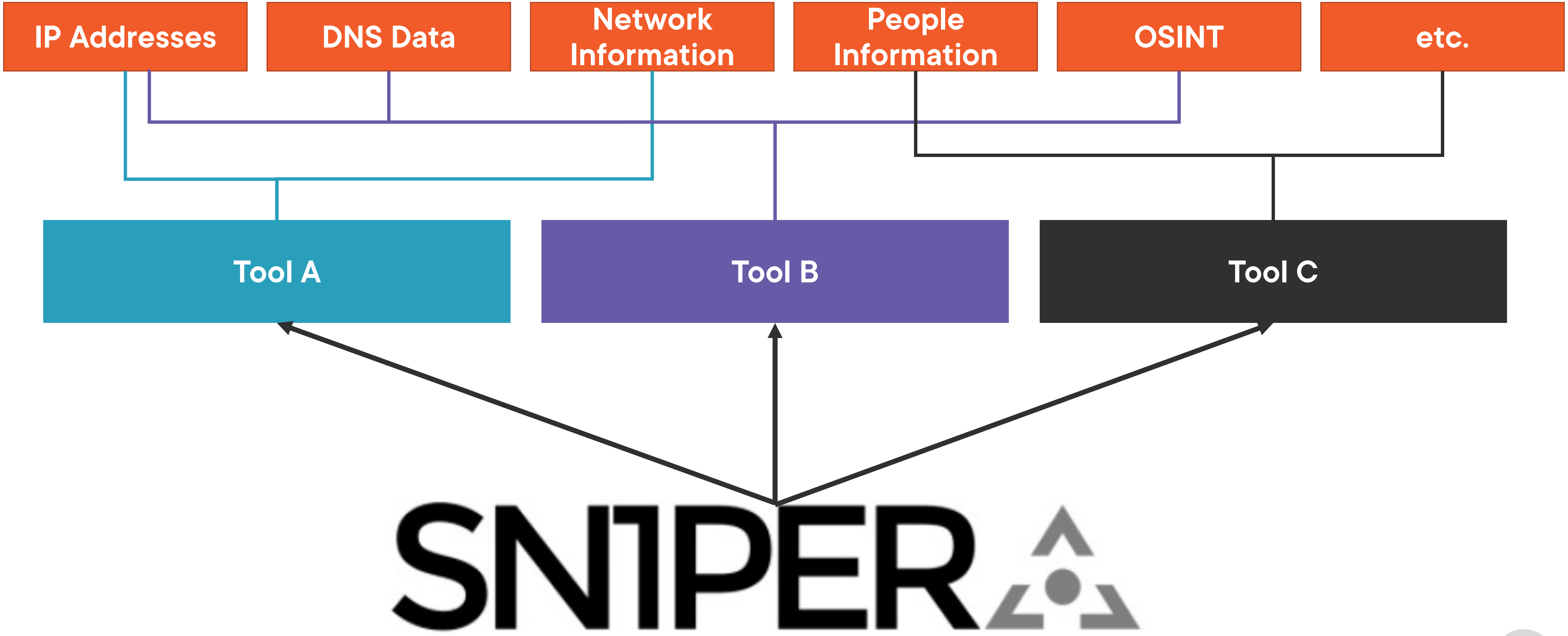
Reconnaissance with Sn1per

Ricardo Reimao, OSCP, CISSP

Cybersecurity Consultant

Automating Reconnaissance



IP Addresses

DNS Data

Network Information

People Information

OSINT

etc.

Tool A

Tool B

Tool C

SN1PER

SN1PER

Creator: Xero Security
https://xerosecurity.com/

A tool for discovering attack surface and prioritizing risks.
It automates the most common reconnaissance techniques.

Community Edition (FREE)
https://github.com/1N3/Sn1per

One of the most complete tools for reconnaissance

Leverage several of the most used recon scripts (NMap, theHarverster, WafWoof, etc.)

Recommended for advanced red teamers

Recon Data

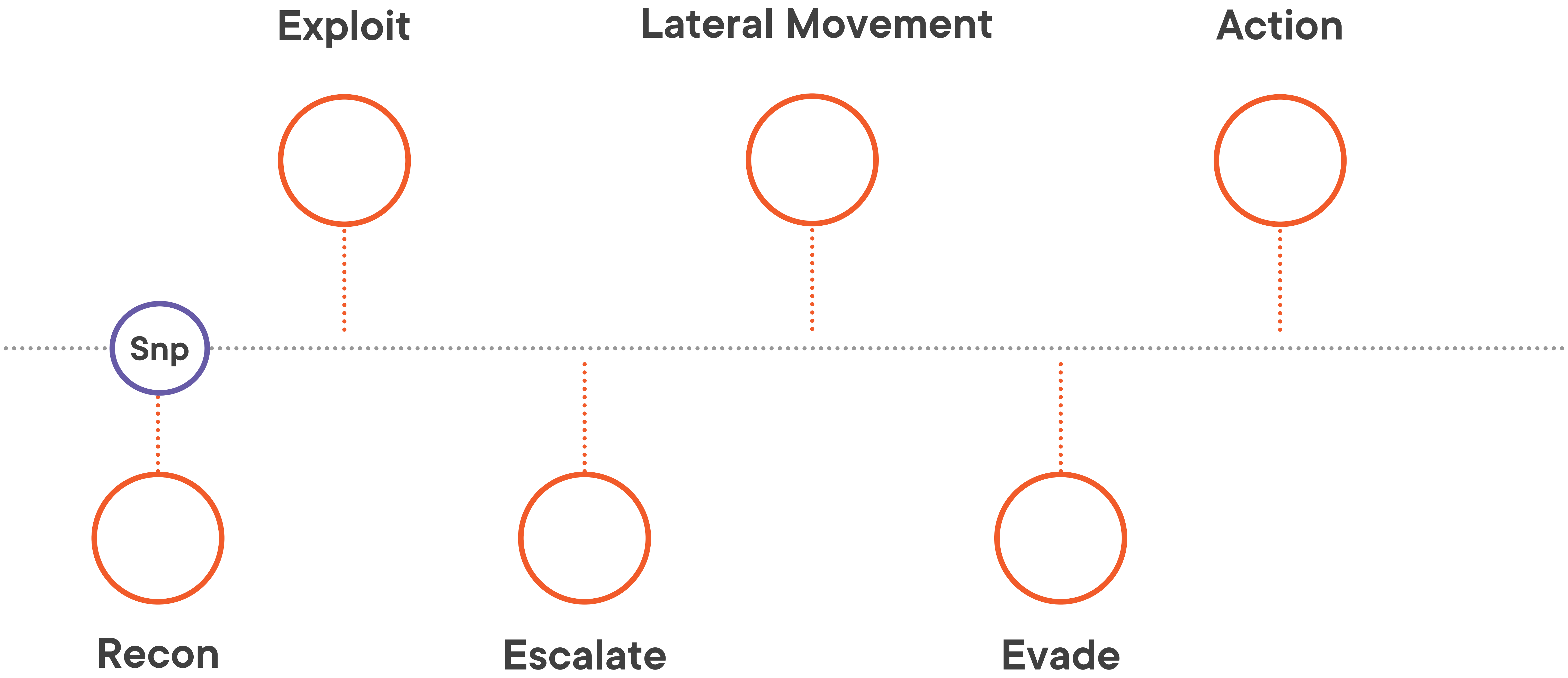
Passive Information Gathering

WHOIS records
DNS queries
OSINT searches
Social media searches
Search engine recon
etc.

Active Information Gathering

NMAP Port scans
Vulnerability scans
Web application probing
etc.

Kill Chain



MITRE ATT&CK

Tactics

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

MITRE ATT&CK

Tactics

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

T1595:
Active Scanning

T1592:
Gather Victim Host Information

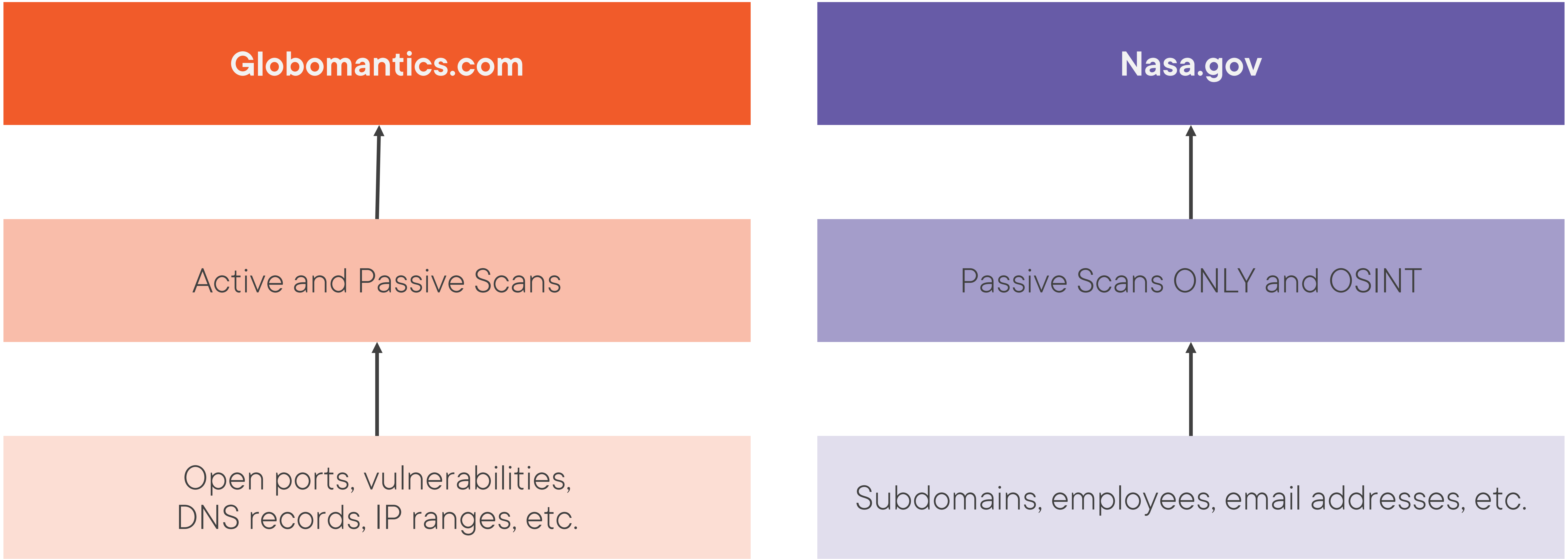
T1590:
Gather Victim Network Information

T1596:
Search Open Source Technical Databases

T1593:
Search Open Source Websites/Domains

T1589:
Gather Victim Identity Information

Demo Explanation



Globomantics.com

Active and Passive Scans

Open ports, vulnerabilities,
DNS records, IP ranges, etc.

Nasa.gov

Passive Scans ONLY and OSINT

Subdomains, employees, email addresses, etc.

Prerequisites

Kali Linux

… or any other Linux distribution

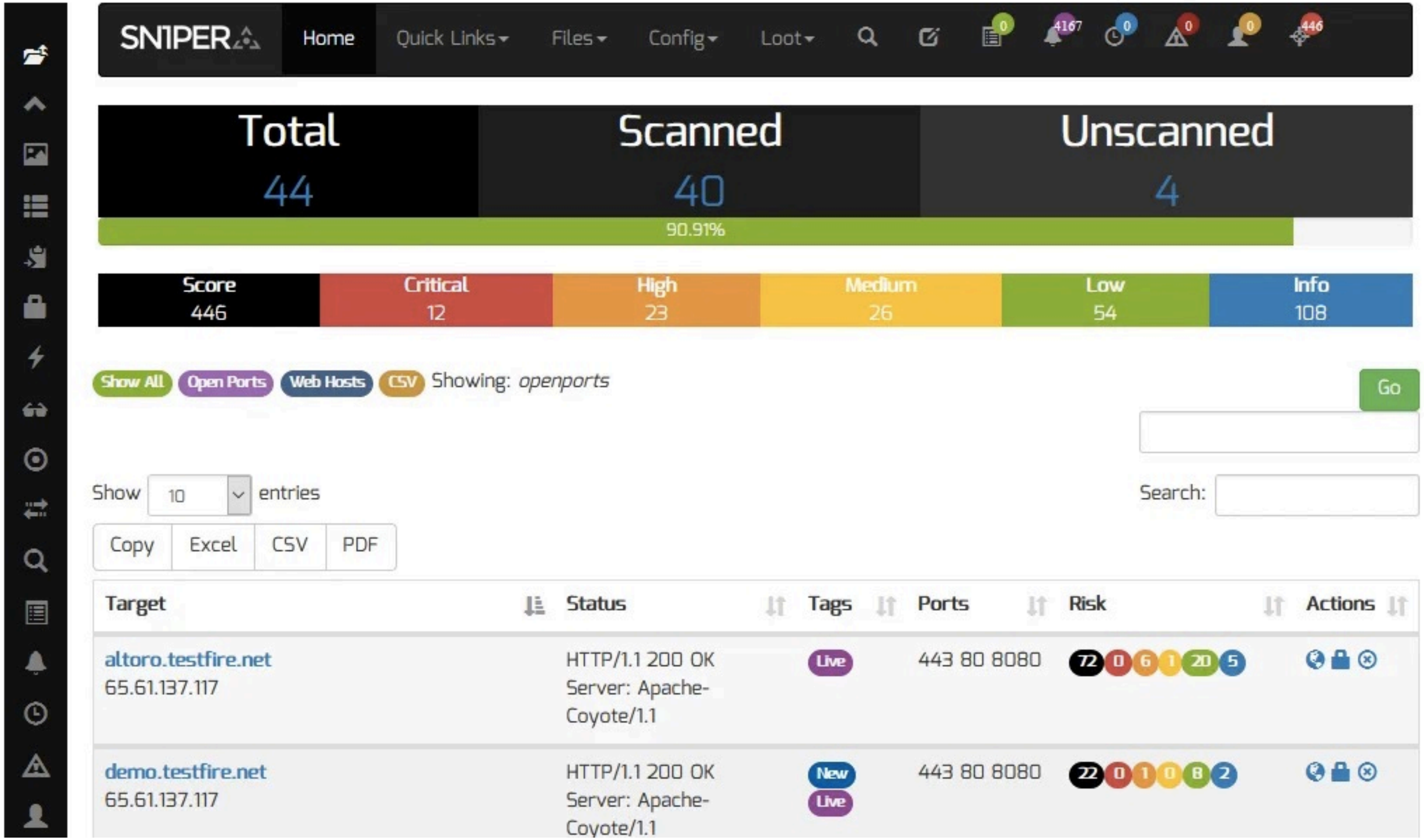
Demo Place Holder

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

Sn1per Pro Version



Total	Scanned	Unscanned
44	40	4

90.91%

Score	Critical	High	Medium	Low	Info
446	12	23	26	54	108

Showing: *openports*

Target	Status	Tags	Ports	Risk	Actions
altoro.testfire.net 65.61.137.117	HTTP/1.1 200 OK Server: Apache-Coyote/1.1	Live	443 80 8080	72 0 6 1 20 5	
demo.testfire.net 65.61.137.117	HTTP/1.1 200 OK Server: Apache-Coyote/1.1	New Live	443 80 8080	22 0 1 0 8 2	

More Information

Official Documentation

Several other capabilities
https://xerosecurity.com/
https://github.com/1N3/Sn1per

Professional Versions

For red team companies and bug bounty professionals

Increases your productivity

Other Recon Courses

“Technical Information Gathering with TheHarvester”

“Technical Information Gathering with Maltego CE”

Remediation

Audit your own company

Ensure personal information is not available to the public

Thank you!

Ricardo Reimao
Cyber security consultant