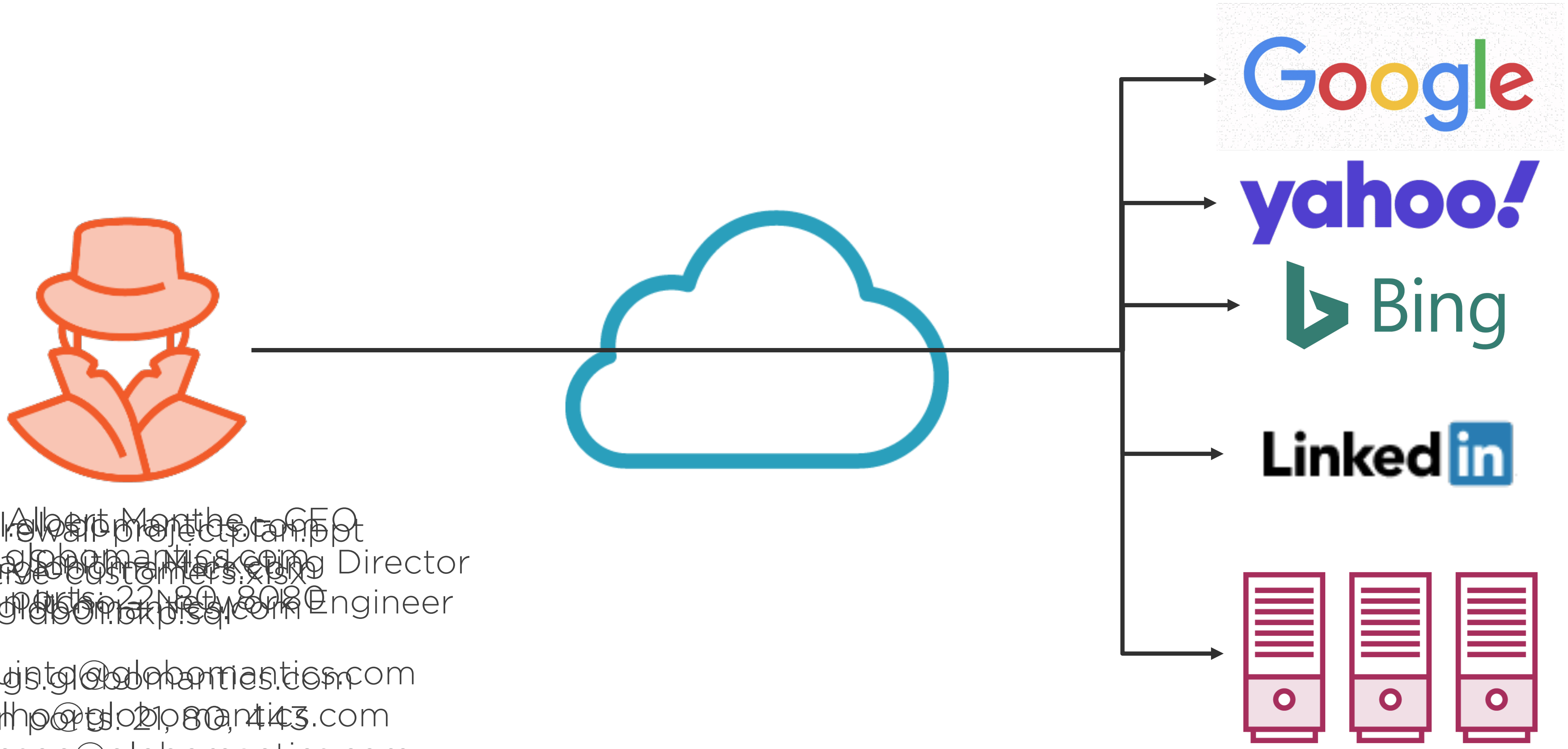
Technical Information Gathering with TheHarvester

Ricardo Reimao
CYBER SECURITY CONSULTANT

Collecting Technical Information

Target: globomantics.com



Albert Monthe - CEO
Patricia Smith - Marketing Director
William Jones - Network Engineer

mail.globomantics.com
dev.globomantics.com
vpn.globomantics.com
hr.globomantics.com

meetings.globomantics.com

dmz-firewall-projectplan.ppt
active-customers.xlsx
db01.bkp.sql

open ports: 22, 80, 8080

open ports: 21, 80, 443

robert.quinto@globomantics.com
oscar.alho@globomantics.com
jeff.smithson@globomantics.com

theHarvester

theHarvester

Publisher: Christian Martorella (@laramies)
http://www.edge-security.com/

theHarvester is a tool for open source intelligence gathering and helping to determine a company's external threat landscape on the internet. The tool gathers emails, names, subdomains, IPs, and URLs using multiple public data sources theHarvester

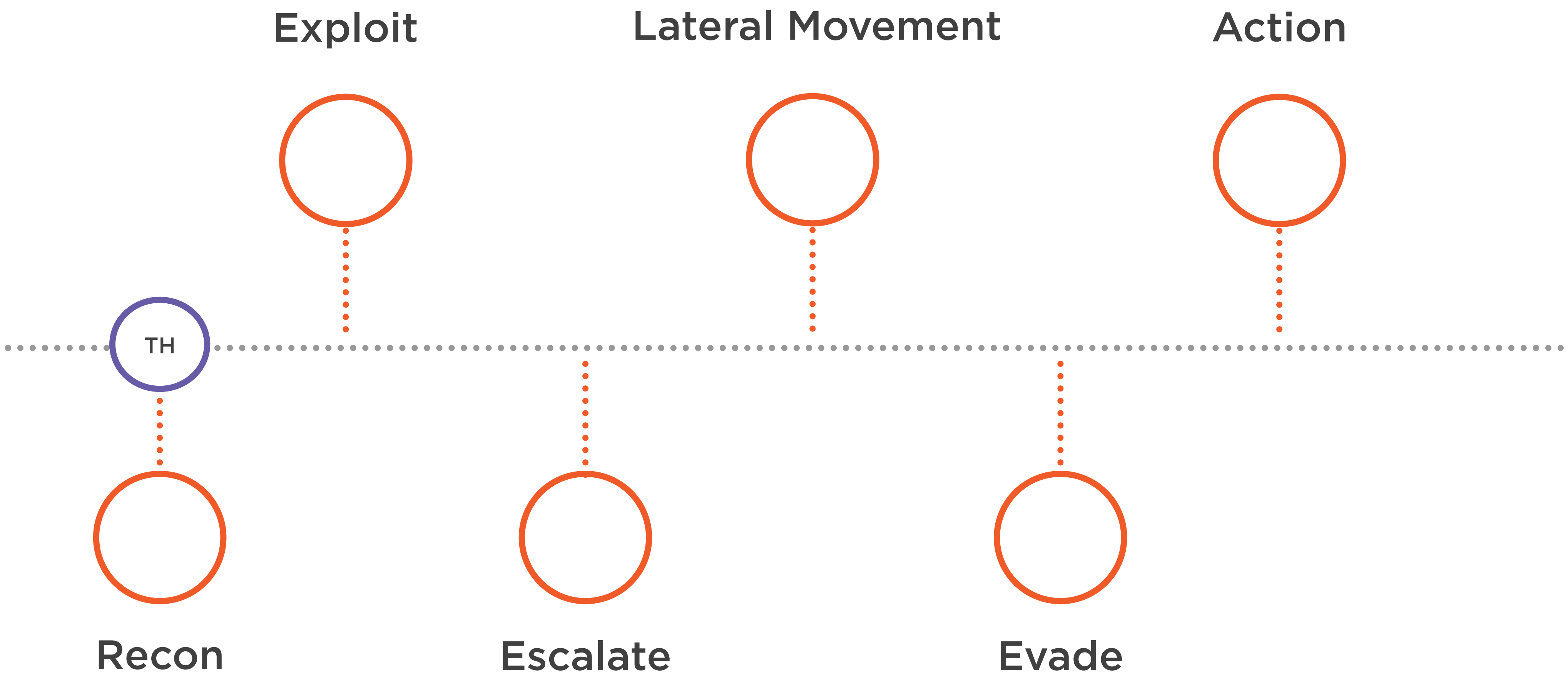
Open source tool
https://github.com/laramies/theHarvester

Pre-installed on Kali Linux

Performs non-intrusive information gathering (as well as intrusive)

- DNS names
- IP addresses
- Email addresses
- Linkedin profiles

Kill Chain



Exploit

Lateral Movement

Action

TH

Recon

Escalate

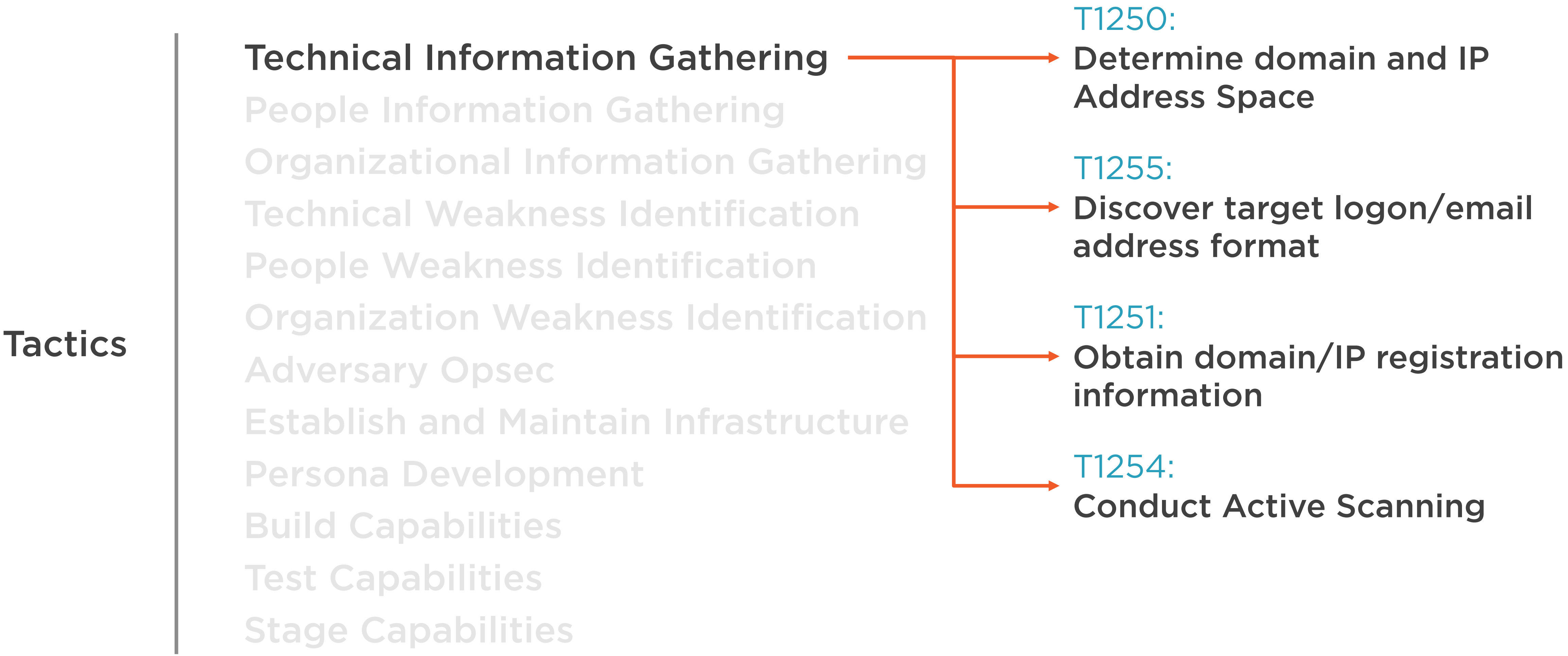
Evade

MITRE PRE-ATT&CK

Tactics

- Technical Information Gathering
- People Information Gathering
- Organizational Information Gathering
- Technical Weakness Identification
- People Weakness Identification
- Organization Weakness Identification
- Adversary Opsec
- Establish and Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

MITRE PRE-ATT&CK



Tactics

- **Technical Information Gathering**
- People Information Gathering
- Organizational Information Gathering
- Technical Weakness Identification
- People Weakness Identification
- Organization Weakness Identification
- Adversary Opsec
- Establish and Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

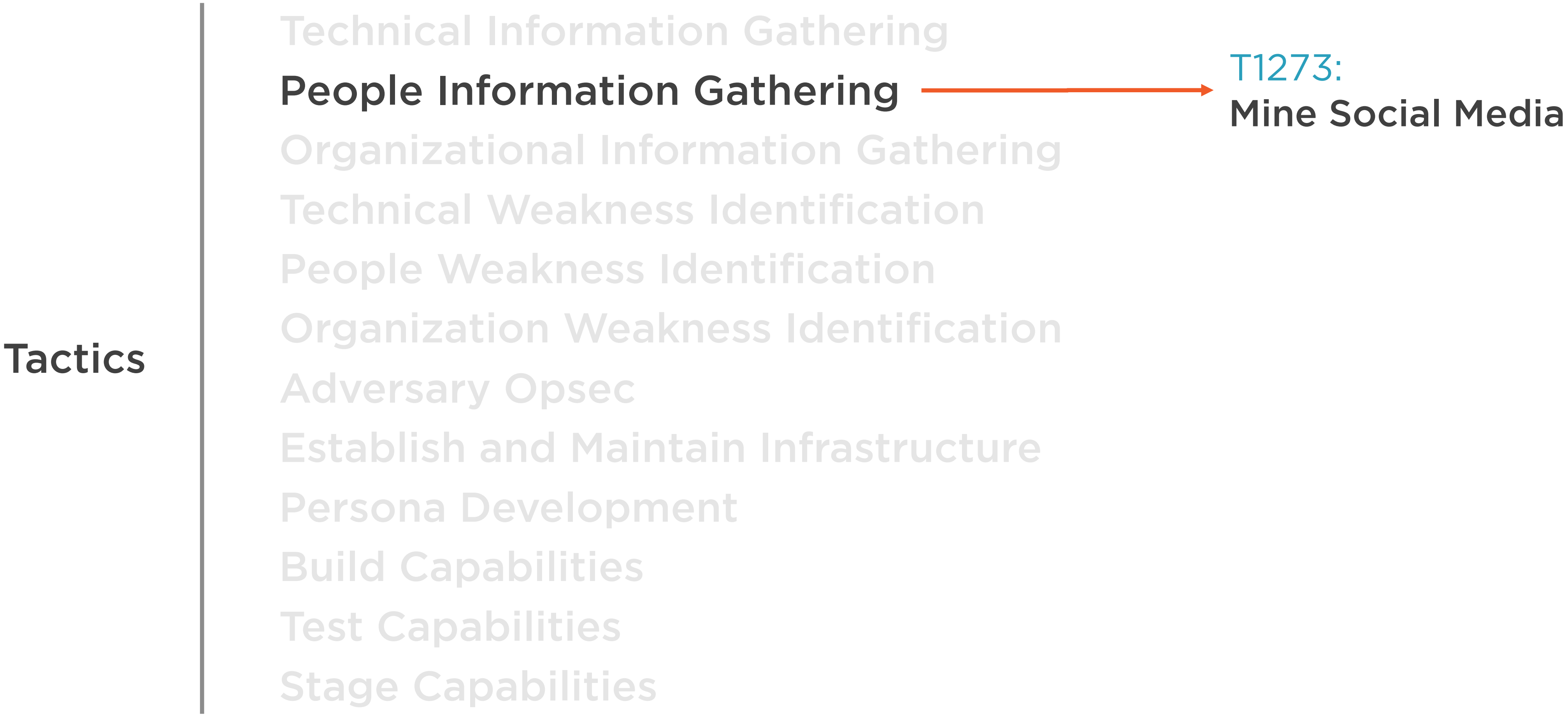
T1250:
Determine domain and IP Address Space

T1255:
Discover target logon/email address format

T1251:
Obtain domain/IP registration information

T1254:
Conduct Active Scanning

MITRE PRE-ATT&CK



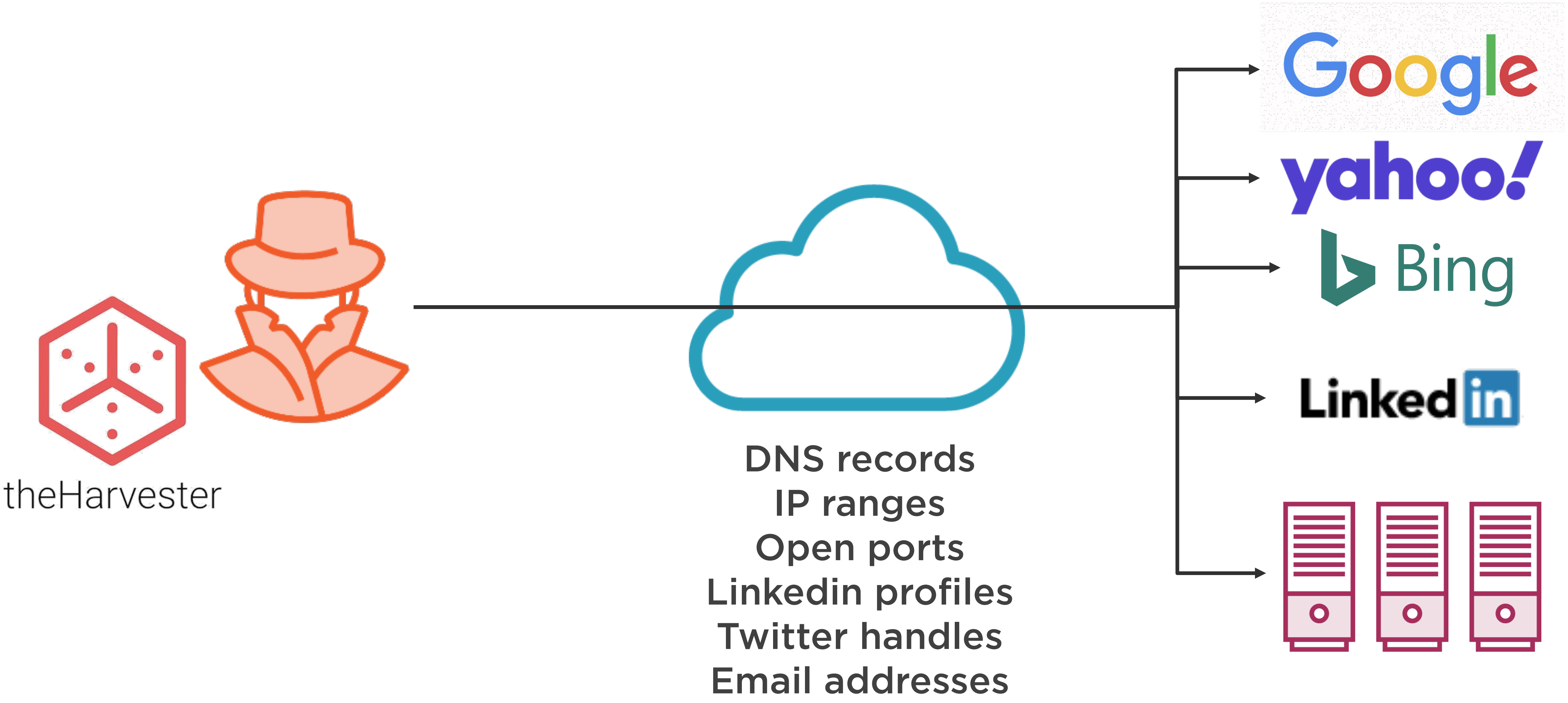
Tactics

- Technical Information Gathering
- People Information Gathering
- Organizational Information Gathering
- Technical Weakness Identification
- People Weakness Identification
- Organization Weakness Identification
- Adversary Opsec
- Establish and Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

People Information Gathering → T1273: Mine Social Media

Attack Explanation

Target: globomantics.com



DNS records
IP ranges
Open ports
Linkedin profiles
Twitter handles
Email addresses

Prerequisites

KALI

BY OFFENSIVE SECURITY

Kali Linux

Version: 2020.2 or superior

Up to date:

```
$ apt-get update
$ apt-get upgrade
```

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

More About the Tool

- Can be easily expanded
- Can be integrated with other tools
- Can be used for automation

https://github.com/laramies/theHarvester

Protecting Your Company

- Perform constant scans to understand which data is externally available
- Reduce your sensitive information footprint
  - DNS records
  - Email addresses
  - Old websites

Thank you!

Ricardo Reimao
Cyber security consultant