

Лабораторная работа №1

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.

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>

Порядок выполнения работы

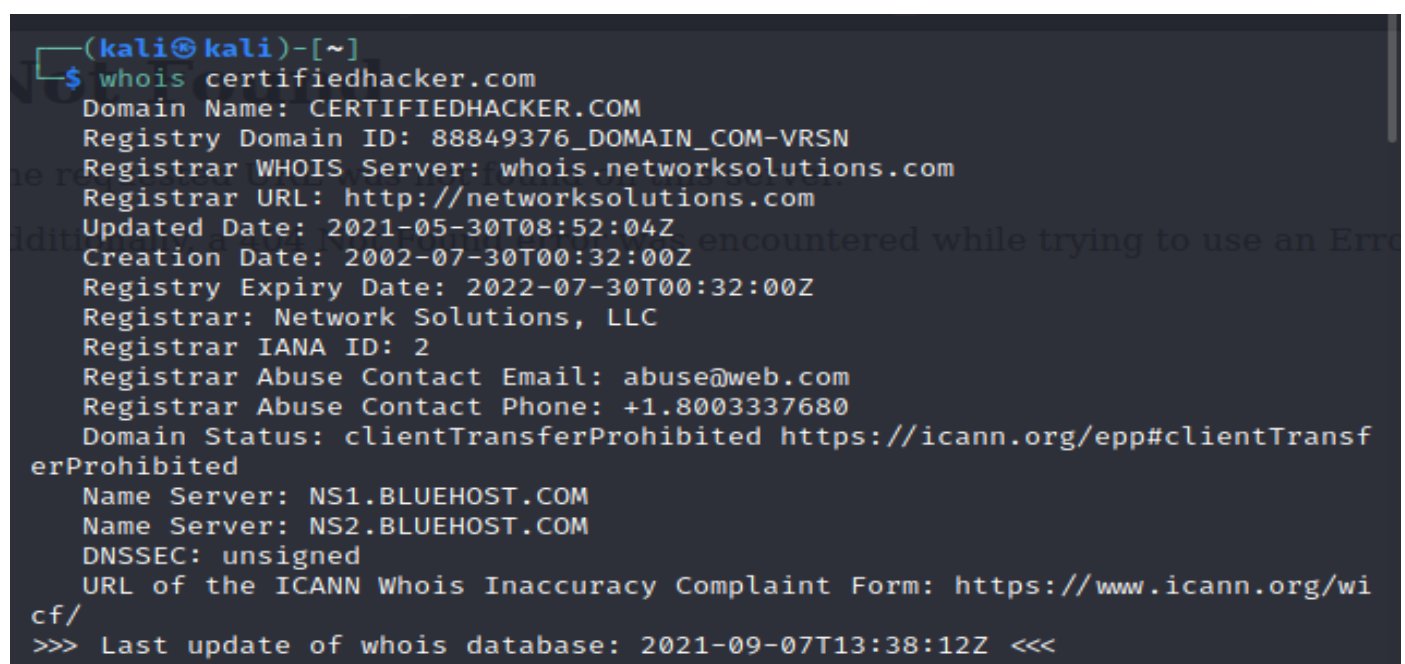
Использование команды whois в системе Kali Linux выглядит следующим образом:

whois <IP-адрес / имя веб-сайта, о котором вы хотите получить информацию>

Например: whois 162.241.216.11 или whois certifiedhacker.com

Команда whois Kali Linux ведет себя по-разному для IP-адреса и имени сайта.

Набрав whois-help, вы получите дополнительную информацию о команде.



```
(kali@kali)-[~]
$ whois certifiedhacker.com
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2021-05-30T08:52:04Z
Creation Date: 2002-07-30T00:32:00Z
Registry Expiry Date: 2022-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransf
erProhibited
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wi
cf/
>>> Last update of whois database: 2021-09-07T13:38:12Z <<<
```

Рисунок 1 Результат работы утилиты whois дистрибутива Kali Linux.

[←](#)
[→](#)
[🏠](#)
[🔒](#)
[who.is/whois/certifiedhacker.com](#)
🔍
☆
🔖
👤

who.is

🔍

[Premium Domains](#)
[Transfer](#)
[Features](#)
[Login](#)
[Sign Up](#)

Registrar Info

Name	Network Solutions, LLC
Whois Server	whois.networksolutions.com
Referral URL	http://networksolutions.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates

Expires On	2022-07-30
Registered On	2002-07-30
Updated On	2021-08-22

Name Servers

NS1.BLUEHOST.COM	162.159.24.80
NS2.BLUEHOST.COM	162.159.25.175

Similar Domains

[certi-5oils.com](#) | [certi-air.eu](#) | [certi-api.org](#) | [certi-box.com](#) | [certi-bru.com](#) | [certi-bruxelles.net](#) | [certi-buy.com](#) | [certi-cable-1.com](#) | [certi-call.com](#) | [certi-camp.com](#) | [certi-camp.net](#) | [certi-car.com](#) | [certi-car.net](#) | [certi-care.com](#) | [certi-cares.com](#) | [certi-cars.com](#) | [certi-cast.com](#) | [certi-chain.com](#) | [certi-chef.com](#) | [certi-clean.com](#) |

Registrar Data

We will display stored WHOIS data for up to 30 days.
 [🔄 refresh](#)

[🔒 Make Private Now](#)

Registrant Contact Information:

Name	PERFECT PRIVACY, LLC
Organization	
Address	5335 Gate Parkway care of Network Solutions PO Box 459
City	Jacksonville
State / Province	FL
Postal Code	32256
Country	US
Phone	+1.5707088780
Email	kr3jq42x9hb@networksolutionsprivateregistration.com

Administrative Contact Information:

Name	PERFECT PRIVACY, LLC
Organization	
Address	5335 Gate Parkway care of Network Solutions PO Box 459
City	Jacksonville
State / Province	FL
Postal Code	32256
Country	US
Phone	+1.5707088780
Email	kr3jq42x9hb@networksolutionsprivateregistration.com

Technical Contact Information:

Name	PERFECT PRIVACY, LLC
Organization	
Address	5335 Gate Parkway care of Network Solutions PO Box 459
City	Jacksonville
State / Province	FL
Postal Code	32256
Country	US
Phone	+1.5707088780
Email	kr3jq42x9hb@networksolutionsprivateregistration.com

Information Updated: 2021-09-04 14:30:05

Рисунок 2 Результат работы утилиты whois веб-сервиса <https://who.is/>

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>

Порядок выполнения работы

Использование утилиты **dig** в системе Kali Linux выглядит следующим образом:

dig [server] [name] [type] где:

[server] – это доменное имя или IP-адрес сервера.

[name] – это имя записи ресурса, которую следует искать.

[type] – указывает, какой тип запроса нужен – любой, A, MX, SIG.

Набрав **dig -h**, вы получите дополнительную информацию об утилите.

Обратите внимание

если аргумент типа не указан, выполняется поиск только для записи A.

```
(kali@kali)-[~]
$ dig certifiedhacker.com

; <<>> DiG 9.16.15-Debian <<>> certifiedhacker.com
;; global options: +cmd
;; Got answer: handle the request.
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 30887
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 4096
;; QUESTION SECTION:
;certifiedhacker.com.          IN      A

;; ANSWER SECTION:
certifiedhacker.com.  7922    IN      A      162.241.216.11

;; AUTHORITY SECTION:
certifiedhacker.com.  87541   IN      NS      ns1.bluehost.com.
certifiedhacker.com.  87541   IN      NS      ns2.bluehost.com.

;; ADDITIONAL SECTION:
ns1.bluehost.com.    69485   IN      A      162.159.24.80
ns2.bluehost.com.    69485   IN      A      162.159.25.175

;; Query time: 4 msec
;; SERVER: 95.158.0.1#53(95.158.0.1)
;; WHEN: Tue Sep 07 11:02:53 EDT 2021
;; MSG SIZE rcvd: 141
```

Рисунок 3 Результат работы утилиты dig дистрибутива Kali Linux.

Получение информации о выбранном домене с помощью сервиса <https://bgp.he.net/>

The screenshot shows the Hurricane Electric Internet Services website. At the top, there is a logo with the letters 'HE' inside a circle, followed by the text 'HURRICANE ELECTRIC INTERNET SERVICES'. Below this, the domain 'certifiedhacker.com' is entered into a search bar. The search results are displayed under the 'DNS Info' tab. The results are organized into sections: 'Start of Authority' (mname: ns1.bluehost.com, serial: 2018011205, refresh: 86400, retry: 7200, expire: 3600000), 'Nameservers' (ns1.bluehost.com, ns2.bluehost.com), 'Mail Exchangers' (mail.certifiedhacker.com(0)), 'TXT Records' (v=spf1 a mx ptr include:bluehost.com ?all), and 'A Records' (162.241.216.11). On the left side, there is a 'Quick Links' menu with various links like 'BGP Toolkit Home', 'BGP Prefix Report', etc. At the bottom, there are social media icons for Twitter and Facebook, and a footer with the text 'Updated 08 Sep 2021 13:57 PST © 2021 Hurricane Electric'.

Рисунок 4 Результат работы сервиса <https://bgp.he.net/>.

Получение информации о выбранном домене с помощью <https://mxtoolbox.com/>.

The screenshot shows the MXToolbox SuperTool interface. At the top, there's a navigation bar with links like Pricing, Tools, Delivery Center, Monitoring, Products, Support, and Login. Below this, a dark header contains various tool categories: SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, and Analyze Headers. The main content area displays the results for a DNS lookup on 'mx:certifiedhacker.com'. It includes a table with columns for Pref, Hostname, IP Address, and TTL. Below this, there's a table with Test and Result columns, showing three tests: DMARC Record Published (No DMARC Record found), DMARC Policy Not Enabled (DMARC Quarantine/Reject policy not enabled), and DNS Record Published (DNS Record found). On the right side, there's a sidebar with various services offered, including Free MxToolBox Account, Delivery Center, Blacklist Monitoring, MailFlow Monitoring, and Bulk Lookup.

Pref	Hostname	IP Address	TTL
0	mail.certifiedhacker.com	162.241.216.11 Oso Grande IP Services, LLC (AS26337)	4 hrs

Test	Result
DMARC Record Published	No DMARC Record found
DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
DNS Record Published	DNS Record found

Рисунок 4 Результат работы сервиса <https://mxtoolbox.com/>.

ЗАДАНИЕ 1

Получите всю информацию о выбранном домене с помощью утилиты **dig** (доказать с помощью снимка экрана). Какие записи доступны (MX/A/AAAA/NS)? 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 A 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

Порядок выполнения работы

Получение информации о выбранном домене с помощью сервиса <https://bgp.he.net/>



Quick Links

[BGP Toolkit Home](#)
[BGP Prefix Report](#)
[BGP Peer Report](#)
[Exchange Report](#)
[Bogon Routes](#)
[World Report](#)
[Multi Origin Routes](#)
[DNS Report](#)
[Top Host Report](#)
[Internet Statistics](#)
[Looking Glass](#)
[Network Tools App](#)
[Free IPv6 Tunnel](#)
[IPv6 Certification](#)
[IPv6 Progress](#)
[Going Native](#)
[Contact Us](#)



DNS Info Website Info IP Info

Start of Authority

mname: ns1.bluehost.com rname: dnsadmin.box5331.bluehost.com
serial: 2018011205
refresh: 86400 retry: 7200
expire: 3600000 minimum: 300

Nameservers

ns1.bluehost.com, ns2.bluehost.com

Mail Exchangers

mail.certifiedhacker.com(0)

TXT Records

v=spf1 a mx ptr include:bluehost.com ?all

A Records

162.241.216.11

Updated 08 Sep 2021 13:57 PST © 2021 Hurricane Electric

Рисунок 4 Результат работы сервиса <https://bgp.he.net/>.

Traceroute – служебная компьютерная программа, предназначенная для определения маршрутов следования данных в сетях TCP/IP. Traceroute может использовать разные протоколы передачи данных в зависимости от операционной системы устройства. Такими протоколами могут являться UDP, TCP, ICMP или GRE. Компьютеры с установленной операционной системой Windows используют протокол ICMP, при этом операционные системы Linux и маршрутизаторы Cisco — протокол UDP.

Traceroute входит в состав большинства современных сетевых операционных систем. В системах Microsoft Windows эта программа называется **tracert**, а в системах GNU/Linux, Cisco IOS и Mac OS — **traceroute**.

Использование команды traceroute в системе Kali Linux выглядит следующим образом:

traceroute [host] [option]

Набрав traceroute -- help, вы получите дополнительную информацию о команде.

```
(kali@kali) ~  
$ traceroute certifiedhacker.com  
traceroute to certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets  
 1 192.168.0.1 (192.168.0.1) 3.362 ms 4.011 ms 3.945 ms  
 2 10.100.126.1 (10.100.126.1) 5.979 ms 6.281 ms 6.357 ms  
 3 border-gw.best.net.ua (95.158.0.213) 3.809 ms 4.546 ms 4.639 ms  
 4 te0-2-0-5.ccr21.kbp01.atlas.cogentco.com (149.6.190.225) 6.572 ms 7.116 ms 7.271 ms  
 5 be3644.ccr22.kbp01.atlas.cogentco.com (130.117.2.70) 7.849 ms 8.023 ms be2046.ccr21.bts01.atlas.cogentco.com (154.54.58.245) 25.949 ms  
 6 be2047.ccr22.bts01.atlas.cogentco.com (154.54.60.205) 25.912 ms be2988.ccr51.vie01.atlas.cogentco.com (154.54.59.86) 23.604 ms be2047.ccr22.bts01.a  
tlas.cogentco.com (154.54.60.205) 22.756 ms  
 7 be2838.ccr52.vie01.atlas.cogentco.com (154.54.73.178) 24.952 ms be3463.ccr52.vie01.atlas.cogentco.com (154.54.59.185) 24.009 ms 25.189 ms  
 8 ae-14.r00.vienat02.at.bb.gin.ntt.net (129.250.9.129) 25.150 ms 24.793 ms 25.766 ms  
 9 ae-3.r20.vienat02.at.bb.gin.ntt.net (129.250.7.18) 53.109 ms 58.424 ms 54.381 ms  
10 ae-1.r20.frnkge13.de.bb.gin.ntt.net (129.250.7.35) 37.759 ms 37.484 ms 38.621 ms  
11 ae-14.r21.londen12.uk.bb.gin.ntt.net (129.250.3.12) 45.162 ms 45.616 ms 42.597 ms  
12 ae-13.r25.asbnva02.us.bb.gin.ntt.net (129.250.2.111) 128.607 ms * 125.877 ms  
13 ae-6.r20.dllstx14.us.bb.gin.ntt.net (129.250.5.12) 167.273 ms 157.962 ms 159.804 ms  
14 ae-14.r24.dllstx09.us.bb.gin.ntt.net (129.250.3.37) 157.523 ms 158.558 ms 157.737 ms  
15 ae-2.r11.dllstx09.us.bb.gin.ntt.net (129.250.5.14) 161.918 ms 154.420 ms 155.070 ms  
16 ce-0-16-0-3.r11.dllstx09.us.ce.gin.ntt.net (131.103.117.42) 155.003 ms 154.373 ms ce-0-16-0-3.r10.dllstx09.us.ce.gin.ntt.net (128.242.179.18) 156.  
242 ms  
17 xe-2-0-0.rtrn1.dall1.net.unifiedlayer.com (162.215.243.3) 155.132 ms 153.462 ms xe-2-0-0.rtrn1.dall1.net.unifiedlayer.com (162.215.243.9) 154.515 ms  
18 162-215-243-21.unifiedlayer.com (162.215.243.21) 160.733 ms 162-215-243-23.unifiedlayer.com (162.215.243.23) 160.506 ms 159.516 ms  
19 162-241-0-30.unifiedlayer.com (162.241.0.30) 158.857 ms * 162-241-0-34.unifiedlayer.com (162.241.0.34) 156.152 ms  
20 po100.router2b.houl.net.unifiedlayer.com (162.241.0.5) 152.826 ms po100.router2a.houl.net.unifiedlayer.com (162.241.0.3) 155.733 ms po101.router2b.  
houl.net.unifiedlayer.com (162.241.0.9) 154.806 ms  
21 108-167-150-122.unifiedlayer.com (108.167.150.122) 154.053 ms 108-167-150-118.unifiedlayer.com (108.167.150.118) 150.985 ms 108-167-150-126.unified  
layer.com (108.167.150.126) 152.704 ms  
22 box5331.bluehost.com (162.241.216.11) 152.717 ms 153.428 ms 152.037 ms
```

Рисунок 5 Результат работы команды traceroute.

ЗАДАНИЕ 1

Получить всю информацию об AS с помощью bgr.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/>

Порядок выполнения работы

Shodan - это поисковая система для устройств, подключенных к Интернету. Системы веб-поиска, такие как Google и Bing, отлично подходят для поиска веб-сайтов. Но что если вам интересно определить, какие страны становятся более взаимосвязанными? Или если вы хотите узнать, какая версия Microsoft IIS самая популярная? Может быть, появилась новая уязвимость, и вы хотите посмотреть, на скольких хостах она применима? Традиционные поисковики не позволяют ответить на эти вопросы. Shodan собирает информацию обо всех устройствах, непосредственно подключенных к Интернету. Если устройство напрямую подключено к Интернету, Shodan запрашивает у него разную общедоступную информацию. Типы индексированных устройств могут сильно отличаться от небольших настольных компьютеров до серверов датацентра.

Так что же индексирует Shodan? Основная часть данных берется из баннеров, представляющих собой метаданные о программном обеспечении, работающих на устройствах. Это может быть информация о серверном программном обеспечении, а также информация о том какие параметры поддерживают службы.

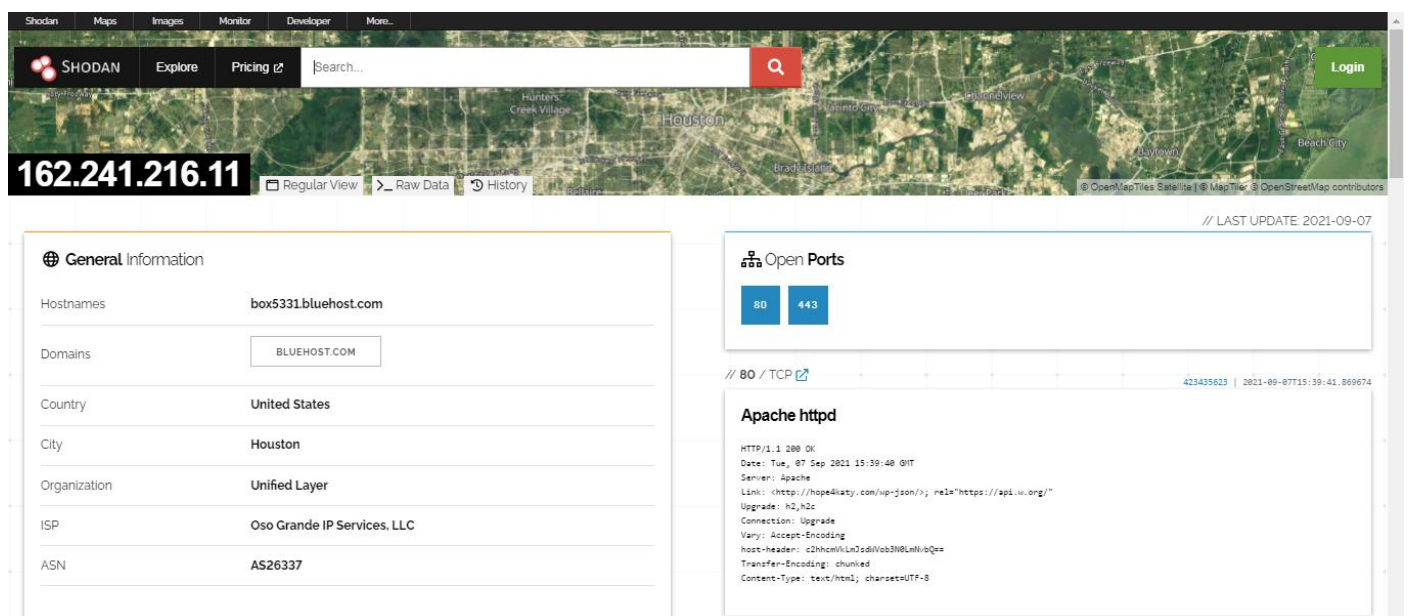


Рисунок 6 Результат работы поисковой системы Shodan.

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

Порядок выполнения работы

Maltego – это инструмент для построения и анализа связей между разными субъектами и объектами. Ее особенностями являются: визуализация полученных данных, разведка на основе открытых источников, комбинирование для глубокого анализа данных, полученных из закрытых и открытых источников, автоматический анализ открытых источников и автоматическое построение взаимосвязей между обнаруженными объектами.

Maltego позволяет собрать воедино информацию, полученную из открытых и закрытых источников, она позволяет визуализировать агрегированные данные.

Maltego – это программа, которая может быть использована для выявления отношений и реальных связей между:

- людьми
- Группами людей (социальные сети)
- компаниями
- организациями
- Веб-сайтами

Интернет инфраструктурами, такими как:

- доменами
- DNS именами
- сетевыми блоками
- IP адресами

Документами и файлами

Эти объекты связываются на основе разведки из открытых источников.

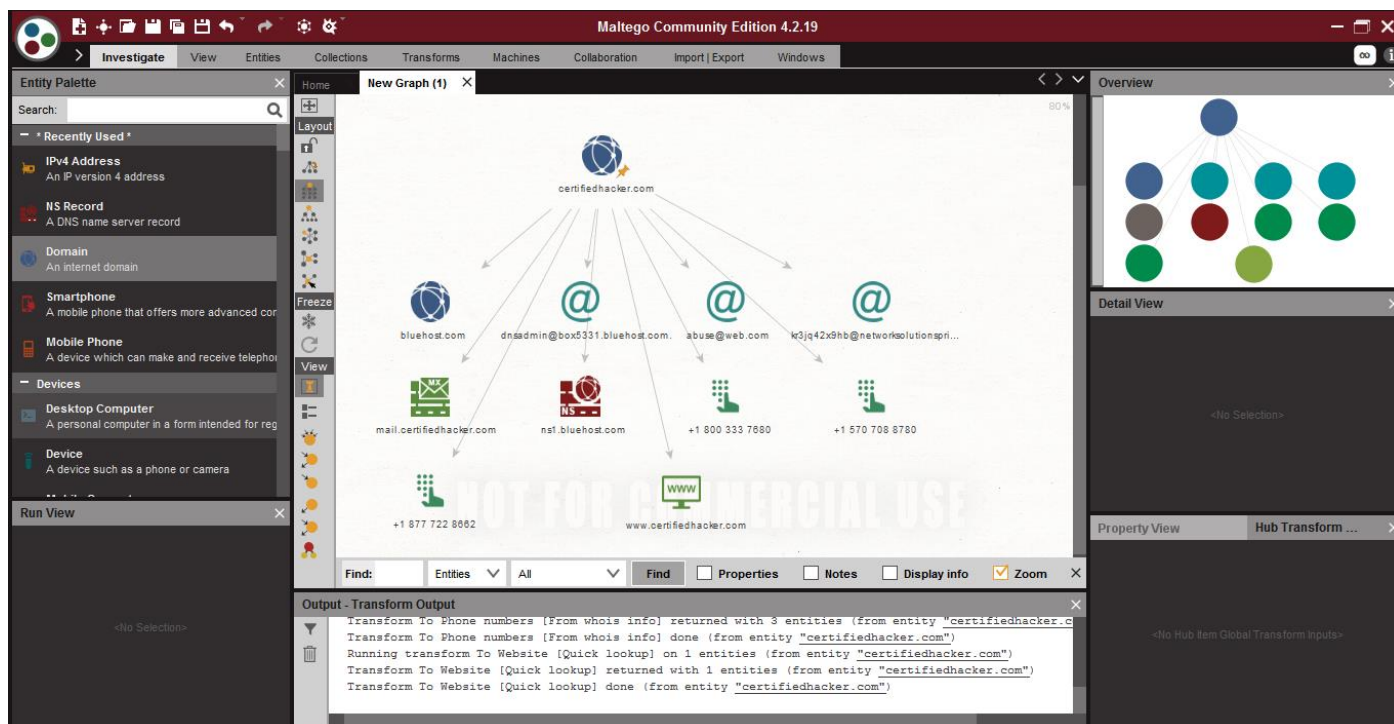


Рисунок 7 Результат работы программы Maltego.

FOCA — это инструмент, который используется в основном для поиска метаданных и скрытой информации в сканированных документах. Эти документы могут находиться на веб-страницах, их можно скачать и проанализировать с помощью FOCA.

Это приложение способно анализировать широкий спектр документов, наиболее распространенными из которых являются файлы Microsoft Office, Open Office или PDF, хотя также можно анализировать файлы Adobe InDesign или SVG.

Эти документы ищутся с помощью трех возможных поисковиков: Google, Bing и DuckDuckGo. Сумма результатов трех поисковых систем составляет множество документов. Также можно добавлять локальные файлы для извлечения информации.

Используем программу FOCA для сбора метаданных из файлов, находящихся на сайте certifiedhacker.com. Для этого в программе FOCA создадим новый проект.

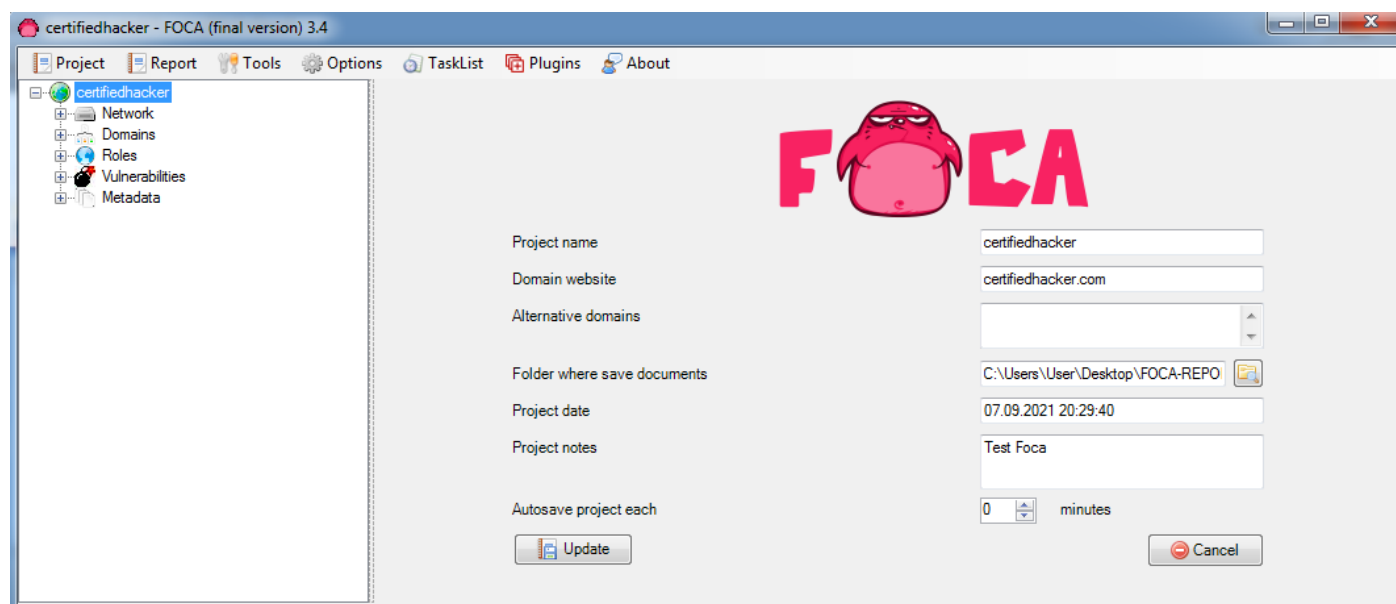


Рисунок 7 Создание проекта в программе FOCA.

Далее выберем типы файлов и поисковую систему, с помощью которой будем искать файлы, которые могут включать в себя метаданные. Нажмем кнопку Search All и получим список найденных файлов.

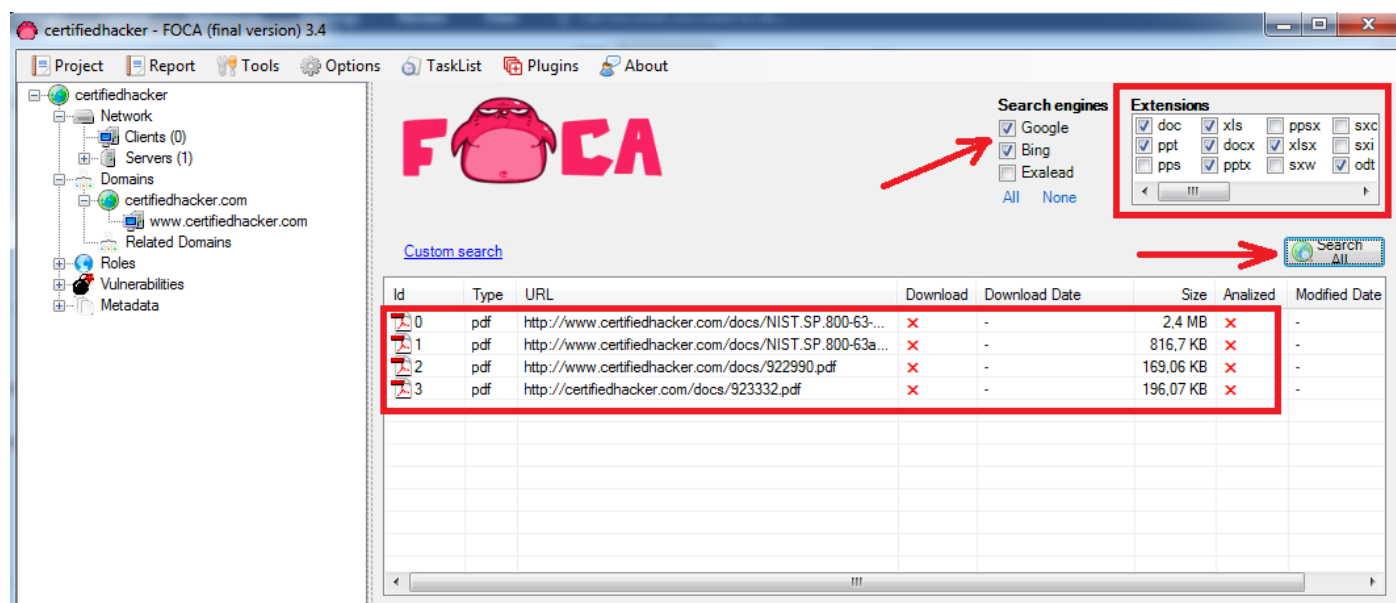


Рисунок 8 Программа FOCA выбор типов файлов и поисковой системы.

Выделим найденные файлы, далее вызываем правой кнопкой мыши дополнительное меню и загрузим файлы выбрав пункт “Download”, после чего извлечем метаданные выбрав в том же меню пункт “Extract Metadata”

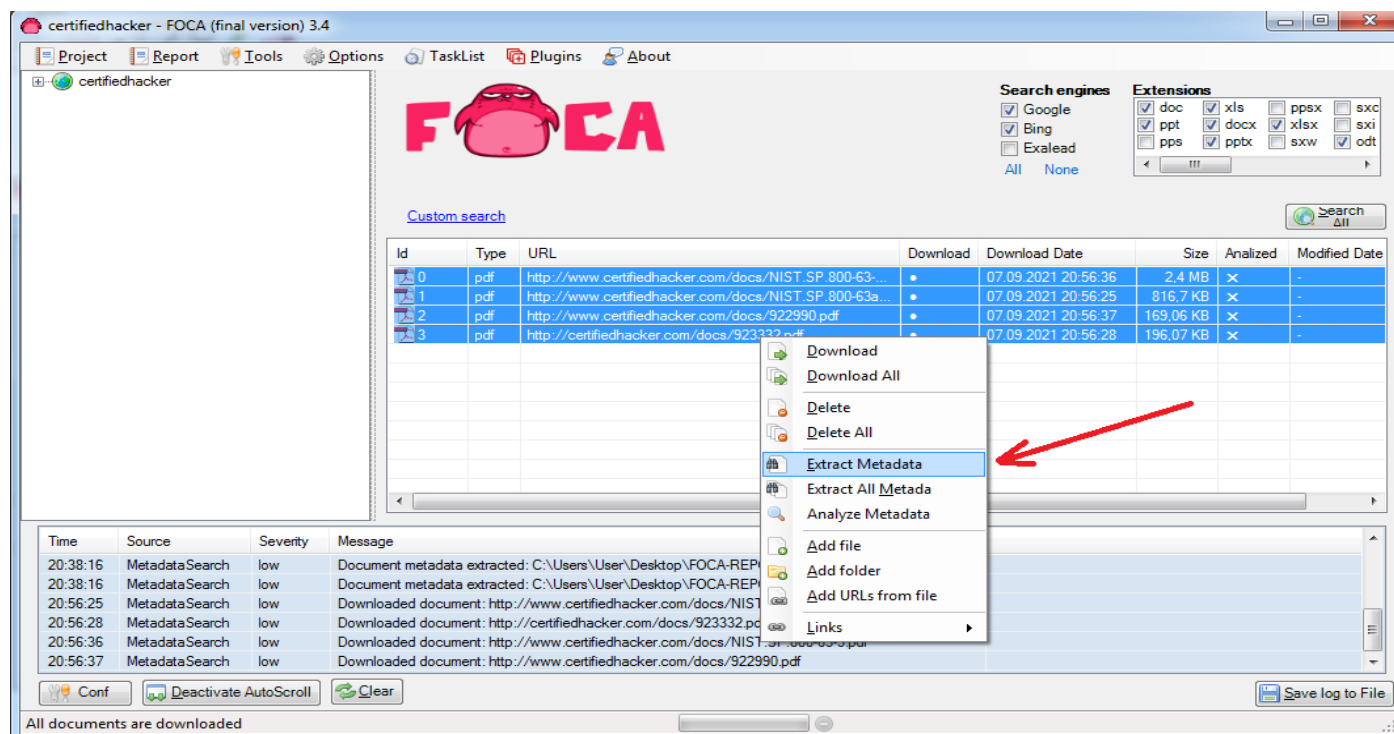


Рисунок 8 Программа FOCA извлечения метаданных из файлов.

Проанализируем извлеченные метаданные. Как видно было найдено 2 пользователя, определены операционные системы и офисные пакеты, в которых созданы документы.

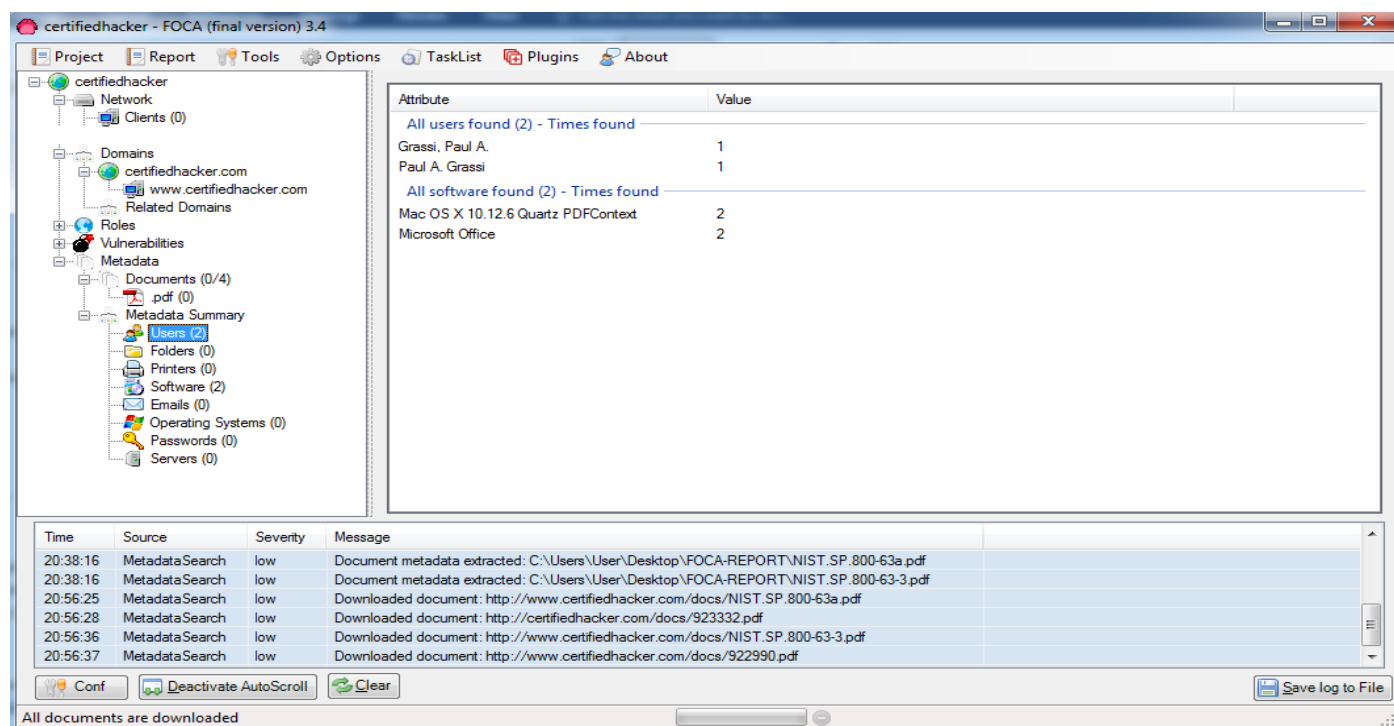


Рисунок 9 Результат работы программы FOCA.

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/>

Порядок выполнения работы

OSINT (англ. Open source intelligence) "Разведка по открытым источникам" - включает в себя поиск и сбор разведывательной информации из общедоступных источников, а также ее анализ.

С помощью сервиса <https://haveibeenpwned.com/> проверим найденный в предыдущих работах электронный ящик `abuse@web.com`

Как видим по результату проверки было найдено 7 нарушений данных и найдено 75 утечек.

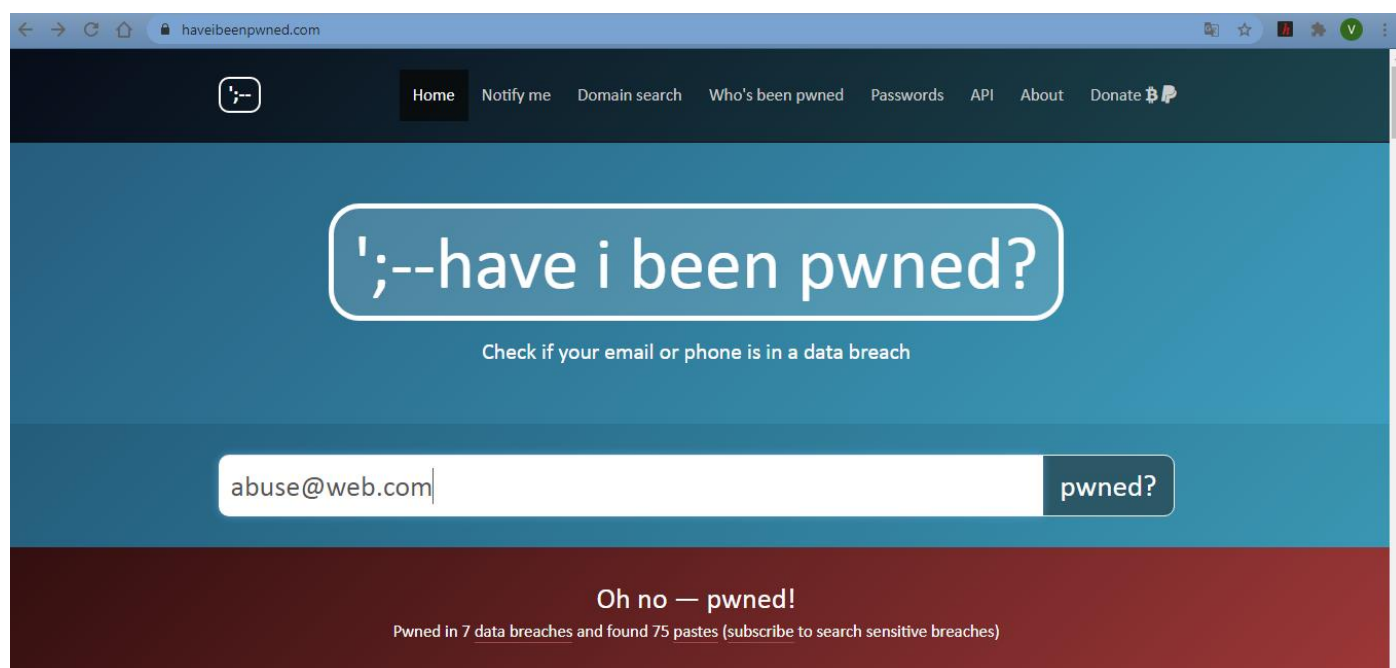


Рисунок 10 Результат работы сервиса <https://haveibeenpwned.com/>.

С помощью сервиса <https://pastebin.com/> также проверим найденный в предыдущих работах электронный ящик abuse@web.com. Для этого в поиске Google введем следующую команду `site:pastebin.com abuse@web.com`.

По результату поиска был найден текст письма, которое было отправлено на почтовый ящик abuse@web.com.

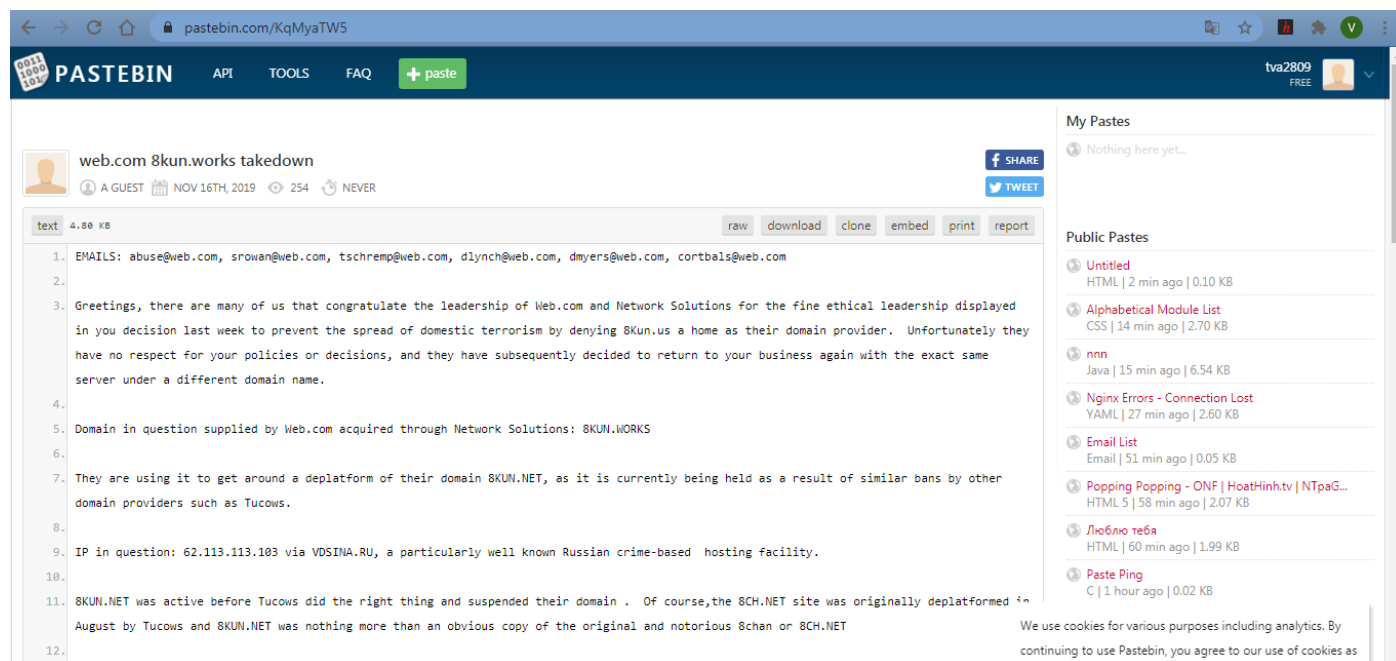


Рисунок 11 Результат работы сервиса <https://pastebin.com/>.

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:
