# Лабораторная работа №1\_Отчет.

# Сбор информации, разведка и OSINT

**Предусловие:** Каждый студент должен выбрать компанию из списка со своей инфраструктурой. Эта компания будет использоваться в качестве цели во время нескольких лабораторных работ.

Для выполнения работ рекомендуется установить программу виртуализации для операционных систем VirtualBox [1] https://www.virtualbox.org/wiki/Downloads, на которую рекомендуется установить дистрибутив Kali Linux [2] https://www.kali.org/get -kali/#kali-virtual-machines – это Linux дистрибутив, созданный на основе Debian с открытым исходным кодом, предназначенный для решения различных задач информационной безопасности, таких как тестирование на проникновение, исследование безопасности и компьютерная криминалистика.

**На установленной машине Kali Linux необходимо:**

1. Переименовать машину Kali на свою фамилию.
2. Создать пользователя со своей фамилией
3. Предоставить созданному пользователю права администратора

**Все дальнейшие задания выполняются от имени нового пользователя!!!**

|  |  |  |
| --- | --- | --- |
| **Название VM** | **Имя пользователя** | **Сайт и описание компании** |
| **ivanov** | **ivanov** | **<https://gorod55.ru> новостной сайт г. Омска** |

## ****Упражнение 1. Получение информации о домене/IP с помощью утилиты whois и сервиса whois****

### **Цель**:

понять какую информацию предоставляет утилита whois

**После окончания работы студент должен**

* знать: как работает утилита whois, какие домены и IP-блоки делегируются клиентам
* уметь: получать всю информацию от утилиты whois.

### Задание:

* собрать информацию о домене выбранной компании с помощью команды whois
* собрать информацию о домене выбранной компании с помощью веб-сервиса whois

### Технические инструменты для выполнения работы

* командная консоль
  + утилита whois
* веб-браузер

### Ссылки

* <https://en.wikipedia.org/wiki/WHOIS>

### ЗАДАНИЕ 1

Получить всю информацию о выбранном домене с помощью команды whois (доказать с помощью снимка экрана). Когда зарегистрировали/изменили домен? Кто владелец домена? Какие отличия между административными, техническими и другими контактами? Объясните.

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 2

Получить всю информацию о выбранном домене с помощью веб-службы whois (доказать с помощью снимка экрана).

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 3

Есть ли отличия между полученными результатами?

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 4

Что такое диапазон сети? Кто региональный регистратор? (доказать с помощью скриншотов)

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 5

Что такое серверы NS?

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## ****Упражнение 2. Получить общую информацию о выбранном домене с помощью службы DNS****

### Цель:

Понять основное предназначение DNS

**После окончания работы студент должен**

* знать: как работает DNS, как работают разные типы записей DNS
* уметь: получать всю информацию о доменных записях от DNS.

### Задание:

* получить общие записи DNS (A, AAAA, NS, MX, SPF, PTR) о домене, выбранной компании с помощью команды dig.
* получить общие записи DNS (A, AAAA, NS, MX, SPF, PTR) о домене выбранной компании с помощью веб-сервисов.

### Технические инструменты для выполнения работы

* командная консоль
  + утилита dig
* веб-браузер
  + <https://bgp.he.net/>
  + <https://mxtoolbox.com/>

### Ссылки

* <https://en.wikipedia.org/wiki/Domain_Name_System>
* <https://en.wikipedia.org/wiki/Reverse_DNS_lookup>
* <https://ru.wikipedia.org/wiki/Dig>

### ЗАДАНИЕ 1

Получите всю информацию о выбранном домене с помощью утилиты dig (доказать с помощью снимка экрана). Какие записи доступны (A, AAAA, NS, MX, SPF, PTR)? На что указывают эти записи? Объясните.

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 2

Получить записи PTR для полученных IP-адресов из записей NS/MX/A (не более 5) (доказать с помощью снимка экрана). Есть ли отличия от А записей? Объясните.

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 3

Проверить записи SPF выбранного домена/субдомена с помощью MxToolbox (доказать с помощью снимка экрана)? Объясните результаты.

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 4

Есть ли информация об AS компании? (доказать с помощью скриншотов). Что это значит?

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## ****Упражнение 3. Получите общую информацию о целевой AS****

### Цель:

Понять назначение протокола BGP

**После окончания работы студент должен**

* знать: что такое AS, как AS передает трафик
* уметь: получать информацию, связанную с AS (номер, подблоки, соединение, маршруты)

### Задание:

* получить информацию об AS целевой компании с помощью https://bgp.he.net/
* получить изменения в маршрутизации BGP в выбранную AS

### Технические инструменты для выполнения работы

* командная консоль
  + утилита traceroute
* веб-браузер
  + <https://bgp.he.net/>
  + <http://www.routeviews.org/routeviews/>
  + <https://stat.ripe.net/widget/bgplay>

### Ссылки

* <https://en.wikipedia.org/wiki/Border_Gateway_Protocol>

### ЗАДАНИЕ 1

Получить всю информацию об AS с помощью bgp.he.net (доказать с помощью снимка экрана). Что такое номер AS? Какие подблоки делегированы данной AS?

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 2

Есть какие-то другие AS, которые объявляют тот же подблок? Это верно?

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 3

Сколько соединений имеет текущее AS? (доказать с помощью скриншота).

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 4

Каков основной путь между целевой AS и вами? Докажите это с помощью команды traceroute и снимка экрана и результата анализа отношений IP-AS.

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## ****Упражнение 4. OSINT с помощью Shodan****

### Цель:

понять назначение Shodan

**После окончания работы студент должен**

* знать: как работает сервис Shodan

### Задание:

* подтвердить, указать и расширить информацию с предыдущих шагов с помощью сервиса Shodan.

### Технические инструменты для выполнения работы

* веб-браузер
  + <https://www.shodan.io/>

**ЗАДАНИЕ 1**

Какую информацию вы смогли получить из Shodan? (покажите с помощью скриншотов)

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ЗАДАНИЕ 2**

Есть ли дополнительная информация об изучаемой цели? (покажите с помощью скриншотов)

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## ****Упражнение 5. Автоматизируйте OSINT с помощью Maltego и FOCA****

### Цель:

понять возможности Maltego и Foca

**После окончания работы студент должен**

* знать: как работает Maltego
* знать: как работает Foca

### Задание:

* получить всю информацию из предыдущих шагов используя Maltego

### Технические инструменты для выполнения работы

* + Maltego
  + FOCA

### ЗАДАНИЕ 1

Какую информацию вы смогли получить с помощью Maltego? (доказать с помощью скриншотов)

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 2

Есть ли отличия от автоматизированного и ручного сбора данных? (доказать с помощью скриншотов) Объясните.

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 3

Загрузить и извлечь метаданные из файлов, полученных из целевого домена/субдоменов компании с помощью FOCA? (доказать с помощью скриншотов) Объясните.

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 4

Есть ли какие-либо имена пользователей/электронные письма? (доказать с помощью скриншотов)

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## ****Упражнение 6. Проверка учетных данных с помощью Pastebin и Haveibeenpwned****

### Цель:

Понять для чего предназначены сервисы **Pastebin и Haveibeenpwned**

**После окончания работы студент должен**

* знать: как проверить учетные данные в общедоступных базах данных

### Задание:

* проверить все учетные данные из предыдущих шагов по предоставленным ресурсам

### Технические инструменты для выполнения работы

* <https://haveibeenpwned.com/>
* <https://pastebin.com/>

### ЗАДАНИЕ 1

Проверить электронные ящики с помощью Haveibeenpwned? (Предоставьте результаты с помощью скриншотов). Что-то интересное?

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ЗАДАНИЕ 2

Проверить электронные ящики, домены и IP-адреса с помощью Pastebin? (Предоставьте результаты с помощью скриншотов). Что-то интересное?

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_