

Osint

Что такое Osint ?



Open Source Intelligence

Этапы проведения Osint

- ▶ 1. Формирование задачи
- ▶ 2. Планирование
- ▶ 3. Сбор информации
- ▶ 4. Анализ результатов

Формирование задачи

Для чего мы проводим Osint?

- ▶ Пассивное сканирование для проведения тестов на проникновение
- ▶ Разведка для проведения тестов на проникновение с использованием методов социальной инженерии

Пассивное сканирование для проведения тестов на проникновение

- ▶ Заголовки сервера
- ▶ CMS и их версии
- ▶ Раскрытие полных путей на сервере
- ▶ /phpinfo.php
- ▶ Информации на старых поддоменах (напр. старые скрипты, настройки программного обеспечения)
- ▶ Robots.txt
- ▶ Кэш гугла
- ▶ Github (проекты компании или исходники самого сайта)
- ▶ Публичные базы (госконтракты)

Разведка для проведения тестов на проникновение с использованием методов социальной инженерии

- ▶ Деятельность компании/отдела
- ▶ Сбор информации о людях (должности телефоны)
- ▶ Информация для атаки на конкретного человека(почта, ники, утекшие пароли, соцсети, увлечения, мероприятия в которых он участвовал)
- ▶ Сбор информации об электронной почте/домене
- ▶ SMTP валидация почты с использование методов VRFY EXPN SEND
- ▶ Определение программного обеспечения используемого в организации

Планирование

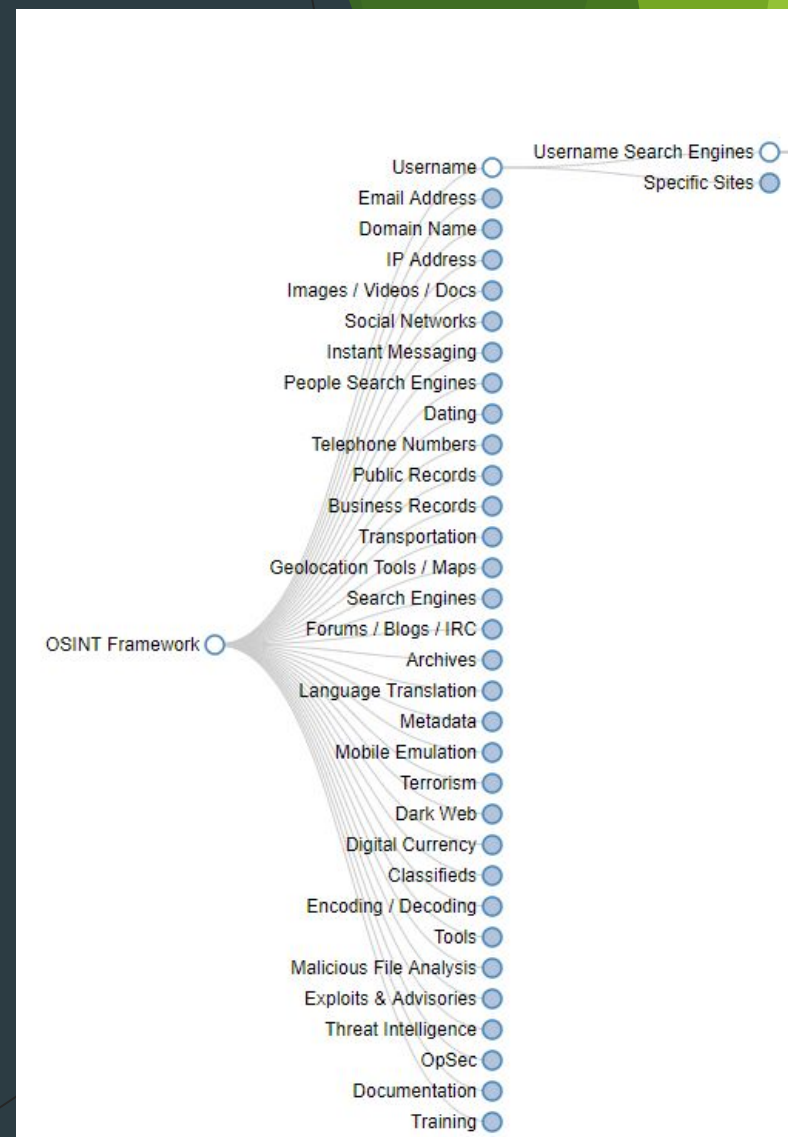
- ▶ Определение направлений и источников получения информации
- ▶ Визуализация полученной информации

Сбор информации

- ▶ Фреймворки
- ▶ Утилиты по сбору информации
- ▶ Веб-ресурсы
- ▶ Telegram боты

Фреймворки

- ▶ **Osint Framework**
(<https://osintframework.com>, <https://github.com/lockfale/osint-framework>)
- ▶ **Awesome OSINT** (<https://github.com/jivoi/awesome-osint>)
- ▶ **Maltego** (<https://paterva.com>)
- ▶ **DataSploit Framework** (<https://github.com/datasploit/datasploit>)



Общедоступные базы

- ▶ Поиск по судебным делам РФ <https://sudrf.ru/index.php?id=300>
- ▶ База дипломов <http://frdocheck.obrnadzor.gov.ru>
- ▶ База судебных приставов <http://fssprus.ru/iss/ip/>
- ▶ База недействительных паспортов <http://services.fms.gov.ru/info-service.htm?sid=2000>
- ▶ База ИНН <https://service.nalog.ru/static/personal-data.html?svc=inn>
- ▶ А также многие другие данные налоговой, доступные на том же сайте.
- ▶ Всё о владельце машины по госномеру, телефону или VIN <https://avinfo.co> или <https://гибдд.рф/check/auto>
- ▶ Информация об ИП и организациях в том числе по ФИО предпринимателя <https://egrul.nalog.ru/index.html>
- ▶ Получить выписку из ЕГРН об основных характеристиках и зарегистрированных правах на объект недвижимости https://rosreestr.ru/wps/portal/p/cc_present/EGRN_1

Поиск по никнейму

- ▶ <https://www.namecheckr.com>
- ▶ <http://usersherlock.com>
- ▶ <https://usersearch.org>
- ▶ <https://thatsthem.com>
- ▶ <https://inteltechniques.com>

Поиск людей в социальных сетях

- ▶ <https://www.namecheckr.com>
- ▶ <http://usersherlock.com>
- ▶ <https://usersearch.org>
- ▶ <https://thatsthem.com>
- ▶ <https://inteltechniques.com>

Поиск по фото

- ▶ <https://images.google.com>
- ▶ <https://yandex.ru/images>
- ▶ <https://www.tineye.com>
- ▶ <https://findmevk.com>
- ▶ <https://vlicco.ru>
- ▶ <https://searchface.ru>
- ▶ <https://findface.pro>

Извлечение EXIF информации из фотографии (может содержать географические координаты места съемки):

- ▶ <http://metapicz.com/>
- ▶ <http://linkstore.ru/exif/>
- ▶ <http://exif.regex.info/exif.cgi>
- ▶ <http://imgops.com/>

Поиск по домашнему телефону

- ▶ <http://spra.vkaru.net>
- ▶ <http://nomerorg.me>.

Поиск по утечкам различных баз данных

- ▶ <https://ghostproject.fr>
- ▶ <https://haveibeenpwned.com/>
- ▶ <https://hacked-emails.com/>
- ▶ <https://weleakinfo.com/>
- ▶ <https://leakedsource.ru/>

Поиск почтовых адресов

- ▶ [hunter.io](#)
- ▶ [Email Finder](#)
- ▶ [theHarvester](#)

Поиск поддоменов

- ▶ [theHarvester](#)
- ▶ [dnsdumpster.com](#)
- ▶ [pentest-tools.com](#)

Поиск уязвимостей

- ▶ cvedetails.com
- ▶ exploit-db.com
- ▶ vulners.com

Определение IP адресов организации

- ▶ *Shodan*
- ▶ *Censys*
- ▶ *bgp.he.net*
- ▶ *www.ididb.ru*

Поиск скрытых директорий и файлов

- ▶ Google Dorks
- ▶ DirBuster

Telegram боты

- ▶ @HowToFind_bot
- ▶ @AvinfoBot
- ▶ @buzzim_alerts_bot
- ▶ @mailsearchbot
- ▶ @deanonym_bot
- ▶ @list_member_bot
- ▶ @telesint_bot

Поисковые системы Telegram

- ▶ Tgstat.ru
- ▶ Lyzem.com
- ▶ Buzz.im

Анализ результатов

- ▶ Wisemapping <http://www.wisemapping.com>
- ▶ Mindmeister <https://www.mindmeister.com>
- ▶ Mindomo <https://www.mindomo.com>
- ▶ Maltego <https://www.paterva.com>

Как защищаться

- ▶ Определить информацию, способствующую проведению атаки
- ▶ Повышение компетентности сотрудников в вопросах обеспечения информационной безопасности
- ▶ Разграничение прав доступа
- ▶ Инструкции по обмену информацией
- ▶ Установка и своевременное обновление антивирусного ПО на всех средствах вычислительной техники