

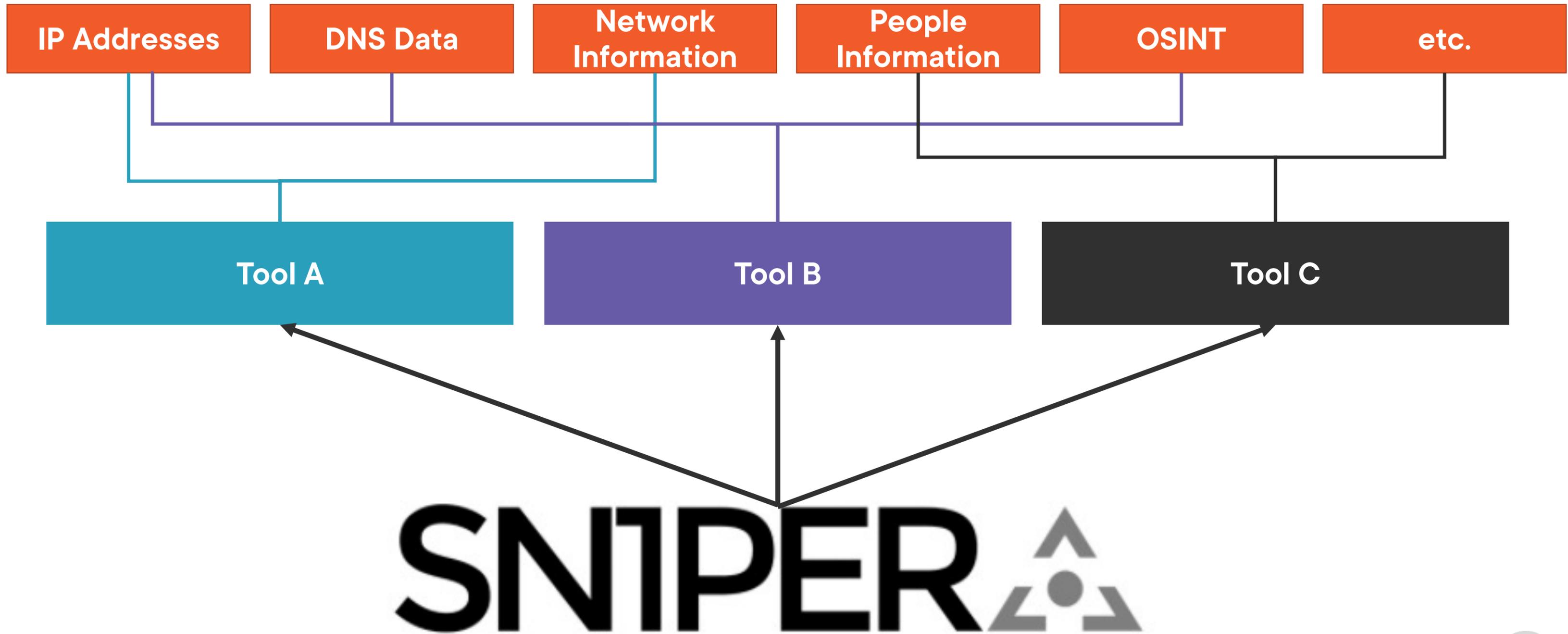
Reconnaissance with Sn1per



Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant



Automating Reconnaissance



SNIPER 



SNIPER

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

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



SNIPER

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, theHarvester, WafWoof, etc.)

Recommended for advanced red teamers



Recon Data

Passive Information Gathering

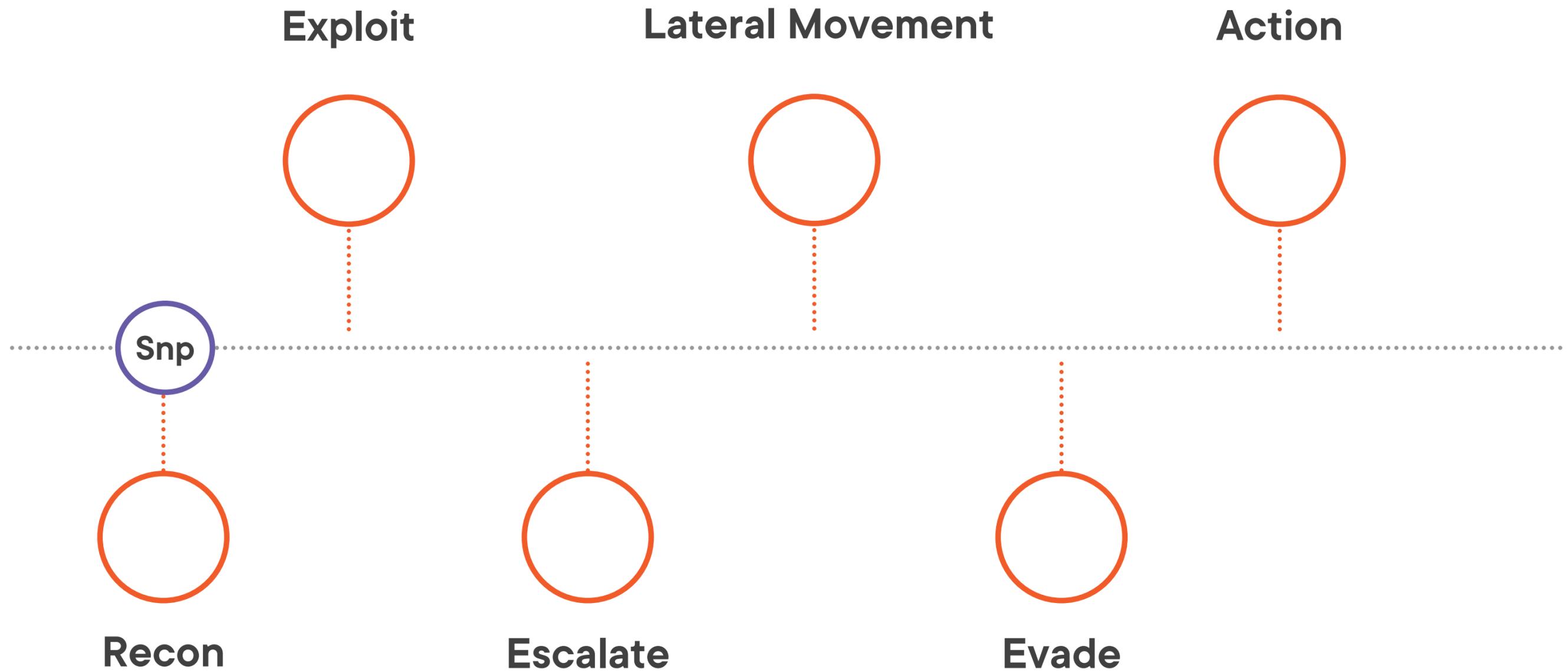
WHOIS records
DNS queries
OSINT searches
Social media searches
Search engine recon
etc.

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



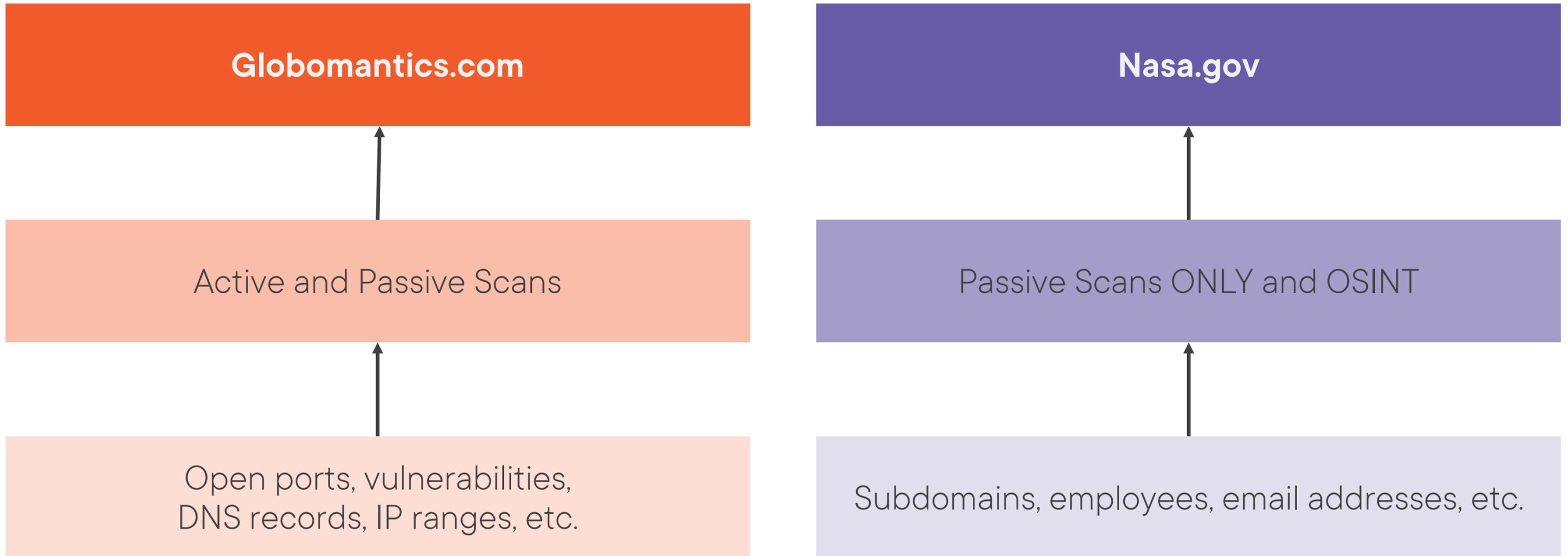
MITRE ATT&CK

Tactics

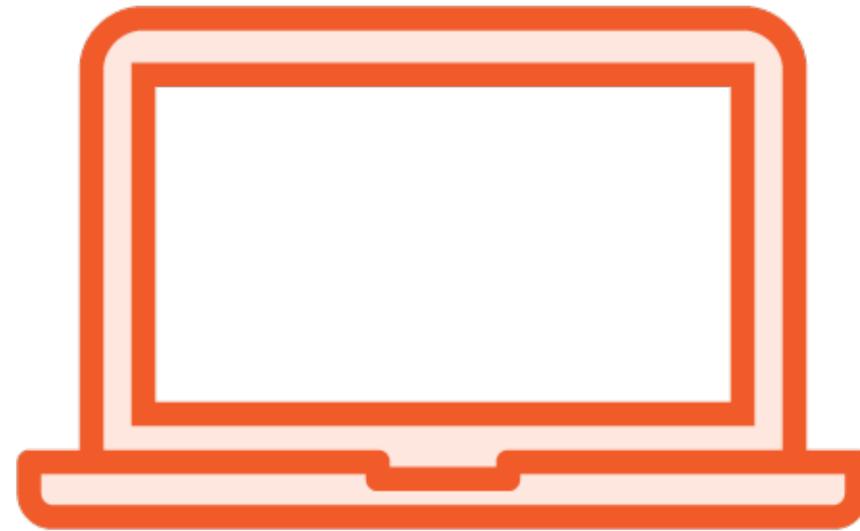
Reconnaissance	T1595: Active Scanning
Resource Development	
Initial Access	T1592: Gather Victim Host Information
Execution	
Persistence	
Privilege Escalation	T1590: Gather Victim Network Information
Defense Evasion	
Credential Access	T1596: Search Open Source Technical Databases
Discovery	
Lateral Movement	
Collection	T1593: Search Open Source Websites/Domains
Command & Control	
Exfiltration	T1589: Gather Victim Identity Information
Impact	



Demo Explanation



Prerequisites



Kali Linux

... or any other Linux distribution

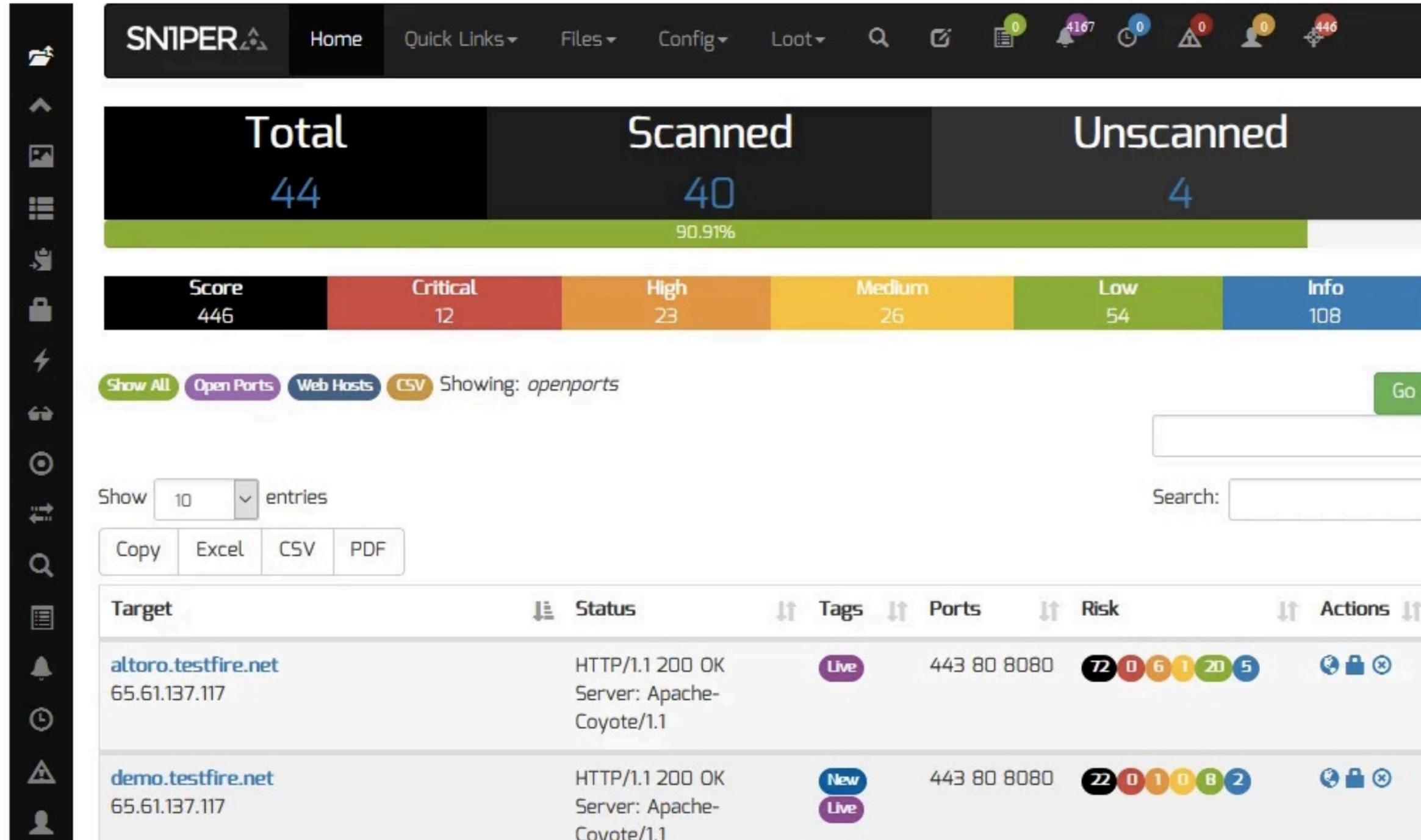


Demo Place Holder

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



The screenshot shows the Sn1per Pro Version dashboard. At the top, there is a navigation bar with the 'SNIPER' logo and menu items: Home, Quick Links, Files, Config, and Loot. On the right side of the navigation bar, there are several notification icons with counts: 0, 4167, 0, 0, 0, and 446. Below the navigation bar, there is a summary section with three main categories: Total (44), Scanned (40), and Unscanned (4). A progress bar below these categories shows 90.91% completion. Underneath, there is a risk score breakdown: Score (446), Critical (12), High (23), Medium (26), Low (54), and Info (108). Below the risk breakdown, there are filter buttons: Show All, Open Ports, Web Hosts, and CSV. The current view is set to 'Showing: openports'. There is a search bar and a 'Go' button. Below the search bar, there is a 'Show' dropdown set to '10 entries' and a 'Search:' input field. At the bottom, there are buttons for 'Copy', 'Excel', 'CSV', and 'PDF'. The main content area is a table with columns: Target, Status, Tags, Ports, Risk, and Actions. The table contains two entries: 'aloro.testfire.net' and 'demo.testfire.net', both with IP address 65.61.137.117. The 'aloro.testfire.net' entry has a 'Live' tag and a risk score of 72. The 'demo.testfire.net' entry has 'New' and 'Live' tags and a risk score of 22.

SNIPER Home Quick Links Files Config Loot

Total 44 Scanned 40 Unscanned 4

90.91%

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

Show All Open Ports Web Hosts CSV Showing: openports

Go

Show 10 entries

Search:

Copy Excel CSV PDF

Target	Status	Tags	Ports	Risk	Actions
aloro.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

