PyRDP: Remote Desktop Protocol Monster-in-the-Middle (MITM)

Olivier Bilodeau (@obilodeau), GoSecure

Olivier Bilodeau

Cybersecurity Research Lead at GoSecure

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

Arsenal Overview

RDP Overview

- Layers
- Virtual Channels
- Security

What can PyRDP do?

- MITM
- Player
- Convert
- Demo
- Honeypot
- Offensive
- Demo

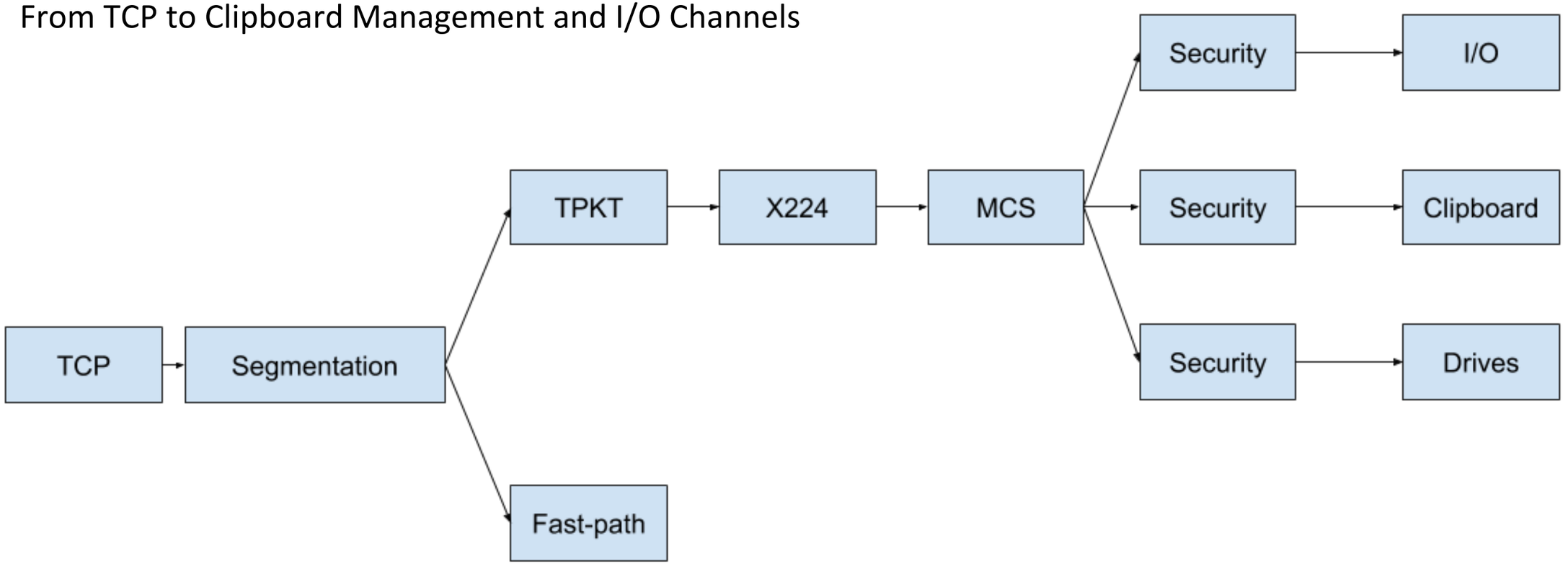
New in 1.1

- New features
- Demo
- What's next?

RDP Overview

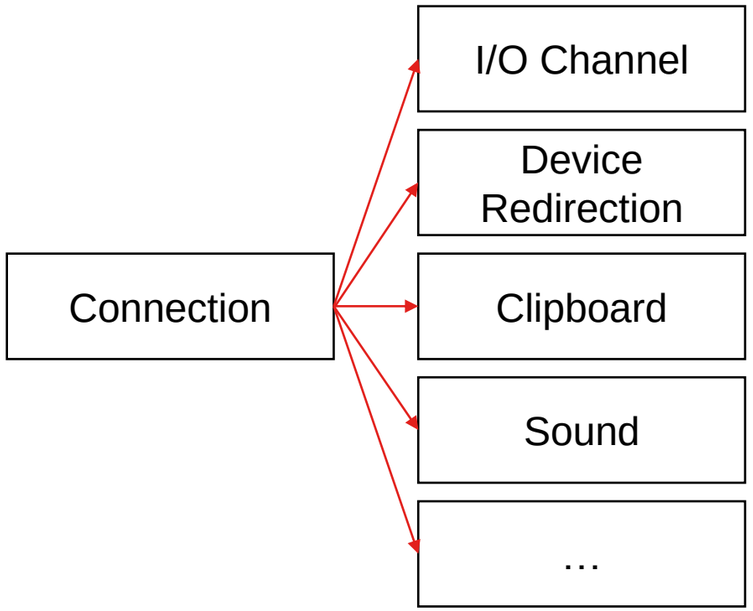
RDP Layers

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 Security

- RC4 + Graphical login (dead)
- TLS + Graphical login (legacy)
- TLS + Network Level Authentication (NLA) which relies on CredSSP

What is PyRDP?

Core Features

MITM

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

Player

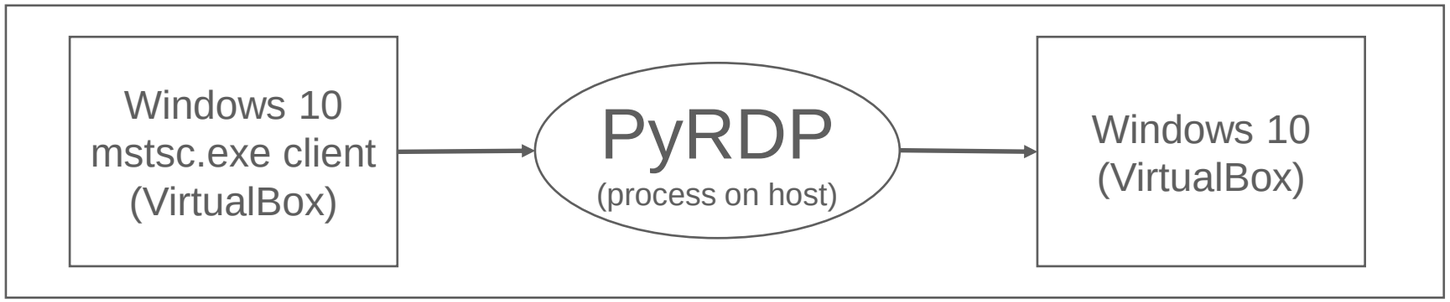
- Live replay of exact keystrokes and mouse movement
- Decoupled from MITM: sessions can be sent over the network
- After the fact replay of sessions recorded by the MITM

Convert

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

PyRDP Core Feature Set Demo

- Credentials, keystrokes and clipboard interception
- Replay capabilities
- Conversion of the replay to video



Honeypot features

Slim image

- No GUI or AV conversion dependencies
- Reduced Image Size
- Architecture Independent
- Headless Player

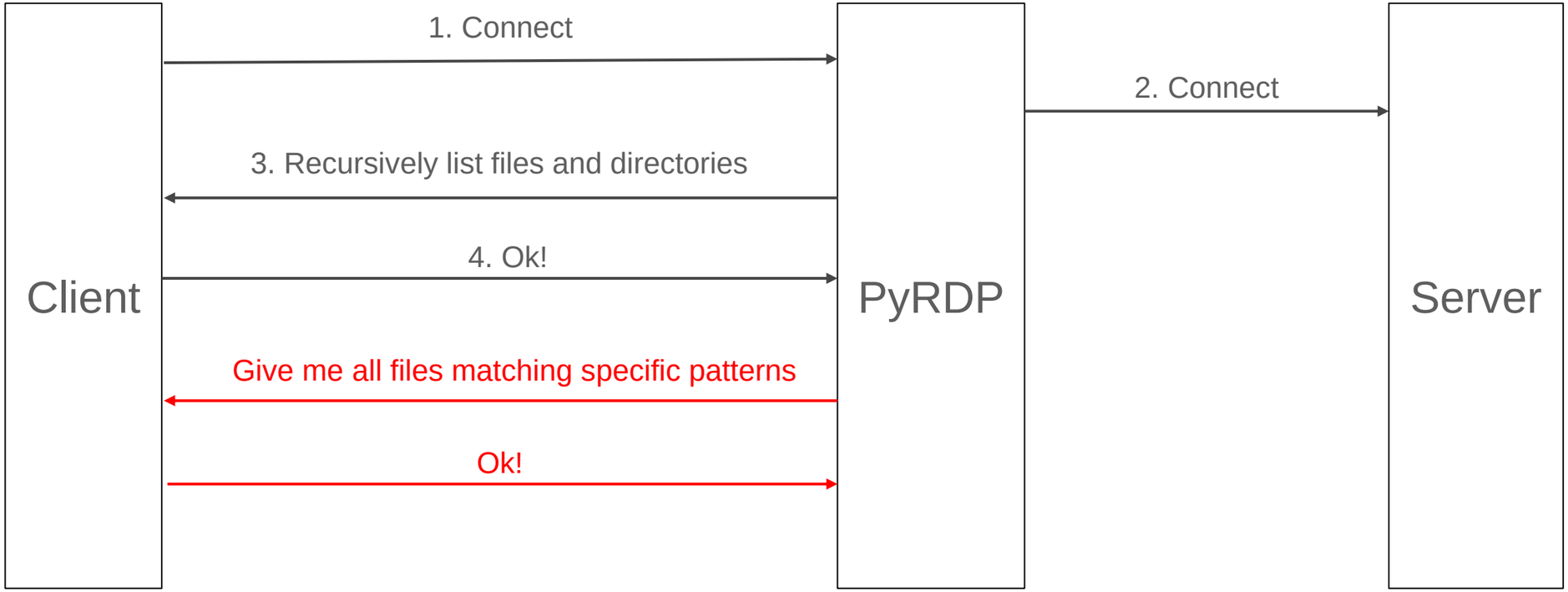
Scenarios

- Credential stuffing: accept anyone
- Non-NLA
- NLA-enabled with extracted private key

File Harvester

- Actively steal files from client mapped drives
- And previously mentioned core features

Mapped drive crawler



Offensive features

Attack Scenarios

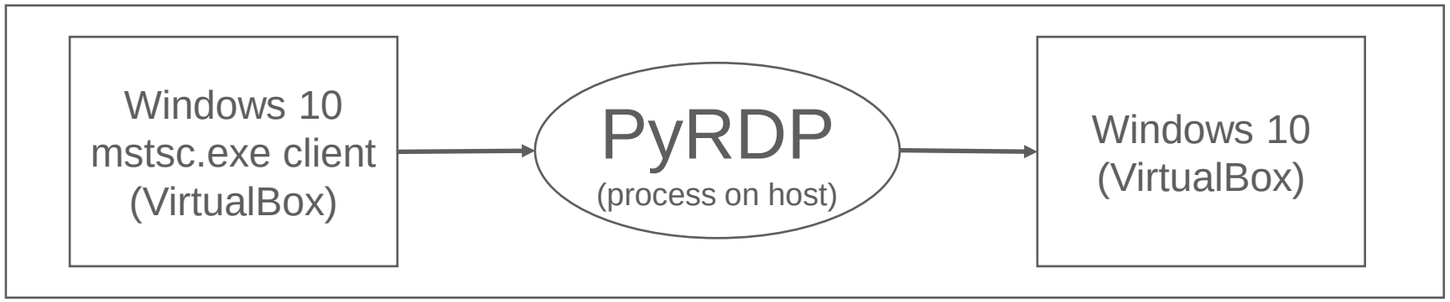
- Credential Theft
- Interactive Session Hijacking
- NLA-enabled Lure Computer

At Scale

- Transparent Proxying
  - Layer 2
  - Layer 3
- Command Injection

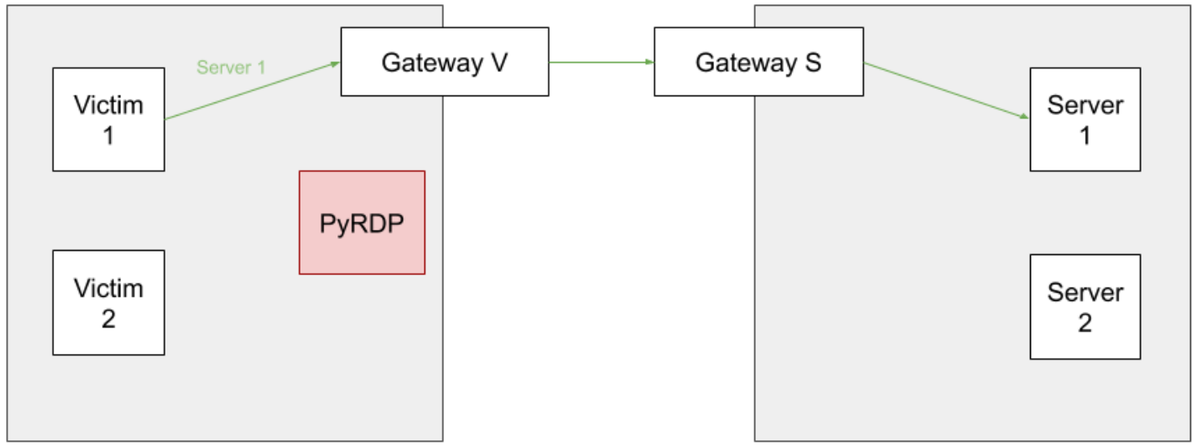
PyRDP Offensive Demo

- Session Hijacking
- Interactive filesystem exploration



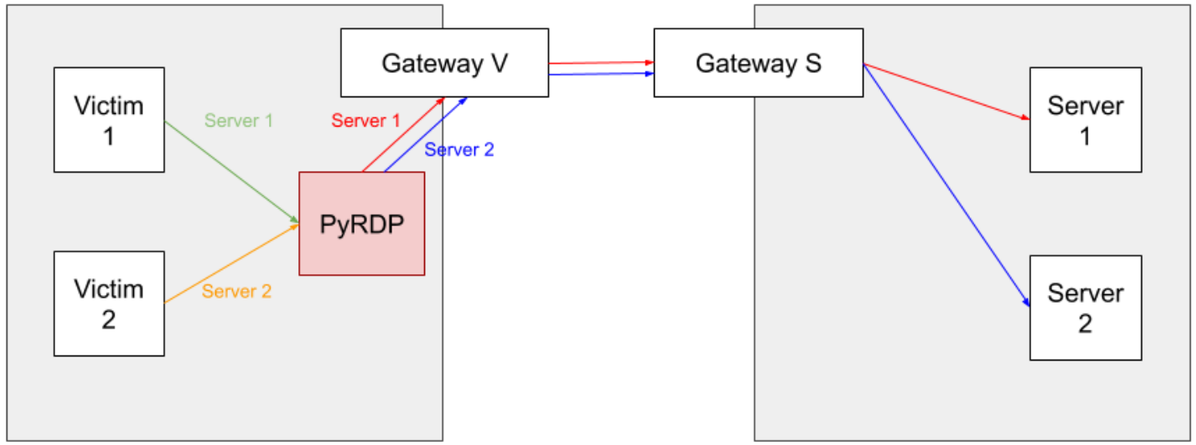
Transparent Proxying

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

New in v1.1

New in v1.1

NLA-related

- NTLMSSP hash logging
- On-the-fly redirect to non-NLA if destination enforces NLA

Collect more

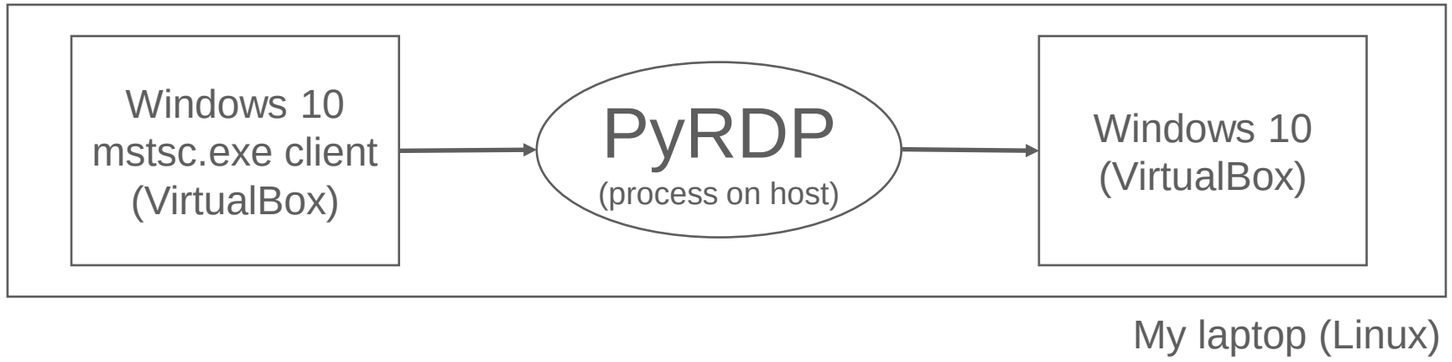
- Attempted credentials on graphical login
- Exploit attempts (protocol deviation)
- Preserve client directory structure on copy

Misc

- Video conversion is twice faster
- Bug fixes

PyRDP Collection Changes in v1.1 Demo

- Improved file transfer interception (mapped drive and clipboard)



What's next?

- PyRDP Attack RasbPi
- Resolve scalability issues around long running sessions and replays
- Research around attacks on RDP systems online

In Conclusion

Attack Limitations

- **Certificate error upon connection**
  - Certs are not CA signed
- **Mapped drives cause an additional warning dialog since Windows 10**
- **Non-NLA connections cause an additional warning dialog since Windows 10**
- **ARP poisoning is risky**

Learn More about PyRDP

Try it out, contribute, give us your feedback!

Source Code / Documentation

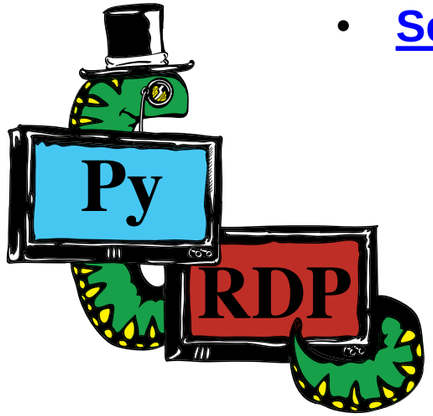
- https://github.com/GoSecure/pyrdp
- PyRDP Transparent Proxying Guide
- RDP Connection Sequence
- RDP Basic Protocol Specification

Past Presentations & Blogs

- Introduction Blog Post
- NorthSec 2019 Talk
- BlackHat Arsenal 2019
- Blog: PyRDP on Autopilot
- DerbyCon 2019 (Video)
- Defcon DemoLabs 2020
- Blog: Announcing PyRDP 1.0
- SecTor 2020 Presentation

Thanks to all PyRDP contributors!

- Alexandre Beaulieu, Francis Labelle, Émilio Gonzalez, Maxime Carbonneau, Sylvain Peyrefitte, @coolacid and more…



Contact us on Twitter

@obilodeau

@gosecure_inc