



OSINT

Руководство по сбору и анализу
открытой информации в интернете



ДЕЙЛ МЕРЕДИТ

Предисловие Грэга Шилдса,
Microsoft MVP и VMware vExpert

Дейл Мередит

OSINT. Руководство по сбору и анализу открытой информации в интернете

Перевела с английского Е. Мансурова

Научный редактор Д. Русин

Дейл Мередит

OSINT. Руководство по сбору и анализу открытой информации в интернете. — 2025. — 224 с.:

Погрузитесь в мир цифровых расследований с книгой, которая станет вашим ключом к пониманию современных угроз и методов защиты от них. Шаг за шагом вы пройдете путь от основ кибербезопасности до тонкостей разведки по открытым источникам (OSINT), ведь только так можно освоить навыки, превращающие информационный шум в ценные инсайты.

Вы узнаете, как находить и анализировать данные, скрытые в публичном пространстве, сохранив анонимность и избегая цифровых ловушек; освоите весь арсенал инструментов OSINT, Recon-ng, Maltego, Shodan, Aircrack-ng и др.; научитесь предотвращать кибератаки и защищать личные и корпоративные данные. Каждая глава — шаг к мастерству: от этичных методов сбора информации до применения профессиональных техник в реальных сценариях.

Практические примеры, четкие инструкции и акцент на безопасности делают книгу незаменимым руководством для тех, кто готов стать цифровым детективом или укрепить свою киберзащиту.

© Packt Publishing 2024.

First published in the English language under the title ‘The OSINT Handbook’

Права на издание получены по соглашению с Packt Publishing. Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав. Информация, содержащаяся в данной книге, получена из источников, рассматриваемых издательством как надежные. Тем не менее, имея в виду возможные человеческие или технические ошибки, издательство не может гарантировать абсолютную точность и полноту приводимых сведений и не несет ответственности за возможные ошибки, связанные с использованием книги. В книге возможны упоминания организаций, деятельность которых запрещена на территории Российской Федерации, таких как Meta Platforms Inc., Facebook, Instagram и др. Издательство не несет ответственности за доступность материалов, ссылки на которые вы можете найти в этой книге. На момент подготовки книги к изданию все ссылки на интернет-ресурсы были действующими.

ОГЛАВЛЕНИЕ

Предисловие	11
Создатели книги	12
Об авторе	12
О рецензентах.....	13
От издательства.....	14
О научном редакторе русского издания	14
Введение.....	15
Для кого эта книга	15
О чем эта книга	15
Условные обозначения	16
Глава 1. Спрятано у всех на виду: раскрываем возможности OSINT	18
Введение в OSINT	19
Поговорим об информации и разведке	19
Пассивная и активная разведка	20
Почему OSINT так важна в цифровую эпоху.....	21
В чём фишка OSINT?.....	21
Как же работает OSINT?.....	22
OSINT Framework	23
Разведка на примере реальных ситуаций	25
Начало работы с OSINT и некоторые рекомендации	27
Полезные советы по сбору информации.....	27
Ресурсы, которые нам пригодятся.....	28
Итоги.....	29

Глава 2. Невидимы и недосягаемы: почему важно сохранять анонимность	30
Основы анонимности и конфиденциальности в OSINT	30
Как может быть нарушена анонимность	31
Подведем итоги: конфиденциальность в OSINT	36
Защита цифрового следа.....	36
Как ограничить СВОЕ присутствие в интернете.....	36
Почему сегодня так важно защищать личные данные	37
Браузеры: первая линия уязвимости.....	38
Как защитить себя	39
Sock puppet: создание и использование виртуальной личности.....	45
Предупреждение киберугроз в OSINT.....	53
Новости о защите конфиденциальности и кибербезопасности	53
Опыт прошлых взломов и инцидентов.....	55
Итоги.....	55
 Глава 3. Арсенал OSINT: методы и приемы сбора и анализа информации	56
Знакомство с методами и приемами OSINT	57
Разнообразие приемов в OSINT.....	57
Выбор подхода в зависимости от задачи.....	62
Поиск информации в видимой сети.....	63
Приемы расширенного поиска	63
Google Dorking: поиск уязвимостей через Google.....	64
Специализированные поисковые системы и каталоги.....	67
Поиск научных публикаций	68
Поиск исходного кода	69
Поиск патентов.....	69
Поиск изображений	70
Разведка по социальным сетям (SOCMINT)	71
Скрытые источники информации	81
Погружение в глубокую сеть и даркнет.....	81
Из чего состоит интернет.....	82
Сбор данных с помощью theHarvester	85
Shodan.....	86

Автоматизация сбора и анализа информации	90
Итоги	92
Глава 4. Исследуем неизвестное: как найти информацию с помощью инструментов поиска	93
Знакомство с инструментами поиска	94
Раскрываем тайны сети	94
Анализ доменов и IP-адресов	95
Как работает WHOIS и зачем он нам нужен	95
Применение WHOIS: домены и блоки IP-адресов	97
Увеличительное стекло: удобные платформы для поиска в WHOIS	98
Поиск взаимосвязей	101
Темная сторона: как злоумышленники используют WHOIS	102
Анализ DNS и IP-адресов: связь доменов с инфраструктурой	103
Трассировка и карты сети: путеводитель по цифровому океану	110
Исследование сайтов: работа со скрытыми данными	115
Веб-скрейпинг и анализ данных	115
Анализ документов и метаданных	124
Выявление скрытой информации в документах и других файлах	124
Анализ содержания документов	126
Визуализация данных OSINT	126
Инструменты и методы визуализации данных OSINT	127
Рекомендации по эффективной работе с инструментами поиска	129
Итоги	130
Глава 5. От Recon-ng до Trace Labs: лучшие инструменты для разведки по открытым источникам	131
Recon-ng: мощный фреймворк OSINT	132
Запуск модулей и сбор информации с помощью Recon-ng	134
Maltego: визуализация данных и связей в OSINT	138
Начало работы с Maltego в OSINT	138
Поиск инфраструктуры	143
Shodan: поисковая система устройств интернета вещей	146
Начало работы с Shodan	146
Использование API Shodan	149

Trace Labs: операционная система для OSINT.....	149
Aircrack-ng: обзор пакета.....	151
Airmon-ng	152
Airodump-ng.....	154
Aireplay-ng.....	156
Aircrack-ng.....	156
Airbase-ng.....	157
Airgraph-ng.....	159
Поиск скрытых сетей	159
Дополнительные инструменты OSINT с открытым исходным кодом	161
SpiderFoot.....	161
Twint	164
Напоследок об инструментах	166
Тенденции в мире инструментов OSINT	167
Блоги и сайты.....	167
Конференции и мастер-классы.....	168
Оценка новых инструментов.....	168
Взаимодействие с сообществом OSINT	169
Итоги	169
 Глава 6. Глаза и уши разведчика: как OSINT помогает снизить киберриски	170
Введение в разведку киберугроз и OSINT	171
Киберугрозы и OSINT	172
Фишинг	172
Социальная инженерия.....	174
Вредоносное ПО и программы-вымогатели	176
Целевые продолжительные атаки (APT).....	181
Сочетание OSINT и внутренних систем безопасности.....	183
Платформы для разведки киберугроз и интеграция OSINT.....	185
Ключевые игроки.....	186
Интеграция OSINT в процессы разведки киберугроз.....	187
Обмен данными OSINT с другими платформами и командами.....	188

Разработка программы разведки киберугроз на основе OSINT	190
Что такое требования к разведке?	190
Значение OSINT	191
Пример из практики: использование OSINT для расследования инцидента	193
Итоги	194
Глава 7. Защита личных и корпоративных данных от киберугроз	195
Как OSINT защищает личные и корпоративные данные	196
Преимущества проактивного подхода к кибербезопасности	196
Личная цифровая гигиена и роль OSINT	197
Выявление и устранение рисков присутствия в Сети	197
Повышение конфиденциальности и безопасности	202
Как OSINT помогает оценить и укрепить безопасность организации	203
Определение потенциальных уязвимостей	203
Программы-вымогатели: выявление и противодействие	205
Обнаружение фишинга и приемов социальной инженерии	207
История хакерской группы Exotic Lily	207
Фишинговые атаки группы Cobalt Dickens	209
Расследование взломов и других нарушений кибербезопасности	210
Выявление источника, масштабов и последствий инцидентов кибербезопасности	212
Создание устойчивой системы киберзащиты на основе OSINT	213
Сотрудничество с сообществом кибербезопасности	214
Адаптация к изменениям в мире киберугроз	214
Обновление стратегии кибербезопасности на основе OSINT	216
Помните об инструментах	217
Итоги	219

Кристе, папиному гику.

В мире технологий и кибербезопасности, где я каждый день погружаюсь в сложные задачи, связанные со взломом и защитой компьютеров, так здорово видеть, что ты разделяешь мою страсть. Ты не просто моя дочь, ты мое второе я. Благодаря твоей любви к технологиям наши беседы такие увлекательные и по-настоящему запоминающиеся.

В этой книге я рассказываю о своих приключениях в мире кибербезопасности, но она посвящена и тебе — за твою искреннюю любовь к технологиям и готовность к новым открытиям. Я надеюсь, что ты продолжишь этот путь, исследуя мир идей с тем же увлечением, что и сейчас.

*С любовью,
nana*

ПРЕДИСЛОВИЕ

В бескрайнем цифровом пространстве сбор информации — залог безопасности. Именно в этой непростой сфере выделяется новая работа Дейла Мередита — всестороннее исследование **разведки по открытым источникам (OSINT)**. Книга Дейла станет незаменимым справочником для специалистов по безопасности, исследователей и всех, кто увлечен разведкой.

Я знаю Дейла почти десять лет — как коллегу, преподавателя и друга. Все это время он занимался кибербезопасностью. Дейл обладает удивительным талантом превращать сложные технические концепции в понятные и увлекательные. Его труды вдохновили множество специалистов, сформировав особый подход к работе в цифровом мире.

Эта книга — результат многолетних исследований, практики и преподавания в области OSINT. Она доказывает стремление Дейла обогатить знания сообщества борцов с киберпреступностью. На страницах книги автор приглашает читателей в увлекательное путешествие по миру OSINT, предлагая инструменты, методы и приемы, которые помогут эффективно использовать общедоступные данные.

Что выделяет эту работу среди других — так это умение Дейла объединять теорию с практикой. Он преодолевает пропасть между абстрактными идеями и их применением в работе, помогая читателям не только понять, каким образом что-то сделать, но и объясня, почему надо действовать именно так. Книга Дейла — больше чем просто руководство. Это увлекательное повествование, раскрывающее суть и потенциал OSINT, способное перевернуть наше представление о безопасности.

Будьте уверены: эта книга станет существенной частью вашего арсенала по кибербезопасности. Неважно, являетесь ли вы опытным специалистом или начинающим энтузиастом: с помощью Дейла вы обогатите свои знания и расширите возможности для борьбы с современными угрозами.

Грег Шилдс
Microsoft MVP и VMware vExpert

СОЗДАТЕЛИ КНИГИ

Об авторе

Дейл Мередит — сертифицированный специалист в области информационной безопасности: этичный хакер, инструктор и тренер, сертифицированный EC-Council и Microsoft. За его плечами более 10 лет работы руководителем в ИТ-сфере, включая работу техническим директором компании-интернет-провайдера. Дейл славится своим мастерством преподавания: он умеет доходчиво объяснять сложные темы и помогать студентам усваивать теорию. Обширные знания и профессионализм Дейла очень востребованы. Он обучал команды компаний из списка Fortune 500, преподавал в университетах по всему миру, проводил занятия в Министерстве внутренней безопасности США и различных военных подразделениях страны. Он создает видеокурсы, консультирует и преподает в классах, но находит возможность регулярно выступать на международных ИТ-конференциях, рассказывая о современных угрозах и инструментах для защиты систем.

Моей жене, Элис Мередит — спутнице на концертах, лучшей подруге и главной опоре в моей жизни. Спасибо за то, что всегда поддерживала мою страсть к технологиям и была рядом в трудные моменты.

Благодарю команду Packt Publishing — Роми, Ашвина, Прачи и многих других: вы с пониманием подстраивались под мой насыщенный график и проявляли терпение в непростые периоды моей жизни.

Моим внукам. Спасибо за то, что дали мне побывать Бэтменом. «Все кажется невозможным, пока не будет сделано», — Брюс Уэйн.

О рецензентах

Дипаншу Кханна (Deepanshu Khanna) – белый хакер, сотрудничающий с министерством обороны Индии. Он активно работает с правительственными организациями, Министерством внутренних дел, полицейскими департаментами, университетами, ведущими мировыми ИТ-компаниями и публицистическими изданиями. Начал свою карьеру с разработки популярных методов взлома GRUB, представленных на конференции HATCON, а также исследования в области систем обнаружения вторжений (IDS) и инструментов целостности данных (AIDE). Дипаншу успешно продемонстрировал уязвимости MD5 и переполнения буфера, а его работы были опубликованы в таких изданиях, как Ptestmag, Hackin9, eForensics, sd-journal и Hack5. Дипаншу выступал на престижных конференциях, включая DEFCON, ToorCon, OWASP, HATCON и H1hackz, в качестве приглашенного докладчика, а также читал лекции в университетах и институтах по всему миру.

Калпа Калхара Сампатх (Kalpa Kalhara Sampath) – выдающийся ученый и исследователь, специализирующийся на информационной безопасности, вредоносном ПО и искусственном интеллекте. Он получил степень бакалавра информационных технологий со специализацией в кибербезопасности в **Институте информационных технологий Шри-Ланки (SLIIT)**, а затем окончил магистратуру по операциям в области кибербезопасности в **Университете Нового Южного Уэльса (UNSW)**. Всего за восемь лет работы Калпа внес значительный вклад в развитие данной научной отрасли благодаря многочисленным публикациям. Он также проявил себя как замечательный лектор и наставник, обучая студентов этичному взлому и цифровой криминалистике. Его исследования востребованы не только в академической среде, но и у практикующих специалистов.

ОТ ИЗДАТЕЛЬСТВА

Мы выражаем огромную благодарность компании КРОК за помощь в работе над русскоязычным изданием книги и вклад в повышение качества переводной литературы.

Ваши замечания, предложения, вопросы отправляйте по адресу

comp@sprintbook.kz

(издательство «SprintBook», компьютерная редакция).

Мы будем рады узнать ваше мнение!

О научном редакторе русского издания

Дмитрий Русин — технический менеджер в компании КРОК. Имеет более пяти лет опыта разработки и внедрения комплексных ИТ-систем, в том числе с применением машинного обучения.

ВВЕДЕНИЕ

Добро пожаловать в захватывающий мир кибербезопасности и **разведки по открытым источникам (Open Source Intelligence, OSINT)**. Эта книга станет вашим надежным проводником по бескрайним просторам цифровой информации и расскажет о том, как применять ее в самых разных областях.

Вы познакомитесь с основами кибербезопасности: узнаете о существующих онлайн-угрозах и освоите эффективные методы защиты. Вы разберетесь, какие угрозы существуют в современном цифровом пространстве, и поймете, что даже простые действия могут значительно повысить уровень вашей безопасности.

OSINT – не просто поиск в Google, а целое искусство сбора данных из общедоступных источников. Вы научитесь находить и анализировать информацию, которая лежит на поверхности, но далеко не всегда заметна на первый взгляд.

Для кого эта книга

Эта книга адресована всем, кто стремится погрузиться в мир цифровых технологий, лучше понять угрозы кибербезопасности и способы защиты, а также освоить этичные методы сбора и анализа общедоступной информации. Вы увлекаетесь кибербезопасностью? Уже работаете в этой сфере или еще учитесь? Кем бы вы ни были, эта книга даст вам ценные знания и практические навыки, которые помогут уверенно ориентироваться в сферах кибербезопасности и OSINT.

О чем эта книга

Глава 1 «Спрятано у всех на виду: раскрываем возможности OSINT» познакомит вас с основами OSINT. Вы узнаете, как, подобно интернет-сыщику, находить ценную информацию, спрятанную от посторонних глаз.

Мы разберемся, почему разведка по открытым источникам так востребована в современном мире.

Глава 2 «Невидимы и недосягаемы: почему важно сохранять анонимность» посвящена конфиденциальности. Вы узнаете, почему при поиске информации анонимность играет такую важную роль, как обезопасить себя от угроз и не выдать, что вы наблюдаете за целью.

Глава 3 «Арсенал OSINT: методы и приемы сбора и анализа информации» погружает вас в мир инструментов OSINT. Вы освоите разнообразные методы сбора и анализа данных из интернета, научитесь применять профессиональные техники и почувствуете себя настоящим цифровым детективом.

Глава 4 «Исследуем неизвестное: как найти информацию с помощью инструментов поиска» отправит вас за сокровищами. Я расскажу, как специальные инструменты помогут найти скрытую информацию, недоступную в обычных поисковых системах.

Глава 5 «От Recon-ng до Trace Labs: лучшие инструменты для разведки по открытым источникам» поведает вам о самых эффективных инструментах OSINT. Вы познакомитесь с мощными программами и сервисами, включая Recon-ng и Trace Labs, и узнаете, как с их помощью усовершенствовать навыки цифровой разведки.

Глава 6 «Глаза и уши разведчика: как OSINT помогает снизить киберриски» рассказывает о том, как OSINT помогает бороться с угрозами кибербезопасности. Вы узнаете, как предотвращать атаки и защищать себя и окружающих в цифровом пространстве с помощью разведки по открытым источникам.

Глава 7 «Задача личных и корпоративных данных от киберугроз» посвящена тому, как уберечь информацию от злоумышленников. Вы научитесь защищать себя и свою организацию от киберугроз, применяя изученные инструменты OSINT.

Условные обозначения

Ниже перечислены условные обозначения, которые используются в этой книге.

Код в тексте. Обозначает ключевые элементы: фрагменты кода, названия таблиц баз данных, условные URL, вводимый текст и учетные записи в Twitter. Пример: «Оператор `inurl:` ищет веб-страницы, в URL которых содержится заданное ключевое слово. В результате можно найти открытые каталоги или конфиденциальную информацию».

Листинг (блок кода) обозначается так:

```
from bs4 import BeautifulSoup
import requests
response = requests.get('https://daledumbsitdown.com')
soup = BeautifulSoup(response.text, 'html.parser')
# Вывести на экран заголовок страницы
print(soup.title.string)
```

Когда нужно обратить внимание на определенную часть кода, строки выделены полужирным:

```
;; ANSWER SECTION:
host1234.examplehosting.com. 3600 IN A 93.184.216.34
site1.com. 3600 IN CNAME host1234.examplehosting.com.
site2.net. 3600 IN CNAME host1234.examplehosting.com.
site3.org. 3600 IN CNAME host1234.examplehosting.com.
```

Ввод и вывод данных в командной строке показан так:

```
nslookup
> set type=MX
> daledumbsitdown.com
```

Полужирный шрифт. Обозначает новый термин, важное понятие.

Шрифт без засечек. Обозначает URL или слова, которые вы видите на экране, а также названия файлов и папок. Например, так оформляются названия пунктов меню или диалоговых окон: «Нажмите правой кнопкой мыши на поток данных и выберите Follow TCP Stream. Эта функция позволит восстановить последовательность данных и найти полезную информацию о функциях и назначении пакетов».

Советы или важные примечания

Выглядят так.

ГЛАВА 1

СПРЯТАНО У ВСЕХ НА ВИДУ: РАСКРЫВАЕМ ВОЗМОЖНОСТИ OSINT

Добро пожаловать в безумную и захватывающую **разведку по открытым источникам (OSINT)**! Мы начинаем главу, где вы раскроете для себя возможности OSINT, познакомитесь с практическими приемами сбора данных и узнаете, почему извлечение информации из открытых источников так ценится в современном цифровом мире. Благодаря изложенным материалам вы научитесь без труда ориентироваться в этой сфере.

В этой главе мы рассмотрим следующие темы:

- Введение в OSINT
- Пассивная и активная разведка
- Почему OSINT так важна в цифровую эпоху
- OSINT Framework
- Начало работы с OSINT и некоторые рекомендации

Я, словно Бэтмен, на всем протяжении главы буду сопровождать вас и приходить на выручку в трудный момент. Вы разберете наглядные примеры и советы профессионалов, узнаете, как не потеряться в общедоступной информации, извлекать данные и применять OSINT для достижения целей. В результате вы получите целый арсенал навыков, которые помогут пре-взойти конкурентов, усилить информационную защиту и уверенно ориен-тироваться в бескрайнем цифровом мире.

Готовы отправиться в увлекательное путешествие по OSINT? Скоро вы узнаете, насколько огромен потенциал разведки по открытым источникам!

Введение в OSINT

Разведка по открытым источникам, или, как ее часто называют, **OSINT** (Open Source Intelligence), — процесс сбора, оценки и интерпретации информации, находящейся в открытом доступе, который помогает найти ответы на конкретные вопросы, поставленные перед исследователем.

Поговорим об информации и разведке

На первый взгляд, информация (information) и данные, полученные в результате разведки (intelligence), кажутся одним и тем же, но на деле отличаются так же сильно, как сырье ингредиенты от готового обеда.

1. Информация: отправная точка.

Сначала нужно понять, что такое информация. Это необработанный материал, исходное сырье. Она окружает нас повсюду, принимая множество форм: мы читаем твиты, просматриваем новостные статьи и листаем публикации, переполняющие ленту в социальных сетях. Информации много, она разнообразна, а ее качество варьируется от высочайшего до совершенно непригодного. В мире OSINT все начинается именно с нее.

2. Данные разведки: готовое блюдо.

Если информация — сырье ингредиенты, то данные разведки — полноценный, с любовью приготовленный обед. Чтобы его получить, необходимо собрать информацию, проанализировать ее, понять с учетом контекста и преобразовать в нечто полезное и имеющее смысл. Цель анализа — интерпретировать данные, выявить закономерности, установить связи и, что самое важное, сформулировать выводы, применимые на практике.

3. Преобразование.

Превращение информации в данные разведки и есть OSINT. Это процесс, требующий высокого мастерства. Начав со сбора информации в открытых источниках, мы переходим к решающему этапу: проверяем ее подобно тому, как повар проверяет свежесть ингредиентов.

4. Анализ.

После проверки информацию необходимо проанализировать. Именно здесь происходит настояще волшебство. Мы выявляем в ней закономерности и аномалии, пытаясь добраться до сути. Сначала разделяем информацию на отдельные факты, а потом вновь объединяем их, чтобы

сформировать целостную картину, — как если бы мы смешивали ингредиенты для создания идеального блюда.

5. Интерпретация.

Наконец наступает этап интерпретации. Мы делаем выводы, оцениваем влияние данных разведки и, опираясь на них, принимаем решение и разрабатываем эффективную стратегию.

Пассивная и активная разведка

Давайте разберемся, в чем разница между пассивной и активной разведкой. Это два подхода к получению данных, но, несмотря на похожие цели, они могут иметь разные последствия для организации.

При пассивной разведке вы, словно призрак, наблюдаете за миром, не взаимодействуя с ним напрямую: перебираете общедоступную информацию, но не комментируете публикации, не пишете личных сообщений, не добавляйтесь в друзья и не подписываетесь на других пользователей. Вы, как подводная лодка, залегаете на дно и пеленгуете все вокруг.

В свою очередь, активная разведка подразумевает прямое взаимодействие с целью расследования: дружбу в социальных сетях, комментарии или даже общение в чате. Вы будто агент под прикрытием — и некоторые компании воспринимают активный OSINT именно так. Так что прежде чем бросаться в бой, обязательно заручитесь согласием руководителя.

Если выбор падет на активную разведку, вам придется смешаться с толпой, проявив максимум смекалки. «*Как же это сделать, Дейл?*» Сначала заведите учетные записи на разных платформах. Так вы будете похожи на рядового пользователя.

А дальше начинаются нюансы. В каждой организации может быть собственный регламент насчет того, какие способы разведки считать пассивными, а какие активными. Например, если вы вступите в закрытую группу Facebook, то для одних компаний останетесь сторонним наблюдателем, а другие могут расценить это как явное взаимодействие. Поэтому крайне важно знать, по каким правилам играет именно ваша организация.

Некоторые вообще уверяют, что участие в группе относится к пассивной разведке, пока вы лишь наблюдаете за происходящим и не общаетесь с людьми.

И как здесь не запутаться?

Почему OSINT так важна в цифровую эпоху

Сегодня OSINT используют органы власти, компании, некоммерческие организации и другие структуры. Разведка открывает немыслимые возможности: благодаря ей выявляются угрозы безопасности, проводятся маркетинговые исследования, анализируется деятельность конкурентов и не только.

Вот неполный список того, где пригодится OSINT:

- **Научные исследования.** OSINT помогает собирать данные на различные темы, например изучать общественное мнение, социальные тенденции и экономические показатели.
- **Бизнес и маркетинговые исследования.** Хотите выяснить, чем занимаются конкуренты, определить направление развития отрасли или узнать больше о поведении потребителей? Благодаря OSINT вы найдете информацию, которая подкрепит ваши решения и стратегии.
- **Безопасность и разведка.** С OSINT у вас на службе будет свой личный Шерлок Холмс, способный обнаружить террористическую деятельность или кибератаки. Кроме того, средства разведки пригодятся для слежки за иностранным правительством, различными организациями и преступными группировками.
- **Журналистские расследования.** Прибегая к стратегиям OSINT, журналисты могут распутывать скандалы, связанные с политикой, бизнесом, криминалом и не только.
- **Судебные разбирательства.** OSINT может значительно повлиять на судебный процесс, начиная со сбора доказательств и заканчивая поиском потенциальных свидетелей или обвиняемых.

В чем фишка OSINT?

Основное внимание в OSINT уделяется сбору открытой, официально доступной информации. Вам не придется тратить время и деньги на работу с засекреченными источниками или обход ограничений.

Вместо этого OSINT предлагает на выбор социальные сети, новостные статьи, отчеты правительств, научные работы и многое другое. Этого хватит, чтобы составить полную картину происходящего в различных сферах.

Еще одно достоинство — актуальность информации. Благодаря разведке в режиме реального времени вы будете в курсе последних событий и тенденций.

Кроме того, поиск данных по открытым источникам экономически эффективен. В отличие от агентурной и радиоэлектронной разведки, OSINT не требует дорогостоящего оборудования и специально обученных сотрудников, что существенно повышает его доступность.

Наконец, любую информацию, полученную средствами OSINT, легко проверить и подтвердить. Значит, полученные сведения будут достаточно достоверными и на них можно будет положиться.

Как же работает OSINT?

Если вам интересно, как вести разведку по открытым источникам, мы приоткроем для вас завесу тайны.

- Поиск.** Соберите информацию из различных источников, включая социальные сети, новостные статьи, отчеты правительства и коммерческие базы данных. Это можно делать вручную или с помощью автоматизированных инструментов.
- Обработка.** Отсейте неточные, неактуальные или дублирующиеся данные. Необходимо фильтровать и классифицировать находки с учетом их важности и актуальности.
- Анализ.** Изучите обработанную информацию, чтобы выявить закономерности и взаимосвязи. Вам помогут инструменты для визуализации и интеллектуального анализа данных, а также обработки естественного языка.
- Распространение.** На последнем этапе поделитесь выводами с теми, кто принимает решения. В зависимости от потребностей организации формат данных разведки может быть разным, например полные отчеты, сжатые обзоры или краткие уведомления.

Весь фокус OSINT — в непрерывности цикла: вы постоянно собираете информацию, совершенствуете ее обработку и анализ, учитывая новые данные и обратную связь. Разумеется, инструмент не идеален, он имеет те же ограничения, что и другие методы исследований. Поэтому необходимо привлекать опытных аналитиков, способных грамотно интерпретировать извлеченные данные.

Под покровом OSINT скрывается масса методов сбора и анализа данных. Вкратце опишем некоторые из них.

- Социальные сети.** Twitter, Facebook, LinkedIn и другие похожие платформы — не просто площадки для онлайн-тусовок. Благодаря им можно

отслеживать тенденции, оценивать настроение общественности, а иногда выявлять потенциальные угрозы.

- **Веб-скрейпинг.** Это автоматический сбор информации, похожий на работу золотоискателя в цифровом пространстве. В ход идут специализированные программы, позволяющие быстро и систематически извлекать из сайтов тонны данных.
- **Поисковые системы.** В старых добрых поисковых системах вроде Google есть расширенный поиск, который помогает получать более точные результаты. Иногда такой процесс называют Google Dorking¹.
- **Юридические документы.** Сундук, битком набитый ценной информацией. Судебные материалы, свидетельства о собственности и документы компаний могут многое рассказать как об организациях, так и об обычных людях.
- **Новости.** Традиционные СМИ, например газеты, журналы и новостные сайты, — настоящая сокровищница. Они помогают держать руку на пульсе и быть в курсе текущих событий, новых тенденций и потенциальных проблем.
- **Инструменты анализа данных.** Excel, Tableau и R незаменимы при работе с огромными массивами данных. Эти и другие инструменты помогают отсеять лишнюю информацию и выявить закономерности и взаимосвязи.

Помните, что OSINT не стоит на месте. Чтобы эффективно собирать и анализировать данные, необходимо следить за появлением новых технологий и источников данных, а также осваивать новейшие методы и инструменты разведки.

OSINT Framework

Фреймворк разведки по открытым источникам, известный как OSINT Framework (<https://osintframework.com/>), — потрясающая платформа для тех, кто осваивает сбор информации. Это обновляемый онлайн-каталог ресурсов для OSINT в форме, удобной для восприятия и навигации.

Фреймворк разработал Джастин Нордин (Justin Nordine), уважаемый человек в сфере кибербезопасности. Он хотел систематизировать и рассказать

¹ Google Dorking — использование расширенных поисковых операторов Google для поиска специфической информации, часто такой, которая не предназначена для публичного доступа. — Примеч. пер.

всем об имеющемся изобилии инструментов для разведки по открытым источникам. OSINT Framework постоянно обновляется благодаря совместным усилиям специалистов по кибербезопасности и широко используется ими по всему миру.

Открыв сайт OSINT Framework, вы увидите интерактивную диаграмму связей. Она начинается с общих категорий, перейдя по которым вы попадете к спискам конкретных ресурсов и инструментов. Благодаря такой структуре можно без труда найти, например, социальные сети, специализированные поисковые системы, утекшие базы данных, правительственные ресурсы — все что угодно.

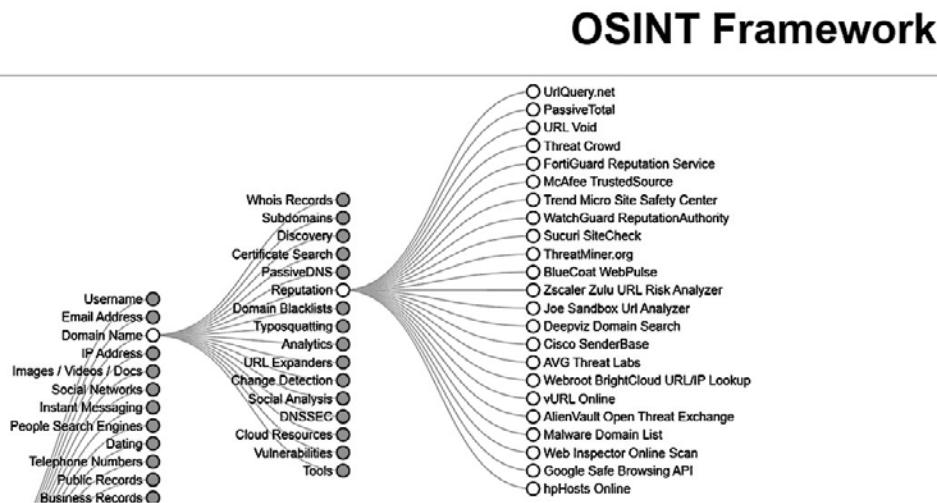


Рис. 1.1. OSINT Framework (<https://osintframework.com/>)

Для специалистов в сфере безопасности OSINT Framework просто незаменим. Он предлагает множество инструментов для сбора информации, с которых удобно начать расследование или оценку степени защищенности компании. Распределение по категориям помогает быстро находить подходящие ресурсы и тем самым экономит ценнное время на ранних этапах разведки.

Стоит отметить, что сам фреймворк не является инструментом. Он, скорее, напоминает карту сокровищ, которая показывает путь к другим полезным ресурсам OSINT. С каждым из них важно обращаться ответственно: помните, что необходимо уважать конфиденциальность других людей и действовать в рамках закона.

OSINT Framework привлекателен из-за своей простоты и широкого охвата ресурсов. Его регулярно обновляют, благодаря чему он остается ценным сайтом для специалистов в области безопасности и всех, кто интересуется разведкой по открытым источникам. OSINT Framework стал ярким примером того, как важно сотрудничать и обмениваться информацией.

Разведка на примере реальных ситуаций

Как насчет фишингового электронного письма? Выявление его отправителя могло бы выглядеть так:

1. **Первичный анализ.** Получатель фишингового письма заметил что-то подозрительное и сообщил об этом в службу безопасности.
2. **Анализ метаданных электронного письма.** Специалисты по безопасности проанализировали заголовок письма и извлекли такие метаданные, как IP-адрес отправителя, метку времени и маршрутную информацию.
3. **Поиск IP-адреса.** Информацию об IP-адресе сопоставили с данными из общедоступных источников OSINT, включая реестры доменных имен, базу данных WHOIS и сервисы репутации IP.
4. **Анализ цифрового следа.** Специалисты изучили социальные сети, онлайн-форумы и сайты, чтобы выявить любое присутствие в Сети, связанное с этим адресом IP или электронной почты.
5. **Анализ собранной информации.** Информацию, полученную из открытых источников, объединили и проанализировали, чтобы найти взаимосвязи и закономерности.
6. **Установление источника и отчетность.** На основе собранных доказательств специалисты определили вероятный источник фишингового письма. Они подготовили подробный отчет, содержащий всю необходимую информацию и рекомендации по устранению угрозы.

А как с помощью OSINT отследить утечку данных?

1. **Обнаружение проблемы.** Организация обнаруживает утечку данных с помощью систем внутренней безопасности или благодаря чьему-то сообщению.
2. **Сбор индикаторов компрометации.** Из взломанной системы или внешних источников собираются фрагменты похищенных данных, псевдонимы хакеров и другие индикаторы.

- **Фрагменты похищенных данных.** Злоумышленники нередко публикуют часть утекших данных, чтобы продемонстрировать доступ к информации и убедить людей в своих возможностях. OSINT помогает найти такие фрагменты на различных платформах, например общедоступных сайтах, форумах или даркнет-рынках, где данные могут продаваться или распространяться. Используя средства разведки по открытым источникам, специалисты по кибербезопасности выявляют и анализируют фрагменты похищенных данных, чтобы определить масштабы и характер взлома.
 - **Псевдонимы хакеров.** Киберпреступники часто создают специальный онлайн-образ или действуют под псевдонимами. Информацию о них можно найти с помощью разведки по открытым источникам, включая социальные сети, форумы и чаты. Во время поиска и анализа специалисты по кибербезопасности могут выявить связи, закономерности или историю действий, связанные с псевдонимами. Это, в свою очередь, поможет установить личности злоумышленников или предполагаемые мотивы взлома.
 - **Анализ взломанных систем.** OSINT также помогает собрать индикаторы компрометации из самой взломанной системы. Изучая журналы событий, сетевой трафик и другие цифровые артефакты, специалисты могут обнаружить следы злоумышленников, например IP-адреса, инфраструктуру управления и контроля (**C2¹**) и сигнатуры вредоносного ПО, которые дают ценные сведения о взломе. Средства OSINT позволяют сопоставить найденные индикаторы с информацией из общедоступных источников и тем самым узнать больше о преступниках и их методике.
3. **Просмотр даркнета.** С помощью инструментов OSINT просматриваются форумы, маркетплейсы и чаты даркнета в поисках любых упоминаний похищенных данных или связанных с ними действий.
 4. **Просмотр социальных сетей.** В общедоступных социальных сетях идет поиск обсуждений, публикаций или комментариев, которые могут дать представление об утечке или злоумышленниках.
 5. **Анализ похищенных данных.** Если фрагменты похищенных данных общедоступны, с помощью методов OSINT анализируется их содержание, в том числе имена пользователей, электронные адреса и другие данные, способные раскрыть личность злоумышленников и помочь в расследовании.

¹ C2 – C&C, Command and Control. – Примеч. пер.

6. **Установление источника и сотрудничество.** Результаты разведки передаются для совместного расследования заинтересованным сторонам: правоохранительным органам, компаниям, специализирующимся на информационной безопасности, или отраслевым организациям.
7. **Правовые меры или устранение последствий.** На основе разведанной информации и найденных доказательств принимаются правовые меры или устраняются последствия взлома. Это позволяет минимизировать ущерб и предотвратить будущие инциденты.

Возможно, теперь вы лучше понимаете, чем OSINT полезен вам и вашей организации.

Начало работы с OSINT и некоторые рекомендации

Разведка по открытым источникам предоставляет ценную информацию и широкие возможности для расследования. Мы собрали несколько полезных советов, идей и ресурсов, которые помогут вам освоить OSINT и заложить прочную основу для исследований.

Полезные советы по сбору информации

Прежде чем начать сбор сведений, определите цель поиска и результаты, которых хотите достичь. Это поможет сфокусироваться на главном и упростит работу. Не бросайтесь в бескрайние дебри информации без структурированной методологии.

Разбейте исследование на логические этапы, чтобы охватить все важные аспекты. При сборе информации обращайтесь к различным источникам: поисковым системам, социальным сетям, юридическим документам, сайтам правительства, специализированным инструментам OSINT и не только. Пропроверяя данные в нескольких источниках, вы повысите точность результатов и сократите риск получения недостоверных сведений.

Учитесь составлять более эффективные поисковые запросы. Операторы, фильтры и расширенные функции поисковых систем помогут сократить объем данных и получить более релевантные результаты.

Изучайте метаданные изображений, документов и других файлов. Анализируя их, вы можете обнаружить ценную информацию, например местоположение, метки времени, данные об авторе или особенностях устройства.

Еще одна хитрость: научитесь находить цифровые следы. Профили в социальных сетях, онлайн-форумы, публикации в блогах и общедоступные документы могут дать исчерпывающее представление об объекте. Не волнуйтесь, потом я покажу, как это делать.

Подробно фиксируйте свои находки, включая метки времени, URL, скриншоты и заметки. Такая систематизация повысит эффективность анализа и поможет без труда находить сохраненную информацию.

Ресурсы, которые нам пригодятся

Хотите узнать, чем раньше занимался кандидат на вакансию? Или определить, опасен ли сайт? Популярные инструменты OSINT помогут собрать информацию для различных целей. Пополнив ими свой арсенал, вы сможете оптимизировать исследование и обнаружить ценные факты для принятия решения. Помните, что главное преимущество OSINT заключается в его способности превращать разрозненную общедоступную информацию в полезные данные. Предлагаем вам *список Дэйла* – 12 лучших инструментов OSINT, с которыми мы будем работать.

- Maltego: <https://www.maltego.com/>
- SpiderFoot: <https://intel471.com/solutions/attack-surface-protection>
- Intelligence X: <https://intelx.io/>
- Shodan: <https://www.shodan.io/>
- OSINT Framework: <https://osintframework.com/>
- Metagoofil: <https://github.com/opsdisk/metagoofil>
- Lampyre: <https://lampyre.io/>
- Spokeo: <https://www.spokeo.com/>
- Recon-ng: <https://github.com/lanmaster53/recon-ng>
- Mitaka: <https://github.com/ninoseki/mitaka>
- Babel Street: [https://wwwbabelstreet.com/](https://wwwbabelstreet.com)
- Seon: <https://seon.io/>

Примечание

Я уже рассказывал о ресурсе OSINT Framework (<https://osintframework.com/>). На нем представлено впечатляющее изобилие сайтов и инструментов для разведки, список которых постоянно обновляется. В этой книге фреймворк OSINT будет упоминаться часто – уж поверьте.

Итоги

Вы познакомились с OSINT и узнали, чем она заслужила такое внимание и почему особенно ценится в современную эпоху. Ее, как и всякую суперспособность (инструмент), можно использовать как во благо, так и во вред — и делать это с соблюдением или с нарушением норм. Мы поговорили о том, как собирать данные ответственно, не пересекая этические и правовые границы. Ведь неосмотрительность еще не помогла ни одному защитнику информационной безопасности!

Затем мы закатали рукава и взяли кое-что посерьезнее — примеры OSINT в действии. Вы увидели, как с ее помощью обнаружить источник фишинга или расследовать утечку данных.

Наконец мы дали несколько полезных советов и ресурсов для подготовки к разведке. Пусть с этого набора начнет пополняться ваш собственный арсенал.

Вот о чём была глава 1. Отличная отправная точка в мир разведки OSINT. Далее мы обсудим методы и техники получения данных.

ГЛАВА 2

НЕВИДИМЫ И НЕДОСЯГАЕМЫ: ПОЧЕМУ ВАЖНО СОХРАНЯТЬ АНОНИМНОСТЬ

Технологии **разведки по открытым источникам (OSINT)** постоянно развиваются, и в этих обстоятельствах анонимность — не просто рекомендация, а обязательное условие для успешного выполнения работы. Во второй главе мы поговорим именно об этом. Изучив каждый раздел, вы поймете, почему в процессе сбора информации так важно обеспечивать собственную конфиденциальность. К концу главы у вас будет достаточно знаний и навыков, чтобы во время разведки сохранять анонимность, не оставлять цифровой след и безопасно взаимодействовать с другими людьми.

В этой главе мы рассмотрим следующие темы:

- Основы анонимности и конфиденциальности в OSINT
- Защита цифрового следа
- Предупреждение киберугроз

Основы анонимности и конфиденциальности в OSINT

Разведка по открытым источникам подразумевает извлечение информации из общедоступных ресурсов. Однако OSINT-аналитики должны действовать анонимно и сохранять конфиденциальность, ведь причин для такой осторожности немало. Давайте посмотрим, какие меры — и почему — необходимо принимать во время разведки.

- **Сохраняйте секретность.** Если представители организаций или обычные люди узнают, что кто-то пытается найти о них информацию, они могут постараться этого избежать, например удалить публикации в социальных сетях, ограничить видимость профиля, приостановить работу сайтов или даже уничтожить доказательства. Анонимность во многом поможет скрыть факт наблюдения.
- **Не компрометируйте расследование.** Аналогично, если объект разведки обнаружит слежку, он может изменить поведение или способы коммуникации. Это может существенно затруднить сбор необходимой информации и тем самым помешать расследованию. Анонимность помогает избежать такого развития событий.
- **Не препятствуйте незаконной деятельности.** Скомпрометировав расследование на ранних этапах, вы можете помешать правоохранительным органам выявить преступный сговор или собрать доказательства для привлечения к ответственности. Пусть злоумышленник продолжает незаконную деятельность, но уже под наблюдением. Анонимность — важная составляющая незаметной слежки.
- **Соблюдайте юридические и этические нормы.** В некоторых штатах и странах слия информации объекту о расследовании в его отношении может обернуться для вас уголовным наказанием. Анонимность позволяет исключить непреднамеренное нарушение этических и юридических норм.
- **Обеспечьте безопасность аналитиков и источники информации.** Хакеры, террористы и другие преступники могут попытаться расправиться с аналитиками и информаторами, которые фигурируют в расследовании. Анонимность и конфиденциальность помогают защитить их.
- **Не допускайте утечки данных.** Секретная информация не должна попадать в чужие руки, а это возможно только при строгих процедурах доступа и управления. Чтобы предотвратить утечку данных и возможные катастрофические последствия, необходимо применять надежные меры по защите конфиденциальности.

Как может быть нарушена анонимность

Как же вас могут обнаружить во время расследования? Есть несколько слабых мест:

- **IP-адрес.** По IP-адресу легко определить ваше местоположение и идентифицировать личность. Если не маскировать ваш реальный IP-адрес с помощью VPN или браузера Тор, сайты будут его фиксировать.

Расскажу вам один случай. Я исследователь в области кибербезопасности и как-то раз столкнулся с непростой задачей. Нужно было найти информацию о кибератаках, которые совершались из определенного региона. Чтобы обнаружить источник и не привлекать внимание, я решил использовать **виртуальную частную сеть (VPN)**, Virtual Private Network). Так я подключился к серверу в другой стране и тем самым скрыл настоящий IP-адрес и местоположение. Казалось, будто я захожу в интернет из региона, в котором расположен этот сервер. В результате я мог спокойно собирать информацию на различных сайтах и форумах, не раскрывая свою личность. Этот случай показал мне, насколько эффективно VPN защищает мою конфиденциальность в цифровом пространстве, особенно при исследовании тем деликатного характера.

- **Отпечаток браузера.** Браузеры собирают невероятное количество данных: от разрешения экрана до списка установленных плагинов. На их основе можно создать уникальный *отпечаток* (также «фингерпринт»). Не верите? Оторвитесь от книги и зайдите на privacy.net/analyzer. Видите? Я же говорил! И если вы считаете, что режим инкогнито вас защитит, — как бы не так. Отпечаток браузера все равно позволяет отслеживать ваши действия независимо от сеанса.

The screenshot shows the homepage of privacy.net. At the top, there's a navigation bar with links for HOME, ANALYZER, and ABOUT. Below the header, a descriptive text explains what the tool does: "What information can a website find out about you when you visit it? A lot more than you probably realize. This tool lists information that any website, advertisement, and widget can collect from your web browser. Such information could be used to identify you and/or track your behavior using tactics like IP lookups and browser fingerprinting. While none of this may be considered personally identifiable information (P), the profile drawn from all these pieces of information can be so distinct that it can only plausibly match a single person." A section titled "Tests" follows, with a sub-section "Basic Info". A progress bar indicates the user is at step 1 of 5. The "Basic Info" section displays the following results: "You are using a Laptop or Desktop running Win32 OS. Your browser is Chrome 119 and resolution is set to 1285x1309. Your Laptop or Desktop has 100% battery remaining."

Рис. 2.1. Мои результаты на сайте privacy.net/analyzer

- **Чрезмерная уверенность в технологиях.** Полагаясь только на инструменты вроде VPN и Тор, но не понимая их ограничений, вы можете обрести ложное чувство безопасности. Например, нередко VPN-сервисы все-таки фиксируют данные пользователей: IP-адреса, действия, метки времени и многое другое, несмотря на их заверения о том, что они *не записывают логи*. В некоторых случаях трафик, проходящий через Тор, могут деанонимизировать влиятельные противники — скажем, правительственные службы. Когда дело касается анонимности, не бывает идеального решения. Необходимо комбинировать сразу несколько инструментов или подходов и учитывать слабые места каждого из них.
- **Файлы cookie.** Это небольшие текстовые файлы, которые сайты размещают на вашем устройстве, чтобы отслеживать и запоминать ваши действия в Сети. С одной стороны, весьма удобно, когда сайты сохраняют данные для входа и содержимое корзины, но с другой — благодаря файлам cookie компании создают подробные портреты пользователей с информацией об их привычках, интересах, поведении и других характеристиках, которую вы оставляете на множестве сайтов и в течение разных сессий. Регулярно очищая файлы cookie, можно ограничить отслеживание, но компании уже разработали более продвинутые методы, включая отпечатки браузера и устройства (по технологии Canvas), которые от этих файлов не зависят.

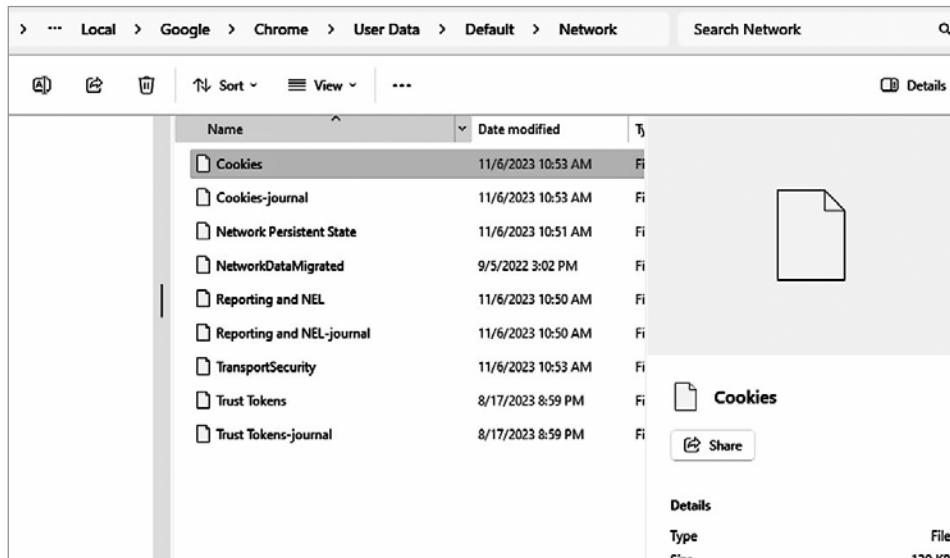


Рис. 2.2. Файлы cookie могут храниться в разных местах и при этом могут содержать довольно много сведений

Чтобы избежать наблюдения, важно использовать Тор и другие браузеры, предназначенные для конфиденциального просмотра веб-страниц, а также время от времени менять свою модель поведения в Сети.

- **Утечки метаданных.** Фото, аудио, видео, документы и другие файлы содержат метаданные — информацию о самом файле, созданную вашим устройством. Так, например, могут сохраняться геотеги, метки времени, серийные номера устройств, история редактирования и многое другое. А в заголовках электронных писем раскрывается IP-адрес, информация о клиенте и т. д. В случае утечки метаданные могут выдать информацию о вашей личности и нарушить анонимность. Поэтому перед публикацией файла необходимо удалять их с помощью специальных инструментов. Кроме того, важно избегать способов коммуникации, которые раскрывают метаданные.

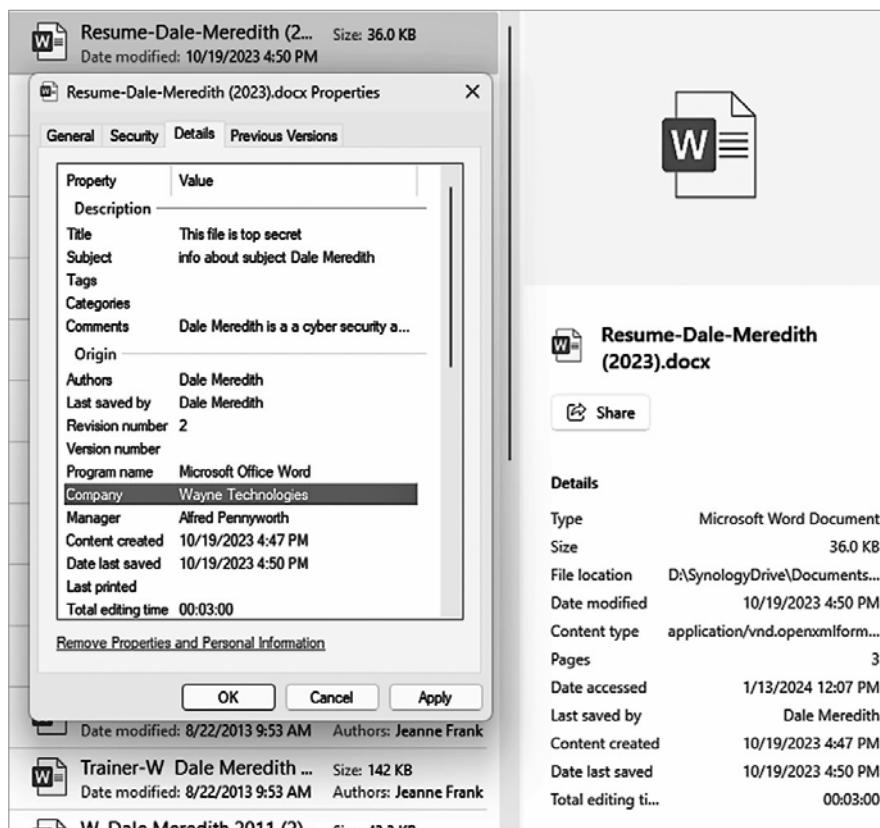


Рис. 2.3. Пример метаданных в файле

- **Незащищенные общественные сети Wi-Fi.** В кофейнях, аэропортах, отелях и других местах сеть Wi-Fi часто не имеет пароля или вообще никак не защищена. В результате любой человек поблизости может перехватить незашифрованный трафик и подсмотреть, что вы делаете в интернете. Подключившись к незащищенной общественной сети Wi-Fi, никогда не входите в учетные записи, содержащие конфиденциальную информацию, например электронную почту или банковские приложения. И обязательно шифруйте трафик при помощи надежного VPN. А еще лучше — придержите конфиденциальные данные до тех пор, пока не подключитесь к знакомой защищенной сети.
- **Социальная инженерия.** В то время как технические средства защиты продолжают развиваться, сам человек остается уязвимым перед обычными методами социальной инженерии вроде фишинга. Не используйте одни и те же пароли в разных учетных записях, включите многофакторную аутентификацию (если это возможно), общайтесь по каналам с шифрованием PGP и научитесь распознавать подозрительные ссылки и вложения. Ни один инструмент для обеспечения анонимности не в силах защитить вас от опрометчивых поступков.
- **Учетные записи для OSINT.** Одна из грубейших ошибок во время OSINT или исследования в сфере кибербезопасности — использовать учетную запись, по которой можно вас вычислить. При разведке в поисковых системах, социальных сетях, на форумах и других онлайн-площадках обязательно заводите анонимные одноразовые учетные записи и маскируйте IP-адреса. Строго разделяйте личную интернет-активность и действия, связанные с расследованиями.
- **Оплошности.** Разрушить свою анонимность легко — достаточно один раз нечаянно раскрыть личную информацию в чате, на форуме или другой площадке для общения. Поэтому будьте предельно осторожны, сообщая данные, по которым можно вас вычислить. Кроме того, тщательно разделяйте своих анонимных персонажей: если использовать одинаковые логины, пароли или схожие электронные адреса для разных учетных записей, установить между ними связь будет проще. Стоит лишь на мгновение потерять бдительность и...
- **Устаревшие знания.** Новые способы взлома, эксплойты и уязвимости появляются постоянно. Если не следить за появлением новых угроз конфиденциальности и безопасности, вашу информацию могут похитить методами, о которых вы еще не знаете — и от которых не защитились. Чтобы этого не произошло, никогда не полагайтесь на текущие знания: обучение должно быть непрерывным. Как мы говорили, рассчитывая на

технологии вроде VPN или Tor, но не понимая их ограничений, вы рискуете обрести ложное чувство безопасности. Помните? Некоторые сервисы VPN фиксируют действия пользователей, да и трафик, проходящий через Tor, не защищен на все сто.

Подведем итоги: конфиденциальность в OSINT

Слушайте, технологии всегда меняют расклад («*Да неужели, Дейл!*»). Они помогают вывести на чистую воду преступников, негодяев и заклятых врагов, но, если действовать неосмотрительно, эти же технологии могут распахнуть двери в нашу личную жизнь.

Нужна система, предусматривающая контроль, проверки, ограничения и, что самое важное, ответственность. Нельзя раздавать мощные инструменты без четких правил. И эти правила должны быть прозрачными, чтобы каждый из нас мог отстоять свои права, если посчитает их нарушенными.

У технологий нет морального компаса — они лишь средство достижения цели. Это мы должны мыслить, действовать этично и, прежде всего, сохранять бдительность. Ведь мы играем в долгую. Если отказаться от принципов ради сиюминутной выгоды, в конечном счете мы понесем значительные потери. Нужно помнить, ради чего мы все это делаем — ради общества, в котором свобода и безопасность идут рука об руку. Именно это хрупкое равновесие стоит наших усилий, друзья. Ладно, довольно проповедей. Думаю, вы меня поняли.

Защита цифрового следа

Цифровой след похож на тень в солнечные дни: он постоянно следует за вами, приобретая новые формы. Но зачастую эта тень показывает больше, чем хотелось бы. Ваша личная информация, включая домашний адрес и паспортные данные, всего в одном клике от посторонних глаз. Да, вы этого не хотели. Но так получилось, и это тревожный факт.

Как ограничить СВОЕ присутствие в интернете

Прежде чем приступить к разведке по открытым источникам, нам, специалистам по безопасности, важно понять, как защитить себя во время расследования. Вы знали, что примерно 91 % киберпреступлений начинается с простого электронного письма? (Источник: <https://www.yeoandyeo.com/resource/91-of-cyberattacks-begin-with-a-phishing-email.>)

Может, поначалу злоумышленник и не знает вашего имени. Но, получив больше данных, он способен составить полную картину о вашей цифровой личности. В современном мире данные ценятся так же высоко, как нефть. И легкость, с которой посторонний может получить информацию о вас, не только вызывает беспокойство, но и подталкивает к действию.

Вашими личными данными могут воспользоваться киберпреступники, недоброжелатели и алчные корпорации. Даже если данные не проданы напрямую, ежедневные действия в интернете раскрывают сведения о вас. Каждый поисковый запрос в Google, каждая публикация в социальных сетях и даже товар, который вы просматриваете в маркетплейсе, дополняют ваш портрет — а вы об этом ни сном ни духом.



Рис. 2.4. Google отслеживает ваше местоположение с помощью телефона
(<https://timeline.google.com/>)

Почему сегодня так важно защищать личные данные

Уязвимость цифровых данных может проявиться *не сразу*. Ее последствия долгосрочны, включая кражу личности и даже угрозу личной безопасности. Невозможно представить, чем обернется утечка. Что, если злоумышленник под вашим именем оформит кредит, заключит незаконную сделку или даже

совершит преступление? Вернуть себе добрую репутацию будет крайне трудно — не только финансово, но и психологически.

Уязвимость данных значительно влияет и на личную жизнь. Например, если потенциальный работодатель обнаружит неточную или малоприятную информацию о вас, его впечатление испортится еще до того, как вы продемонстрируете свои способности.

Ставки высоки, и шансы (увы!) не в вашу пользу. Но отчаиваться рано. Позвольте дать вам несколько советов, которые помогут не только повысить цифровую грамотность, но и действовать увереннее в цифровом мире. Ваша личная информация бесцenna — давайте относиться к ней именно так.

Браузеры: первая линия уязвимости

Браузер — ваш внимательный цифровой штурман, который поможет добраться до пункта назначения по оживленной информационной магистрали. Именно в браузере вы читаете новости, смотрите видео, спорите в социальных сетях и делаете многое другое. Однако под удобным интерфейсом скрывается система сбора данных, которой позавидовала бы любая шпионская контора. Нет, я не собираюсь пичкать вашу голову теориями заговора. Но запомните: «*Если я не вижу, что за мной следят, это не значит, что за мной не следят!*»

Основные и сторонние файлы cookie

Да, наш браузер пожирает разные типы файлов cookie:

- **Основные файлы cookie** (first-party cookies). Создаются сайтом, который вы посещаете. Запоминают ваши настройки, содержимое корзины и т. д.
- **Сторонние файлы cookie** (third-party cookies). Создаются не тем сайтом, на котором вы находитесь, а другим — например, рекламным сервисом. Именно с их помощью компании отслеживают ваши действия в интернете и предлагают ту самую обувь, которую вы когда-то посмотрели, но не купили.

Знакомьтесь: граббер файлов cookie

Граббер файлов cookie (cookie grabber) — инструмент, предназначенный для их похищения. В чем его опасность? Он может перехватывать как основные, так и сторонние файлы cookie, даже те, что содержат секретную информацию, например данные для входа.

Допустим, вы открываете сайт со встроенным граббером. Без тени сомнения вы входите в систему, и у вас тут же похищают временные файлы cookie.

Теперь у злоумышленников есть ключ к вашему цифровому королевству и доступ к учетным записям на других платформах — и все это в результате простой незаметной кражи.

Причин для тревоги все больше и больше. Давайте обсудим сайты, которые хранят учетные данные — имена пользователей и пароли — в виде обычного текста прямо в браузере. Прозвучит технически сложно, но вот в чем суть: иногда сайт сохраняет их в формате, который может прочитать любой желающий. Если вы работаете на чужом компьютере или кто-то получил доступ к вашему, этот человек может посмотреть учетные данные с помощью простого инструмента вроде hex-редактора. Это все равно что положить ключи от дома на скамейку и уйти.

Представьте: вы входите в учетную запись на сайте, владельцев которого совершенно не волнует ваша конфиденциальность. Данные для входа сохраняются в файлах cookie в виде обычного текста. И вы даже не догадываетесь о том, что какой-нибудь хакер или любопытный сосед по комнате может с легкостью извлечь эту информацию и войти в вашу учетную запись, как в свою собственную.

.casalemedia.com	TRUE	/	FALSE	2597573456	CMPRO	5499
.lijit.com	TRUE	/	FALSE	2597573456	ljt_reader	GZyPuLZH0kCSSIDSVGbeDx9
.facebook.com	TRUE	/	FALSE	2597573456	datr	
.facebook.com	TRUE	/	FALSE	2597573456	c_user	
.facebook.com	TRUE	/	FALSE	2597573456	sb	
.facebook.com	TRUE	/	FALSE	2597573456	xs	
.facebook.com	TRUE	/	FALSE	2597573456	fr	
.facebook.com	TRUE	/	FALSE	2597573456	wd	
.c.bing.com	TRUE	/	FALSE	2597573456	MR	0

Рис. 2.5. С помощью граббера файлов cookie можно присвоить себе чужую учетную запись или личность

Как защитить себя

Считается, что VPN и цепочки прокси-серверов эффективно сохраняют конфиденциальность. Они помогают скрыть настоящий IP-адрес и мешают сторонним файлам cookie отслеживать ваши действия в Сети. Это особенно ценится в современную цифровую эпоху, где веб-трекинг и нарушение конфиденциальности стали основными проблемами. Однако важно, чтобы поставщики VPN и прокси были надежными, ведь у них будет доступ к данным, которыми вы обмениваетесь в интернете. Всегда выбирайте сервисы, которые известны строгой политикой конфиденциальности и отличаются заботой о безопасности пользователей.

DuckDuckGo: невоспетый герой конфиденциальности

Пока распространенные браузеры ищут внимания в цифровом мире, словно звезды реалити-шоу, DuckDuckGo держится в стороне — гений, о котором никто не слышал (а стоило бы). Его миссия — повысить конфиденциальность в интернете. Бесстрашные профессионалы блокируют скрытые системы, которые отслеживают ваши действия. Встроенный брандмауэр пресекает попытки собрать историю поиска и личную информацию.

Все продукты DuckDuckGo созданы для того, чтобы вы могли контролировать свои данные: поисковая система никогда не сохраняет историю запросов и информацию о пользователях, а введенные запросы конфиденциальны по умолчанию. Кроме того, есть расширение для браузера и мобильное приложение, которые активно блокируют трекеры, скрывающиеся на сайтах и посягающие на вашу информацию.

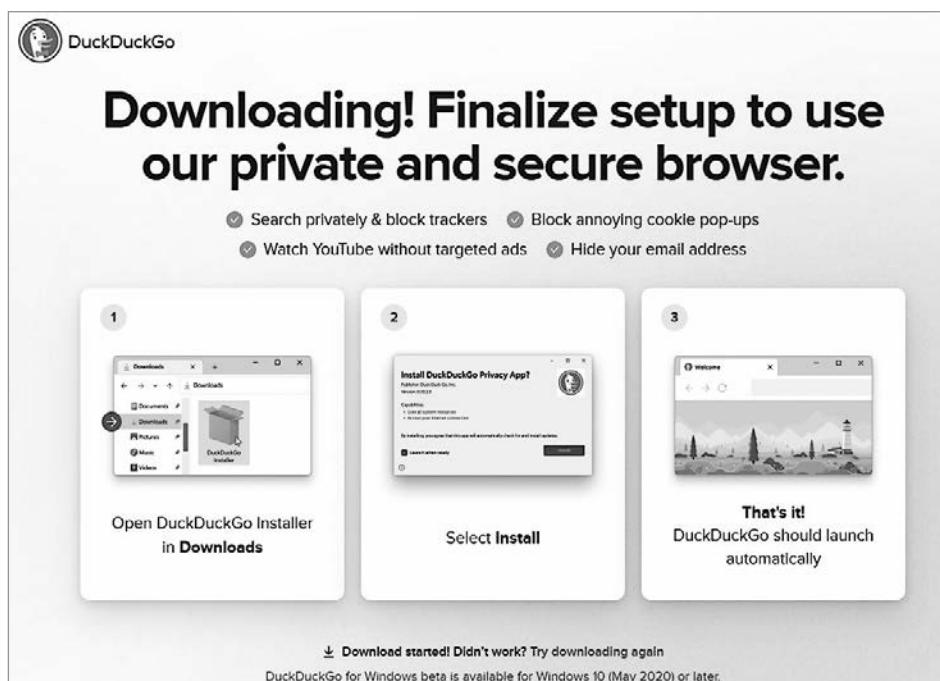


Рис. 2.6. DuckDuckGo — отличный браузер, который поможет скрыться

Еще один уровень защиты возможен благодаря шифрованию соединения между браузером и сайтом. Вместе эти инструменты окружают вас барьером,

который не позволяет рекламным сервисам и другим сторонним компаниям собирать интересующую их информацию о вас.

DuckDuckGo зарабатывает, показывая рекламу на основе ключевых слов из поискового запроса, поэтому браузеру незачем создавать портреты из личных данных. Бизнес-модель соответствует миссии компании: конфиденциальность превыше всего.

Ну что, готовы к переходу на новый браузер? Прекрасно. Однако разорвать старые отношения и начать новые невозможно без некоторой подготовки. Вот что потребуется:

- Скачивание и установка.** Установите браузер, ориентированный на конфиденциальность.
- Импортирование настроек.** Большинство браузеров позволяют импортировать закладки и настройки.
- Выбор по умолчанию.** Укажите новый браузер в качестве основного для своих цифровых похождений.

Альтернативные браузеры: плюсы и минусы других программ

А теперь давайте перестанем превозносить DuckDuckGo как единственного супергероя. Есть и другие варианты, каждый со своими преимуществами и недостатками.

Браузер Brave

Браузер, который я рекомендую всем. Своего рода новичок на рынке.

Brave (<https://brave.com/>) создан для защиты конфиденциальности и хорошо подходит тем, кто только начинает скрывать действия в Сети. Этот браузер по умолчанию блокирует трекеры, что мешает сторонним сервисам за вами следить.

Если не хочется менять браузер, посмотрите расширения вроде Startpage — они выполняют аналогичные функции.

Startpage оценивает уровень конфиденциальности по шкале от одного до пяти, показывая, сколько трекеров и файлов cookie было обезврежено. Результаты могут шокировать, но в итоге придадут сил. Кроме того, Startpage скрывает вашу личность от оставшихся трекеров, маскируя цифровой отпечаток.

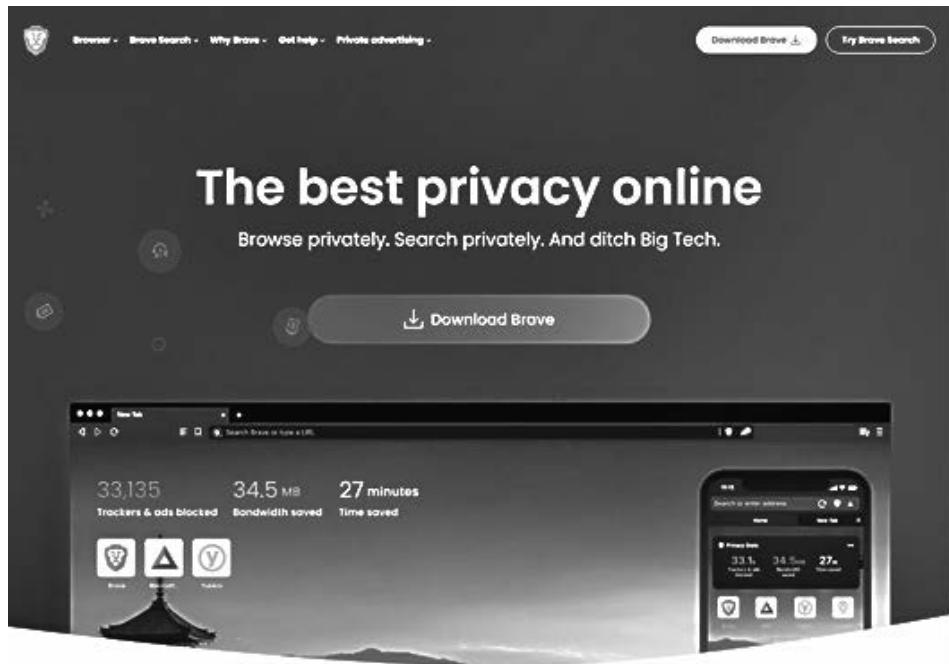


Рис. 2.7. Brave — мой выбор для защиты конфиденциальности

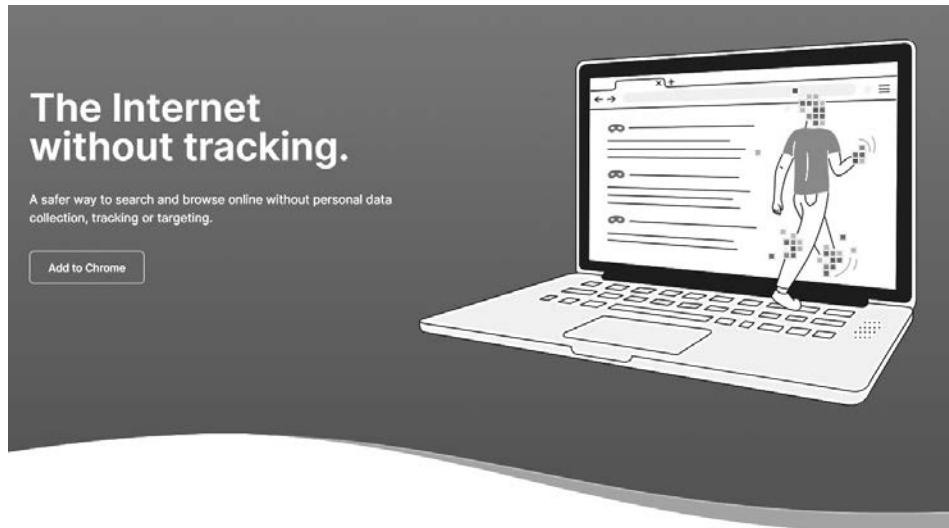


Рис. 2.8. Расширение Startpage доступно в интернет-магазине Chrome

Возможно, вы захотите блокировать не все трекеры, ведь некоторые файлы cookie безвредны и помогают сайтам правильно работать. Startpage позволяет одобрять только отдельные файлы cookie вместо того, чтобы принимать их все. Тем, кто активно использует поисковые системы, может понравиться, что Startpage отправляет запросы анонимно, так что они не дополняют портрет вашей цифровой личности.

Таким образом, с надежной защитой Brave и информацией от Startpage вы получите мощное оружие для уничтожения своей цифровой тени и больше не будете безвольной жертвой трекеров. Посмотрите, в чем плюсы и минусы этого браузера:

- **Плюсы:** по умолчанию блокирует рекламу и трекеры.
- **Минусы:** встроенная система рекламы понравится не каждому.

Браузер Tor

Tor (The Onion Router) — интернет-сообщество, объединенное стремлением защитить конфиденциальность в Сети. Оно появилось как символ свободы и сопротивления: пока правительство следит за своими гражданами, а корпорации собирают информацию, Тор борется за приватность. Это всемирное движение добровольцев, которые помогают анонимизировать трафик с помощью собственных серверов, ретрансляторов и узлов. Ни один элемент в цепочке не может отследить полный путь данных.

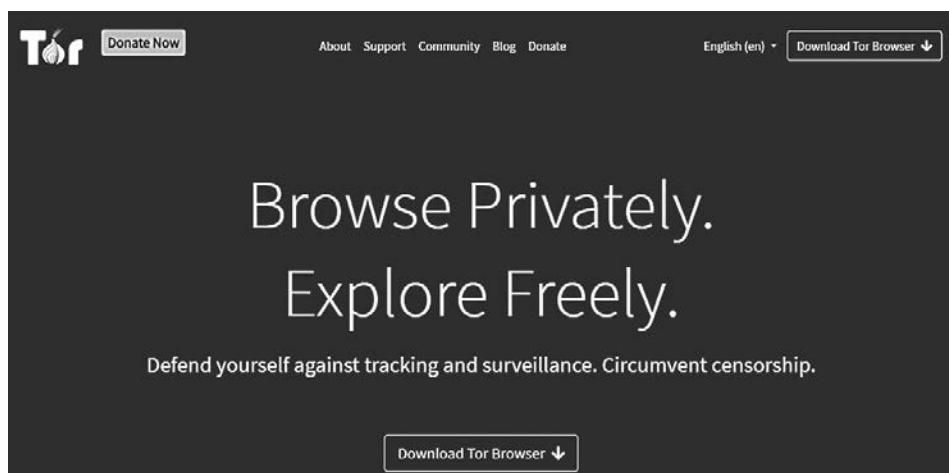


Рис. 2.9. Сайт Тор

Тор подчищает метаданные и маскирует IP-адреса. Трафик, проходящий через частную сеть, шифруется снова и снова. Ретрансляторы создают многослойную¹ защиту: каждый узел знает лишь то, откуда он получил данные и куда должен их передать. Конечный адрес неизвестен.

Такой подход возможен только благодаря большому числу участников, поэтому тысячи добровольцев самоотверженно запускают узлы Тор на своих компьютерах. Распределенные узлы — входные, промежуточные и выходные — создают децентрализованную сеть, благодаря чему соединение зашифровано и его нелегко заблокировать.

За Тор не нужно платить. Это бесплатная программа (<https://torproject.org>), созданная сообществом единомышленников, с открытым исходным кодом, который всегда можно проверить и улучшить. Такая прозрачность гарантирует, что Тор верно исполняет свою миссию и в инструменте нет лазеек или возможности скрытого контроля. Посмотрите, в чем плюсы и минусы этого браузера:

- **Плюсы:** Тор обеспечивает высочайший уровень анонимности.
- **Минусы:** веб-страницы загружаются медленнее из-за множества переходов между серверами.

Дейл, а каких браузеров лучше избегать? Что ж, друзья, вот примерный список (в произвольном порядке):

- Google Chrome;
- Microsoft Edge;
- Firefox;
- Opera;
- Safari.

Ваш браузер — первая линия защиты от киберугроз. Это не просто ворота в интернет, а крепость, оберегающая ваши данные. Позаботьтесь о своей конфиденциальности и установите надежный браузер уже сегодня. Ваше цифровое «я» скажет спасибо за дополнительную защиту.

¹ Отсюда название Onion (лук): слоистая структура, как у луковицы. — *Примеч. пер.*

Sock puppet: создание и использование виртуальной личности

Нет-нет, придержите свое воображение, речь не о забавных куклах, спитых из любимой пары носков. Sock puppet¹ (сокпапет) – несуществующая виртуальная личность, созданная для обмана, сбора информации или манипулирования людьми. Благодаря ей человек, словно кукольник в театре, примеряется на себя разные роли и взаимодействует с аудиторией, оставаясь инкогнито.

Хотя сокпапеты не запрещены законом, к ним часто относятся неодобрительно из-за высокого риска злоупотребления: с их помощью нередко распространяют ложную информацию, накручивают популярность, анонимно причиняют вред другим людям или обманывают путем проникновения в сообщества. Однако цифровые персонажи применяются и в законных целях, например в журналистских расследованиях или для проверки систем защиты.

Организации или обычные люди могут использовать виртуальную личность по нескольким причинам.

- **Анонимность.** Основная цель — избежать установления связи между действиями в интернете и настоящей личностью. Благодаря анонимности можно собирать информацию, не раскрывая себя.
- **Обман.** Маскируясь за виртуальной личностью, люди влияют на обсуждения, публикуют ложную информацию и манипулируют мнениями других. Это используется для скрытного проникновения или социальной инженерии.
- **Разведка.** Сокпапет — эффективный инструмент для незаметного сбора информации о людях и организациях, а также материалов на разные темы.
- **Конфиденциальность.** Некоторые просто хотят защитить личные данные и для этого действуют в интернете от имени нескольких не связанных между собой профилей.

Создаем виртуальную личность

В руках ответственного человека сокпапет, то есть фальшивый аккаунт, становится мощным инструментом для анонимного сбора информации. Действуя от имени виртуальной личности, следователь, подобно хамелеону, сливаются с интернет-средой и может вести разведку по открытым источникам, не раскрывая свои настоящие данные. Это особенно важно,

¹ Буквально: «кукла из носка». — Примеч. пер.

когда разглашение может помешать сбору информации или подвергнуть исследователя риску.

Представьте, что специалисту по кибербезопасности нужно оценить защищенность финансовой организации. Создав виртуальную личность и действуя в рамках этики, он может взаимодействовать с подозрительными сайтами или самими злоумышленниками, чтобы понять их тактику и не подвергать опасности себя или организацию. Как полицейский под прикрытием, но в цифровом районе: наблюдает, изучает, но не вмешивается.

Кроме того, виртуальные личности важны при отслеживании киберугроз. Сокпапет помогает просматривать форумы в даркнете и проникать в сети киберпреступников в поисках информации о возникающих угрозах, утечках или продаже похищенных данных. В результате специалисты могут предупредить потенциальную жертву и позаботиться о безопасности еще до того, как злоумышленники нанесут вред.

Правила ответственного использования сокпапета лежат в основе строгого кодекса поведения: цифровые персонажи нельзя применять для обмана и манипулирования — они должны лишь скрывать личность специалистов во время разведки и помогать нам укреплять системы защиты. Сокпапет — мантия-невидимка, под которой честный и порядочный человек может наблюдать за угрозами, не становясь мишенью.

Вот что нужно учесть при создании сокпапета:

- Четко определите назначение виртуальной личности, например исследование, сбор данных или проверка кибербезопасности. Всегда помните о своей цели и держитесь в рамках этических норм.
- Виртуальная личность должна быть правдоподобной. Представьте, что вы продумываете персонажа книги: представьте его прошлое, интересы и особые черты. Создать правдоподобную личность помогут такие инструменты, как Fake Name Generator (<https://www.fakenamegenerator.com/>) или NameFake (<https://namefake.com/>).

Дополните имя следующей информацией:

- дата и место рождения;
- родной город;
- образование и работа;
- интересы и хобби;
- любимые книги, фильмы, музыка;
- политические взгляды;

- религия;
- фото и изображения.

Это своего рода претекстинг.

Примечание

Встретили новое словечко? Знаете, для меня претекстинг – больше чем просто попытка притвориться другим человеком. Вы должны быть убедительны: тщательно продумайте предысторию, обстоятельства и сценарий.

- Чтобы виртуальная личность выглядела как можно более реально, необходимо подобрать ей фото. Для этого пригодится сайт <https://thispersondoesnotexist.com/> — на нем можно генерировать изображения людей с помощью искусственного интеллекта (ИИ). Поиск по сгенерированному фото не даст результатов, а значит, разоблачить ваш обман будет труднее.



Рис. 2.10. Да, этой девушки не существует, изображение сгенерировано ИИ (<https://thispersondoesnotexist.com/>)

- Виртуальной личности необходим электронный адрес. Его можно создать, например, в сервисе 20 Minute Mail (<https://www.20minutemail.com/>).
- Подготовьте поддельные учетные записи и профили в различных социальных сетях.

Примечание

Помните, что вымышленный образ должен быть единственным на всех платформах, поэтому старайтесь вести себя последовательно.

- Маскируйте свой IP-адрес с помощью VPN (например, <https://www.expressvpn.com/>) и постарайтесь использовать Тор (<https://www.torproject.org/>) или другие браузеры, ориентированные на конфиденциальность. Тогда ваша настоящая личность останется в тайне.

Как-то раз я давал интервью одному репортеру, и мне хотелось сделать это анонимно. Поэтому я использовал браузер Тор, который зашифровывает трафик, перенаправляя его между несколькими серверами по всему миру. Кроме того, я выбрал зашифрованный сервис для обмена сообщениями, найденный в даркнете, и в результате общался с репортером, не опасаясь за свою безопасность. Разговор был абсолютно конфиденциальным, и никто не мог нас отследить.

Не забудьте, что у виртуальной личности также должен быть номер телефона! С помощью сервиса TextFree (<https://textfree.us/>) можно обмениваться текстовыми сообщениями, не раскрывая свой настоящий номер. И это здорово.

Настраиваем анонимный канал связи

Чтобы по виртуальной личности было невозможно отследить ее создателя, необходимо создать анонимный канал связи. Для этого понадобятся одноразовые телефоны и электронные адреса, которые нельзя отследить.

Создавая электронный адрес для виртуальной личности, учитывайте следующее:

- избегайте необычных провайдеров;
- выбирайте привычные всем сервисы, например Gmail или Outlook;
- чтобы сохранить анонимность, создавайте электронные адреса, подключившись к общественному Wi-Fi или через VPN;
- не вводите случайные символы, адрес должен выглядеть реалистично;
- помните, что электронный адрес понадобится для регистрации учетных записей, поэтому сохраняйте анонимность.

Одноразовые телефоны (burner phone) позволяют держать расследование в тайне, но даже с ними необходимо проявлять осторожность. Используйте их только для задач, связанных с расследованием: позвонить, написать сообщение или получить код для входа в учетную запись.

Никогда не сохраняйте на устройстве конфиденциальные документы, имена, даты, местоположение или другую информацию. Помните, что даже одноразовый телефон можно прослушать, взломать или скомпрометировать.



Рис. 2.11. Одноразовые телефоны,
которые я использовал для взаимодействий

Поэтому не помешают дополнительные меры предосторожности: общайтесь в приложениях, шифрующих чаты (Signal и WhatsApp), не добавляйте на устройство личные учетные записи, выключите GPS, удаляйте метаданные изображений и регулярно очищайте кэш. Связываясь с информаторами, используйте кодовые имена вместо настоящих.

Во время использования одноразового телефона ни на минуту не теряйте бдительность. Если вы завершили расследование или подозреваете, что устройство скомпрометировано, обязательно выведите его из эксплуатации, чтобы злоумышленники не могли получить доступ к данным. Подойдет один из двух способов:

- **Архивируйте устройство надлежащим образом**, словно обращаетесь с материалами после секретной операции, и документируйте все действия, связанные с его хранением и использованием. Передайте одноразовое устройство и все оборудование, которое применялось в ходе разведки, клиенту — тогда все ресурсы, данные и потенциальные доказательства будут под должным контролем. Однако помните, что мы не стремимся бессмысленно складировать технику. Подход к хранению продиктован профессиональными стандартами и необходимостью разделять обязанности.

- **Выведите устройство из эксплуатации.** Для начала сбросьте систему до заводских настроек, чтобы удалить все данные, — это стандартная процедура. Затем разберите устройство. Извлеките и уничтожьте SIM-карту, например, разрезав ее на части, чтобы предотвратить восстановление информации, — так рекомендуют протоколы безопасности. Дальнейшая разборка, включая снятие экрана и батарейки, помешает злоумышленникам восстановить устройство или его компоненты. Уничтожьте устройство по частям, не привлекая постороннего внимания и в разных местах, чтобы минимизировать риск восстановления данных.

Перечисленные меры предосторожности — не шпионские тактики из острожных боевиков, а основа основ профессионального цифрового расследования и взлома с целью защиты. Одноразовый телефон помогает сохранить анонимность и избежать компрометации работы. Применяя его и затем утилизируя по всем правилам, специалист достигает безопасности и конфиденциальности в сфере, где ставки неизменно высоки.

Помните, что наша цель — укреплять защиту и выявлять уязвимости еще до того, как злоумышленники попытаются ими воспользоваться. Все действия должны быть законны, прозрачны для клиентов и направлены на защиту активов и информации в мире, который все больше зависит от цифровых технологий.

Если каналы общения анонимны, никто не свяжет сокапета с его создателем. Поддельные учетные записи будут казаться совершенно естественными и самостоятельными.

Только сохранивая анонимность при создании виртуальных личностей, вы обеспечите конфиденциальность своих данных и сможете выдавать себя за другого человека. А для этого важно, чтобы канал связи не отслеживался.

Управляем виртуальной личностью

Итак, теперь сокапет может выходить на сцену, и важно соблюсти следующие этические нормы:

- **Информирование заинтересованных сторон.** Если в исследовании или корпоративных проверках используются сокапеты, сообщайте о своих методах и намерениях заинтересованным сторонам.
- **Защита данных.** Позаботьтесь о безопасности данных. Собирайте только информацию, необходимую для расследования, и обращайтесь с ней как можно более ответственно.

- **Документация и отчетность.** Тщательно документируйте действия сокапета. Так будет проще представить результаты разведки и соблюсти правовые и этические нормы.

Гендерные взаимоотношения при использовании виртуальной личности

Создание альтер эго в мире киберрасследований сочетает в себе элементы искусства и науки и требует постоянного соблюдения этических норм — особенно когда речь заходит о гендерных взаимоотношениях, то есть отношениях между мужчинами и женщинами. Да, интернет заполнен гендерными стереотипами, но при создании виртуальной личности не помешает осторожность.

Представьте, что для маскировки вы выбрали женский образ. В некоторых ситуациях он и правда помогает, ведь в обществе установились определенные правила взаимодействия. Но помните, что сам по себе обман не является нашей целью. Мы действуем профессионально и не желаем причинить вред. Дело в том, что женский образ позволяет вести себя немного кокетливо и притворяться уязвимым, чтобы привлечь внимание объекта. Но с такой стратегией очень важно не переступать границы этических норм. Ведь наша цель — собрать информацию, а не манипулировать людьми.

Чтобы виртуальная личность выглядела правдоподобно, необходимо учесть каждую мелочь. Откажитесь от стереотипов и сформируйте неповторимый цифровой образ. Добавьте уникальные черты, и сокапет станет не просто набором пикселей, а убедительным персонажем, который сможет завоевать доверие там, где это действительно нужно.

Примечание

Совет профессионала: полностью изолируйте виртуальную личность от своей реальной интернет-активности. Попробуйте использовать виртуальные машины, песочницы в браузере и другие похожие инструменты. Смешивать активность вымышленного человека и свою настоящую жизнь — все равно что носить сандалии с носками. Просто нелепо. Разделив их, вы создадите по-настоящему правдоподобный персонаж и убережете собственные данные от чужих глаз.

Обман оправдан, если вы действуете на «светлой стороне». Благодаря сокапетам можно проникнуть в подозрительное интернет-сообщество и выявить риски безопасности или притвориться новичком в собственной компании и проверить, кто из сотрудников клонет на фишинг. Приняв на себя роль специалиста по кибербезопасности, вы должны использовать свои возможности во благо.

Так что давайте действовать профессионально и этично и помнить: мы здесь, чтобы остановить зло, а не примкнуть к нему.

Анонимность электронных адресов и переписки

Если специалист OSINT хочет скрыть свою личность и сохранить конфиденциальность при взаимодействии в интернете, ему не обойтись без анонимного электронного адреса. Нередко обычные электронные адреса содержат подсказки о реальной личности человека и позволяют ее разоблачить. Если во время разведки специалист пренебрежет анонимностью и привяжет собственный адрес на форумах, в сервисах или социальных сетях, он подвергнет риску свои личные данные. В результате он может стать жертвой взлома, деанонимизации и мести, или его могут ошибочно ассоциировать с определенной группой людей или событиями.

Чтобы этого не произошло, чрезвычайно важно создавать изолированные электронные адреса, не связанные с какими-либо идентификационными данными. Но такие адреса ни в коем случае нельзя использовать там, где вы рискуете раскрыть информацию о себе: в социальных сетях, на профессиональных сайтах вроде LinkedIn, в учетных записях магазинов и т. д. В идеале анонимный адрес нужно создавать в таких сервисах, как Proton Mail (<https://protonmail.com/>).

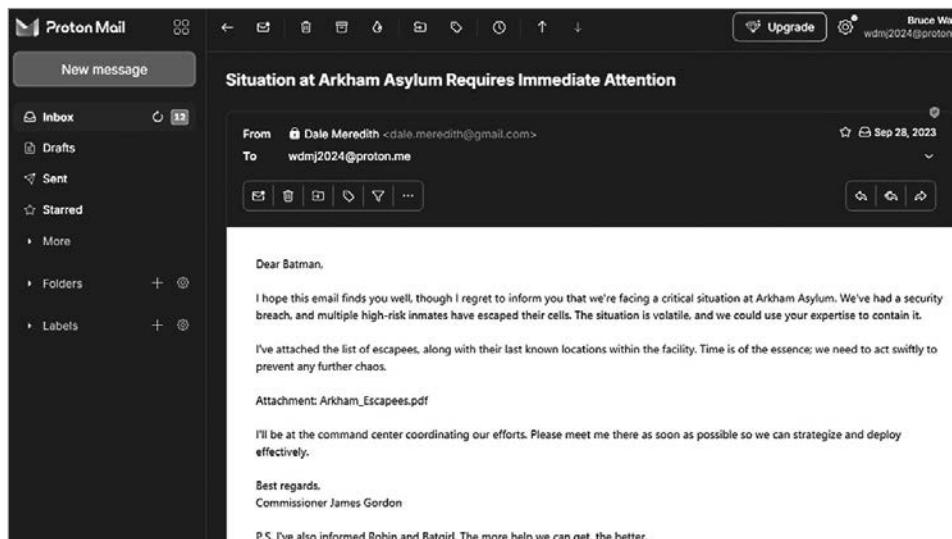


Рис. 2.12. Proton Mail помогает скрыть настоящую личность

Другой сервис электронной почты — Tuta (<https://tuta.com/>); в нем можно создать адрес, не указывая настоящие личные данные.

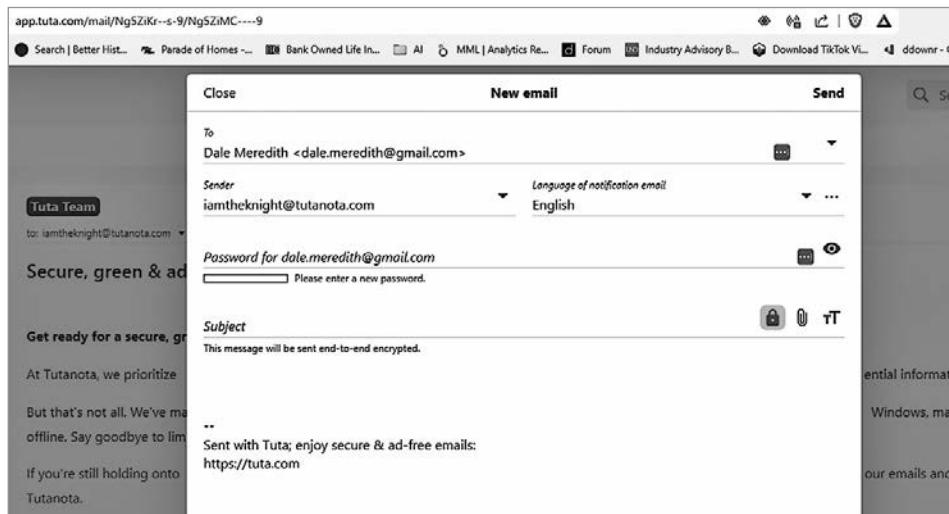


Рис. 2.13. Анонимное электронное письмо от адреса tutanota

Благодаря такому электронному адресу специалист OSINT может регистрироваться на форумах, делать запросы данных и общаться, не опасаясь раскрыть себя. Это важнейший инструмент для сохранения анонимности.

Предупреждение киберугроз в OSINT

Разведка по открытым источникам влечет за собой риски кибербезопасности. Конфиденциальность и анонимность — краеугольные камни OSINT. Именно поэтому специалисты должны постоянно прилагать усилия, чтобы опережать технологические угрозы, в том числе следить за последними новостями в сфере безопасности, анализировать происшествия и совершенствовать собственные навыки.

Новости о защите конфиденциальности и кибербезопасности

Чтобы отслеживать угрозы и понимать, как меняется сфера защиты конфиденциальности и кибербезопасности, необходимо следить за новостями.

Подписавшись на рассылки специализированных информационных платформ, вы будете получать уведомления об уязвимостях и новых техниках злоумышленников:

- раздел об угрозах кибербезопасности Cybersecurity Threats на портале CIS (Center for Internet Security) (<https://www.cisecurity.org/cybersecurity-threats>);
- буллетени центра кибербезопасности US-CERT (<https://www.cisa.gov/news-events/bulletins>).

Бюллетени US-CERT — один из моих любимых сервисов. Он не отдает предпочтение какой-либо компании и предлагает качественный и подробный анализ киберугроз (рис. 2.14).

А если вы хотите стать крутым специалистом по кибербезопасности, читайте следующие блоги и новостные сайты:

- Krebs on Security (<https://krebsonsecurity.com/>);
- новости OSINT от Sangoma (<https://www.sangoma.com/>).

Перечисленные ресурсы помогут следить за последними разработками.

The screenshot shows the homepage of the US-CERT website. At the top, there's a header with the text "CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY" and "AMERICA'S CYBER DEFENSE AGENCY". Below the header is a search bar and a "REPORT A CYBER ISSUE" button. The main navigation menu includes "Topics", "Spotlight", "Resources & Tools", "News & Events", "Careers", and "About". On the left side, there's a sidebar titled "Filters" with a "What are you looking for?" input field and a "Sort by (optional)" dropdown set to "Relevance". Below the sidebar, there are three links to "Vulnerability Summary for the Week of February 19, 2024", "Vulnerability Summary for the Week of February 12, 2024", and "Vulnerability Summary for the Week of February 5, 2024". The main content area has a heading "Bulletins" and a brief description: "Bulletins provide weekly summaries of new vulnerabilities. Patch information is provided when available."

Рис. 2.14. Бюллетени US-CERT

Кроме того, рекомендую подписаться на ведущих специалистов по информационной безопасности в социальных сетях и по возможности посещать тематические конференции, например DEF CON, Blackhat или Bsides.

Опыт прошлых взломов и инцидентов

Вы можете многому научиться, проанализировав крупные взломы, совершенные ранее. Взлом LinkedIn в 2016 году показал, как утечка данных сторонних лиц спровоцировала цепную реакцию атак (<https://www.forbes.com/sites/daveywinder/2024/01/23/massive-26-billion-record-leak-dropbox-linkedin-twitterx-all-named/?sh=2ab1fc93ab58>). Нашумевший случай деанонимизации и преследования, получивший название Gamergate, продемонстрировал, каким разрушительным бывает OSINT, если использовать ее как оружие (<https://www.nytimes.com/interactive/2019/08/15/opinion/what-is-gamergate.html>). Проанализировав методы, к которым прибегают недобросовестные исследователи, вы также узнаете о той социальной инженерии, что порицается в кругах ответственных специалистов.

Итоги

Итак, первой линией обороны специалиста OSINT служит строгое соблюдение анонимности. Регулярно проверяйте, упоминается ли в интернете ваше имя, фиксируйте свои цифровые следы и устранийте лазейки для утечки данных. Возьмите за правило использовать Тог, виртуальные телефонные номера, анонимные электронные адреса и другие похожие инструменты, чтобы скрыть свою настоящую личность. Изолируйте свои личные данные, чтобы избежать идентификации, а во время разведки применяйте отдельные устройства и учетные записи. Обязательно совершенствуйте свои навыки и следите за новостями в сфере конфиденциальности: новые угрозы идентификации возникают постоянно.

Перечисленные рекомендации помогают специалистам OSINT уберечь себя от деанонимизации и безопасно вести разведку. Каждый день появляются новые угрозы, поэтому важно постоянно быть на шаг впереди злоумышленников. Далее мы рассмотрим методы и приемы, которые можно использовать во время разведки по открытым источникам.

ГЛАВА 3

АРСЕНАЛ OSINT: МЕТОДЫ И ПРИЕМЫ СБОРА И АНАЛИЗА ИНФОРМАЦИИ

Налейте кружку любимого пива и устройтесь поудобнее в кресле: вас ждет увлекательная экскурсия по оживленным проспектам **разведки по открытым источникам**. В этой главе мы раскроем тайны OSINT и продемонстрируем великолепие мира, где каждая крупица информации становится ценным вкладом в ваши навыки этичного взлома — ради защиты, а не разрушения.

Вы переживаете увлекательнейшее приключение и, словно на американских горках, промчитесь по киберпространству, расшифровывая язык интернета и примеряя на себя роль цифрового детектива. А чтобы вам было еще приятнее, мы приправили текст шутками, ведь учиться с улыбкой всегда легче.

Итак, хотите узнать, что нас ждет в этом путешествии? Вот краткий список тем:

- Знакомство с методами и приемами OSINT
- Поиск информации в видимой сети
- Погружение в глубокую сеть и даркнет
- Анализ изображений и геоданных
- Автоматизация сбора и анализа информации

К концу этой главы вы научитесь профессионально извлекать и анализировать информацию из открытых источников, соблюдая принципы этики. Мы наполним ваш «ящик с инструментами» проверенными стратегиями и приемами, с которыми вы сможете уверенно отправиться в мир OSINT.

Знакомство с методами и приемами OSINT

OSINT — это кладезь методов и приемов, позволяющих исследователям без труда ориентироваться в бескрайнем информационном пространстве. Эти передовые инструменты позволяют извлекать ценную информацию, забираясь вглубь малоизученных уголков интернета или анализируя геоданные. Давайте рассмотрим основные приемы, без которых не обойтись при этичном взломе и разведке.

Возьмите что-нибудь вкусненькое, расположитесь поудобнее и приготовьтесь узнать удивительные способы расследования, каждый из которых — словно звезда в сияющей галактике этичного хакинга. Пора начинать.

Разнообразие приемов в OSINT

OSINT предлагает изумительное изобилие методов и приемов, каждый из которых открывает уникальные возможности для поиска и анализа информации. С их помощью осуществляются этичный взлом и извлечение данных. Давайте подробнее изучим некоторые из них.

Веб-скрейпинг

При веб-скрейпинге специалист использует программы для автоматического извлечения данных из сайтов. Это основной инструмент OSINT, благодаря которому можно быстро и без лишних усилий собирать большие объемы информации.

Какие же возможности открывает веб-скрейпинг? Давайте рассмотрим основные преимущества.

- **Удобная автоматизация.** Представьте, что у вас на службе неутомимый виртуальный ассистент. С помощью скриптов на языках программирования вроде Python он просматривает сайты и извлекает информацию, пока вы попиваете кофе. Он умеет находиться сразу везде, где требуется, легко и непринужденно собирая нужные данные.
- **Сбор полезной информации.** Веб-скрейпинг похож на охоту за самыми цennыми данными в бескрайнем цифровом океане. Благодаря этому приему вы быстро собираете нужную информацию: от списка контактов из онлайн-каталогов до полезных комментариев на технических форумах.
- **Цифровой наблюдатель.** Скрейперы служат надежными наблюдателями, которые отслеживают любые изменения на сайтах. Они оперативно предупреждают вас о новостях и обновлениях, что бывает весьма удобно,

особенно если сайт не предлагает информационную рассылку по удобной кнопочке «Подписаться».

- **Путешествие во времени.** Веб-скрейперы могут выступать в роли машины времени и делать регулярные снимки веб-страниц, по которым вы увидите, что на них изменилось. Эта особенность здорово выручает, если нужно получить доступ к старой информации или восстановить удаленную.
- **Интерпретация данных.** Получив информацию, вы можете надеть шляпу детектива и поискать доказательства и взаимосвязи. Представьте, что вы собираете пазл, где каждая деталь помогает сформировать полную картину.
- **Поддержка комплексных исследований.** Данные, собранные с помощью веб-скрейпинга, можно объединить с другой информацией и провести более глубокий анализ. Вы словно смешиваете краски, чтобы получить идеальный оттенок, который делает палитру богаче и насыщеннее.

Для создания веб-скрейперов часто используют язык Python и, в частности, такие библиотеки, как BeautifulSoup. Узнать о ней больше можно на сайте <https://www.crummy.com/software/BeautifulSoup/>. Эта библиотека поможет найти нужную информацию в HTML- и XML-файлах сайта. Ниже приведен простой пример такого скрейпера:

```
from bs4 import BeautifulSoup
import requests
response = requests.get('https://daledumbsitdown.com')
soup = BeautifulSoup(response.text, 'html.parser')
# Вывести на экран заголовок страницы
print(soup.title.string)
```

Рассмотрим каждую строку кода, чтобы понять, что он делает.

1. На этом этапе мы вызываем BeautifulSoup:

```
from bs4 import BeautifulSoup
```

2. Затем приглашаем requests — библиотеку Python, которую часто используют для выполнения HTTP-запросов, например GET или POST:

```
import requests
```

3. Теперь отправляем GET-запрос сайту <https://daledumbsitdown.com>, чтобы он присоединился к нашей тусовке. Функция `requests.get()` извлекает контент, расположенный по указанному URL. Этот контент отвечает на приглашение и попадает в переменную `response`:

```
response = requests.get('https://daledumbsitdown.com')
```

4. Далее мы передаем управление в руки Beautiful Soup. Библиотека извлекает контент из переменной `response` (информацию о сеансе, если вам так удобнее) и использует `html.parser`, чтобы разобраться в структуре HTML, организуя хорошо спланированное событие, где каждый тег знает свое место:

```
soup = BeautifulSoup(response.text, 'html.parser')
```

5. Наконец, мы просим Beautiful Soup дать нам название веб-страницы. Библиотека находит в HTML-документе тег `<title>` и выводит из него на экран искомый заголовок:

```
print(soup.title.string)
```

Итак, этот скрипт — золотой ключик к заголовку веб-страницы. Да, пример прост, но он послужит хорошей основой для дальнейшего обучения. С каждым шагом вы будете открывать более сложные приемы, которые помогут не только отточить навыки, но и углубить знания.

Работа с социальными сетями

Twitter, Facebook, LinkedIn, Instagram и другие социальные сети могут служить не только развлечением, но и ценным источником информации. В этой главе мы проанализируем их подробнее, но сперва поговорим о том, зачем это нужно. Основная задача разведки по социальным сетям — сбор и обработка информации. На таких платформах, как Facebook, Twitter, LinkedIn и Instagram, можно получить сведения о сотрудниках и деятельности организаций, а иногда даже выявить потенциальные уязвимости.

Давайте разберем, какие подходы используют специалисты.

- **Сбор профилей и данных из них.** Специалисты по безопасности собирают и объединяют информацию о сотрудниках, компаниях и стейкхолдерах, используя инструменты вроде Pipl или Spokeo. Полученные данные, например должности или увлечения, могут применяться для направленных фишинговых атак.
- **Анализ активности.** Публикации, отметки «Нравится», репосты и комментарии могут многое рассказать о поведении пользователей. Например, если на общедоступном форуме сотрудник компании обсуждает программное обеспечение, применяемое в работе, это может случайно раскрыть важную информацию об используемых технологиях.
- **Геолокация и метаданные.** Нередко фотографии и публикации содержат метаданные, которые могут сообщить о местоположении критически важных объектов инфраструктуры, например серверных комнат или центров

обработки данных. Кроме того, метаданные фотографий иногда хранят марку и модель устройства — благодаря им можно предположить, какое оборудование использует организация.

- **Выявление контактов.** С помощью таких инструментов, как Maltego, специалисты выстраивают визуальные карты связей между сотрудниками компании. Проанализировав контактную сеть отдельного человека, можно представить структуру организации или даже выявить неформальные связи с другими сотрудниками, партнерами или конкурентами.
- **Анализ настроений.** В некоторых компаниях специалисты даже анализируют сообщения сотрудников, чтобы определить общий моральный дух. Если в коллективе преобладают пессимистические настроения, то люди относятся к работе небрежно и растет риск инсайдерских угроз, что снижает уровень безопасности компании.
- **Выявление событий и моделей поведения.** Аналитики ищут упоминания о сбоях или обновлениях системы — такая информация помогает определить периоды, когда организация наиболее уязвима. Кроме того, сообщения о корпоративных мероприятиях могут подсказать, когда офицы пустуют или ИТ-специалисты занимаются задачами, не связанными с безопасностью.
- **Просмотр вакансий.** Объявления о вакансиях на LinkedIn и в других профессиональных сообществах могут раскрыть используемые технологические стеки, текущие проекты и даже планы компании на будущее. Благодаря этим сведениям можно получить представление о ее инфраструктуре, планируемой бизнес-экспансии или смене технологий.

Разведка по социальным сетям требует соблюдения тонкого баланса: нужно уважать личное пространство, но в то же время изучать доступные данные. Обычно аналитики не взаимодействуют с людьми и не пытаются обойти настройки конфиденциальности. Они предпочитают пассивный подход и для того, чтобы обеспечить безопасность компании, собирают только общедоступную информацию.

В центре внимания OSINT — человеческий фактор. Ведь безопасность зависит не только от технологий, но и от людей, которые их используют и обсуждают. С помощью анализа сведений из социальных сетей можно превратить цифровой след сотрудников в полезные данные разведки и защитить компанию от потенциальных угроз.

Анализ изображений и геоданных

Анализ геоданных (также «геопространственный анализ») — исследование географической информации, которое помогает выявить скрытые закономерности и тенденции. Благодаря ему специалисты OSINT интерпретируют данные о местоположении объекта исследования, открывая детали, которые остаются незамеченными при стандартных методах анализа. Вы получаете не просто возможность полюбоваться красивыми спутниковыми снимками (хотя они бывают умопомрачительно прекрасны), а мощный инструмент для наблюдения за различными явлениями — от изменений окружающей среды до роста городов.

Возьмем для начала возможности спутниковой и аэросъемки. Нет, речь идет не о снимках, которые вы время от времени просматриваете на ресурсе Google Планета Земля, а о специализированных сервисах, например Sentinel Hub (<https://www.sentinel-hub.com/>). Такие платформы позволяют анализировать спутниковые изображения, выявлять закономерности, отслеживать перемещения и даже находить объекты, не указанные на картах.

Но самое интересное связано с методами геолокации. С помощью специальных инструментов и платформ можно с высокой точностью определять, где было сделано фото, вплоть до конкретного места съемки.

Какие инструменты пригодятся для OSINT? Анализировать местность во время разведки можно с помощью карт, встроенных в поисковые системы Google, Bing или Яндекс. А бывают инструменты более узкого применения: одни позволяют отслеживать воздушный трафик, другие — просматривать недавние снимки определенного региона, третьи передают изображения с уличных камер.

Правоохранительные органы могут наблюдать за передвижением воздушного и морского транспорта, выявляя подозрительную деятельность. Как видите, геоданные раскрывают специалистам OSINT ценные сведения из самых разных сфер.

Но это только начало! Чтобы заглянуть еще глубже, можно анализировать изображения, ведь в них скрывается множество подсказок. Например, тени указывают на время съемки, а объекты и ландшафт на заднем фоне помогают установить местоположение. В работе с изображениями пригодятся такие сайты, как FotoForensics (<http://fotoforensics.com/>), — на них можно детально исследовать фото в поисках скрытой информации.

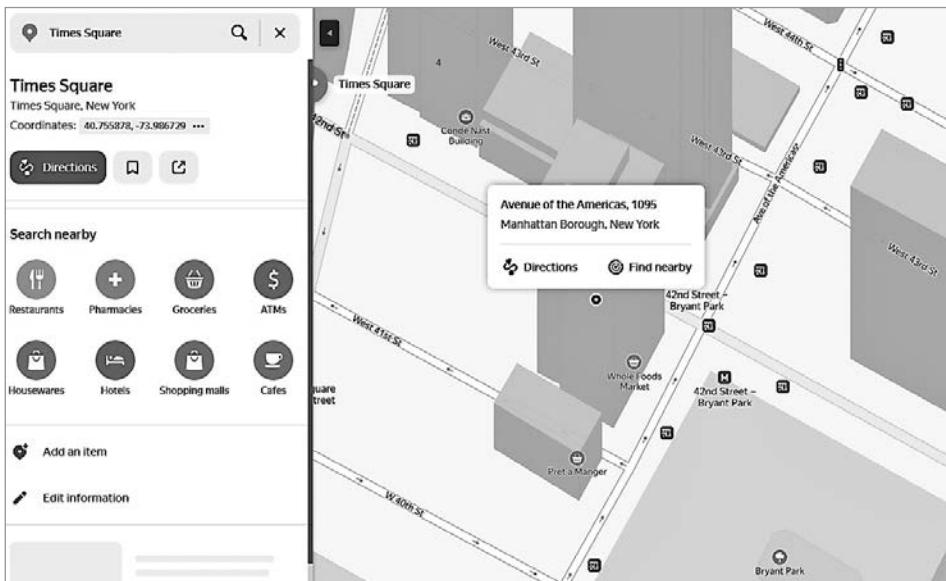


Рис. 3.1. Координаты здания на yandex.com

Анализ информации из глубокой сети и даркнета

Чтобы собирать данные из глубокой сети (deep web) и даркнета (dark web), необходимо заглянуть в самые темные и потаенные уголки интернета. Не волнуйтесь, все не так страшно. В следующих разделах я подробно расскажу об инструментах и приемах для безопасной работы в этом цифровом пространстве.

Важно помнить: сбор информации — лишь часть OSINT. Только тщательный анализ данных позволяет лучше изучить объект исследования и принимать взвешенные решения.

Выбор подхода в зависимости от задачи

Подбор приемов OSINT напоминает поиск идеального инструмента: правильное решение может стать ключом к успеху, а неверное — привести к провалу. Каждая задача требует индивидуального подхода.

- **Предотвращение корпоративного шпионажа.** Представьте, что вы консультант по кибербезопасности, которому поручено защищать секреты компании. Чтобы предотвратить потенциальные утечки, вам придется анализировать действия сотрудников в социальных сетях.

В таком случае вы будете этичным хакером, которых иногда называют «белые шляпы»¹.

- **Реагирование на бедствия.** В случае чрезвычайных ситуаций анализ спутниковых снимков *в прямом смысле* спасает жизни: позволяет выявить пострадавшие районы и эффективнее организовать спасательные операции.
- **Исследование рынка.** Хотите выяснить, что думают о вашем бренде? Исследуйте тенденции и настроения в социальных сетях. Вы узнаете много нового и будете лучше понимать рынок.

Примечание

В каждом случае успех зависит от того, какой подход вы выберете. Ваша цель – не просто собрать информацию, а извлечь полезные знания. И вот что еще. Вы помните мой девиз, когда дело доходит до хакинга (и OSINT в придачу)? Нет? Вот он: «*Не всякое МОГУ означает МОЖНО*». Так что во время разведки всегда придерживайтесь этических норм.

Итак, OSINT – обширная быстроразвивающаяся сфера с богатым набором инструментов для тех, кто хочет собирать и анализировать информацию из открытых источников. И неважно, как вы ее будете получать: массово извлекая во время веб-скрейпинга или собирая по крупицам в социальных сетях – успех зависит от выбранного подхода.

Поиск информации в видимой сети

Видимая сеть (surface web) – огромное хранилище информации, проиндексированной поисковыми системами, и важнейший источник данных для OSINT. Сейчас я расскажу, какие знания и навыки пригодятся для работы в этой части интернета, и предложу несколько приемов разведки.

Приемы расширенного поиска

Поисковые системы – незаменимые товарищи в путешествии по бескрайним просторам интернета. Однако по-настоящему раскрыть их потенциал

¹ Понятия «белые» и «черные шляпы» как обозначение хороших и плохих парней пришли, вероятно, из вестернов, где главные герои носили белые шляпы, а отрицательные – черные. – Примеч. ред.

помогут расширенные поисковые запросы. Научившись их использовать, вы будете получать именно ту информацию, которая вам нужна.

Например, оператор `site:` сообщает системе, что данные нужно искать на указанном сайте, а `intext:` позволяет найти веб-страницы с заданной фразой. Только представьте, какие возможности это открывает. Благодаря продвинутым поисковым запросам вы сможете получать более релевантные результаты.

Оператор `site:` — один из моих любимых. С ним можно искать данные на определенном сайте. Почему это важно? Потому что бывает весьма полезно просматривать всю информацию, доступную в каком-либо уже известном источнике. Вот как это работает:

```
site:daledumbsitdown.com "cyber security"
```

В результатах поиска по этому запросу будут только страницы сайта `daledumbsitdown.com`, которые содержат фразу `cyber security`. Легко, правда?

В свою очередь, оператор `intext:` позволяет увидеть только те сайты, где ис-комая фраза встречается в тексте веб-страницы, а не в других ее элементах. Так вы упростите себе процесс поиска. Вот пример запроса:

```
intext:"recent cyber attacks"
```

В ответ на этот запрос поисковая система предложит веб-страницы, текст которых содержит фразу `recent cyber attacks`. В результате вы быстро найдете последние новости о кибератаках. Правда здорово?

Научившись комбинировать различные операторы, вы значительно повысите точность поисковой выдачи и сможете без труда находить нужную информацию. Этот навык обязательно пригодится во время разведки по открытым источникам.

Google Dorking: поиск уязвимостей через Google

Google Dorking, или **Google Hacking**, — техника, при которой с помощью операторов расширенного поиска ищут определенную информацию или потенциальные уязвимости на сайтах, проиндексированных Google. Это ключевой инструмент OSINT, который позволяет находить конфиденциальные данные, попавшие в открытый доступ.

Например, оператор **filetype:** поможет найти файлы определенного формата с заданным содержанием. Откройте Google и посмотрите, как работает этот запрос:

```
filetype:pdf "annual security report"
```

В результатах поиска вы увидите документы PDF с фразой **annual security report**, из которых можно многое почерпнуть о тенденциях и инцидентах в области безопасности. А теперь на секунду представьте себя в роли злоумышленника и задумайтесь: какие данные вашей организации можно найти?

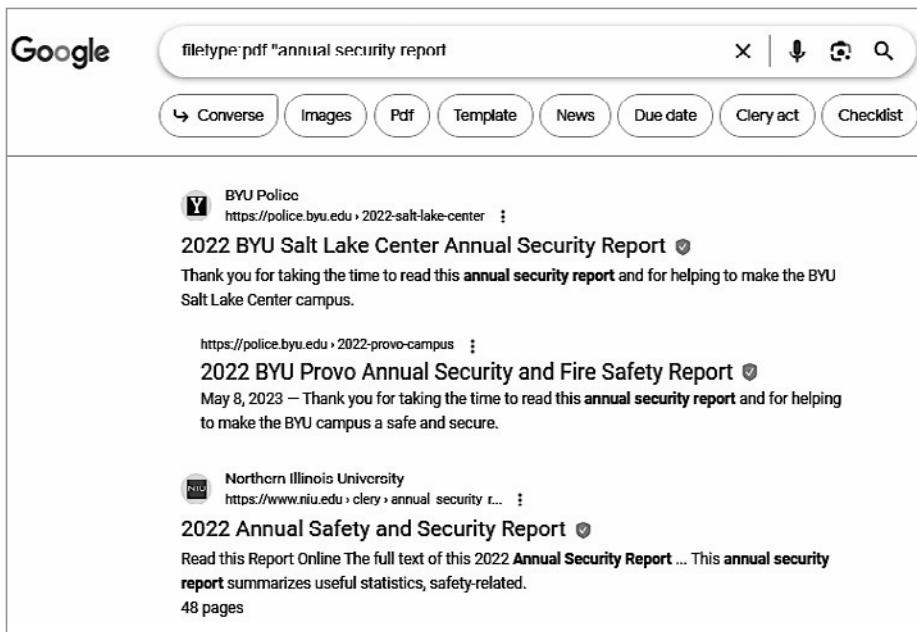


Рис. 3.2. Интересные данные по запросу filetype:pdf «annual security report»

Уже страшно? Нет? Тогда вот вам еще один пример:

Оператор **inurl:** ищет веб-страницы, в URL которых содержится заданное ключевое слово. В результате можно найти открытые каталоги или конфиденциальную информацию. Посмотрите, как работает такой запрос:

```
inurl:admin login
```

В результатах поиска по этому запросу вы увидите веб-страницы, в адресе которых присутствуют слова `admin` и `login`. Некоторые из найденных сайтов могут оказаться весьма занимательными. Попробуйте — я подожду!

Научившись работать с основными операторами, вы сможете комбинировать их, создавая более сложные запросы. И тогда вам откроется большой объем информации, недоступной при использовании обычных методов поиска. Рассмотрим несколько примеров:

```
intext:"Login" inurl:/secure
```

В этом запросе применяются операторы `intext:` и `inurl:`. Вот что делает каждый из них:

- `intext:"Login"`. Оператор `intext:` ищет заданное слово или фразу в основном тексте веб-страницы. В нашем случае указано слово `Login`, по которому можно найти формы входа в систему.
- `inurl:/secure`. Оператор `inurl:` ищет URL с заданными ключевыми словами. Здесь мы просим его найти вхождение слова `/secure`, которое может указывать на защищенные страницы сайта, например страницу администратора или входа в систему.

Вместе эти операторы помогают найти защищенные страницы входа в учетную запись, а также получить доступ к конфиденциальной информации или функциям сайта. Благодаря им вы можете выявить потенциальные уязвимости.

А теперь попробуйте этот запрос (да-да, очередной Google-дорк):

```
intitle:"index of" ".ssh" OR "ssh_config" OR "ssh_known_hosts" OR "authorized_keys" OR "id_rsa" OR "id_dsa"
```

Сможете разобрать, что здесь происходит? В запросе несколько операторов. Подумайте пару секунд... Готовы?

Комбинация операторов из этого примера позволяет находить открытые каталоги (их легко распознать по выражению `index of` в заголовке), содержащие файлы конфигураций или ключей **SSH (Secure Shell)**. Давайте посмотрим, как это работает.

- `intitle:"index of":`. Оператор `inttitle:` ищет веб-страницы, в заголовке которых упоминаются заданные слова или выражения (в нашем случае — `index of`). Обычно такие заголовки встречаются, если сервер отображает содержимое каталога в формате веб-страницы.

- `".ssh" OR "ssh_config" OR "ssh_known_hosts" OR "authorized_keys" OR "id_rsa" OR "id_dsa"`. Эта часть запроса ищет веб-страницы, на которых присутствует любое из заданных выражений. Мы перечислили файлы конфигураций и ключей SSH, которые используются для аутентификации и обеспечивают безопасное подключение к серверам. Рассмотрим их по отдельности.
 - `.ssh`. Каталог, в котором обычно хранятся файлы конфигурации и ключей SSH.
 - `ssh_config`. Файл с настройками клиента SSH, позволяющий задавать параметры подключения.
 - `ssh_known_hosts`. Файл, где хранятся ключи серверов, используемые для подтверждения их подлинности клиентами SSH.
 - `authorized_keys`. Файл, содержащий публичные ключи SSH, используемые для аутентификации пользователей с соответствующими закрытыми ключами.
 - `id_rsa`. Файл с закрытым ключом RSA, необходимым для аутентификации через SSH.
 - `id_dsa`. Файл с закрытым ключом DSA, который также применяется для аутентификации через SSH.
 - Оператор `OR` позволяет искать веб-страницы, на которых встречается хотя бы одно из заданных выражений. В нашем случае результаты будут содержать любое упомянутое имя файла или каталога.

Я мог бы написать целую книгу о поиске уязвимостей по запросам в Google. Google Dorking открывает безграничные возможности: позволяет находить камеры видеонаблюдения, устройства интернета вещей (IoT), страницы входа в SharePoint и даже принтеры. Хотите продемонстрировать уязвимость системы? Поверьте, нет способа нагляднее, чем подключиться к принтеру какой-нибудь компании и отправить на печать «Войну и мир».

Специализированные поисковые системы и каталоги

Специализированные поисковые системы и каталоги — незаменимые инструменты исследователей, особенно тех, кто ведет разведку по открытым источникам. Они предназначены для поиска информации по предметным областям, которые могут быть недостаточно представлены в обычных поисковиках. В этом разделе мы рассмотрим особенности таких платформ и узнаем, как эффективно работать с ними в рамках OSINT.

Специализированные поисковые системы охватывают определенный тип данных и представляют собой более целенаправленный подход к сбору информации. Благодаря им вы сможете глубже проанализировать выбранную область знаний. Мы изучим основные категории таких систем и их применение в разведке по открытым источникам.

Поиск научных публикаций

Такие платформы можно считать секретной дверью в эксклюзивную библиотеку оцифрованных знаний. Здесь каждый запрос ведет вас по вселенной научных открытий и значительно повышает качество разведданных. Рассмотрим основные поисковые системы.

- **Google Академия** (scholar.google.com). Виртуальное VIP-хранилище научных статей, диссертаций, книг, патентов и докладов с конференций. Здесь можно найти самые передовые исследования, минуя ненужные материалы и информационный шум, с которым мы сталкиваемся в обычной поисковой системе Google.

The screenshot shows the Google Scholar interface. At the top, there's a search bar with the query 'bruce wayne'. Below it, a sidebar on the left offers filtering options: 'Articles', 'Any time', 'Since 2023', 'Since 2022', 'Since 2019', 'Custom range...', 'Sort by relevance', 'Sort by date', 'Any type', and 'Review articles'. The main content area displays search results for 'What's Wrong with Bruce Wayne?' by RS Rosenberg, published in 2008, and 'A Psychoanalysis on Internal Conflict of Bruce Wayne as Seen in Matt Reeves' The Batman (2022) Movie' by MA Masyhur and M Fithratullah, published in 2023. Each result includes a 'Save' button, a 'Cite' button, a 'Cited by' count (e.g., 7 or 97), and a 'Related articles' link.

Рис. 3.3. Результаты поиска на scholar.google.com по запросу Bruce Wayne

- **PubMed** (pubmed.ncbi.nlm.nih.gov). Незаменимый инструмент для поиска информации в области биологии, медицины и прочих наук о живой природе. Его создатели стремятся улучшить состояние здоровья всех жителей планеты — и ваше тоже!

Немного о цифрах. База данных PubMed насчитывает более 36 миллионов цитат и рефератов, что делает ее ценным источником тематической

литературы. И пусть вас не смущает, что на сайте нет полных текстов статей. Платформа предлагает удобные ссылки на все доступные источники, будь то сайты издательств или ресурс **PubMed Central**, на который всегда можно положиться. Так что вы будете всего в одном клике от погружения в мир науки.

- **IEEE Xplore** (<https://ieeexplore.ieee.org/Xplore/home.jsp>). Кладезь профессиональной литературы для специалистов в области электроники, электротехники и информатики. Платформа предлагает доступ к высококачественному контенту и подходит для всех любителей технологий, которые стремятся углубить свои знания.

Поиск исходного кода

Такие платформы не только хранят множество проектов с открытым исходным кодом, но также временами случайно раскрывают конфиденциальную информацию и подсказывают преступникам уязвимости.

- **GitHub** (github.com). Ax, GitHub! Уникальная площадка, на которой разработчики размещают свои проекты. Настоящая золотая жила для тех, кто ищет программы с открытыми исходниками или полезные фрагменты кода для собственных задач. Однако иногда здесь раскрывается конфиденциальная информация и сведения об уязвимостях в ПО.
- **SourceForge** (sourceforge.net). Еще один отличный сайт с функцией поиска, на котором можно бесплатно создавать и публиковать ПО с открытым исходным кодом. Здесь вы найдете множество программных проектов и сможете сотрудничать с другими разработчиками.

Поиск патентов

На таких ресурсах можно познакомиться с новейшими технологиями и чертежами изобретений, изменивших наш мир.

- **Google Patents** (patents.google.com). Платформа, которая предлагает подробную информацию о патентах. Благодаря ей можно узнать о технологических достижениях и проанализировать рынок.
- **База данных ведомства по патентам и товарным знакам США** (uspto.gov). Одна из *крупнейших* патентных баз мира. Здесь можно найти подробное описание патентов, формулы, ссылки и другие сведения, что повышает ее ценность при глубоком анализе изобретений и инноваций.

Поиск изображений

Системы визуального поиска — мощный инструмент для выявления уязвимостей и потенциальных угроз безопасности. Благодаря таким инструментам можно находить изображения инфраструктур, веб-приложений и сетей, а иногда даже пароли, записанные на стикерах, — что и произошло во время интервью сотрудников канала TV5Monde в 2015 году.



Рис. 3.4. Пароли, записанные на стикерах, попали в кадр во время интервью

Платформы поиска изображений незаменимы, когда речь заходит о проверке их подлинности или сборе дополнительной информации.

- **TinEye** (tineye.com). Потрясающий инструмент обратного поиска, который помогает найти источник изображения или узнать, где еще оно встречалось. Я постоянно использую TinEye в разведке: проверяю подлинность изображений или ищу связанную с ними информацию.
- **Google Картинки** (images.google.com). Один из самых популярных инструментов для поиска изображений, который любят за простой интерфейс и огромную коллекцию материалов. Платформа опирается на обширную базу данных Google, что позволяет находить не только картинки, но и уязвимости. С помощью систем поиска изображений и видео злоумышленники могут отслеживать действия в сети в режиме реального времени, получая актуальную информацию о своей цели. Такой подход

позволяет быстро фиксировать изменения в системе или сети и принимать соответствующие меры.

Итак, я показал вам основные инструменты для поиска изображений. Согласитесь: поражает, сколько данных можно найти всего за пару кликов. Но это лишь малая часть возможностей OSINT. Теперь давайте заглянем в мир социальных сетей — в нем всегда что-то происходит, и новые данные появляются непрерывно. Вы словно смотрите шоу не в записи, а в прямом эфире: можете в любой момент получить самую свежую информацию о людях и компаниях. Золотое дно для специалиста OSINT. Так что давайте узнаем, какие сведения можно извлечь на этих платформах.

Разведка по социальным сетям (SOCMINT)

SOCMINT (Social Media Intelligence), «младший брат» OSINT, подразумевает поиск информации в постоянно развивающемся мире социальных сетей. В отличие от OSINT, где приходится довольствоваться общедоступными данными, SOCMINT заманивает вас глубже и предлагает информацию, изначально предназначенную для узкого круга пользователей.

Социальные сети превратились в настоящие информационные центры: день за днем представители организаций и обычные люди делятся там новостями и мнениями. В результате специалистам OSINT открывается огромное количество данных, что делает такие платформы незаменимыми для разведки. Давайте посмотрим, какие площадки завоевали популярность и какую пользу можно из этого извлечь.

- **X (ранее — Twitter) (twitter.com):**
 - **Центр активности.** Пользователи Twitter неустанно обсуждают последние новости и слухи на множество тем. Именно сюда приходят OSINT-аналитики в поисках свежих сенсаций.
 - **Мощный поиск.** Удобный инструмент поиска с различными фильтрами позволяет легко находить твиты и получать необходимую информацию.
 - **API для работы с данными.** Интеграция API Twitter значительно экономит время и упрощает сбор большого объема данных.
- **Facebook (facebook.com):**
 - **Мириады сообществ.** На Facebook создается бесчисленное количество сообществ и обсуждений, где пользователи делятся информацией

на самые разные темы. Изобилие актуальных данных притягивает и OSINT-аналитиков.

- **Торговая площадка.** В Marketplace всегда кипит жизнь — чего только там не продают! Благодаря этому аналитики могут выявить последние тенденции рынка и проанализировать поведение потребителей.
 - **Нескончаемые мероприятия.** Одна из полезных функций Facebook — создание и продвижение мероприятий (ивентов). С ее помощью исследователи OSINT собирают данные о различных мероприятиях и их участниках.
- **LinkedIn** (linkedin.com):
- **Сообщество специалистов.** LinkedIn — площадка для создания и укрепления деловых связей. Здесь вы найдете бесценную информацию о компаниях, отраслях и влиятельных представителях профессионального мира. Идеально подходит для бизнес-исследований.
 - **Размещение вакансий.** На LinkedIn можно просматривать актуальные вакансии, а значит, отслеживать изменения на рынке труда и тенденции развития отрасли.

Примечание

Больше всего мне нравятся доски вакансий: в объявлениях о работе встречается уйма сведений о компании.

- **Разнообразие контента.** Пользователи LinkedIn делятся множеством материалов — от статей до презентаций. В них содержится много информации для исследователей OSINT.
- **Instagram** (instagram.com):
- **Визуальное наполнение.** Instagram — платформа, полная изображений и видео, которые отлично подходят для различных видов анализа — от тенденций до настроений.
 - **Магия тегов.** Публикации Instagram можно дополнять хештегами и геометками, которые помогают классифицировать контент и быстро находить нужную информацию, что особенно пригождается специалистам OSINT.
 - **Влияние блогеров.** В Instagram обитает множество влиятельных пользователей, которые формируют общественное мнение. Анализируя их публикации и стратегии продвижения, можно узнать о текущих тенденциях и общественном настроении.

Ну что ж, мы разобрались с основными источниками и типами информации. Теперь нужно понять, как использовать их в разведке.

Погружение в принципы SOCMINT

Чтобы вести разведку по социальным сетям, важно понять концепции и термины SOCMINT. Рассмотрим их подробнее.

- **Профиль пользователя.** Данные, указанные в профиле, дают краткое представление о пользователе — как о личной, так и о профессиональной жизни. Страница в LinkedIn может рассказать о текущей должности (скажем, «администратор Windows»), уровне образования и ключевых навыках («Microsoft Exchange Server 2013» или «Sharepoint»). В профиле Twitter указаны хобби и интересы, а также тип информации, с которой человек взаимодействует, — вместе это помогает создать более полное представление о его личности и предпочтениях.
- **Взаимодействия** — действия, которые пользователи совершают в социальных сетях. Например, на Facebook человек может активно участвовать в дискуссиях о кибербезопасности, обмениваясь мнениями и ресурсами с другими участниками. В Instagram и на других похожих платформах — комментировать публикации об инструментах для безопасности беспроводных сетей или размещать истории о недавнем вебинаре по этичному взлому. Благодаря таким взаимодействиям исследователи получают огромное количество информации и могут узнать, какие темы волнуют пользователей и какой контент вызывает наибольший отклик прямо сейчас.
- **Метаданные** — контекстные данные, которые сопровождают основной контент в социальных сетях. Например, фотография может содержать геолокацию, время и дату публикации, а также сведения об устройстве, с которого она была загружена. Эти данные помогают исследователям анализировать модели поведения и строить более полные портреты как отдельных пользователей, так и целых групп.

Примечание

Информация, которую люди размещают в социальных сетях, поражает своей откровенностью. Многие без задней мысли раскрывают свое имя, пол и электронный адрес. Но что меня особенно тревожит, так это родители, которые публикуют фото своих детей. Почему? Во-первых, если фото попало в интернет, его уже не удалить. Во-вторых, родители часто подписывают фото, указывая имена детей. Порой изображения содержат дополнительную информацию, об опасности которой никто не задумывается: например, на фотографиях ребенка, сделанных перед домом в первый школьный день, может быть видна табличка с домашним адресом. Ладно, мое дело предупредить.

Типы информации в цифровом мире

По чисто формальному признаку собираемую информацию можно разделить на два основных типа.

- **Эксплицитная информация.** То, чем пользователи сознательно делятся в социальных сетях. Эти данные формируют цифровой образ человека и доступны без всяких танцев с бубном. Например, пользователь может написать твит, поделившись мнением о последних разработках в сфере кибербезопасности, или опубликовать в LinkedIn недавно полученный сертификат по этичному взлому. К этой категории также относятся данные профиля, например должность, образование, список групп или сообществ. Эксплицитная информация дает четкое представление о профессиональной жизни, интересах и взглядах человека, а также его действиях в интернете.
- **Имплицитная информация.** Более деликатные сведения, которые пользователи раскрывают непреднамеренно. Приведу пример. Проанализировав отметки «Нравится» и репосты на Facebook и других похожих платформах, исследователи могут понять, какие темы или сообщества нравятся пользователю больше всего. Аналогично, метаданные опубликованного контента, например геолокация или тип устройства, помогают узнать о местах, которые человек часто посещает, и других привычках. Таким образом, имплицитная информация позволяет выявить факты и закономерности, которые неочевидны на первый взгляд, и создать более полный и детализированный цифровой портрет пользователя.

Сочетая эксплицитную и имплицитную информацию, специалисты SOCMINT ткут гобелен, отражающий мельчайшие подробности жизни человека, и это помогает провести более глубокий анализ. Такая разведка напоминает сбор пазла, где каждый кусочек дополняет общую картину.

Нам нужен Шерлок

Именно эту фразу я часто повторяю своим детям, и она уже изрядно им наскутила. Всякий раз, когда они задают вопрос, ответ на который они могут найти самостоятельно, я предлагаю им поиграть в сыщиков и говорю: «*Нам нужен Шерлок*¹». Как же я был рад, когда появился инструмент с таким названием!

¹ В оригинале «Sherlock it» (по аналогии с «Google it» — «погугли»). Смысл примерно такой: «включи Шерлока», «додумай сам». — Примеч. ред.

Sherlock – простой и удобный инструмент, который проверяет, есть ли в социальных сетях учетная запись с указанным именем пользователя или названием организации. Представьте, что вы наняли виртуального детектива, сообщили ему имя или ник и отправили тщательно просматривать веб-страницы в поисках всевозможных профилей, которые могут быть с ними связаны.

Давайте попробуем. Вот пошаговая инструкция по установке Sherlock на Kali Linux – моей основной платформе для OSINT-исследований:

1. **Обновите систему.** Прежде чем приглашать Шерлока в гости, сделайте в своем цифровом жилище свеженький ремонт. Для этого откройте терминал и выполните следующую команду:

```
sudo apt update && sudo apt upgrade -y
```

2. **Установите Git.** Теперь надо установить на вашу Kali Linux популярную систему контроля версий Git. Она нужна для скачивания и установки Sherlock. Выполните следующую команду:

```
sudo apt install git -y
```

Эта команда вежливо попросит вашу систему установить Git, автоматически подтверждая все запросы (благодаря флагу `-y`).

3. **Клонируйте репозиторий Sherlock.** Далее нужно скачать с GitHub репозиторий Sherlock – дом нашего детектива, где хранятся все инструменты, необходимые ему для сыска. Для этого выполните команду:

```
git clone https://github.com/sherlock-project/sherlock.git
```

4. **Установите зависимости.** Прежде чем использовать Sherlock, нужно правильно настроить среду. Перейдите в каталог Sherlock и выполните команду:

```
python3 -m pip install -r requirements.txt
```

5. После завершения установки попробуйте Sherlock в деле. Для этого используйте простую команду:

```
sherlock <имя_пользователя>
```

Учтите, что результаты поиска не всегда бывают точными. Например, вот выдача при поиске по имени `dalemeredith`:

```
[kali㉿kali)-[~]
└─$ sherlock dalemereedith
[*] Checking username dalemereedith on:

[+] About.me: https://about.me/dalemereedith
[+] Audiojungle: https://audiojungle.net/user/dalemereedith
[+] Behance: https://www.behance.net/dalemereedith
[+] Disqus: https://disqus.com/dalemereedith
[+] Facebook: https://www.facebook.com/dalemereedith
[+] Fiverr: https://www.fiverr.com/dalemereedith
[+] Flipboard: https://flipboard.com/@dalemereedith
[+] GeeksforGeeks: https://auth.geeksforgeeks.org/user/dalemereedith
[+] Gravatar: http://en.gravatar.com/dalemereedith
[+] Houzz: https://houzz.com/user/dalemereedith
[+] Instagram: https://www.instagram.com/dalemereedith
[+] Issuu: https://issuu.com/dalemereedith
[+] NationStates Nation: https://nationstates.net/nation=dalemereedith
[+] NationStates Region: https://nationstates.net/region=dalemereedith
[+] Periscope: https://www.periscope.tv/dalemereedith/
[+] Reddit: https://www.reddit.com/user/dalemereedith
[+] SlideShare: https://slideshare.net/dalemereedith
[+] Smule: https://www.smule.com/dalemereedith
[+] Snapchat: https://www.snapchat.com/add/dalemereedith
[+] Strava: https://www.strava.com/athletes/dalemereedith
[+] ThemeForest: https://themeforest.net/user/dalemereedith
[+] TrashboxRU: https://trashbox.ru/users/dalemereedith
```

Рис. 3.5. Результаты поиска в Sherlock по запросу dalemereedith

Итак, если вам понадобится найти больше информации об имени пользователя или просто связать разрозненные данные в интернете, Sherlock станет вашим верным помощником. Этот инструмент интуитивно понятен, прост в использовании и, сказать честно, в корне меняет подход к разведке по открытым источникам.

Хештеги и геолокация

Чтобы найти в интернете настоящие самородки, нужно уметь пользоваться хештегами и метками геолокации. С ними у вас в руках появляется карта сокровищ, которая откроет путь к кладу.

Хештеги, простые слова с символом #, словно хлебные крошки, приведут вас в самое сердце оживленных разговоров на популярные темы. Представьте, что вы хотите найти недавние публикации о... ну, не знаю. Скажем, о самом крутом супергерое. Который борется со злом по ночам — без сверхспособностей, но в плаще. Есть такой на примете? У меня есть: Бэтмен. Итак, откройте

любимую социальную сеть, наберите в строке поиска #Batman — и вуаля! Вы попали в самую гущу событий. Так что хештеги позволяют без труда следить за тенденциями и собирать информацию в режиме реального времени. Посмотрим, как с их помощью искать информацию.

- **Анализ тенденций.** Отправляясь в путешествие по вселенной хештегов, обязательно захватите с собой сервисы вроде **Hashtagify** (<https://hashtagify.me/>) и **RiteTag** (<https://ritetag.com/>). Они помогут найти популярные хештеги и даже предложат лучшие варианты для увеличения охвата. Вы будто окажетесь за кулисами самых обсуждаемых тем интернета и увидите все, что происходит за сценой.
- **Взаимодействие с сообществом.** Благодаря платформе **X Pro**, ранее известной как TweetDeck (<https://pro.twitter.com/>), можно отслеживать обсуждения и взаимодействовать с сообществом. Укажите нужные теги — и вы погрузитесь в разговоры на специфические темы и получите важную информацию из первых рук.
- **Поиск контента.** Сервис **BuzzSumo** (<https://buzzsumo.com/>) поможет найти популярный контент по хештегам. Он работает как увеличительное стекло, выводя на первый план самые интересные и обсуждаемые материалы на выбранную тему.

Поговорим о геолокации

Геолокация — своего рода цифровая версия фразы «Здесь был Дейл». С помощью этого инструмента можно определить географические координаты (широту и долготу) любого устройства, подключенного к интернету, будь то телефон, планшет или даже умные часы. Выделяют три основных способа определить геолокацию: с помощью сервера, с помощью устройства и по всем источникам. Рассмотрим их подробнее.

- **Сбор данных на стороне сервера: вычисление по IP.**
Благодаря базам геоданных, созданным за годы сбора информации, цифровой сыщик может отслеживать физическое местоположение устройств по их IP-адресам. Однако таким данным не всегда можно доверять, так как их точность зависит от сторонних поставщиков. Они диктуют стандарты и предлагают собственные решения для определения геолокации, в результате чего на вашей карте сокровищ постоянно меняются ориентиры.
- **Сбор данных на стороне устройства: GPS-трекер.**
В вашем кармане спрятан мини-детектив, который неустанно передает информацию о вашем местоположении. В основном он использует GPS

и сигналы сотовых вышек, благодаря чему в густонаселенных местах планеты геолокация определяется довольно точно. Чего не скажешь об отдаленных регионах, где детектив может заблудиться — и тогда данные содержат ошибки, поставляются с задержкой или вовсе отсутствуют. Чтобы геолокация при таком подходе определялась максимально точно, функция определения местоположения должна быть включена на каждом устройстве и в каждом приложении. Однако это может быть затруднительно из-за риска для конфиденциальности.

- **Сбор данных из обоих источников: лучшее от каждого подхода.**

Сыщик и детектив объединяются в команду, используя преимущества сбора информации как на сервере, так и на устройстве. При сочетании обоих способов местоположение будет определяться даже в условиях, когда одна из технологий не работает. Это особенно важно для сайтов, которые нацелены на активное взаимодействие с посетителями.

- **Примеры использования геолокации.**

Сервисы геолокации сыграли важную роль в расследовании событий, произошедших 6 января 2021 года в США¹. В связи с захватом Капитолия компания Google активно сотрудничала с правоохранительными органами и в ответ на соответствующие ордера передавала информацию о том, какие устройства находились в определенное время в запрашиваемом районе. Хотя отслеживание устройств помогает найти подозреваемых, нельзя забывать о конфиденциальности, ведь данные невиновных людей тоже могут попасть в базу. В этой непростой ситуации Google попыталась найти компромисс, балансируя между помощью правоохранительным органам и защитой конфиденциальности пользователей.

Произошедшие события свидетельствуют о решающей роли технологических компаний в современных уголовных расследованиях. Однако они также напоминают о хрупкости равновесия между сотрудничеством с властями и уважением частной жизни. Оно не должно нарушаться, иначе доверие и поддержка общества будут утрачены. С развитием технологий необходимо создавать механизмы, которые обеспечат правосудие без ущерба для конфиденциальности добродорядочных граждан. Тогда будущее, где правоохранительные органы регулярно используют технологии без угрозы правам человека, кажется мне возможным. Однако пока подобное вмешательство государства вызывает беспокойство.

¹ 6 января 2021 года толпа сторонников Дональда Трампа захватила Капитолий США, чтобы прервать совместную сессию Конгресса по утверждению результатов выборов в президенты, на которых победил Джо Байден. — Примеч. пер.

Магия данных EXIF

Данные EXIF¹ всегда привлекают внимание специалистов OSINT. Когда вы что-то фотографируете, телефон или цифровая камера незаметно добавляют к снимку различные метаданные, например GPS-координаты, по которым можно точно определить, где именно сделано фото. Казалось бы, легкий доступ к информации! Но все не так просто: большинство сайтов и социальных сетей удаляют эти данные, чтобы защитить конфиденциальность пользователей. Так что найти в интернете изображение с полным набором метаданных EXIF так же сложно, как иголку в стоге сена. Однако если вам все же удастся отыскать оригинальное фото, вы узнаете много интересного. Чтобы извлечь метаданные из изображений, можно воспользоваться такими инструментами, как **Jimpl** (jimpl.com). Я загрузил на сайт один из снимков и сейчас покажу вам, что получилось:

The screenshot shows the Jimpl website interface. At the top, there's a logo with a camera icon and the word 'Jimpl'. Below it are four tabs: 'IMAGE METADATA' (selected), 'CAMERA SETTINGS', 'LOCATION', and 'FULL METADATA'. A 'UPLOAD ANOTHER IMAGE' button is also present. The main area displays a black and white photo of a man with a lanyard. To the right, under 'Image metadata', is a table of data:

Name	20220810_111727.jpg
File size	1.05 MB (1097976 bytes)
File type	JPEG
MIME type	image/jpeg
Image size	1500 x 2821 (4.2 megapixels)
Color space	sRGB
Created	August 10, 2022 11:17

Below this, a note states: "Metadata takes 2.57 KB (0.2%) of this image and may include sensitive info. To protect your privacy, download this image without metadata by clicking the button below." To the right, under 'Location', it says: "This photo doesn't include location data. We can't find where it was taken."

Рис. 3.6. Информация о фото, извлеченная на jimpl.com

¹ EXIF (Exchangeable Image File Format) — стандарт метаданных для изображений. — Примеч. ред.

Вы, наверное, заметили, что информация о местоположении отсутствует. Дело в том, что мой телефон настроен на высокий уровень защиты: я запретил отслеживание геолокации для всех снимков, в том числе и этого, сделанного на конференции BlackHat. Но взгляните на метаданные, которые вытянул сервис:

Camera settings	
Make	samsung
Model	SM-S908U
Focal length	3.8 mm
Aperture	2.2
Exposure	1/20
ISO	1000
Flash	No Flash

Рис. 3.7. Jumpi даже определил настройки камеры

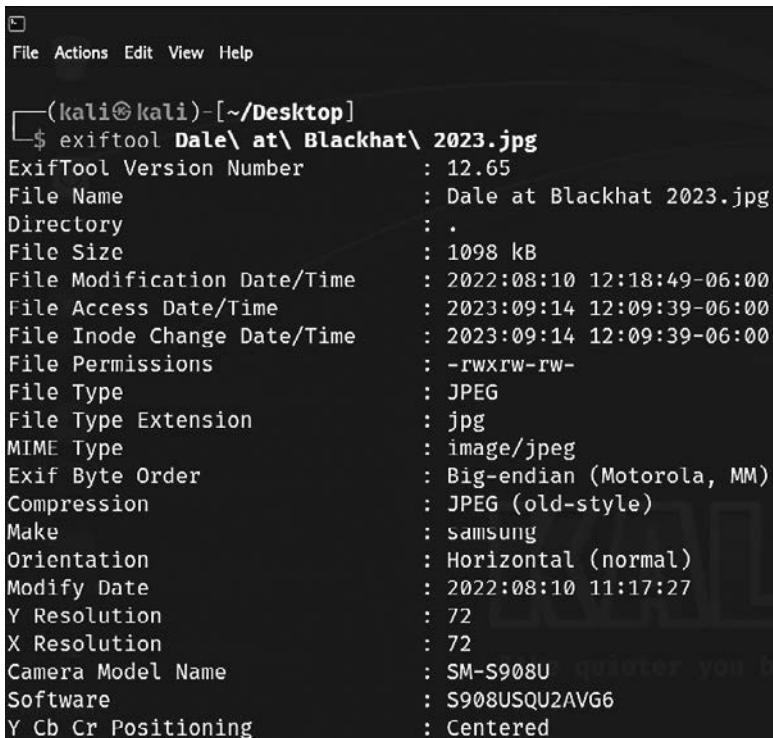
ExifTool — популярная программа для просмотра и редактирования метаданных в медиафайлах. Она уже встроена в Kali Linux, так что давайте запустим систему и посмотрим, какие возможности нам предлагают.

Первый шаг работы с метаданными — научиться их считывать. Для этого достаточно выполнить простую команду:

```
exiftool yourmasterpiece.jpg
```

Эта команда раскроет все метаданные файла `yourmasterpiece.jpg`, включая настройки камеры, дату съемки и многое другое.

По мере освоения ExifTool вы откроете для себя несметное количество полезных функций, ведь инструмент предлагает огромные возможности: от пакетной обработки файлов до копирования метаданных из одного изображения в другое. Чтобы узнать больше, изучите документацию или используйте флаг `-h`.



```
(kali㉿kali)-[~/Desktop]
└$ exiftool Dale\ at\ Blackhat\ 2023.jpg
ExifTool Version Number      : 12.65
File Name                   : Dale at Blackhat 2023.jpg
Directory                   : .
File Size                    : 1098 kB
File Modification Date/Time : 2022:08:10 12:18:49-06:00
File Access Date/Time       : 2023:09:14 12:09:39-06:00
File Inode Change Date/Time : 2023:09:14 12:09:39-06:00
File Permissions             : -rwxrw-rw-
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Big-endian (Motorola, MM)
Compression                 : JPEG (old-style)
Make                         : Samsung
Orientation                  : Horizontal (normal)
Modify Date                 : 2022:08:10 11:17:27
Y Resolution                 : 72
X Resolution                 : 72
Camera Model Name           : SM-S908U
Software                      : S908USQU2AVG6
Y Cb Cr Positioning         : Centered
```

Рис. 3.8. Результаты обработки фото Dale at Blackhat 2023.jpg в ExifTool

Скрытые источники информации

Прежде чем изучать **скрытые источники информации**, необходимо понять, что это вообще такое. Итак, скрытые источники — это малоизвестные уголки интернета, например небольшие форумы, специализированные сайты или базы данных, которые не индексируются основными поисковыми системами, а значит, могут ускользнуть от нашего внимания. Сюда же относятся ресурсы, которые находятся «на виду», но часто игнорируются, например, устройства с минимальной защитой при подключении к интернету — или вовсе без нее. Именно такие менее очевидные источники могут хранить бесценную информацию, недоступную в видимой сети.

Погружение в глубокую сеть и даркнет

Пристегнитесь покрепче, потому что мы отправляемся в путешествие по глубокой сети и даркнету, самым загадочным уровням интернета. Как

правило, в глубокой сети хранится контент, который недоступен в обычных поисковых системах. И он не всегда противозаконный: чаще всего это базы данных, конфиденциальная информация и ресурсы с доступом по подписке. Да, на этом уровне есть много сомнительных материалов, но мы не будем заострять на них внимание.

Из чего состоит интернет

Прежде всего вы должны понимать, что интернет разделяется на несколько уровней. Да, он охватывает больше, чем обычный Google Chrome, в котором вы набираете www.daledumbstdown.com, чтобы почитать о технологиях, или делаете покупки на сайте Amazon.

Интернет похож на айсберг. То, чем мы пользуемся ежедневно, — лишь видимая сеть (surface web), небольшая часть, что выступает над поверхностью воды. Но под водой залегают глубокая сеть (deep web) и даркнет (darknet web), скрытые от посторонних глаз. Именно там интернет хранит древние знания и тайны.

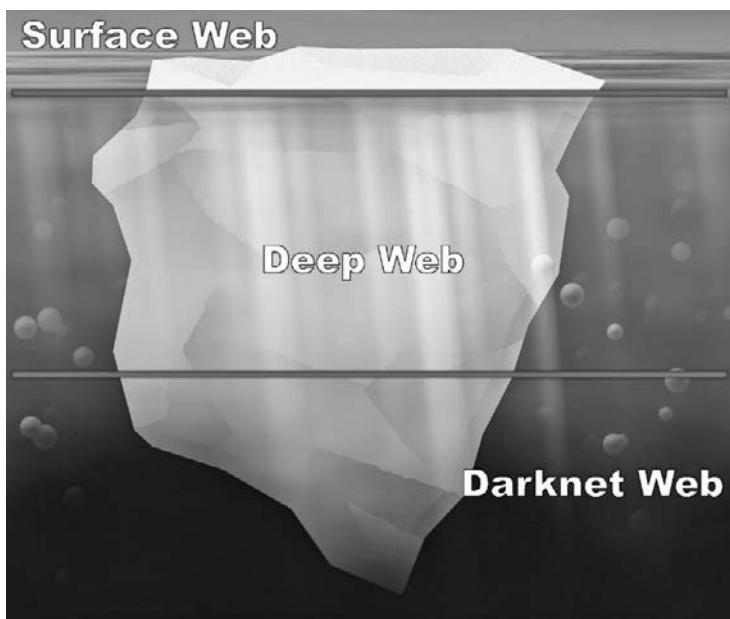


Рис. 3.9. Уровни интернета: видимая сеть, глубокая сеть и даркнет

Но не бойтесь! Я стану вашим проводником и, когда мы отправимся в неизведанные глубины, буду освещать вам путь.

- **Уровень 1: видимая сеть.**

Представьте, что мы еще не погрузились в океан. Перед нами видимая сеть — яркий, шумный мегаполис. YouTube, Wikipedia и прочие сайты, которые появляются в результатах обычного поиска Google. Этот уровень интернета можно сравнить с городской площадью: оживленный, доступный каждому жителю — и полностью проиндексированный.

- **Уровень 2: глубокая сеть.**

Надев водолазный костюм, мы опускаемся под воду и попадаем в глубокую сеть, полную загадок. Она похожа на огромный архив, где хранятся базы данных, учетные записи электронной почты, сервисы по подписке и конфиденциальная информация. Глубокая сеть гораздо больше видимой и не индексируется обычными поисковыми системами. Заглянуть в нее — все равно что попасть в закрытый клуб — можно лишь по VIP-пропуску, который есть только у посвященных.

- **Уровень 3: даркнет.**

Погрузившись еще глубже, вы попадете в даркнет — самый потаенный уровень интернета. Представьте себе запутанные улочки старого рынка, спрятанного в отдаленном городском районе, где каждый поворот таит в себе что-то неизведанное. Даркнет — небольшая часть глубокой сети, намеренно скрытая и защищенная от стандартных браузеров. Здесь на первом месте анонимность, поэтому для обезличенного доступа используются специальные программы вроде Тор. Но помните, что с большой силой приходит большая ответственность. Даркнет может быть средоточием незаконной деятельности, так что необходимо соблюдать осторожность и придерживаться этических принципов.

Отправной точкой любого OSINT-исследования будет видимая сеть. В ней вы собираете массу общедоступной информации, которая проиндексирована поисковыми системами. Это идеальное пространство для любого исследователя с навыками работы в интернете. Но давайте разберемся, что нужно для сбора информации в остальной части сети:

1. **Настройте VPN.**

Сперва обзаведитесь **VPN**, он поможет защитить конфиденциальность: скроет ваш IP-адрес, обеспечив анонимность при работе в интернете.

2. Скачайте специализированный браузер.

Установите браузер, который откроет доступ в даркнет, например Tor, Waterfox или Freenet — они позволяют просматривать сайты с доменом .onion, недоступные в обычных браузерах.

3. Откройте поисковую систему.

Если вы уже настроили программы, самое время приступить к исследованию! Но не спешите открывать Google, он здесь бесполезен. Вам понадобится поисковая система, которая специализируется на работе с доменами .onion, например DuckDuckGo, доступная по адресу <https://duckduckgo.com/>. Она станет вашим надежным спутником в путешествии по неизведанным глубинам.

Рис. 3.10. Поиск в системе Haystak с помощью браузера Tor
(обратите внимание на домен .onion)

4. Исследуйте onion-сайты.

Браузер и поисковая система готовы, и вы можете приступать к изучению onion-сайтов. Однако будьте предельно осторожны: некоторые уголки даркнета весьма опасны. Страйтесь посещать только проверенные ресурсы и избегать подозрительных ссылок. Здесь царит атмосфера Дикого Запада, так что важно всегда быть начеку.

Погружаясь в глубины интернета, помните, что безопасность должна быть на первом месте. Это путешествие не для слабонервных, но с надежными инструментами и средствами защиты вы сможете эффективно исследовать потаенные уголки интернета, не подвергая себя риску.

Сбор данных с помощью theHarvester

Инструмент **theHarvester** входит в состав Kali Linux и предназначен для автоматизированного сбора таких данных, как электронные адреса, поддомены, имена хостов и сотрудников. Он извлекает информацию из поисковых систем, серверов PGP-ключей и глубокой сети. К этому инструменту часто обращаются специалисты по безопасности и исследователи на ранних этапах киберрасследования или проверки систем защиты. Чтобы запустить theHarvester, откройте терминал и введите команду:

```
theHarvester -d <домен> -l <число результатов>-b <источник>
```

Рассмотрим ее по частям:

- **-d** определяет домен, о котором нужно найти информацию;
- **-l** ограничивает число результатов;
- **-b** указывает источник поиска (Google, Bing, PGP, LinkedIn, Twitter). Обратите внимание, что для работы с некоторыми источниками могут понадобиться API-ключи, иначе при выполнении команды возникнут ошибки.

Ну что, попробуем?

```
theHarvester -d hackthissite.org -l 500 -b all
```

Результаты выполнения команды показаны на следующем скриншоте:

```
[*] InterestingUrls found: 13
-----
http://mail-old.hackthissite.org
https://hackthissite.org/
https://mail.hackthissite.org/
https://mail.hackthissite.org/?r=/login
https://stats.hackthissite.org/
https://www.hackthissite.org/
https://www.hackthissite.org/?adlt=strict
https://www.hackthissite.org/missions/
https://www.hackthissite.org/missions/basic/11/
https://www.hackthissite.org/missions/basic/11/e/l/t/o/n/
https://www.hackthissite.org/missions/realistic/12/cgi-bin/internet.pl
https://www.hackthissite.org/missions/realistic/2/
https://www.hackthissite.org/missions/realistic/9/

[*] LinkedIn Links found: 0
-----

[*] IPs found: 45
-----
67.21.66.227
67.21.66.228
67.21.66.229
67.21.66.230
89.41.169.49
89.106.200.1
137.74.187.100
137.74.187.101
```

Рис. 3.11. Результаты в theHarvester

Полученной информации настолько много, что она не уместилась на экране. Вылилась как из рога изобилия.

Shodan

Shodan (<https://shodan.io>) — это своего рода Google Поиск устройств интернета вещей. С его помощью можно находить разнообразные устройства и сервисы, подключенные к интернету. Обычные пользователи используют Shodan, чтобы проверить, не взломана ли их веб-камера, но специалисты по безопасности находят инструменту другое применение. Мы ищем уязвимости во всевозможном оборудовании с выходом в Сеть — от серверов до промышленных систем управления.

Shodan позволяет находить массу привлекательных целей и делать это прямо на собственном ноутбуке.

Хотите попробовать? Введите доменное имя, чтобы найти доступные устройства или сервисы:

TOTAL RESULTS
6

TOP ORGANIZATIONS
Staff HackT... 5
OVH SAS 1

Partner Spotlight: Looking for a place to store all the Shodan data?
Check out Gravwell

Hack This Site

137.74.187.1 04
hackthissite.org

SSL Certificate Issued By: 2022-12-20T02:31:25.666912

HTTP/1.1 200 OK
Date: Tue, 20 Dec 2022 02:31:25 GMT
Upgrade: h2,h2c

Рис. 3.12. Поиск на shodan.io по запросу hackthissite.org

Поиск по запросу `hackthissite.org` в основном показывает информацию об SSL-сертификатах. Однако если с сайтом связаны устройства интернета вещей (камеры, датчики, системы удаленного управления), которые подключены к интернету и неправильно настроены, они тоже появятся в результатах. Попробуйте вот что: введите в строку поиска `os:windows 7`, и вы увидите все найденные устройства с Windows 7.

TOTAL RESULTS
375,940

TOP COUNTRIES
China 167,167
United States 38,691
Russian Federation 19,238
Hong Kong 12,661
Korea, Republic of 11,409
More...

Partner Spotlight: Looking for a place to store all the Shodan data? Check out Gravwell

119.96.103.5

CHINANET Hubei province network
■ China, Shanghai
self-signed

SSL Certificate Issued By: Remote Desktop Protocol
I-Common Name: \x03\xad\x0d\x0b\x13\xde\x0f\x00\x00\x00\x12\x00\x02\x02\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol IISU Info:
OS: Windows 7/Windows Server 2008 R2
OS Build: 6.1.7601
Target Name: 38-60009854-004
NetBIOS Domain Name: 38-60009854-004
NetBIOS Computer Name: 38-60009854-004

Supported SSL Versions:
TLSv1, TLSv1.1,
TLSv1.2

Diffe-Hellman Fingerprint:
RFC2409/Oakley
Group 2

TOP PORTS
3389 193,836

95.110.250.126

2022-12-20T02:31:25.666912

Рис. 3.13. Похоже, ОС Windows 7 установлена более чем на 375 000 устройств, подключенных к Сети

Ничего себе! Даже в 2023 году 375 940 систем продолжают работать на Windows 7. Это ведь огромное поле для потенциального взлома!

Помимо прочего, Shodan позволяет отслеживать, не появились ли новые устройства на заданных сайтах и IP-адресах. Благодаря функции мониторинга специалисты по кибербезопасности могут отслеживать действия в определенном диапазоне IP-адресов, например 71.6.146.0/24. Это дает несколько важных преимуществ.

- **Обнаружение новых устройств.** Благодаря отслеживанию выбранного диапазона можно фиксировать новые подключения к сети. Так вы будете знать, что в ней находятся только авторизованные устройства, и выявлять несанкционированный доступ, который может представлять угрозу безопасности.
- **Выявление уязвимостей.** С помощью Shodan специалисты находят устройства с известными уязвимостями в заданном диапазоне IP-адресов. Это позволяет устранять проблемы безопасности еще до того, как ими воспользуются злоумышленники.
- **Отслеживание изменений и отклонений.** Инструмент помогает отслеживать изменения в сетевой конфигурации, например фиксировать открытые порты, активные службы или обновления прошивки. Любые отклонения могут свидетельствовать о возможной угрозе безопасности.
- **Анализ исторических данных.** Shodan хранит исторические данные, по которым можно анализировать изменения в безопасности устройств из выбранного диапазона IP-адресов за определенный период. Тем самым инструмент помогает выявлять долгосрочные риски и оценивать эффективность мер защиты.
- **Настройка оповещений.** В Shodan можно настраивать оповещения на случай выполнения определенных условий в заданном диапазоне IP-адресов. Благодаря этому вы мгновенно узнаете, если появится новое устройство, активируется какой-нибудь сервис или произойдут другие изменения в сети.

Если вы хотите отслеживать диапазон 71.6.146.0/24 с помощью Shodan, необходимо сделать следующее.

1. **Настройка диапазона.** Откройте в Shodan настройки отслеживания и укажите диапазон IP-адресов 71.6.146.0/24.

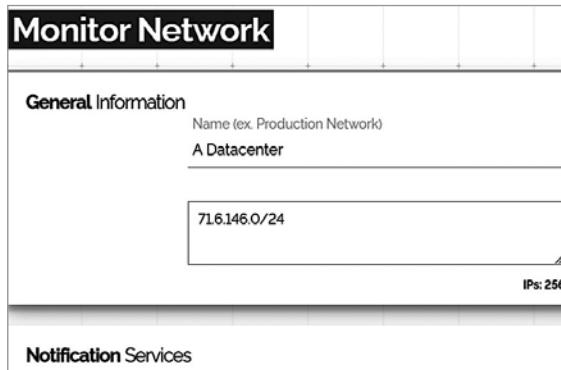


Рис. 3.14. Функция отслеживания Shodan помогает наблюдать за изменениями

- Настройка оповещений.** Опираясь на собственные требования к безопасности, укажите, при каких событиях система должна вас оповещать. Например, список может включать появление новых устройств, выявление уязвимых сервисов или неожиданные изменения в конфигурации.
- Анализ отчетов.** Shodan формирует отчеты с результатами отслеживания. Необходимо регулярно их просматривать, чтобы понимать текущее состояние сети и оперативно выявлять угрозы безопасности.

The screenshot displays Shodan search results for an IP address. It includes:

- General Information:** Shows the device is located in the United States, specifically in San Jose, belonging to LUOELANG (FRANCE) LIMITED with ASN AS135097.
- Open Ports:** Lists ports 21, 80, and 3306.
- Vulnerabilities:** Lists two issues:
 - CVE-2022-31629: A PHP vulnerability allowing network and same-site attackers to set an insecure cookie.
 - CVE-2022-31628: A PHP vulnerability where the phar decompressor would recursively uncompress "quines" gzip files.
- nginx:** Shows a sample HTTP response header.
- // 21 / TCP:** Shows the vsftpd service.
- // 80 / TCP:** Shows the httpd service.
- // 3306 / TCP:** Shows the mysql service.

Рис. 3.15. Shodan показывает сервисы, порты и уязвимости

4. **Реагирование на оповещения.** Когда система сообщает вам об изменениях в сети, проверьте оповещение и оцените, представляют ли они реальную угрозу безопасности или, наоборот, безобидны.

Научившись применять функцию отслеживания в Shodan, вы сможете держать под контролем безопасность сети в указанном диапазоне IP-адресов, своевременно выявлять потенциальные киберугрозы и предотвращать их, прежде чем уязвимостями воспользуются злоумышленники.

Автоматизация сбора и анализа информации

Итак, настало время поговорить о том, как OSINT меняется с приходом искусственного интеллекта (ИИ). Применяя новые технологии, вы словно устанавливаете мощный турбонаддув, с которым двигатель разведки работает быстрее, эффективнее и, чего скрывать, намного круче.

Где же может пригодиться ИИ? Вот основные направления, в которых он уже демонстрирует свои сильные стороны:

- **Веб-скрейпинг.** С помощью ИИ можно с легкостью извлекать огромные объемы информации из интернет-источников, например форумов и новостных порталов.
- **Анализ тональности.** ИИ способен выявлять эмоциональные оттенки и «вайб» относительно каких-то тем, анализируя громадные объемы текста.
- **Распознавание изображений.** ИИ эффективно собирает ключевую информацию из фото и видео.
- **Выявление закономерностей.** Еще одна интересная область, в которой ИИ наделал шуму. Он просеивает большие массивы данных и выявляет тенденции и закономерности, в том числе помогая разоблачать ложную информацию или фиксировать признаки незаконной деятельности — и все это гораздо быстрее и точнее, чем сделал бы человек.
- **Краткое изложение текста.** Благодаря автоматической обработке больших объемов текста ИИ помогает отслеживать тенденции и смену общественного мнения на различные темы.

ИИ не просто ускоряет процессы. Он выводит анализ данных на совершенно новый уровень, помогая решать сложные задачи и собирать информацию из разных источников.

Успехи в области ИИ вдохнули новую жизнь в уже знакомый нам сервис Maltego (<https://www.maltego.com>), незаменимый в разведке, как степлер в работе офисного служащего. Этот инструмент предлагает визуальную среду, в которой можно создавать карты сетей и киберугроз. Вы словно берете в руки лупу и рассматриваете через нее каждую деталь соединенных воедино фактов, получая более полное представление о ситуации.

Maltego отлично подходит как для отслеживания цифровых следов, так и для анализа кибератак. Благодаря плагинам и трансформациям с органично интегрированным в них ИИ такие задачи стали выполняться донельзя просто. Сервис объединяет разрозненные фрагменты данных в целостную структуру, что позволяет проводить более глубокий и сложный анализ. На этой платформе вы получаете наглядные графы, которые демонстрируют связи и отношения между различными цифровыми сущностями. Нити взаимосвязей переплетаются в единое полотно прямо на ваших глазах. Посмотрите, что сервис обнаружил в следующем примере.

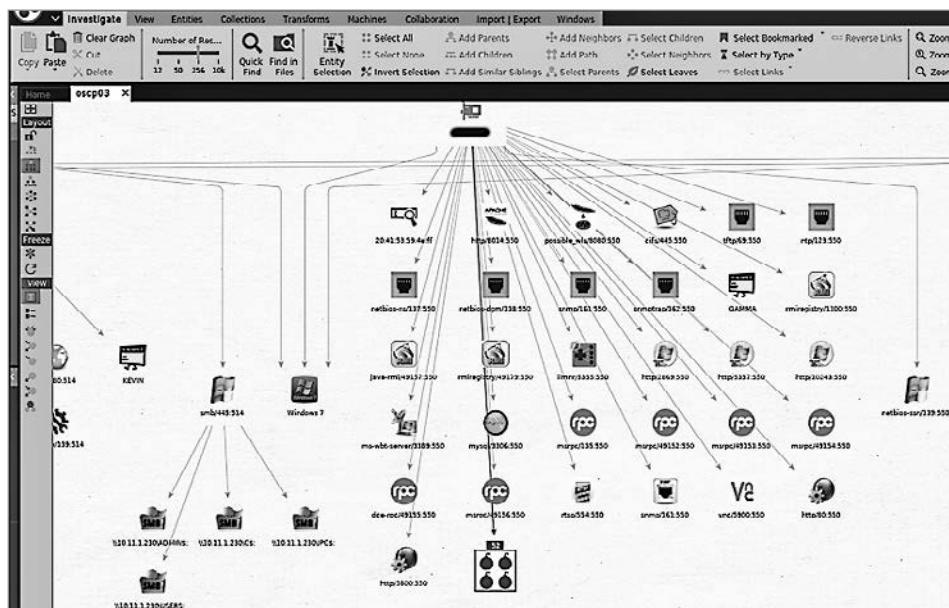


Рис. 3.16. Результаты расследования Maltego

Я считаю, что использование ИИ в OSINT — уже не модное увлечение, а суро-вая необходимость. Традиционные способы извлечения информации больше не справляются с лавиной данных, которую нам приходится обрабатывать.

Итоги

Важно помнить, что интернет наводнен различного рода сведениями, но среди них пустой руды не меньше, чем золотого песка. Во время анализа каждого фрагмента данных используйте свое критическое мышление, чтобы отделять факты от вымыслов. Это ваш способ защитить себя в цифровом мире: прежде чем посчитать какую-либо информацию достоверной, проверьте ее в авторитетных источниках. Простой осторожности недостаточно — важно научиться распознавать обман и действовать рационально. Мы видели, что даже изображения, метаданные или устройства интернета вещей могут содержать ценную информацию о вашей компании или цели расследования. И порой мы об этом даже не задумываемся. Но, опять же, сведения, извлеченные в ходе разведки, необходимо проверять дважды, а то и трижды. Так что включайте голову и помните, что благодаря здоровому скептицизму можно добиться точных и объективных результатов.

В следующей главе мы обсудим полезные инструменты и техники для поиска *скрытых* жемчужин информации.

ГЛАВА 4

ИССЛЕДУЕМ НЕИЗВЕСТНОЕ: КАК НАЙТИ ИНФОРМАЦИЮ С ПОМОЩЬЮ ИНСТРУМЕНТОВ ПОИСКА

В этой главе я познакомлю вас с инструментами поиска и важнейшими утилитами, которые помогают добиться большего успеха во время разведки по открытым источникам (OSINT). Без этих знаний не обойтись, если вы хотите выйти за рамки обычного поиска и в полной мере использовать информационные ресурсы.

Инструменты поиска позволяют находить скрытые или труднодоступные данные, что повышает точность и интерпретируемость результатов расследования. Такие средства просто необходимы каждому специалисту OSINT, чем бы он ни занимался: анализом потенциальных угроз, анализом конкурентов или просто исследованием материалов на определенную тему.

В этой главе вас ждут следующие разделы:

- Знакомство с инструментами поиска
- Анализ доменов и IP-адресов
- Исследование сайтов: работа со скрытыми данными
- Анализ документов и метаданных
- Визуализация данных OSINT
- Рекомендации по эффективной работе с инструментами поиска

К концу главы вы будете лучше понимать роль инструментов поиска в OSINT, научитесь правильно использовать их для сбора, анализа и интерпретации данных и тем самым усовершенствуете навыки разведки.

Давайте погрузимся в эту главу и откроем еще больше возможностей OSINT!

Знакомство с инструментами поиска

В OSINT-исследованиях инструменты поиска играют ключевую роль, позволяя аналитикам находить в общедоступных источниках ту информацию, которая осталась бы незамеченной при других подходах. Они помогают выявлять скрытые детали и взаимосвязи, а также формировать новые гипотезы, что делает их неотъемлемой частью профессиональных расследований.

Существуют различные типы инструментов поиска, каждый из которых используется для собственных целей. Например, средства анализа доменов и IP-адресов могут восстанавливать историю владения сайтами или сетями, а также получать сведения об их регистрации. Инструменты веб-скрейпинга и архивирования извлекают контент, код и метаданные веб-страниц. Программы для анализа документов позволяют находить метаданные и другую скрытую информацию внутри файлов, а средства визуализации упрощают поиск взаимосвязей в запутанных массивах данных.

Правильно применяя такие инструменты, OSINT-аналитики способны перейти от простого поиска в Google к извлечению ценных сведений из общедоступных источников. Словно с металлоискателем в руках, они находят клад — информацию, которая проливает свет на объект расследования. Однако помните, что применять такие средства нужно строго в рамках правовых и этических норм.

Освоив работу с инструментами поиска, специалисты по безопасности смогут находить важные сведения о людях, организациях, местах и событиях.

Раскрываем тайны сети

Цифровой след — настоящая сокровищница, в которой хранится полное досье на нашу онлайн-личность. Развитие интернета заставляет нас внимательнее следить за тем, какую информацию люди и организации оставляют в Сети.

Почему же цифровой след играет такую большую роль? Дело в том, что мы живем в эпоху взаимосвязей, где данные ценятся так же высоко, как и золото. Вместе с информацией вы получаете возможности разрабатывать стратегии, внедрять инновации или превосходить конкурентов.

Мы поговорили о том, как инструменты поиска в OSINT помогают вам достигать целей, а теперь пора сосредоточиться на одном из ключевых навыков в арсенале аналитика: анализе доменов и IP-адресов. Поразительно, как много можно узнать об истории и связях сайта, просто изучив эти данные. Давайте разберемся, как именно происходит анализ и почему специалисты по безопасности так ценят этот инструмент.

Анализ доменов и IP-адресов

Знакомьтесь, **WHOIS** — инструмент, проливающий свет на регистрацию доменов и поднимающий завесу онлайн-анонимности. Доменные имена, которые мы видим при посещении сайтов или отправке электронных писем, — не просто цифровые адреса. Это настоящие врата в хранилище данных, а WHOIS — ключ, способный их открыть.

Как работает WHOIS и зачем он нам нужен

Чтобы выполнить поиск в WHOIS, нужно отправить запрос на один из его серверов, которые управляют базами **доменов верхнего уровня** (TLD, top-level domains). Сервер проверяет базу и в ответ выдает доступные сведения о регистрации объекта, которые включают информацию о регистраторе, контакты владельца, серверы имен, даты регистрации и окончания срока действия, а также текущий статус. Вот как это происходит:

1. Вы отправляете команду WHOIS. Она перенаправляется на соответствующий сервер WHOIS, который обрабатывает запросы о доменах верхнего уровня. Например, для доменов .com, .org или .net это один сервер, а для национальных кодов, таких как .uk или .ca, — другой. Каждому домену выделен свой сервер WHOIS.
2. Сервер WHOIS принимает и обрабатывает ваш запрос. Затем он ищет в своей базе данных сведения, относящиеся к заданному доменному имени или IP-адресу.
3. Если сервер обнаруживает совпадение, он формирует ответ, содержащий множество сведений. Среди них:
 - **Информация о владельце** (registrante): имя, адрес и контактные данные.
 - **Информация о регистраторе**: сведения о компании, зарегистрировавшей домен.
 - **Серверы имен**: серверы, управляющие DNS-записями домена.

- **Даты создания и окончания срока:** время регистрации домена и окончания срока действия.
 - **Статус:** текущее состояние домена (активен, приостановлен или находится в другом состоянии).
 - **DNSSEC:** использует ли домен расширения протокола DNS для дополнительной защиты.
4. Сервер WHOIS подготавливает структурированный ответ и отправляет его на ваш компьютер. Формат может отличаться в зависимости от сервера WHOIS и заданного домена верхнего уровня, но чаще всего ответ представляет собой обычный текст.
5. Компьютер выводит ответ WHOIS на экран. Как специалист по кибербезопасности вы анализируете выдачу, чтобы получить информацию о владельце домена, историю регистрации и другие важные сведения.

Когда я открыл терминал, меня встретил черный экран в ожидании команды. Отправив простой запрос, я пробудил зверя:

```
whois daledumbsitdown.com
```

Результаты выполнения команды показаны на следующем скриншоте.

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: daledumbsitdown.com
Registry Domain ID: 1972026533_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.eu
Registrar URL: http://www.registrar.eu
Updated Date: 2023-09-26T19:42:16Z
Creation Date: 2015-10-26T17:41:51Z
Registrar Registration Expiration Date: 2024-10-26T17:41:51Z
Registrar: Hosting Concepts B.V. d/b/a Registrar.eu
Registrar IANA ID: 1647
Registrar Abuse Contact Email: abuse@registrar.eu
Registrar Abuse Contact Phone: +31.104482297
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Whois Privacy Protection Foundation
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Zuid-Holland
Registrant Postal Code: REDACTED FOR PRIVACY
```

Рис. 4.1. Результаты поиска WHOIS по запросу daledumbsitdown.com

Экран ожила, заполнившись строками данных о домене. Я получил не просто ответ — я получил историю, биографию, уникальный отпечаток.

WHOIS – больше чем обычный инструмент; это общедоступная база данных, содержащая важную информацию о доменах и IP-адресах. Кому принадлежит домен? Когда он был зарегистрирован? Когда заканчивается срок его действия? Вопросы, эхом отзывающиеся в сердцебиении домена, которое не всегда слышат, но существование которого бесспорно.

Применение WHOIS: домены и блоки IP-адресов

Мир сетевой информации гораздо сложнее, чем кажется на первый взгляд. Если у каждого сайта есть уникальный домен, то у каждого устройства в интернете – собственный IP-адрес, неповторимый набор цифр, который позволяет отличать его от миллионов других устройств. А некоторые компании владеют целыми блоками IP-адресов, что делает разведку еще интереснее, добавляя больше возможностей для сбора полезной информации.

С помощью протокола WHOIS можно анализировать эти блоки и получать данные о распределении IP-адресов и организациях, которые их контролируют.

Например, исследовав IP-адрес 8.8.8.8, я быстро обнаружил полный блок адресов, принадлежащих компании Google.

NetRange:	8.8.8.0 - 8.8.8.255
CIDR:	8.8.8.0/24
NetName:	GOGL
NetHandle:	NET-8-8-8-0-2
Parent:	NET8 (NET-8-0-0-0-0)
NetType:	Direct Allocation
OriginAS:	
Organization:	Google LLC (GOGL)
RegDate:	2023-12-28
Updated:	2023-12-28
Ref:	https://rdap.arin.net/registry/ip/8.8.8.0
 KALI LINUX ...become, the more you are able	
OrgName:	Google LLC
OrgId:	GOGL
Address:	1600 Amphitheatre Parkway
City:	Mountain View
StateProv:	CA
PostalCode:	94043
Country:	US
RegDate:	2000-03-30
Updated:	2019-10-31

Рис. 4.2. Блок IP-адресов Google, найденный с помощью WHOIS

WHOIS помогает составить карту современного интернета. Этот инструмент очерчивает границы и записывает историю, вселяя надежду, что огромный, непредсказуемый цифровой мир не останется неизведанным.

Увеличительное стекло: удобные платформы для поиска в WHOIS

Киберпространство заполнено ресурсами, которые говорят на языке WHOIS, но мало кто действительно понимает этот язык. Некоторые из таких ресурсов заслуживают особого внимания.

DomainTools

DomainTools (<https://www.domaintools.com/>) — инструмент для поиска в WHOIS, показывающий весьма подробную информацию о доменном имени. Просто введите имя в строку поиска DomainTools, и вы получите сведения о регистраторе, статусе регистрации и серверах имен, а также контактные данные владельца.

The screenshot shows the DomainTools homepage with the search bar set to "Whois Lookup". Below the search bar, the URL "Home > Whois Lookup > DaleDumbSitDown.com" is displayed. The main content area is titled "Whois Record for DaleDumbSitDown.com". Under the heading "Domain Profile", there is a table with the following data:

Registrar	Hosting Concepts B.V. d/b/a Registrar.eu IANA ID: 1647 URL: https://www.registrar.eu , http://www.openprovider.com Whois Server: whois.registrar.eu abuse@registrar.eu (p) +31.104482297
Registrar Status	clientTransferProhibited
Dates	3,046 days old Created on 2015-10-26 Expires on 2024-10-26 Updated on 2023-09-26
Name Servers	NS1.DNS-PARKING.COM (has 4,521,574 domains) NS2.DNS-PARKING.COM (has 4,521,574 domains)
IP Address	154.62.106.83 - 787 other sites hosted on this server
IP Location	CA - California - Los Angeles - Hostinger International Limited

Рис. 4.3. Результаты поиска в DomainTools

Среди важных данных, которые предоставляет инструмент:

- даты регистрации и окончания срока действия домена;
- компания-регистратор, зарегистрировавшая домен;
- имя, номер телефона и адрес владельца домена;
- контактные данные администратора и технического специалиста для управления доменом;
- серверы имен и информация о DNS.

DomainTools берет данные из авторитетных баз WHOIS для каждого домена верхнего уровня, предоставляя быстрый доступ к перечисленным сведениям. Благодаря этому инструменту можно анализировать домены и отслеживать регистрации, что полезно в целях безопасности.

Whois.com

Whois.com — элегантный и лаконичный. Сайт словно развеивает цифровой туман, обнажая истинную сущность каждого домена и оставляя за кадром лишние детали (рис. 4.4).

В то время как WHOIS раскрывает регистрационные данные о доменных именах, владельцы сайтов, наоборот, все чаще пытаются скрыть эти сведения, прибегая к сервисам по защите конфиденциальности или прокси-серверам, которые заменяют имя, адрес, телефон и электронный адрес владельцев своей собственной контактной информацией. Благодаря этому регистранты могут сохранить анонимность.

Однако такие сервисы не обеспечивают абсолютной конфиденциальности. По закону в случае судебного запроса они обязаны раскрыть сведения о владельце домена. Так что правоохранительные органы или владельцы прав на интеллектуальную собственность могут обратиться в суд с требованием прекратить защиту конфиденциальности и сообщить им данные, которые помогут выявить мошенников и других нарушителей. Услуги, которые предлагают сервисы конфиденциальности, хоть и повышают анонимность, но не гарантируют ее в случае запроса от органов власти.

А хотите заглянуть в прошлое? В те времена, когда пользователи еще не заботились о конфиденциальности? Если да, у меня для вас кое-что есть! Сайт WHOXY (<https://www.whoxy.com/>) открывает доступ к исторической информации о доменах. Например, вот такие данные удалось получить о сайте <https://www.daledumbssitdown.com/> (рис. 4.5).

The screenshot shows the Whois.com website interface. At the top, there is a navigation bar with links for Domains, Hosting, Servers, Email, Security, Whois, and Deals, along with a search bar and a button labeled "Enter Dom". Below the navigation bar, the domain name "daledumbsitdown.com" is displayed, with a timestamp "Updated 1 second ago" and a refresh icon. The main content area is divided into two sections: "Domain Information" and "Registrant Contact".

Domain Information

Domain:	daledumbsitdown.com
Registrar:	Hosting Concepts B.V. d/b/a Registrar.eu
Registered On:	2015-10-26
Expires On:	2024-10-26
Updated On:	2023-09-26
Status:	clientTransferProhibited
Name Servers:	ns1.dns-parking.com ns2.dns-parking.com

Registrant Contact

Organization:	Whois Privacy Protection Foundation
State:	Zuid-Holland
Country:	NL
Email:	https://contact-form.registrar.eu/?domainName=daledumbsitdown.com&purpose=owner

Рис. 4.4. Результаты поиска на whois.com
по запросу daledumbsitdown.com

Каждый из инструментов предлагает уникальный способ анализа цифровой среды. Они работают как разные линзы микроскопа, показывая слои, детали и грани, которые в противном случае остались бы неисследованными.

Who owned daledumbositdown.com in the past? (4 records)

Name: DALE MEREDITH (14 domains)
Company: SMARTYPANTZ (15 domains)
Email: dale.meredith@gmail.com (14 domains)
Country: United States (223 million domains from United States for \$6,000)
Nameservers: ns1.bluehost.com, ns2.bluehost.com
Status: clientTransferProhibited
Name: REDACTED FOR PRIVACY (329 million domains) [UPDATED]
Company: Whois Privacy Protection Foundation (2.45 million domains) [UPDATED]
Country: Netherlands (6.2 million domains from Netherlands for \$500)
Nameservers: ns1.dns-parking.com, ns2.dns-parking.com [UPDATED]
Status: clientTransferProhibited, ok [UPDATED]
Name: REDACTED FOR PRIVACY (329 million domains)
Company: Whois Privacy Protection Foundation (2.45 million domains)

Рис. 4.5. Результаты поиска на whoxy.com по запросу daledumbositdown.com

Поиск взаимосвязей

Изучение взаимоотношений между доменами и определение их владельцев с помощью WHOIS — важная часть расследования в сфере кибербезопасности, особенно если вы хотите понять, связаны ли между собой различные онлайн-ресурсы. Ниже подробно описан процесс работы:

- Исследуйте основной домен.** Для начала запросите в базе WHOIS информацию об основном домене, который вас интересует. Например:
whois daledumbositdown.com

Так вы получите доступ к сведениям о регистрации и владельце.

2. **Найдите серверы имен.** В результатах от WHOIS найдите серверы имен. Они отвечают за хранение записей DNS для домена. Часто данные бывают представлены следующим образом:

```
Registrar Abuse Contact Phone: +31.104482297
Domain Status: clientTransferProhibited https://ica
Name Server: NS1.DNS-PARKING.COM
Name Server: NS2.DNS-PARKING.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: h
>> Last update of whois database: 2023-10-16T20:38:28
```

Рис. 4.6. Серверы имен для daledumbsitdown.com

3. **Проанализируйте серверы имен.** Теперь отправьте отдельные WHOIS-запросы о каждом найденном сервере имен. Например:

```
whois ns1.dns-parking.com
whois ns2.dns-parking.com
```

Примечание

В ответ на эти запросы вы получите информацию о самих серверах имен и сможете выявить другие домены, которые используют те же серверы. Такая информация поможет найти связанные домены.

4. **Определите общих владельцев.** Просмотрите результаты поиска серверов в WHOIS и найдите общих registrantов. (Напомню, registrant — это организация или человек, зарегистрировавший домен.) Совпадения в именах или контактных данных в нескольких доменах могут указывать на потенциальную связь с общим владельцем.
5. **Изучите поддомены и дополнительные домены.** Помимо серверов имен, стоит изучить поддомены и другие домены, связанные с основным. Например:

```
whois subdomain.daledumbsitdown.com
whois additional-daledumbsitdown.com
```

Темная сторона: как злоумышленники используют WHOIS

А теперь задумайтесь: с помощью WHOIS хакеры могут собрать имена и электронные адреса, указанные при регистрации доменов, и впоследствии совершить грандиозную фишинговую атаку. Большинство людей не

задумается, увидев письмо со знакомым именем отправителя. Скорее всего, жертва откроет письмо, нажмет ссылку и попадет в ловушку. Идеальная приманка.

Но это еще не все. Злоумышленники зорко следят за сроком действия доменов, и, когда он истекает, выкупают домен быстрее, чем вы успеете сказать «кибербезопасность». Для чего? Завладев им, можно без труда распространять вредоносные программы или перенаправлять наивных пользователей на вредоносные сайты.

Но погодите, на этом киберпреступники не останавливаются. Они используют приемы социальной инженерии, чтобы обмануть владельцев доменов или тех, кто указан в базе WHOIS как контактное лицо, и выманивать у них право на домен. Похоже на махинации с недвижимостью, только в цифровом мире: злоумышленники захватывают сайты и используют их в своих преступных целях.

О серверах имен тоже не стоит забывать. Данные WHOIS могут раскрывать информацию о компонентах интернет-инфраструктуры, делая их мишенью для DDoS-атак или перехвата DNS-запросов. Подделав DNS-запросы, киберпреступники перенаправляют ничего не подозревающих пользователей на вредоносные ресурсы.

Чтобы замести следы, злоумышленники применяют прокси-серверы, когда атакуют базы данных WHOIS в поисках новых целей и уязвимостей. Для таких людей WHOIS – не просто источник сведений, а готовый план действий для осуществления разрушительных замыслов.

Анализ DNS и IP-адресов: связь доменов с инфраструктурой

Инструменты OSINT открывают доступ к данным о DNS и IP-адресах, помогая выявлять скрытые связи между доменами и их инфраструктурой. Например, запрос DNS для домена `hackthissite.org` (команда `dig hackthissite.org`) может показать IP-адреса, которые с ним связаны.

```
(kali㉿kali)-[~]
└$ dig hackthissite.org

; <>> DiG 9.19.17-1-Debian <>> hackthissite.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 13300
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;hackthissite.org.      IN      A

;; ANSWER SECTION:
hackthissite.org.    3600    IN      A      137.74.187.102
hackthissite.org.    3600    IN      A      137.74.187.100
hackthissite.org.    3600    IN      A      137.74.187.101
hackthissite.org.    3600    IN      A      137.74.187.104
hackthissite.org.    3600    IN      A      137.74.187.103
```

Рис. 4.7. Результаты выполнения команды dig hackthissite.org

И наоборот — можно выполнить обратный поиск DNS по IP-адресу (`dig -x 137.74.187.102`), чтобы найти связанные имена хостов.

```
(kali㉿kali)-[~]
└$ dig -x 137.74.187.102

; <>> DiG 9.19.17-1-Debian <>> -x 137.74.187.102
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 35
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;102.187.74.137.in-addr.arpa. IN      PTR

;; ANSWER SECTION:
102.187.74.137.in-addr.arpa. 21600 IN      PTR      hackthissite.org.

;; Query time: 220 msec
;; SERVER: 10.10.10.1#53(10.10.10.1) (UDP)
;; WHEN: Mon Oct 16 16:17:15 MDT 2023
;; MSG SIZE  rcvd: 86
```

Рис. 4.8. PTR-запись для 137.74.187.102

В этом примере мы не видим других доменов, потому что их нет на этом хосте, но в некоторых случаях можно получить вот такие результаты:

```
;; ANSWER SECTION:  
host1234.examplehosting.com. 3600 IN A 93.184.216.34  
site1.com. 3600 IN CNAME host1234.examplehosting.com.  
site2.net. 3600 IN CNAME host1234.examplehosting.com.  
site3.org. 3600 IN CNAME host1234.examplehosting.com.
```

Если вы используете клиент на Windows, выручит команда nslookup. Она будет выглядеть так:

```
nslookup hackthissite.org
```

Результаты выполнения команды показаны на следующем скриншоте.

```
Non-authoritative answer:  
Name: hackthissite.org  
Address: 137.74.187.102  
Name: hackthissite.org  
Address: 137.74.187.100  
Name: hackthissite.org  
Address: 137.74.187.104 (14 domains)  
Name: hackthissite.org (13 domains)  
Address: 137.74.187.101  
Name: hackthissite.org  
Address: 137.74.187.103  
Name: hackthissite.org  
Address: 2001:41d0:8:ccd8:137:74:187:102  
Name: hackthissite.org  
Address: 2001:41d0:8:ccd8:137:74:187:100  
Name: hackthissite.org  
Address: 2001:41d0:8:ccd8:137:74:187:104  
Name: hackthissite.org  
Address: 2001:41d0:8:ccd8:137:74:187:103  
Name: hackthissite.org  
Address: 2001:41d0:8:ccd8:137:74:187:101
```

Рис. 4.9. Результаты выполнения команды nslookup для `hackthissite.org`

И это далеко не все!

Записи DNS – кладезь информации для OSINT-расследования. Запрашивая определенные их типы, аналитик может заполучить ценные сведения об интернет-ресурсах и инфраструктуре организации. Далее мы рассмотрим основные типы записей DNS и то, как с их помощью извлекать информацию.

A- и AAAA-записи

A- и **AAAA**-записи используются для связи доменных имен с IP-адресами: A-запись с IPv4 и AAAA – с IPv6. Исследование A-записи помогает определить IP-адрес, на котором размещен домен, и тем самым открывает возможность для более глубокого анализа: применив обратный поиск DNS, вы найдете другие домены в том же IP-адресе и выявите связь между ними.

Обратиться к A-записи можно с помощью команды nslookup:

```
nslookup
> set type=A
> daledumbositdown.com
```

Результаты выполнения команды показаны на следующем скриншоте:

```
PowerShell 7.3.8
PS C:\Users\dalem> nslookup
Default Server: dns.google
Address: 8.8.8.8

> set type=A
> daledumbositdown.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: daledumbositdown.com
Address: 84.32.84.227

>
```

Рис. 4.10. Поиск A-записи для daledumbositdown.com

MX-записи

MX-записи (Mail Exchange) задают почтовые серверы, которые будут обрабатывать электронную почту в домене. Просматривая такие записи, можно

получить информацию о почтовой инфраструктуре и впоследствии совершить атаку, например, с помощью взлома или социальной инженерии. Для перечисления MX-записей можно использовать инструменты вроде nslookup. Запросим записи напрямую и посмотрим, как устроена почтовая система.

Сначала введите nslookup и нажмите Enter:

```
nslookup  
> set type=MX  
> daledumbositdown.com
```

Результаты выполнения команды показаны на следующем скриншоте.

```
> set type=mx  
> daledumbositdown.com  
Server: dns.google  
Address: 8.8.8.8  
  
Non-authoritative answer:  
daledumbositdown.com      MX preference = 10, mail exchanger = mx2.hostinger.com  
daledumbositdown.com      MX preference = 5, mail exchanger = mx1.hostinger.com  
> |
```

Рис. 4.11. MX-записи, полученные в результате выполнения команды nslookup

Мы видим, что у домена daledumbositdown.com два приоритетных почтовых сервера.

Примечание

Когда речь заходит о приоритетах, значение в строке preference = X определяет, к какому серверу подключаться в первую очередь. Чем меньше число, тем выше приоритет. Так что в нашем случае запись с номером 5 (`mx1.hostinger.com`) будет использована раньше всех.

TXT-записи

TXT-записи предназначены для хранения произвольной текстовой информации о домене. Они часто содержат SPF-записи, определяющие авторизованные почтовые серверы домена, и другие конфигурационные данные. Сбор таких сведений из TXT-записей помогает узнать, как именно организована инфраструктура отправки почты.

```
> set type=txt
> daledumbssitdown.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
daledumbssitdown.com      text =
"google-site-verification=FZnGQZA-xR4TrUjCak_3zyPfhSc8BTM1zV0w2X80LAE"
daledumbssitdown.com      text =
"v=spf1 include:_spf.mail.hostinger.com ~all"
daledumbssitdown.com      text =
"pinterest-site-verification=881a39213331c0b4ead786126f31d959"
daledumbssitdown.com      text =
"google-site-verification=7NNP3Uqgi8cVyDGbcpy8BOGItdFQV1Ug0YFVBsiWlaU"
>
```

Рис. 4.12. TXT-записи, полученные в результате выполнения команды nslookup

CNAME-записи

CNAME-записи (Canonical Name) связывают псевдоним («алиас») домена с настоящим доменным именем и могут выдать связь между доменами и upstream-провайдерами.

```
> set type=cname
> hackthissite.org
Server: dns.google
Address: 8.8.8.8

hackthissite.org
    primary name server = c.ns.buddyns.com
    responsible mail addr = admin.hackthissite.org
    serial = 2023040305
    refresh = 3600 (1 hour)
    retry = 900 (15 mins)
    expire = 604800 (7 days)
    default TTL = 86400 (1 day)
> |
```

Рис. 4.13. Псевдонимы для hackthissite.org

С помощью этих и других записей DNS специалисты OSINT могут составить подробную карту интернет-объектов и связей, имеющихся у интересующей

организации или домена. В следующей главе мы рассмотрим дополнительные приемы сбора информации об инфраструктуре.

Карта цифрового следа: анализ DNS и IP-адресов

Анализ DNS и IP-адресов помогает раскрыть сетевую инфраструктуру и взаимосвязи организации с другими пользователями. Вот для чего это может пригодиться:

- **Создание карты инфраструктуры.** Запросы на DNS-сервер помогают найти IP-адреса, серверы имен, почтовые серверы и другие узлы сети, связанные с заданным доменным именем. Обратный поиск DNS по IP-адресам дополнительно выявляет новые домены и объекты, связанные с инфраструктурой. Собрав все данные воедино, можно визуализировать цифровой след объекта разведки.
- **Определение виртуального хостинга.** Запросы DNS часто помогают выявить несколько доменов, размещенных на одном сервере или в диапазоне IP-адресов. Такое размещение может указывать на то, что домены принадлежат одной организации, даже если их данные в WHOIS отличаются.
- **Подтверждение связей между доменами.** Благодаря сопоставлению подсетей, серверов имен, IP-адресов и других записей DNS можно установить, связаны ли домены между собой. Если да, этот факт, в свою очередь, подтверждает существование дочерних сайтов, поддоменов, партнерских ресурсов и т. п.
- **Обнаружение новых доменов.** Наблюдая за изменениями записей DNS, можно находить недавно зарегистрированные домены, возникающие в текущей инфраструктуре, что особенно важно для отслеживания новых объектов.
- **Отслеживание изменений в инфраструктуре.** Изменения записей DNS могут сигнализировать о миграции серверов, реструктуризации сети, сбоях или смене владельца.
- **Определение местоположения хостинга.** Анализ IP-геолокации помогает определить физическое расположение серверов, дополняя знания об инфраструктуре географическими данными.
- **Выявление сторонних служб.** Исследуя DNS и IP-адреса, а также анализируя имена хостов, можно обнаружить сторонних поставщиков услуг, например CDN, средства защиты от DDoS-атак или сервисы облачного хостинга.

- **Проверка подлинности домена.** Сопоставление IP-адресов с настоящими сайтами позволяет подтвердить подлинность домена и избежать обмана.

Анализ DNS и IP-адресов помогает увидеть цифровой след организации, включая инфраструктуру, взаимосвязи, местоположение, используемые услуги и внесенные изменения. Дополнив свой арсенал разведки этими приемами, вы будете получать бесценную информацию о присутствии цели в интернете.

Трассировка и карты сети: путеводитель по цифровому океану

Работа с современными сетями может оказаться обескураживающе сложной, если не вооружиться подходящими инструментами. **Трассировка и карты сети** помогают разобраться в запутанных потоках информации и без труда в них ориентироваться. Благодаря этим инструментам можно проследить путь данных и получить наглядные маршруты.

Трассировка и утилиты Traceroute

Трассировка — это способ диагностики, который помогает определить маршрут между источником и получателем в IP-сети, например с помощью утилиты Tracerout. Для этого утилита отправляет пакеты UDP или ICMP с нарастающим **временем жизни (TTL, time to live)** и фиксирует адреса устройств, через которые проходят данные.

При отправке пакета первый маршрутизатор («хоп») уменьшает TTL на единицу, а затем пересыпает пакет дальше. Когда значение TTL достигает нуля, маршрутизатор, получивший нулевой пакет, отбрасывает его и возвращает ICMP-уведомление о превышении времени.

В результате система определяет каждый транзитный узел на пути пакета по IP-адресам устройств, отправивших ICMP-ответ. Утилита трассировки увеличивает TTL поэтапно и «шагает» от одного маршрутизатора к другому, пока не достигнет конечной цели.

Пример трассировки маршрута от хоста А к хосту В:

1. Хост А отправляет UDP-пакет с TTL = 1 хосту В.
2. Первый маршрутизатор (R1) уменьшает TTL до 0, отбрасывает пакет и отправляет ICMP-ответ хосту А. В результате идентифицируется R1.

3. Хост А отправляет новый пакет, теперь с TTL = 2. Маршрутизатор R1 уменьшает TTL до 1 и передает пакет дальше на R2. Затем R2 снижает TTL до 0, отбрасывает пакет и отправляет ICMP-ответ. Это позволяет идентифицировать R2.
4. Процесс повторяется с увеличением TTL, пока пакет не достигнет своей цели — хоста В.

На каждом этапе утилиты трассировки (**Tracerout** для Linux и **Tracert** для Windows) фиксирует IP-адрес маршрутизатора и задержку передачи данных. В результате получается наглядная карта маршрута и его производительности, что делает инструмент незаменимым для диагностики сбоев и изучения топологии сети.

Для работы с утилитой Tracerout нужно ввести команду в терминале, указав целевое имя хоста или IP-адрес. В Linux или macOS команда выглядит так:

traceroute destination

Например, чтобы узнать маршрут до сайта daledumbsitdown.com, выполните следующую команду:

traceroute daledumbsitdown.com

Команда запустит трассировку с помощью UDP-пакетов и выведет маршрут, как показано ниже.

```
(kali㉿kali)-[~/Desktop]
└─$ traceroute daledumbsitdown.com
traceroute to daledumbsitdown.com (191.96.144.104), 30 hops max,
 1  firewalla.lan (10.10.10.1)  0.365 ms  0.401 ms  0.359 ms
 2  192.168.1.1 (192.168.1.1)  8.908 ms  8.899 ms  8.828 ms
 3  lo0.mar1.slc.xmission.net (166.70.255.53)  11.686 ms  11.642 ms
 4  br2.core.xmission.net (166.70.1.22)  11.490 ms  11.473 ms  1 ms
 5  ae-15.a03.lsanca07.us.bb.gin.ntt.net (129.250.195.105)  45.1 ms
 6  ae-13.r24.lsanca07.us.bb.gin.ntt.net (129.250.3.141)  44.811 ms
 7  ae-3.r22.dllstx14.us.bb.gin.ntt.net (129.250.7.68)  60.907 ms
 8  ae-15.r21.dllstx14.us.bb.gin.ntt.net (129.250.2.58)  64.911 ms
 9  ae-4.r25.atlnga05.us.bb.gin.ntt.net (129.250.4.117)  86.958 ms
10  129.250.4.67 (129.250.4.67)  86.739 ms  82.010 ms  81.878 ms
```

Рис. 4.14. Результаты трассировки к сайту daledumbsitdown.com

В каждой строке содержится номер и IP-адрес маршрутизатора, а также время задержки.

Звездочки (*) в результатах Traceroute указывают на то, что маршрутизатор на определенном участке пути не отправил ответ. Причин этому может быть несколько:

- **Блокировка брандмауэром.** Маршрутизатор может использовать брандмауэр, который запрещает передачу пакетов ICMP TTL или UDP/TCP, отправляемых утилитой Traceroute. В этом случае маршрутизатор не возвращает ответ.
- **Ограничение частоты ответов.** Для предотвращения перегрузок некоторые маршрутизаторы ограничивают количество обрабатываемых пакетов Traceroute. Если оно превышается, маршрутизатор перестает возвращать ответы.
- **Потери в сети.** Перегрузка сети или сбой при передаче данных могут привести к потере пакета Traceroute, из-за чего маршрутизатор не сгенерирует ответ.
- **Неверный адрес.** Если IP-адрес маршрутизатора недоступен или неверно настроен, пакеты Traceroute не достигают цели, а значит, ответ не формируется.
- **Сбой маршрутизатора.** Устройство может быть выключено, неисправно или недоступно, в результате чего обработка запросов Traceroute невозможна.

Кроме того, при работе с утилитой можно использовать специальные флаги: -T для TCP-трассировки, -m для ограничения числа маршрутизаторов и -r для выполнения обратной трассировки. Пример:

```
traceroute -T -m 50 -r daledumbsitdown.com
```

Эта команда запускает трассировку с использованием TCP в обратном направлении (от конечного узла к исходному), разрешая не более 50 транзитных маршрутизаторов.

Карта сети

Составление карты сети — один из ключевых методов в арсенале OSINT, помогающий изучить цифровой след организации. Этот способ позволяет визуализировать маршруты данных, выявлять критически важные элементы сети и находить связи между устройствами, подключенными к интернету.

Nmap

Nmap помогает исследовать доступные узлы в сети, определяя их службы и операционные системы. Например:

```
nmap 192.168.1.1
```

Команда выполняет базовое SYN-сканирование узла на наличие открытых TCP-портов:

```
nmap -sU -p 123,161 10.0.0.0/24
```

UDP-сканирование для поиска SNMP-сервисов в подсети.

Хотите узнать, какая операционная система работает на целевом узле? Воспользуйтесь следующей командой:

```
nmap -O hackthissite.org
```

А если нужно провести более глубокое, но незаметное исследование, пригодится режим скрытного сканирования:

```
nmap -sS hackthissite.org
```

Возможности Nmap настолько обширны, что этому инструменту можно посвятить отдельную книгу. И такие книги уже есть.

Wireshark

Wireshark – инструмент с открытым исходным кодом, предназначенный для глубокого анализа сетевого трафика, взаимодействий и протоколов. Он позволяет перехватывать пакеты, проходящие через проводные, беспроводные и виртуальные интерфейсы. И о нем тоже уже написаны книги! Итак, вот основные этапы работы с этим инструментом:

1. Запустите Wireshark и начните перехват пакетов на выбранном сетевом интерфейсе. Чтобы выделить трафик, связанный с целевым IP-адресом, примените фильтр, например `ip.addr==154.41.250.193`.
2. Изучите перехваченные пакеты, чтобы найти другие IP-адреса, взаимодействующие с целью. Они могут принадлежать клиентам, серверам или соседним маршрутизаторам.
3. Примените дополнительные фильтры, чтобы изолировать трафик, связанный с обнаруженными IP-адресами. Например, фильтр

`ip.src==192.168.1.105` покажет весь трафик, исходящий с заданного IP-адреса.

4. Проанализируйте запросы и ответы DNS, чтобы изучить сетевой трафик и определить имена хостов. Исследуйте протоколы — это поможет найти открытые порты и узнать, какие сервисы работают на узлах.
5. Нажмите правой кнопкой мыши на поток данных и выберите **Follow TCP Stream**. Эта функция позволит восстановить последовательность данных и найти полезную информацию о функциях и назначении пакетов.

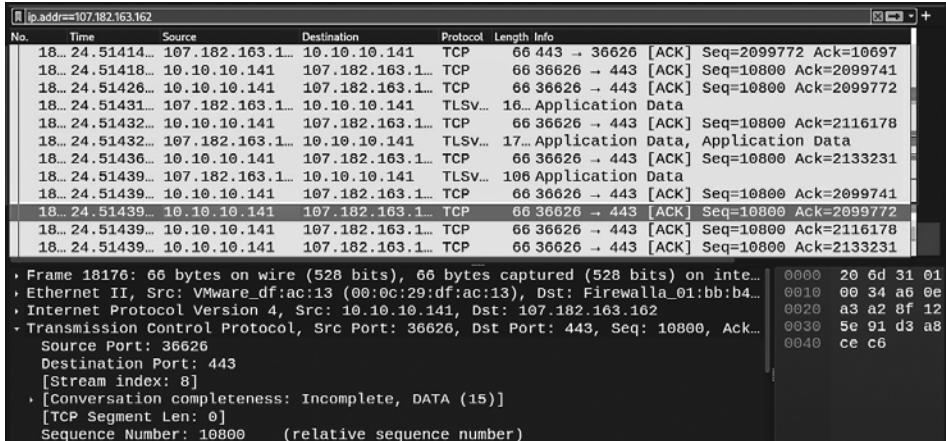


Рис. 4.15. Подключения к сайту daledumbstdown.com, найденные с помощью Wireshark

Используйте возможности Wireshark: применяйте фильтры, анализ TCP и декодирование пакетов, чтобы расширить карту сети. Начиная с целевого IP-адреса (например, `154.41.250.193`), находите новые адреса, имена хостов и взаимосвязи, а также определяйте, какую роль играют соседние узлы.

Чтобы дополнить результаты анализа Wireshark, используйте внешние ресурсы, включая обратный поиск DNS, WHOIS и Nmap. Они помогут лучше исследовать IP-адреса и определить характеристики хостов.

Как видите, Wireshark — незаменимый инструмент для анализа сетевых взаимосвязей и выявления скрытых данных; он может стать вашим

могущественным союзником. Однако на этом разведка не заканчивается. Подготовив карту сети, вы можете перейти на следующий этап — извлечение информации из сайтов.

Исследование сайтов: работа со скрытыми данными

Kali Linux предлагает богатый набор инструментов для исследования сайтов, позволяя собирать и глубоко анализировать информацию, скрытую за привычным интерфейсом.

В этом разделе мы рассмотрим основные средства из арсенала Kali Linux. Вы научитесь автоматизировать сбор данных с помощью веб-скрейпинга, анализировать метаданные в **Metagoofil**, исследовать историю сайта по выдаче **Wayback Machine**, а также искать скрытые файлы и каталоги. Эти техники закладывают фундамент, на который опирается анализ веб-ресурсов и разведка в Сети.

Веб-скрейпинг и анализ данных

Веб-скрейпинг, как мы уже говорили ранее, представляет собой автоматическое извлечение данных с сайтов. В этом помогут специализированные инструменты и скрипты для структурированного сбора и обработки контента, метаданных и другой информации веб-страниц.

Веб-скрейперы извлекают текст, изображения, документы и структурированные данные в больших объемах по всему интернету. Анализируя эти данные, можно выявлять скрытые взаимосвязи, отслеживать изменения, пополнять наборы данных или решать другие задачи.

Итак, о возможностях веб-скрейпинга я рассказал. Теперь рассмотрим инструмент Metagoofil.

Metagoofil

Хотя метаданные хранят полезную информацию, публикация и распространение документов, которые ее содержат, может значительно угрожать безопасности, ведь конфиденциальные сведения становятся доступны всем. Если файлы с метаданными, загруженные в интернет, попадут в руки

злоумышленников, они смогут извлечь скрытую информацию средствами OSINT, чтобы затем использовать ее в своих преступных целях.

И в этом им помогут инструменты вроде Metagoofil, которые позволяют извлекать метаданные из опубликованных документов. Благодаря им можно узнать, к примеру, кто работает в организации или какое ПО в ней используется. Собранные метаданные помогают исследовать безопасность и проверять системы защиты, в том числе:

- разрабатывать более эффективные сценарии для атак с использованием социальной инженерии;
- выявлять версии ПО и тем самым определять его потенциальные уязвимости;
- искать имена и электронные адреса отдельных сотрудников.

Пока что Metagoofil входит в стандартный набор Kali Linux, однако его могут исключить из сборки (такое случается, друзья). Но не беда: вы всегда можете установить его вручную с помощью команды `apt-get`.

Для этого откройте терминал и введите следующее:

```
sudo apt-get install metagoofil
```

Установив Metagoofil, можно отправлять его на поиск метаданных. Например, мы хотим извлечь данные из сайта sans.org, популярного образовательного ресурса по кибербезопасности.

Для этого нужно выполнить команду:

```
metagoofil -d packtpub.com -t doc,pdf -l 20 -n 10 -o packt -f html
```

Рассмотрим ее по частям:

- `-d packtpub.com` — задает домен, на котором нужно выполнить поиск;
- `-t doc,pdf` — определяет форматы искомых файлов;
- `-l 20` — ограничивает количество результатов до 20;
- `-n 10` — ограничивает количество загружаемых файлов до 10;
- `-o` — определяет каталог для сохранения файлов (`packt`);
- `-f html` — задает формат для сохранения результатов (HTML).

Через пару минут Metagoofil начнет выводить результаты в терминале.

```
(kali㉿kali)-[~]
└─$ metagoofil -d packtpub.com -t doc,pdf -l 20 -n 10 -o packt -f hmtl
[*] Searching for 20 .doc files and waiting 30.0 seconds between searches
[*] Results: 0 .doc files found
[*] Searching for 20 .pdf files and waiting 30.0 seconds between searches
[*] Results: 20 .pdf files found
https://www.packtpub.com/sites/default/files/downloads/65720T_ColoredImages.pdf
https://www.packtpub.com/sites/default/files/downloads/Reinforcement_Learning.pdf
https://www.packtpub.com/sites/default/files/downloads/84200T_Bonus_Chapter.pdf
https://www.packtpub.com/sites/default/files/downloads/29010S_ColoredImages.pdf
```

Рис. 4.16. Извлечение метаданных из файлов .doc и .pdf на сайте packtpub.com с помощью Metagoofil

Результаты поиска можно посмотреть в HTML-файле, который сохранен по пути /root/packt/index.html. В нем вас ждет аккуратно оформленная таблица с извлеченными метаданными. Иногда Metagoofil находит названия программ или даже электронные адреса. Это действительно впечатляет!

Да-да, я знаю, о чём вы думаете. Мы все с этим сталкивались: только запускаешь веб-скрейпинг, и вдруг Google выдает ошибку HTTP 429, блокируя IP за слишком большое количество запросов. Досадно! Однако решение есть: с помощью правильных инструментов можно обойти эти ограничения и продолжить поиск. Секрет — прокси-серверы.

Сначала установите proxychains — с ним вы будете вести трафик через несколько прокси-серверов. Запустить установку можно с помощью следующей команды Linux:

```
sudo apt install proxychains4 -y
```

Затем установите файл конфигурации proxychains по пути /etc/proxychains4.conf. Включите режим round_robin, чтобы случайно переключаться между разными прокси-серверами:

```
vim /etc/proxychains4.conf
round_robin
chain_len = 1
proxy_dns
remote_dns_subnet 224
tcp_read_time_out 15000
tcp_connect_time_out 8000
[Список прокси-серверов]
socks4 [ip прокси-сервера и порт]
socks4 [ip прокси-сервера и порт]
```

Примечание

Формат последних строк должен быть таким: `socks4 192.168.0.1 8000`. Напоминаю, чем больше прокси-серверов, тем лучше.

В результате Metagoofil будет автоматически переключаться между прокси-серверами, и вы сможете извлекать информацию без ограничений. Более того, благодаря ротации множества IP-адресов сократится задержка при сборе данных. Однако помните о принципах этичной разведки: соблюдайте правила сайтов, ограничение по количеству данных и требования, описанные в robots.txt. Используя цепочку прокси-серверов, вы сможете избежать блокировки IP-адреса и беспрепятственно извлекать данные.

Анализ и обработка

Следующий этап после извлечения данных — их анализ. В этом пригодится инструмент **grep**, который просеивает контент и ищет определенные шаблоны, ключевые слова или другие запрашиваемые данные. Возможность фильтровать и структурировать информацию превращает обычные данные в полезные данные разведки:

```
grep -ri "pattern" /path/to/downloaded/website/data
```

Знаю, выглядит сложновато, так что давайте разобьем команду на части:

- **grep**. Утилита командной строки для поиска текстовых выражений в файлах. Название расшифровывается как **global regular expression print** (глобальный поиск регулярных выражений и их вывод).
- **-ri**. Параметры команды **grep**:
 - **-r** (или **--recursive**) — поиск выполняется не только в указанном каталоге, но и во всех его подкаталогах.
 - **-i** (или **--ignore-case**) — поиск становится нечувствительным к регистру, поэтому в выдаче по нашему запросу также могут быть, например, Pattern, pattern и pAtTeRn.
- **"pattern"**. Текстовое выражение, которое мы хотим найти. Замените pattern конкретным искомым выражением.
- **/path/to/downloaded/website/data**. Каталог, с которого начинается поиск. Флаг **-r** указывает, что нужно проверить этот каталог и все его подкаталоги.

В результате команда будет просматривать все текстовые файлы в каталоге `/path/to/downloaded/website/data` и его подкаталогах, пытаясь найти строки, совпадающие с заданным текстовым выражением. По окончании поиска утилита выведет результаты на экран.

Wayback Machine и веб-архивы

Wayback Machine открывает окно в прошлое и позволяет узнать, как веб-ресурсы выглядели раньше. В этом сервисе хранятся снимки сайтов, и вы можете получить доступ к версиям веб-страниц и контента, которые уже исчезли из онлайн-пространства.

Архив Wayback Machine бывает невероятно полезен для веб-скрейпинга и OSINT-исследований, предлагая следующие возможности:

- **Доступ к удаленному или измененному веб-контенту.** Wayback Machine хранит версии страниц, которые уже недоступны. Благодаря этому можно извлекать информацию, которую пользователи удалили с сайта.
- **Анализ изменений на сайте.** На платформе легко отслеживать изменения сайта, сравнивая различные версии его кода и структуры.
- **Исследование доменов.** Можно посмотреть, кто владел доменом в разные периоды времени, найти другие сайты, связанные с определенным электронным адресом или именем, а также исследовать предыдущие домены.
- **Поиск скрытых или забытых сайтов.** Архив содержит множество сайтов, которые уже давно не принимают посетителей. Среди них бывают настоящие бриллианты.
- **Создание наборов данных.** Можно целиком извлекать данные как из текущих, так и прошлых версий ресурсов.

Раскрытие информации

Каждый архивированный URL — кусочек сложной головоломки. Он раскрывает важные сведения о безопасности веб-сайта, изменениях контента и структуры. Анализируя такие данные, можно выявлять закономерности и слабые места, а также получать информацию, которая недоступна в текущей версии сайта.

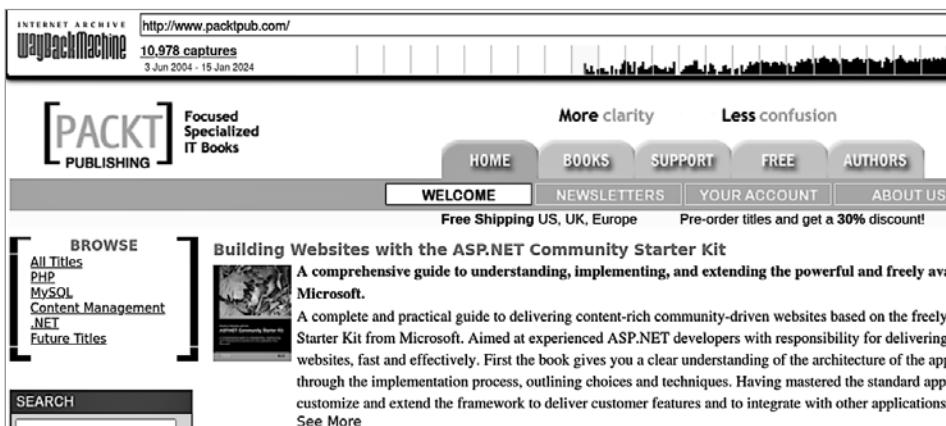


Рис. 4.17. Первая версия веб-страницы издательства «Packt», датированная 2004 годом

Ретроспективный анализ данных с использованием Wayback Machine помогает лучше оценить безопасность сайта. Благодаря этому сервису специалисты могут изучать прошлые уязвимости, отслеживать их исправление и прогнозировать угрозы. Каждая сохраненная страница, каждый архивированный URL становится ценным ресурсом для анализа и помогает формировать стратегию кибербезопасности.

Последовательный перебор файлов и каталогов

На многих сайтах скрываются неопубликованные файлы и каталоги с ценной информацией — настоящие сокровища. Чтобы их обнаружить, специалисты по безопасности используют инструмент **DirBuster** (<https://gitlab.com/kalilinux/packages/dirbuster>). Он отправляет сайту запросы со специальными словами, чем помогает выявлять данные, которые владельцы предпочли скрыть. Опираясь на заранее подготовленный список слов, DirBuster перебирает множество возможных путей к файлам и каталогам, пытаясь найти те, что возвращают не ошибки, а ответы об успешном взаимодействии.

Если DirBuster находит файлы или каталоги, он записывает пути, чтобы вы могли проверить результаты позже. Зачастую эти пути ведут в самые дебри сайта, куда, по мнению его владельца, никто не рискнет заглянуть.

Для тщательного исследования сайта важно запастись терпением и хорошо продумать списки слов, которые подошли бы именно этому ресурсу. DirBuster будет методично «стучаться» во все двери по всем возможным путям, пока не найдет спрятанные цифровые объекты. Его работа похожа на археологические раскопки, где каждая находка пополняет наш сундук с сокровищами.

Инструмент прост в использовании благодаря интуитивно понятному графическому интерфейсу: в DirBuster вы быстро настроите параметры, запустите всесторонний поиск и затем получите точные, исчерпывающие результаты.

Чтобы запустить DirBuster, откройте терминал и выполните команду:

```
dirbuster
```

И вуала! Появился графический интерфейс.

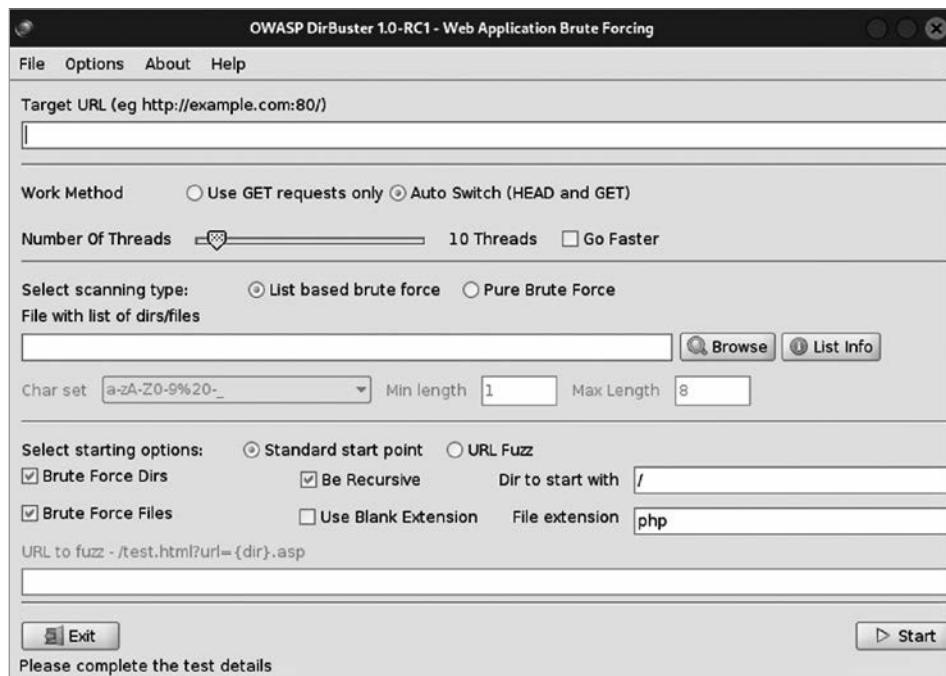


Рис. 4.18. Графический интерфейс DirBuster в Kali Linux

Настройка DirBuster предполагает ввод интересующего вас URL и выбор подходящего списка слов, например из каталога `/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt`. Получив задание, DirBuster отправится на разведку в цифровые лабиринты, и от списка слов и заданных расширений файлов зависит, найдет ли он скрытые ресурсы.

Нажмите **Start**, и DirBuster примется за работу, в точности как показано на скриншоте.

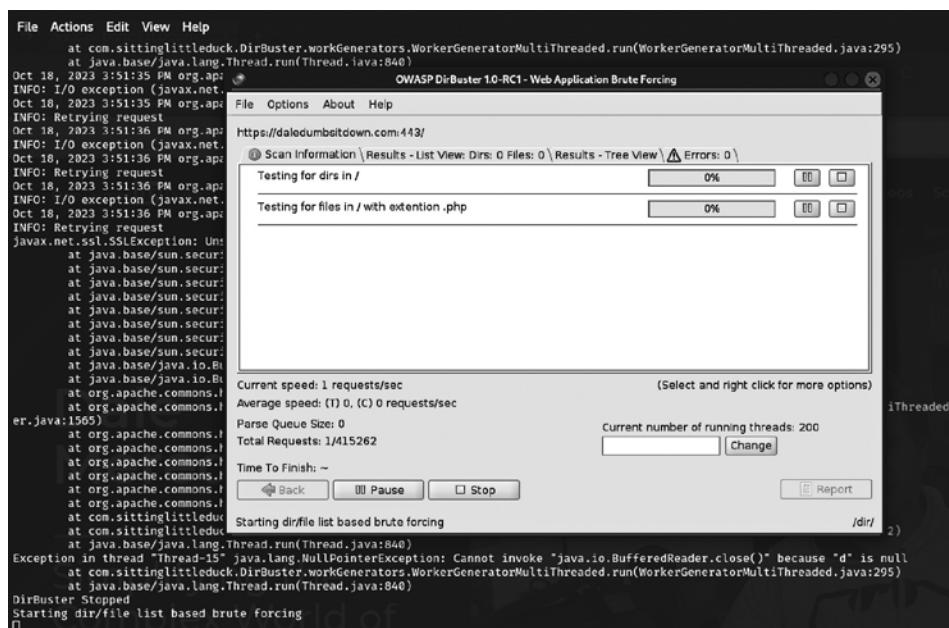


Рис. 4.19. DirBuster сканирует daledumbstidown.com

Анализ robots.txt

Прежде чем запускать DirBuster, стоит проанализировать файл `robots.txt`, чтобы понять, какие разделы сайта скрыты от индексации поисковыми системами. С его помощью сайты передают инструкции поисковым роботам, или веб-краулерам, о том, какие страницы и файлы владелец хочет уберечь от просмотра и индексации. Вот некоторые особенности `robots.txt`:

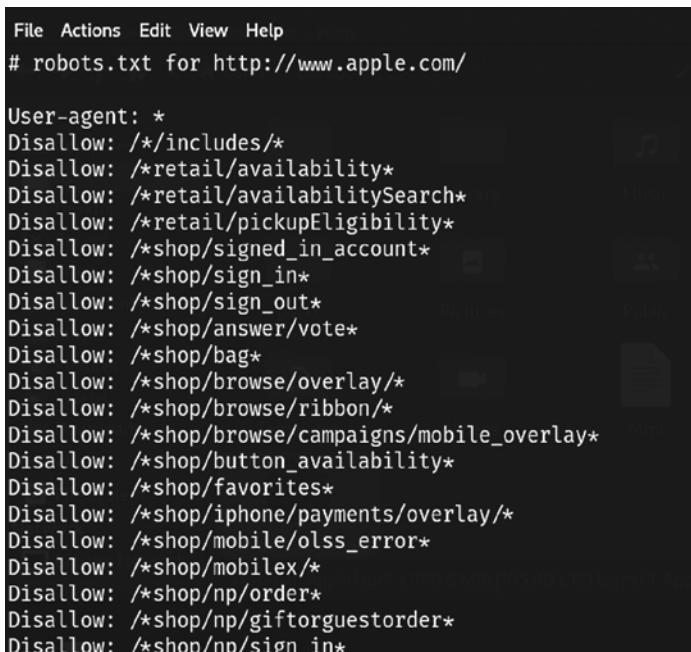
- это текстовый файл, который обязательно должен называться `robots.txt` и размещаться в корневом каталоге сайта;

- он содержит правила, определяющие, каким программным агентам (роботам/краулерам) разрешен доступ к страницам сайта, а каким — запрещен;
- правила исключений записаны в стандартном формате.

Чтобы посмотреть примерное содержимое robots.txt, попробуйте следующую команду:

```
curl -s https://www.apple.com/robots.txt | less
```

Результат показан на скриншоте: вы увидите каталоги, которые владельцы сайта закрыли от поисковых систем.



```
File Actions Edit View Help
# robots.txt for http://www.apple.com/

User-agent: *
Disallow: /*/includes/*
Disallow: /*retail/availability*
Disallow: /*retail/availabilitySearch*
Disallow: /*retail/pickupEligibility*
Disallow: /*shop/signed_in_account*
Disallow: /*shop/sign_in*
Disallow: /*shop/sign_out*
Disallow: /*shop/answer/vote*
Disallow: /*shop/bag*
Disallow: /*shop/browse/overlay/*
Disallow: /*shop/browse/ribbon/*
Disallow: /*shop/browse/campaigns/mobile_overlay*
Disallow: /*shop/button_availability*
Disallow: /*shop/favorites*
Disallow: /*shop/iphone/payments/overlay/*
Disallow: /*shop/mobile/olss_error*
Disallow: /*shop/mobilex/*
Disallow: /*shop/np/order*
Disallow: /*shop/np/giftorguestorder*
Disallow: /*shop/np/sign_in*
```

Рис. 4.20. Структуры каталогов, исключенные из обработки поисковыми роботами

Файл robots.txt предлагает ценную информацию в удобном формате и позволяет заглянуть в потаенные уголки сайта без лишних усилий. Изучив перечисленные в нем пути и каталоги, вы поймете, какие важные или конфиденциальные данные хотят скрыть владельцы сайта.

Объединение DirBuster и robots.txt

Если подкрепить мощные функции DirBuster сведениями, извлеченными из robots.txt, можно сформировать комплексный подход к поиску скрытой информации. По карте, предложенной файлом robots.txt, DirBuster прокладывает путь по неизведанным тропам сайта, помогая обнаружить то, что лежит за пределами нашего взора, — конфиденциальные данные, ценные ресурсы и важные конфигурации, необходимые для комплексного анализа безопасности.

Оба инструмента прекрасно дополняют друг друга, позволяя проникнуть в наглухо запечатанные уголки сайта и создать целостную картину его архитектуры и контента.

Примечание

Вы помните, что с большой силой приходит большая ответственность? А я предпочитаю говорить так: «Не всякое “могу” означает “можно”».

Итак, мы неплохо провели время: узнали, как сканировать файлы и каталоги, чтобы найти зарытые сокровища сайтов. Теперь пора отвлечься от веб-скрейпинга и с головой окунуться в анализ документов и метаданных. Мы взглянем на привычную информацию под новым углом и раздобудем еще больше ценных сведений.

Анализ документов и метаданных

Файлы PDF, документы Word, таблицы Excel и другие файлы снабжены метаданными, которые напоминают жемчужины, скрытые от посторонних глаз. Каждая из них может хранить в себе ценные сведения: имя автора, дату создания и изменения документа, а порой и конфиденциальную информацию, не предназначенную для всеобщего обозрения.

Выявление скрытой информации в документах и других файлах

Поиск информации, скрытой в документах и других цифровых файлах, похож на охоту за сокровищами и ведет нас к ценным знаниям в различных областях: кибербезопасности, судебной экспертизы и многих других. Вашим верным помощником в этом путешествии станет Kali Linux — система, заслужившая признание профессионалов благодаря широкому набору инструментов.

Извлечение метаданных

Каждый файл обладает собственным набором метаданных, уникальным для его формата. Умение правильно их извлекать — важнейший навык OSINT-аналитика. Если вы знаете, какой инструмент нужен для конкретного формата, то наверняка сможете получить полную и точную информацию.

Освоив мастерство работы с метаданными, вы научитесь распутывать плотный клубок информации: каждый фрагмент станет нитью, ведущей к новым находкам и открытиям. В этом и заключается OSINT-расследование.

FOCA

Хочу предложить вам классный инструмент. Знакомьтесь: **FOCA**, что означает **Fingerprinting Organizations with Collected Archives**¹ (<https://github.com/ElevenPaths/FOCA>). Утилита, предназначенная для извлечения документов из сайтов и анализа их метаданных — скрытой информации. FOCA вытягивает именно ее: имена пользователей, редактировавших документ, версию ПО, в котором его создали, исходное расположение файла и множество других деталей. Благодаря найденным сведениям можно больше узнать об объекте разведки.

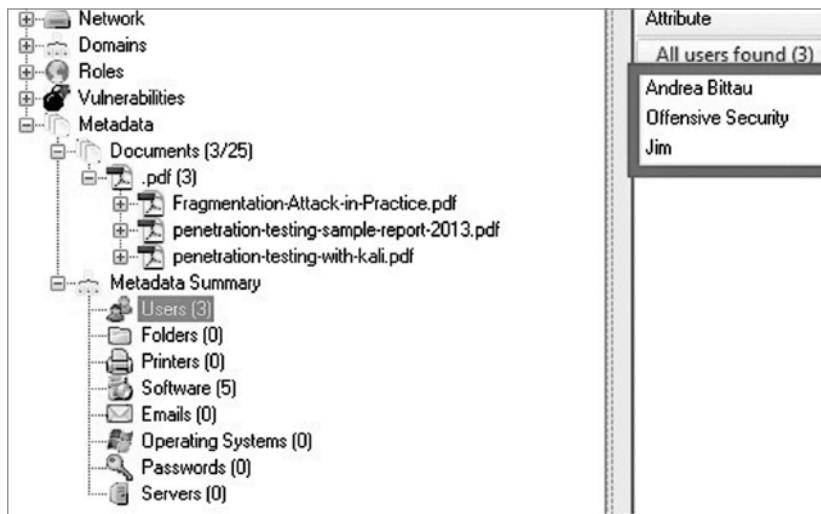


Рис. 4.21. Имена пользователей, найденные с помощью FOCA

¹ Поиск цифровых отпечатков организаций через коллективные архивы. — Примеч. пер.

FOCA, хотя и не самый продвинутый инструмент, все же обладает двумя значительными преимуществами: бесплатно распространяется и предлагает простой интерфейс на Windows. Через системы Google, Bing и DuckDuckGo программа автоматически ищет документы различных форматов, включая Word, PDF, Excel и PowerPoint — все, что доступно на заданном домене. И что самое приятное — она работает незаметно, избегая действий, которые могли бы привлечь внимание владельцев сайта.

Все извлеченные метаданные открывают огромные перспективы для дальнейших исследований. Вот тут-то и начинается самое интересное! Скажем, по именам пользователей, которые обнаружила программа, можно найти профили этих людей на других платформах и составить более полный цифровой портрет. А можно проанализировать информацию о версии ПО и проверить, нет ли в нем известных уязвимостей, которыми может воспользоваться кто-то с не очень добрыми намерениями. Потенциал для исследований и правда почти безграничен!

Анализ содержания документов

Файлы PDF, MS Office и другие документы нередко содержат важные сведения, которые проливают свет на деятельность, планы и связи организаций или обычных людей. С помощью методов извлечения текста, анализа метаданных и выделения ключевых фрагментов можно находить имена, даты, места и события, упущеные при обычном просмотре. Кроме того, документы часто содержат скрытые метаданные, включая геолокацию, сведения об авторах и историю правок — из них легко сделать выводы о происхождении и распространении файла. Тщательный анализ текста и метаданных, собранных в ходе OSINT-исследования, позволяет аналитикам выявлять скрытые взаимосвязи и дополнять картину об объекте разведки.

Итак, представьте, что анализ документов принес множество полезных находок: имена, даты, местоположения — что угодно. Теперь пора объединить эти фрагменты информации и рассмотреть их в совокупности. И здесь в ход пойдут средства визуализации данных OSINT. Благодаря специальным инструментам мы придадим данным смысл, и нам будет проще выявлять ключевые закономерности, которые часто приводят к неожиданным открытиям.

Визуализация данных OSINT

Во время визуализации сложные, необработанные данные OSINT преобразуются в интерактивные форматы, более удобные для восприятия. Графики,

тепловые карты, схемы сетей и другие приемы позволяют быстрее находить закономерности, выявлять тенденции и выдвигать идеи. Так гораздо проще анализировать большие объемы информации и извлекать наиболее значимые данные разведки. В результате аналитики выявляют скрытые взаимосвязи и аномалии быстрее, чем если бы имели дело с необработанным массивом в текстовом формате.

Но почему визуализация настолько важна? Что она дает?

- **Ясность и понимание.** Благодаря визуализации вам будет проще понять данные. Когда запутанная, абстрактная информация предстанет в наглядном виде, будут очевидны скрытые в ней закономерности, тенденции и ключевые факты, и вам станет проще их анализировать.
- **Скорость и эффективность.** Визуализация позволяет аналитику быстро и эффективно просеивать целые горы информации, выявлять закономерности и принимать решения с быстротой, невозможной при работе с сырыми данными.
- **Принятие решений.** Успех принимаемых решений напрямую зависит от качества исходных данных. С помощью инструментов визуализации можно сделать шаг от необработанной информации к практическим выводам — и далее к действиям. Каждая диаграмма, схема или карта действуют как увеличительное стекло, привлекая наше внимание к сложным, часто скрытым деталям. Информация становится проще для восприятия и может послужить основой для наших решений.

Вот сижу я за компьютером, передо мной груды разрозненных данных — профилей в социальных сетях, публикаций, фрагментов кода сайтов. И я точно знаю: всего пара нажатий, и этот хаос превратится в стройную цепочку захватывающих открытий.

Ведь истинная сила визуализации — в ее способности проливать свет на скрытые идеи и выявлять едва уловимый шепот из беспорядочного хора голосов. Только пожелайте, и абстрактные данные обретут смысл, превратившись в сети взаимосвязей, временные шкалы, географические карты и статистические диаграммы.

Инструменты и методы визуализации данных OSINT

Во время разведки вам потребуются инструменты и методы, которые помогут обнаружить скрытую информацию. Пока я просто перечислю любимые находки, а в следующей главе мы поговорим о них подробнее.

- **Maltego** (<https://www.maltego.com/>). Визуализирует связи между сущностями: людьми, сайтами, доменами, IP-адресами, организациями и не только.

Используя автоматизированные преобразования, Maltego собирает, фильтрует и сопоставляет данные из открытых и внутренних источников. Это мой любимый инструмент.

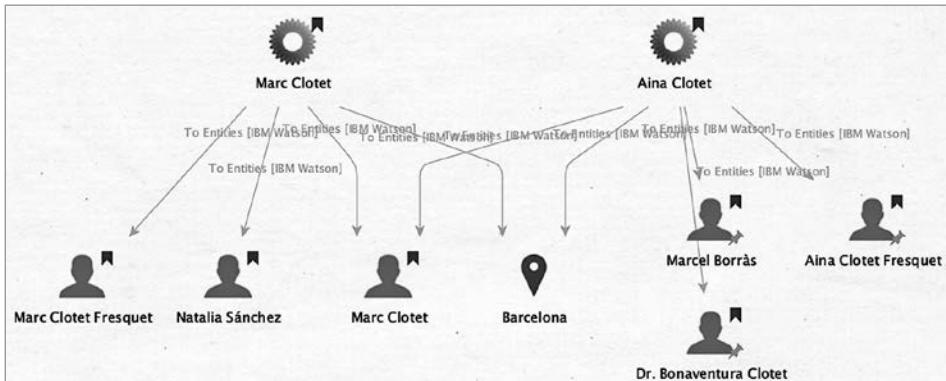


Рис. 4.22. Граф связей Maltego между именами и электронными адресами на linkedin.com

- **Gephi.** Бесплатный инструмент с открытым исходным кодом для анализа графов и сетей. Его часто применяют для анализа и визуализации связей внутри карт инфраструктуры, графов отношений, социальных сетей и т. п. Скачать Gephi можно на сайте <https://gephi.org>. Инструмент написан на Java и совместим с Windows, Mac и Linux.
- **CaseFile.** Что такое Maltego CaseFile? Объясню на примере. Представьте: вы ведете киберрасследование и с головой ушли в море служебных данных, среди которых финансовые отчеты, записи телефонных разговоров, подозрительные электронные письма и многое-многое другое. И как во всем разобраться? Вот тут-то и пригодится CaseFile. С ним груды разрозненных фактов превратятся в визуальные карты взаимосвязей — и это произойдет быстрее, чем вы допьете чашку утреннего кофе.

Каждый фрагмент служебных данных найдет свое место в общей картине взаимосвязей, и закономерности станут вам очевидны даже без доступа в интернет.

Каждый из перечисленных инструментов OSINT обладает уникальными возможностями, а вместе они помогают превратить какофонию разрозненных и противоречивых фактов в великолепную симфонию.

Рекомендации по эффективной работе с инструментами поиска

Мир цифровых данных весьма переменчив, а его обитатели постоянно эволюционируют, поэтому инструменты, которые еще вчера были нам полезны, завтра уже могут устареть. Каждый день, погружаясь в глубины OSINT, я всегда держу в уме, что осторожность не просто желательна: она жизненно необходима. Так что я выработал привычку (или даже отчасти ритуал) постоянно искать новейшие, лучшие, самые продвинутые подходы к сбору и обработке информации. RSS-каналы, форумы и тематические платформы стали для меня незаменимыми ресурсами — маяками, которые помогают ориентироваться в бескрайнем и изменчивом океане инструментов OSINT.

Обычно я рекомендую попробовать сразу несколько инструментов, а не ограничиваться одним. Каждый из них обладает уникальными преимуществами: одни лучше подходят для анализа социальных сетей, другие — для работы с юридическими документами или техническими базами данных. Подобрав подходящий инструмент, вы получите более полное и точное представление об объекте.

Не забывайте экспериментировать с ключевыми словами: используйте синонимы, схожие термины или даже возможные опечатки — всё, чтобы не упустить важные данные. Применяйте встроенные фильтры по дате, местоположению или типу источника: они помогут выявить наиболее подходящие результаты.

Собрав данные, тщательно оцените достоверность, надежность и репутацию источников, а также проверьте, есть ли другие объективные подтверждения вашим находкам. Структурируйте извлеченные сведения: используйте диаграммы связей, карты и временные шкалы — это поможет установить взаимоотношения между объектами.

И не забывайте заметать следы. Заведите VPN, применяйте прокси-серверы и создавайте анонимные учетные записи. И, разумеется, строго-настрого соблюдайте пользовательское соглашение платформ и местное законодательство. Этический подход — основа любого OSINT-исследования.

Мы могли бы углубиться и в другие темы: поговорить о том, как обеспечивать собственную безопасность, совершенствовать профессиональные навыки или отслеживать произошедшие изменения. Но уже сейчас, следуя лучшим практикам проверки источников, подбора ключевых слов и структурирования данных, а также соблюдая этические нормы, вы заложите прочную основу для успешной работы в сфере OSINT.

Итоги

Теперь вы вооружены знаниями и готовы к новым открытиям в мире OSINT! Мы рассмотрели основные приемы поиска скрытой информации в сведениях о доменах, в IP-адресах, сайтах и документах — да где угодно. С новым набором инструментов вы сможете объединить разрозненные фрагменты данных в целостную и полную смысла картину. Итак, пришло время применить новые знания на практике!

В следующей главе мы познакомимся с инструментами для автоматического сбора данных OSINT и операционной системой, созданной специально для этих задач.

ГЛАВА 5

ОТ RECON-NG ДО TRACE LABS: ЛУЧШИЕ ИНСТРУМЕНТЫ ДЛЯ РАЗВЕДКИ ПО ОТКРЫТЫМ ИСТОЧНИКАМ

В пятой главе мы продолжим удивительное путешествие по миру инструментов для разведки по открытым источникам (OSINT). В этот раз мы уделим особое внимание дополнительным средствам, которые откроют доступ к огромным массивам данных, спрятанных в Сети. Описанные здесь инструменты эффективно помогают искать и анализировать информацию из цифрового пространства, а потому будут весьма полезны для специалистов по кибербезопасности и журналистов, занимающихся независимыми расследованиями.

В этой главе мы обсудим следующие темы:

- Recon-ng: мощный фреймворк OSINT
- Maltego: визуализация данных и связей в OSINT
- Shodan: поисковая система устройств интернета вещей (IoT)
- Trace Labs: операционная система для OSINT
- Aircrack-ng: обзор пакета
- Дополнительные инструменты OSINT с открытым исходным кодом
- Тенденции в мире инструментов OSINT

К концу главы вы узнаете о многих инструментах для разведки по открытым источникам, которые откроют перед вами новые исследовательские горизонты, а также научитесь с ними работать.

Recon-ng: мощный фреймворк OSINT

Recon-ng — продвинутый фреймворк веб-разведки, в котором есть несколько по-настоящему полезных функций для сбора и анализа информации. Его архитектура позволяет без труда добавлять новые возможности, легко и быстро устанавливая дополнительные модули. Список этих модулей постоянно расширяется благодаря активному сообществу, стремящемуся поддерживать актуальность Recon-ng.

Кроме того, Recon-ng предлагает удобный интерактивный интерфейс командной строки и поэтому легок в освоении даже для начинающих пользователей. Однако не дайте себя обмануть, ведь за простым интерфейсом скрывается огромная мощь: фреймворк автоматически сохраняет собранные данные в структурированную базу, упрощая их поиск и экспорт.

Таким образом, Recon-ng сочетает в себе гибкую модульную архитектуру, поддержку API, интуитивно понятный интерфейс, надежную систему управления данными и репозиторий доступных модулей, пополняемый сообществом. Благодаря этому он стал одним из самых эффективных фреймворков для веб-разведки.

Вот как установить и настроить Recon-ng в Kali Linux:

1. Откройте терминал.
2. Клонируйте репозиторий Recon-ng с помощью следующей команды:

```
git clone https://github.com/lanmaster53/recon-ng.git
```

3. Перейдите в клонированный каталог:

```
cd recon-ng
```

4. Установите необходимые зависимости:

```
pip3 install -r REQUIREMENTS
```

5. Запустите Recon-ng:

```
./recon-ng
```

Если вы работаете на Windows, установка Recon-ng тоже не вызовет трудностей:

1. Для начала вам понадобится Python, так как Recon-ng разработан на базе этого языка. Лучше всего подходит версия Python 2.7.x, ее можно скачать с официального сайта Python. Во время установки обязательно отметьте галочкой **Add Python to PATH** («Добавить Python в PATH») — так система найдет его из любого каталога.

2. После установки откройте командную строку (для этого найдите `cmd` в меню `Start`) и выполните команду `python --version`. На этом шаге мы как будто проверяем снаряжение перед трудным походом. Если установка прошла без ошибок, вы увидите номер версии Python.
3. Подготовив Python, переходите к установке Recon-ng. Для этого в том же окне командной строки введите следующую команду:
`pip install recon-ng`
4. Это сродни загрузке виртуального ящика с инструментами. Менеджер пакетов `pip` устанавливает все необходимые компоненты, как профессиональный снабженец, подбирающий экипировку для миссии.

Теперь все готово к запуску:

```
recon-ng
```

О пользователях macOS я тоже не забыл. Установка Recon-ng на этой операционной системе немного отличается от аналогичного процесса на Windows. Вы словно готовитесь к экспедиции в другой климатической зоне (ОС), и вам необходимо адаптировать снаряжение под погодные особенности.

Как установить Recon-ng на macOS:

1. Прежде всего понадобится Homebrew, менеджер пакетов для macOS, – настоящий швейцарский нож для установки программ на Mac. Откройте терминал (его можно найти в разделе `Программы > Утилиты`) и введите следующую команду:

```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

Получив эту команду, система скачает и запустит скрипт для установки Homebrew.

2. Обычно в macOS уже предустановлен Python, но версия часто бывает устаревшей. Для работы Recon-ng понадобится версия Python 2.7. Установите ее с помощью Homebrew, выполнив следующую команду:

```
brew install python@2
```

3. Чтобы убедиться, что установка прошла корректно, введите в терминале `python2 --version`. В ответ должна отобразиться версия Python; если это произошло, значит, инструмент готов к работе.

4. Подготовив Python, установите Recon-ng с помощью менеджера пакетов `pip`. Введите в терминале следующую команду:

```
pip2 install recon-ng
```

Получив эту команду, система скачает и установит Recon-*ng* — так же, как вы бы устанавливали в системе последние обновления безопасности.

Итак, установка завершена, пора запустить Recon-ng. Просто введите в терминале команду `recon-ng`, и вы окажетесь в шаге от начала киберразведки. Теперь вы почти готовы погрузиться в исследование цифрового мира.

Запуск модулей и сбор информации с помощью Recon-ng

Фреймворк Recon-*ng* объединяет несметное количество инструментов и методов, представляя их в виде удобной системы модулей. Чем бы вы ни решили заняться, от анализа доменов до сбора данных из социальных сетей, каждый модуль поможет извлечь точную информацию о цели.

Итак, Recon-*ng* установлен, но, прежде чем приступать к разведке, надо разобраться, что такое рабочее пространство. Чтобы создать рабочее пространство, используйте команду:

```
workspaces create [имя_рабочего_пространства]
```

Вот что вы увидите:

Рис. 5.1. Загрузка рабочего пространства с именем gotham при помощи команды
workspaces load [имя рабочего пространства]

Рабочее пространство в Recon-ng похоже на отдельную папку проекта на компьютере: оно помогает разделять данные и настройки для каждого проекта. Такой подход имеет несколько чрезвычайно важных преимуществ.

- **Изоляция проектов.** Каждое рабочее пространство в Recon-ng похоже на отдельный контейнер, где хранятся данные, модули и конфигурации проекта. Если вы ведете сразу несколько расследований, такое разделение исключает риск «перекрестного заражения» данных между проектами, что критически важно для успеха в разведке.
- **Фокусировка на проекте.** Сегментирование данных по рабочим пространствам помогает сосредоточиться на текущем проекте, не отвлекаясь на посторонние сведения. Это особенно полезно при работе с большими объемами данных: вы избежите путаницы и не будете отвлекаться на информационный шум.
- **Сохранение целостности данных.** Если работать в отдельных пространствах, данные одного проекта не изменяются при работе над другим. Тогда вы можете, например, вернуться к старым проектам для проверки результатов или дополнительного анализа и увидеть все на своих местах, что весьма удобно.
- **Подготовка отчетов.** Все данные проекта хранятся в едином пространстве, что значительно упрощает их обработку и создание отчетов. Вам не нужно просеивать информацию в поисках актуальной, а результатами разведки можно поделиться сразу.
- **Совместная работа.** Если вы действуете в команде, рабочим пространством можно поделиться с ее участниками, так что каждый сможет заниматься своей частью проекта без риска изменить чужие данные. Кроме того, такое распределение удобно для одновременной работы над разными задачами и проектами, ведь каждый исследователь сможет переключаться между рабочими пространствами в любой момент.

Теперь поговорим о модулях. Фреймворк предлагает огромный выбор модулей для различных задач разведки. Благодаря функции поиска вы легко найдете нужный инструмент, а для его установки потребуется всего одна команда: `marketplace install [имя_модуля]`.

Примечание

Добавить API-ключи тоже не составляет труда. Чтобы использовать Shodan и другие сервисы, просто выполните команду `keys add [имя] [значение]`. Вот это возможности!

Если вы научитесь работать с командами модулей, каждая из которых выполняет свою задачу, то сможете запросто ориентироваться в выбранном инструменте и использовать его возможности в полной мере. Рассмотрим некоторые команды поближе.

- **Поиск модулей:**

Чтобы найти нужный модуль, введите:

```
marketplace search
```

- **Просмотр доступных модулей:**

Используйте следующую команду, чтобы увидеть доступные категории и модули. Среди них вы найдете инструменты для работы с доменами, местоположением и многие другие — каждый для выполнения определенной задачи.

```
show modules
```

- **Выбор и использование модулей:**

Чтобы скачать и установить выбранный модуль, воспользуйтесь командой:

```
marketplace install [имя_модуля]
```

Чтобы загрузить модуль, введите его название после соответствующей команды. Например, для модуля `hackertarget` введите `modules load hackertarget`.

```
[recon-ng][gotham] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][gotham] > modules load hackertarget
[recon-ng][gotham][hackertarget] > █
```

Рис. 5.2. Пример команд для установки и загрузки модуля

- **Настройка параметров модуля:**

Для начала посмотрите список доступных параметров с помощью команды:

```
options lists
```

Список параметров, которые необходимы для запуска модулей, различаются. Как правило, нужно внести информацию о цели, например доменное имя или IP-адрес. Я собираюсь ввести следующее:

```
options set SOURCE example.com
```

- **Запуск модуля:**

После настройки параметров модуль можно запускать. Введите следующую команду, и он начнет свою работу, извлекая информацию в соответствии со своим назначением:

run

Когда модуль завершит работу, сохраненные результаты можно будет посмотреть с помощью команды:

show [название_таблицы]

Например, чтобы увидеть список обнаруженных хостов, введите:

show hosts

В окне терминала появится нечто подобное.

[recon-ng][gotham][hackertarget] > show hosts			
+-----	rowid host	ip_address	+-----
1 data.packtpub.com 52.215.120.22			
2 salesdb.packtpub.com 83.166.169.242			
3 hub.packtpub.com 172.67.31.83			
4 datahub.packtpub.com 172.67.31.83			
5 epic.packtpub.com 52.19.26.156			
6 staging-epic.packtpub.com 52.48.37.122			
7 dev-epic.packtpub.com 52.18.34.177			
8 subscription-rc.packtpub.com 172.67.31.83			
9 dtc.packtpub.com 192.168.0.110			

Рис. 5.3. Результаты извлечения данных из packtpub.com
с помощью Recon-ng

Преимущество Recon-ng заключается в его итеративности: каждый цикл сбора данных помогает раскрывать все больше подробностей о цели. Огромная библиотека модулей — еще одна сильная сторона.

Я показал вам основы работы с Recon-ng, однако к каждому инструменту нужен собственный подход. Теперь дело за вами: изучайте доступные модули и следите за их обновлениями, чтобы оставаться в курсе новых возможностей.

Maltego: визуализация данных и связей в OSINT

Инструмент Maltego позволяет визуализировать данные и устанавливать взаимосвязи между объектами. Благодаря ему вам будет проще отслеживать цифровую активность и анализировать киберугрозы.

Maltego выгодно отличается от других инструментов разведки уникальной способностью объединять множество задач в едином интуитивно понятном интерфейсе. А пользователи Kali Linux получают дополнительное преимущество: они могут использовать специальную версию для сообщества (Community Edition), в которой доступно некоторое количество сканирований без первоначальных затрат.

С помощью Maltego можно извлекать различную информацию: о людях (имена, электронные адреса и псевдонимы), организациях (название компаний, сайты), документах и файлах. Кроме того, инструмент позволяет анализировать интернет-инфраструктуру, включая домены, IP-адреса и связанные сети.

Такие инструменты, как Maltego, активно применяются даже крупными государственными структурами, включая Агентство национальной безопасности США, что позволяет им выявлять сложные взаимосвязи и эффективно отслеживать потенциальные угрозы.

Начало работы с Maltego в OSINT

Итак, Maltego — незаменимый инструмент для OSINT-расследований, предназначенный в первую очередь для визуализации данных. Он превращает разрозненные факты в наглядную схему, благодаря чему понять цифровой хаос становится гораздо проще.

Инструмент уже предустановлен в Kali Linux, но если в вашей системе его нет, установка потребует всего пары нажатий клавиш. Просто введите команду `apt-get`:

```
sudo apt-get install maltego
```

При первом запуске Maltego откроется мастер настройки. Вам потребуется создать или войти в учетную запись Paterva, которая необходима для доступа к некоторым функциям и трансформациям.

После регистрации в системе можно выбрать **машину** (machine) для анализа. В Maltego «машина» определяет тип данных, которые требуется найти об объекте расследования, и глубину поиска.

Чтобы использовать все преимущества инструмента, необходимо добавить **трансформации** (transforms) — плагины, которые подключаются к сторонним сервисам с целью извлечения данных. Некоторые из них доступны бесплатно, а за другие, получше, придется заплатить. Здесь я постараюсь обойтись только бесплатными предложениями.

Отключить *платные* трансформации можно на главной панели управления, выбрав опцию Free (with API key). Например, вот список плагинов, которые я установил на своей системе:

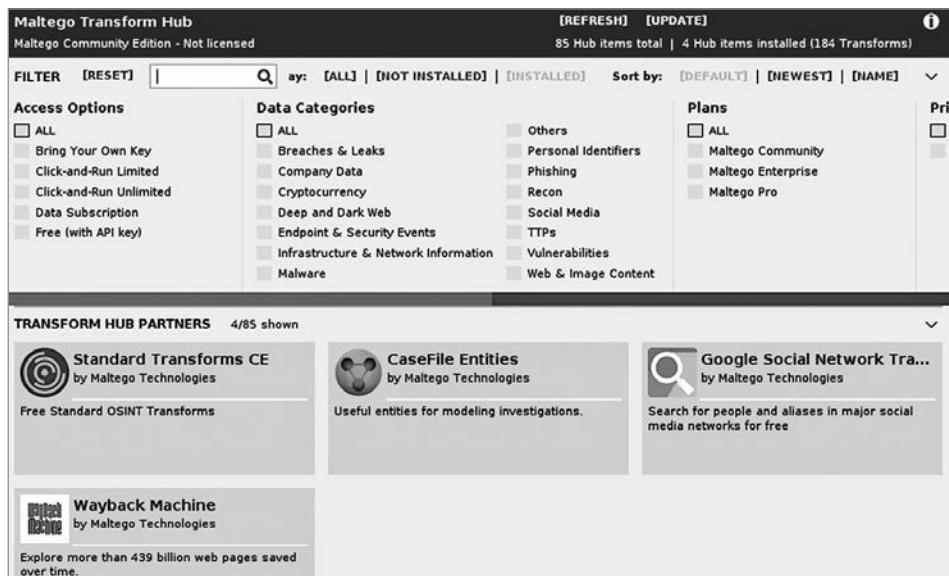


Рис. 5.4. Трансформации, установленные на моей системе

Чтобы начать визуализацию данных, создайте граф. Для этого нажмите New на верхней панели. Затем выберите сущность, которая станет основным объектом анализа (я пролистал список и выбрал Person — «Человек»), и перетащите ее значок на график. Вот как это выглядит:

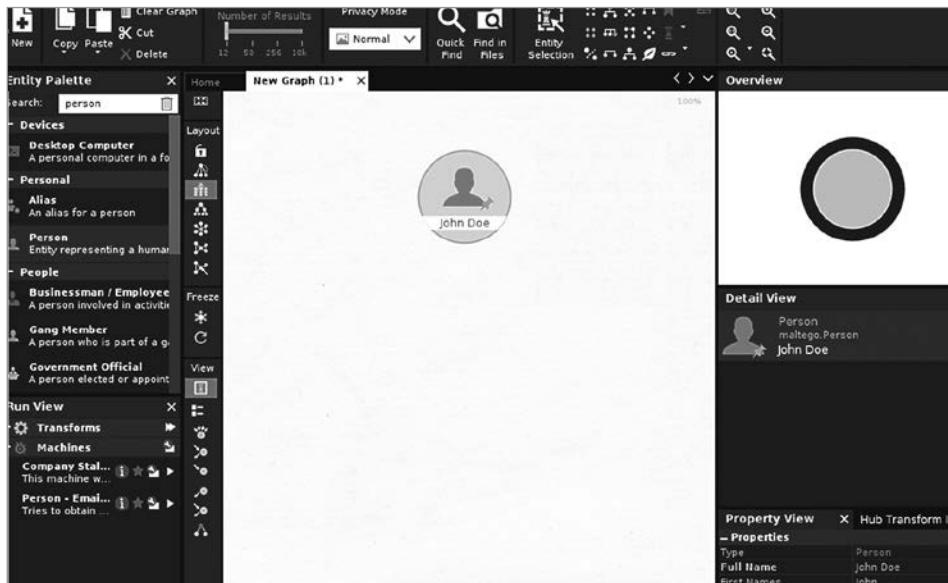


Рис. 5.5. Я перетащил сущность Person на граф

Вы, наверное, заметили, что по умолчанию имя добавленной сущности — John Doe. Поскольку это всего лишь шаблон и никакой John Doe нам не нужен, заменим его настоящим человеком, о котором мы хотели бы побольше узнать. Для этого дважды щелкните по значку сущности и введите новое имя. Я выбрал Илона Маска, просто ради шутки. Нажмите OK. После этого нажмите правой кнопкой мыши на значок сущности, чтобы увидеть список доступных трансформаций.



Рис. 5.6. Нажав правой кнопкой мыши на объекте, вы увидите доступные трансформации

Давайте запустим все доступные трансформации и посмотрим, что получится.

Итак, сначала появилось несколько электронных адресов. Среди них могут быть как настоящие контакты (например, elon.musk@spacex.com), так и случайные адреса или даже спам. Я нажал правой кнопкой мыши на elon.musk@spacex.com и запустил все трансформации.

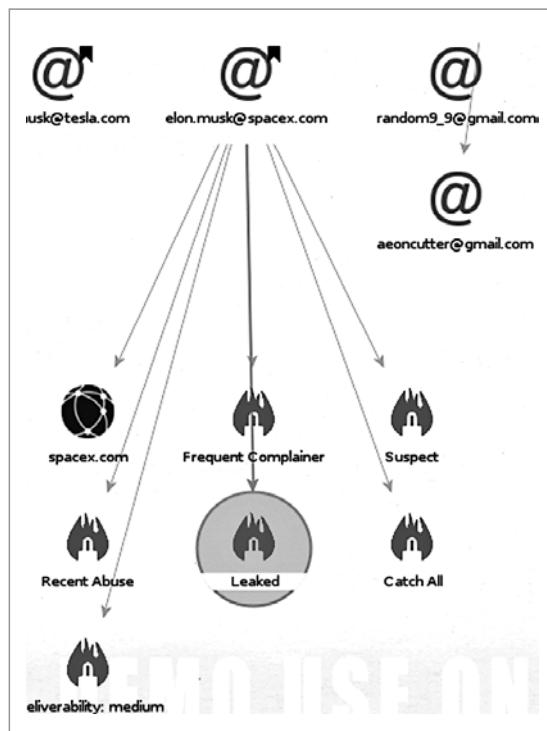


Рис. 5.7. Интересные результаты трансформаций для elon.musk@spacex.com

Выбрав значок с пометкой **Leaked** (Утечки), слева я увидел, что заданный электронный адрес фигурировал в утекших базах данных (рис. 5.8).

Каждый объект, обнаруженный в результате запуска трансформаций, можно анализировать дальше, чтобы найти еще больше информации о цели. Например, я запустил трансформации для домена **spacex.com**. Если вы сделаете то же самое, то заметите: система обнаружила так много объектов, что ей

пришлось изменить масштаб, и теперь граф представляет собой только точки, соединенные линиями. Увеличив масштаб, можно рассмотреть каждый объект и продолжить извлечение данных.



Рис. 5.8. В разделе подробной информации видно, что электронный адрес был скомпрометирован

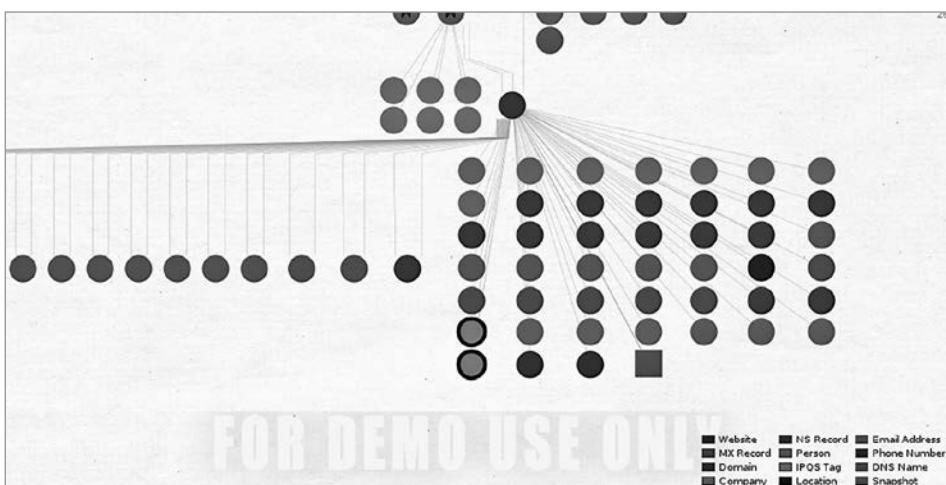


Рис. 5.9. Результаты для домена `spacex.com`

Обратите внимание, что при увеличении масштаба на графике появились имена людей, номера телефонов и другие данные. Такая детализация открывает

новые возможности для анализа и увлекает все глубже в пучину киберрасследований.

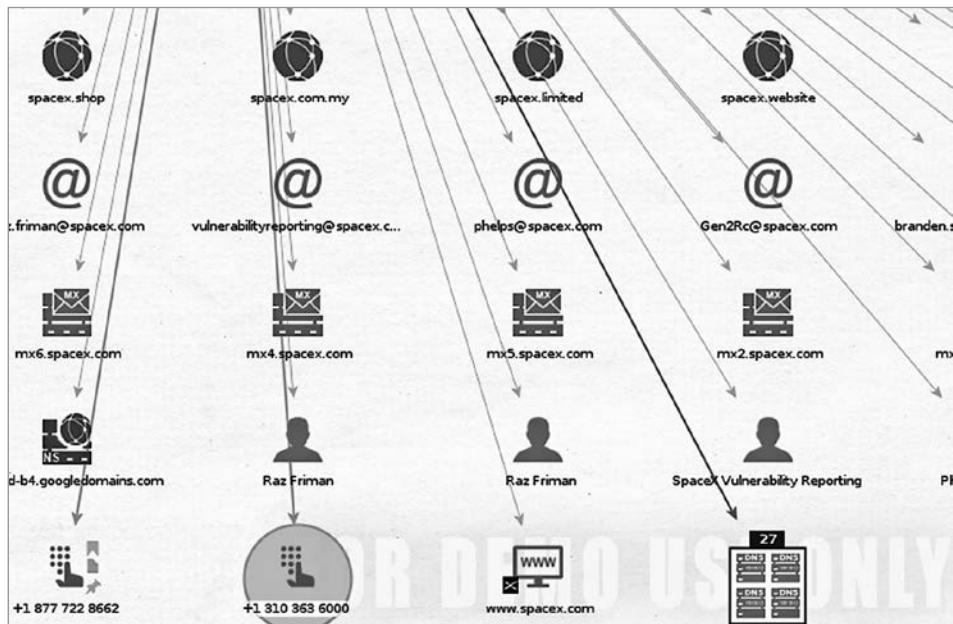


Рис. 5.10. На экране появились имена и даже номера телефонов

Поиск инфраструктуры

Для начала укажите интересующий вас домен и изучите доступные трансформации — набор различных функций и задач, которые можно выполнить. Например, давайте узнаем побольше о DNS. Затем можно запустить другие трансформации, чтобы собрать больше данных, например о почтовых серверах или службе имен, а также найти связанные домены верхнего уровня или сайты.

Предлагаю сначала найти сайт, связанный с доменом. Далее, нажав правой кнопкой мыши на значке домена, выберем сервис имен и соберем о нем данные. После этого перечислим поддомены и изучим почтовый сервис, чтобы определить, где обрабатывается почта, и выявить соответствующие почтовые серверы.

Давайте рассмотрим другие домены верхнего уровня, связанные с `yahoo.com`. С помощью трансформаций мы можем обнаружить такие домены, как `yahoo.au`, `yahoo.email`, `yahoo.tokyo` и др.

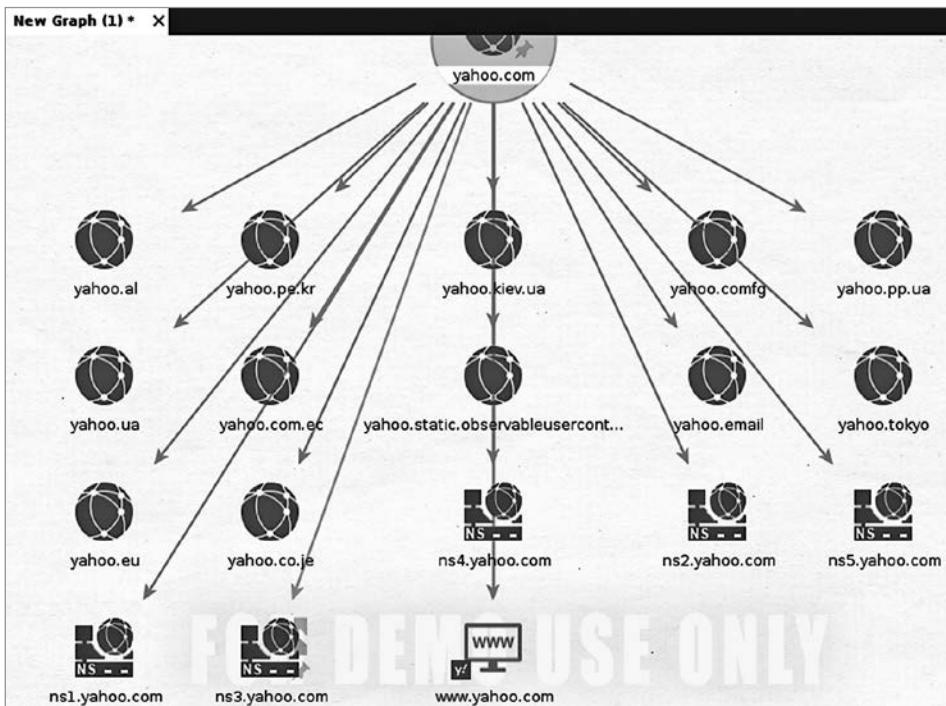


Рис. 5.11. Обнаруженные домены верхнего уровня, имена серверов и сайты

На следующем этапе нужно проверить, найдутся ли какие-нибудь электронные адреса. Для этого можно попробовать сервисы WHOIS и PGP или обратиться к поисковым системам. Однако если поиск в Сети не даст результата — не беда.

Попробуем получить IP-адреса, связанные с серверами имен. Кроме того, можно изучить общие домены или сайты, работающие на этих серверах. Обнаружив IP-адреса, мы сможем подтвердить информацию о владельце и найти его электронные адреса, прошерстив различные источники.

Например, можно найти адреса вроде `admin@yahooinc.com`, которые бывают весьма полезны. Обнаружив упомянутые домены, мы можем сгруппировать их и определить, с какими серверами имен они связаны, — чаще всего это стандартные серверы Yahoo. Объединив данные по серверам имен, мы выявим все домены, которые на них размещены прямо сейчас.

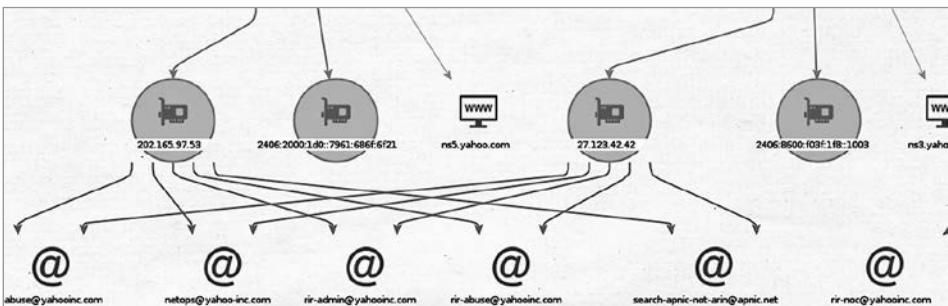


Рис. 5.12. Больше электронных адресов, IP-адресов и сайтов

Трансформации могут занять некоторое время, но в результате вы получите полный обзор структуры. В примере мы нашли информацию о таких ресурсах Yahoo, как yahoologins.com, yahoochatrooms, rocketmail.ru и не только.

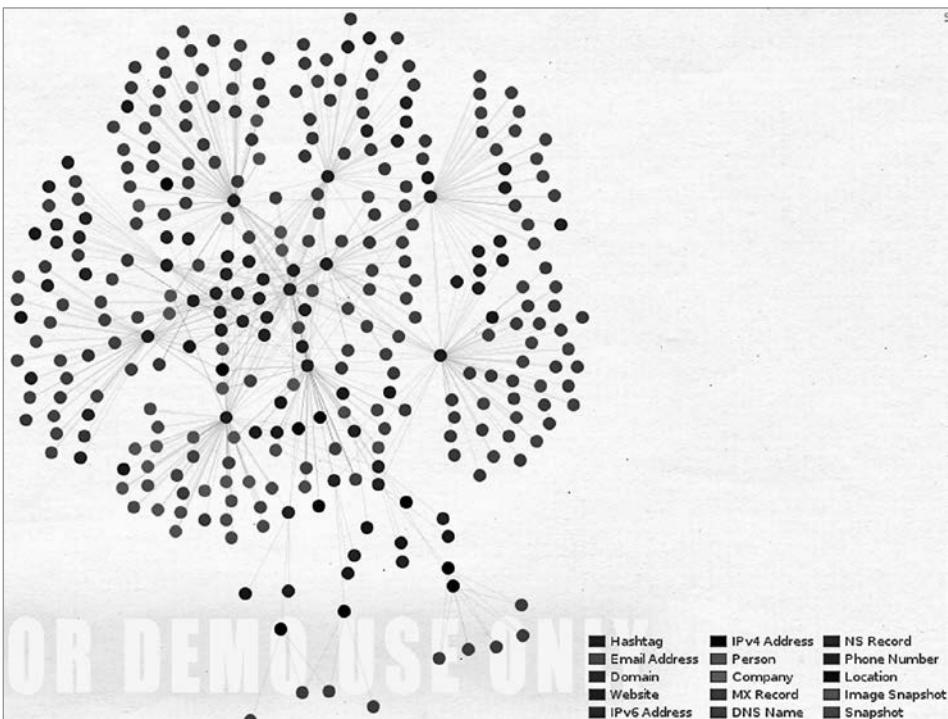


Рис. 5.13. Обзор инфраструктуры yahoo.com

В результате домены, серверы имен, почтовые серверы и другая извлеченная информация, а также связи между объектами предстают как на ладони. Впечатляет, правда?

Shodan: поисковая система устройств интернета вещей

Shodan — уникальная поисковая система, которая вместо привычного поиска сайтов сканирует интернет и ищет подключенные к нему устройства, от веб-камер до светофоров. Число IoT-устройств растет экспоненциально и, учитывая это, инструмент становится незаменимым помощником для всех специалистов по кибербезопасности и OSINT.

В то время как Google ищет для нас сайты, Shodan специализируется на устройствах и помогает *увидеть* их в интернете. Целью его поиска может стать что угодно: умный холодильник, промышленная система управления (ICS, industrial control system) или даже городская электросеть. Если устройство недостаточно защищено, Shodan, скорее всего, его обнаружит.

Начало работы с Shodan

Чтобы использовать возможности, которые предлагает Shodan, выполните следующие действия:

1. Перейдите на официальный сайт Shodan (<https://www.shodan.io/>) и создайте учетную запись.
2. После регистрации вы получите доступ к интерфейсу поиска, где можно вводить IP-адреса или другие запросы, а также применять различные фильтры.
3. Например, простой запрос `webcam` покажет вам бесчисленное множество подключенных камер по всему миру. Однако Shodan раскрывает свой потенциал в полной мере, когда вы начинаете экспериментировать с фильтрами. Хотите найти веб-камеры в Чикаго? Просто введите `country: US city:Chicago webcam` — и вуаля! Вот вам готовый список.

Однако инструмент может искать устройства не только по их географическому местоположению. Допустим, вас интересуют устройства pi-hole, тогда введите запрос `"dnsmasq-pi-hole" "Recursion: enabled"`, и система покажет их расположение по всему миру:

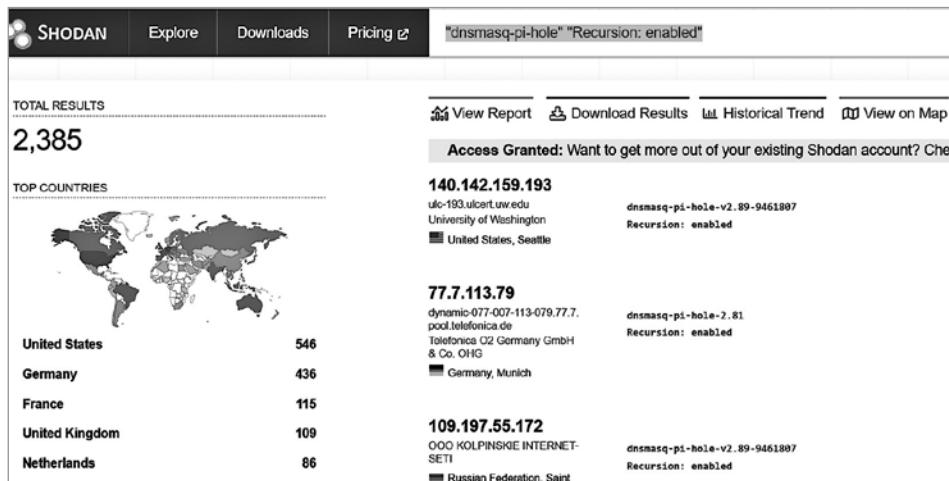


Рис. 5.14. Результаты поиска устройств pi-hole в Shodan

Shodan — незаменимый помощник для специалистов по кибербезопасности, особенно при оценке степени защиты компании. Допустим, вы хотите увидеть все устройства, принадлежащие компании Microsoft: тогда используйте фильтр `org: Microsoft`, и система покажет полный список.

А как насчет поиска серверов с определенными службами или ПО? В Shodan это тоже не составит труда. Скажем, для поиска серверов с SSH (где обычно используется порт 22) введите `port:22`. Чтобы найти серверы с уязвимыми версиями ПО, например Apache версии 2.2.15, используйте фильтр по версии (`version`). Функция особенно полезна для тех, кто пытается выявить потенциальные уязвимости.

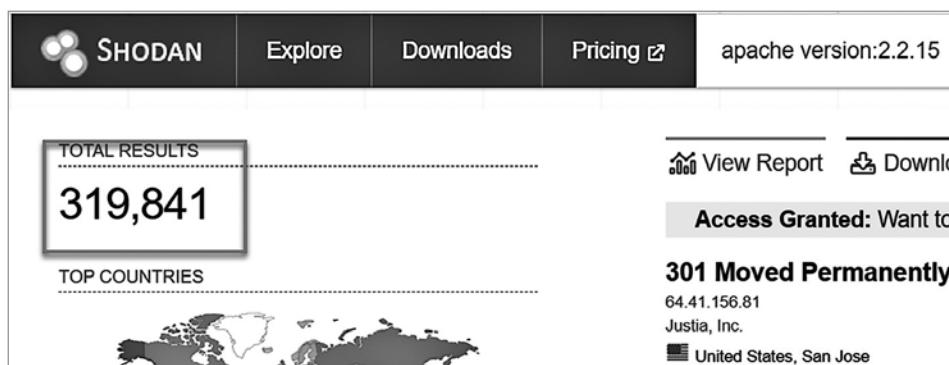


Рис. 5.15. Сейчас работает более 319 000 уязвимых серверов Apache

Возможности Shodan не ограничиваются поиском веб-камер и серверов. Инструмент открывает доступ к исследованию промышленных систем управления (ICS) — и все это с помощью фильтра `tag:ics`. А если вы интересуетесь безопасностью, то можете обнаружить устройства, в которых по-прежнему используются стандартные пароли. Это одна из самых распространенных уязвимостей современных систем.

Однако наиболее интересной функцией Shodan можно считать выявление баз данных, доступных в интернете. Например, простой запрос `MongoDB` может вывести тысячи открытых баз данных, и это в очередной раз показывает, насколько небрежно люди относятся к защите информации. Согласно этическим принципам, специалисты по кибербезопасности обязаны защищать такие системы, а не использовать их уязвимости. Так что помните мой девиз: «*Не всякое “могу” означает “можно”*». Если вы обнаружили уязвимую базу данных, всегда стоит сообщить об этом ее владельцам.

Более того, Shodan позволяет отслеживать данные в режиме реального времени: например, можно наблюдать за трансляциями с IP-камер NetWave, задав при этом фильтр по географическому местоположению.

А если хотите получить более подробную информацию об устройстве, просто нажмите на его название в результатах поиска! И сведения высыплются на экран как из рога изобилия.

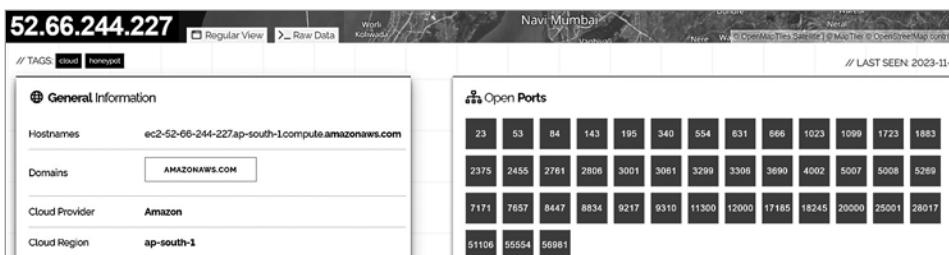


Рис. 5.16. Я нажал на IP-камеру, чтобы узнать о ней побольше

Еще одна примечательная особенность Shodan — способность находить умные устройства и системы интернета вещей (IoT). Чтобы увидеть, какие из них подключены к Сети в определенной области, введите `iot` в поисковую строку. Легкость, с которой вы найдете результаты, подчеркивает повсеместное распространение этих устройств и их потенциальную уязвимость.

Но на этом возможности Shodan не заканчиваются. Инструмент может находить даже специфические ошибки на веб-серверах, включая взломанные заголовки ответов. Такая информация особенно полезна для веб-разработчиков и системных администраторов.

С помощью Shodan можно также обнаруживать устройства, об уязвимости которых люди обычно не задумываются, например принтеры с доступом в интернет. Это важно для компаний, ведь такие устройства нередко становятся причиной утечки конфиденциальной информации. И для специалистов в области кибербезопасности, и для людей, просто увлеченных OSINT, Shodan представляет собой настоящий кладезь информации о конфигурациях серверов, настройках брандмауэров и мерах защиты. С ним вы можете анализировать состояние устройств в режиме реального времени.

Использование API Shodan

Если вы хотите использовать Shodan в своих приложениях или автоматизировать рутинные задачи, все необходимые инструменты можно получить с помощью API.

Уникальный API-ключ появится на панели управления после регистрации на платформе инструмента.

Благодаря API вы сможете автоматизировать поиск информации, интегрировать Shodan в другие инструменты, например Maltego, или даже создавать собственные приложения с функциями сканирования устройств, подключенных к интернету.

Trace Labs: операционная система для OSINT

Настало время познакомиться с Trace Labs — великолепной платформой OSINT-исследований, предназначеннной для настоящих мастеров разведки по открытым источникам! Стоит только войти в систему, и вы увидите, что в ней предусмотрено все необходимое для успешного расследования. Trace Labs создана на базе упрощенной версии Kali Linux, благодаря чему специалистов по киберрасследованиям ждет привычный, интуитивно понятный интерфейс. Все инструменты для эффективного поиска информации находятся под рукой, что позволяет сосредоточиться на задачах, а не тратить время на настройку системы.



Рис. 5.17. Рабочий стол Trace Labs

И это еще не все! Этот чудо-ящик с инструментами предлагает все необходимое для разведки. Разработчики продумали каждую мелочь, чтобы вы могли организовать свою работу наиболее эффективно.

Обязательно стоит упомянуть сообщество! Ведь это настоящая команда профессионалов, готовых помочь в трудной ситуации. Опытные пользователи делятся советами, поддерживают новичков и помогают раскрыть весь потенциал платформы. Благодаря такой поддержке вы обретете новые знания и умения гораздо быстрее.

Компания Trace Labs разработала уникальный подход к поиску пропавших людей: она использует помощь общественности для быстрого сбора информации. Платформа объединяет сотни специалистов OSINT для участия в мероприятиях вроде **Capture The Flag (CTF)** и других поисковых операциях и помогает полиции выявлять новые зацепки в делах, используя только открытые источники данных.

Вы можете скачать готовую виртуальную машину прямо с сайта Trace Labs (<https://www.tracelabs.org/initiatives/osint-vm>), принять участие в инициативах платформы и получить доступ к мощным инструментам, которые она предлагает.

Aircrack-ng: обзор пакета

Aircrack-ng представляет собой не только набор инструментов для оценки безопасности Wi-Fi, но и мощное подспорье для специалистов OSINT, ведь благодаря ему можно собирать информацию об общедоступных сетях, чтобы изучать их структуру и особенности.

Один из важнейших компонентов разведки по открытым источникам — поиск уязвимостей в сетях. Aircrack-ng позволяет выявлять слабые места, которые привлекают злоумышленников. На основе информации, собранной этим инструментом, специалисты узнают о потенциальных угрозах и продумывают меры защиты.

Наблюдение за сетевой активностью позволяет установить важные закономерности. Например, можно определить периоды наибольшей нагрузки на сеть или заметить необычные сигналы.

Aircrack-ng позволяет создавать карты Wi-Fi в выбранной местности, благодаря чему легко понять, как распределены сети, например, в городском квартале или даже в целом мегаполисе.

Для специалистов в области кибербезопасности Aircrack-ng открывает широкие возможности работы с данными. Извлекая информацию из разных сетей, можно получать ценные знания и создавать более защищенные и устойчивые сети Wi-Fi.

Примечание

Не забывайте, что хотя Aircrack-ng помогает найти большое количество информации, его следует использовать ответственно. Как и любой другой мощный инструмент, он должен служить благой цели: защищать и обучать людей, а не быть орудием преступления.

Aircrack-ng предлагает различные инструменты для выполнения определенных задач. Каждый из них имеет собственное назначение и может использоваться для защиты беспроводных сетей как самостоятельно, так и вместе с другими. В пакет Aircrack-ng включены:

- Airmon-ng — переводит адаптер Wi-Fi в режим мониторинга для захвата трафика.
- Airodump-ng — перехватывает сетевой трафик, идентифицирует доступные беспроводные сети и захватывает пакеты данных.

- Airgraph-ng — визуализирует сетевой трафик в удобной графической форме.
- Aireplay-ng — генерирует сетевой трафик и выполняет атаки (например, деаутентификацию или инъекцию пакетов) для проверки устойчивости сети.
- Aircrack-ng — основной инструмент для проверки безопасности, позволяющий расшифровывать ключи **Wired Equivalent Privacy (WEP)** и **Wi-Fi Protected Access (WPA)/WPA2**.
- Airbase-ng — создает фальшивые **точки доступа Wi-Fi (APs)** для атак с применением социальной инженерии и **MitM (Man-in-the-Middle, «человек посередине»)**.

В состав пакета также входят airdecap-ng, airdecloak-ng и airtun-ng, но мы не будем на них останавливаться в этой книге.

Примечание

Важно понимать разницу между Aircrack-ng (пакет инструментов) и aircrack-ng (отдельный инструмент). Пока я пишу эту книгу, Aircrack-ng встроен в сборку Kali Linux, но в будущем все может измениться.

Если этого пакета инструментов не окажется в вашей системе или он понадобится на другом дистрибутиве Linux, его легко установить с помощью команды:

```
sudo apt-get install aircrack-ng
```

После установки Aircrack-ng можно переходить к работе.

Airmon-ng

Итак, что делает Airmon-ng? Словно по щелчку пальцев, он превращает ваш адаптер Wi-Fi (штука, по которой компьютер подключается к интернету) в прослушивающее устройство. Обычно адаптер просто обращает внимание на доступные интернет-устройства. Но с Airmon-ng он начинает слушать все сигналы Wi-Fi вокруг себя, даже те, которые ему не предназначались. Это называется **режимом мониторинга**.

Почему этот режим так для нас важен? Допустим, вы специалист по кибербезопасности или любой другой человек, решивший проверить: а безопасна ли сеть Wi-Fi? С помощью Airmon-ng можно прослушать все беспроводные

соединения, выявить слабые места в сети, а также обнаружить попытки несанкционированного доступа.

Использовать инструмент довольно просто. Сначала нужно узнать имя вашего адаптера Wi-Fi (обычно `wlan0`), что легко сделать с помощью простых команд на ПК. Узнав имя, используйте `Airmon-ng`, чтобы перевести адаптер в режим мониторинга. В отличие от стандартного управляемого режима, при котором принимаются только пакеты, адресованные вашему устройству по заданному MAC-адресу, в режиме мониторинга адаптер может получать все пакеты в пределах досягаемости, вне зависимости от адресата. Сейчас я покажу вам, как перевести адаптер Wi-Fi в режим мониторинга:

1. Определите имя интерфейса с помощью команды:

```
ifconfig
```

2. Проверьте наличие конфликтующих процессов, которые могут мешать работе интерфейса:

```
sudo airmon-ng
```

Запишите имя интерфейса — оно понадобится на следующем этапе.

3. Убедитесь, что другие процессы не мешают работе `Airmon-ng`:

```
sudo airmon-ng check
```

4. Если обнаружены мешающие процессы, остановите их:

```
sudo airmon-ng check kill
```

5. Чтобы начать мониторинг и увидеть магию Wi-Fi в действии, выполните команду:

```
sudo airmon-ng start <имя адаптера, которое вы определили на шаге ранее>
```

6. Теперь введите следующую команду:

```
ifconfig
```

Вы увидите, что имя адаптера изменилось с `wlan0` на `wlan0mon`.

```
wlan0mon: flags=4163<UP,BROADCAST  
          unspec 50-3E-AA-76-4  
          RX packets 1032 bytes  
          RX errors 0 dropped  
          TX packets 0 bytes  
          TX errors 0 dropped
```

Рис. 5.18. `Airmon-ng` изменил имя нашего адаптера

На скриншоте видно, что в режиме мониторинга интерфейс будет называться `wlan0mon`.

Помимо перечисленных команд, `Airmon-ng` предлагает несколько дополнительных функций. Например, команда `airmon-ng stop` переводит адаптер в стандартный режим, а `airmon-ng --channel` позволяет задать канал, который будет по умолчанию использоваться при активации режима мониторинга.

После того как **сетевой адаптер (NIC)** перешел в режим мониторинга, можно начинать сбор данных и оценку безопасности беспроводных сетей. Это основной этап для последующего анализа с использованием инструментов `Aircrack-ng`.

Airodump-ng

`Airodump-ng` — еще один мощный инструмент из пакета `Aircrack-ng`, незаменимый для анализа безопасности беспроводных сетей. Его основная задача — собирать подробную информацию о сетях Wi-Fi в зоне действия.

Вот какие возможности предлагает `Airodump-ng`:

- **Перехват данных Wi-Fi.** `Airodump-ng` прослушивает трафик и перехватывает данные из окружающих сетей Wi-Fi, включая пакеты, не предназначенные вашему устройству.
- **Просмотр сведений о сетях.** Инструмент выводит список всех обнаруженных сетей Wi-Fi и ключевые сведения о них, включая уровень сигнала, используемый канал и тип шифрования.
- **Отслеживание подключений.** `Airodump-ng` показывает, какие устройства (например, телефоны или ноутбуки) подключены к каждой из сетей.

Для начала работы с `Airodump-ng` необходимо перевести адаптер Wi-Fi в режим мониторинга с помощью команды `airmon-ng` (мы показали, как это сделать, в предыдущем разделе). После этого нужно выполнить команду:

```
sudo airodump-ng wlan0mon
```

Результаты выполнения команды показаны на следующем скриншоте.

CH 5][Elapsed: 12 s][2023-10-20 11:46										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
AA:80:88:33:F4:19	-81	4	1 0	5	130	WPA2	CCMP	PSK	MiCasa_2	
28:80:88:3B:3B:6F	-81	3	0 0	5	130	WPA2	CCMP	PSK	Mi Casa	
92:80:88:3B:3B:60	-75	3	0 0	5	130	WPA2	CCMP	PSK	MiCasa_2	
28:80:88:33:F4:18	-81	3	0 0	5	130	WPA2	CCMP	PSK	Mi Casa	
80:02:9C:C9:A7:13	-82	4	0 0	1	360	WPA2	CCMP	PSK	GryphonH	
80:02:9C:C9:A7:14	-80	6	0 0	1	360	WPA2	CCMP	PSK	GryphonG	
9C:A2:F4:16:22:AA	-73	13	9 0	1	130	WPA2	CCMP	PSK	BanburyG	
CC:2D:21:B0:47:41	-67	18	11 0	1	130	WPA2	CCMP	PSK	BanburyG	
EC:74:27:EF:FB:05	-81	0	0 0	10	-1				<length:	
72:03:9F:04:ED:A4	-53	20	0 0	11	48	WPA2	CCMP	PSK	BatLight	
22:E0:19:53:E1:BA	-48	20	0 0	11	360	WPA2	CCMP	PSK	<length:	
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes			
28:80:88:3B:3B:6F (not associated)	38:88:59:9E:C0:7E B8:E9:37:F9:60:97	-84 -64	0 - 1 0 - 1	0	3				Sonos_M	
	F6:53:E6:36:39:E	-74	0 - 5	11	2					
9C:A2:F4:16:22:AA	D8:07:B6:BF:8B:72	-1	12e- 0	0	1					
9C:A2:F4:16:22:AA	10:5A:17:78:0B:4E	-77	0 - 1	0	4					

Рис. 5.19. Airodump-ng отображает сигналы Wi-Fi

Чтобы ограничить область мониторинга и повысить точность перехвата, можно воспользоваться следующими командами airodump-ng:

- **--channel** — указывает определенный канал для прослушивания.
- **--bssid** — позволяет фильтровать результаты по выбранному **идентификатору точки доступа (BSSID)**.
- **-w:** — задает имя выходного файла для сохранения результатов.
- **--encrypt** — позволяет фильтровать сети по типу шифрования.
- **--showack** — выводит статистику подтверждений (ACK), чтобы выявить уязвимости для инъекций пакетов.

Пример использования команд для перехвата данных:

```
sudo airodump-ng wlan0mon --channel 6 --bssid <AA:BB:CC:DD:EE:FF> -w output
```

Airodump-ng позволяет собирать важные данные, включая MAC-адреса точек доступа и подключенных устройств. Они, в свою очередь, используются для анализа и более сложных проверок безопасности при помощи других инструментов Aircrack-ng.

Aireplay-ng

Aireplay-ng — инструмент для моделирования атак на беспроводные сети, в том числе атак деаутентификации, во время которых соединение между устройством и точкой доступа принудительно разрывается. Для этого используются специальные пакеты деаутентификации, предусмотренные протоколом Wi-Fi. Эти атаки позволяют проверить, насколько сеть устойчива к **DoS-атакам** (отказам в обслуживании) и эффективно ли она защищена от захвата рукопожатий WPA/WPA2.

Для работы с командой aireplay-ng нужно указать несколько параметров:

- тип атаки, например -- deauth для деаутентификации;
- целевую сеть, указав флаг -a и BSSID точки доступа;
- интерфейс мониторинга, например wlan0mon, а также MAC-адреса целевой точки доступа или устройства.

Вот пример команды для запуска атаки через aireplay-ng:

```
sudo aireplay-ng --deauth 100 -a <AA:BB:CC:DD:EE:FF> -c <11:22:33:44:55:66>
wlan0mon
```

Некоторые из распространенных команд и флагов aireplay-ng:

- --deauth — выполняет атаку деаутентификации.
- --fakeauth — имитирует процесс аутентификации.
- --arp replay — воспроизводит **ARP-запросы** (Address Resolution Protocol).
- -a — указывает BSSID целевой точки доступа.
- -c — задает MAC-адрес целевого устройства.

Aireplay-ng позволяет моделировать различные сценарии атак, от простых атак деаутентификации до сложных инъекций ARP-запросов. Инструмент помогает не только выявить слабые места в сети, но и оценить ее реакцию на угрозы. Он дает ценную информацию о текущем состоянии безопасности и позволяет проверить, насколько эффективно работают меры защиты.

Aircrack-ng

Aircrack-ng — важнейший инструмент для анализа безопасности сетей, позволяющий тестировать их уязвимости путем взлома шифров WEP и WPA/WPA2. Рассмотрим, как это происходит. Протокол WEP, устаревший

и уязвимый, поддается взлому значительно легче. WPA и WPA2, хотя и считаются более надежными, тоже могут быть скомпрометированы более продвинутыми методами, особенно если используются слабые пароли.

Для взлома WPA/WPA2 Aircrack-ng применяет два основных подхода: атаки по словарю и перебором (брутфорс). В первом случае программа тестирует пароли из заранее подготовленного списка, а во втором — последовательно проверяет все возможные комбинации символов. Эффективность этих методов напрямую зависит от сложности пароля и качества используемого словаря.

Кроме того, для успешного взлома WPA/WPA2 важно использовать файл .cap, который содержит перехваченные пакеты данных из целевой сети. Aircrack-ng анализирует их данные, чтобы попытаться расшифровать сетевой ключ, при этом особую ценность представляют пакеты, связанные с процессом рукопожатия. Результат взлома напрямую зависит от качества перехваченной информации в файле .cap, ведь это основной источник сведений для расшифровки ключа.

Рассмотрим ключевые команды aircrack-ng:

- **-w** — указывает путь к словарю паролей.
- **-b** — задает BSSID точки доступа.
- **-e** — указывает **ESSID (Extended SSID)** целевой сети.
- **-a** — определяет режим атаки, например 2 для WPA/**WPA2-PSK (WPA2-Pre-Shared Key)**.

Чтобы взломать скрытые сети WPA/WPA2-PSK, укажите имя сети с помощью флага **-e**:

```
sudo aircrack-ng -w dictionary.txt -b <AA:BB:CC:DD:EE: FF> -e <имя_сети>
output-01.cap
```

Обнаружив потенциальный ключ, Aircrack-ng проверяет, позволит ли он расшифровать данные сети. Благодаря этому шагу можно оценить надежность шифрования и выявить уязвимости, а также понять, какие пароли наиболее подвержены взлому, и сформировать правила о том, как их создавать.

Airbase-ng

Airbase-ng — отдельный набор инструментов в пакете Aircrack-ng, предназначенный для создания поддельных точек доступа. С его помощью можно настроить фальшивую сеть Wi-Fi и подготовить хитроумную ловушку, чтобы

проверить надежность ваших сетей и реакцию пользователей. Вы словно создаете сцену, где будете наблюдать за разворачивающимися событиями и одновременно изучать эффективные способы защиты собственной сети Wi-Fi от потенциальных угроз.

Настройка поддельной точки доступа не требует больших усилий. Нужно выбрать канал и задать ESSID — название Wi-Fi, — которое должно выглядеть убедительно. Затем решите, будет ли точка доступа защищена паролем. Главное, чтобы все выглядело по-настоящему.

Но увы! Фальшивые точки доступа создают не только ради эксперимента. Они могут стать инструментом для атак вроде MitM (Man-in-the-Middle, «человек посередине»). Во время такой атаки злоумышленник незаметно перехватывает сообщения, которыми обмениваются пользователи, наивно полагающие, что общаются напрямую друг с другом. Благодаря фальшивой сети Wi-Fi хакер втайне становится посредником между ничего не подозревающими жертвами, подслушивает их и даже может изменить передаваемые данные.

Чтобы настроить поддельную точку доступа через `airbase-ng`, нужно учесть несколько технических деталей. Прежде всего, задать ESSID (название сети Wi-Fi) и канал, а также выбрать, будет ли точка доступа зашифрована. Также важно перевести устройство в режим мониторинга на интерфейсе `wlan0mon`, который создается с помощью `airmon-ng`. Затем нужно настроить параметры так, чтобы поддельный Wi-Fi выглядел максимально убедительно. В этом поможет следующая команда:

```
sudo airbase-ng -a <AA:BB:CC:DD:EE:FF> --essid <имя_фальшивой_точки_доступа>
--channel <#> wlan0mon
```

Ниже перечислены основные команды `airbase-ng` для настройки фальшивой точки доступа:

- `-a` — задает фальшивый BSSID точки доступа.
- `--essid` — указывает фальшивый ESSID.
- `--channel` — определяет канал.
- `-W 1` — включает шифрование WEP.
- `-z` — активирует WPA/WPA2.

Как видите, `Airbase-ng` — весьма гибкий инструмент в арсенале `Aircrack-ng`, незаменимый для проверки безопасности сетей.

Airgraph-ng

Airgraph-ng — один из ключевых инструментов пакета Aircrack-ng, предназначенный для глубокого анализа беспроводных сетей. Он превращает сложные данные сети в наглядные графики, которые помогают узнать, сколько данных проходит через сеть, какие устройства подключены и какие уязвимости могут быть обнаружены.

Прежде чем воспользоваться Airgraph-ng, нужно собрать данные с помощью Airodump-ng — их мы и будем использовать для создания графиков. Для работы airgraph-ng понадобится файл CSV от airodump-ng и название другого файла, в котором будет сохраняться график. Например, если вы хотите построить график **связей устройств с точками доступа** (CAPR, client to AP relationship), который показывает соединения и передаваемые пакеты, выполните следующую команду:

```
sudo airgraph-ng -i output-01.csv -o output.png -g CAPR
```

Основные команды airgraph-ng, которые помогают собрать и обработать данные для анализа:

- **-i** — задает входной CSV-файл с данными.
- **-o** — указывает имя выходного файла для графа.
- **-g** — определяет тип графа.
- **-c** — применяет фильтр по каналам.
- **--essid** — фильтрует данные по ESSID.

Благодаря графикам, созданным в Airgraph-ng, вам будет проще понять структуру сети. Инструмент визуализирует сложные данные, помогает выявлять важные закономерности и потенциальные проблемы. Например, можно узнать, какие устройства активны и сколько данных передается в определенное время, или обнаружить подозрительные устройства, которые не должны находиться в сети. Такие графы особенно полезны для выявления необычной, вредоносной активности.

Поиск скрытых сетей

Научившись работать с Aircrack-ng, вы делаете большой шаг к обнаружению скрытых сетей. Важно понимать, что хотя такие сети и скрыты, они не невидимы. Представьте фокусника на детском празднике, который пытается спрятать предмет, — внимательный зритель обязательно заметит трюк.

Точно так же, используя подходящие инструменты, можно обнаружить и SSID «спрятанных» сетей. Это вполне выполнимая задача, если знать, как правильно за нее взяться.

Прежде всего нужно перевести беспроводной адаптер в режим мониторинга, чтобы он улавливал все сигналы Wi-Fi, включая скрытые:

```
airmon-ng start wlan0
```

Теперь вы готовы приступать к наблюдению за ближайшими сетями. Для этого используйте команду:

```
airodump-ng wlan0mon
```

В списке обнаруженных сетей SSID будут обозначены как <length: x>. И вот тут начинается самое интересное: устройства, подключенные к такой сети, регулярно отправляют запросы на переподключение. Они невольно раскрывают скрытый SSID, и вы можете его легко обнаружить!

CH 9][BAT: 3 hours 9 mins][Elapsed: 8 s][2012-05-20 11:10										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
28:EF:01:34:64:91	-29	19	1 0	6	54e	WPA2	CCMP	PSK	Linksys	
28:EF:01:35:34:85	-42	17	0 0	6	54e	WPA2	CCMP	PSK	<length:6>	
<hr/>										
BSSID	STATION	PWR	Rate	Lost	Packets	Probes				
28:EF:01:35:34:85	28:EF:01:23:46:68	-57	0 - 1	0	1					

Рис. 5.20. В airodump-ng скрытая точка доступа отображается как <length:6>

Итак, нам нужно, чтобы подключенное устройство отправило запрос. Для этого временно отключим его от сети с помощью специальной команды:

```
aireplay-ng -0 30 -a [MAC_точки_доступа] -c [MAC_устройства] wlan0mon
```

Флаг -0 отправляет сигнал разъединения, а значение 30 определяет количество передаваемых пакетов.

После деаутентификации устройства возвращайтесь к airodump-ng: благодаря нашим действиям как по волшебству появится скрытый SSID сети! Проще пареной репы!

28:EF:01:35:34:85 -42	17	0	0	6	54e	WPA2	CCMP	PSK	SkyNet
BSSID	STATION	PWR	Rate	Lost	Packets	Probes			
28:EF:01:35:34:85	28:EF:01:23:46:68	-57	0 - 1	0	1	SkyNet			

Рис. 5.21. Теперь мы видим, что сеть называется SkyNet

На первый взгляд кажется, что, скрыв SSID, вы хорошо защитите свою сеть, но для опытного хакера это лишь небольшая преграда. Не поддавайтесь ложному чувству безопасности! По-настоящему защитить может только надежное шифрование, сложные пароли и дополнительные меры безопасности.

Раз уж мы заговорили про деаутентификацию, отмечу, что ее могут использовать в атаках типа MitM (Man-in-the-Middle, «человек посередине»), которые позволяют злоумышленнику перехватывать данные. Это серьезная угроза, требующая особого внимания.

Сначала злоумышленник отправляет команду деаутентификации, чтобы отключить вас от настоящей сети Wi-Fi. Крайне неприятно!

Затем запускает поддельную точку доступа с тем же именем, что и у оригинала (мы называем такую сеть «злой двойник»). Ваше устройство, не заметив разницы, подключается к фальшивой сети, думая, что это настоящая.

На этапе *MitM-атаки* все данные, передаваемые через поддельную сеть, перехватывает хакер. Он может получить доступ к конфиденциальной информации: паролям, сообщениям, электронным письмам. Только представьте, какой вред это может причинить!

Дополнительные инструменты OSINT с открытым исходным кодом

Инструменты разведки по открытым источникам предлагают широкий спектр возможностей: от анализа доменов до мониторинга социальных сетей. Благодаря открытому исходному коду они доступны каждому и могут быть адаптированы под специфические задачи. Далее мы рассмотрим ключевые инструменты OSINT с открытым кодом, их функции и применение в Kali Linux.

SpiderFoot

SpiderFoot — невероятно мощный инструмент для автоматизации разведки, который объединяет и централизует данные из множества источников. Он подходит для анализа информации об IP-адресах, доменных именах, электронных адресах и даже именах пользователей. SpiderFoot включает в себя более 200 модулей, которые охватывают широкий набор цифровых данных, помогая специалистам эффективно их интерпретировать и анализировать.

Для установки SpiderFoot откройте терминал и выполните следующую команду:

```
sudo apt install spiderfoot
```

Чтобы запустить SpiderFoot, выполните файл `sf.py` из каталога установки. Но обратите внимание, что для его работы нужен Python версии 3. На некоторых дистрибутивах Linux по умолчанию установлен Python 2.7, поэтому перед запуском версию стоит проверить:

```
python3 sf.py -l 127.0.0.1:5001
```

Результаты выполнения команды показаны на следующем скриншоте.

```
File Actions Edit View Help
docker-compose.yml      modules          sf.py        VERSION
Dockerfile               README.md        sfscan.py
Dockerfile.full          requirements.txt  sfwebui.py

└─(kali㉿kali)-[~/spiderfoot]
$ sf.py -l 127.0.0.1:5001
Command 'sf.py' not found, did you mean:
  command 'rsf.py' from deb routersploit
Try: sudo apt install <deb name>

└─(kali㉿kali)-[~/spiderfoot]
$ python3 sf.py -l 127.0.0.1:5001
*****
Use SpiderFoot by starting your web browser of choice and
2023-01-19 15:15:20,881 [INFO] sf : Starting web server at 127.0.0.1:5001 ...
browse to http://127.0.0.1:5001/
2023-01-19 15:15:20,881 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****
```

Рис. 5.22. Запуск SpiderFoot с помощью команды `sf.py`

После запуска SpiderFoot откройте браузер и введите URL:

127.0.0.1:5001

Перед вами откроется удобный веб-интерфейс, как на скриншоте ниже. Перейдите на вкладку New Scan и заполните информацию для идентификации цели. В этом примере я укажу сайт `hackthissite.org`.

The screenshot shows the 'New Scan' configuration page. At the top, there are two input fields: 'Scan Name' containing 'Hitting HackThisSite' and 'Scan Target' containing 'hackthissite.org'. To the right of these fields is a note: 'Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:' followed by examples for Domain Name, IPv4 Address, IPv6 Address, Hostname/Sub-domain, Subnet, and Bitcoin Address. Below this, there are three tabs: 'By Use Case' (selected), 'By Required Data', and 'By Module'. Under 'By Use Case', there are four options: 'All' (selected), 'Footprint', 'Investigate', and 'Passive'. Each option has a brief description and some explanatory text below it. At the bottom left is a 'Run Scan Now' button, and at the bottom right is a link: 'Want more OSINT automation capabilities? Check out SpiderFoot HX.'

Рис. 5.23. Настройка нового сканирования в SpiderFoot

Нажмите кнопку Run Scan Now и дождитесь окончания сканирования. Оно может занять какое-то время, но в результате вы получите информацию о выбранной цели. Поразительное изобилие разнообразных сведений! Поговорим не скажешь (рис. 5.24).

SpiderFoot предлагает удобную функцию масштабирования, которая позволяет подробнее рассмотреть любой столбец данных. Просто нажмите на столбец, который заинтересовал вас, и инструмент покажет дополнительную информацию. Благодаря масштабированию вы в два счета проанализируете свои данные!

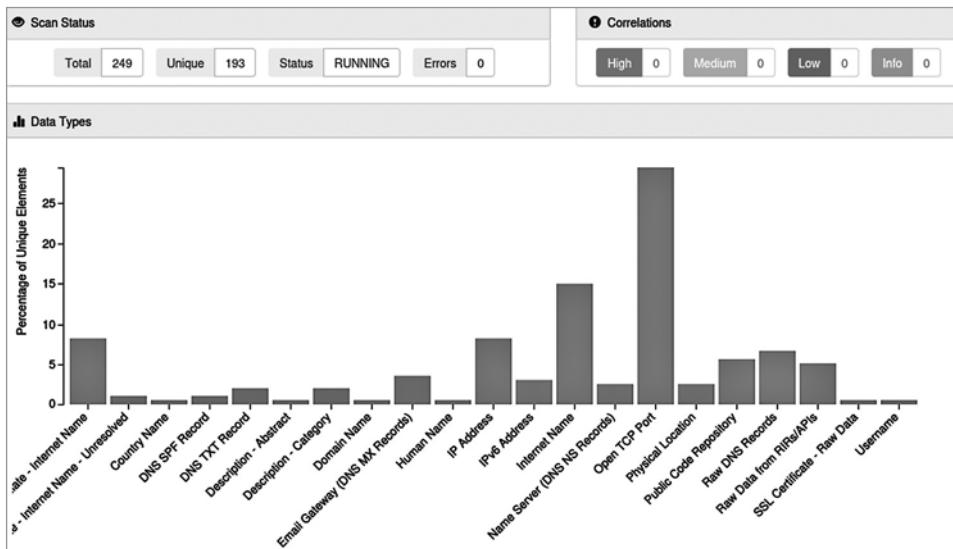


Рис. 5.24. Результаты сканирования SpiderFoot

Twint

Twint (Twitter Intelligence Tool) — это усовершенствованный инструмент анализа X (ранее Twitter), который позволяет извлекать твиты без официального API. С его помощью вы получаете значительное преимущество — обход ограничений API, включая лимиты скорости и блокировку доступа к старым твитам.

Важнейшее преимущество Twint — работа без привязки к официальному API Twitter. Программа собирает широкий спектр данных из твитов, включая дату, время и содержание, а также информацию о лайках и ретвитах. Кроме того, она получает данные из профилей пользователей Twitter, например количество подписчиков, подписок и твитов, а также информацию о местоположении.

Установить Twint можно на Kali Linux или Trace Labs. Для этого откройте терминал и выполните следующие команды:

```
git clone --depth=1 https://github.com/twintproject/twint.git
cd twint
pip3 install . -r requirements.txt
pip3 install twint
```

Основная команда для извлечения твитов:

```
twint -u имя_пользователя
```

Она выгружает все твиты из истории пользователя. Чтобы искать публикации по ключевому слову, выполните следующую команду:

```
twint -u имя_пользователя -s batman
```

Здесь флаг `-s` находит твиты с ключевым словом «`batman`». Чтобы выполнить глобальный поиск по всем публикациям, воспользуйтесь командой:

```
twint -s batman
```

Вот несколько примеров:

```
twint -u имя_пользователя --year 2023 # Твиты до 2023 года  
twint -u имя_пользователя --since 2020-12-20 # Твиты после 20 декабря 2020 года  
twint -u имя_пользователя -o tweets.csv --csv # Сохранить твиты в формате CSV
```

Следующая команда выведет информацию профиля:

```
twint -u имя_пользователя --user-full
```

Чтобы посмотреть подписчиков и подписки пользователя, введите следующее:

```
twint -u имя_пользователя --followers  
twint -u имя_пользователя --following
```

Команды ниже помогут получить полную информацию о подписчиках и подписках пользователя:

```
twint -u имя_пользователя --followers --user-full  
twint -u имя_пользователя --following --user-full
```

Кроме того, твиты можно просматривать в разных форматах:

```
twint -u username -o tweets.json -json  
twint -u username -o tweets.db -database  
twint -u username -o file.txt
```

Twint также поддерживает экспорт данных в Elasticsearch или SQLite. Кроме того, импортировав Twint как модуль, можно настроить формат и объем выводимой информации под свои потребности.

Как видите, Twint открывает доступ к твитам и метаданным, которые X (Twitter) обычно скрывает. Освоив язык запросов этого инструмента, вы

обзаведетесь собственным батискафом, с которым легко и просто сможете исследовать глубины океана полезнейших данных из Twitter.

Напоследок об инструментах

Мы обсудили множество инструментов для извлечения и анализа общедоступной информации. Несмотря на их впечатляющие возможности, беспокоят меня все не они, а объем данных, который пользователи невольно раскрывают. Социальные сети, приложения и другие онлайн-сервисы делают нашу информацию доступной для всех. И что самое тревожное — получить доступ к ней можно не только с помощью специальных инструментов, но и просто вооружившись простейшими навыками анализа и толикой интуиции.

Расскажу вам о Шей (Shay), известной исследовательнице, которая идентифицирует незнакомцев в интернете по самым незначительным подсказкам. Она публикует свои находки в TikTok (@shay.nanigans87) и к ноябрю 2023 года набрала уже более 360 000 подписчиков. В своих роликах она с удивительной точностью интерпретирует мельчайшие детали фотографий, восстанавливает размытые изображения и шаг за шагом собирает информацию, чтобы вычислить людей, которые бросили ей вызов (предложили отыскать их).



Рис. 5.25. Пользователь TikTok @shay.nanigans87 ищет свои цели

В одном из своих видео Шей определяет адрес всего лишь по части наклейки с коробки, попавшей на фото. В другом случае она восстанавливает размытый текст на магазинном чеке и читает имя покупателя. Ее работы — захватывающий пример цифрового расследования.

Шей утверждает, что применяет свои навыки исключительно в этичных целях, но ее видео — серьезное напоминание о том, насколько уязвима наша личная жизнь в эпоху цифровых технологий.

Часто мы даже не задумываемся, как легко наши данные могут попасть в чужие руки. Что ж, поговорим об этом далее.

Тенденции в мире инструментов OSINT

Технологии не стоят на месте, и вместе с ними развиваются инструменты и приемы разведки. Специалистам в сфере OSINT крайне важно следить за новыми платформами и передовыми инструментами, чтобы работать продуктивно и идти в ногу со временем.

Блоги и сайты

Многие специалисты по кибербезопасности, исследователи и просто энтузиасты разведки по открытым источникам ведут блоги и сайты, где обсуждают новейшие инструменты, подходы и случаи их успешного применения. Если вы будете регулярно читать такие ресурсы, то сможете следить за тенденциями в профессиональной сфере и всегда применять наиболее современные методы. Особенно хочу отметить следующие платформы, которые по праву считаются сокровищницами знаний:

- **Bellingcat** (<https://www.bellingcat.com/>). Платформа для журналистских расследований, которая специализируется на проверке фактов с помощью OSINT. Здесь вы найдете детальное описание расследований, которое можно использовать как учебное пособие.
- **OSINT Curious** (<https://www.osintcurio.us/>). Проект, который освещает новости и предоставляет ресурсы OSINT. Незаменим для исследователей благодаря вебинарам, блогам, полезным инструментам и советам.
- **Week in OSINT от Sector035** (<https://sector035.nl/>). Еженедельные подборки ссылок и новостей из мира OSINT.
- **IntelTechniques** (<https://inteltechniques.com/>). Сайт, созданный Майклом Баззелем (Michael Bazzell), бывшим следователем ФБР. Здесь вас ждет

изобилие разнообразных инструментов, тренингов и материалов по OSINT.

- **OSINT Essentials** (<https://www.osintessentials.com/>). Универсальный ресурс для профессионалов и новичков OSINT, полный руководств, ссылок и инструментов.
- **OSINT Techniques** (<https://www.osinttechniques.com/>). Удобная платформа с разделами по категориям инструментов OSINT и образовательным контентом.

Конференции и мастер-классы

Каждый год на крупных конференциях по кибербезопасности, включая *DEF CON*, *Black Hat* и *Bsides*, проводятся отдельные секции, посвященные OSINT. На них вы получаете уникальную возможность не только учиться у лучших специалистов, но и наблюдать OSINT в реальных условиях. Помимо обучающих лекций и практических занятий, такие мероприятия позволяют завести полезные знакомства с профессионалами отрасли, что поможет открыть новые горизонты и достичь значительных успехов.

Оценка новых инструментов

При выборе нового инструмента для OSINT важно убедиться, что он действительно полезен. Для этого обратите внимание на следующие критерии оценки:

- **Разработчик.** Узнайте, кто создал инструмент. Найдите информацию о разработчике в интернете, посмотрите отзывы и убедитесь, что он заслужил доверие в сообществе специалистов OSINT.
- **Польза.** Задайте себе несколько вопросов. Решает ли инструмент задачи, с которыми не справляются текущие средства разведки? Работает ли он быстрее или точнее? Если инструмент делает то же, что и другие программы, возможно, он будет лишним.
- **Отзывы.** Изучите опыт других пользователей. Ищите их отзывы и комментарии на форумах, в социальных сетях и на специализированных сайтах, посвященных OSINT. Важно выяснить, насколько удобен инструмент, какие у него преимущества и с какими проблемами вы можете столкнуться.
- **Обновления.** Надежные инструменты регулярно обновляются: разработчики добавляют новые функции, исправляют ошибки и адаптируют

инструмент к новым задачам разведки. Проверьте, как часто выходят обновления и действительно ли они повышают качество работы.

Приняв во внимание перечисленные критерии, вы найдете самые эффективные, безопасные и полезные инструменты OSINT, которые помогут всегда идти на шаг впереди злоумышленников.

Взаимодействие с сообществом OSINT

Сообщество OSINT объединяет профессионалов и увлеченных разведкой людей с разным уровнем опыта и поэтому считается ценным ресурсом для каждого специалиста. Преимущества, которые вы получите, взаимодействуя с коллегами:

- **Совместное обучение.** Обсуждая задачи и решения, можно обмениваться опытом и делать свой вклад в развитие сообщества.
- **Свежие идеи.** Каждый исследователь по-своему подходит к решению проблемы. Общение с коллегами поможет вам открыть для себя новые методы и приемы.
- **Нетворкинг.** Знакомства с другими специалистами нередко приводят к плодотворному сотрудничеству, успешному наставничеству или даже удачному трудоустройству.

Итоги

В этой главе я рассказал вам о Recon-*ng*, Maltego, Shodan, OC TraceLabs и других по-настоящему полезных инструментах OSINT. Каждый из них решает уникальные задачи. Так, Maltego помогает анализировать связи между данными, а Shodan фокусируется на исследовании устройств интернета вещей. Мы поговорили и о таких инструментах, как Aircrack-*ng*, SpiderFoot и Twint, и поняли, как важно учиться и обмениваться опытом с сообществом специалистов OSINT.

В следующей главе речь пойдет о том, как разведка помогает выявлять и предотвращать киберугрозы, защищая людей и компании в цифровом пространстве.

ГЛАВА 6

ГЛАЗА И УШИ РАЗВЕДЧИКА: КАК OSINT ПОМОГАЕТ СНИЗИТЬ КИБЕРРИСКИ

Глава 6 станет важной вехой нашего путешествия: мы перейдем от теоретических основ разведки по открытым источникам (OSINT) к ее практическому применению. Пришло время вооружиться накопленными знаниями и бесстрашно отправиться в путь на поиски спрятанных сокровищ.

В этой главе мы обсудим следующие темы:

- Введение в разведку киберугроз и OSINT
- Киберугрозы и OSINT
- Платформы для разведки киберугроз и интеграция OSINT
- Разработка программы разведки киберугроз на основе OSINT
- Пример из практики: использование OSINT для расследования инцидента

К концу этой главы вы еще больше узнаете об OSINT, поймете, почему разведка по открытым источникам так важна, а также как сочетание аналитического мышления, цифровых инструментов и интуиции помогает выявлять потенциальные угрозы. Более того, вы будете готовы стратегически применять полученные знания, когда в расследовании кибербезопасности потребуется взаимодействие с людьми, что актуально почти во всех современных сценариях разведки. Пора перейти от слов к делу — начнем!

Введение в разведку киберугроз и OSINT

Для начала разберемся, почему OSINT играет такую важную роль в разведке киберугроз. В цифровом мире информация стала источником силы и власти, а OSINT открывает доступ к огромному массиву общедоступных данных, будь то социальные сети, форумы, сайты или целые базы. С помощью разведки этих ресурсов можно обнаружить важные детали, которые в других случаях легко упустить из виду. Это помогает предотвратить опасное распространение киберугрозы, а иногда и пресечь ее на корню.

Но как именно применяется OSINT для противодействия киберугрозам? Благодаря инструментам разведки вы объединяете разрозненные кусочки цифровой головоломки. Например, OSINT помогает выявлять уязвимости, которыми могли бы воспользоваться хакеры, а также отслеживать цифровые следы, изучать тактику и поведение киберпреступников. Такие сведения бесцennы, ведь они позволяют не только быстро реагировать на угрозы, но и предотвращать их.

Больше всего мне нравится, что OSINT прекрасно дополняет другие виды разведки, например **агентурную** и **сигнальную**. Агентурная, или иначе называемая «разведка по людям» (HUMINT, human intelligence), предполагает общение с людьми и наблюдение за их действиями — так можно глубже понять причины атак. Сигнальная (SIGINT, signal intelligence), в свою очередь, специализируется на коммуникациях, например перехвате электронных писем, которые могут раскрыть информацию о потенциальных опасностях.

Объединив все три подхода, мы можем получать более полное представление о киберугрозах, точнее их предсказывать и эффективнее предотвращать, а также быстрее реагировать на возникающие проблемы цифровой безопасности.

Однако без трудностей тоже не обходится. OSINT как часть разведки киберугроз подразумевает не только сбор, но и тщательный анализ данных. Их объем может быть огромным, а точность и актуальность не всегда идеальны. И тогда на помощь приходят опытные аналитики, которые, опираясь на свои знания и навыки, способны отфильтровать информационный шум и извлечь по-настоящему ценные сведения. Чтобы выполнять такую работу эффективно, необходимо постоянно учиться и адаптироваться к изменениям в цифровой среде, ведь злоумышленники тоже не сидят на месте.

Киберугрозы и OSINT

Ежедневно появляются все новые и новые киберугрозы, которые подвергают риску безопасность наших систем и данных. Хакеры и киберпреступники, проявляя завидную изобретательность, постоянно исследуют уязвимости, чтобы извлечь выгоду или причинить вред. Они доставляют неприятности пользователям и нередко используют такие события, как политические конфликты, чтобы усилить хаос и привести в исполнение свои замыслы. Что самое важное, киберпреступники все искуснее обходят меры защиты, включая тот самый проверочный код, который вы получаете в SMS.

И это далеко не все! Злоумышленники все чаще похищают конфиденциальную информацию — от личных данных до коммерческих тайн. Словно виртуальные карманники, они незаметно завладевают вашими данными. Стоит только придумать меры киберзащиты, и тут же появляются новые лазейки и методы атак. Поэтому нужно всегда быть начеку и предвидеть следующий ход преступников. Это вечный бой за безопасность в цифровом мире. Фишинг и социальная инженерия — по-прежнему в топе самых опасных угроз, с которыми сталкиваются организации. Эти методы основаны на человеческих слабостях, а не технических уязвимостях систем, и поэтому их особенно трудно обнаружить и предотвратить. Однако OSINT предлагает действенные инструменты и подходы, позволяя эффективнее выявлять и анализировать даже такие угрозы, что делает ее незаменимым помощником для организаций, которые стремятся опередить киберпреступников.

Кроме того, инструменты разведки по открытым источникам позволяют эффективно бороться с фейками. Ложная информация заполонила все вокруг, и инструменты OSINT помогают отделить реальные факты от злого вымысла.

Фишинг

Представьте: вы просматриваете электронную почту и видите письмо, которое выглядит точь-в-точь как официальное уведомление от банка. В нем вас просят перейти по ссылке и обновить некоторые личные данные. Вы уже навели курсор, чтобы нажать на ссылку, ввести нужную информацию и... Стоп-стоп-стоп! Именно так и происходит фишинг. Такие схемы — настоящая головная боль, ведь они могут привести к утечке конфиденциальной информации или, что еще хуже, заражению компьютера вредоносным ПО.

Но полученное письмо — лишь завязка детективной истории. Фишинговые атаки не исчезают бесследно. По всему интернету разбросаны цифровые кусочки головоломки — здесь и пригодится умение работать с инструментами OSINT. Расследуя атаку, специалисты обращают внимание на поддельные сайты, практически неотличимые от настоящих, анализируют подозрительные шаблоны электронных писем, сигнализирующие о подмене отправителя (**спуфинг**). Кроме того, они изучают форумы и даркнет в поисках утечек, которые могут свидетельствовать о текущей фишинговой активности.

Рассмотрим один из самых удобных инструментов OSINT – theHarvester. Вы же помните, что мы обсуждали его в главе 3? Настоящий швейцарский нож для сбора информации в Сети. Он помогает аналитикам находить электронные адреса, поддомены, имена сотрудников, открытые порты и море других данных в общедоступных источниках: поисковых системах и социальных сетях. Например, команда `theHarvester -d packtpub.com -b all` позволяет извлечь всевозможные сведения о конкретном домене. Они особенно пригодятся для выявления ловушек, например поддельных сайтов, очень похожих на настоящие и созданных для похищения учетных данных.

Рис. 6.1. theHarvester ищет информацию о домене packtpub.com

Однако есть важная особенность: в действительности, как только становится известно о фишинговой атаке, особенно покушении на крупную организацию, поддельные домены злоумышленников почти сразу удаляются. Напоминает

видеоигру «Ударь крота» — стоит найти угрозу, и она тут же исчезает. Поэтому командам кибербезопасности нужно реагировать максимально оперативно. Инструменты вроде theHarvester помогают быстро отслеживать фишинговые атаки до того, как все следы испарятся.

Социальная инженерия

Социальная инженерия — одна из самых сложных и динамичных угроз в цифровом мире. Она выходит за рамки простой кражи IP-адресов и охватывает широкий спектр приемов: от манипуляций с именами пользователей и адресами электронной почты до проникновения в домашние веб-камеры и другие подключенные устройства. Социальная инженерия поражает своим размахом и коварством, ведь атаки становятся частью повседневной цифровой жизни и для большинства остаются незаметными.

Мониторинг преступной среды

Специалисты по кибербезопасности применяют OSINT, чтобы изучать приемы и анализировать действия злоумышленников. Преступники тоже часто ведут себя беспечно и допускают ошибки: оставляют улики или даже хващаются своими успехами. Вот почему опытные аналитики внимательно анализируют определенные ключевые слова, хештеги и темы, связанные с фишингом и социальной инженерией. Например, резкий рост жалоб на подозрительные письма в социальных сетях может указывать на активную фишинговую атаку.

Инструменты анализа

Один из ваших мощных союзников в борьбе с социальной инженерией — **SpiderFoot**. Инструмент, словно цифровой детектив, автоматически собирает данные из многочисленных источников. Введя команду `spiderfoot -l 127.0.0.1:5001 -s packtpub.com`, аналитик запускает глубокое сканирование, в результате которого может обнаружить информационную золотую жилу: электронные адреса, доменные имена, профили в социальных сетях — все, чем злоумышленники могут воспользоваться во время атак.

Однако социальная инженерия — сложное явление, которое включает в себя не только видимые, но и скрытые механизмы воздействия на жертв. Для выявления неочевидных связей специалисты обращаются к Maltego. Инструмент способен провести глубокий анализ, выявляя такие взаимосвязи между людьми, организациями и цифровой инфраструктурой, которые не всегда заметны невооруженным взглядом.

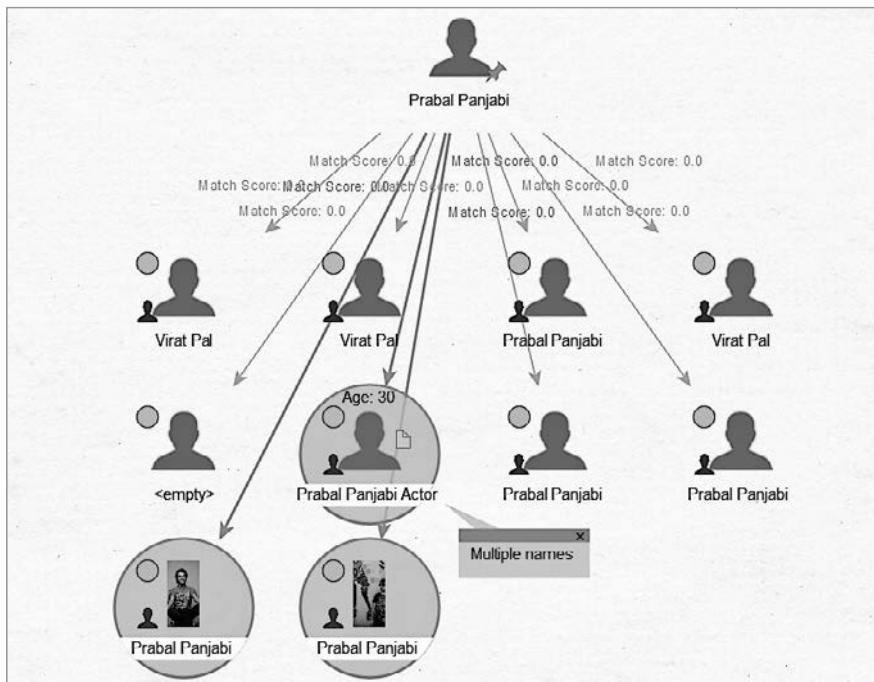


Рис. 6.2. В Maltego показаны социальные связи, которые не всегда очевидны

Maltego может отследить цифровую активность, связанную, казалось бы, с безобидным электронным адресом. Например, обнаружить подключенные устройства — даже домашнюю веб-камеру, которая могла быть взломана без ведома владельца.

Как OSINT заполняет бреши в киберзащите

Социальная инженерия опасна не только во время атаки; иногда проблема кроется в последствиях уже совершенных взломов. Существуют сервисы, например *Have I Been Pwned*, которые помогают узнать, не скомпрометированы ли ваши данные, и тем самым служат своеобразными системами раннего предупреждения. Однако это лишь верхушка айсберга. Полноценная социальная инженерия включает уязвимости, которые часто остаются вне поля зрения: заброшенные сайты, незащищенные веб-камеры, уязвимые сетевые устройства и даже неправильно настроенные брандмауэры с доступом в интернет. Все это может открыть двери для злоумышленников.

Еще одним важным направлением OSINT считается анализ утечек и случаев взлома. Ресурсы вроде *Have I Been Pwned* (<https://haveibeenpwned.com/>)

помогают пользователям определить, фигурирует ли информация о них в известных утечках. Знать об этом крайне важно, ведь скомпрометированные данные зачастую служат отправной точкой для последующих атак социальной инженерии.

Социальные сети — настоящая сокровищница для злоумышленников. Здесь они собирают личную информацию, чтобы завоевать доверие своих жертв или выдать себя за другого человека в фишинговых атаках. В этой ситуации методы OSINT направлены на глубокий анализ публикаций, взаимодействий и моделей поведения, что помогает выявить потенциальные уязвимости.

Всесторонний анализ

Благодаря методичной работе с инструментами OSINT специалисты по кибербезопасности разоблачают сложные стратегии социальной инженерии. Они могут не только понять, каким образом осуществляются атаки, но и выявить, *кто* за ними стоит и *какие цели* преследует. Специалисты получают знания, которые помогают укреплять киберзащиту: информировать пользователей о популярных уловках фишинга или совершенствовать протоколы безопасности для наиболее уязвимых отраслей.

Всесторонний анализ угроз позволяет выявить, какие организации находятся в группе риска, какие регионы чаще всего становятся целями атак и насколько продуманы методы злоумышленников. В результате можно в корне изменить ситуацию, превратив потенциальных жертв в осведомленных и подготовленных защитников.

Вредоносное ПО и программы-вымогатели

Современное вредоносное ПО становится все более сложным и разрушительным. Особенно часто встречаются программы-вымогатели, вызывающие массовые сбои в работе систем.

- **Развитие вредоносного ПО.** Изначально в числе вредоносных программ были простейшие вирусы и черви. Со временем они развились в сложные инструменты, включая шпионское ПО, трояны и кейлоггеры, предназначенные для кражи данных, нарушения работы систем или получения несанкционированного доступа.
- **Программы-вымогатели.** Современные программы-вымогатели шифруют данные жертв, а за ключ расшифровки злоумышленники требуют выкуп, чаще всего в криптовалюте. Жертвами таких атак становятся обычные люди, компании и даже государственные структуры.

Борьба с вредоносным ПО средствами OSINT

Анализ программ-вымогателей и другого вредоносного ПО является весьма актуальным направлением OSINT. Вот какие возможности оно предлагает:

- **Выявление злоумышленников.** Вредоносное ПО разрабатывается как отдельными хакерами, так и организованными преступными группами или даже компаниями, которые спонсируются государством. Анализируя такие программы средствами OSINT, можно исследовать **тактики, техники и процедуры (TTPs)** злоумышленников, выяснить цели атаки и даже узнать, кто за ней стоял.
- **Тенденции кибербезопасности.** Анализ вредоносного ПО помогает выявить актуальные и будущие киберугрозы, а значит, лучше предсказывать последующие атаки и оставаться на шаг впереди злоумышленников.
- **Цифровые следы.** Вредоносное ПО нередко оставляет за собой цифровые следы, которые можно подробно изучить, например домены или IP-адреса. Сопоставляя их с данными из открытых баз и применяя инструменты OSINT, специалисты могут глубже исследовать природу угроз.
- **Обмен информацией об угрозах.** Проанализировав вредоносное ПО, специалисты по кибербезопасности могут поделиться результатами с сообществом, чтобы предупредить об опасности или обменяться опытом. Спаянная работа помогает укреплять защиту и развивать сферу OSINT.
- **Противодействие угрозам.** Понимая, как работают разные типы вредоносного ПО, можно разрабатывать эффективные стратегии защиты и снижать риски. Организациям, которые стремятся защитить свои активы, это поможет построить надежные системы безопасности с использованием OSINT.

Отслеживая IP-адреса и информацию о регистрации доменов, специалисты по кибербезопасности выявляют инфраструктуры, которые используются для распространения вредоносного ПО.

Проанализировать такие программы, понять их поведение, источник и потенциальную угрозу можно с помощью инструмента VirusTotal. Например, если вы сомневаетесь в безопасности сайта packtpub.com, введите его URL в сервис VirusTotal и проверьте репутацию (рис. 6.3).

VirusTotal проверяет URL по своей базе известных угроз, чтобы определить, связан ли сайт с вредоносной активностью, например распространением вредоносного ПО или фишинговыми атаками. Благодаря мгновенному анализу пользователям проще избегать опасных ресурсов, а команды кибербезопасности быстрее реагируют на обнаруженные угрозы.

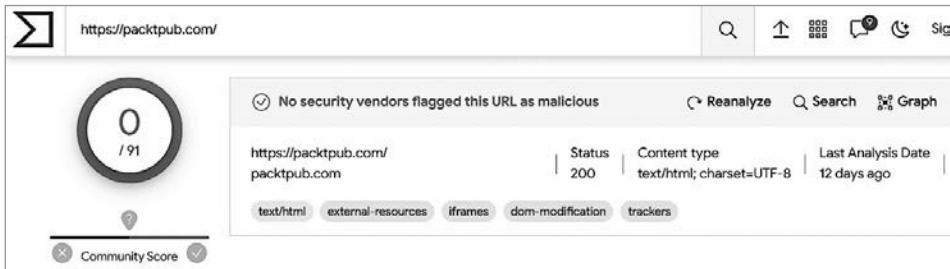


Рис. 6.3. Проверка packtpub.com на virustotal.com

Если вам сложно представить, как это работает, разберем на примере. Представьте, что, наблюдая за сетью, вы заметили подозрительную активность, похожую на атаку вредоносного ПО. Чтобы расследовать инцидент, вы решили использовать VirusTotal, инструмент OSINT. Вот как это могло бы происходить:

- Сбор подозрительных данных.** Сначала вы извлекаете из сетевого трафика подозрительные файлы и URL. Например, скачанные документы или ссылки, по которым кликали обманутые пользователи.
- Анализ в VirusTotal.** Вы загружаете найденные файлы или вводите URL в сервисе VirusTotal. Инструмент анализирует их поведение и проверяет по базам данных известных угроз.
- Изучение отчета.** VirusTotal формирует подробный отчет о каждом объекте, указывая на вредоносные действия, связь с известными семействами вредоносного ПО и подозрительными IP-адресами.
- Сопоставление данных.** Получив информацию из VirusTotal, вы ищете **индикаторы компрометации (IoCs)**, например IP-адреса, домены или хеши файлов, в других базах данных OSINT. Это помогает выявить, связаны ли они с другими, более крупными кибератаками.
- Меры защиты.** На основе полученных данных обновляете защитные механизмы в сети: блокируете подозрительные IP-адреса, обновляете систему или обучаете пользователей тому, как избежать угрозы.
- Распространение результатов.** Наконец, вы готовите краткий отчет о расследовании, уделяя внимание тому, какие инструменты OSINT использовали для устранения угрозы. И делитесь отчетом с сообществом по кибербезопасности, чтобы каждый мог укрепить защиту своих систем.

Анализ сетевого трафика для поимки вредоносного ПО

Анализ сетевого трафика — отличный способ обнаружить вредоносное ПО еще до того, как оно нанесет ущерб. Исследуя входящие и исходящие

данные, специалисты могут выявлять отклонения, потенциально связанные с заражением системы. Например, если резко увеличился объем данных, отправляемых на подозрительный сайт, возможно, действует ботнет или проходит утечка информации. Непрерывно отслеживать сетевую активность и проверять пакеты можно с помощью инструмента Wireshark (<https://www.wireshark.org/>). Любые подозрительные соединения, протоколы и нагрузку нужно тщательно анализировать.

Мониторинг сетевого трафика позволяет своевременно обнаруживать и устранять проблемы, предотвращая их распространение. Однако ни одна организация не может отслеживать все, что происходит в интернете. Именно тогда на помощь приходят коллективные платформы. Благодаря тому, что исследователи анализируют в VirusTotal вредоносные программы и подозрительные файлы, сообщество быстрее выявляет новые угрозы и распространяет информацию об их сигнатурах. В результате базы данных, созданные усилиями сообщества, включая VirusTotal и ThreatCrowd (<http://ci-www.threatcrowd.org/>), действуют как системы раннего предупреждения об атаках.

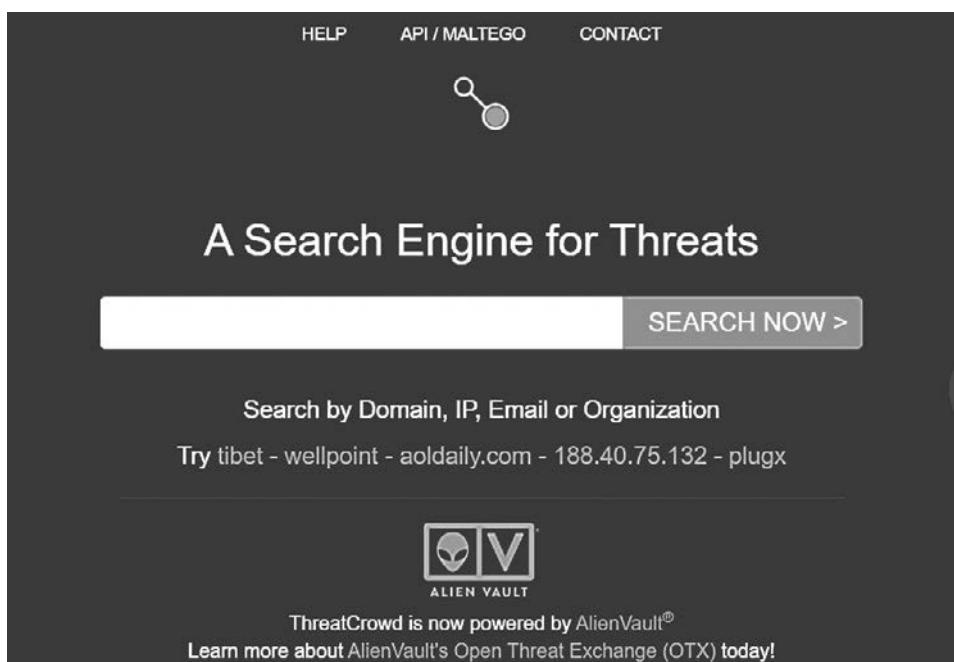


Рис. 6.4. threatcrowd.org может рассказать о доменах, IP и электронных адресах

Мониторинг сетей, подкрепленный данными сообщества об угрозах, помогает организациям увереннее противодействовать программам-вымогателям и другому вредоносному ПО. Чтобы успешно предотвращать атаки, нужно не только тщательно наблюдать за собственной инфраструктурой, но и сотрудничать с коллегами.

Актуальная информация о киберугрозах

Представьте себе ленту в социальных сетях, только в ней не обычные фото и публикации, а последние новости о киберугрозах. Такие ленты собирают информацию из множества интернет-источников: от форумов по безопасности и хакерских сайтов до твитов специалистов по кибербезопасности. Они в режиме реального времени сообщают вам о новых типах вредоносного ПО, включая программы-вымогатели.

- Почему это важно?

Такая информация жизненно необходима тем, кто защищает компьютеры и данные от хакеров. В приложении с прогнозом погоды вы узнаете о надвигающемся шторме, а ленты аналитики оповещают о предстоящих «цифровых буряках» — кибератаках.

- Как это помогает?

- **Раннее предупреждение.** Эти ленты предупреждают о распространении новых вирусов или всплеске попыток взлома. Такая своеобразная система оповещения дает время подготовиться и защитить инфраструктуру до предполагаемой атаки.
- **Анализ тенденций.** Просматривая ленту, специалисты могут выявлять распространенные типы атак, что помогает прогнозировать предстоящие угрозы и готовиться к изменениям в цифровом мире.

Допустим, отдел кибербезопасности регулярно просматривает новости на сайте AlienVault OTX. Однажды специалисты замечают предупреждение о новом виде программы-вымогателя, которая распространяется через фишинговые электронные письма. В ленте опубликовали индикаторы компрометации: IP-адреса вредоносных ресурсов, темы электронных писем, хеши файлов, связанных с угрозой, и многое другое.

С помощью обнаруженной информации отдел оперативно обновляет фильтры электронной почты, чтобы блокировать письма с подозрительными темами и индикаторами. Дополнительно специалисты настраивают системы безопасности, которые выявляют и изолируют попытки взаимодействия с вредоносными IP-адресами. Благодаря тому, что AlienVault OTX публикует

новости в режиме реального времени, отдел кибербезопасности оперативно реагирует на угрозу и защищает сеть от программы-вымогателя. Этот пример наглядно демонстрирует всю пользу таких ресурсов для проактивной борьбы с киберугрозами.

Целевые продолжительные атаки (APT)

Целевые продолжительные атаки повышенной сложности, или **APT-атаки** (advanced persistent threats), — одна из самых изощренных и скрытных форм киберугроз. Группы злоумышленников, часто финансируемые государством, проводят длительные атаки с целью шпионажа, извлечения информации или причинения вреда. В постоянно развивающемся мире киберугроз OSINT становится важнейшим инструментом для выявления и анализа АРТ-атак.

Что такое АРТ-атака?

АРТ-атаки проводятся группами высококвалифицированных хакеров с применением сложных методов для взлома сетей и устройств. В отличие от обычных кибервзломщиков они крайне настойчивы и долгое время могут оставаться в системах незамеченными. Обычно атаки нацелены на различные организации, включая правительственные учреждения и крупные компании. Злоумышленники пытаются похитить критически важную информацию, нарушить рабочие процессы или причинить вред иным способом.

Как помогает OSINT

Прежде всего, специалисты OSINT анализируют веб-ресурсы в поисках следов АРТ-атаки, при этом не ограничиваясь только очевидными уликами. Ценная информация может быть скрыта в огромном потоке данных: подозрительное доменное имя, не связанное с реальной компанией, или публикации на хакерских форумах, намекающие на подготовку к атаке. Такие находки можно сравнить с уликами на месте преступления: каждая из них помогает выявить злоумышленников.

Поиск взаимосвязей

На следующем этапе специалисты OSINT начинают собирать разрозненные данные, как детали пазла. Я сразу представляю детективов: на доске они соединяют линиями улики, чтобы раскрыть коварный замысел. Например, подозрительная попытка входа из-за рубежа и публикация конфиденциальных документов на другом сайте может указывать на определенную АРТ-атаку. Соединяя точки на доске, специалисты устанавливают закономерности

и стратегии хакерской группы. Однако для этого требуются терпение, внимательность и глубокий анализ каждого элемента.

Поиск цифровых следов

Даже самые осторожные хакеры во время АРТ-атаки неизбежно оставляют следы в цифровом пространстве, пусть и едва заметные: цифровые записи, файлы транзакций или даже незначительные отклонения сетевого трафика. Специалисты OSINT получают шанс все это исследовать. Например, журнал сервера помогает выявить подозрительную активность, а метаданные взломанного документа — раскрыть время и место его создания. Каждая такая находка становится важной частью головоломки, позволяя не только установить личности, но и определить тактику хакеров.

Понимание общего контекста

OSINT подразумевает не только сбор данных, но и понимание контекста для их точного анализа. Специалистам важно узнать, *почему* и *как* действуют хакеры, совершающие АРТ-атаку.

Например, если злоумышленник атакует энергетический сектор, аналитики OSINT попытаются выяснить причину. Есть ли здесь политическая подоплека? Пытаются ли хакеры нарушить энергоснабжение в стране? Такой анализ помогает предсказывать будущие действия злоумышленников и лучше понимать их стратегию.

Реальные примеры АРТ-атак

Рассмотрим несколько атак, которые произошли на самом деле и в которых OSINT сыграл или мог сыграть важную роль в поиске кибершпионов:

- **Атака Stuxnet (2010).** Компьютерный червь Stuxnet использовался при атаке на иранскую ядерную программу. Предполагается, что этот невероятно сложный червь создан каким-то государством, но вот каким — не выяснено до сих пор. Специалисты OSINT изучили структуру Stuxnet, чтобы понять, как он работал, кто был целью атаки и какой ущерб червь мог нанести.
- **Взлом Национального комитета (2016).** Во время этой атаки хакеры проникли в почтовые серверы Национального комитета Демократической партии США. Специалисты OSINT проверили оставленные цифровые следы, включая источник электронных писем и тип вредоносного ПО, заключив, что за АРТ-атакой, вероятно, стояла российская группа хакеров.

- **Взлом MGM Resorts International (2023).** Хакерская группа **Scattered Spider** атаковала компанию MGM Resorts International, что привело к отключению компьютерных систем в нескольких ее казино и отелях по всей территории США. Пострадали и такие знаменитые комплексы, как Bellagio и Cosmopolitan. Атака с применением программы-вымогателя вынудила компанию приостановить работу компьютерных систем, что сильно повлияло на ее деятельность. К ноябрю 2023 года полный размер ущерба еще не подсчитан, но поверьте, специалисты по кибербезопасности продолжают расследовать эту атаку средствами OSINT.

Взлом MGM наглядно демонстрирует, что киберугрозы становятся все сложнее. Чтобы эффективно им противодействовать, специалисты должны использовать OSINT, быстро адаптироваться к изменениям и настойчиво бороться с теми, кто покушается на безопасность в Сети.

Сочетание OSINT и внутренних систем безопасности

Представьте, что специалист OSINT — это детектив, скрупулезно собирающий улики. Объединяя данные из открытых источников с информацией от внутренних систем безопасности, он может получить более полное представление о возможных угрозах. Именно такая кропотливая работа лежит в основе эффективных мер кибербезопасности. Рассмотрим, как объединение данных из разных источников помогает специалистам:

- **Интеграция с SIEM.** Системы управления событиями безопасности (SIEM, security information and event management) помогают централизовать данные из разных источников для анализа угроз. При интеграции OSINT они получают дополнительную информацию, благодаря которой лучше выявляют риски и реагируют на них. Например, система может обнаружить всплеск сетевого трафика из определенного региона — необычный, но сам по себе недостаточно подозрительный, чтобы на него реагировать. Но если соотнести его с данными OSINT о недавних киберугрозах или действиях хакеров в том же регионе, можно точнее оценить риски и запустить соответствующие протоколы безопасности.
- **Синергия с системами EDR.** Системы обнаружения и устранения атак на конечные точки (EDR, endpoint detection and response) выявляют угрозы в устройствах организации. Интеграция OSINT значительно расширяет возможности системы, помогая понять происхождение и развитие новых рисков. Вы спросите, *каким образом?* Представим, что система EDR обнаружила неизвестное вредоносное ПО на корпоративном ноутбуке. Пока она локализует и устраниет угрозу, вы с помощью OSINT выясняете

происхождение этого ПО. Например, оно используется в происходящей сейчас хакерской деятельности, о которой сообщали источники OSINT или форумы киберразведки. Дополнительная информация поможет отделу безопасности усилить защиту и лучше справиться с последующими атаками.

- **Проактивный подход на основе SIEM, EDR и OSINT.** Объединение OSINT с внутренними системами безопасности позволяет перейти от устранения последствий к предупреждению угроз. Благодаря анализу огромных массивов общедоступной информации специалисты могут заранее выявлять потенциальные атаки и устранять их еще до того, как они нанесут вред.

Например, система SIEM с интеграцией OSINT обнаружила на форумах даркнета разговоры о готовящейся атаке на организацию вашей отрасли. Благодаря этому специалисты по безопасности могут заранее ужесточить меры защиты и начать отслеживать определенные сигнатуры атак. Одновременно система EDR, получив обновленные данные, будет выявлять ранние проявления компрометации устройств в сети, предотвращая развитие угрозы.

Разработка эффективной стратегии кибербезопасности

Как объединить возможности OSINT и внутренних систем в надежную стратегию? Чтобы этого достичь, важно не только реагировать на угрозы, но и предупреждать их. Вместо того чтобы просто дожидаться, когда придет беда, вы заранее предвидите, где и каким образом может произойти следующая кибератака. Интеграция данных OSINT о текущих угрозах с информацией, получаемой от внутренних систем в режиме реального времени, позволяет увидеть полную картину.

В результате вы не только эффективно реагируете на текущие инциденты, но и прогнозируете следующие возможные угрозы. Допустим, в вашей отрасли участились атаки с использованием программ-вымогателей. Вы выясняете это с помощью инструментов OSINT, а благодаря анализу данных от внутренних систем находите слабые места вашей системы, которыми могут воспользоваться злоумышленники. В результате вы вовремя отреагируете на угрозу и усилите защиту.

Непрерывное обучение

Киберпреступники постоянно совершенствуют свои методы, и ваши стратегии защиты не должны от них отставать. Регулярное обучение и повышение

квалификации — неотъемлемая часть работы специалистов по кибербезопасности. Крайне важно следить за новейшими инструментами, методами защиты и видами атак.

Для этого я рекомендую обмениваться опытом с коллегами, например на форумах и в специальных группах, где вы можете обсуждать новые виды угроз, делиться мнениями и учиться на примере других. Если вы в курсе новинок и постоянно взаимодействуете с профессиональным сообществом, то сможете улучшить свои стратегии защиты и будете на несколько шагов впереди потенциальных киберугроз.

Платформы для разведки киберугроз и интеграция OSINT

Платформы для разведки киберугроз можно представить как смотровые башни цифрового мира, дежурство на которых позволяет дозорным оставаться в курсе всего, что происходит в округе. Они собирают, анализируют и структурируют информацию из всей Сети, сообщают ее специалистам по кибербезопасности и помогают им своевременно выявлять потенциальные угрозы. Благодаря этим платформам организации получают шанс подготовиться к атакам до того, как они нанесут вред.

Однако функции этих платформ не ограничиваются сбором данных. Они выполняют несколько важных задач, обеспечивая комплексную защиту:

- **Сбор данных.** Платформы сканируют множество источников — от новостных сайтов и блогов до ресурсов в самых потаенных уголках интернета. Они ищут любые признаки угроз, будь то вредоносное ПО или планы кибератак.
- **Анализ в режиме реального времени.** Платформы для разведки киберугроз обладают возможностями почти мгновенно обрабатывать огромные объемы данных. С помощью специальных технологий они быстро анализируют информацию и выявляют опасность. Вот парочка используемых ими технологий:
 - **Машинное обучение.** Благодаря алгоритмам машинного обучения платформы способны анализировать закономерности в данных и учиться на предыдущих инцидентах. В результате они точнее предсказывают новые угрозы и выявляют отклонения от привычной активности, которые свидетельствуют о потенциальном нарушении безопасности.

- **Обнаружение сигнатур.** Более традиционный, но оттого не менее важный метод защиты. Платформа сканирует поступающие данные в поисках известных сигнатур — цифровых отпечатков, которые оставляет вредоносное ПО. Так она особенно эффективно предотвращает уже известные угрозы.
- **Рассылка оповещений.** Обнаружив опасность, будь то новое вредоносное ПО или активная атака, платформа моментально отправляет предупреждение. Это позволяет специалистам быстро принимать меры.
- **Интеграция с другими инструментами.** Платформы для разведки интегрируются с другими системами. Они взаимодействуют с антивирусными программами, брандмауэрами и прочими инструментами. Такое сотрудничество гарантирует комплексную защиту всех компонентов инфраструктуры организации.

Ключевые игроки

Познакомимся с наиболее известными платформами для анализа киберугроз:

- **Trellix** (ранее **FireEye**) (<https://www.trellix.com/platform/>). Помогает не только выявлять, но и устранять сложные киберугрозы.
- **IBM X-Force Exchange** (exchange.xforce.ibmcloud.com). Это, скорее, сообщество, где специалисты из разных стран обмениваются информацией о киберугрозах. Нашел сам — поделись с другим!
- **CrowdStrike Falcon X** (crowdstrike.com/falcon-platform). Гармонично сочетает технологии и агентурную разведку. Платформа автоматически выявляет угрозы, а привлеченные специалисты помогают ей развивать системы.
- **Recorded Future** (recordedfuture.com). Вот мой фаворит! Прорицатель в мире кибербезопасности. Обрабатывая огромнейшие объемы данных, платформа предсказывает возможные угрозы, помогая к ним подготовиться. Кроме того, она предлагает массу бесплатных ресурсов для исследования вопросов защиты.

На всех перечисленных платформах OSINT играет важную роль. С помощью информации, извлеченной из открытых источников, аналитические системы работают еще эффективнее, формируя более полное представление о потенциальных киберугрозах. Ну, *теперь-то* вы понимаете, насколько OSINT мощный инструмент?

Интеграция OSINT в процессы разведки киберугроз

Разведка по открытым источникам помогает защитить организации от постоянно совершенствующихся киберугроз. Службы безопасности могут использовать общедоступную информацию для разработки надежных стратегий защиты. Тем не менее для интеграции OSINT в существующие системы нужно тщательно продумать, как из информационного шума извлекать важные сигналы.

Меня постоянно спрашивают: *Дейл, ты же киберковбой, как бы ты интегрировал OSINT в разведку?* Ну, для начала не забываем, что каждая компания уникальна, но в целом я рекомендовал бы организовать интеграцию так:

1. Шаг первый: определите цели! Прежде чем садиться в седло и отправляться в путь, четко сформулируйте, чего вы добиваетесь. Боретесь с угрозами в отрасли или расследуете атаку? Научитесь отличать врагов от друзей. Думаю, вам пригодится моделирование угроз. Это помогает выявить потенциальные опасности с учетом особенностей отрасли, масштаба компании и ее цифрового следа. Такой подход классифицирует угрозы по их вероятности и возможному влиянию, позволяя расставить приоритеты.
2. Затем приступайте к сбору информации: просматривайте форумы и социальные сети — все, где толчется народ. Но помните, что не все источники одинаково полезны, опирайтесь только на авторитетные ресурсы. Используйте веб-скрейперы для систематического извлечения информации из интернета. Одни инструменты, вроде Shodan, подходят для поиска устройств, подключенных к Сети, а другие собирают данные на форумах и в социальных сетях. С помощью API различных платформ можно автоматизировать сбор информации об угрозах.
3. Теперь данные нужно привести в порядок, чтобы поймать плохих парней. Дедупликация избавит от повторяющейся информации, нормализация унифицирует формат данных и упростит их анализ. Не забудьте добавить контекст: в каждом элементе отметьте надежность источника и степень соответствия вашей модели угроз. Теперь можно двигаться дальше!
4. Используйте полученную информацию, чтобы построить взаимосвязи, выявить закономерности и схватить негодяев! Вы можете собрать данные о кампаниях злоумышленников, проанализировать тенденции киберугроз и даже установить источник опасности. Правильно обученный ИИ поможет находить отклонения и подозрительные закономерности, которые указывают на возникающую угрозу безопасности. Инструменты для анализа сети позволят связать разрозненные данные и выявить потенциальных злоумышленников и методы их работы. Отличная работа, дружище!

5. Вооружившись информацией, нужно поделиться ею с коллегами, чтобы каждый мог противостоять угрозе. Для этого используйте специальные инструменты, предназначенные для совместной работы, или интегрируйте находки в существующие системы безопасности. Не помешает также обратная связь: проводите регулярные встречи или обменивайтесь идеями на цифровых платформах, чтобы понять, как улучшить процессы. Я сам учитываю все отзывы и предложения, стараясь постоянно совершенствовать свой подход.
6. Наконец, дайте команду «сторожить!» своим верным псам. Настройте брандмауэры для блокировки известных вредоносных IP-адресов, обновите спам-фильтры, чтобы предотвратить новые фишинговые атаки, или опишите новые угрозы в обучающих программах для сотрудников. В общем, сделайте все возможное, чтобы враг не прошел.
7. Регулярно анализируйте результаты и пересматривайте подходы. Я вне-дляю новые инструменты, чтобы автоматизировать рутинные задачи и готовиться к новым уловкам злоумышленников. А благодаря сотрудничеству с другими парнями мы станем лучшими киберковбоями на всем Диком Западе!
8. Итак, садимся на коней, друзья! Вместе мы защитим нашу компанию от бандитов и грабителей. В путь!

Делясь с сообществом данными разведки, вы словно предупреждаете соседей о подозрительной машине: теперь каждый будет присматриваться и вести себя осторожнее. Точно так же работает OSINT в цифровом мире. Сообщая другим о выявленных опасностях и хакерских приемах, вы помогаете коллегам защититься.

Обмен данными OSINT с другими платформами и командами

Решив поделиться данными, полученными во время разведки, выберите, как и кому их передать. Сначала рассмотрим, кому они могут пригодиться:

- **Отдел безопасности вашей организации.** Это специалисты вашей компании, которые занимаются ИТ и безопасностью. Им нужна подробная информация, которая поможет эффективно реагировать на угрозы. Поделитесь с ними данными о типах вредоносного ПО, методах атак, индикаторах компрометации и прочими техническими сведениями. Благодаря этому они быстро разработают защитные механизмы.

- **Другие отделы.** Не все сотрудники компании нуждаются в сложных технических подробностях. Коллег от отдела из маркетинга, продаж или других отделов важно проинформировать об угрозах, объяснив ситуацию доступно и понятно. Например, так: «Сейчас постоянно приходят фишинговые письма от имени клиента. Будьте бдительны, если вас просят перечислить средства или сообщить какую-то информацию».
- **Внешние платформы.** Тематические форумы и другие цифровые пространства, на которых специалисты по кибербезопасности из разных организаций обмениваются информацией о киберугрозах и обсуждают данные разведки. Среди таких платформ, например, ThreatConnect (threatconnect.com) и IBM X-Force Exchange, о которой я рассказывал всего несколько страниц назад. Мы обмениваемся информацией не только чтобы следить за новостями, но и для повышения общего уровня защиты от киберугроз. Однако важно сохранять баланс: данные должны быть достаточно подробными, чтобы нести пользу, но не создавать новые уязвимости.

Как адаптировать сообщение для конкретной аудитории:

- **Для технических специалистов.** Им важно получить исчерпывающую информацию, включая подозрительные IP-адреса, доменные имена, хеши файлов, связанные с угрозой, и другие технические находки. На основе этих данных специалисты смогут эффективно настроить защиту, например, обновить брандмауэры или антивирусное ПО, что позволит своевременно выявлять новые опасности.
- **Для людей без технического опыта.** Здесь важно объяснить суть проблемы доступно, без сложных терминов и сленга. Например, если возникла угроза фишинговых атак, дайте простой и понятный совет: «Будьте осторожны с письмами, в которых просят сообщить конфиденциальную информацию, и никогда не переходите по ссылкам от неизвестных отправителей».

Быстрый обмен полезной информацией

Сфера кибербезопасности развивается стремительными темпами, а угрозы постоянно меняются и становятся сложнее. Оперативный обмен данными позволяет специалистам реагировать быстрее, чем угроза распространится или эволюционирует.

Делитесь только той информацией, которая важна и полезна для аудитории. Если данные не имеют прямого отношения к человеку или не предполагают конкретных действий, лучше оставить находку при себе. Чрезмерное

количество информации может отвлечь, и важный факт затеряется в океане ненужных подробностей.

Обмениваясь данными, особенно на внешних платформах, сохраняйте конфиденциальность информации. Важно находить баланс между пользой и защитой передаваемых сведений. Например, сообщить об учащении определенного типа атак будет полезно, а раскрыть конкретные уязвимости компании — нет.

Спросите у других их мнение. Когда вы делитесь данными разведки, просите обратную связь и дополнительную информацию. Так вы больше узнаете об угрозе и повысите точность анализа. В командной работе вклад каждого участника помогает всем достичь наилучшего результата.

Обмениваясь знаниями о киберугрозах, вы не только приносите пользу своей команде или компании, но и помогаете мировому сообществу обеспечить безопасность в интернете. Помните: благодаря сотрудничеству каждый специалист по безопасности становится только сильнее.

Разработка программы разведки киберугроз на основе OSINT

В этом разделе мы рассмотрим важнейшую сторону OSINT: разработку **программы разведки киберугроз (СТИ, cyber threat intelligence)**. Звучит как название миссии секретного агента, но на практике все намного проще. Начнем с самого важного — определим требования.

Что такое требования к разведке?

Они основа кибербезопасности. Требования к разведке позволяют сосредоточиться на данных, которые наиболее важны для защиты вашей организации. Представьте, что именно вы отвечаете за кибербезопасность в компании. Ваш первый вопрос: *«Какая информация поможет мне обеспечить защиту?»* Ответ на этот вопрос и формирует требования к разведке. Благодаря им специалист может эффективнее определять наиболее актуальные угрозы и правильно на них реагировать.

Определение ключевых потребностей

Возникает вопрос: как понять, какие именно данные вам нужны? Здесь подход будет индивидуальным для каждой компании. Например, игровая студия больше беспокоится о защите серверов и данных игроков, тогда

как розничный магазин стремится обезопасить транзакционные данные клиентов.

Главное — точность и конкретика. Недостаточно сказать просто «*Мы хотим защитить сеть*». Важно четко сформулировать задачи. Какие именно элементы требуют защиты? Какие типы атак для вас наиболее опасны? Чем подробнее и точнее вы сформулируете свои потребности, тем эффективнее сможете выстроить меры безопасности.

Кроме того, убедитесь, что требования к разведке соответствуют общим целям организации. Если руководство больше всего волнуют утечки данных, то нужно всеми силами постараться их предотвратить.

Значение OSINT

В огромном потоке информации OSINT, словно мощное увеличительное стекло, помогает сфокусироваться на актуальных данных. С помощью инструментов OSINT специалисты по кибербезопасности просматривают социальные сети, форумы, блоги, новостные сайты и другие общедоступные ресурсы в поиске данных об угрозах: от обсуждений нового вредоносного ПО на хакерских форумах до утечек данных, освещаемых в СМИ. Благодаря OSINT специалисты могут опережать преступников и заранее принимать меры для защиты организаций. «*Как?*» — спросите вы. Давайте разберемся.

OSINT и жизненный цикл организации

Подход к OSINT напрямую зависит от этапа развития организации. Во время становления разведка может сводиться к просмотру новостей и тенденций отрасли. По мере роста организации подход к OSINT становится более структурированным, и разведка превращается в неотъемлемую часть системы безопасности. Зрелые компании создают специализированные команды и применяют довольно продвинутые инструменты для обработки общедоступных данных. С помощью OSINT такие команды не только узнают текущее положение дел, но и прогнозируют будущие события, анализируют тенденции и даже предотвращают вероятные угрозы.

Интеграция внутренних и внешних данных

Эффективность OSINT возрастает, если объединить результаты разведки с данными от внутренних систем, включая журналы безопасности, отчеты об инцидентах или обратную связь от сотрудников. Такая интеграция дает более полное представление о защите компании от киберугроз.

Программа киберразведки должна включать постоянный мониторинг как внутренних, так и внешних источников информации. Отслеживайте события в цифровом мире, регулярно обновляйте базы данных разведки и поддерживайте их актуальность, чтобы организация всегда была на шаг впереди преступников.

Создание сильной многопрофильной команды

Успех программы зависит от работающих в ней людей. У них должны быть разнообразные навыки и опыт. Вам потребуются специалисты по кибербезопасности, аналитики данных, исследователи и даже психологи, способные понять мотивы хакеров. Формируя такую команду, обратите внимание на следующие факторы.

- Постоянно развивайте навыки специалистов. Поощряйте обучение и повышение квалификации: организуйте регулярные тренинги и мастер-классы, а также отправляйте сотрудников на конференции по кибербезопасности. С таким подходом команда всегда будет в курсе новых угроз и технологий.
- Поддерживайте командный дух и атмосферу сотрудничества и создайте среду, в которой идеи и мнения будут только приветствоваться. Поощряйте инновации и нестандартное мышление, вдохновляя команду на разработку новых методов извлечения и анализа данных.
- Чтобы повысить эффективность программы, обеспечьте команду подходящими инструментами. Тщательно выберите ПО для сбора и анализа данных, средства мониторинга угроз и платформы киберразведки. Отдавайте предпочтение масштабируемым, удобным инструментам, которые включают все необходимое для вашей организации.
- Если инструменты не покрывают всех ваших потребностей, будьте готовы создавать индивидуальные решения, например ПО для анализа данных или алгоритмы для выявления специфических угроз.

Помните: прежде чем разрабатывать программу киберразведки с применением OSINT, важно определить, какая именно информация поможет обеспечить безопасность компании.

Теперь вы знаете все об интеграции OSINT в киберразведку. Объединяйте данные разведки с информацией от внутренних систем безопасности, выбирайте подходящие инструменты и всегда старайтесь учиться и адаптироваться к изменениям цифровой среды. Отслеживайте возникающие угрозы и обменивайтесь опытом с сообществом, и тогда ваши данные будут в безопасности.

Пример из практики: использование OSINT для расследования инцидента

В июле 2020 года произошел масштабный взлом учетных записей Twitter, в результате которого знаменитые люди и компании стали невольными участниками мошенничества с биткоинами. Среди пострадавших оказались Барак Обама, Илон Маск, Джейф Безос и компания Apple: хакеры использовали их профили для продвижения криптовалютной аферы (<https://www.theverge.com/22163643/twitter-hack-bitcoin-scam-july-2020-elon-musk>).

Атака началась с тщательно продуманной фишинговой кампании, жертвами которой стали сотрудники Twitter. Злоумышленники совершали телефонные звонки, целенаправленно связываясь с теми, кто имел доступ к внутренним документам.

Они выдавали себя за сотрудников ИТ-отдела Twitter, убеждая «коллег» предоставить свои учетные данные. Приемы социальной инженерии открыли хакерам доступ к внутренним системам компании.

После атаки специалисты по кибербезопасности исследовали инцидент с помощью OSINT. Они изучили общедоступную информацию, включая IP-адреса и данные о регистрации доменов, чтобы определить источник мошеннических сообщений.

Проанализировав криптовалютные кошельки, указанные в твитах мошенников, и сопоставив данные блокчайна с общедоступной информацией, специалисты проследили перемещение средств. С помощью инструментов OSINT они отслеживали распространение атаки и ее влияние в социальных сетях, что позволило быстро понять масштабы взлома. В ответ на атаку Twitter заблокировал скомпрометированные учетные записи, удалил мошеннические твиты и временно ограничил публикации для верифицированных пользователей.

OSINT продемонстрировал свою эффективность и после инцидента: разведка по открытym источникам помогла определить методы злоумышленников и предотвратить подобные атаки в будущем. В результате взлома Twitter стало ясно, насколько важно обучать сотрудников противодействию социальной инженерии и разрабатывать надежные меры внутренней безопасности. Случай также показал, что инструменты OSINT помогают оперативно реагировать на атаку и проводить анализ произошедшего.

Таким образом, взлом стал ярким примером того, как продуманные фишинговые атаки и приемы социальной инженерии могут привести к серьезным

нарушениям в системе безопасности. Он подчеркнул ключевую роль OSINT в расследовании инцидентов, ведь благодаря инструментам разведки по открытым источникам специалисты могут быстро обнаружить киберугрозу, отреагировать на нее и проанализировать инцидент для предотвращения последующих атак. Это событие напоминает о том, как важно постоянно совершенствовать подходы к кибербезопасности и всегда быть начеку. Теперь-то вы понимаете, как OSINT помогает в киберразведке?

Итоги

В этой главе мы прошли путь от теоретических основ OSINT до ее практического применения в сфере кибербезопасности. Я рассказал, как интеграция OSINT в разведку киберугроз помогает выявлять потенциальные проблемы и улучшать механизмы защиты, а вы убедились в этом, изучив примеры расследования инцидентов, которые произошли в реальной жизни. Полученные знания помогут вам эффективно использовать OSINT, сочетая цифровые технологии и аналитическое мышление. В постоянно развивающемся мире цифровой безопасности, где многое строится на взаимодействии людей, эти знания станут весомым преимуществом.

В следующей главе мы рассмотрим, как защитить от киберугроз личную и корпоративную информацию.

ГЛАВА 7

ЗАЩИТА ЛИЧНЫХ И КОРПОРАТИВНЫХ ДАННЫХ ОТ КИБЕРУГРОЗ

Современный человек проводит в интернете все больше времени, перенося в виртуальное пространство значительную часть своей жизни, из-за чего киберзащита становится одной из важнейших задач. В этой главе я покажу вам, как эффективно защищать свою цифровую личность и данные организации. Вы узнаете, как превратить общедоступную информацию в мощный инструмент для противодействия угрозам. Мы обсудим ее двойственную природу: узнаем, как данные из открытых источников могут скомпрометировать — или, наоборот, защитить — человека и компанию. В конце этой главы разведка по открытым источникам (OSINT) станет для вас практическим инструментом, который пополнит арсенал средств кибербезопасности.

Мы обсудим следующие темы:

- Как OSINT защищает личные и корпоративные данные
- Личная цифровая гигиена и роль OSINT
- Как OSINT помогает оценить и укрепить безопасность организации
- Выявление и устранение киберугроз
- Расследование взломов и других нарушений кибербезопасности
- Создание устойчивой системы киберзащиты на основе OSINT

Пришло время подробно рассмотреть эти темы. Материал может показаться сложным, но вы обязательно справитесь — особенно если не пропустили ни одной предшествующей главы. Итак, начнем!

Как OSINT защищает личные и корпоративные данные

Добро пожаловать в раздел, посвященный эффективной защите вас и вашей организации от киберугроз! Разведка по открытым источникам стала мощным инструментом, который помогает противостоять цифровым опасностям. Собирая и анализируя данные из новостных статей, юридических документов, социальных сетей и других общедоступных ресурсов, мы можем принимать обоснованные решения.

OSINT имеет множество применений в кибербезопасности. Обычным людям он помогает защищать личные данные, доступные в интернете. В наше время, когда цифровая активность оставляет многочисленные следы, особенно важно осознавать, какие сведения *о вас* сохранились в Сети. Используя методы OSINT, вы можете обнаружить уязвимости, включая незащищенные личные данные, и узнать, как устраниить такие риски и укрепить свою цифровую безопасность.

Для организаций OSINT стал незаменимым инструментом в борьбе с разнообразными киберугрозами. Он помогает определить слабые места в цифровой инфраструктуре, понять тактику потенциальных злоумышленников и оперативно реагировать на новые угрозы. Кроме того, OSINT позволяет отслеживать упоминания об организации в интернете, своевременно выявляя репутационные риски или возможности для сотрудничества.

Преимущества проактивного подхода к кибербезопасности

Проактивный подход к OSINT дает несколько важных преимуществ в вопросах кибербезопасности. Прежде всего, предварительная разведка помогает обнаружить угрозы на самых ранних этапах. Постоянно отслеживая открытые источники информации, организации могут выявить потенциальную опасность до того, как произойдет реальная атака, и заранее принять необходимые меры защиты.

Вторым значимым преимуществом проактивного подхода я считаю вклад в понимание природы киберугроз. С помощью предварительной разведки организации получают больше информации о кибератаках, в том числе о мотивах и тактике злоумышленников. Благодаря этому можно разрабатывать эффективные стратегии защиты.

Проактивный подход в OSINT также незаменим для управления рисками. Постоянный анализ и оценка угроз позволяют организациям адаптировать свои стратегии кибербезопасности к новым обстоятельствам. С таким гибким подходом механизмы защиты становятся надежнее и лучше справляются с актуальными угрозами.

Наконец, предупредить угрозу всегда дешевле, чем устранять последствия, особенно в кибербезопасности. Я рассматриваю такой подход как *гарантию вашей занятости*, ведь он укрепляет позиции специалиста в профессиональной сфере.

Личная цифровая гигиена и роль OSINT

Ваш цифровой след — совокупность данных, которые вы оставляете в интернете. Он содержит взаимодействия в социальных сетях, публикации на форумах, онлайн-транзакции и другие записи. И не только с помощью компьютера. Только подумайте, сколько данных вы оставляете, пользуясь мобильным телефоном!

Существуют инструменты, которые способны просматривать ресурсы в интернете, чтобы составить ваш цифровой портрет. Агрегаторы данных, поисковые системы, специализированное ПО — с их помощью можно выявить уязвимости, созданные неосторожным поведением в Сети. Например, если вы публикуете в социальных сетях чрезмерное количество личной информации, злоумышленник может ею воспользоваться, чтобы притвориться вами и обмануть других людей, либо использовать приемы социальной инженерии. Привычка регулярно проверять цифровой след поможет вам лучше контролировать свои данные в Сети и обезопасить себя.

Выявление и устранение рисков присутствия в Сети

Итак, вы сделали первый шаг к цифровой безопасности: выяснили, что такое цифровой след и как он появляется в Сети. Следующий важный шаг — сократить связанные с ним риски. Для этого нужно изменить настройки конфиденциальности в социальных сетях, закрыв личную информацию, внимательно оценивать сведения, которые вы публикуете в интернете, и регулярно проверять учетные записи, чтобы вовремя заметить подозрительные действия или признаки взлома.

В этом помогут следующие рекомендации:

- **Контролируйте свое присутствие в Сети.** Регулярно проверяйте учетные записи и профили в социальных сетях. Проверьте, какая информация находится в открытом доступе: можно ли ее использовать против вас (например, для кражи личных данных или атак социальной инженерии)? Ниже перечислены инструменты, которые помогут провести аудит присутствия в интернете:
 - **Sprout Social** (<https://www.sproutsocial.com/>). Универсальный инструмент для управления профилями в социальных сетях, в том числе для аудита и анализа информации.
 - **Hootsuite** (<https://www.hootsuite.com/>). Сервис для управления несколькими учетными записями в социальных сетях и анализа их эффективности.
 - **Google Аналитика** (<https://analytics.google.com/>). Инструмент для анализа и отслеживания работы вашего сайта.
- **Ужесточите настройки конфиденциальности.** Проверьте и настройте параметры конфиденциальности в социальных сетях, например Facebook, Twitter, Instagram или LinkedIn. Ограничьте доступ к публикациям, контактным данным и информации профиля так, чтобы они были видны только тем, кому вы доверяете.
- **Поиските информацию о себе в Google.** Проверьте, какие данные о вас доступны в интернете, с помощью поисковых систем (рис. 7.1).
Информация, которую вы увидите в результатах поиска по имени, электронным адресам и номерам телефона, при желании увидит и злоумышленник.
- **Удалите лишнюю информацию.** Если вы заметили, что в интернете опубликованы ваши конфиденциальные данные (например, в старых блогах, публикациях или на форумах), удалите их. При необходимости свяжитесь с администраторами ресурса.

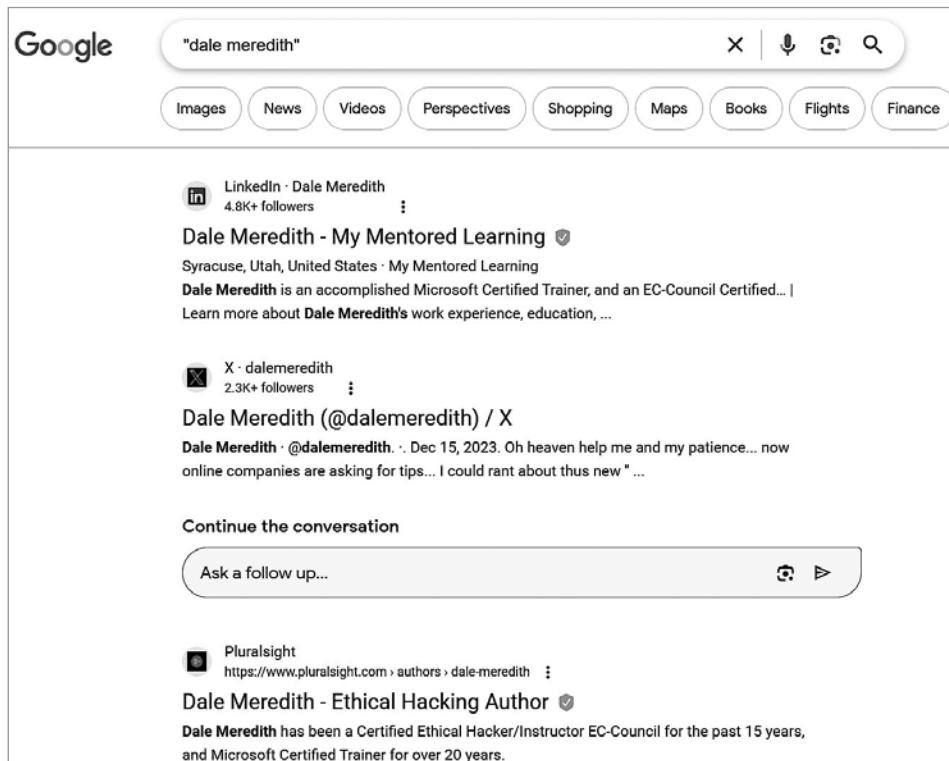


Рис. 7.1. Найдите в Google информацию о себе или своей компании, чтобы понять, что известно в Сети

Следующие инструменты помогают управлять своим присутствием в Сети:

- **Google Оповещения** (<https://www.google.com/alerts>). Настройте оповещения на случай упоминания вашего имени или других личных данных. Если в Сети появятся данные, содержащие эти идентификаторы, вы получите уведомление. Сервис не раз помогал мне вовремя узнать о новой информации, связанной с моим именем, и принять меры.

The screenshot shows the Google Alerts configuration page. At the top, it says "Monitor the web for interesting new content". Below is a search bar with the query "packtpub.com". The configuration options are as follows:

- How often: As-it-happens
- Sources: Automatic
- Language: English
- Region: Any Region
- How many: Only the best results
- Deliver to: RSS feed

At the bottom left is a "Create Alert" button, and at the bottom right is a "Hide options" link.

In the main content area, titled "Alert preview", it states: "There are no recent results for your search query. Below are existing results that match your search query." Below this, under the "NEWS" section, there is one result:

Automated Machine Learning - Packt
Packt
This book reviews the underlying techniques of automated feature engineering, model and hyperparameter tuning, gradient-based approaches, and much ...
Packt - packtpub.com
Packt | LinkedIn - LinkedIn
Packt - GitHub - GitHub
Full Coverage

Рис. 7.2. Сервис Google Оповещения может сообщать о новых результатах поиска

- **Have I Been Pwned?** (<https://haveibeenpwned.com/>). Этим сайтом управляет мой приятель Трой Хант (Troy Hunt). Здесь можно проверить, не фигурируют ли ваши электронные адреса в похищенных базах данных. Вы сможете оценить риски и принять меры, например сменить пароль или усилить защиту учетной записи. Активируйте функцию **Notify me**,

чтобы получать уведомления, если обнаружится, что ваши данные скомпрометированы.

- Настройки конфиденциальности и инструменты в социальных сетях.** Большинство социальных сетей предлагает разные параметры конфиденциальности. Изучите доступные инструменты и настройте, кто может видеть информацию о вас. Обратите внимание, что настройки могут обновляться, поэтому следите за изменениями через официальные каналы платформ.
- Услуги по удалению данных.** Если вы не можете удалить определенную информацию самостоятельно, обратитесь в специализированные сервисы, например DeleteMe (<https://joindeleteme.com/>). Специалист свяжется с брокерами данных и администраторами сайтов от вашего имени и запросит удаление.

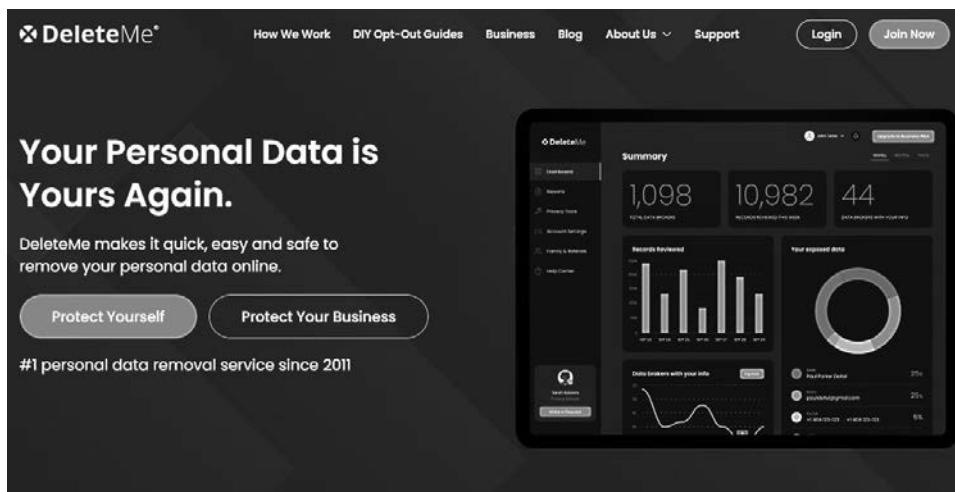


Рис. 7.3. joindeleteme.com помогает управлять личной информацией в интернете

DeleteMe – по-настоящему хороший сервис для защиты конфиденциальности, хотя его услуги дороговаты. Но разве можно экономить, когда речь идет о конфиденциальности?

- Следите за актуальной информацией.** Оставайтесь в курсе последних тенденций в области конфиденциальности и безопасности. Изучайте новые приемы киберпреступников и знакомьтесь с инструментами и сервисами для защиты цифровой идентичности.

- **Узнайте больше о фишинге и социальной инженерии.** Учтесь распознавать фишинговые атаки и приемы социальной инженерии. Эти знания помогут вам избежать обмана и защитить личную информацию. Самый простой способ узнать об этих атаках — посмотреть прекрасное выступление пентестера Криса Пritcharda (Chris Pritchard) с конференции DefCon: <https://www.youtube.com/watch?v=jfXwdH-fkLE>.

Следуя этим рекомендациям и используя доступные инструменты, обычные пользователи могут существенно снизить риски, связанные с присутствием в Сети. Проактивный подход к цифровой гигиене не только убережет личную информацию, но и снизит шансы стать жертвой кибератак.

Повышение конфиденциальности и безопасности

Однако отслеживать и устранять риски недостаточно — важно повышать конфиденциальность и безопасность своих данных. Начните с создания надежных, уникальных паролей для каждой учетной записи. Хороший пароль должен быть длинным, содержать буквы, цифры и специальные символы, а также избегать очевидных данных, включая имя, дату рождения или другие элементы, доступные в открытых источниках (например, хобби или любимые спортивные команды). Помните золотое правило надежного пароля: *чем длиннее, тем лучше*. Кроме того, никогда не используйте один и тот же пароль для разных учетных записей. Для удобства я настоятельно рекомендую использовать менеджер паролей. Также обязательно активируйте двухфакторную аутентификацию во всех сервисах, которые ее поддерживают, и регулярно изучайте новые методы фишинга и мошенничества.

Инструменты OSINT помогают обнаружить уязвимости, возникшие из-за ваших действий в интернете, либо уязвимости ваших цифровых ресурсов. К примеру, можно выяснить, попала ли ваша личная информация в утекшие базы данных и используют ли ваш электронный адрес для рассылки спама.

Наконец, важно следовать важнейшим рекомендациям по цифровой гигиене. Регулярно обновляйте программное обеспечение, чтобы устраниТЬ уязвимости в системе безопасности, и тщательно выбирайте приложения и сервисы. Изучайте новые угрозы в киберпространстве и способы их предотвращения. Я бы еще уделил особое внимание растущей популярности **искусственного интеллекта (ИИ)**, возможности которого меня пугают. Генеративный ИИ и технологии дипфейк стремительно развиваются, и злоумышленники

неизбежно начнут их использовать против вас. Поэтому добавьте изучение ИИ в список своих приоритетов.

Как OSINT помогает оценить и укрепить безопасность организации

Общий уровень защиты организации от киберугроз определяется безопасностью ее самого слабого элемента. Злоумышленники нередко атакуют компоненты внешней инфраструктуры, включая сайты, серверы электронной почты и облачные сервисы. *Крайне важно* понять, как работают эти элементы, и принять меры для повышения их безопасности. Здесь в дело вступает OSINT, благодаря которому можно подробно проанализировать потенциальные уязвимости и угрозы.

Оценка и укрепление безопасности сети включают поиск уязвимостей в веб-приложениях, почтовых серверах, DNS-конфигурациях и других общедоступных ресурсах, а также разработку эффективных мер для сокращения рисков.

Определение потенциальных уязвимостей

Каждый компонент инфраструктуры имеет собственные уязвимости. Ниже вы найдете инструменты, которые помогут выявить слабые места.

- Веб-приложения и сайты.** Чаще всего первые атаки приходятся именно на веб-приложения. Например, инструмент Nikto2 (<https://cirt.net/Nikto2>) сканирует веб-приложения, проверяя их на уязвимости. Он может находить более 7000 известных уязвимостей, в том числе на сложных формах, которые включают несколько этапов ввода информации, и в защищенных паролем элементах.

```
(kali㉿kali)-[~]
└─$ nikto -h scanme.nmap.org
- Nikto v2.5.0

+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2024-02-12 18:27:28 (GMT-7)
```

Рис. 7.4. Nikto сканирует scanme.nmap.org

Инструмент работает с двумя типами сканирования: полным и частичным, сочетая их так, чтобы проверять всю систему.

- **Серверы электронной почты.** Электронная почта остается одной из главных мишеней для фишинга и вредоносного ПО. Для защиты можно использовать инструмент Vipre (<https://vipre.com/>), который обеспечивает комплексную безопасность почтовых систем. Он предотвращает вирусные атаки, распространение программ-вымогателей и похищение данных, предоставляя актуальную информацию о возникающих угрозах для оперативной защиты от них.
- **Сети.** Защита сетевой инфраструктуры — основа безопасной работы. Программа Zeek (<https://zeek.org/>) наблюдает за сетевым трафиком, не вмешиваясь в его поток. Она создает подробные журналы транзакций, фиксирует содержимое файлов и предоставляет данные для дальнейшего анализа.

```
root@debian12:/opt/zeek/logs/current# cat dns.log | zeek-cut id.orig_h query answers
10.0.2.15      -      -
10.0.2.15      httpredir.debian.org    debian.map.fastlydns.net,199.232.46.132
10.0.2.15      httpredir.debian.org    debian.map.fastlydns.net,2a04:4e42:48::644
10.0.2.15      _http._tcp.security.debian.org  debian.map.fastlydns.net
10.0.2.15      [REDACTED]
10.0.2.15      [REDACTED]
10.0.2.15      [REDACTED]
10.0.2.15      [REDACTED]
10.0.2.15      httpredir.debian.org    debian.map.fastlydns.net,199.232.46.132
10.0.2.15      httpredir.debian.org    debian.map.fastlydns.net,2a04:4e42:48::644
10.0.2.15      download.opensuse.org   195.135.221.134
10.0.2.15      download.opensuse.org   2001:67c:2178:8::13
root@debian12:/opt/zeek/logs/current#
```

Рис. 7.5. Инструмент Zeek с открытым исходным кодом наблюдает за запросами в Сети

Если вы занимаетесь кибербезопасностью уже несколько лет, то, возможно, помните программу **Bro**. Так вот, Zeek — ее обновленная версия. По умолчанию Zeek генерирует более 60 журналов, отслеживает более 3000 сетевых событий и установлен более чем на 10 000 устройствах по всему миру. Интеграция с DNS-системами помогает предотвратить атаки перенаправления или перехват трафика, а регулярный анализ DNS — вовремя выявлять ошибки конфигурации или несанкционированные изменения. Поверьте, инструмент просто отличный.

- **Регулярный поиск уязвимостей.** Для защиты цифровых ресурсов важно регулярно их сканировать с помощью специализированных инструментов, например SanerNow (<https://www.secpod.com/>). Он помогает выявлять уязвимости и ошибки конфигурации, а также может исправлять их в режиме реального времени.
- **Безопасность устройств.** Устройства конечных пользователей крайне важно защищать от вредоносного ПО и других угроз. Malwarebytes (<https://www.malwarebytes.com/>) предлагает полный комплекс инструментов, включая поиск отклонений, анализ поведения и предотвращение угроз в режиме реального времени.

Примечание. О конфиденциальности при использовании онлайн-инструментов

Если правильно применять инструменты Nikto2, Vipre, Zeek, SanerNow и Malwarebytes и соблюдать осторожность, можно проверить защиту своей системы, не раскрывая конфиденциальную информацию. Выбирая инструменты для оценки безопасности, учитывайте их надежность, соблюдение конфиденциальности и соответствие требованиям организации.

Мир цифровых технологий стремительно развивается, а вместе с ним и методы, которые хакеры используют для взломов. Чтобы оставаться в безопасности, важно постоянно следить за появлением новых инструментов и подходов к киберзащите. Пусть это войдет в привычку так же, как обновление устройств и программ.

Программы-вымогатели: выявление и противодействие

Современный цифровой мир постоянно меняется, и киберпреступники становятся все изощреннее. Одну из опаснейших форм атак совершают программы-вымогатели — вредоносное ПО, которое шифрует данные в системе и блокирует к ним доступ, пока вы не заплатите выкуп злоумышленникам. Такие программы известны своим разрушительным влиянием как на отдельных пользователей, так и на компании или даже общественную инфраструктуру.

- **Основные характеристики программ-вымогателей.** Как правило, такие программы шифруют файлы на устройстве жертвы, полностью блокируя

к ним доступ. Злоумышленники предлагают ключ расшифровки за определенную сумму, часто в криптовалюте, например биткоинах, из-за чего их трудно отследить.

Ранее программы-вымогатели распространялись хаотично и поражали случайных пользователей. Однако в последние годы атаки приобретают более целенаправленный характер. Их жертвами становятся компании, государственные учреждения и другие организации, у которых злоумышленники могут требовать гораздо более высокий выкуп. Подобно многим другим киберугрозам, программа-вымогатель проникает в систему через фишинговые письма, которые обманом заставляют пользователей скачать вредоносное ПО.

- **Последствия атаки.** Помимо необходимости заплатить деньги, жертвы сталкиваются с огромными финансовыми убытками из-за простоев, утраты данных и подрыва репутации. Программа-вымогатель может полностью парализовать работу всех систем, что особенно опасно для сферы здравоохранения и других государственных служб. Даже если жертва выплатит выкуп, это не гарантирует полного восстановления данных. Кроме того, злоумышленники могут похитить и распространить конфиденциальную информацию.
- **Профилактика и снижение рисков.** Чтобы надежно защититься от программ-вымогателей, необходимо принять следующие меры: регулярно сохранять резервные копии данных, обучать сотрудников распознавать фишинг и своевременно обновлять системы безопасности. Резервное копирование позволяет восстановить информацию без необходимости платить выкуп. Обучение персонала помогает предотвратить заражение вредоносным ПО еще на этапе его распространения. А обновление системы безопасности и установка актуальных патчей мешает злоумышленникам использовать известные уязвимости. Кроме того, важно разработать четкий план действий во время инцидентов, который позволит минимизировать последствия атаки.
- **Направление развития программ-вымогателей.** Последние новости о программах-вымогателях подтверждают, что атаки становятся все более продуманными и целенаправленными. Злоумышленники тщательно изучают отдельные организации или целые отрасли, чтобы проводить атаки с большей точностью. Особую тревогу вызывает тактика *двойного вымогательства*: помимо шифрования данных, хакеры угрожают опубликовать конфиденциальную информацию жертвы, если та откажется платить выкуп.

Обнаружение фишинга и приемов социальной инженерии

Чтобы выявлять программы-вымогатели и другое вредоносное ПО с помощью инструментов OSINT, нужно придерживаться проактивного подхода к кибербезопасности. Специалисты отслеживают хакерские форумы и даркнет-рынки, чтобы заранее получать информацию о новых типах вредоносного ПО и действиях киберпреступников. Специализированные ресурсы публикуют информацию об угрозах в режиме реального времени. Анализ фишинговых писем, которые часто служат каналом распространения вредоносного ПО, помогает определить векторы атак. Изучение IP-адресов, URL и хешей файлов в открытых базах данных позволяет выявить вредоносные объекты. Все эти методы OSINT помогают специалистам по кибербезопасности прогнозировать и предотвращать угрозы, эффективно защищая цифровые ресурсы компаний.

Анализ подозрительных URL с использованием OSINT открывает ценную информацию о регистрации домена, его текущем статусе и возможной преступной активности. Большшим подспорьем для специалистов стал сервис WHOIS, где можно найти данные о владельцах доменов и выявить потенциальные проблемы с подлинностью.

Заголовки электронных писем — еще один важный источник информации об угрозе. Тщательный анализ заголовков позволяет определить отклонения от закономерностей или признаки подмены адреса. Например, строка `Received: from` может содержать важную информацию о настоящем источнике письма и часто помогает обнаружить скрытые намерения отправителя.

Анализ социальных сетей помогает определить угрозы социальной инженерии. Изучая профили и публикации, специалисты обращают внимание на личные данные, информацию об интересах и связях: все это злоумышленник может использовать для целенаправленных атак. Аналогично регулярное отслеживание других онлайн-платформ позволяет обнаружить общедоступные сведения о сотрудниках и тем самым предотвратить атаки с использованием приемов социальной инженерии.

История хакерской группы Exotic Lily

Деятельность хакерской группы Exotic Lily наглядно демонстрирует, как злоумышленники проводят целенаправленные фишинговые атаки с помощью методов OSINT.

Exotic Lily предпочтает целевой фишинг (spear-phishing). Он напоминает рыбалку с гарпуном: вместо того чтобы ловить всю рыбу в озере, рыбак выбирает определенную цель. Аналогично злоумышленники из Exotic Lily не делают массовые рассылки, отправляя электронные письма тысячам пользователей. Вместо этого они тщательно подбирают жертву — конкретного человека или компанию — и создают письмо именно для нее. В результате письмо выглядит правдоподобно и внушает доверие: оно может имитировать сообщение от друга, начальника или известной компании.

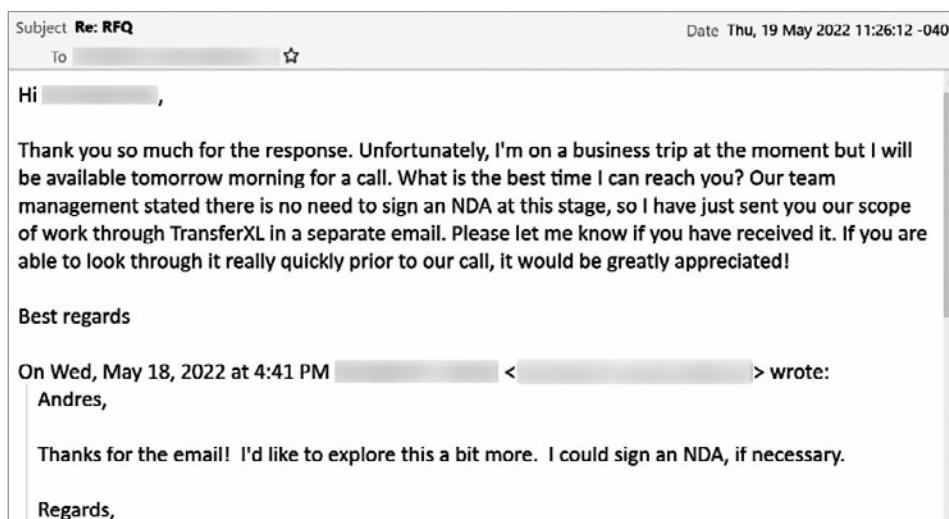


Рис. 7.6. Пример электронного письма от Exotic Lily¹

¹ Привет, ...

Большое спасибо за ответ. К сожалению, я сейчас нахожусь в деловой поездке, но завтра утром буду доступен для звонка. В какое время вам удобнее позвонить? Руководство нашей команды говорит, что на данном этапе необязательно подписывать NDA [соглашение о неразглашении], так что я просто отправил вам описание характера работы через TransferXL, в отдельном письме. Пожалуйста, подтвердите его получение. Будет очень неплохо, если вы сможете быстро проглядеть его, прежде чем мы созвонимся.

С наилучшими пожеланиями

Андрес

Спасибо за письмо. Я бы хотел узнать побольше подробностей. Если надо, могу подписать NDA.

С уважением...

Как же Exotic Lily проводит успешные атаки? Прежде всего хакеры не пренебрегают домашней работой и тщательно готовятся. Они изучают цифровой мир, в котором живет их цель: просматривают социальные сети, сайты компаний и любую общедоступную информацию. Это позволяет им писать максимально убедительные и достоверные письма.

Приведу пример. Допустим, если хакеры узнают, что вы участвуете в конференции по кибербезопасности, они могут отправить вам письмо, представившись организаторами мероприятия. В письме они сообщают об изменениях в расписании и предложат перейти по ссылке для получения подробностей. Однако, нажав на нее, вы незаметно скачаете вредоносное ПО. Как только программа попадет на ваш компьютер, она может заблокировать файлы, требуя выкуп за их восстановление, начать тайно следить за вашими действиями, передавая конфиденциальные данные преступникам, или причинить другой вред.

Фишинговые письма от Exotic Lily составлены очень искусно. Они содержат настоящие имена, логотипы и даже имитируют языковой стиль, чтобы вы поверили в обман. Более того, злоумышленники могут упоминать подробности из вашей личной или профессиональной жизни, о которых, как вам кажется, никто не знает. Именно из-за такой персонализации атаки Exotic Lily крайне опасны, и их очень трудно распознать.

Поняв, как действует хакерская группировка, вы на шаг приближаетесь к защите. Помните, что в цифровом пространстве не все так просто, как кажется на первый взгляд. Будьте внимательны, особенно к письмам с просьбой перейти по ссылке или скачать вложение. Ваша бдительность — первая линия обороны. В следующих разделах мы рассмотрим, как защититься от подобных угроз и уберечь свою информацию.

Фишинговые атаки группы Cobalt Dickens

Вы слышали о хакерской группе Cobalt Dickens? Эти хакеры обманывают сотрудников университетов с помощью очень убедительных электронных писем. Представьте: вы получаете письмо якобы от ИТ-отдела учебного заведения с просьбой обновить пароль. И, конечно же, думаете, что оно безопасно? Именно на это и рассчитывают злоумышленники.

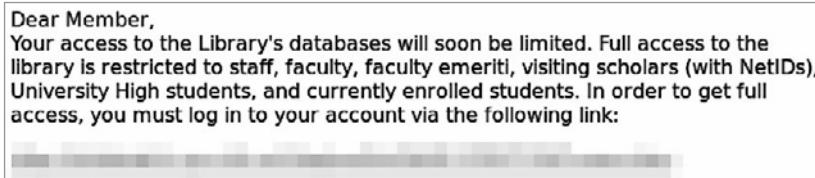


Рис. 7.7. Фишинговое письмо от Cobalt Dickens¹

Но вот в чем особенность этой группы: хакеры не ограничиваются электронными письмами. Они создают поддельные сайты, которые полностью копируют настоящие ресурсы университета. Когда вы, ничего не подозревая, вводите на таких сайтах свои учетные данные, ваши логин и пароль сразу попадают к злоумышленникам.

А знаете, что самое интересное? Они используют инструменты OSINT, из-за чего гораздо лучше скрываются от преследователей. Проникая в системы университетов, Cobalt Dickens получает доступ к ценным материалам: исследованиям и разработкам, над которыми трудятся ученые. Но это еще не все. Они также похищают личные данные студентов и преподавателей, что создает большую угрозу для всех участников образовательного процесса.

Изучив, как действуют группы Cobalt Dickens и Exotic Lily, вы будете готовы реагировать на угрозу. Представьте, будто знаете наперед все фокусы иллюзиониста: понимая, в чем состоит коварный план хакеров, вы будете готовы к атаке и обезопасите как организацию, так и себя лично. Поэтому при работе с электронной почтой будьте бдительны и всегда проверяйте сайты, на которых вводите свои данные. Это лучшая защита от хакеров, которые так и норовят сунуть нос в наш мир, словно хитрые лисы в курятник!

Расследование взломов и других нарушений кибербезопасности

Расследование инцидентов кибербезопасности не обходится без технического анализа задействованных сайтов. С помощью инструментов OSINT

¹ Уважаемый клиент,

Ваш доступ к базам данных библиотеки вскоре будет ограничен. Полный доступ предоставляется штатным сотрудникам, преподавательскому составу, почетным профессорам, студентам-вольнослушателям (с NetID), учащимся университета и недавно зачисленным студентам. Чтобы получить полный доступ, вам необходимо зайти в свой личный профиль по ссылке: ...

специалисты по кибербезопасности исследуют их технические характеристики и выявляют уязвимости. Например, информация о хостинге и SSL-сертификатах уже помогает обнаружить слабые места, а ведь расследование еще практически не началось. Представьте, что сайт компании размещен на сервере с известными проблемами безопасности. Такие инструменты, как WHOIS и DomainTools, позволяют узнать информацию о хостинг-провайдере и исследовать связанные с ним уязвимости. В свою очередь, SSL Test от SSL Labs (<https://www.ssllabs.com/ssltest/>) раскрывает недостатки сертификатов, например устаревшие алгоритмы шифрования или ненадежность организаций, выдавшей сертификат.

The screenshot shows the Qualys SSL Labs SSL Report for the domain `daledumbsitdown.com`. At the top, there's a navigation bar with links to Home, Projects, Qualys Free Trial, and Contact. Below that, a breadcrumb trail shows the user's path: Home > Projects > SSL Server Test > `daledumbsitdown.com`. The main title is "SSL Report: `daledumbsitdown.com`". Below it, it says "Assessed on: Wed, 31 Jan 2024 22:27:32 UTC | Hide | Clear cache". There's a link to "Scan Another >>". The report table has four columns: "Server", "Test time", and "Grade". It lists two entries:

Server	Test time	Grade
2a02:4780:22:47ea:796f:cee5:a437:3c1a Unable to connect to the server	Wed, 31 Jan 2024 22:26:21 UTC Duration: 15.476 sec	-
154.41.250.227 Ready	Wed, 31 Jan 2024 22:26:36 UTC Duration: 56.303 sec	A

Рис. 7.8. Проверка надежности сертификатов с помощью SSL Labs

Старые версии сайтов, доступные через Wayback Machine (<https://web.archive.org/>), могут оказаться настоящим кладезем полезной информации. Зачастую на сайтах компании указывали контактные данные руководителей, и теперь такая информация, даже после удаления из текущей версии сайта, может попасть в руки злоумышленников. Узнав, что компания размещала контакты в открытом доступе, вы способны оценить масштабы угрозы.

Во время расследования не менее важно изучить поддомены целевого сайта. На них нередко размещается конфиденциальная информация, например адреса VPN-порталов или внутренних серверов. Вы можете многое узнать о сетевой архитектуре атакуемой системы, используя специальные команды Google для поиска поддоменов и сервисы Shodan и Censys.

Одним из недооцененных источников данных я считаю открытые ресурсы, например вакансии или резюме сотрудников. В вакансиях порой упоминается об операционных системах серверов, сетевом оборудовании, конфигурациях брандмауэров и других элементах ИТ-инфраструктуры организаций.

Кроме того, инструменты OSINT помогают находить конфиденциальные данные компаний, случайно опубликованные на открытых серверах. Изучив метаданные таких файлов, вы получите дополнительные сведения, включая имя автора, а также ПО и операционную систему устройства, на котором они были созданы.

Выявление источника, масштабов и последствий инцидентов кибербезопасности

Во многом успех расследования инцидентов кибербезопасности зависит от правильно подобранных инструментов OSINT. Они позволяют анализировать сетевой трафик и определять *нормальное* состояние системы, любые отклонения от которого могут указывать на подозрительную активность. Поиск закономерностей помогает выявить автоматизированные механизмы злоумышленников, например вредоносное ПО.

Очень важно находить отклонения от обычных процессов системного администрирования. Тщательно изучая собранные данные, можно заметить необычные действия или ошибки, которые могут свидетельствовать о вмешательстве.

Еще одну часть головоломки вы соберете, исследуя артефакты хоста: запущенные процессы, службы, хеши файлов или действия учетных записей. Каждый элемент может свидетельствовать о несанкционированном доступе или изменениях системы.

Для более глубокого анализа исследователи проверяют подозрительные интернет-соединения, команды PowerShell, используемые для бесфайловых атак, и процессы, связанные с похищением данных. Странные или нетипичные входы в систему также могут указывать на попытки взлома.

Анализ сетевых артефактов — тоже важная часть расследования. Специалисты проверяют DNS-трафик, протоколы удаленного доступа, журналы доступа к сайту и другие данные, которые помогают выявить утечку информации или несанкционированный доступ.

Для расследования кибератак и сбора улик специалисты используют два основных подхода: цифровую криминалистику и OSINT. Цифровой криминалист

напоминает детектива, который исследует улики, оставленные на устройствах и в сетях. Он анализирует список запущенных программ и активность учетных записей в поиске подозрительных интернет-подключений. И все это для того, чтобы выявить признаки скрытого доступа или похищения данных.

Специалиста OSINT, в свою очередь, можно сравнить с сыщиком, который собирает информацию из открытых источников, включая новостные сайты, социальные сети и базы данных. Он не изучает атакуемые системы, а дополняет расследование информацией извне.

Оба подхода очень важны. Первый детально объясняет, что именно произошло в ходе атаки, а второй — предоставляет важный контекст и справочную информацию. В результате сыщик и детектив работают сообща: один изучает место преступления, а другой опрашивает свидетелей и собирает данные из внешних источников. Вместе они воссоздают полную картину о случившемся и помогают значительно усилить защиту от подобных атак в будущем.

Создание устойчивой системы киберзащиты на основе OSINT

OSINT помогает выявить наиболее значительные риски для компании. С его помощью организации обнаруживают целенаправленные угрозы и распространение конфиденциальной информации в открытых источниках, а также предотвращают похищение учетных данных. Специалисты отслеживают угрозы на множестве онлайн-платформ, включая как видимую сеть, так и даркнет. Благодаря OSINT компания может узнать об уязвимостях системы и понять, какие объекты подвергаются риску, что позволит разработать механизмы защиты в соответствии с текущими тенденциями кибербезопасности.

Выделяют активную и пассивную разведку по открытым источникам:

- Для пассивной разведки можно настроить Google Оповещения так, чтобы отслеживать последние тенденции кибербезопасности в вашей отрасли.
- Активный подход предполагает более глубокое и целенаправленное исследование, включая доступ к закрытым форумам даркнета. В результате вы можете составить более подробное представление о потенциальных угрозах.

Но как OSINT помогает организации? Все сводится к тому, чтобы адаптировать собранные данные к ее уникальным особенностям и слабым местам. Все

находки нужно соотносить с принятым профилем риска. Помните: угроза, которая кажется незначительной для одной компании, может стать большой проблемой для другой. Разведка никогда не заканчивается: вы постоянно отслеживаете новые опасности, анализируете их значимость и корректируете стратегии защиты. Словно шахматная партия с высокими ставками, где каждый ваш ход просчитан, а каждая фигура критически важна для защиты от киберугроз.

Сотрудничество с сообществом кибербезопасности

Важным шагом в стратегии кибербезопасности является сотрудничество. Обмениваясь данными OSINT с другими организациями, вы формируете альянс, противостоящий общим угрозам. Вы объединяете усилия, превращая совместные знания в надежный щит.

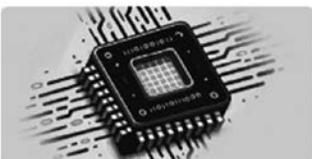
Для этого важно участвовать в обсуждениях на форумах и посещать профессиональные конференции; и не просто слушать, но и активно делиться собственным опытом. Результаты вашей разведки могут стать ключом к решению чьей-то головоломки. Профессиональные мероприятия собирают людей с разными идеями, стратегиями и опытом. Участвуя в конференциях, вы обогащаете свои знания и улучшаете собственные механизмы кибербезопасности. Сотрудничество выгодно всем, ведь обмен опытом помогает укрепить защиту всего сообщества.

Адаптация к изменениям в мире киберугроз

Первый шаг к цифровой адаптации — осведомленность. Мир кибербезопасности меняется стремительно: стратегии, которые вчера считались передовыми, сегодня могут стать неэффективными. Чтобы успешно адаптироваться к изменениям, необходимо следить за последними тенденциями и разработками. Для этого важно участвовать в онлайн-форумах, регулярно посещать профильные семинары, изучать специализированные издания и следить за публикациями профессионалов в социальных сетях. Вот несколько полезных ресурсов:

- **Отраслевые издания.** Изучайте новости и аналитические материалы на сайтах вроде The Hacker News (<https://thehackernews.com/>) и Krebs on Security (<https://krebsonsecurity.com/>). Я просматриваю их почти каждый день.

The screenshot shows the homepage of TheHackerNews.com. At the top, there is a navigation bar with links for Home, Cyber Attacks, Vulnerabilities, Store, and Contact. Below the navigation bar, there are four news cards, each featuring a small image, a title, a date, and a brief description.

- Glupteba Botnet Evades Detection with Undocumented UEFI Bootkit**

 Feb 13, 2024 Cryptocurrency / Rootkit
 The Glupteba botnet has been found to incorporate a previously undocumented Unified Extensible Firmware...
- PikaBot Resurfaces with Streamlined Code and Deceptive Tactics**

 Feb 13, 2024 Cyber Threat / Malware
 The threat actors behind the PikaBot malware have made significant changes to the malware in what has been...
- Midnight Blizzard and Cloudflare-Atlassian Cybersecurity Incidents: What to Know**

 Feb 13, 2024 SaaS Security / Data Breach
 The Midnight Blizzard and Cloudflare-Atlassian cybersecurity incidents raised alarms about the vulnerabilities inherent in...
- Ivanti Vulnerability Exploited to Install 'DSLog' Backdoor on 670+ IT Infrastructures**

 Feb 12, 2024 Vulnerability / Cyber Threat

Рис. 7.9. TheHackerNews.com помогает оставаться в курсе событий

- **Вебинары и онлайн-курсы.** Обучающая платформа Pluralsight (<https://www.pluralsight.com/>) предлагает широкий выбор ресурсов для тех, кто хочет всегда быть в форме. На сайте есть автор, опубликовавший более 30 качественных курсов, — крайне рекомендую ознакомиться с его материалами.

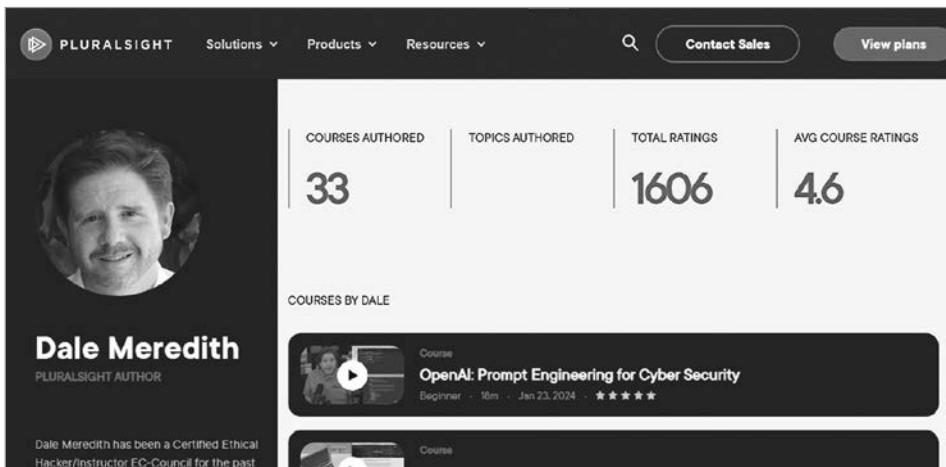


Рис. 7.10. Потрясающий автор на pluralsight.com

Вы также можете участвовать в конференциях. Я каждый год посещаю мероприятия Blackhat и Defcon в Лас-Вегасе, и вы частенько можете увидеть меня на мастер-классах.

- **Социальные сети.** Просматривайте новости в LinkedIn, Twitter и на других платформах, чтобы обмениваться опытом и быть в курсе последних тенденций. Я знаю парня под ником @dalemeredith, очень рекомендую на него подписаться!

Не забывайте: в сфере кибербезопасности информация — не только оружие, но и крепкий щит. Следите за новостями и всегда стремитесь заранее узнать о возможных угрозах. Любопытство — ваш верный друг.

Обновление стратегии кибербезопасности на основе OSINT

Нельзя разработать эффективную стратегию раз и навсегда. Механизмы кибербезопасности с применением OSINT нужно постоянно анализировать, корректировать и обновлять в соответствии с последними данными разведки и тенденциями. Рекомендую уделить внимание следующим аспектам:

- **Переоценка профиля рисков.** С развитием организаций меняются и ее уязвимости. Регулярно пересматривайте профиль рисков, используя актуальные данные разведки, чтобы своевременно выявлять и устранять новые опасности.

- **Усиление защиты.** Изучайте данные о последних кибератаках и, опираясь на них, повышайте уровень защиты: обновляйте брандмауэры, совершенствуйте механизмы сетевой безопасности и обучайте сотрудников распознавать новые приемы фишинга.
- **Актуализация инструментов.** Технологии OSINT постоянно меняются. Следите за появлением новых инструментов и платформ, которые могут улучшить процесс сбора и анализа данных.

Помните об инструментах

Эффективная киберзащита, основанная на OSINT, невозможна без специализированных инструментов и платформ. Мы уже обсудили их в предыдущих главах.

Примечание

Большинство этих инструментов поставляются вместе с Kali Linux, Parrot и Trace Labs. Каждый из них – отличная платформа OSINT.

Я хотел бы напомнить вам об изученных инструментах. Вы увидите, как получить к ним доступ и для чего использовать.

- **Shodan** (<https://www.shodan.io/>). «Поисковая система хакера», в которой вы найдете актуальную информацию об устройствах, подключенных к интернету. В Shodan можно найти общедоступные базы данных; например, если вы хотите отыскать MongoDB, то в поисковой строке введите запрос `product:MongoDB`. Shodan покажет список запрашиваемых баз данных, которые доступны в Сети, что поможет вам выявить потенциально уязвимые системы. При использовании этого инструмента соблюдайте правовые и этические нормы.
- **Google Hacking Database** (<https://www.exploit-db.com/google-hacking-database>). База данных, в которой перечислены специальные поисковые запросы для Google. Например, введите `intitle: index.of`, укажите версию сервера или тип файла, и вы найдете общедоступные каталоги, которые могут хранить конфиденциальные данные. Ресурс помогает выявлять утечки данных и устранять слабые места сайтов. Используйте эту информацию ответственно и не забывайте об этических нормах.
- **Maltego** (<https://www.maltego.com/>). Инструмент для визуализации связей между цифровыми объектами, благодаря которому можно построить карту сетей и проанализировать взаимосвязи между ее элементами. Для начала

можно проанализировать цифровой след доменного имени. Введите доменное имя, а затем используйте встроенные трансформации для поиска связанных элементов: электронных писем, поддоменов или социальных сетей. Благодаря этому инструменту вы можете изучить инфраструктуру домена и связанную с ним цифровую информацию.

- **theHarvester** (<https://github.com/laramies/theHarvester>). Инструмент, доступный на GitHub, предназначен для сбора данных о домене. Указав домен, вы получите список связанных электронных адресов, поддоменов и потенциально связанных с ними обычных пользователей или же сотрудников компании. Полученная информация помогает выявить потенциальные уязвимости в системе и связи с целью.
- **OSINT Framework** (<https://osintframework.com/>). Не самостоятельный инструмент, а удобный каталог, который группирует разные инструменты OSINT по типам искомой информации, например для анализа доменов, поиска людей или работы с социальными сетями. Ресурс помогает быстро найти подходящий инструмент для конкретной задачи, упрощая процесс извлечения данных из открытых источников. Обратите внимание, что на сайте часто обновляются ссылки и появляются новые инструменты.
- **SpiderFoot** (<https://intel471.com/solutions/attack-surface-protection>). Инструмент для автоматического сбора информации. Чтобы начать работу, настройте сканирование выбранного объекта, например доменного имени или IP-адреса. SpiderFoot автоматически соберет различные данные о цели: подробную информацию о домене, электронные адреса и потенциальные уязвимости. Он значительно упрощает этап анализа и помогает выявить слабые места в системе кибербезопасности.
- **Recon-ng** (<https://github.com/lanmaster53/recon-ng>). Инструмент, который работает по модульному принципу. Чтобы его использовать, надо выбирать модуль, учитывая, какие данные необходимо найти (например, электронные адреса, связанные с доменом). Когда вы настроите параметры и запустите Recon-ng, инструмент автоматически соберет информацию из открытых источников. Он помогает создавать цифровые портреты и анализировать общедоступные сведения о цели.
- **TinEye** (<https://tineye.com/>). Система обратного поиска изображений, которая помогает проверить их подлинность и выяснить, встречались ли они на других сайтах. Загрузите изображение или укажите его URL, а система найдет совпадения или похожие изображения в своей базе. Инструмент очень полезен для специалистов OSINT, особенно если в расследовании требуется проверить подлинность изображений.

- **X Pro**, ранее TweetDeck (<https://pro.twitter.com/>). Инструмент для мониторинга и анализа лент Twitter в режиме реального времени. С его помощью можно наблюдать за лентами новостей, отслеживать хештеги, упоминания и многое другое. X Pro особенно полезен для исследований OSINT, связанных с выявлением тенденций, анализом тональности и сбором актуальной информации.
- **Creepy** (<https://github.com/ilektrojohn/creepy>). Инструмент для поиска геолокаций в рамках исследования OSINT. Он собирает данные о местоположении из социальных сетей и создает карту передвижений человека, опираясь на его цифровой след. Полезно для расследований, в которых нужно анализировать перемещение объекта.

Несмотря на то что перечисленные инструменты обладают огромным потенциалом для OSINT, необходимо использовать их с соблюдением правовых и этических норм. И помните: вместе с развитием цифровой среды эволюционируют и технологии, поэтому специалист по кибербезопасности должен следить за новостями, постоянно учиться и идти в ногу со временем.

Итоги

В этой главе мы уделили особое внимание тому, как важно постоянно развивать свои знания и навыки в области кибербезопасности. Благодаря таким ресурсам, как The Hacker News и Pluralsight, мы можем всегда оставаться в курсе происходящего. Чтобы противостоять новым угрозам, необходимо регулярно обновлять стратегии и обучаться новым методам киберзащиты. Участвуя в вебинарах и общаясь с другими специалистами, вы будете пополнять свой багаж знаний. Помните, что осведомленность и умение адаптироваться — залог личного благополучия и безопасности вашей организации.

Итак, книга подошла к концу, и я надеюсь, что вы поняли всю значимость разведки по открытым источникам. Мы изучили основы, ознакомились с *потрясающим изобилием* полезных инструментов и приемов, поговорили о безопасности и анонимности в Сети. Вы узнали, как OSINT помогает выявлять скрытые угрозы и защищать как вас лично, так и вашу организацию. Благодаря ему вы сможете всегда быть на шаг впереди злоумышленников и бороться за безопасность цифрового пространства. OSINT — незаменимый инструмент для противостояния киберугрозам.