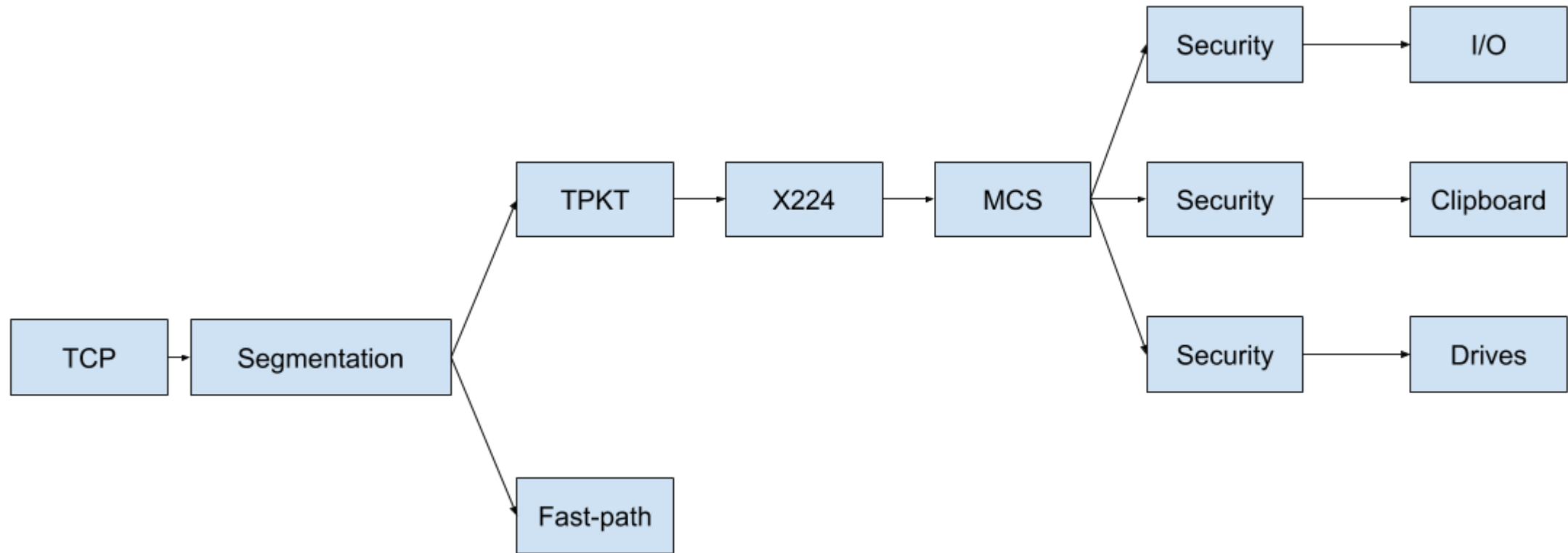


- RDPat a Glance
- PyRDPCore Features
- PyRDPas a Honeypot
- PyRDPas an Attack Tool
- Resources

RDP at a Glance

RDP-A Layered Protocol

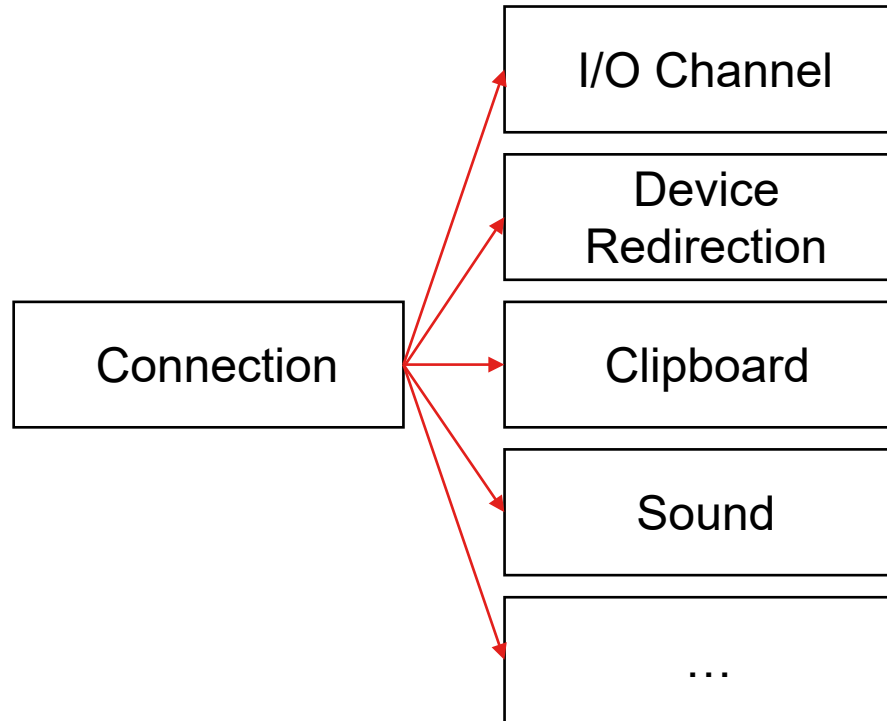
From TCP to Clipboard Management and I/O Channels



RDP– Virtual Channels

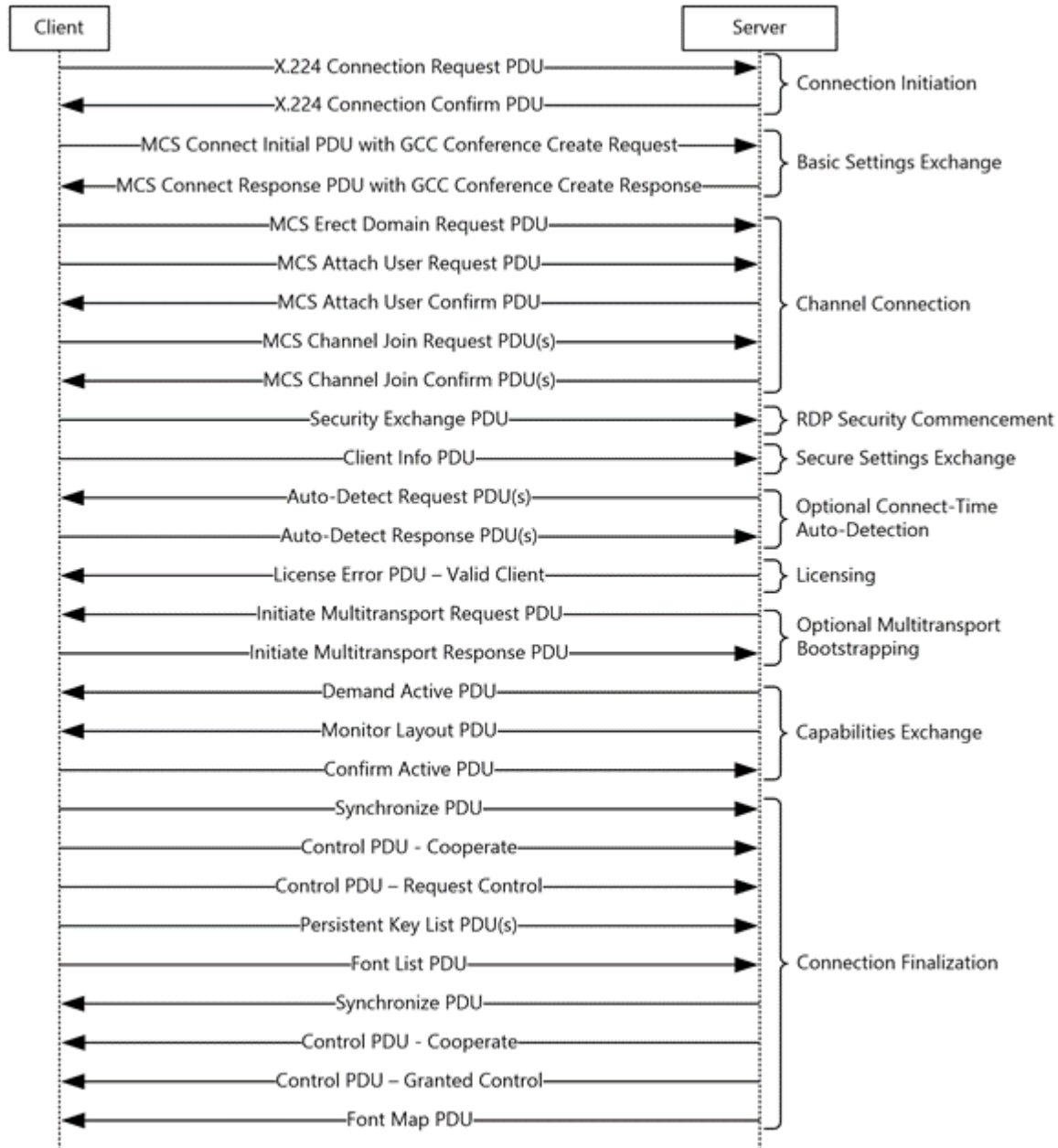


Multiplexing data and extensions within a single connection



- 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

PyRDPCore Features

Core Features



Keylogging

All keyboard and mouse interactions are logged and saved in the PyRDPsession file.

Keystrokes can be retrieved without video playback with

```
pyrdp-player.py \  
--headless
```

Screen Recording

PyRDPrecords the video output from the server from the moment the connection is established

Recorded sessions can be replayed on demand or converted to MP4

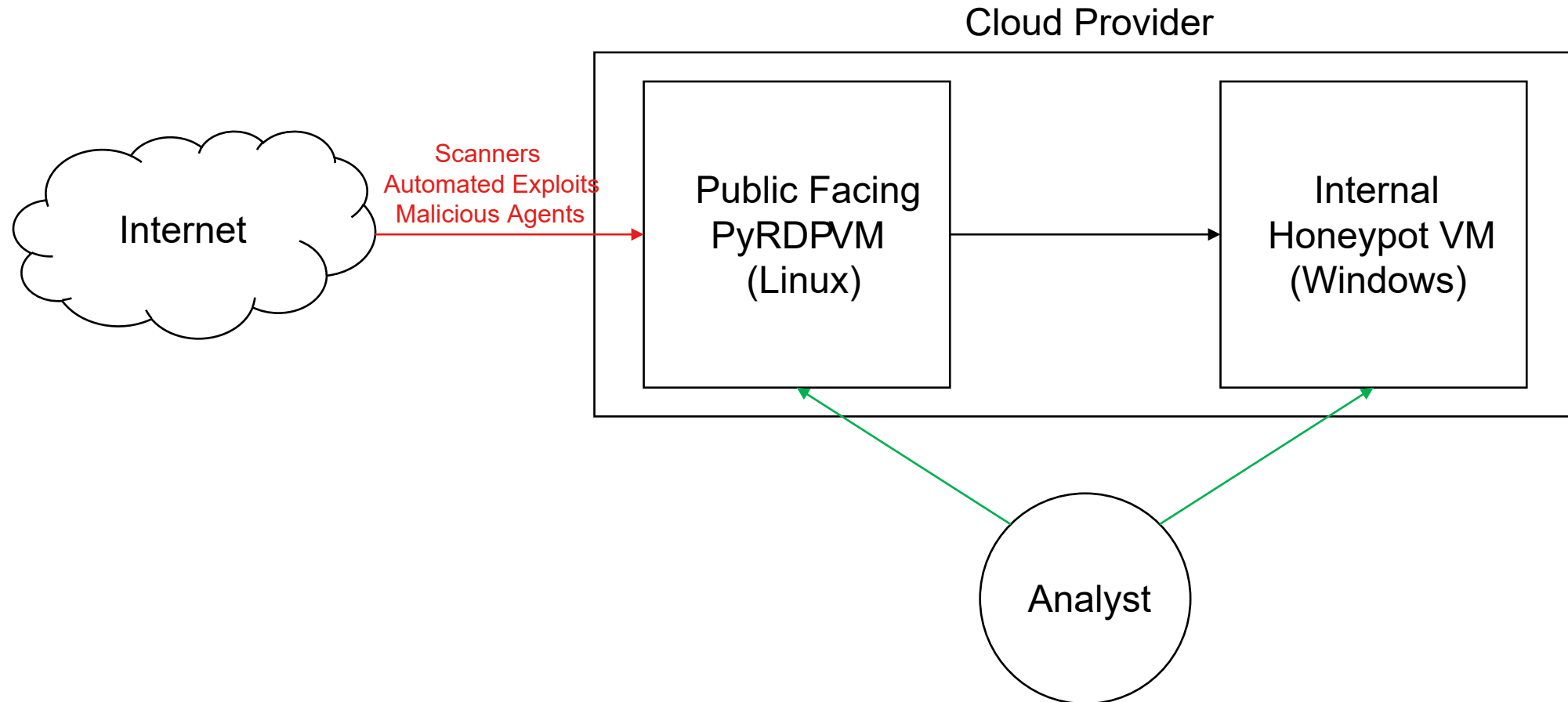
Credential Capture

Credentials are dumped to the terminal and log files when stored in the connection request

Keyboard heuristics to detect them in other cases

PyRDP as a Honeypot

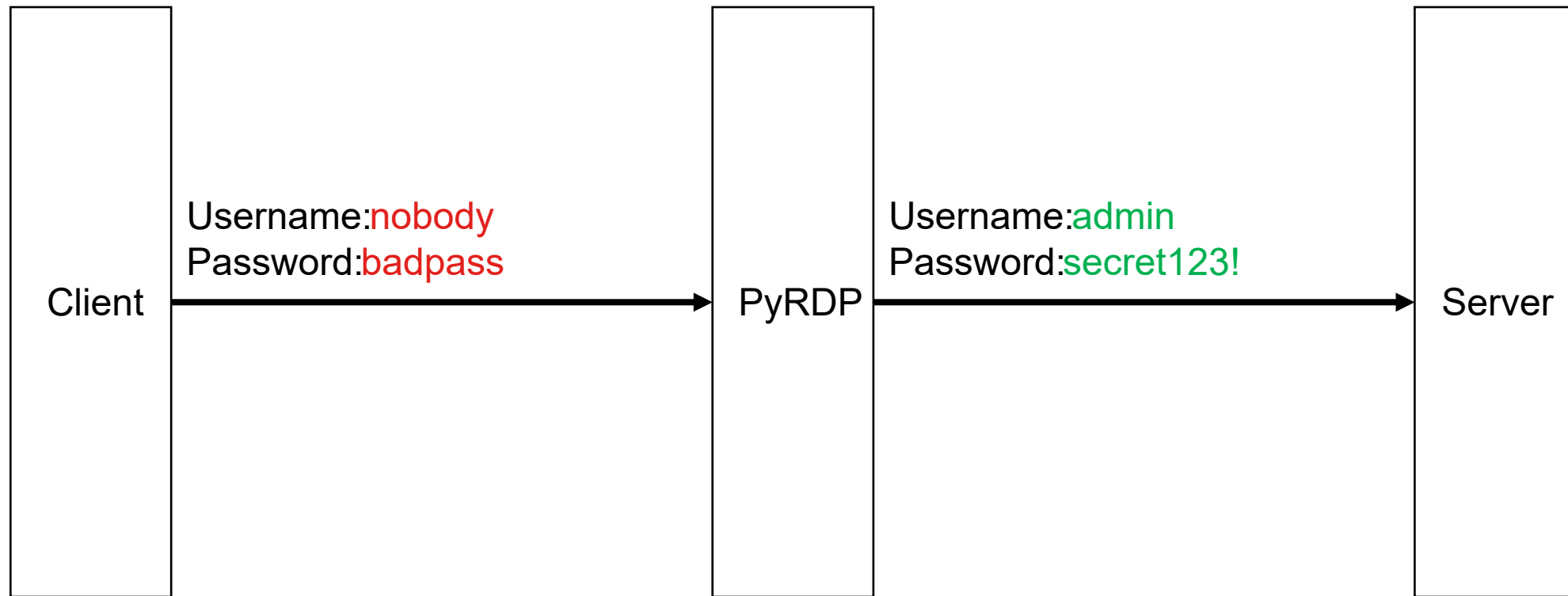
RDP Honeypot Overview



RDP Honeypot– Credential Stuffing

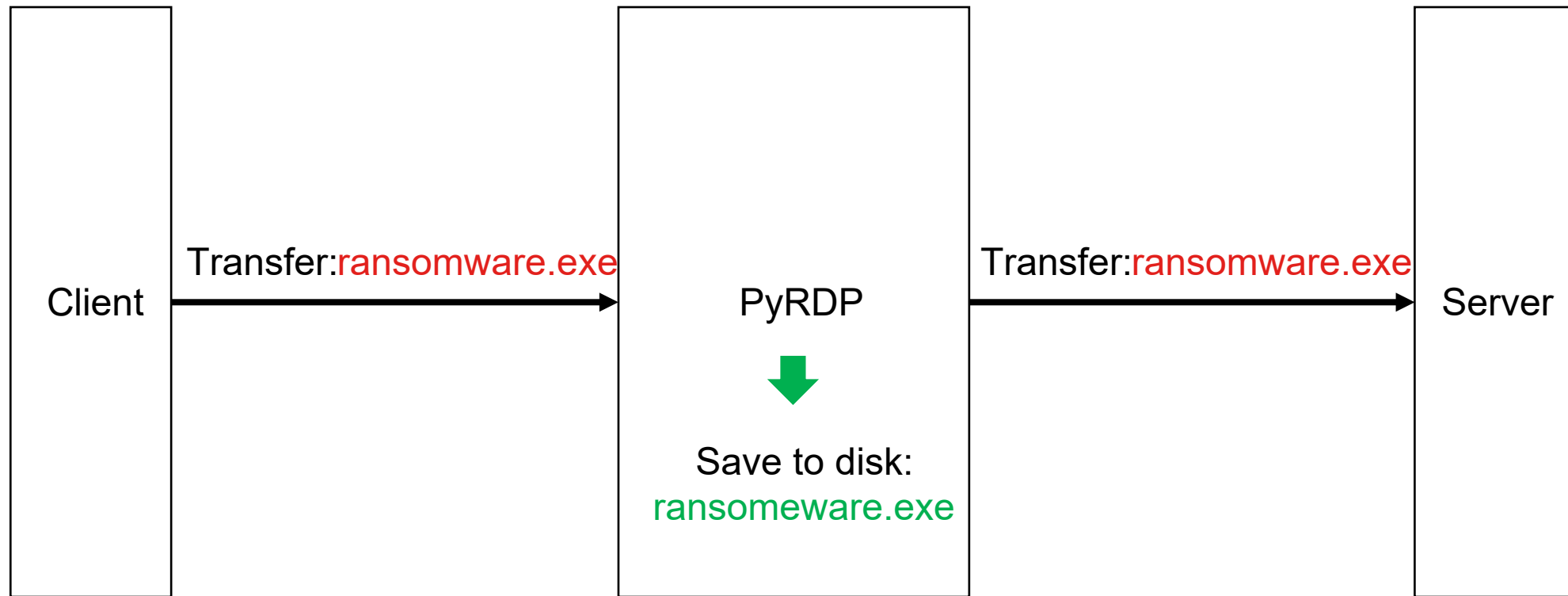


Force valid server credentials regardless of what the client requests



RDP Honeypot–File Carving

Transferred files are intercepted and stored to disk

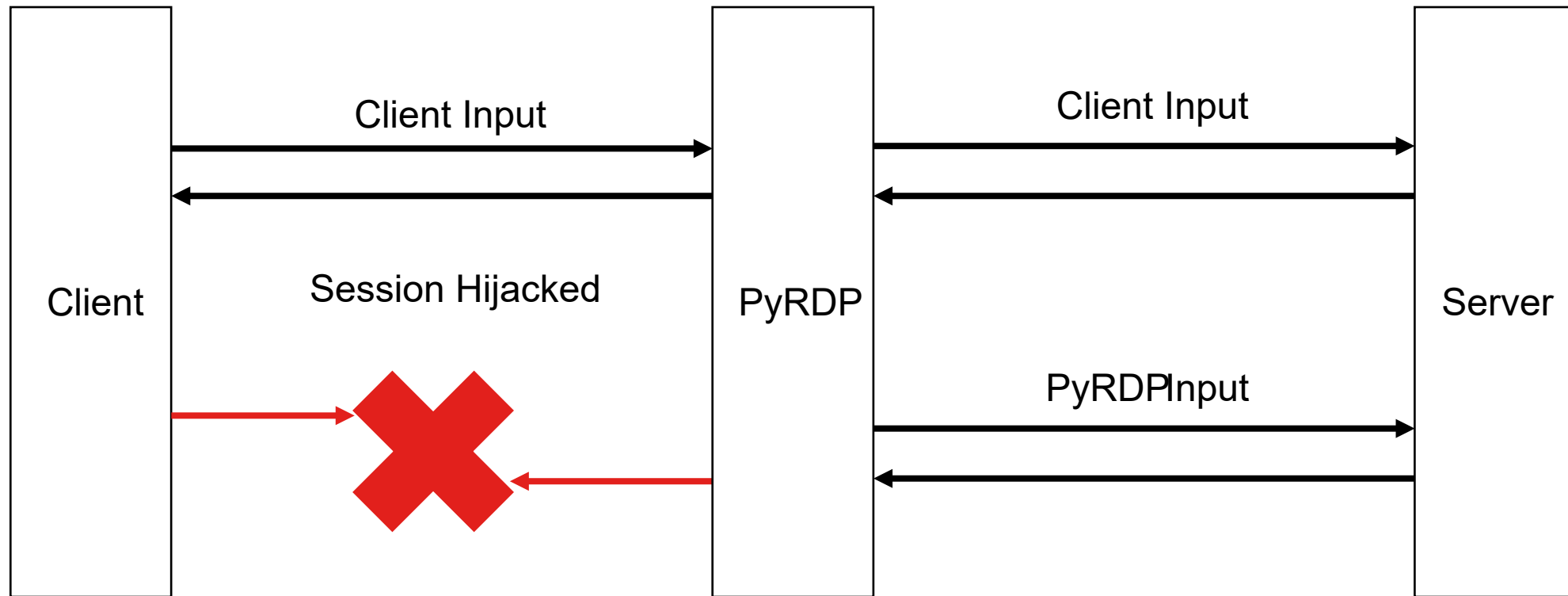


PyRDPas an Attack Tool

RDP Attacks – Session Hijacking



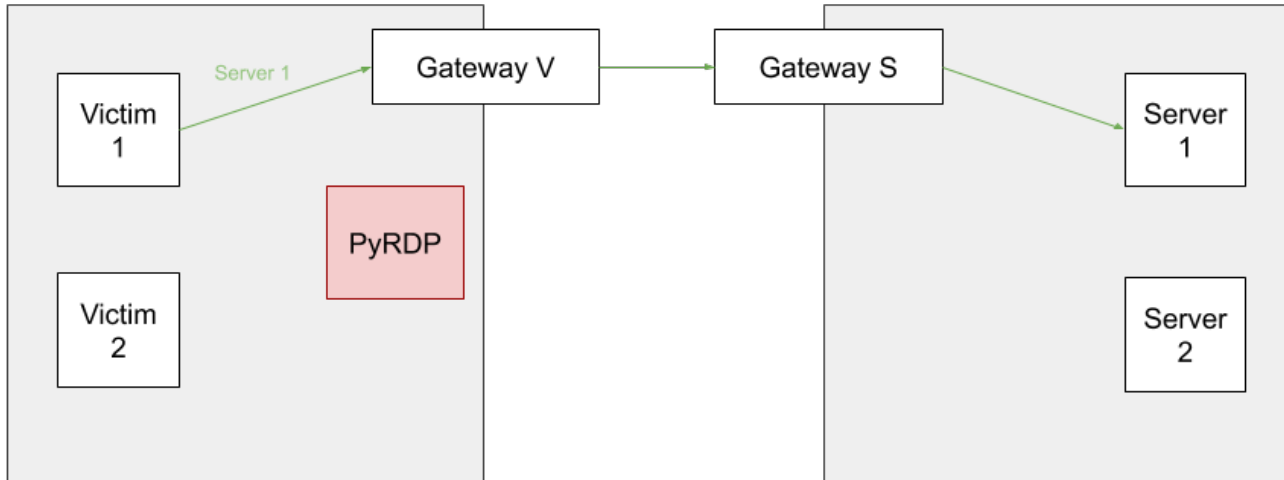
Taking over an interception RDP connection with a single button



RDP Attacks – Transparent Proxying

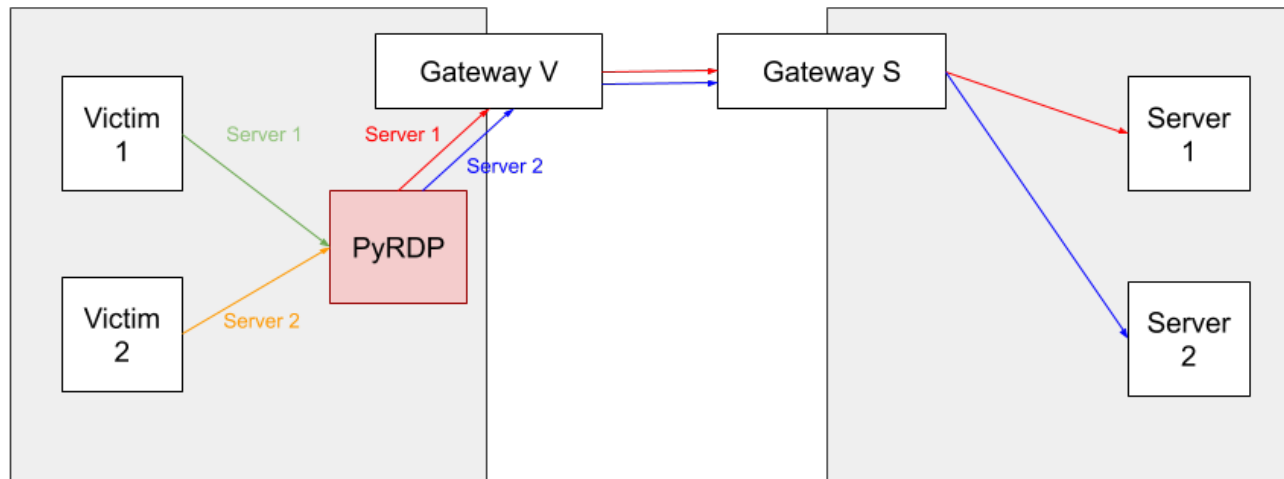


Transparently intercept subnets at scale with ARP spoofing



No ARP Spoofing / TPROXY

Clients must directly connect to PyRDP



ARP Spoofing + TPROXY

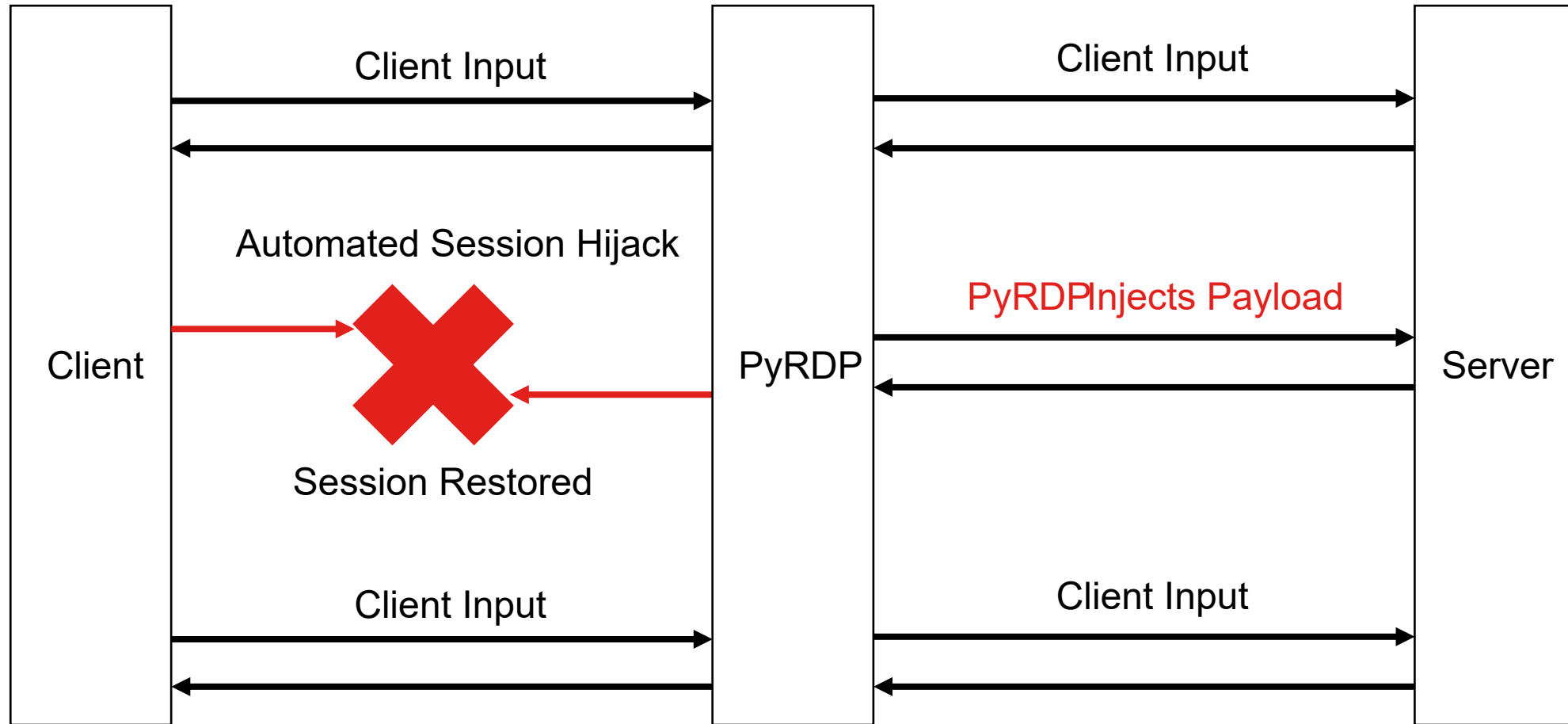
Clients are intercepted and redirected to their intended server*

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

RDP Attacks – Command Injection



Automatically run arbitrary code on any intercepted connection



Resources



Learn More About PyRDP

Try it out, contribute, give us your feedback!

Source Code / Documentation

- <https://github.com/GoSecure/pyrdp>
- [PyRDPTransparent Proxying Guide](#)
- [RDP Connection Sequence](#)
- [RDP Basic Protocol Specification](#)

Past Presentations & Blogs

- [Introduction Blog Post](#)
- [NorthSec 2019 Talk](#)
- [BlackHat Arsenal 2019](#)
- [Blog: PyRDPon Autopilot](#)
- [DerbyCon2019](#) ([Video](#))

Contact us on Twitter

@obilodeau

@alxbl_sec

