

# Collection with PowerSploit

---

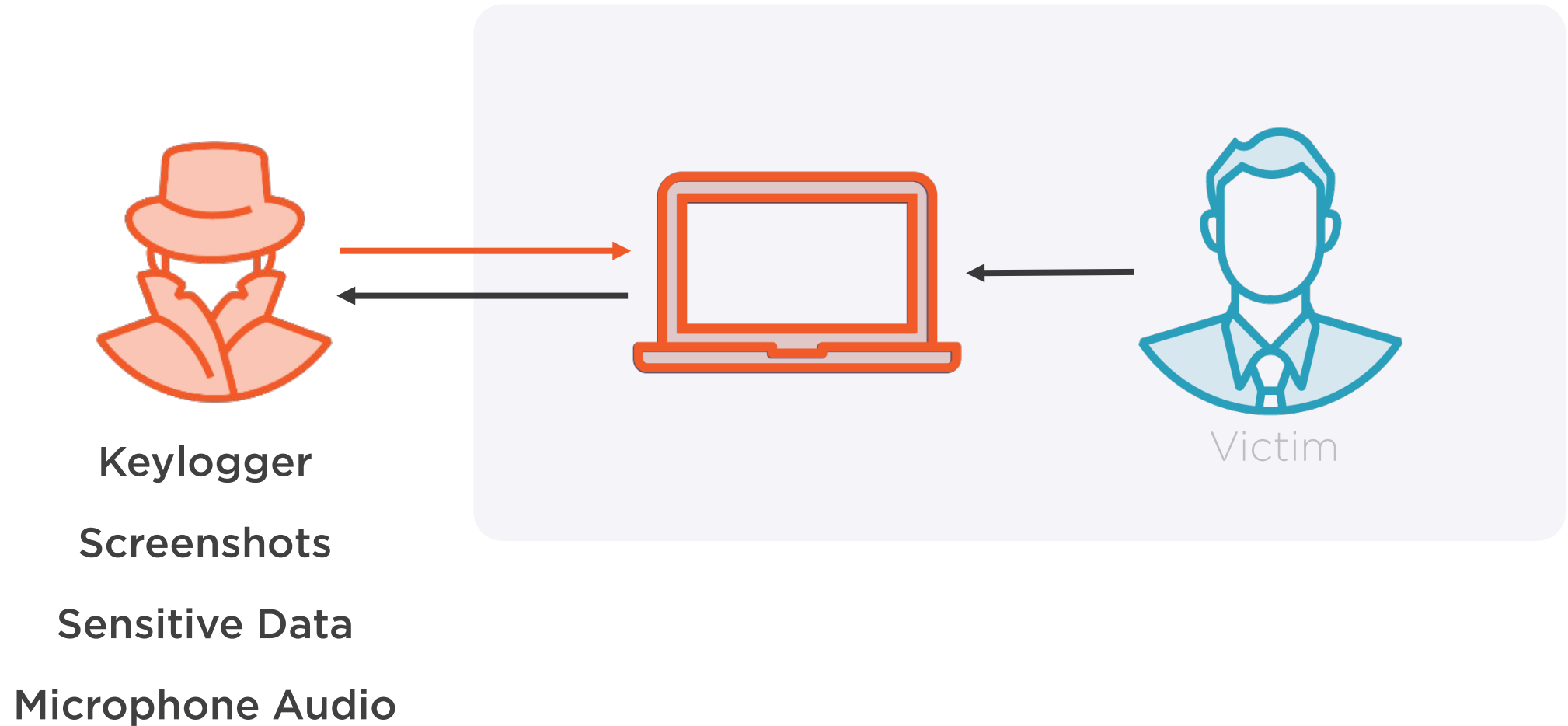


**Ricardo Reimao**

CYBER SECURITY CONSULTANT



# Collecting Sensitive Data



# PowerSploit



# PowerSploit

Author: Matt Graeber  
@mattifestation

---

PowerSploit is a collection of Microsoft PowerShell modules that can be used to aid penetration testers during all phases of an assessment.



# PowerSploit

Open source tool (GNU v3.0)

<https://github.com/PowerShellMafia/PowerSploit>

Full framework for red teaming

Already comes in most of Command and Control tools

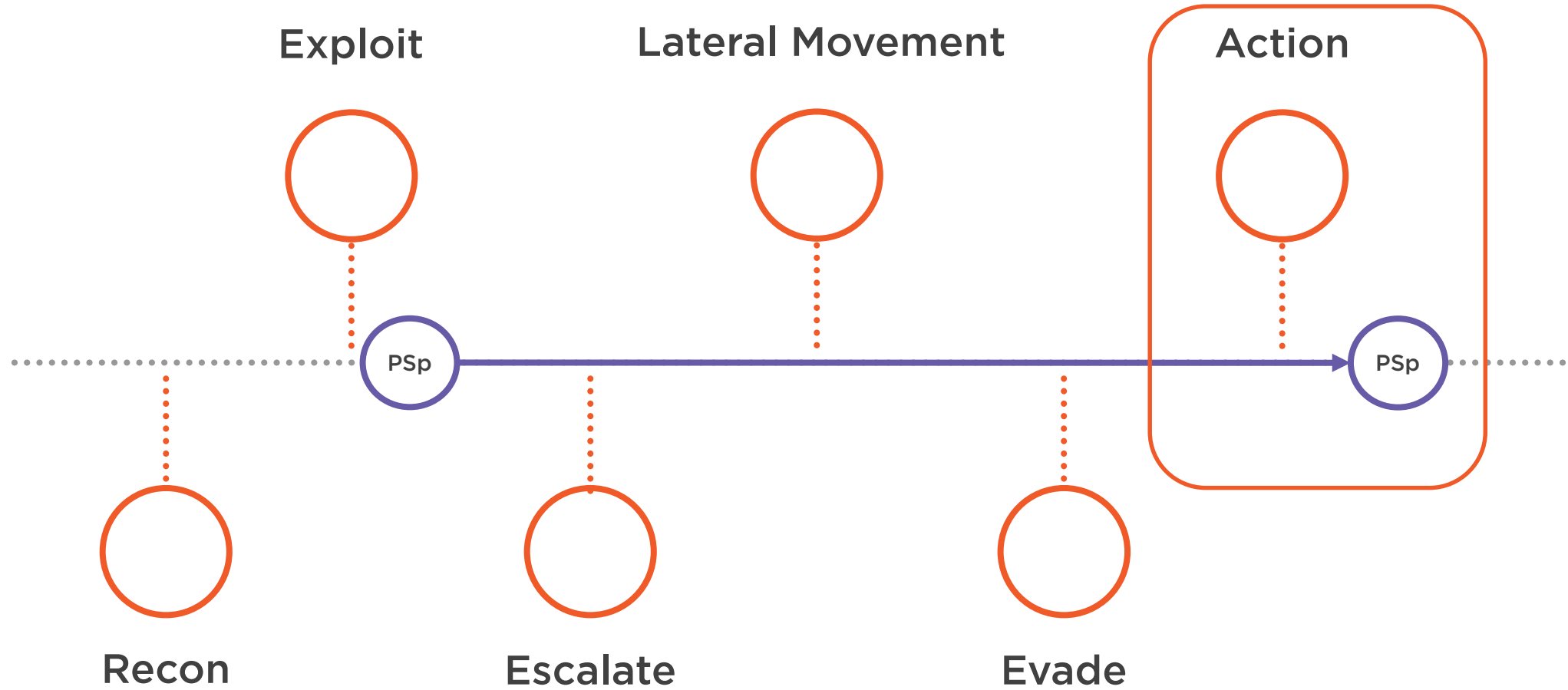
- Covenant, Pupy, etc.

Automate collection of sensitive data

- Sensitive files
- Microphone audio
- Screenshots
- Keylogger



# Kill Chain



# MITRE ATT&CK

## Tactics

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact



# MITRE ATT&CK

## Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact



# MITRE ATT&CK

## Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

**Collection**

Command & Control

Exfiltration

Impact

T1123:

Audio Capture

T1056:

Input Capture

T1113:

Screen Capture

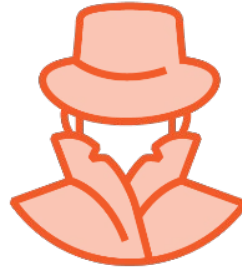
T1039:

Data from Network Shared Drive



# Staying Legal

Stealing data without authorization is **ILLEGAL** in most countries



Letter of engagement, detailing dates and scope of what will be executed

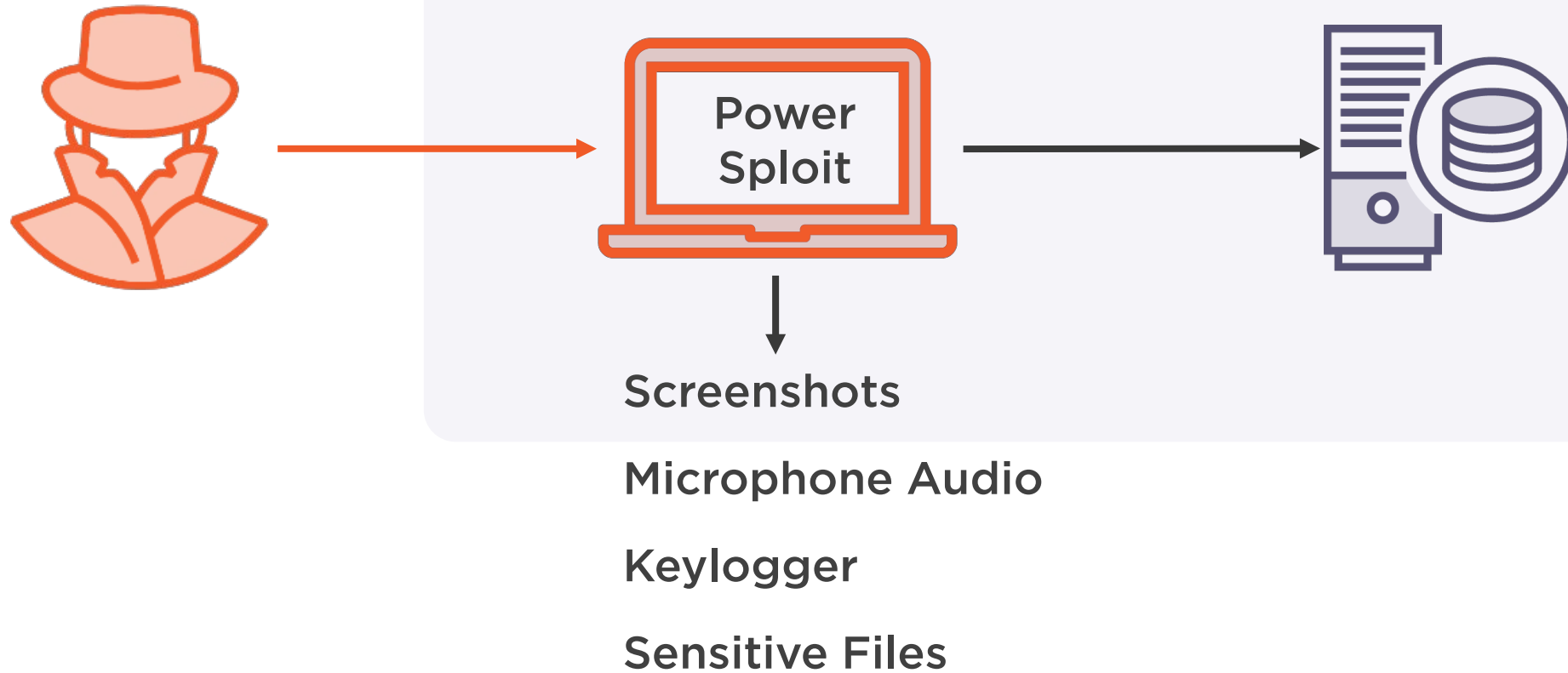
Formal document, signed by the client, authorizing the types of attack you may perform

Always consult the client before any attack that may impact the network



# Attack Explanation

Client network



# Anti-Virus Detection

## Anti-Virus Bypassing

- **Several techniques**
- **Script obfuscation**  
Course: “Defense Evasion with Invoke-Obfuscation”
- **Always test in a cloned environment**
- **Preferred method, usually do not generate logs**

## Anti-Virus Disabling

- **Easiest way**
- **Disabling all detection mechanisms**
  - > Anti-virus and HIPS
  - > End point protection
  - > Windows defender
- **Usually generate logs to SIEM**
- **Suspicious activity**



# Prerequisites

## Small Lab Environment

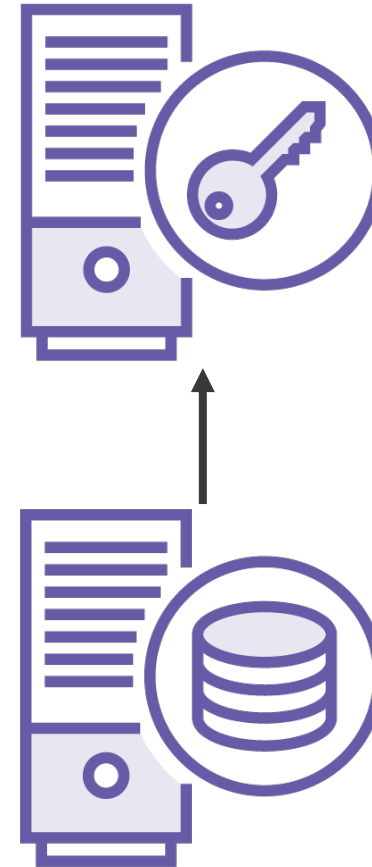
### Windows 2016 Domain

#### Including:

- Windows 2016 domain controller
- Windows 2016 server

#### Alternative:

- Windows virtual machine



# Demo Place Holder

1. Installation Tips and Tricks
2. First use instructions and common usage syntax
3. Use of main features on live targets or in live environment



# Other PowerSploit Features

**Reconnaissance**

**Code  
Execution**

**Privilege  
Escalation**

**Persistence**

**Anti-virus  
Bypass**

**Exfiltration**

**Covers 23 tactics from the Mitre Att&ck Framework**



# More Information

## Official Documentation

Several other capabilities

<https://github.com/PowerShellMafia/PowerSploit>

## PowerSploit Course

“Getting Started with PowerSploit”

<https://pluralsight.com/courses/getting-started-powersploit>

## Anti-virus Evasion

“Defense Evasion with Invoke-Obfuscation”

<https://pluralsight.com/courses/defense-evasion-invoke-obfuscation/>

## Remediation

Abnormal user behaviour detection

Network traffic behaviour detection



# Thank you!



**Ricardo Reimao**  
Cyber security consultant

