



Attacking the Remote Desktop Protocol

A Hands-On Workshop

Olivier Bilodeau (@obilodeau), GoSecure





Olivier Bilodeau

Cybersecurity Research Lead at GoSecure

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





Agenda



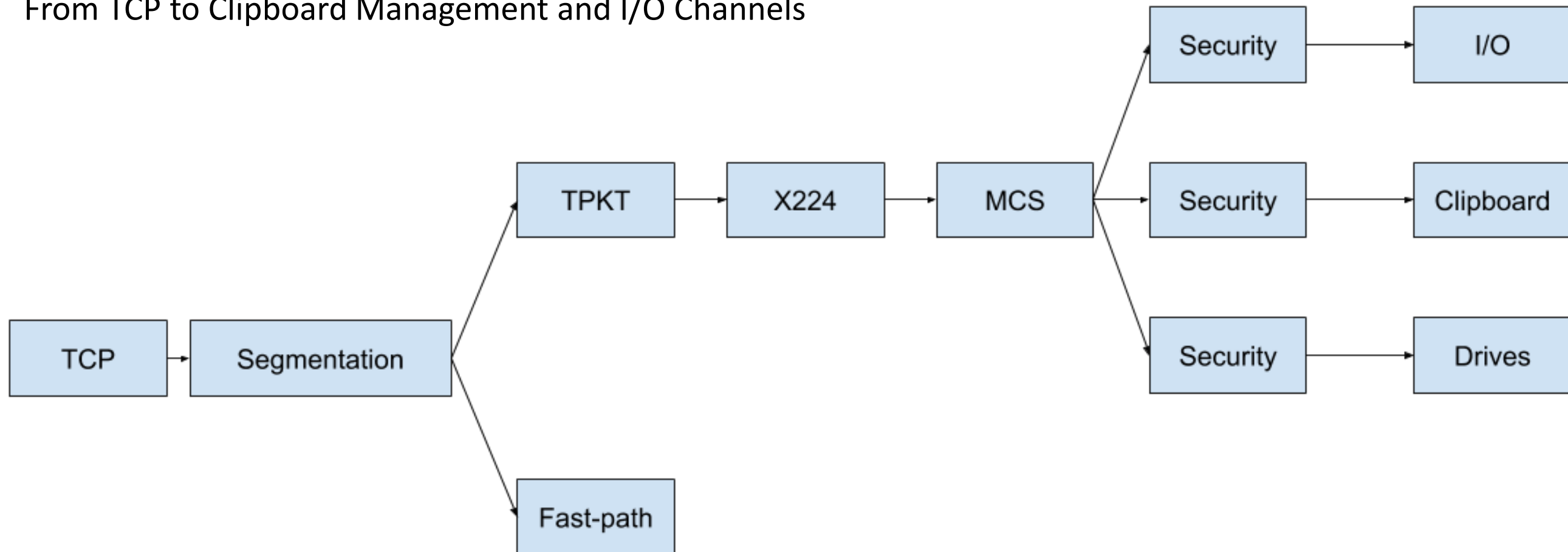
- Introduction to RDP
- What is the PyRDP attack tool?
- Interactive Demos
 - Perform an eavesdropping monster-in-the-middle attack
 - Watch previously recorded sessions
 - Use the interactive player to crawl client filesystem
 - Perform a hijacking monster-in-the-middle attack
 - Extract private RDP keys from Windows and use them in PyRDP

Introduction to RDP



RDP Layers

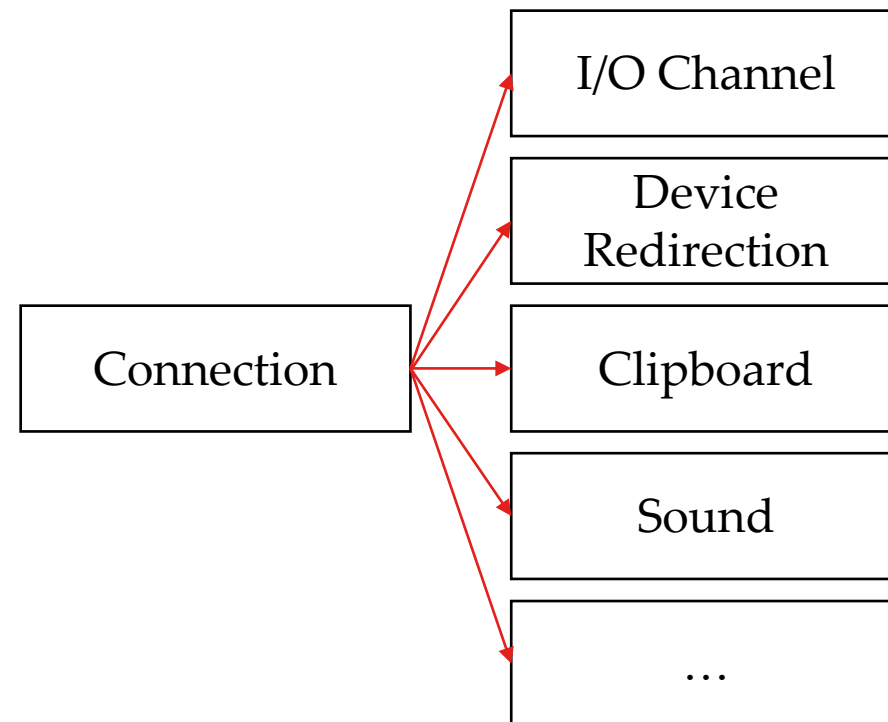
From TCP to Clipboard Management and I/O Channels





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

Lab 1

Install the tool

Follow instructions here:

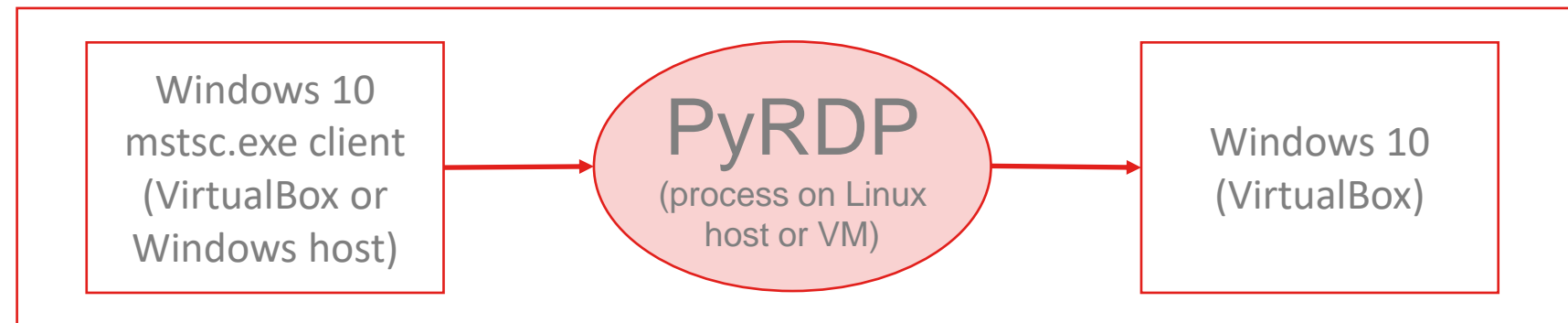
<https://github.com/GoSecure/pyrdp#from-git-source>



Lab 2

Perform an Eavesdropping MITM Attack

- Credentials, keystrokes and clipboard interception
- Take a look at the logs



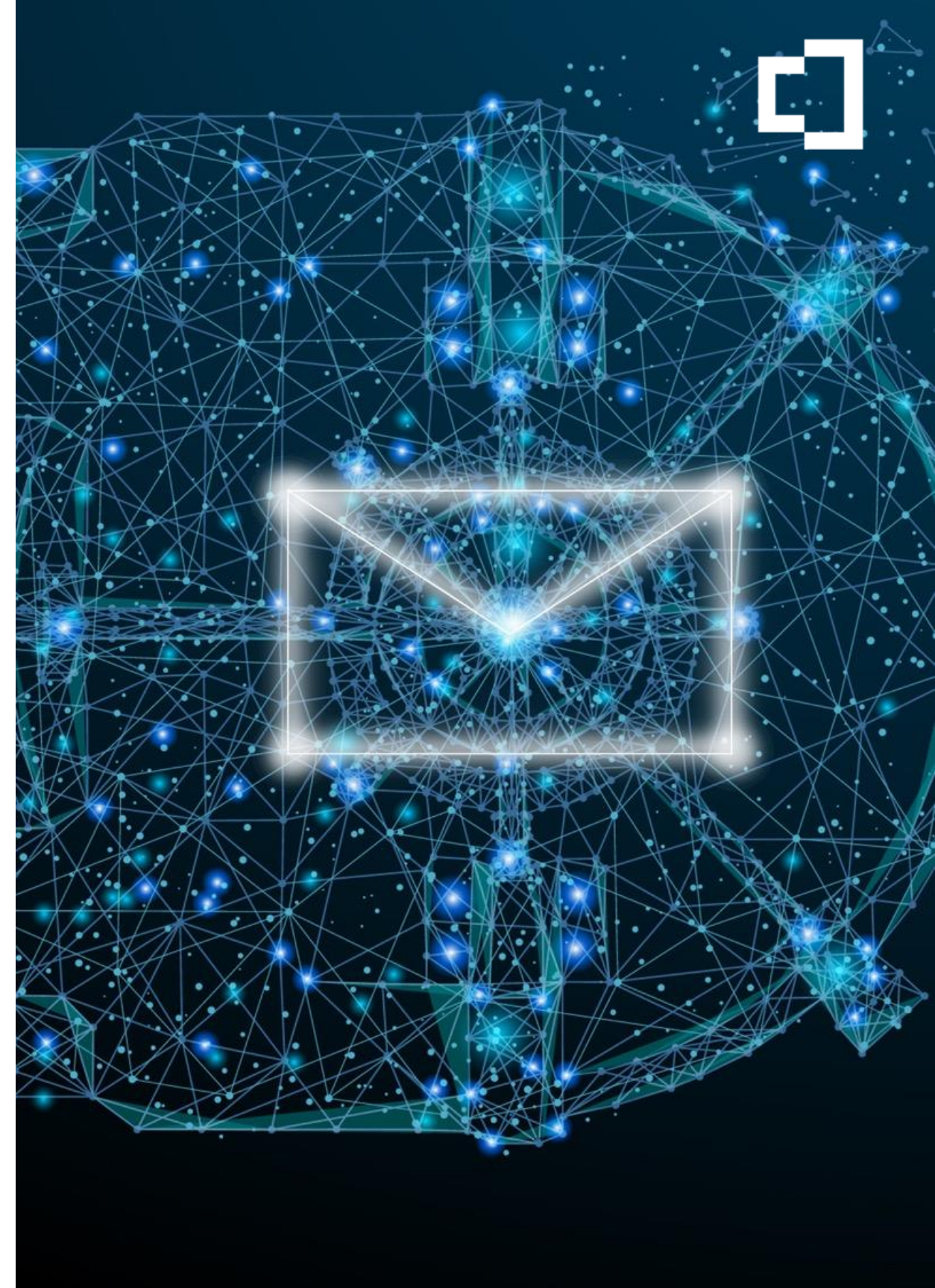
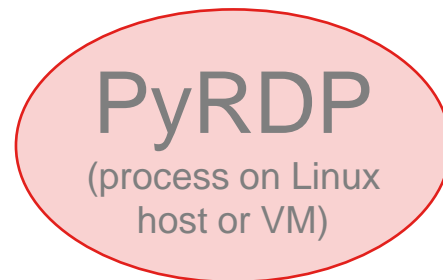
My laptop (Linux)



Lab 3

Use PyRDP Player to View Past Sessions

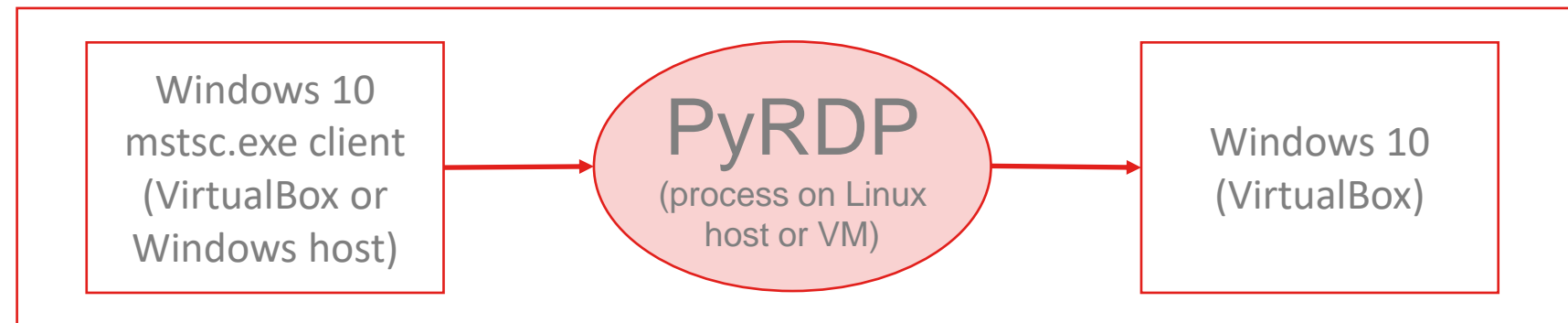
- Things that were collected



Lab 4

Use the Interactive Player

- Crawl client-side filesystem
- See screen, keystrokes, clipboard stealer in real-time



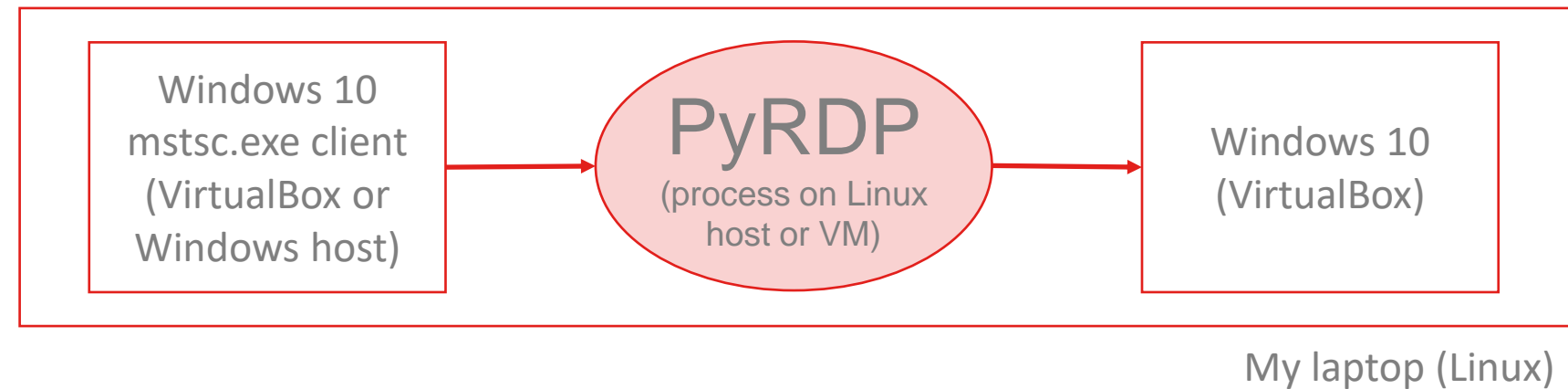
My laptop (Linux)



Lab 5

Use the Interactive Player

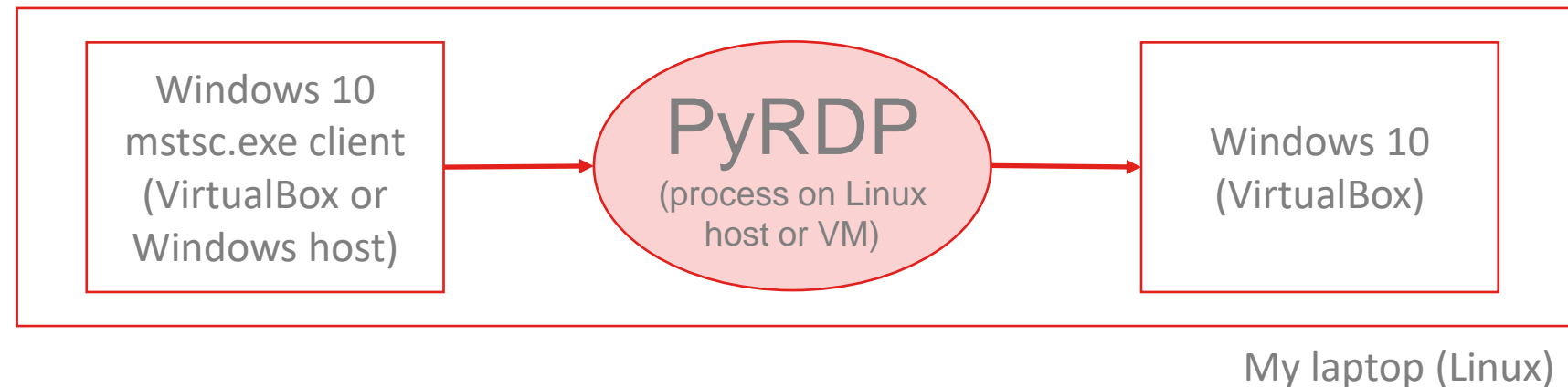
- Hijack the client's connection
- Run a payload



Lab 6

Attacks on Network Level Authentication

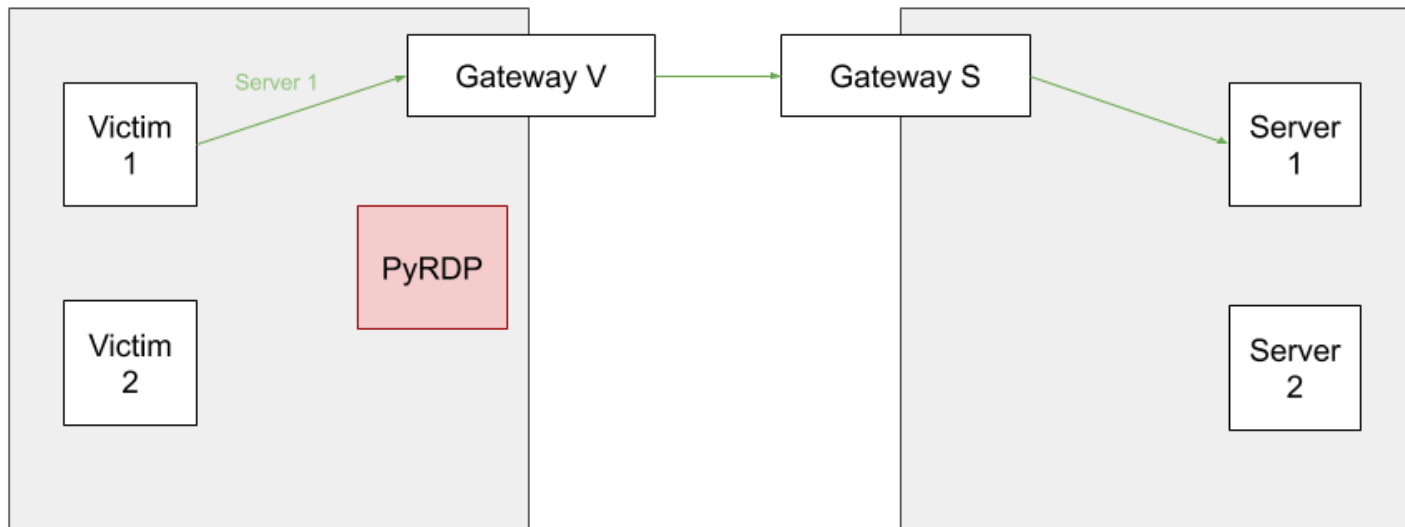
- Extract the private certificate
- Install it on host
- Perform MITM with CredSSP and certificate and private key





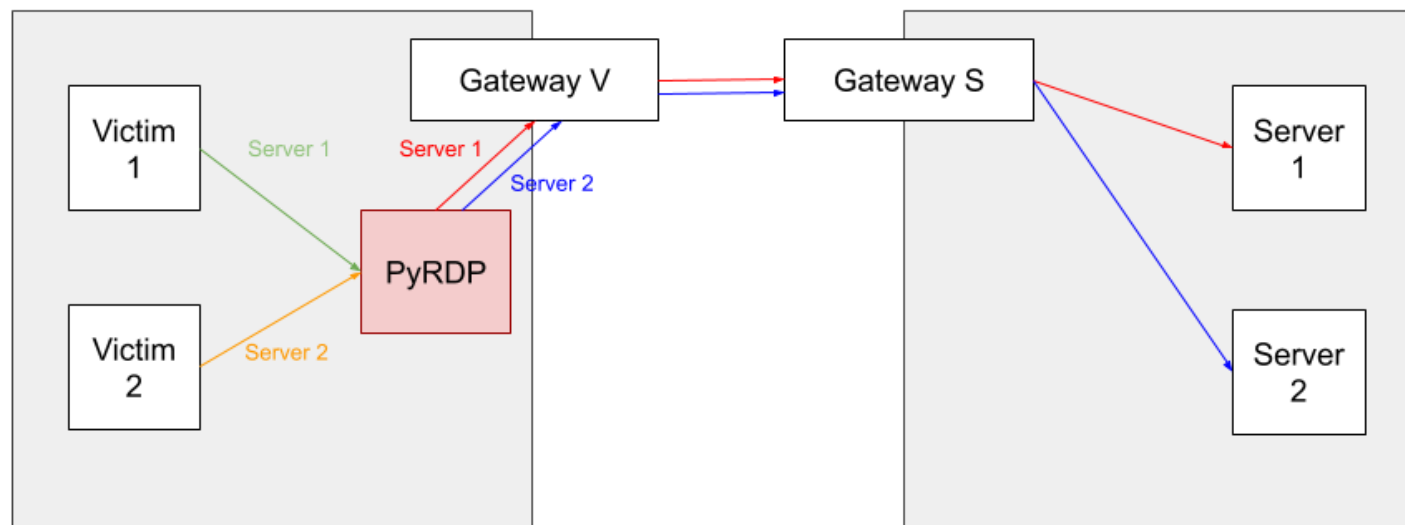
Transparent Proxying

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

Wrapping Up

Attack Limitations



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

- **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

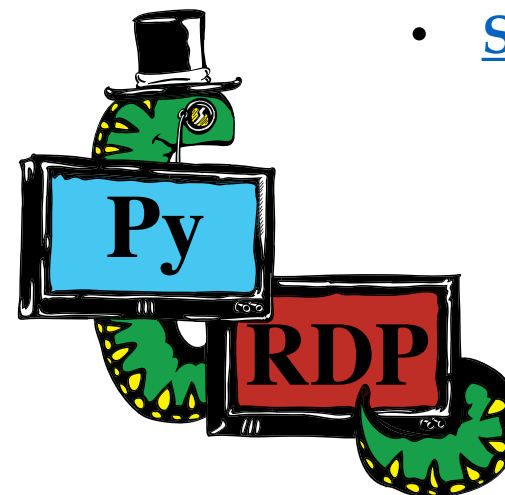
Try it out, contribute, give us your feedback!

Source Code / Documentation

- <https://github.com/GoSecure/pyrdp>
- [PyRDP Transparent Proxying Guide](#)
- [RDP Connection Sequence](#)
- [RDP Basic Protocol Specification](#)
- [Certificate Extraction for NLA](#)

Thanks to all PyRDP contributors!

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



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](#)

Contact us on Twitter
@obilodeau
@gosecure_inc

#gosec @gosec2021