1. Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Институт кибербезопасности и защиты информации

**КУРСОВАЯ РАБОТА**

**OSINT средствами Linux**

по дисциплине «Безопасность операционных систем»

1. Выполнила
2. студентка гр. 4851003/90801 Кулеева А.Г.



1. Руководитель Павленко Е.Ю.
2. к.т.н., доцент

«\_\_» \_\_\_\_\_\_\_\_\_\_ 2022 г.

1. Санкт-Петербург
2. 2022

Содержание

|  |  |  |
| --- | --- | --- |
| Введение............................................................................................................ | | 3 |
| 1 | Основные принципы OSINT.............................................................. | 4 |
| 1.1 | Используемая информация................................................................ | 4 |
| 1.2 | Методы разведки................................................................................ | 5 |
| 1.3 | Инструменты....................................................................................... | 6 |
| 1.3.1 | Доменные имена................................................................................. | 7 |
| 2 | Обзор дистрибутивов......................................................................... | 7 |
| 2.1 | NST....................................................................................................... | 7 |
| 2.2 | Kali....................................................................................................... | 8 |
| 2.3 | DEFT.................................................................................................... | 9 |
| 2.4 | Tsurugi.................................................................................................. | 10 |
| 2.5 | Parrot..................................................................................................... | 10 |
| 2.6 | BlackArch............................................................................................. | 11 |
| 2.7 | BackBox............................................................................................... | 12 |
| 3 | Исследование Kali Linux.................................................................... | 13 |
| 3.1 | Краткий обзор всех средств............................................................... | 13 |
| 3.2 | Средства OSINT.................................................................................. | 22 |
| 3.2.1 | Sherlock................................................................................................ | 22 |
| 3.2.2 | Theharvester......................................................................................... | 23 |
| 3.2.3 | Sublist3r................................................................................................ | 28 |
| 3.2.4 | Spiderfoot............................................................................................. | 30 |
| 3.2.5 | Subfinder............................................................................................... | 31 |
| 3.2.6 | Metagoofil............................................................................................. | 33 |
| 3.2.7 | Dmitriy.................................................................................................. | 33 |
| Заключение........................................................................................................ | | 37 |
| Список использованных источников.............................................................. | | 39 |

Введение

**Актуальность**

OSINT (Open Source INTelligence) — это раз­ведка по откры­тым источни­кам, это методология сбора и анализа данных, находящихся в открытом доступе, для получения дополнительной информации о цели. С развитием интернета фокус внимания аналитиков сместился в киберпространство как один из главных источников информации. В рамках OSINT 90 % информации дает обычное чтение — постов, новостей, комментариев и так далее. Но есть и способы легального расширения информационной воронки. OSINT работает со всеми данными, которые не являются конфиденциальными, не составляют коммерческую или государственную тайну.

**Объект исследования:** OSINT.

**Предмет исследования:** утилиты ОС Linux для осуществления анализа OSINT.

**Цель работы**: провести сравнительный анализ различных утилит OSINT, работающих под управлением ОС Linux.

**Задачи**:

1. Познакомиться с основными принципами разведки по открытым источникам,
2. Рассмотреть несколько дистрибутивов Linux, предоставляющих средства для разведки, и выбрать один для более глубокого исследования,
3. Рассмотреть несколько утилит для OSINT,
4. Выявить их ключевые особенности, преимущества и недостатки.

# Основные принципы Osint

## Используемая информация

С помощью обычного поиска в интернете можно найти и исследовать следующую информацию:

* Метаданные файлов позволяют уточнить дату создания документа, имена пользователей, модели принтеров, ПО, установленное на компьютерах, иногда геолокацию. Зачастую это помогает отличить реальный документ от фейкового;
* Поиск по изображениям позволяет выяснить, действительно ли данное фото относится к этому событию, или это просто взятая из сети картинка;
* Непубличная документация — из-за человеческого фактора множество документов, не предназначенных для всеобщего сведения, находятся в свободном доступе. Например, из-за небрежного хранения в открытых папках в Гугл-документах. Ознакомление с ними в этом случае не нарушает законов;
* Данные о домене — множество отрытых данных, позволяющих уточнить данные об источнике, а также проверить его достоверность. Е-мейлы, телефоны, факсы, технологии, на которых построен сайт, криптографические сертификаты, субдомены;
* Интернет вещей — без всякого взлома, просто через индексацию устройств: сервера, роутеры, камеры видеонаблюдения, веб-камеры, онлайн-накопители и т.д. Это даст техническую информацию, например, запущенные сервисы, провайдера, геолокацию; [3]
* Открытые персональные данные пользователей (username, адреса электронной почты, номера телефонов);
* Пользовательская активность в социальных сетях (посты, комментарии и т.д.);
* Пользовательские запросы в поисковых системах;
* HTML-код сайта. [2]

## Методы разведки

Все методы и инструменты, используемые в разведке по открытым источникам, можно разделить на две категории.

**Пассивные:** позволяют получать общую информацию об объекте. Она собирается вручную или с помощью специальных сервисов и инструментов, упрощающих сбор, систематизацию и анализ данных.К пассивным методам можно отнести:

* сбор информации (в том числе по фотографиям) из открытых поисковых систем;
* анализ пользовательской активности в социальных сетях и блогах, на форумах, иных виртуальных платформах;
* поиск открытых персональных данных пользователей в социальных сетях, мессенджерах;
* просмотр сохраненных копий сайтов в поисковых системах, интернет-архиве;
* получение геолокационных данных с помощью общедоступных ресурсов вроде Google Maps или Яндекс.Карты.

**Активные:** такие методы подразумевают непосредственное влияние аналитика на исследуемый объект, использование специализированных средств получения данных или совершение действий, требующих определенных усилий, например:

* сбор данных на закрытых ресурсах, доступ к которым возможен только по подписке;
* использование сервисов, сканирующих приложения, файлы или сайты на наличие вредоносного кода;
* создание поддельных веб-ресурсов, каналов в мессенджерах, собирающих данные пользователей, конфиденциальные или секретные сведения; [2]
* применение специализированных сервисов и программ, которые активно воздействуют на исследуемый объект: скан портов, перебор директорий, фаззинг параметров, резолвинг большого количества доменных имен на серверах цели и т.д. Такие действия создают много логов в SIEM-системах, триггеров в SOC и могут даже положить несколько серверов. [1]

В логике OSINT пассивные методы, направленные на сбор общей информации из легкодоступных источников, предваряют применение активных способов, предназначенных для сбора конкретных данных об объекте.

## Инструменты

Общедоступных инструментов сотни, платных — десятки, продвинутых, с использованием элементов ИИ и технологий bigdata— единицы (среди них есть как закрытые, так и коммерческие системы). Однако мало кто знает, как много можно найти обычным поиском в Google, используя Dorks— запросы со специальными операторами. Совершенно легальный и бесплатный инструмент, которым надо просто уметь пользоваться.

Приведем несколько примеров специализированных сервисов и ПО, скорее, для того чтобы сориентировать, какие они вообще бывают. Каждая из этих программ имеет множество аналогов.

[*Emailsherlock*](https://www.emailsherlock.com/) — автоматический поиск по *email-*адресу. Найдет, к каким сайтам привязан адрес почты.

[*WhatsMyName*](https://whatsmyname.app/) — сервис поиска никнейма на сайтах, в соцсетях, по тематическим форумам и сайтам знакомств. Люди склонны использовать один ник во многих местах.

[*Email2phonenumber*](https://github__com.teameo.ca/iansangaji/email2phonenumber) — собирает данные со страниц восстановления аккаунта во множестве сервисов и находит номер телефона, что позволяет привязать его к емейлу.

[*Shodan*](https://www.shodan.io/) — поисковик по устройствам, подключенным к сети: интернет вещей, камеры, веб-приложения и так далее.

[*Maltego*](https://www.maltego.com/) — ПО для визуализации данных, собранных при помощи *OSINT*.

[*Foca*](https://github.com/ElevenPaths/FOCA/releases) — программа для извлечения и анализа метаданных с веб-страницы или документа. [3]

### Доменные имена

Самое первое и простое что можно сделать — это решить доменные имена. Для этого есть десятки утилит, как терминальных, так и доступных онлайн. Неполный список таких простейших средств:

* Nslookup (linux\windows nslookup <domain-name>);
* Ping (linux\windows ping <domain-name>);
* Traceroute (linux traceroute <domain-name> \ windows tracert <domain-name>);
* Dig (linux dig @8.8.8.8 <domain-name> ANY);
* Host (linux host <domain-name>);
* getent (linux getent hosts <domain-name>);
* resolveip (linux resolveip -s <domain-name>).

Помимо соответствия IP-домен можно узнать, например, DNS-серверы, с помощью утилиты nslookup, а также можно получить все DNS-записи, например, командой dig. При наличии IP-адресов веб-приложений можно начать смотреть соседние IP-адреса в подсетях, перебирать виртуальные хосты и изучать владельцев этих IP-адресов. DNS-серверы могут в дальнейшем помочь при активной разведке для перебора поддоменов и проведения различных атак. [1]

# Обзор дистрибутивов

Существует множество дистрибутивов для пентеста. Все они преследуют цель дать хакеру удобный и надежный инструмент на все случаи жизни.

## NST

Первый релиз: 2003 год

Основан на: Fedora

Платформы: x64

Графическая оболочка: MATE

NST (Network Security Toolkit) основан на Fedora и предназначен для сетевых атак. В комплекте идет несколько десятков самых важных инструментов, в основном сетевые сканеры, клиенты для всевозможных служб и разного рода перехватчики трафика.

Больше всего можно найти в папке Applications → Internet. Тут есть такие средства, как Angry IP Scanner, Ettercap, и даже OWASP ZAP. Есть неплохой сборник модулей для всевозможного спуффинга и скана пакетов netwag.

## Kali

**Первый релиз:** 2013 год

**Основан на:** Debian

**Платформы:** x86, x64, ARM, VirtualBox

**Графическая оболочка:** Xfce

Kali — один из самых известных дистрибутивов для хакеров. Доступность — несомненный плюс, однако система слегка перегружена набором инструментов, к тому же часть из них из коробки работает не совсем корректно или не работает вообще.

Защиты от случайных ошибок пользователя в Kali тоже не предусмотрено, поэтому не стоит делать эту систему основной. От ядра до оболочки она была создана и оптимизирована для выполнения специализированных задач в области ИБ и плохо пригодна для ежедневной работы. Многие нужные в быту механизмы там попросту отсутствуют, а попытка их установить, скорее всего, вызовет сбои в нормальной работе ОС, если не выведет ее из строя полностью.

Kali предназначена для широкого спектра задач, но основная из них — атаки в сетевой среде, например, поиск уязвимостей в веб-приложениях и получение доступа к беспроводным сетям. Как наследник BackTrack, Kali неплохо приспособлена для работы с беспроводными каналами связи, в особенности Wi-Fi. Проверка на прочность удаленных хостов тоже возможна с помощью утилиты Metasploit, но именно на работу с Wi-Fi ориентировано ядро и значительная часть инструментов.

Также из плюсов стоит отметить наличие в штатной поставке большого количества словарей для различных атак, не только на Wi-Fi, но и на аккаунты в интернете и на сетевые службы.

## DEFT

Первый релиз: 2005 год

Основан на: Ubuntu

Платформы: x86

Графическая оболочка: LXDE

DEFT имеет разнообразные инструменты для разведки и взлома. При этом они вполне гармонично встроены в него. Все вместе напоминает интересный и полезный в жизни швейцарский нож.

Разработан DEFT на платформе [Lubuntu](https://ru.bmstu.wiki/Lubuntu) и снабжен удобным графическим интерфейсом. В продукт входит набор профильных утилит, начиная с антивирусов, систем поиска информации в кеше браузера, сетевых сканеров и заканчивая инструментами, которые необходимы при поиске скрытой информации на диске. При использовании этой ОС не составит труда получить доступ к стертым, зашифрованным или поврежденным данным на различных видах физических носителей.

Изначально этот дистрибутив был предназначен для нужд сетевой полиции и специалистов по реагированию на инциденты в области ИБ, поэтому еще одна сильная сторона DEFT — это конкурентная разведка, в том числе анализ взаимосвязей аккаунтов соцсетей. Есть даже интересная утилита для обнаружения геолокации заданного аккаунта LinkedIn или Twitter.

В отличие от Kali Linux или Tsurugi, в DEFT встроена защита от случайных ошибок пользователя. Без должной подготовки почти ни один инструмент не запустить. Буквально каждое приложение или опция требует прав root.

В итоге эта система хороша для форензики и расследования инцидентов, в особенности если есть физический доступ к носителям информации — будь то диск, флешка или смартфон.

## Tsurugi

Первый релиз: 2018 год

Основан на: Ubuntu

Платформы: x86 (частично), x64

Графическая оболочка: MATE

Tsurugi — детище, рожденное совместными усилиями создателей DEFT и Kali. Предназначен он больше для форензики или OSINT, нежели для пентеста, однако его инструментарий, как и некоторые особенности, позволяют использовать его и в этом направлении. Изначально система поставляется в режиме live-образа, но при желании можно произвести постоянную установку.

В глаза сразу бросается обилие предустановленных инструментов, которые нужны далеко не всегда. При этом интерфейс системы выглядит более чем минималистично и компактно. А вот логика работы системы безопасности, как и работы с вебом или защиты от отслеживания, основана на лучших практиках DEFT.

Весь основной арсенал расположен в Applications → TSURUGI. Здесь и работа с образами, и анализ вредоносного ПО, и восстановление данных, и, как упоминалось, набор утилит для OSINT.

Стоит иметь в виду, что эта ОС, как и Kali, не имеет защиты от случайных ошибок пользователя. Она подойдет тем, кто имеет хорошие навыки работы с Linux и действует предусмотрительно и вдумчиво.

Обширный инструментарий позволяет использовать систему как мультитул для широкого спектра задач. При том что некоторые из утилит так же, как и в Kali, работают некорректно или не работают вообще, процент таких проблемных приложений здесь намного меньше.

## Parrot

Первый релиз: 2013

Основан на: Debian

Платформы: x86, x64, ARM

Графическая оболочка: MATE

Этот красивый дистрибутив разработан специально для тестов безопасности компьютерных систем, поиска и оценки различного ряда уязвимостей. В разделе Application находится довольно интересная утилита Anon Surf. Одна из особенностей Parrot: в ней предустановлены некоторые средства анонимизации, и при выборе Anonsurf Start весь трафик системы будет перенаправлен через Tor. В этом же разделе есть возможность использовать DNS проекта OpenNIC — это вненациональная альтернатива реестрам доменов верхнего уровня. Здесь же при выборе параметра Check IP можно проверить текущий внешний IP.

Второй раздел — Cryptography. Здесь стоит обратить внимание на утилиту GPA — это графический интерфейс программы GnuPG, предназначенной для шифрования информации и создания электронных цифровых подписей. Это, по сути, альтернатива шифрованию PGP. Если необходим именно GPG, то есть утилита zuluCrypt — аналог VeraCrypt, который позволяет шифровать папки, разделы, флешки и прочее.

Следующий раздел — Parrot. В нем собраны утилиты для тестирования защищенности компьютерных систем. Многие из представленных утилит также можно найти в Kali Linux, но есть и некоторые уникальные.

Подробнее хотелось бы остановиться на вкладке «Интернет». Здесь есть предустановленный Tor Browser и биткойн-кошелек Electrum, а также утилита XSSer — фреймворк для обнаружения и эксплуатации XSS-уязвимостей в веб-приложениях. Тут же есть почтовый клиент Claws Mail, это полноценный почтовый клиент с поддержкой шифрования GPG. Бонусом идет Ricochet IM — децентрализованный анонимный мессенджер, работающий через сеть Tor. Как видно, Parrot OS подходит не только для тестов на проникновение, она может и служить ОС для ежедневного пользования.

## BlackArch

Первый релиз: неизвестно

Основан на: Arch

Платформы: x64

Графическая оболочка: отсутствует, есть несколько менеджеров рабочего стола

BlackArch — самый крупный по объему образа дистрибутив. Актуальная версия занимает больше 14 Гбайт! После установки нужно ввести логин и пароль, о которых есть информация на сайте в инструкции по установке. Далее: после логина не видно никаких намеков на меню или что-то в этом роде. Оно вызывается по клику правой кнопкой мыши в любом месте рабочего стола.

Все приложения удобно разложены по категориям в подменю blackarch основного меню. Представлены 49 категорий, в которых есть инструменты на любой случай жизни. Тут представлены все популярные утилиты для взлома, включая такие, как Metasploit и BeEF XSS.

Терминал, как и в целом графическая оболочка системы, выглядит скудно, зато версии ПО актуальные. В итоге, данная ОС подойдет больше для профессионалов и завсегдатаев Linux, новичку здесь разобраться будет крайне тяжело.

## BackBox

Первый релиз: 2010

Основан на: Ubuntu

Платформы: x64

Графическая оболочка: Xfce

BackBox основан на Ubuntu (точнее, Xubuntu), что делает удобным его использование как домашней ОС, к тому же по Ubuntu доступно множество документации и форумов с ответами на распространенные вопросы. Инструментов из коробки поставляется не так и много, всего около 200 штук, но для первых шагов в ИБ вполне достаточно. Отлично подойдет для ежедневного использования. Важный плюс — все инструменты очень удобно сгруппированы в меню. [4]

# Исследование Kali Linux

## Краткий обзор всех средств

Для исследования на практике был выбран дистрибутив Kali Linux, поскольку является наиболее популярным. Как уже говорилось выше, Kali предоставляет широкий спектр средств для разведки, проникновения и не только. Рассмотрим каждое из них.

1. Nmap — это бесплатная утилита с открытым исходным кодом для обнаружения сетей и аудита безопасности.
2. Hydra — это взломщик входа в систему, который поддерживает множество протоколов для атаки. Он очень быстрый и гибкий, а новые модули легко добавлять.
3. metasploit-framework — это платформа с открытым исходным кодом, которая поддерживает исследование уязвимостей, разработку эксплойтов и создание пользовательских инструментов безопасности.
4. Sqlmap — это инструмент тестирования на проникновение с открытым исходным кодом, который автоматизирует процесс обнаружения и использования недостатков SQL-инъекций и захвата серверов баз данных.
5. Gobuster — инструмент, используемый для перебора URI, включая каталоги и файлы, а также поддомены DNS.
6. Wireshark — это передовой и широко используемый в мире анализатор сетевых протоколов.
7. Sherlock — содержит инструмент для поиска имен пользователей в социальных сетях.
8. Cewl — это приложение, которое просматривает заданный URL-адрес с точностью до указанной глубины и возвращает список слов, которые затем могут быть использованы для взломщиков паролей.
9. aircrack-ng — это программа для взлома WEP/WPA стандарта 802.11a/b/g, которая может восстановить 40-битный, 104-битный, 256-битный или 512-битный ключ WEP после сбора достаточного количества зашифрованных пакетов. Также он может атаковать сети WPA1/2 с помощью некоторых продвинутых методов или просто с помощью грубой силы.
10. Wpscan сканирует удаленные установки WordPress для поиска проблем с безопасностью.
11. Dirbuster — приложение, предназначенное для перебора имен каталогов и файлов на серверах веб-приложений.
12. Wifite — это инструмент для аудита беспроводных сетей с шифрованием WEP или WPA.
13. Dirb — это сканер веб-контента. Он ищет существующие (и/или скрытые) Веб-объекты. В основном это работает путем запуска атаки на основе словаря против веб-сервера и анализа ответов.
14. Maltego — это приложение для разведки и криминалистики с открытым исходным кодом, которое предлагает своевременный анализ и сбор информации, а также представление этой информации в удобном для понимания формате.
15. Wordlists — этот пакет содержит rockyou.txt список слов.
16. Ettercap поддерживает активное и пассивное разделение многих протоколов (даже зашифрованных) и включает в себя множество функций для анализа сети и хоста.
17. beef-xss — Browser Exploitation Framework, это инструмент тестирования на проникновение, который фокусируется на веб-браузере.
18. Tcpdump можно использовать для фильтрации пакетов, отслеживания сетевых проблем, обнаружения атак или мониторинга сетевой активности.
19. Subfinder содержит инструмент обнаружения поддоменов, который обнаруживает действительные поддомены для веб-сайтов с помощью пассивных онлайн-источников.
20. Crunch — это генератор списков слов, в котором можно указать стандартный набор символов или любой набор символов, которые будут использоваться при создании списков слов. Списки слов создаются путем комбинирования и перестановки набора символов. Пользователь может определить количество символов и размер списка.
21. Hashcat поддерживает пять уникальных режимов атаки для более чем 300 высокооптимизированных алгоритмов хэширования.
22. Netcat — простая утилита Unix, которая считывает и записывает данные через сетевые подключения с использованием протокола TCP или UDP.
23. Nikto — это подключаемый веб-сервер и CGI-сканер, написанный на Perl, использующий rfp LibWhisker для выполнения быстрых проверок безопасности или информации.
24. Armitage — это инструмент с возможностью написания сценариев для Metasploit, который визуализирует цели, рекомендует эксплойты и предоставляет расширенные возможности фреймворка после эксплуатации.
25. Testdisk — проверяет раздел и загрузочные сектора ваших дисков. Это очень полезно в криминалистике, при восстановлении потерянных разделов.
26. hping3 — это сетевой инструмент, способный отправлять пользовательские пакеты ICMP/UDP/TCP и отображать целевые ответы, как это делает ping с ответами ICMP. Он обрабатывает фрагментацию и произвольный текст пакета и его размер, а также может использоваться для передачи файлов по поддерживаемым протоколам.
27. Goldeneye — это инструмент тестирования HTTP DoS.
28. Powershell — состоит из кроссплатформенной оболочки командной строки и связанного с ней языка сценариев.
29. John — это инструмент, предназначенный для того, чтобы помочь системным администраторам находить слабые (легко угадываемые или взламываемые с помощью грубой силы) пароли и даже автоматически отправлять пользователям сообщения с предупреждением об этом, если это необходимо.
30. Theharvester содержит инструмент для сбора имен поддоменов, адресов электронной почты, виртуальных хостов, открытых портов/баннеров и имен сотрудников из различных общедоступных источников (поисковые системы, серверы ключей pgp).
31. Traceroute отображает маршрут, используемый IP-пакетами на их пути к указанному сетевому (или интернет-) узлу.
32. Whois предоставляет клиент командной строки для протокола WHOIS (RFC 3912), который запрашивает у онлайн-серверов такую информацию, как контактные данные для доменов и назначения IP-адресов.
33. Fcrackzip — это быстрый взломщик паролей, частично написанный на ассемблере.
34. Burpsuite — это интегрированная платформа для проведения тестирования безопасности веб-приложений.
35. Steghide — это программа стеганографии, которая скрывает биты файла данных в некоторых наименее значимых битах другого файла таким образом, что существование файла данных не видно и не может быть доказано.
36. Responder содержит ответчик/MultiRelay, LLMNR, NBT-NS и MDNS-отравитель. Он будет отвечать на конкретные запросы NBT-NS (служба имен NetBIOS) на основе их суффикса имени.
37. recon-ng — это полнофункциональный фреймворк веб-разведки, написанный на Python.
38. Ffuf — это веб-фаззер fest, написанный на Go, который позволяет обнаруживать обычные каталоги, виртуальные хосты (без записей DNS), а также фаззить GET/POST запросы.
39. Autopsy — представляет собой графический интерфейс к инструментам цифрового криминалистического анализа командной строки в наборе Sleuth.
40. Bettercap — это мощный, легко расширяемый и переносимый фреймворк для выполнения разведки и атаки на сети Wi-Fi, устройства с низким энергопотреблением Bluetooth, беспроводные HID устройства и сети Ethernet.
41. Metagoofil — это инструмент сбора информации, предназначенный для извлечения метаданных общедоступных документов (pdf, doc, xls, ppt, docx, pptx, xlsx), принадлежащих целевой компании.
42. Mimikatz — использует права администратора в Windows для отображения паролей пользователей, вошедших в систему в данный момент, в виде открытого текста.
43. Wfuzz — это инструмент, предназначенный для брутфорсинга веб-приложений, его можно использовать для поиска ресурсов.
44. Reaver — выполняет атаку методом перебора на PIN-код защищенной настройки Wi-Fi точки доступа.
45. Lynis — это инструмент аудита для усиления защиты систем на базе GNU/Linux и Unix. Он сканирует конфигурацию системы и создает обзор системной информации и проблем безопасности, который может быть использован профессиональными аудиторами.
46. Amass содержит инструмент, помогающий выполнять сетевое картографирование поверхностей атак и обнаружение внешних активов с использованием методов сбора информации с открытым исходным кодом и активной разведки.
47. Arpwatch поддерживает базу данных MAC-адресов Ethernet, просматриваемых в сети, с соответствующими IP-парами. Оповещает системного администратора по электронной почте, если происходят какие-либо изменения, такие как новая станция/активность, триггеры, измененные и повторно используемые старые адреса.
48. sublist3r содержит средство безопасности Python, предназначенное для перечисления поддоменов веб-сайтов с использованием OSINT.
49. skipfish — это активный инструмент для проверки безопасности веб-приложений.
50. netdiscover — это инструмент активного/пассивного поиска адресов, в основном разработанный для тех беспроводных сетей, в которых нет dhcp-сервера.
51. mdk3 — это инструмент проверки концепции для использования общих недостатков протокола IEEE 802.11 (Wi-Fi).
52. kismet — это детектор беспроводной сети и устройств, сниффер, инструмент для управления охраной и платформа WIDS (wireless intrusion detection).
53. impacket-scripts содержит ссылки на полезные скрипты impacket.
54. dmitry — это приложение командной строки UNIX/(GNU) Linux, написанное на Cи. Дмитрий может находить возможные поддомены, адреса электронной почты, информацию о времени безотказной работы, выполнять сканирование tcp-порта, поиск whois и многое другое.
55. airgeddon — это управляемая меню оболочка сторонних инструментов для аудита беспроводных сетей с множеством функций.
56. scapy — это мощный интерактивный инструмент для обработки пакетов, генератор пакетов, сетевой сканер, анализатор пакетов.
57. legion — инструмент тестирования на проникновение в сеть, который помогает в обнаружении, разведке и эксплуатации информационных систем.
58. impacket — это набор классов Python3, ориентированных на предоставление доступа к сетевым пакетам. Impacket позволяет разработчикам Python3 создавать и декодировать сетевые пакеты простым и последовательным образом.
59. hash-identifier — программное обеспечение для идентификации различных типов хэшей, используемых для шифрования данных и особенно паролей.
60. dsniff содержит несколько инструментов для сниффинга и создания сетевого трафика.
61. dnsmap сканирует домен на наличие общих поддоменов с помощью встроенного или внешнего списка слов.
62. bloodhound использует теорию графов для выявления скрытых и часто непреднамеренных взаимосвязей в среде Active Directory.
63. binwalk — это инструмент для поиска встроенных файлов и исполняемого кода в заданном двоичном изображении.
64. wifiphisher содержит средство безопасности, которое проводит автоматические фишинговые атаки на сети Wi-Fi с целью получения секретных парольных фраз или других учетных данных.
65. sslstrip содержит средство безопасности, которое проводит автоматические фишинговые атаки на сети Wi-Fi с целью получения секретных парольных фраз или других учетных данных.
66. slowhttptest — это легко настраиваемый инструмент, который имитирует некоторые атаки типа "Отказ в обслуживании" на прикладном уровне.
67. rkhunter сканирует системы на наличие известных и неизвестных руткитов, бэкдоров, снифферов и эксплойтов.
68. medusa задумана как быстрое, массово параллельное, модульное средство грубой силы для входа в систему. Цель состоит в том, чтобы поддерживать как можно больше сервисов, которые позволяют удаленную аутентификацию, насколько это возможно.
69. fierce — сканер, который помогает находить несмежные IP-адреса и имена хостов в указанных доменах.
70. crackmapexec — многофункциональное средство пентестинга сред Windows/Active Directory.
71. commix — [comm]and [i]njection e[x]ploiter.
72. chntpw предоставляет способ просмотра информации и изменения пользовательских паролей в файле базы данных пользователей Windows NT/ 2000.
73. arp-scan — это инструмент командной строки, который использует протокол ARP для обнаружения и снятия отпечатков пальцев с IP-хостов в локальной сети.
74. xsser — это автоматический фреймворк для обнаружения, использования уязвимостей XSS в веб-приложениях и сообщения о них.
75. spiderfoot автоматизирует процесс сбора информации о заданной цели, которая может быть IP-адресом, доменным именем, именем хоста, сетевой подсетью, ASN, адресом электронной почты или именем человека.
76. parsero считывает Robots.txt файл веб-сервера и просматривает запрещенные записи. Запрещенные записи сообщают поисковым системам, какие каталоги или файлы, размещенные на веб-сервере, не должны индексироваться.
77. nuclei содержит быстрый инструмент для настраиваемого целевого сканирования на основе шаблонов, предлагающий огромную расширяемость и простоту использования.
78. ghidra содержит платформу обратного проектирования программного обеспечения (SRE).
79. foremost — это основанная на форензиках программа для восстановления потерянных файлов на основе их верхних и нижних колонтитулов и внутренних структур данных.
80. dnsrecon — анализатор сети по DNS.
81. Dirsearch содержит инструмент командной строки, предназначенный для перебора каталогов и файлов на веб-серверах.
82. capstone — инструмент командной строки для разбора шестнадцатеричных строк.
83. bed — это программа, которая предназначена для проверки демонов на предмет возможного переполнения буфера, форматирования строк и т.д.
84. whatweb идентифицирует веб-сайты. Он распознает веб-технологии, включая системы управления контентом (CMS), платформы для ведения блогов, пакеты статистики/аналитики, библиотеки JavaScript, веб-серверы и встроенные устройства.
85. shellter — это инструмент для динамического внедрения шелл-кода, он же dynamic PE infector.
86. Rainbowcrack взламывает хэши с помощью радужных таблиц.
87. maryam — OWASP Maryam модульная платформа, основанная на OSINT и сборе данных.
88. macchanger — это утилита, которая упрощает манипулирование MAC-адресами сетевых интерфейсов.
89. jsql — это легкое приложение, используемое для поиска информации в базе данных с удаленного сервера.
90. hakrawler — быстрый веб-сканер golang для сбора URL-адресов и расположения файлов JavaSript.
91. dnsenum — это многопоточный perl-скрипт для перечисления DNS-информации домена и обнаружения несмежных ip-блоков.
92. chisel содержит быстрый туннель TCP/UDP, передаваемый по протоколу HTTP, защищенный через SSH.
93. arjun — содержит инструменты для поиска параметров запроса для конечных точек URL.
94. android-sdk — Android SDK предоставляет вам библиотеки API и инструменты разработчика, необходимые для создания, тестирования и отладки приложений для Android.
95. amap — инструмент сканирования нового поколения для пентестеров. Он пытается идентифицировать приложения, даже если они запущены на другом порту.
96. wafw00f — идентифицирует и снимает отпечатки пальцев с продуктов брандмауэра веб-приложений (WAF).
97. veil — это инструмент, предназначенный для создания полезных нагрузок metasploit, которые обходят обычные антивирусные решения.
98. sslyze может анализировать конфигурацию SSL сервера, подключаясь к нему.
99. sslscan запрашивает службы SSL, такие как HTTPS, чтобы определить поддерживаемые шифры.
100. set — Social-Engineer Toolkit, предназначен для тестирования на проникновение в области социальной инженерии. [5]

## Средства OSINT

### Sherlock

На целевую машину была установлена данная утилита, по неизвестным причинам, её не было в системе заранее. Рассмотрим подробнее некоторые функции данной утилиты (Рисунок 1).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 1 — Опции утилиты

Обязательным аргументом является имя пользователя, по которому будет совершаться поиск. Можно ввести сразу несколько имён. Сохранить результаты можно в специальную папку или файл, также поддерживается создание файлов CSV, Excel и json. Возможен поиск через Tor браузер, ограничение поиска по указанным сайтам, с использованием proxy. [6]

В качестве имени пользователя было выбрано собственное имя, которое используется в некоторых аккаунтах в соцсетях. Данная утилита ищет по конечной строке, а не по подстроке. Таким образом, при вводе имени heatherhoney были исключены результаты, содержащие различные вариации, например: \_heatherhoney\_, heatherhoneyy, heatherhoney.y.y и им подобные: которые повторяют первую или последнюю букву, содержат точки и нижние подчеркивания. Соответственно, чтобы понизить свою узнаваемость, лучше использовать несколько видоизменённые никнеймы в различных соцсетях.

На Рисунке 2 можно наблюдать мой Telegram, но Instagram отсутствует, хотя в нем такой же ник. Также нет результатов с адресами почт. Например, при нахождении Google почты можно узнать имя от аккаунта Google в целом, а отсюда раскрывается большое множество сайтов, поскольку очень много где можно войти под учетной записью Google.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 2 — Результат поиска аккаунтов

Также можно отметить, что без указания выходного файла, он все равно создается. А с указанием выходного файла, все равно происходит печать в консоль. Также по умолчанию используется аргумент --print-found, который выводит информацию только о найденных аккаунтах. Флаг --print-all выводит информацию обо всех сайтах, даже если они не дали результата.

### Theharvester

Он выполняет сбор данных с целью определения  
ландшафта внешних угроз домена. Выполняет как пассивную, так и активную разведку. Пассивная разведка включает в себя поиск в нескольких специализированных поисковых системах, а также разведку на сайтах (например, github). Список всех этих ресурсов внушителен. Активная разведка включает DNS brute force, то есть перебор доменов по словарю. [7]

Поиск осуществляется по домену. Из дополнительных функций: можно использовать proxy, делать скриншоты найденных доменов, искать по виртуальным хостам, проводить проверку takeover.

Поддерживается поиск в Shodan. Это поисковая система, позволяющая пользователям искать различные типы серверов, подключённых к сети Интернет, с использованием различных фильтров. Её также описывают как поисковую систему сервисных баннеров, представляющие собой метаданные, которые сервер отправляет обратно клиенту. Этими метаданными могут быть информация о серверном программном обеспечении, какие опции поддерживает сервис, приветственное сообщение или что-то ещё, что клиент должен выяснить перед взаимодействием с сервером. [8] С помощью такого поиска можно проникнуть в чужую сеть как на предприятии, так и в умном доме и нанести значительный ущерб.

В качестве ресурса для поиска можно указать: anubis, baidu, bevigil, binaryedge, bing, bingapi, bufferoverun, censys, certspotter, crtsh, dnsdumpster, duckduckgo, fullhunt, github-code, hackertarget, hunter, intelx, omnisint, otx, pentesttools, projectdiscovery, qwant, rapiddns, rocketreach, securityTrails, sublist3r, threatcrowd, threatminer, urlscan, virustotal, yahoo, zoomeye

На Рисунке 3 представлены все функции утилиты.

В качестве исследуемого домена был выбран neobit.ru. Во-первых, это не такой большой и популярный сайт, поэтому его анализ будет быстрее. Во-вторых, сервера географически находятся в России, поэтому было интересно проверить, насколько адекватными будут результаты.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3 — Опции утилиты

В результате тестирования выяснилось, что без указания ресурса ничего работать не будет. Следовательно, нужно все ресурсы перебирать вручную. На Рисунках 4-5 представлены запросы к некоторым ресурсам.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 4 — Результат поиска домена через bing

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 5 — Результат поиска домена через otx

При этом для некоторых ресурсов требуются API ключи (Рисунок 6).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 6 — Результат поиска домена через github

Также при использовании флагов brute-force, lookup тоже требуется ресурс поиска. Результат вывода с этими флагами представлен на Рисунках 6 и 7 соответственно.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 7 — Результат брут-форса домена

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 8 — Результат запроса lookup домена

### Sublist3r

Этот пакет содержит средство безопасности Python, предназначенное для перечисления поддоменов веб-сайтов с использованием OSINT. Это помогает пентерстерам и охотникам за ошибками собирать поддомены для домена, на который они ориентируются по сети. Sublist3r перечисляет поддомены с помощью многих поисковых систем, таких как Google, Yahoo, Bing, Baidu и Ask. Sublist3r также перечисляет поддомены, используя Netcraft, Virustotal, ThreatCrowd, DNSdumpster и ReverseDNS. Имеется опция брутфорса, которая увеличивает возможность поиска большего количества поддоменов с помощью грубой силы с улучшенным списком слов.

Данное средство также не было предустановлено в систему. На Рисунке 1 представлены все его функции.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 9 — Опции утилиты

По итогу с этой утилитой ничего не удалось выяснить. В самом начале исследования запросы были заблокированы ресурсом Virustotal, а через несколько попыток ещё и Google (Рисунок 10).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 10 — Попытка запуска утилиты

Далее было принято решение искать только на одном ресурсе и в качестве цели выбрать такой домен, который точно должен выдать ответ. В качестве такой цели был выбран google.com. К сожалению, это тоже не принесло никаких плодов (Рисунок 11).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 11 — Попытка запуска утилиты с новыми аргументами

### Spiderfoot

С помощью данной утилиты можно анализировать не только сети, но и получать информацию об адресах почты и людях. Утилита предоставляет достаточно обширный функционал для исследования (Рисунок 12).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 12 — Опции утилиты

Данное средство разработано не совсем удачно. Во-первых, при поиске по умолчанию логируется процесс работы, из-за чего данные теряются. Во-вторых, при работе необходимо указывать конкретный модуль. По умолчанию выводятся все модули подряд и опять в выводе ничего невозможно разобрать. Один из модулей вообще начал парсить весь сайт. Тем не менее, на Рисунках 13-14 представлен вывод некоторых модулей.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 13 — Результат вывода

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 14 — Результат вывода

### Subfinder

Создан исключительно для обнаружения поддоменов. Оптимизирован по скорости и памяти. Все флаги данной утилиты в основном форматируют вывод, указывают тип файла, указывают параметры вывода (например, можно убрать маски и мертвые поддомены). На Рисунке 15 представлены все опции средства. На Рисунке 16 — результаты запроса. На Рисунке 17 — используемые для поиска ресурсы. В отличие от theharvester, в выводе отсутствуют ip-адреса.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 15 — Опции утилиты

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 16 — Результат поиска поддоменов

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 17 — Используемые ресурсы

### Metagoofil

Утилита выполняет поиск в Google определенных типов файлов, публично размещенных на веб-сайте, и при необходимости загружает локальную копию. Это полезно для сбора разведданных с открытым исходным кодом, тестов на проникновение или определения того, какие файлы организация передает поисковым индексаторам, таким как Google.

При работе возможно получение ошибки HTTP 429: Google определил вас как бота и заблокировал IP на определенный период времени. Одним из решений является использование прокси-цепочек и банка прокси-серверов для циклического поиска. На Рисунке 18 представлены все функции средства. На Рисунке 19 показан результат работы: файлы скачиваются.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 18 — Опции утилиты

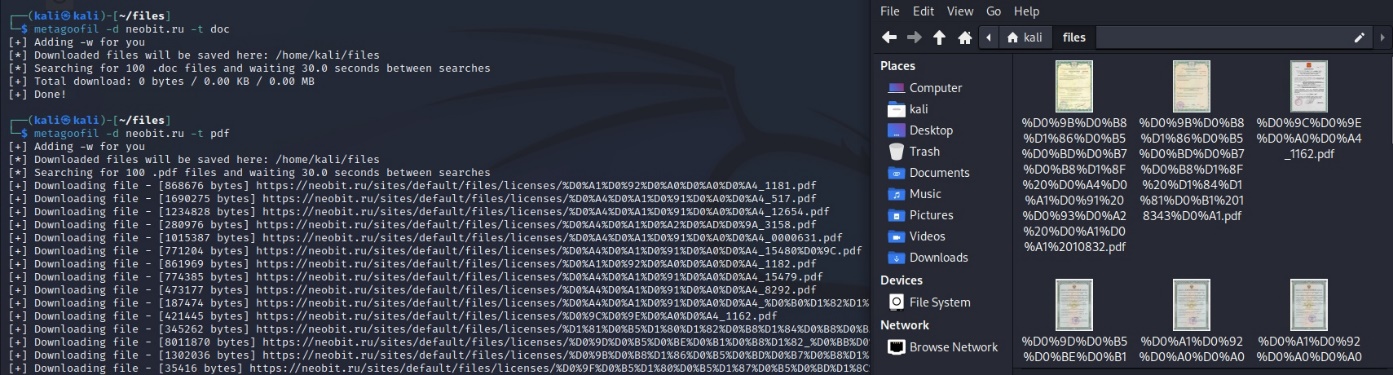


Рисунок 19 — Результат работы

### Dmitry

Утилита может находить возможные поддомены, адреса электронной почты, выполнять поиск whois по ip и по домену. При сканировании tcp-порта можно проверить фильтрацию пакетов и просмотреть баннерные сообщения. Также доступен запрос к Netcraft.com. Компания Netcraft предоставляет анализ веб-серверов и веб-хостингов, включая анализ с каких операционных систем и браузеров был посещён сайт. На Рисунке 20 показаны все функции.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 20 — Опции утилиты

Без указания параметров будут выполняться сразу все по умолчанию. На Рисунках 21-22 показан вывод whois. На Рисунке 23 происходит поиск поддоменов и почтовых адресов. На Рисунке 24 показано сканирование портов.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 21 — Вывод whois

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 22 — Вывод whois

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 23 — Поиск поддоменов и почтовых адресов

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 24 — Сканирование портов

Заключение

В ходе выполнения данной курсовой работы были получены знания об основных принципах разведки по открытым источникам, о методах и инструментах разведки. Было рассмотрено несколько дистрибутивов Linux, созданных специально для задач информационной безопасности. Определить их удобство объективно невозможно, но можно провести небольшой сравнительный анализ. Для профессионалов больше подойдут BlackArch, Kali и Tsurugi, поскольку в них нет защиты от непреднамеренных ошибок слабо подготовленного пользователя. Для новичков больше подойдет DEFT, поскольку он имеет более user-friendly интерфейс и есть вышеупомянутая защита. Практически все дистрибутивы дают обширное поле для работы с сетями. В Kali также есть средства разведки. В Tsurugi работа с сетями больше подразумевают анонимизацию, что помогает в разведке и пентестинге. Но в основном данная ОС нацелена на поиск и эксплуатацию уязвимостей. DEFT в свою очередь полностью направлен на OSINT и криминалистику, что делает его более пригодным для данного исследования.

Однако выбор был сделан всё же в пользу Kali Linux, поскольку данная система является наиболее популярной среди хакеров. Всего для исследования было выбрано 7 утилит, однако их на самом деле больше, также средства можно использовать в совокупности. Из всех утилит для получения информации о конкретном человеке можно использовать только Sherlock. Она справилась со своей работой отлично, однако можно было бы добавить такую модификацию, как поиск не по строке, а по подстроке, чтобы получить больший охват вариаций имен пользователей. Также было бы эффективнее добавить поиск возможных email адресов и аккаунта в Instagram. Эти данные позволили бы найти намного больше информации.

Также можно выделить отдельно Metagoofil, которая находит и скачивает файлы различных форматов на локальную машину. Она сработала корректно, никаких замечаний по поводу неё нет.

Все остальные утилиты направлены в основном на поиск поддоменов. Наиболее полную информацию выдала утилита Dmitriy. Ни одна другая утилита не нашла юридический адрес и номер телефона искомой компании. Также хорошо себя показал Subfinder: он хорошо находит поддомены, однако не указывает соответствующие им ip-адреса. В целом он дает информацию только по доменам и ничего больше. Среди фаворитов также Theharvester. Он выдает всю требуемую пользователем информацию корректно. Единственный недостаток — нельзя перебрать все источники сразу, их нужно указывать в явном виде каждый отдельно, что тратит больше времени разведчика. Среди аутсайдеров находятся Spiderfoot и Sublist3r. Первый достаточно сложен в использовании для новичка. Чтобы разобраться с данной утилитой как следует, обязательно придется читать документацию, а все вышеописанные утилиты можно было легко использовать с опорой только на -help. Однако, если вникнуть в суть каждого модуля, то Spiderfoot может выдать очень много полезной информации о цели. Sublist3r же не выдал совсем ничего, поскольку сервера некоторых источников его забанили, а другие сервера в принципе не дали никакого ответа.

В итоге можно сделать вывод о том, что утилит для OSINT, как в Kali, так и у других дистрибутивах достаточно много, причем все они предоставляют самый различный функционал.

Список использованных источников

1. OSINT или разведка по открытым источникам [Электронный ресурс]. URL: <https://habr.com/ru/company/deiteriylab/blog/595801/>. — (дата обращения: 9.12.2022).
2. OSINT [Электронный ресурс]. URL: <https://blog.skillfactory.ru/glossary/osint/>. — (дата обращения: 9.12.2022)
3. OSINT — курс домашней разведки для чайников [Электронный ресурс]. URL: <https://dzen.ru/a/YmwRuZjxJT9UdUxx>. – (дата обращения: 9.12.2022).
4. Боевой Linux. Обзор самых мощных дистрибутивов для пентестов и OSINT [Электронный ресурс]. URL: <https://xakep.ru/2020/07/29/pentest-distros/>. – (дата обращения: 9.12.2022).
5. Kali Tools. Tool Documentation [Электронный ресурс]. URL: <https://www.kali.org/tools/>. – (дата обращения: 10.12.2022).
6. Sherlock [Электронный ресурс]. URL: <https://github.com/sherlock-project/sherlock>. – (дата обращения: 10.12.2022).
7. Theharvester [Электронный ресурс]. URL: <https://github.com/laramies/theHarvester>. – (дата обращения: 10.12.2022).
8. Shodan [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/Shodan_(сайт)> . – (дата обращения: 10.12.2022).