# ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ВЕБ-СЕРВИСА SHODAN.IO И ДЛЯ СКАНИРОВАНИЯ ОБЩЕДОСТУПНЫХ РЕСУРСОВ СЕТИ ИНТЕРНЕТ

THE MAIN POSSIBILITIES OF APPLICATION OF THE SHODAN.IO WEB SERVICE FOR SCANNING PUBLIC INTERNET RESOURCES

**УДК 004.455 + 004.056**

**Федосенко Максим Юрьевич,** магистрант, Национальный исследовательский университет ИТМО г. Санкт-Петербург

**Fedosenko M.Y.,** fedosenkomaksim98@gmail.com

## Аннотация

В статье рассматриваются возможности проведения сканирования ресурсов в глобальной сети. Прежде всего, это используется для обнаружения уязвимости и слабых мест в безопасности ресурса. У сетевых инженеров имеется множество утилит и специальных рабочих средств для мониторинга состояния сети и осуществления тестирований. Однако современная тенденция развития информационных технологий всё большое внимания уделяет облачным сервисам и интеграции приложений в web пространство. Таким образом, материал статьи содержит описание web сервиса для сканирования интернет-ресурсов shodan.io. Рассмотрены его возможности, варианты настройки. Продемонстрировано практическое применение на общедоступном ресурсе – сайте Университета ИТМО.

**Annotation**

The article presents the possibilities of scanning resources in the global network. Most often it is used to detect vulnerabilities and weaknesses in the security of a resource. Network engineers have many utilities and special tools to monitor network and perform tests. However, the current trend in the development of information technology is paying more attention to cloud services and the integration of applications into the web. The material of the article contains a description of the web service for scanning Internet resources Shodan.io. Its capabilities, configuration options are considered. A practical application is demonstrated on a public resource - the ITMO University website.

**Ключевые слова:** сетевая безопасность, интернет-ресурс, web, nmap, shodan.io, сканирование сети, мониторинг состояния сети

**Keywords:** network security, internet resource, web, nmap, shodan.io, network scanning, network status monitoring

## Введение

Роль сетевой безопасности увеличивается пропорционально возрастающему числу устройств, подключённых к глобальной сети. Наибольший прирост наблюдается в связи с активным внедрением устройств интернета вещей (IoT) и развитием протокола IPv6. И основной задачей сетевых инженеров становится не только грамотное построение архитектуры сети, но и обеспечение высокого уровня безопасности и сохранности пользовательских данных. В арсенале сетевых инженеров имеется множество утилит под различные операционные системы для мониторинга, сбора статистики, тестирования сети. Особую нишу занимают продукты, способные протестировать отказоустойчивость сети и найти в ней слабые места в безопасности, такие как открытые сетевые порты, доступные внутренние сервисы извне, использование слабых криптографических алгоритмов. С задачей тестирование сети на безопасность хорошо справляется специально

разработанный дистрибутив Kali Linux и входящие в его состав утилит: Burp site, Wireshark, Netscan, Nmap [1].

Стоит уделить внимание последней утилите Nmap, поскольку её основное отличие – возможность проводить разведку уязвимости ресурса вне сети. Это утилита с открытым исходным кодом, предназначенная для сканирования IP-сетей с множеством объектов, определения состояния объектов и их служб. Для этого Nmap использует множество сканирований, таких как UDP, TCP FTP, Reverse-ident, ICMP, FIN, ACK, NULL-сканирование. Также поддерживает множество дополнительных возможностей: определение операционной системы удалённого хоста, скрытое сканирование, вычисление времени задержки и повтор передачи пакетов, параллельное сканирование, прослушивание, определение неактивных хостов. Утилита является консольной, не требует большого объёма вычислительных ресурсов. Однако необходима установка, чтение документации и специальная вычислительная среда [2].

Однако разработки, направленные на доступность сервисов и упрощение их использования не стоят на месте, что привело к тенденции создания web-версий популярных приложений, например WebTelegram или Steganography Online [3]. Аналогично имеется web аналог Nmap, правда от стороннего разработчика. Называется ресурс Shodan.io

**Shodan**

Shodan.io является интернет интернет-ресурсом, позволяющим получать информацию о подключённых к сети устройствах по их IP адресу. Название Shodan является отсылкой к SHODAN - персонажу из серии компьютерных игр System Shock. Сайт был запущен в 2009 году программистом Джоном Мэтерли, у которого возникла идея разработать ресурс для поиска устройств, подключённых к Интернету по аналогии с поисковиком Google. Основа идеи заключалась в том, что глобальная сеть представляет всемирную паутину, соединённого между собой оборудования,

имеющего IP адреса. Другими словами, ресурс представляет собой поисковую систему, позволяющую пользователям искать подключённые к интернету сервера: веб-камеры, маршрутизаторы, и т. д. Некоторые также описывают его как поисковую систему сервисных баннеров, представляющие собой метаданные, которые сервер отправляет обратно клиенту при ответе. Этими метаданными может быть информация о программном обеспечении, какие опции поддерживает сервис, приветственное сообщение или что-то ещё, что клиент должен выяснить перед взаимодействием с сервером.

В своей работе, Shodan главным образом собирает данные о веб-серверах HTTP/HTTPS (порты 80, 8080, 443, 8443), а также FTP (порт 21), SSH (порт 22), Telnet (порт 23), SNMP (порт 161), IMAP (порты 143, 993), SMTP (порт 25), SIP (порт 5060), RTSP (порт 554). Последний протокол может использоваться для доступа к веб-камерам и их видеопотоку. Согласно информации с заглавной страницы ресурса, он имеет следующие возможности [4]:

- **Информация:** веб-сайты – это лишь часть всемирной паутины. Используйте Shodan чтобы узнать обо всём, что в ней есть: от электростанций, мобильных телефонов до холодильников серверов в Minecraft
- **Мониторинг сети:** следите за всеми вашими устройствами, к которым есть прямой доступ из интернета. Shodan представляет исчерпывающий обзор всех предоставляемых услуг, чтобы помочь вам оставаться в безопасности
- **Интернет-разведка:** узнайте больше о том, кто использует различные продукты и как они меняются с течением времени. Shodan даёт вам основанное на данных представление о технологиях, лежащих в основе Интернета.

Стоит заметить, что ресурс является англоязычным, однако при помощи браузерного перевода становится понятным для носителя любого

языка. Помимо упомянутого выше, сервис также имеет расширенный функционал:

- **Shodan Maps:** позволяет исследовать мир устройств, подключенных к Интернету при помощи карты. Доступно увеличение, сжатие, панорамизация результатов на основе GeoIP
- **Shodan Images:** Shodan собирает скриншоты множества различных сервисов и даёт вам, как участнику, доступ к новому интерфейсу поиска, который значительно упрощает просмотр этих сделанных «снимков»
- **Shodan Developer API:** все ресурсы Shodan полностью построены на основе общего API, доступного всем пользователям

Рассмотрим подробнее Shodan Developer API и возможность использования ресурса в промышленных масштабах. Разработчикам предоставляется удобный API и возможность работать с функционалом ресурса через командную строку, Python, node.js. Однако, существуют ограничения на количество запросов, для увеличения которых необходимо оформлять подписку. Перечень подписок и их возможностей приведён в Таблице 1.

Таблица 1 "Сравнительная характеристика подписок shodan и доступного для них функционала"

| | ***Membership*** | ***Freelancer*** | ***Small Business*** | ***Corporate*** | ***Enterprise*** |
|---|---|---|---|---|---|
| ***Price*** | $49 (one-time) | $59/ month | $299/ month | $899/ month | |
| ***Query credits (per month)*** | 100 | 10,000 | 200,000 | Unlimited | Unlimited |

| | | | | | |
|---|---|---|---|---|---|
| ***Scan credits (per month)*** | 100 | 5,120 | 65,536 | 327,680 | Unlimited |
| ***Monitored IPs*** | 16 | 5,120 | 65,536 | 327,680 | Unlimited |
| ***Available search filters*** | All except vuln and tag | All except vuln and tag | All except tag | All | All |
| ***Number of users*** | 1 | 1 | 1 | 1 | Custom |
| ***Shodan Search page*** | 20 | 20 | 200 | 200 | 200 |
| ***Shodan Monitor*** | yes | yes | yes | yes | yes |
| ***Private firehose*** | yes | yes | yes | yes | yes |
| ***IP lookups*** | yes | yes | yes | yes | yes |
| ***Batch IP lookups*** | - | - | - | yes | yes |
| ***Bulk Data*** | - | - | - | - | yes |
| ***InternetDB*** | - | - | - | - | yes |
| ***Full firehose*** | - | - | - | - | yes |
| ***Internet scanning API*** | - | - | - | - | yes |
| ***600+ Million hostnames scan*** | - | - | - | - | yes |

Таким образом, помимо большого пула запросов к серверу, корпоративная подписка предоставляет множество возможностей не только для мониторинга, но и управления рисками информационной безопасности ресурса, проведения аналитики, закрытия уязвимостей. Стоит отметить, что для пользования упомянутым функционалом требуется регистрация. А для использования в промышленных масштабах понадобится регистрация из-за имеющихся на сервере ограничений на запросы. Однако ресурс предоставляет такую возможность и готов поддерживать разработчиков.

Рассмотрим практическое применение ресурса на примере сайта технического университета ИТМО: https://itmo.ru/ru/ [5]. Для этого необходимо в поисковую строку ввести IP адрес сайта. В результате манипуляции отобразилась информация о сервере (провайдер, месторасположение и т.д.), открытые порты и что на них расположено (криптографические ключи, версия веб-сервера, SSH и т.д.). Результат работы можно наблюдать согласно рисунку 1.

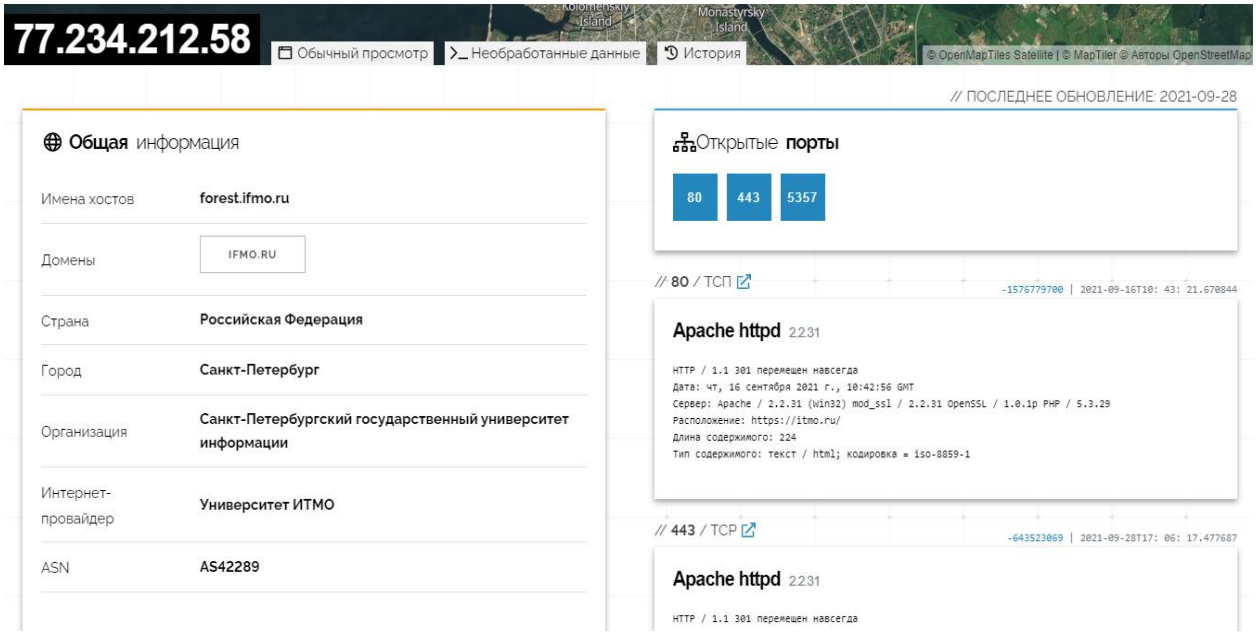


Рисунок 1 – Shodan.io в работе

Также, стандартный функционал способен находить уязвимости ресурса и выводить их CVE, благодаря чему можно найти методы решения

воспользовавшись общей базой https://cve.mitre.org/ [6]. Пример обнаружения уязвимостей приведён на рисунке 2.

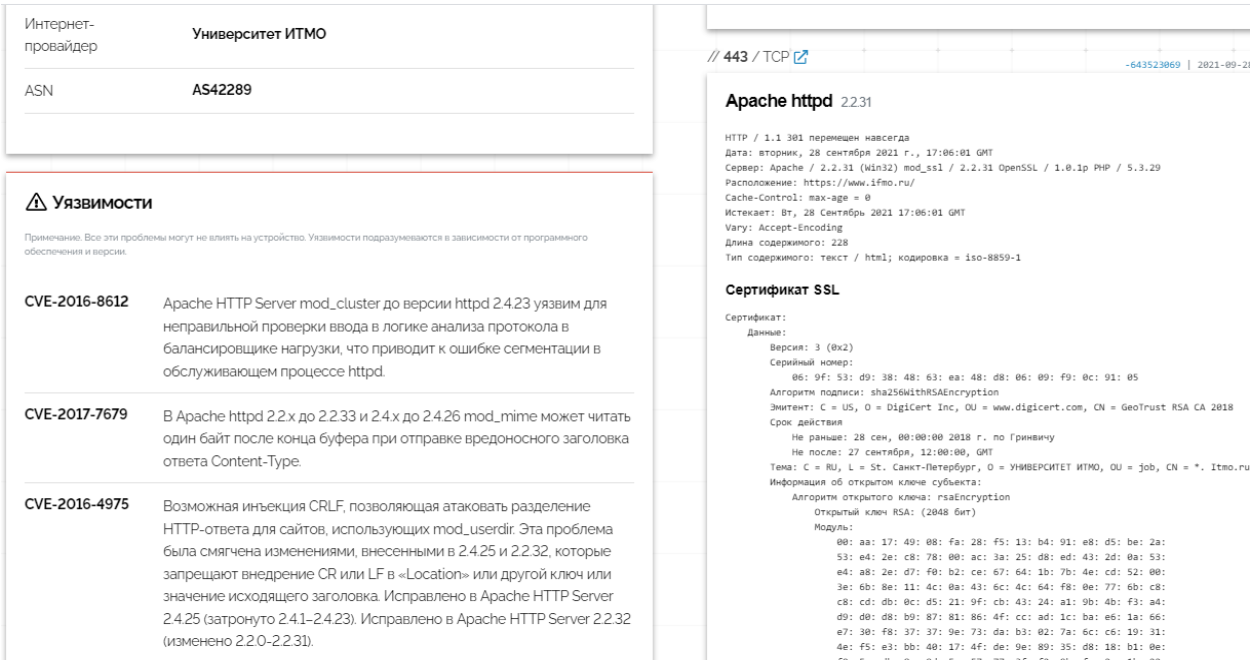


Рисунок 2 - Уязвимости и SSL сертификат для сайта itmo.ru

Имея эти данные, уже можно произвести аналитику ресурса на предмет уязвимости, производить сканирование и мониторинг интересующего вас ресурса (или целой сети) в режиме реального времени: обнаруживать утечки данных в облако, фишинговые веб-сайты, взломанные базы данных и т.д. Shodan предоставляет инструменты для мониторинга всех подключенных устройств в Интернете. Стоит также заметить, что можно настроить удобное оповещение по результатам мониторинга и выявления каких-либо аномалий. Уведомления доступны на почту, аккаунты Slack, Telegram, Discord, MS Teams. Демонстрация функционала проведения аналитики устройства представлено на рисунке 3 [7]:

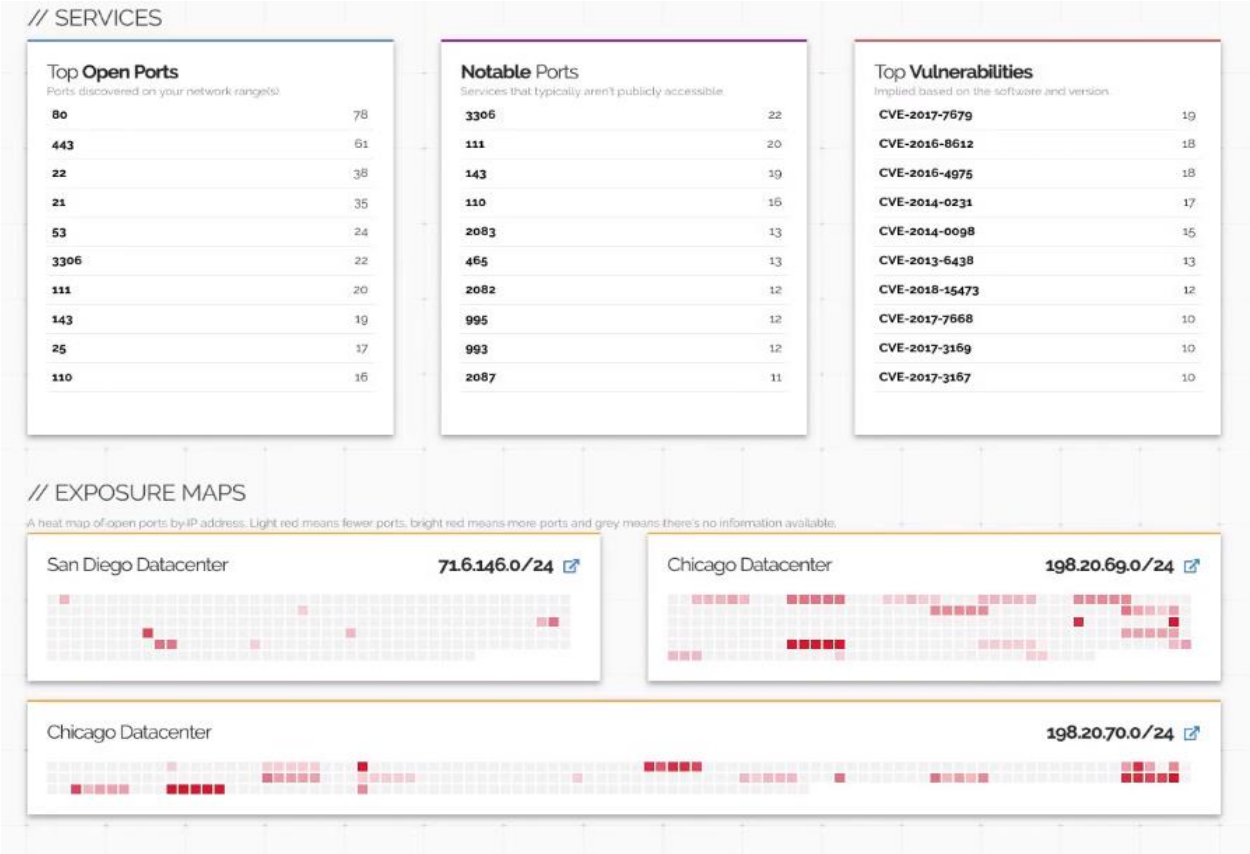


Рисунок 3 - Shodan Monitoring

**Заключение**

Подводя итог вышесказанному, стоит вновь вернуться к сравнению Shodan.io с аналогами. Как было упомянуто ранее, наиболее похожей по функционалу является утилита NMap. NMap имеет больше возможностей для тонкой настройки (выбор диапазона портов, режим «прослушивания») и является полностью бесплатной. Однако данная утилита, в отличие от рассматриваемого веб-сервиса, использует для работы ресурсы вычислительной машины, на которой запущена и не имеет удобного графического интерфейса, с возможностью визуализации аналитических данных. Также, данная утилита не находит не умеет определять уязвимости по CWE и предоставлять рекомендации по их устранению.

Существует также ресурс Urlscan.io со схожим набором функций. Он представляет собой сканер веб-сайтов, способный классифицировать почти 100 000 URL-адресов каждый день. В них входят материалы, отправленные тысячами пользователей и исследователями безопасности, а также все URL-

адреса в openphish, phishtank, certstream, urlhaus и т. д. Urlscan выполняет весь анализ на своих серверах: записывает данные http-запроса, все взаимодействия домена, все ссылки на отсканированной страницы, используемые технологии веб-сайта, хеш каждого файла на странице, и определение сертификата ssl, а также связанных сканирований, информации об IP, информации о безопасном просмотре Google для домена. Делает всю эту информацию доступной бесплатно через интуитивно понятный и хорошо продуманный API. По умолчанию интеграция с Urlscan не требует каких-либо дополнительных настроек [8].

Стоит также упомянуть про FAQ сервиса Shodan, где можно найти ответ на типовые вопросы и задать свой. Находится он здесь: https://help.shodan.io/ [9] и имеет в себе все инструкции для использования возможностей ресурса. Чтобы получить полные возможности сервера - достаточно зарегистрироваться, сделать это возможно через аккаунт *Google, Twitter, Windows Live.* В качестве альтернативы дизайнерского решения продукта, владелец ресурса разработал специальный интерфейс в стиле 2000-х годов, с возможностью использования командной строки и музыки из мини-игр той эпохи. Данную вариацию можно наблюдать по ссылке из источников [10] и на рисунке 4.

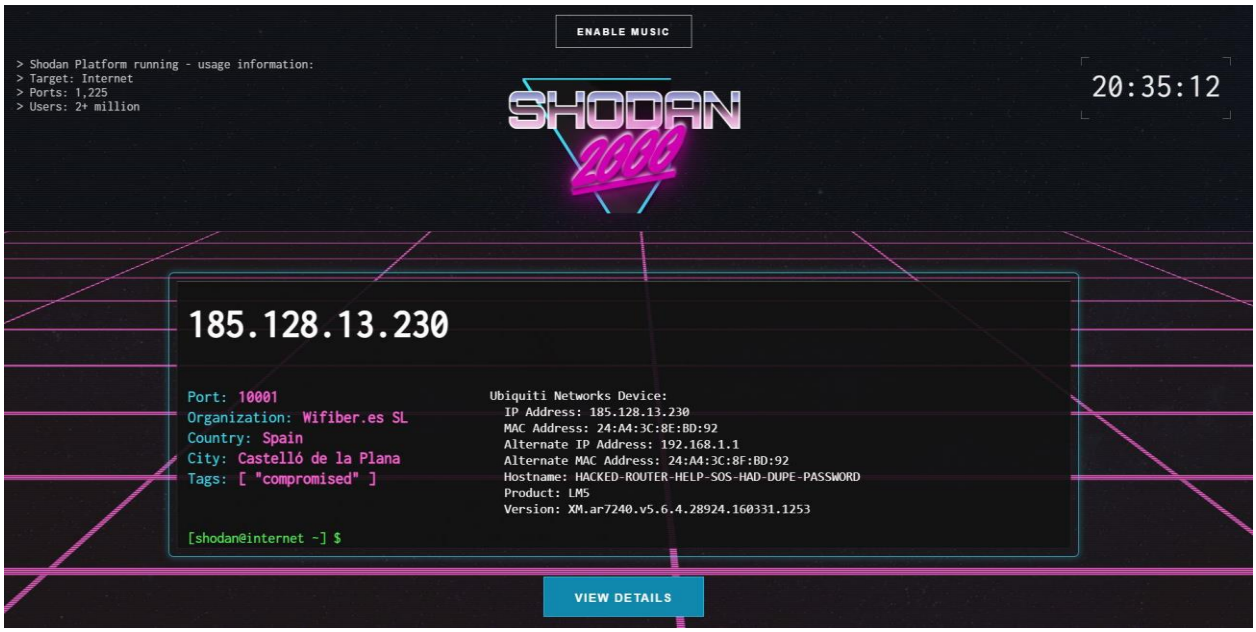


Рисунок 4 - Disco Shodan 2000

## Литература


1. Kali Tools. Tool Documentation / OffSec Services Limited https://www.kali.org/tools/ (18.01.2022).
2. Nmap Reference Guide. Documentation / NMAP.ORG. https://nmap.org/docs.html (18.01.2022).
3. Steganography Online /Stylesuxx. http://stylesuxx.github.io/steganography/ (18.01.2022).
4. Search Engine for the Internet of Everything / Shodan https://www.shodan.io/ (18.01.2022).
5. Университет ИТМО / Минобрнауки России https://itmo.ru/ru/ (18.01.2022).
6. CVE-CVE / The MITRE Corporation https://cve.mitre.org/ (18.01.2022).
7. Introduction to Shodan Monitor / Shodan https://www.youtube.com/watch?v=T-9UvZ-l-tE (18.01.2022).
8. Urlscan.io. A sandbox for the web / SecurityTrails https://urlscan.io/ (18.01.2022).
9. Shodan Help Center / Shodan https://help.shodan.io/ (18.01.2022).
10. Shodan 2000 / Shodan https://2000.shodan.io/#/ (18.01.2022).


## Literature


1. Kali Tools. Tool Documentation / OffSec Services Limited https://www.kali.org/tools/ (18.01.2022).
2. Nmap Reference Guide. Documentation / NMAP.ORG. https://nmap.org/docs.html (18.01.2022).
3. Steganography Online / Stylesuxx. http://stylesuxx.github.io/steganography/ (18.01.2022).
4. Search Engine for the Internet of Everything / Shodan https://www.shodan.io/ (18.01.2022).

5. ITMO University / Ministry of Education and Science of Russia https://itmo.ru/ru/ (18.01.2022).

6. CVE-CVE / The MITRE Corporation https://cve.mitre.org/ (18.01.2022).

7. Introduction to Shodan Monitor / Shodan https://www.youtube.com/watch?v=T-9UvZ-l-tE (18.01.2022).

8. Urlscan.io. A sandbox for the web / SecurityTrails https://urlscan.io/ (18.01.2022).

9. Shodan Help Center / Shodan https://help.shodan.io/ (18.01.2022).

10. Shodan 2000 / Shodan https://2000.shodan.io/#/ (18.01.2022).