

# Discovery with ADRecon

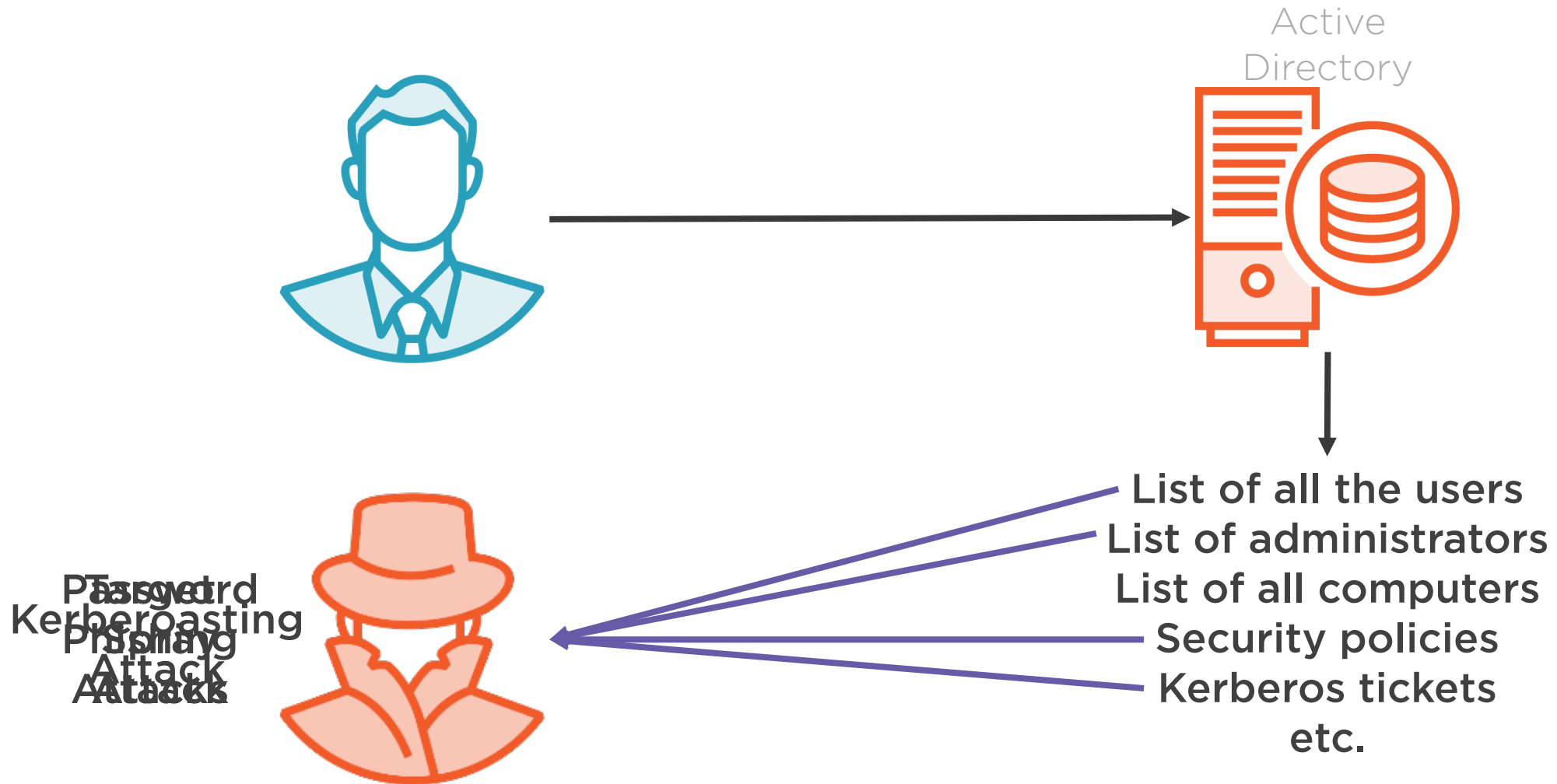
---



**Ricardo Reimao**  
CYBER SECURITY CONSULTANT



# Information Gathering from Active Directory



# ADRecon



# ADRecon

Author: Prashant Mahajan  
@prashant3535

---

A tool which gathers information about the Active Directory and generates a report which can provide a holistic picture of the current state of the target AD environment.



# ADRecon

Open source tool (GNU v3.0)

<https://github.com/adrecon/ADRecon>

Version for Azure Active Directory

<https://github.com/adrecon/AzureADRecon>

Usually not detected by anti-virus

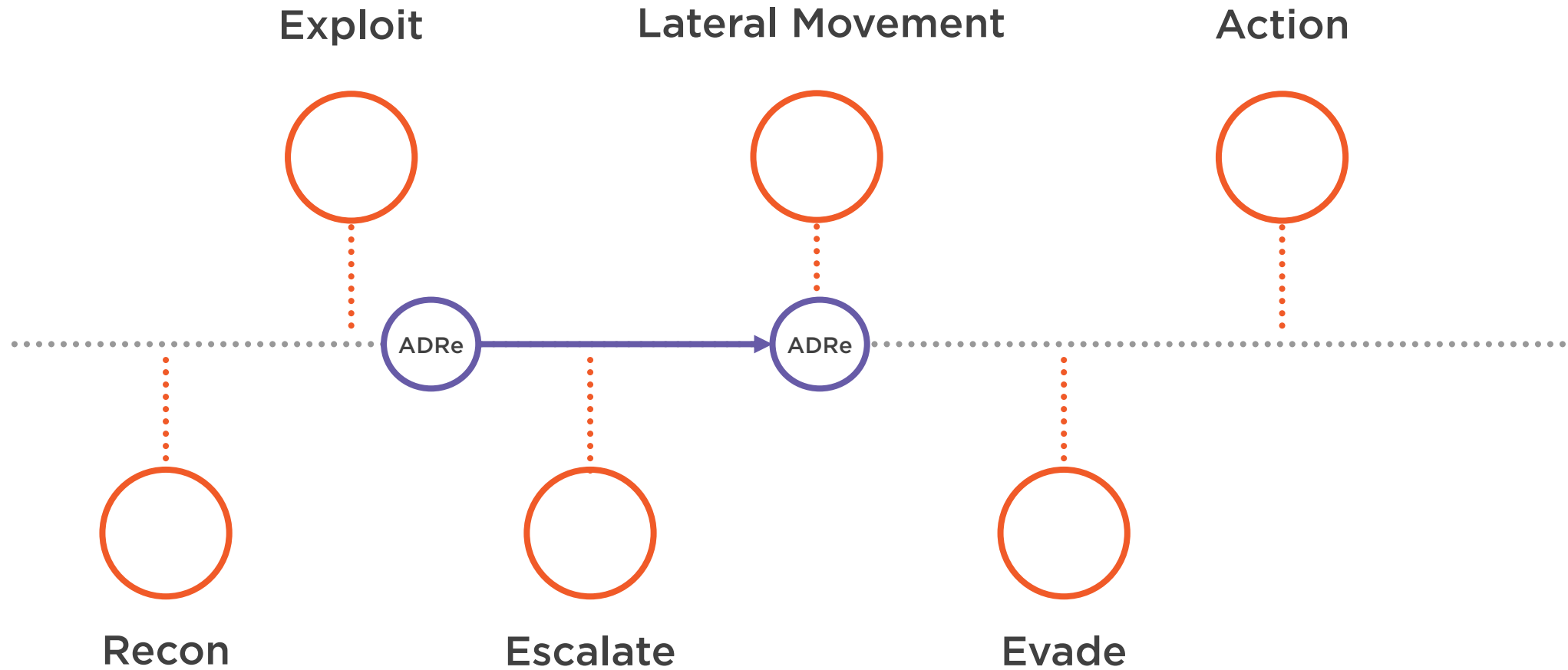
Does not require admin privileges

Gathers several interesting information

- Users
- Service accounts
- Security policies
- Computers
- etc.



# 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

T1201:

Password Policy Discovery

T1069 :

Permission Groups Discovery

T1087:

Account Discovery



# MITRE ATT&CK

## Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

**Credential Access**

Discovery

Lateral Movement

**Collection**

Command & Control

Exfiltration

Impact

T1558:

Steal or Forge Kerberos Tickets

T1558.003:

Kerberoasting

T1213:

Data from Information Repositories



# Staying Legal

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



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

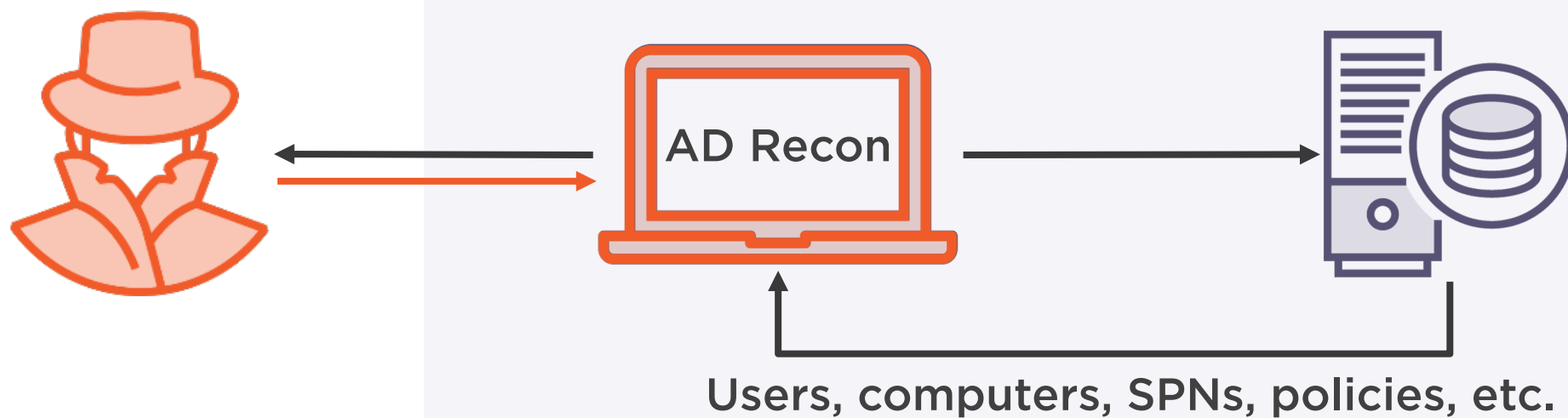
Formal document, signed by the client, authorizing the types of attack you may perform

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



# Attack Explanation

Client network



# Prerequisites

## Small Lab Environment

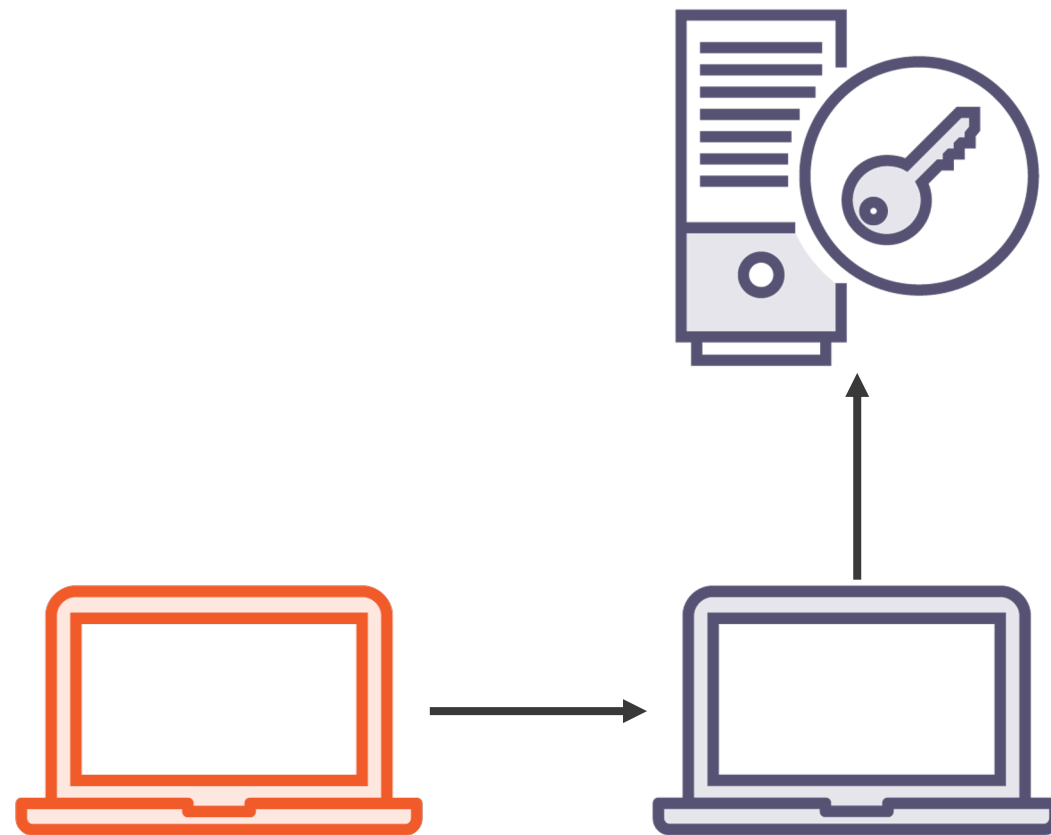
### Windows 2016 Domain

#### Including:

- Windows 2016 domain controller
- Windows workstation

#### Additional:

- Attacker machine: Kali Linux



# 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



# More Information

## Official Documentation

Few other capabilities

<https://github.com/adrecon/ADRecon>

<https://github.com/adrecon/AzureADRecon>

## Author's talk on the tool

OWASP Conference

<https://www.youtube.com/watch?v=hNwXd54O8tU>

## Password Cracking Tools

Hashcat

<https://hashcat.net/>

John-The-Ripper

<https://github.com/magnumripper/JohnTheRipper>

## Remediation

Monitor high traffic of AD requests

Use complex passwords for service accounts



# Thank you!



**Ricardo Reimao**  
Cyber security consultant

