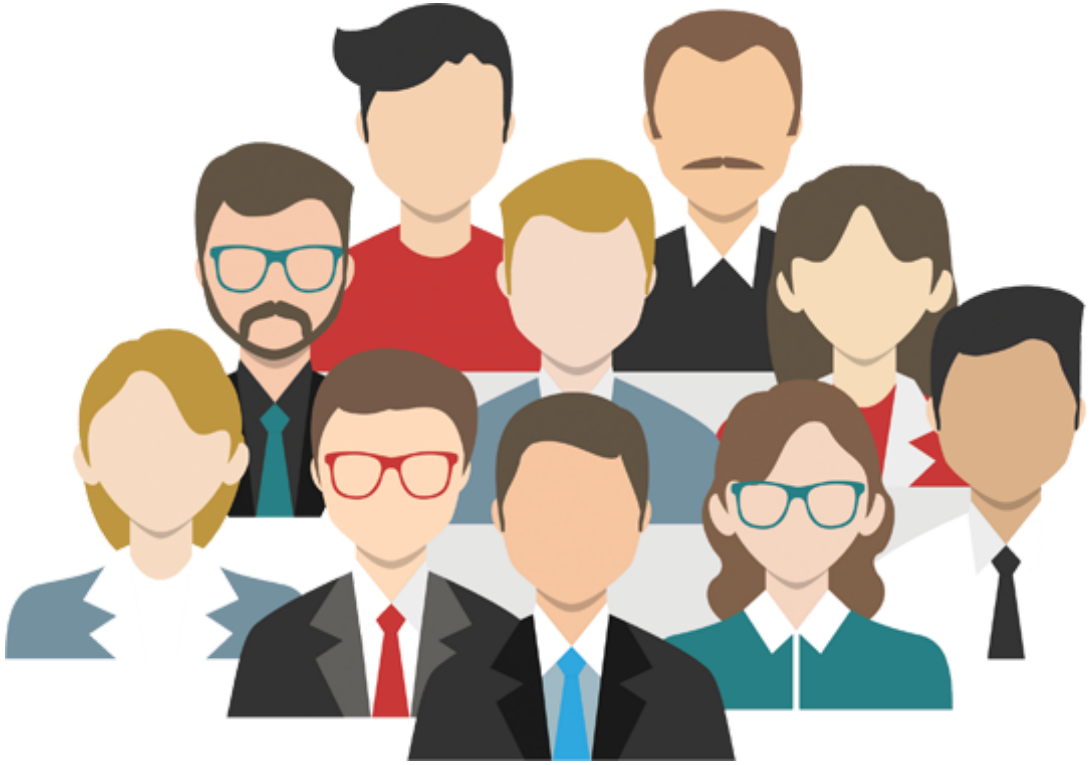
BREACHLOCK™

Top 5 Open Source OSINT Tools

REQUEST A QUOTE



17 JAN, 2019

Top 5 Open Source OSINT Tools

This article addresses various OSINT (Open Source Intelligence) tools. A critical first step is gathering information about an appropriate target within the scope of the project. This enables a Pen Tester to find possible weaknesses and vulnerabilities in a company's security system that may be exploitable.

What is Open Source Intelligence?

OSINT stands for Open Source Intelligence. OSINT is a process to collect data/intelligence about people, companies, and organizations using an extensive collection of sources including the Internet.

As per DoD, OSINT is “produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for addressing a specific intelligence requirement.”

The expanding explosive growth of internet users now pays for goods and services online sharing their thoughts via personal blogs and expose sharing their day to day lives to other people.

This generates extensive data or intelligence in various forms like audio, video, images, and text which is free and accessible to everyone unless restricted by an organization or law.

OSINT sources can be divided up into six different categories of information flow:

Media: print newspapers, magazines, radio, and television from across and between countries.

Internet, online publications, blogs, discussion groups, citizen media (i.e. – cell phone videos, and user-created content), YouTube, and other social media websites (i.e. – Facebook, Twitter, Instagram, etc.). This source also outpaces a variety of other sources due to its timeliness and ease of access.

Public – government data, public government reports, budgets, hearings, telephone directories, press conferences, websites, and speeches. Although this source comes from an official source they are publicly accessible and may be used openly and freely.

Professional – academic publications, information acquired from journals, conferences, symposia, academic papers, dissertations, and theses.

Commercial Data, commercial imagery, financial and industrial assessments, and databases.

Grey literature, technical reports, preprints, patents, working papers, business documents, unpublished works, and newsletters.

[Source: https://en.wikipedia.org/wiki/Open-source_intelligence]

So to collect and analyze the massive amount of data /intelligence we need tools that will help us reduce the analysis time.

Below are the freely available OSINT tools that are mostly used by Penetration Testers, social engineers and security researchers for their different projects.

1. Maltego

Maltego is a product of Paterva and is a part of the Kali Linux operating system. Maltego tools help to play out a critical observation against targets with the assistance of different built-in transforms and it is open source so it gives the capability to write custom transform or modules.

To use Maltego first, the user should be registered on the Paterva site.

After registering, the user can run machines on the target or the user can make another machine according to what intelligence they want to collect. After configuring those machines need to be started. There are various footprints built-in inside Maltego which can easily collect information from various sources and based on the result it will also create graphical results about the target.

2. Shodan.io or Censys.io

Shodan and Censys are search engine just like Google but instead of showing websites, hosted files links; and other results, Shodan and Censys shows the servers, networks; and internet connected devices which is very crucial information for security researches and Pentester and help them to test for many common vulnerabilities.

The devices/servers may vary from computers, laptops, webcams, traffic signals, and various IOT devices.

3. The Harvester

The Harvester is an outstanding tool for collecting intelligence like email and domain for the specified target. This tool is a part of the Kali Linux operating system and very popular for harvesting intelligence used in the early stages of a penetration test or phishing.

Following pieces of information, we can gather from the tool

We use this tool to gather the following:

email address, usernames, subdomains, IPs; and URLs using multiple public data sources.

4. Recon-Ng

Recon-ng is another powerful tool for target intelligence collection which also comes with the Kali Linux operating system. Recon-ng builds with a modular approach in mind just like Metaspoilt. So according to the need, we can use different modules on the target to extract information. Just add the domains in the workspace and use the modules.

5.tin Eye

TinEye is a reverse image search engine. You'll submit a picture to TinEye to seek out wherever it came from and how it's getting used. TinEye uses neural networks, pattern recognition, machine learning, and image recognition technology instead of keywords or metadata.

Link: https://www.tineye.com

6. Google Dorks (Bonus)

Yes, Google! Don't be shocked. I know Google is a search engine and not an open source tool but we generally use Google to find anything we want. Google is the most powerful and largest search engine in the world that crawls and processes/index billions of pages every day. There is a technique known as Google dorking or simply Google hacking. In this, we use the Google advanced search parameter directly in the browser to refine our search results and find the information that we are looking for.

Following are some google dorks:

1. site:example.com ext:pdf|docs

This specific query will show all pdf and docs files link present on the example.com

2. site:example.com intext:"@example.com"

This specific query will show all emails that end with "@example.com" on example.com

3. inurl: login intitle: login

This specific query will show all the login pages of different websites.

Category

Application Security Testing	9
AWS Penetration Testing	4
Cloud Penetration Testing	5
DAST-Dynamic Application Security Testing	9
DevSecOps	6
GDPR	1
HIPAA	3
Infographics	3
network penetration test	1
OSINT Penetration Testing	1
PCI DSS Compliance	2
Penetration Testing as a Service	10
Uncategorized	2

Recent Post

Importance of Black Box Penetration Testing in Application Security

16 JUL, 2019

Benefits of Automated Penetration Testing

13 JUL, 2019

Vulnerability Scanning and Penetration Testing For HIPAA [Infographic]

12 JUL, 2019

Security Testing

Penetration Testing Service

Continuously find and fix your security gaps.

Application Penetration Testing

Conduct manual penetration tests on applications to achieve compliance

DAST

Dynamic application security testing

IOT Penetration Testing

Check Our IoT Penetration Testing expertise

Social Engineering

Our unique OSINT and Phishing Exposure Assessment

Web Application Penetration Testing

OWAS compliant Web Penetration Testing Services

DevSecOps

Find vulnerabilities fast and early, empower your DevOps

Network Penetration Testing

External and Internal Penetration Testing

Cloud Penetration Testing

Benefit from our Cloud Penetration Testing expertise

Vulnerability Assessment

Benefit from our Vulnerability Assessment expertise

Compliance

Vendor Assessments

Respond to Vendor Security Assessments with confidence

PCI DSS

PCI DSS Penetration Testing and ASV Scans

HIPAA

HIPAA Risk Assessment and Penetration Testing

GDPR

GDPR Compliance with BreachLock™ Security Testing

Follow us

Tell us about your requirements. We respond the same business day.

Fill out the form below to let us know your requirements. We will contact you to determine if BreachLock™ is right for your business or organization.

Once you do, we'll reach out to:

- Ask you a few questions
- Understand your scope and timeline
- Determine if there's a good fit
- Provide a competitive quote within 24 hours

Name

Phone Number

Email

Security needs, scoping details, etc

GET A QUOTE

Menu

How It Works

Cloud Platform

FAQ

Company

Blog

Contact

Privacy Policy

Contact

BreachLock Inc.
276 5th Avenue
Suite 704 – 3031
New York NY 10001

Terms Of Use

E: sales@breachlock.com

P: +1 917-779-0009

F: +1 302 516-7152