

< Teach
Me
Skills />

OSINT

Собираемся и отмечаемся

Вопросы по предыдущим темам или ДЗ

Mini-quiz по прошлым темам:

1. Что такое дамп памяти?
2. Какие основные модули мы можем применять в Volatility?
3. Как мы можем обнаружить инцидент? Какой инструментарий поможет в этом?
4. Из чего формируется ущерб от компьютерного инцидента?

Mini-quiz по новой теме:

1. Какие основные «открытые» источники для OSINT?
2. Является ли противозаконным «пробив» по открытым источникам?
Если использовать сливы баз данных?
3. Какие основные законы и моральные нормы - необходимо соблюдать при проведении OSINT?
4. Для чего можно или нужно проводить OSINT?

План занятия

1. Рассмотрим основные открытые источники для сбора информации
2. Рассмотрим некоторые фишки для поиска информации
3. Попробуем некоторые инструменты и рассмотрим возможные пути для поиска информации

OSINT - Open Source Intelligence - это практика сбора и анализа информации о цели из публично доступных (законно доступных) источников, без какого-либо прямого взаимодействия с ней.

Разведка в сети - это процесс сбора и анализа информации об информационных системах, их ресурсах, устройствах, программном обеспечении, уязвимостях и средствах защиты.

Практическими задачами разведки при проведении пентеста являются:

1. Поиск дополнительных активов для включения в объем работ;
2. Обнаружение адресов электронной почты и учетных записи для брутфорса (взлома перебором комбинаций);
3. Выявление утечек важной информации, которая может способствовать компрометации системы: учетных данных, исходного кода и т.д.
4. Получение информации о характеристиках объектов без их активного сканирования (Shodan и тп)

Алгоритм OSINT

1.Идентификация Целей:

Необходимо определить, кто или что является целью. Это может быть человек, организация или событие.

2.Сбор Информации:

Используем поисковые системы для поиска открытых источников информации. Анализируем социальные сети для получения данных о цели. Изучаем новости, блоги и другие общедоступные публикации.

3.Анализ Социальных Сетей:

Следует изучить профили в социальных сетях для получения информации о личной жизни, интересах и связях.

4.Анализ Веб-Сайтов:

Можно произвести поиск по официальным веб-сайтам организаций или персональным страницам. Проанализировать историю веб-сайтов через архивы (Wayback Machine).

5.Поиск Публичных Записей:

Можно использовать публичные базы данных и реестры (например, реестр компаний, судебных решений).

6.Использование Геопространственных Данных:

Используем геопространственные данные для определения местоположения событий или объектов. Анализируем карты, фотографии и видео с геотегами.

7.Использование Специализированных Инструментов:

Используем специальные инструменты для анализа социальных сетей, поиска информации и визуализации данных.

8.Анализ Контекста:

Обязательно проверяем источники данных.

Типы разведки

Существуют два основных способа сбора информации: пассивный и активный

Пассивная разведка

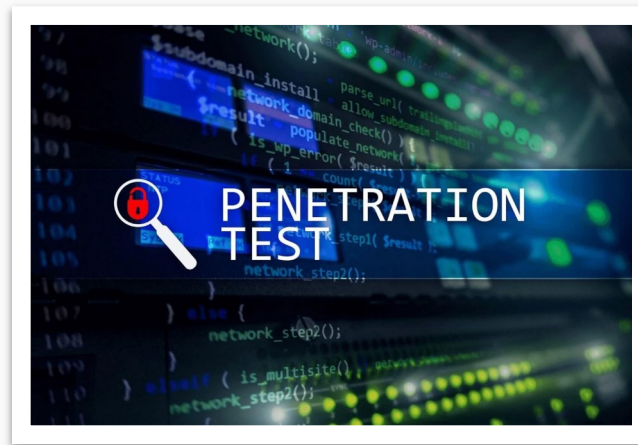
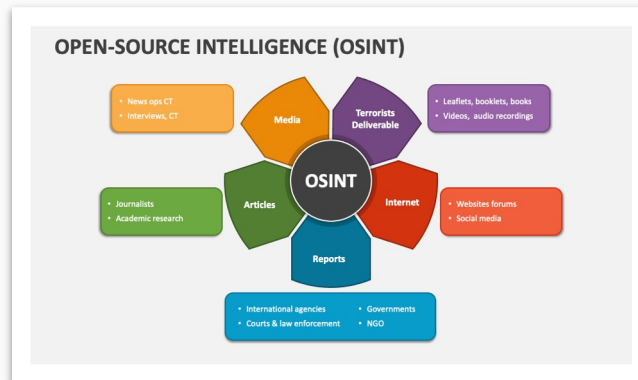
Во время пассивной разведки вы не взаимодействуете с целью.

Примеры данного этапа разведки:

Поиск в поисковых системах Google, и прочих поисковых системах, просмотр баз данных с утечками, анализ вакансий на HH и linkedin, извлечение метаданных из публично доступных файлов и т.д.

Активная разведка

Взаимодействие с инфраструктурой организации: скан портов, перебор директорий, запуск сканеров (Acunetix, Burp suite scanner) фаззинг параметров, резолвинг большого количества доменных имен на серверах цели и т.д.



Что отличает OSINT от разведки и шпионажа

Легальность

Сбор и анализ информации, находящейся в общественном достоянии, не противоречат нормам международного законодательства, а также законам большинства государств. Несмотря на это - некоторые источники и способы их исследования могут находиться на грани законности.

Во время же промышленного или коммерческого шпионажа используются незаконные методы и инструменты для получения информации, такие как подкуп и шантаж членов конкурирующей организации, несанкционированное проникновение в закрытые базы данных, похищение информации, составляющей коммерческую тайну, и т.д.

Доступность

Мониторить и анализировать общедоступные источники может любая организация и даже отдельный человек без использования специализированного оборудования или «связей» в органах госбезопасности.

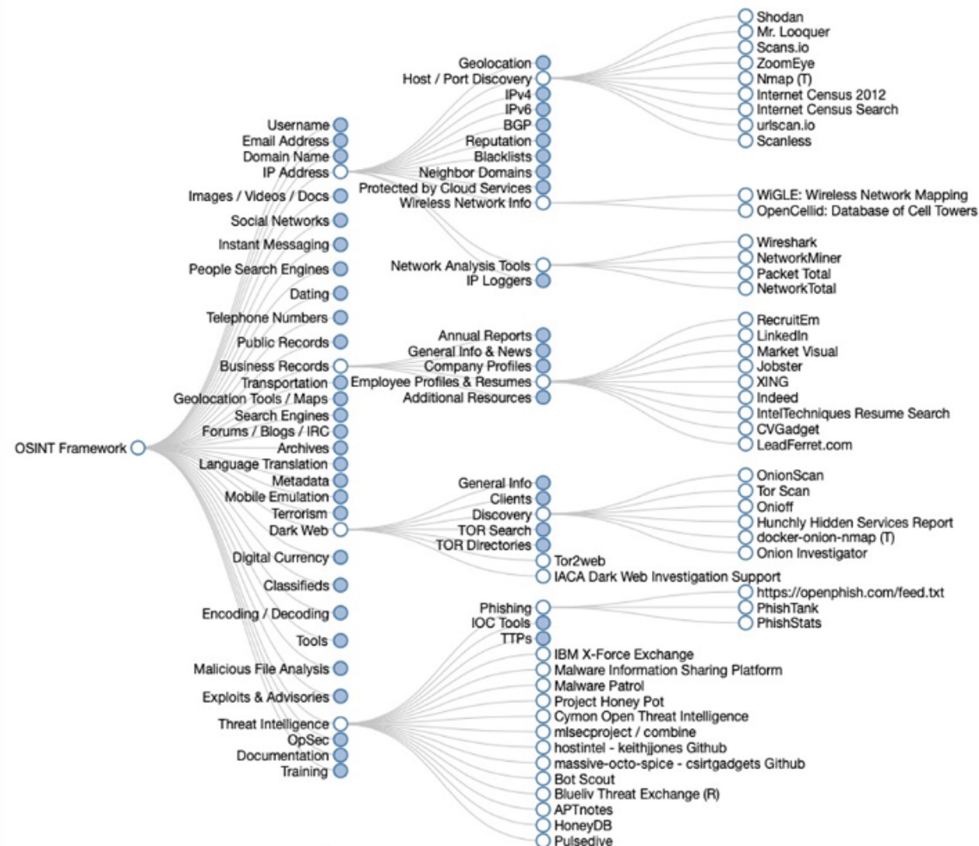
OSINT Framework

The OSINT framework это систематизированный по задачам/видам необходимой информации сборник ссылок на инструменты OSINT, представленный в виде иерархической древовидной структуры.

<https://osintframework.com/>

Список инструментов из модели OSINT можно найти на Гитхабе:

<https://github.com/jivoi/awesome-osint>



WHOIS

WHOIS — это служба TCP, инструмент и тип базы данных и сетевой протокол прикладного уровня, базирующийся на протоколе TCP (порт 43).

Основное применение — получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем. Эта информация часто является общедоступной, поскольку регистраторы взимают плату за скрытие данных в базе.

Протокол WHOIS подразумевает архитектуру «клиент-сервер» и используется для доступа к публичным серверам баз данных (БД) регистраторов IP-адресов и регистраторов доменных имён.

Существует большое количество веб-служб по запросу информации whois

Например на whoer.net

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ whois ya.ru  
% TCI Whois Service. Terms of use:  
% https://tcinet.ru/documents/whois_ru_rf.pdf (in Russian)  
% https://tcinet.ru/documents/whois_su.pdf (in Russian)  
domain: YA.RU  
nserver: ns1.yandex.ru.  
nserver: ns2.yandex.ru.  
state: REGISTERED, DELEGATED, VERIFIED  
org: YANDEX, LLC.  
taxpayer-id: 7736207543  
registrar: RU-CENTER-RU  
admin-contact: https://www.nic.ru/whois  
created: 1999-07-12T14:40:22Z  
paid-till: 2024-07-31T21:00:00Z  
free-date: 2024-09-01  
source: TCI  
Last updated on 2024-03-27T06:21:30Z
```

Поиск информации в DNS

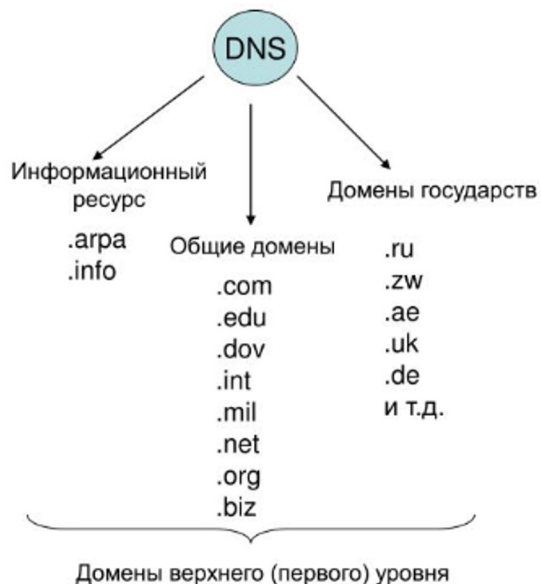
Что такое DNS

Система доменных имен (Domain Name System - DNS) - это распределенная база данных, отвечающая за преобразование удобных для пользователя доменных имен в IP-адреса.

Имеет иерархическую структуру, разделенная на несколько зон, начиная с корневой зоны верхнего уровня.

DNS (Domain Name System)

Логическая структура DNS



Размер доменного имени до 63 символов латиницей.

Корневых серверов 9, их адреса прописаны на всех зонах DNS-серверах. Зона – область, подконтрольная одному DNS-серверу.

Примеры доменов 3 уровня:

golgen.spb.ru

www.golden.spb.ru

Важно: www обозначается специализированный сервер, как уровень не считается!

Состав DNS-записи

Информацию о доменах хранят специальные DNS-серверы в виде ресурсных записей (DNS-записей ресурса). Чтобы новый сайт получил официальную «прописку» в Сети, нужно сначала прикрепить (делегировать) его домен на DNS-серверы, а затем прописать на этих серверах ресурсные записи.

Типы записей DNS

В каждом домене могут использоваться различные типы записей DNS. К наиболее распространенным типам записей DNS относятся:

A-запись (Address record)

Address record указывает на конкретный IP-адрес домена. Без нее сайт работать не будет. По этой записи система определяет к какому серверу обращаться за получением информации, когда пользователь вводит название сайта в адресную строку веб-браузера.

Типы записей DNS

CNAME (Canonical name)

CNAME («каноническое имя») указывает на расположение хостов на одном сервере. С ее помощью, можно прописать несколько доменов и поддоменов в рамках одного сервера.

Каноническое имя позволяет создать наследование, при котором поддомен получает свойства всех ресурсных записей одного домена (кроме NS), через псевдоним (алиас).

Перед ее заполнением, надо прописать A-запись. После, можно создавать псевдонимы (их количество не ограничено).

MX (Mail exchanger)

MX-запись задает почтовый сервер, который будет принимать и отправлять почту для данного домена. Запись может указывать на внутренний или внешний почтовый сервер.

NS (Name Server)

Этой записью определяется доменный адрес DNS-сервера, обслуживающий конкретный домен. Интернет-соединение с доменом не функционирует, если не указана NS-запись.

Типы записей DNS

TXT (Text String)

TXT-запись используется для хранения текстовых данных о домене. Их число может быть любым, если содержание одной записи не противоречит другим. TXT-запись ограничена размером до 255 байт. Часто применяется для подтверждения прав на владение доменом. Например, когда осуществляется привязка к стороннему почтовому серверу, а также при подключении метрик и в других ситуациях.

SOA (Start of Authority)

Указывает местоположение сервера с эталонной информацией о домене. Запись создается автоматически в самом начале и не может быть отредактирована или удалена.

SRV (Service record)

Указывает расположение серверов (имя хоста, № порта) для определенных сервисов. Выполняет ассоциативную роль.

Например, через него можно задать:

IMAP-сервер для example.net находится по адресу mail.example.net. При этом, example.net — веб-сервер.

Типы записей DNS

PTR (Reverse DNS)

Обратная запись DNS служит для связывания отдельного IP-адреса с доменным именем. В основном, запись используется для отправки почты с домена. Если PTR-запись совпадет с именем почтового сервера из параметра HELO (EHLO), повысится шанс миновать спам-фильтры почтовых серверов на стороне получателя письма.

CAA (Certification Authority Authorization)

Запись определяет, SSL/TLS-сертификаты каких центров сертификации могут применяться для указанного домена или поддомена. Обычно она генерируется на хостинге автоматически. Если CAA-запись не указана, это будет интерпретировано центром, как разрешение на выпуск сертификата.

Типы записей DNS

HINFO (Host Information)

В ней указывается архитектура и операционная система заданного хоста. Запись надо применять с крайней осторожностью, а лучше совсем не пользоваться самостоятельно (обычно ее заполняет хостинг-провайдер). Злоумышленники часто используют HINFO-запись для подготовки хакерских атак.

RP (Responsible person)

Здесь прописаны реквизиты ответственных за домен. Указать можно как одного человека, так группу людей. Поле «Text Record Name» хранит Ф.И.О. ответственного работника, а поле «E-mail Address» — его электронную почту.

LOC (Location information)

В соответствующие поля этой записи указываются широта и долгота физического местонахождения DNS-сервера, к которому привязан домен. Используется редко. Может быть полезна только для крупных компаний.

файл hosts

До появления DNS соответствие между символьными именами и IP-адресами можно было определить в специальном файле hosts. Этот способ можно использовать и сейчас.

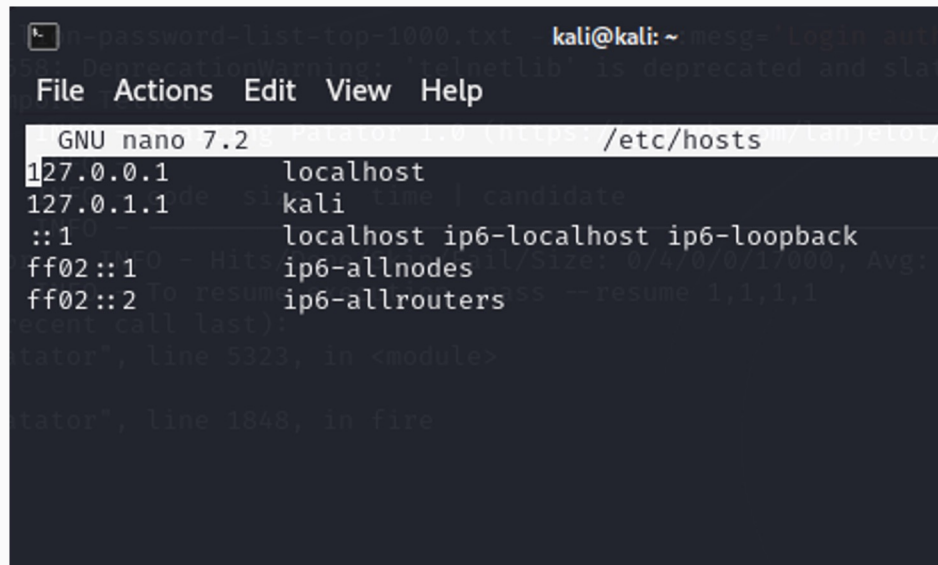
Windows:

WinDir\system32\drivers\etc\hosts

UNIX:

/etc/hosts

Файл hosts содержит строки, Каждая из которых определяет одно соответствие между именем и IP-адресом



```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/hosts  
127.0.0.1 localhost  
127.0.1.1 kali  
::1 localhost ip6-localhost ip6-loopback  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters
```

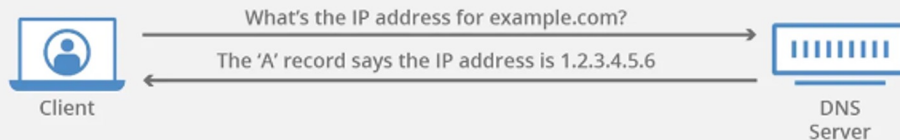
Поиск информации в DNS

Вы можете обнаружить в DNS дополнительные доменные имена и поддомены и другую полезную информацию

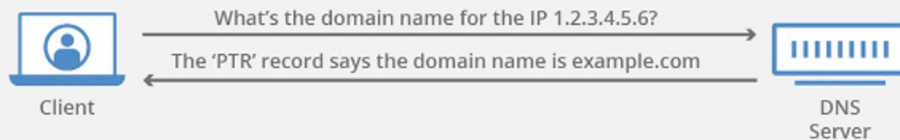
Используйте либо

- прямой поиск DNS, чтобы найти IP-адрес, связанный с доменным именем, или
- обратный (reverse) DNS-поиск для определения доменного имени, связанного с IP-адресом.

Forward(standard) DNS Resolution



Reverse DNS Resolution



Утилиты, которые можно использовать:

- **host**
- **nslookup**
- **dig**

host - DNS lookup utility

[https://en.wikipedia.org/wiki/Host_\(Unix\)](https://en.wikipedia.org/wiki/Host_(Unix))

host - это простая утилита для выполнения запросов к DNS.

Примеры поиска записей:

```
(kali㉿kali)-[~]
└─$ host ya.ru
ya.ru has address 5.255.255.242
ya.ru has address 77.88.55.242
ya.ru has IPv6 address 2a02:6b8::2:242
ya.ru mail is handled by 10 mx.yandex.ru.
```

Брутфорс поддоменов с host:

```
for ip in $(cat ~/YAWR/Recon/all-dns.txt); do host $ip.test.ru | grep address; done
```

```
kali@kali: ~
File Actions Edit View Help
└─$ host
Usage: host [-aCdilrTvVw] [-c class] [-N ndots] [-t type] [-W time]
          [-R number] [-m flag] [-p port] hostname [server]
-a is equivalent to -v -t ANY
-A is like -a but omits RRSIG, NSEC, NSEC3
-c specifies query class for non-IN data
-C compares SOA records on authoritative nameservers
-d is equivalent to -v
-l lists all hosts in a domain, using AXFR
-m set memory debugging flag (trace|record|usage)
-N changes the number of dots allowed before root lookup is done
-p specifies the port on the server to query
-r disables recursive processing
-R specifies number of retries for UDP packets
-s a SERVFAIL response should stop query
-t specifies the query type
-T enables TCP/IP mode
-U enables UDP mode
-v enables verbose output
-V print version number and exit
-w specifies to wait forever for a reply
-W specifies how long to wait for a reply
-4 use IPv4 query transport only
-6 use IPv6 query transport only
```

Nslookup

Несмотря на отсутствие в списке LOLBAS, nslookup является еще одной замечательной утилитой для перечисления DNS в Windows и по-прежнему используется в сценариях “Living off the Land”.

LOLBAS - Living Off The Land Binaries and Scripts

<https://github.com/LOLBAS-Project/LOLBAS>

Также применяется при необходимости проверить работоспособность DNS, увидеть скорость получения IP адреса для доменного имени.

Команда Nslookup присутствует в большинстве операционных систем

```
`$ nslookup example.com`
```

Посмотреть отдельные типы записей:

```
`$ nslookup -type=ns example.com`  
`$ nslookup -type=soa example.com`  
`$ nslookup -query=mx example.com`
```

Посмотреть все записи:

```
`$ nslookup -type=any example.com`
```

dig - “Domain Information Groper”

[https://en.wikipedia.org/wiki/Dig_\(command\)](https://en.wikipedia.org/wiki/Dig_(command))

DIG (domain information groper) - это инструмент командной строки сетевого администрирования для запроса системы доменных имен (DNS). DIG полезен для устранения неполадок в сети и в образовательных целях. Без каких-либо аргументов он запрашивает корневую зону DNS.

DIG является компонентом программного пакета BIND и заменяет функциональность более старых инструментов, таких как nslookup. Тем не менее, старые инструменты все еще используются в качестве дополнения. Он может идентифицировать записи IP-адресов, записывать маршрут запроса при получении ответов от авторитетного сервера имен, диагностировать другие проблемы DNS

<http://pyatilistnik.org/installing-dig-on-windows/>

Web Dig: <https://toolbox.googleapps.com/apps/dig/>

Другие инструменты для работы с DNS

dnsrecon

<https://github.com/darkoperator/dnsrecon>

```
$ dnsrecon -d example.com
```

Этот скрипт позволяет выполнять:

- Проверку всех NS-записей на предмет трансфера зоны.
- Перечисление общих DNS-записей для данного домена (MX, SOA, NS, A, AAAA, SPF и TXT).
- Выполнить перечисление общих SRV-записей.
- Расширение доменов верхнего уровня (TLD).
- Проверку разрешения с помощью Wildcard.
- Поиск поддоменов и хостов по записям A и AAAA с заданным доменом и списком слов.
- Поиск PTR-записей для заданного диапазона IP-адресов или CIDR.
- Проверку кэшированных записей DNS-сервера на наличие A, AAAA и CNAME-записей при наличии списка записей хоста в текстовом файле для проверки.

Поиск поддоменов

Dork

Один из самых простых способов начать поиск поддоменов - использовать Google Dork. Для поиска поддоменов мы воспользуемся следующим шаблоном:

```
site:*.domain.com -www
```

site:domain.com - эта часть команды указывает Google искать только в пределах домена domain.com.

Звездочка * - подстановочный знак, который соответствует всем поддоменам домена domain.com. Он ищет только поддомены типа subdomain.domain.com.

-www Эта часть исключает все результаты, содержащие www. Знак минус (-) используется для отрицания поискового запроса, поэтому в данном случае он отфильтровывает результаты, содержащие www.

recon-ng

<https://hackertarget.com/recon-ng-tutorial/>

Recon-ng - это полнофункциональный фреймворк для разведки, разработанный с целью создания мощной среды для быстрого и тщательного проведения веб-разведки.

theHarvester

<https://github.com/laramies/theHarvester>

theHarvester - это простой в использовании, но мощный инструмент, предназначенный для использования на этапе разведки в рамках редтиминга или теста на проникновение.

Инструмент собирает:

- имена пользователей,
- адреса электронной почты
- IP-адреса
- поддомены
- URL-адреса

subfinder

<https://github.com/projectdiscovery/subfinder>

kali:

```
sudo apt install subfinder
```

subfinder - это инструмент для поиска поддоменов, который возвращает действительные поддомены для веб-сайтов, используя пассивные онлайн-источники. Он имеет простую модульную архитектуру и оптимизирован для скорости. subfinder создан для выполнения только одной задачи - пассивного перечисления поддоменов, и он делает это очень хорошо.

Еще несколько полезных инструментов для поиска поддоменов:

<https://github.com/aboul3la/Sublist3r>

<https://github.com/resurrecting-open-source-projects/dnsmap>

<https://dnsmap.io>

www.virustotal.com/gui/domain/example.com/relations

<https://subdomainfinder.c99.nl>

<https://github.com/ffuf/ffuf>

Google Dorks

Google можно использовать для взлома, используя операторы, которые фильтруют результаты. Следующий список включает наиболее часто используемые операторы:

База гуглдорков на exploit-db

<https://www.exploit-db.com/google-hacking-database>

Другой интересный вариант работы с гуглдорками:

<https://dorksearch.com>

УСЛОВИЯ	РЕЗУЛЬТАТ ПОИСКА
Site:{сайт}	Поисковая система будет отображать только результаты из указанного сайта.
Inurl:{термин}	Поисковая система ограничит результаты сайтам, содержащим этот термин в URL-адресе.
Related:{сайт}	Поисковая система отфильтрует результаты по сайтам, похожим на указанный.
Intext:{термин}	Поисковая система будет искать этот термин на сайтах или в документах.
Link:{сайт}	Поисковая система отобразит другие сайты, связанные с данным сайтом.
*	Звездочка, или астериск - «что угодно».

Google Dorks

Примеры:

`ext:pwd (administrators | users | lamers | service)` - Найдёт все файлы с расширением `.pwd`, в которых есть хотя бы одно из слов, указанных в скобках.

`inurl:wp-config -intext:wp-config "'DB_PASSWORD'"` - Найдёт незакрытый файл конфига для WordPress и покажет пароли в плейнтексте.

`inurl:/proc/self/cwd` - Служит для обнаружения уязвимых или взломанных серверов.

`intitle:"index of" inurl:ftp` - Публичные FTP.

`intitle:index.of id_rsa -id_rsa.pub` - Ключи.

`filetype:xls inurl:"email.xls"` - Списки email.

Камеры:

`inurl:top.htm inurl:currenttime`

`intitle:"webcamXP 5"`

`inurl:"lvappl.htm"`

Файлы:

`intitle: index of mp3` - Музыкальная дорожка mp3.

`intitle: index of pdf` - Документ PDF.

`intext: .mp4` - Видео формата mp4.

`intitle:"Weather Wing WS-2"` - Погода.

`inurl:zoom.us/j and intext:scheduled for` - Митинги Zoom.

`"index of" "database.sql.zip"` - Дампы SQL.

Утечки

Проверьте слитые базы данных. *Snusbase* и *Haveibeenpwned* индексируют информацию с веб-сайтов, которые были взломаны и если их базы данных просочились. Они разрешают искать по электронной почте, имени и никнейму пользователя, IP-адресу, телефону, хэшу или даже паролю.

Haveibeenpwned

<https://haveibeenpwned.com>

IntelligenceX

<https://intelx.io>

Git Search

Для создания дампа найденной на узле папки .git по URL-адресу используйте <https://github.com/arthaud/git-dumper>.

Используйте <https://www.gitkraken.com/> для проверки содержимого.

Если в веб-приложении обнаружен каталог .git, вы можете загрузить все его содержимое с помощью `wget -r http://web.com/.git`. Затем вы можете просмотреть внесенные изменения с помощью `git diff`.

Инструменты: **Git-Money**, **DVCS-Pillage** и **GitTools** можно использовать для получения содержимого git-каталога.

Git Search

git-vuln-finder <https://github.com/cve-search/git-vuln-finder> используется для поиска CVE и сообщений об уязвимостях безопасности внутри сообщений коммитов.

GitRob <https://github.com/michenriksen/gitrob> позволяет искать конфиденциальные данные в репозиториях организаций и их сотрудников.

GitGot <https://github.com/BishopFox/GitGot> - это полуавтоматизированный инструмент с обратной связью, позволяющий пользователям быстро искать секретные секреты в массивах открытых данных на GitHub.

Repo security scanner <https://github.com/techjacker/repo-security-scanner> - это инструмент командной строки, который был написан с единственной целью: помочь вам обнаружить секреты GitHub, которые разработчики случайно сделали, выложив конфиденциальные данные. Как и другие, он поможет вам найти пароли, закрытые ключи, имена пользователей, токены и многое другое.

TruffleHog <https://github.com/trufflesecurity/trufflehog> ищет в репозиториях GitHub и копается в истории коммитов и ветках в поисках случайно опубликованных секретов.

Архивные копии веб-страниц

<https://archive.org/web/>

Хранит моментальные снимки веб-сайтов.

“...25+ лет веб-истории, доступной через Wayback Machine ...”.



Адреса электронной почты

Можно найти корпоративные почтовые адреса. Подобрать пароли или же применив социальную инженерию будет просто получить доступ к важным или личным данным.

Самое полное руководство по поиску email'a

<https://perma.cc/JUE9-XRJL>

Адреса электронной почты

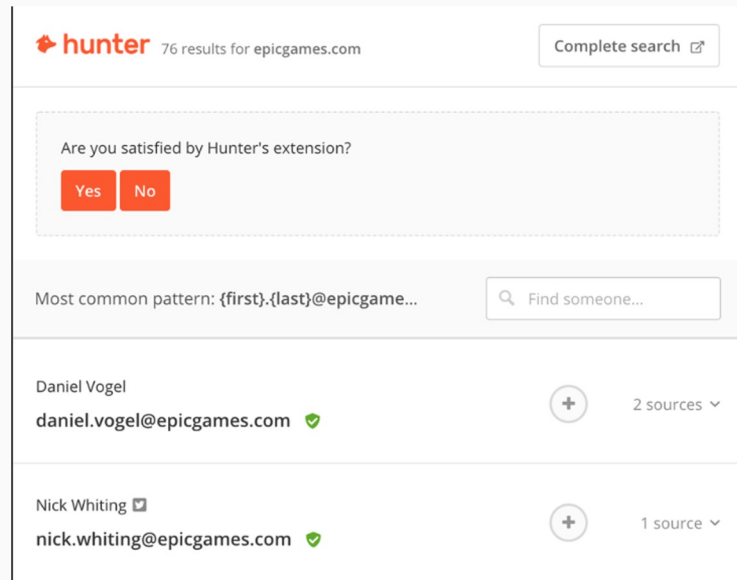
Hunter

Hunter - это многоцелевой дружественный инструмент для рекрутеров, предпринимателей, профессионалов и других, используемый для:

- поиска адресов электронной почты нужного вам домена
- поиска Email-адреса любого специалиста, работающего в любой компании
- проверки любого адреса электронной почты.

Запрос на Hunter может быть выполнен:

- По домену, чтобы найти адреса электронной почты этого домена.
- По полному имени и доменному имени - чтобы найти официальный адрес электронной почты конкретного специалиста, работающего в компании.
- По адресу электронной почты можно проверить, может ли



Адреса электронной почты

Infoga

<https://github.com/GiJ03/Infoga>

Infoga - это инструмент, который собирает информацию об учетных записях электронной почты (IP, имя хоста, страна и т.д.) из различных открытых источников (поисковые системы, серверы ключей PGP и Shodan) и проверяет, была ли утечка электронной почты, используя API haveibeenpwned.com.

Это простой инструмент, но очень эффективный для ранних стадий теста на проникновение или для того, чтобы узнать о видимости вашей компании в Интернете.

Установка и запуск:

```
$ git clone  
https://github.com/m4ll0k/Infoga.git  
$ cd Infoga  
$ python setup.py install  
$ python infoga.py
```

Поиск пользователей

Поиск всех учетных записей пользователя может помочь составить неплохой словарь для брутфорса. Можно узнать об увлечениях или личной жизни в целях компрометации.

Агрегированный поиск людей в соцсетях:

<https://github.com/sherlock-project/sherlock>

<https://www.social-searcher.com>

Поиск пользователей

Социальные сети

После поиска учетных записей в других утилитах, можно прогнать список по всем социальным сетям вручную, иногда получается найти, что-то полезное.

- [VK](#)
- [OK](#)
- [FB](#)
- [Inst](#)

Поиск пол

Leakedif0bot



Бот для пробива. Может найти доступную информацию о физических и юридических лицах из государственных баз данных, взломанных баз, социальных сетей, из других публичных платформ и источников. Оснащён всегда актуальными базами данных. Есть ограничение поиска по России для граждан не из РФ.

HimeraSearch



Работает с OSINT, так и с закрытыми HUMINT (выкупленными конфиденциальными). Список функций: проверка номера, проверка ФЛ, E-mail, поиск по Авто, поиск по паспорту, проверка и поиск по ИНН, поиск по СНИЛС, поиск по ФОТО, проверка адреса.

GetContact



GetContact - мобильное приложение, позиционирующее себя как менеджер звонков и блокировщик спама. В 2017, было в топе всех маркетов. Получало доступ к телефонной книге, путем запроса у пользователя и дампило имена/номера телефонов и отправляло на сервера приложения.

TeleSINT



Позволяет узнать, в каких публичных чатах состоит пользователь. Сейчас в базе данных бота находится более двух миллионов публичных чатов и записи о более чем 366+ миллионах пользователей.

Сбор информации об транспорте

nomerogram.ru



vesseltracker.com



marinetraffic.com



vindecoderz.com



flightradar24.com



openrailwaymap.org



Мы так же можем использовать для сбора информацию из публичных карт, как ЯндексКарты, GoogleMaps и сторонние ресурсы.

Функциональные OSINT машины

TheHarvester

<https://github.com/laramies/theHarvester>

Очень простой в использовании, но мощный и эффективный инструмент, предназначенный для использования на ранних стадиях теста на проникновение. Инструмент собирает электронные письма, имена, поддомены, IP-адреса и URL-адреса, используя несколько общедоступных источников данных, и включает: Пассивную и Активную разведку.

Функциональные OSINT машины

OSINT-SAN

<https://github.com/Bafomet666/OSINT-SAN>

Инструмент дает возможность быстро находить информацию и деанонимизировать пользователей сети интернет. Программное обеспечение представляет собой фреймворк, в котором содержатся 30 функций для поиска информации либо деанонимизации пользователей.

Для работы использует API:

- API для получения информации о номере
- API для получения информации whois
- Shodan API
- Gmap для gui n
- VirusTotal бесплатная служба проверки
- Hunter.io API для получения сведений о @mail
- ZoomEye API, вход осуществляется путем авторизации в самом инструменте
- Torrent API

Spiderfoot

Функциональные OSINT машины

<https://www.spiderfoot.net>

<https://github.com/smicallef/spiderfoot?ref=d>

SpiderFoot - это инструмент автоматизации разведывательной деятельности (OSINT) с открытым исходным кодом. Он интегрируется практически со всеми доступными источниками данных (через API) и использует ряд методов для анализа данных, делая эти данные удобными для навигации.

SpiderFoot имеет встроенный веб-сервер для обеспечения чистого и интуитивно понятного веб-интерфейса, но также может использоваться полностью через командную строку.

Установка:

```
$ git clone https://github.com/smicallef/spiderfoot.git
$ cd spiderfoot
$ pip3 install -r requirements.txt
$ python3 ./sf.py -l 127.0.0.1:5001
```

Запускается <https://127.0.0.1:5001>

Спасибо за внимание!