RED TEAM

Introduction OSINT – Open Source Intelligence

redteams.net

Open Source Intelligence (OSINT) is the collection and analysis of information gathered from publicly available sources.

OSINT accounts for ~90% of [actionable] intelligence, which is generally not protected or classified.

What is the value of OSINT for Red Teaming?

Simple:

Learning, connecting & tracking.

There are different tools and techniques for OSINT:

Collection Tools (Recorded Future, Paterva, Pipl, Spokeo, NetGlub…)

Search Engines (Google, iSeek, Shodan, Addictomatic...)

Job Search Websites (Monster, CareerBuilder…)

Social Media (Facebook, LinkedIn, Twitter, Pastebin, Reddit, youtube…)

Intelligence sources (Darkreading, The Hacker News, Crytome, intel sharing organizations…)

Types of OSINT collection:

Passive

Semi-passive

Active

What can we learn using OSINT?

Physical information about our target.

Partners and associates of the target.

Competitors.

Internal structure of the target: employees, positions, departments, product lines, etc.

Job openings.

Recent people fired.

Company events.

Company digital structure.

Metadata.

Company financial information.

Information about specific individuals.

Yes, including physical location.

Challenges?

Ever expanding information sources. The volume grows in size as well as in complexity.

Remember:
When in doubt, Red Team it.