Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет прикладной информатики (ФПИН)

Лабораторная работа №3

по дисциплине: Основы кибербезопасности

Автор: доцент практики, кандидат технических наук

Кравчук Алексей Владимирович

Санкт-Петербург
2025

Тема занятия: Пассивная разведка и расширение поверхности атаки с помощью общедоступных инструментов.

Disclaimer / Предупреждение об ответственности за преступления в сфере компьютерной информации (Глава 28 Уголовного Кодекса РФ «Преступления в сфере компьютерной информации»).

Статья УК РФ	Название	Что охватывает	Максимальное наказание
ст. 272	Неправомерный доступ к компьютерной информации	Несанкционированное проникновение в компьютер, сеть, систему или базу данных. Пример: взлом сайта, сервера, базы.	до 7 лет лишения свободы
ст. 273	Создание, использование и распространение вредоносных программ	Разработка, внедрение, передача вирусов, троянов, эксплойтов, ботнетов и т.п.	до 7 лет лишения свободы
ст. 274	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации	Нарушения, повлекшие уничтожение, блокирование или модификацию данных. Например, халатное администрирование, приведшее к утечке.	до 5 лет лишения свободы
ст. 274.1	Неправомерное воздействие на критическую информационную инфраструктуру РФ	Атаки на объекты КИИ: энергосистемы, транспорт, связь, госпорталы (ГИСы) и др.	до 10 лет лишения свободы (при тяжких последствиях — до 15 лет)

В ходе проведения лабораторной работы мы ничего не ломаем, на исследуемую систему активно не воздействуем, а только собираем и анализируем информацию из открытых источников.

Запуск активных сканов без официального разрешения организации ЗАПРЕЩЕН!!!

Ни в коем случае не пытайтесь осуществлять несанкционированный доступ к устройствам или сервисам, которые найдете. Не пытайтесь логиниться на обнаруженные веб-интерфейсы, использовать пароли по умолчанию (это нарушает закон). Ваша задача ограничивается анализом открытой информации.

Работаем в рамках законодательства!

Если вы нашли уязвимость в системе (например, БД с логином/паролем по умолчанию), нужно немедленно уведомить преподавателя о найденной уязвимости.

Не публикуйте эту информацию нигде и не пытайтесь взаимодействовать с сервисом.

Грустный пример из реальной жизни Военно-космической академии (май 2025 г.):

https://www.securitylab.ru/news/559246.php
https://vk.com/wall-28905875_35029615

Цель работы.

- Изучить методы пассивной разведки (OSINT) для увеличения внешней поверхности атаки организации (всех открытых сетевых ресурсов, которые могут стать целями злоумышленников).
- Освоить работу с поисковыми сервисами для поиска интернет-устройств и открытых сервисов: Shodan, Censys и/или Netlas.
- Оценить риски, связанные с обнаруженными открытыми ресурсами, и понять, какие *меры* можно предпринять для сокращения поверхности атаки (в том числе из Приказа № 17 ФСТЭК и Методич.документа).

Краткие теоретические сведения.

OSINT (Open Source Intelligence) – комплекс методов для сбора, анализа и систематизации информации *из общедоступных источников*, таких как социальные сети, СМИ, форумы, открытые базы данных, поисковые системы. Полученная информация используется для исследования/увеличения поверхности атаки.

Поверхность атаки (attack surface) — это совокупность всех точек входа (векторов атаки) в устройство/сеть, через которые злоумышленник может воздействовать на систему.

Под точками входа понимают:

- интерфейсы (открытые сетевые порты, веб-интерфейсы, API);
- компоненты инфраструктуры (оборудование, ОС, службы, ПО);
- уязвимые версии программного обеспечения;
- неправильные настройки (misconfiguration);
- слабые пароли и так далее.

Чем больше поверхность атаки, тем больше возможностей для злоумышленника взломать систему и получить доступ к конфиденциальной информации. Поэтому одной из задач обеспечения безопасности является *минимизация поверхности атаки* (отключение ненужных служб, управление конфигурациями и уязвимостями и т.д.).

В первой части лабораторной вы будете заниматься *расширением поверхности атаки* посредством использования популярных платформ: Shodan, Censys и Netlas. Эти инструменты регулярно сканируют интернет и индексируют полученные данные, предоставляя интерфейсы поиска по ним.

Shodan — это поисковая система для интернет-устройств, которая регулярно сканирует адресное пространство, пытается подключиться к открытым портам и сохраняет баннеры служб (***service banners*** - сообщения, которые устройство или сервис отправляет отправителю при попытке установления соединения с ним).

Рассмотрим баннер сервиса ssh, представленный на рисунке 1:

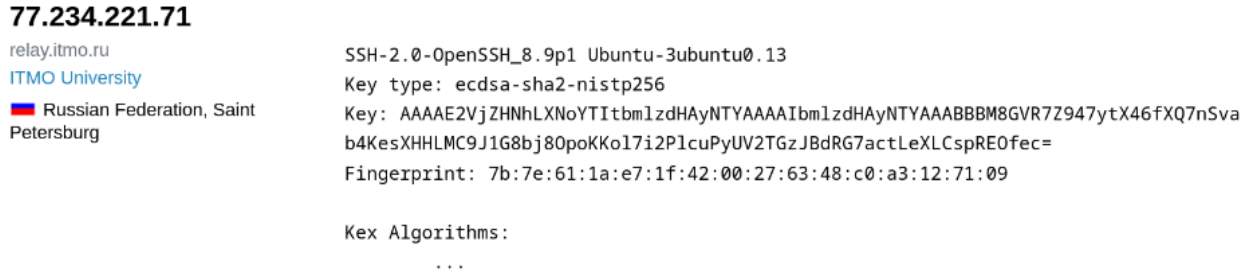


Рисунок 1. Баннер сервиса ssh

Структура баннера (из рисунка 1):

- SSH-2.0 — версия протокола SSH (здесь: SSH версии 2.0).
- OpenSSH_8.9p1 - реализация SSH и её версия: OpenSSH 8.9p1.
- Ubuntu-3ubuntu0.13 - информация о сборке/пакете, обычно указывает на пакетную версию в дистрибутиве.
- Key type: ecdsa-sha2-nistp256 - тип ключа, используемый для проверки подлинности сервера при установлении SSH-сессии.
- Key: AAAAE2Vj...Ofec= - публичный ключ хоста в виде Base64-кодированной строки.
- Отпечаток (fingerprint) — короткое представление публичного ключа, обычно в виде последовательности байт в hex с двоеточиями.
- Kex Algorithms — перечень алгоритмов обмена ключами (Key Exchange), которые сервер поддерживает/предлагает.

Баннеры сервисов составляют основу информации в Shodan, но он также использует информацию о SSL-сертификатах, HTTP-заголовках, номерах автономных систем, геолокации, а также метаинформацию о версиях пакетов.

Shodan в бесплатной версии скрывает имеет ограничение на размер показываемых результатов (2 страницы). Поэтому в отчёте о лабораторной работе допустимо указывать *«Shodan показал X результатов, детали не доступны в бесплатной версии»*.

ПРИМЕЧАНИЕ: Баннеры могут быть ложными или неполными. Сервер может отдавать «фейковый» баннер или скрывать информацию. В данном случае Shodan проиндексирует этот «фейковый» баннер.

Таким образом, Shodan не гарантирует достоверность.

Практическая часть:

В этой лабораторной работе вы работаете как этичный хакер (специалист по кибербезопасности), выполняющий внешнее обследование безопасности для инфраструктуры ИТМО. Прямое сканирование сети запрещено (помним про уголовную ответственность), поэтому вы проводите пассивную разведку, используя открытые источники.

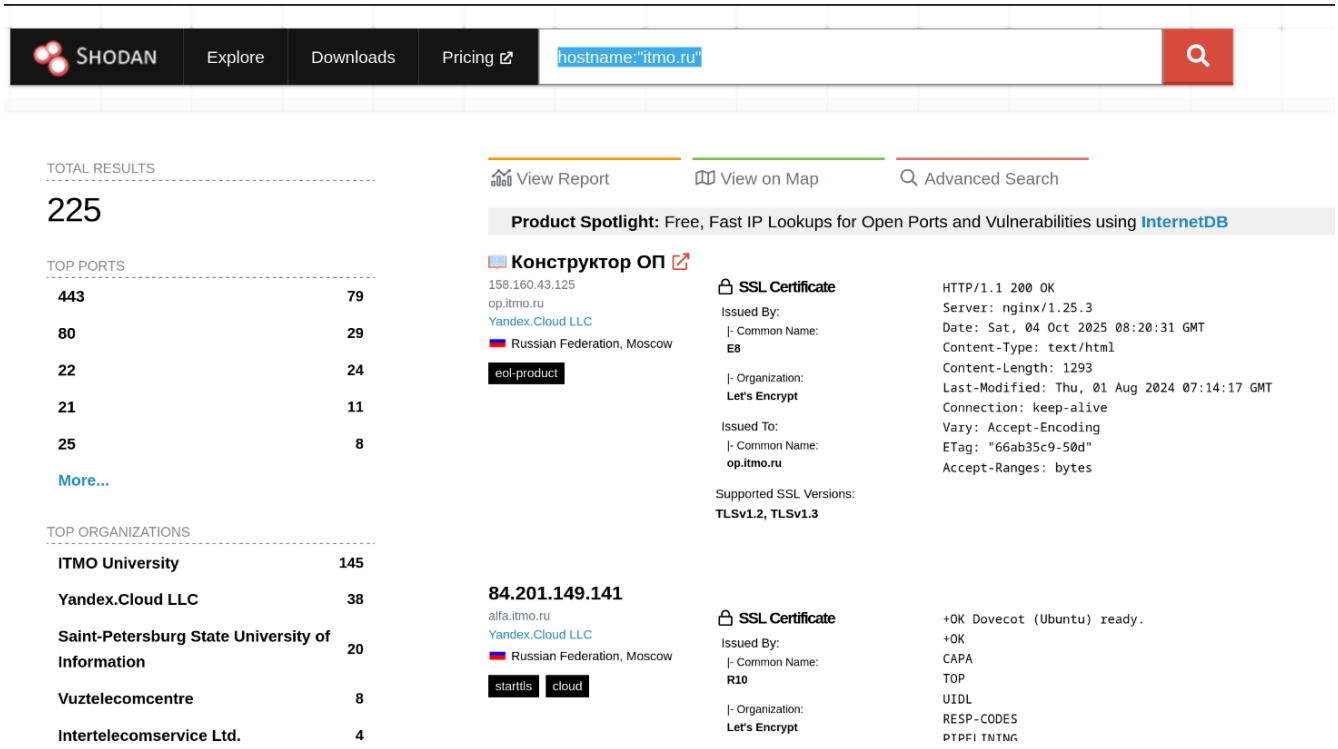
Ваша задача – расширить поверхность атаки, то есть собрать как можно больше сведений об интернет-активах вашего университета (серверы, устройства, домены, открытые порты, сервисы, версии ПО, уязвимости и пр.) из открытых источников, не взаимодействуя напрямую с системами/подсистемами ИТМО.

ПОРЯДОК РАБОТЫ.

1. Зарегистрировать новый почтовый ящик в сервисе Proton Mail (https://proton.me/mail). Этот шаг нам нужен для последующей регистрации на сервисах Censys, Shodan и Netlas (чтобы использовать стороннюю учетную запись без привязки к номеру телефона). В случае отсутствия VPN (для обхода блокировок) допускается использование вашего личного e-mail.

2. Зарегистрироваться в сервисе Shodan: https://www.shodan.io/.

3. В строке поиска Shodan вводим фильтр: ***hostname:"itmo.ru"*** и приступаем к анализу полученной информации.



В отчете необходимо отразить ход (!!! **обязательно прилагаем свои скриншоты !!!**) и результаты работы с интерфейсом Shodan:

TOTAL RESULTS

225

TOP PORTS

443	79
80	29
22	24
21	11
25	8

More...

TOP ORGANIZATIONS

ITMO University	145
Yandex.Cloud LLC	38
Saint-Petersburg State University of Information	20
Vuztelecomcentre	8
Intertelecomservice Ltd.	4

More...

TOP PRODUCTS

nginx	52
Apache httpd	32
OpenSSH	23
Postfix smtpd	14
GitLab Self-Managed	2

More...

TOP OPERATING SYSTEMS

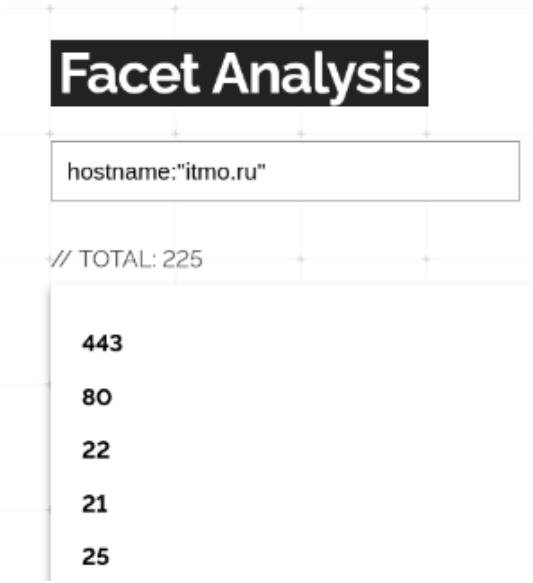
Ubuntu	42
Linux	16
Debian	1
FreeBSD	1
Unix	1

More...

3.1. Необходимо открыть подраздел «Top Ports» (перейти по ссылке «More…»), проанализировать информацию, представленную на странице, и внести в отчет.

В отчете требуется представить в табличной форме информацию о сервисах, которые работают на следующих портах: **22, 2222, 3306, 3389, 5060, 5432, 7443, 10000**.

Для получения развернутой информации нужно нажать на соответствующий номер порта в web-интерфейсе, см. рисунок ниже, либо использовать фильтр в



строке поиска shodan (*hostname:"itmo.ru" port:7443*)

Образец таблицы для заполнения представлен ниже (берем по 1-2 записи (строке) на каждую службу).

№ п/п	IP-адрес	Порт	Название сервиса	Примечание (насколько это хорошо с точки зрения ИБ; как эта информация может быть использована злоумышленником и так далее, КОРОТКО, что позволяет ваша текущая квалификация)
1.	77.234.222.71	22	ssh	ssh работает на стандартном порту; с точки зрения обеспечения ИБ это плохо; может использоваться для подбора пароля по словарю (brute force)
2.	77.234.222.93	2222	ssh	ssh работает на нестандартном порту, но этот порт очень часто используют для ssh; с точки зрения обеспечения ИБ это лучше, чем оставлять 22 порт; может использоваться для подбора пароля по словарю (brute force)

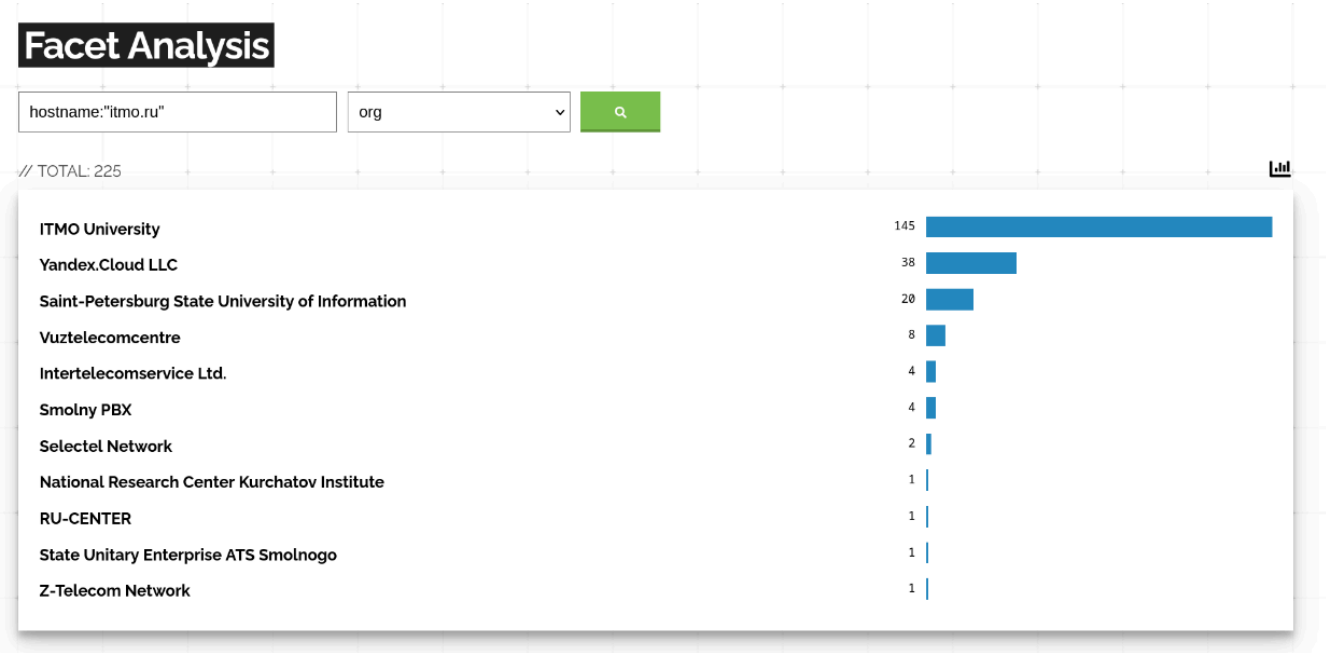
3.	77.234.215.140	3306	база данных MySQL	порт 3306 считается стандартным (well-known) портом для MySQL; для минимизации поверхности атаки рекомендуется изменить порт

3.2. Необходимо открыть подраздел «Top Organizations» (перейти по ссылке «More…»), проанализировать информацию, представленную на странице, и внести в отчет.

Раздел «Top Organizations» показывает владельцев IP-адресов, на которых Shodan обнаружил сервисы, связанные с itmo.ru (см. рисунок ниже).

Для формирования «Top Organizations» Shodan делает следующее:

- находит все IP-адреса, у которых в DNS (в прямой или обратной записи, SSL-сертификате и т.д.) встречается **itmo.ru** (например, ns.itmo.ru, mail.itmo.ru, vpn.itmo.ru, lms.itmo.ru и т.д.).
- берёт каждый из этих IP и смотрит, кому принадлежит IP-адрес по базе WHOIS / ASN.
- заносит эту информацию в поле org и группирует найденные IP по владельцу сетевого блока и считает, сколько устройств найдено в каждой организации.



Как мы видим, ИТМО использует не один сервер и не одного провайдера. Инфраструктура ВУЗа распределена:

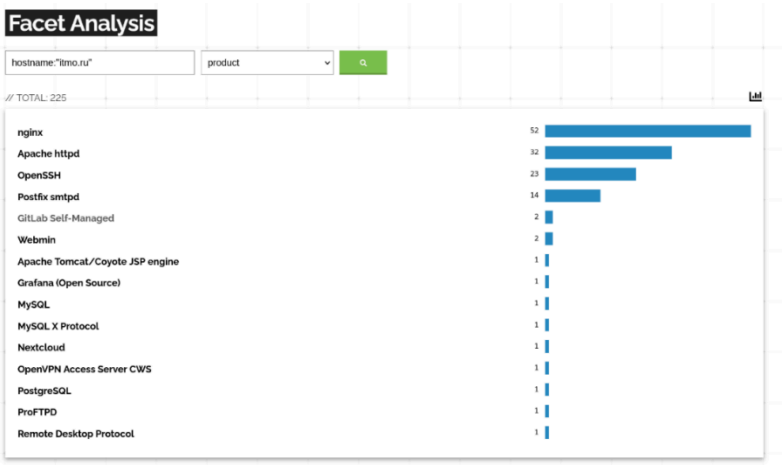
- часть сервисов работает внутри ИТМО (в собственном дата-центре);
- часть – у внешних провайдеров (Selectel, Yandex Cloud, …);
- часть — на партнёрских площадках (институт Курчатова …);

- кое-где остаются старые записи DNS с упоминанием itmo.ru, даже если это уже не активные сервера.

В отчет вставляем **полностью заполненную** таблицу:

Организация	Возможная интерпретация
ITMO University (145)	Большая часть IP действительно принадлежит подсетям, зарегистрированным на сам университет (у ИТМО есть собственная автономная система, AS60340, и пул адресов). Это основная инфраструктура вуза.
Yandex.Cloud LLC (38)	Некоторые сервисы ИТМО (например, веб-сайты, тестовые порталы, API, возможно облачные лаборатории) размещены в облаке Яндекса.
Saint-Petersburg State University of Information (20)	
Vuztelecomcentre (8)	
Intertelecomservice Ltd. (4)	
Smolny PBX (4)	
Selectel Network (2)	
National Research Center Kurchatov Institute (1)	
RU-CENTER (1)	АО «Региональный Сетевой Информационный Центр», крупнейший регистратор доменных имён и хостинг-провайдер в России.
State Unitary Enterprise ATS Smolnogo (1)	Смольный, инфраструктура Правительства Санкт-Петербурга. Вероятно, сетевой сегмент, предоставленный вузу для связей с городскими системами.
Z-Telecom Network	

3.3. Необходимо открыть подраздел «Top Products» (перейти по ссылке «More…»), проанализировать информацию, представленную на странице, и внести в отчет. Раздел «Top Products» предоставляет сводку по названиям программного обеспечения или устройств (например, nginx, OpenSSH т.д.), используемым в организации (см. рисунок ниже).



Нужно выбрать 5 сервисов, наиболее критичных с точки зрения возможности взлома (по вашему мнению). В отчет вставляем **полностью заполненную** таблицу (дополнительно к скриншотам):

Название ПО	Краткое описание того, какие возможности предоставляются злоумышленнику

3.4. Выбрать аналог Shodan'a: Censys **ИЛИ** Netlas (что-то одно; оба сервиса работают только через VPN) и самостоятельно попробовать несколько возможностей («фич»), предоставляемых этими сервисами (4-7 скриншотов с короткими пояснениями, позволяющими увидеть, что вы поработали с сервисом).

Censys больше ориентирован на сертификаты: CT (Certificate Transparency), цепочки, история, множественные домены. По доменному имени не всегда можно установить реальное название организации – на помощь приходит информация о выданных сертификатах (раздел «ISSUER» позволяет посмотреть, какие организации выдавали сертификаты).

Netlas отлично подходит для построения графа связей между доменами, поддоменами, IP-адресами, DNS-записями NS («кто отвечает за домен») и PTR (обратный DNS – показывает какое имя связано с IP-адресом). Может быть удобнее, чем просто список хостов.

3.5. Развиваем цепочку разведки, начиная с поддомена «aip.itmo.ru» (Академия информатики и программирования).

Для этого в Shodan в строке поиска вводим следующий фильтр «***hostname:"itmo.ru" http.html:"ifmo"***», копируем IP-адрес из результата выдачи, после чего проверяем скопированный IP в сервисе https://2ip.ru/lookup/. Из результатов выдачи копируем номер автономной сети «ASN (BGP)», и проверяем

его в сервисе https://bgp.he.net/ , переходим на вкладку «Prefixes v4» (в bgp.he.net). Из результатов видно, что:

- часть инфраструктуры ИТМО находится на IP- из представленных диапазонов (собственная адресная ёмкость), остальная часть – в облаке Яндекса и т.д.
- любые адреса из представленных диапазонов могут принадлежать инфраструктуре университета — сайты, почтовые серверы, VPN, камеры, IoT.
- найденный IP принадлежит автономной системе AS42289 — ITMO University.
- эта AS объявляет несколько IPv4-префиксов, включая основной диапазон 77.234.192.0/19.
- веб-ресурс «Академия информатики и программирования» размещён внутри сетевой инфраструктуры университета.

Результаты отражаем в отчете. Желательно дополнительно указать свою интерпретацию приведенных диапазонов и того, как эта информация может использоваться злоумышленником.

3.6. Промежуточные выводы по первой части лабораторной работы № 3.

Как мы видим, в ИТМО нарушен следующий важный принцип:«*Ни одна система мониторинга не должна быть доступна напрямую из Интернета*».

Grafana/Zabbix нельзя публиковать наружу поскольку:

- Grafana и Zabbix часто имеют слабые пароли или очень часть стандартные учётные записи администраторы забывают поменять.
- Частые уязвимости, например CVE-2023-3128 (Grafana) и CVE-2023-29445 (Zabbix).
- Через панель мониторинга можно увидеть топологию сети, хосты, метрики БД и учётные данные API.

В данном случае самым простым способом уменьшить поверхность атаки является использование промежуточного сервера (jump-host или bastion) для доступа к Graphana извне – в этом случае Grafana не будет иметь публичного IP.

В целом общий подход к уменьшению поверхности атаки таков: нужно держать только нужные сервисы, сегментировать сеть, защищать периметры, управлять доступом.

В таблице ниже представлены требования некоторых зарубежных нормативных документов/стандартов касающихся размещения публичных интерфейсов в открытом доступе.

Раздел зарубежного стандарта (аналог «наших мер»)	**Требование в части размещения публичных интерфейсов в открытом доступе**
NIST SP 800-53, раздел SC-7 Boundary Protection	административные интерфейсы и внутренние панели должны быть изолированы от внешних сетей
CIS, раздел Control 4 (Controlled Use of Administrative Privileges)	административные интерфейсы должны быть выделены в отдельную зону, с ограничением доступа.
OWASP Top 10, раздел A05:2021 (Security Misconfiguration)	открытые административные панели являются типичным примером ошибки конфигурации

В отчете необходимо представить аналогичную таблицу, но только с мерами из Приказа ФСТЭК № 17 и Методического документа «Меры защиты информации…». Там есть меры, которые по смыслу соответствуют
«не выставлять административные интерфейсы / системы мониторинга наружу» и «давать доступ только через контролируемые каналы».

Мера из нормативных документов ФСТЭК (Приказ 17 и Метод.документ)	**Описание меры**
УПД.X	[про сегментирование сети]
УПД.У	[про VPN/бастион-шлюз]
ОПС.Z	
ЗИС.W	

4. Поиск поддоменов организации.

Вспоминаем, что мы занимаемся расширением поверхности атаки. В данном случае работаем с DNS. Способов поиска поддоменов много. Нам предстоит познакомиться с некоторыми из них.

4.0. Подготовка окружения.

Вам потребуется дистрибутив Linux и любой менеджер виртуальных машин. Проще всего использовать Kali Linux – в этом случае у вас не будет «танцев с бубном» при установке необходимых пакетов (например, feroxbuster, но его на Kali Linux ставится одной командой через «apt install»).

Можно Ubuntu. С Debian будут «танцы».

Примечание: для разработки лабораторной работы использовалась архитектура amd64, и, возможно, под другие архитектуры подготовка окружения будет отличаться. Так, на arm64 может сразу не получиться запустить httpx – для этого на гитхабе потребуется выбрать актуальный архив.

Обновляем список доступных пакетов для установки:
sudo apt update

Создаем каталог, в котором будем работать:
mkdir -p ~/osintlab_3/

Переходим в каталог **osintlab_3:**
cd osintlab_3

При работе с очередным инструментом рекомендуется создавать каталог с наглядным именем и работать внутри него.

Устанавливаем необходимые пакеты для выполнения лабораторной работы:
sudo apt install -y tree curl nmap jq gobuster dnsutils seclists dnsrecon

tree – показывает структуру каталогов в виде древовидного списка.

curl – предназначена для отправки HTTP-запросов (GET, POST, PUT, DELETE и др.) по различным сетевым протоколам и получения данных с серверов.

nmap – сетевой сканер: обнаружение хостов, открытых портов, сервисов и базовое определение ОС. Используется для разведки сети.

jq – утилита для парсинга, фильтрации и форматирования JSON в командной строке. Очень удобна при обработке вывода API.

gobuster – инструмент для перебора (brute-forcing) директорий/файлов на веб-сервере и поддоменов (wordlist-based directory/file & DNS bruteforce).

dnsutils – набор утилит для DNS (включая dig, nslookup, host и т.д.) — для запросов к DNS и диагностики.

seclists – коллекция полезных словарей для тестирования безопасности (директории, пароли, поддомены, наборы фраз и т.д.), нам он понадобится для работы gobuster.

dnsrecon – инструмент для автоматизированной DNS-разведки (зоны, записи, перебор поддоменов и т.п.).

Может так случиться, что в вашем дистрибутиве не будет пакета **seclists**. В этом случае ставим его так:

sudo git clone --depth 1 https://github.com/danielmiessler/SecLists.git /usr/share/seclists

Настраиваем права доступа:

sudo chmod -R a+r /usr/share/seclists

sudo find /usr/share/seclists -type d -exec chmod a+rx {} \;

Скачиваем сырой скрипт установки (raw content) пакета **feroxbuster**:

curl -sL https://raw.githubusercontent.com/epi052/feroxbuster/main/install-nix.sh -o install_feroxbuster.sh

Визуально убеждаемся, что в скачанном скрипте нет криминала:

kate feroxbuster (или используем любой другой редактор).

Устанавливаем feroxbuster:

bash install_feroxbuster.sh

Для успешной установки пакета pdtm нам потребуется установить go1.24.3.

(в google class будет лежать скрипт **install_golang.sh** для установки go1.24.3 на Debian).

После установки go1.24.3 проверяем, что всё правильно установилось:

go version

go version go1.24.3 linux/amd64

go env GOROOT GOPATH GOBIN

/usr/local/go
/home/USER_NAME/go
[empty string]

pdtm (**P**roject**D**iscovery **T**ool **M**anager) – лёгкий менеджер для установки, обновления и удаления инструментов ProjectDiscovery:

- nuclei (ставим на перспективу),
- subfinder,
- dnsx,
- httpx,
- naabu,
- katana и др.

Устанавливаем **pdtm**:
go install -v github.com/projectdiscovery/pdtm/cmd/pdtm@latest

Добавляем путь к go в **~/.bashrc**:
*grep -qxF 'export PATH=$PATH:$HOME/go/bin' ~/.bashrc 2>/dev/null || *
* echo 'export PATH=$PATH:$HOME/go/bin' >> ~/.bashrc*

И применяем:
source ~/.bashrc

Проверяем:
which pdtm && pdtm -version

Устанавливаем пакеты nuclei,subfinder,dnsx с помощью pdtm (не забываем при этом отключить ваш VPN):
pdtm -i nuclei,subfinder,dnsx

4.1. Поиск поддоменов с помощью dork-запросов (например, Google Dorks).

Dork-запросы – это специальные поисковые запросы, которые используют операторы расширенного поиска (например, site:, filetype:, intitle:, inurl: и т. д.) для нахождения специфической информации в интернете, в том числе которую владельцы сайтов не собирались делать общедоступной.

Примеры дорк-запросов:

Базовый запрос (ищет все страницы на сайте itmo.ru).
«site:itmo.ru» ограничивает поиск страницами и файлами, размещёнными в домене itmo.ru

site: itmo.ru

Можно с помощью символа подстановки (wildcard) поискать поддомены:
site:*.itmo.ru

Ранее, когда не было средств автоматизации так искали поддомены, последовательно записывая новые поддомены и исключая их в строке поиска:
site:*.itmo.ru -expert -abit -bonustrack
до тех пор, пока результат поиска не окажется пустым.

Интересный дорк-запрос для поиска определенных типов:
site:itmo.ru filetype:txt -site:github.com
filetype:txt просит показать только ресурсы, которые поисковик распознал как текстовые файлы.

Такой запрос находит, например, файл «robots.txt», который часто содержит подсказки о структуре сайта, в том числе запрещает индексацию некоторых путей (но они по-прежнему могут быть доступны по HTTP). Блок Disallow часто подсказывает интересные маршруты.

Ваша задача сформировать несколько дорк-запросов и попробовать интерпретировать полученные результаты с точки зрения пользы, которую может дать данная информация для злоумышленника.

Например, можно попросить ИИ-шку составить bash-скрипт, который проверит доступность всех путей, указанных в блоке Disallow:

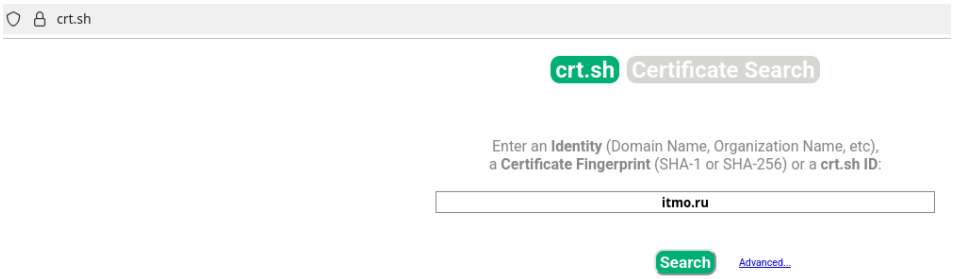
```
kav@bqpc:~/osintlab_3/robots$ ./check_itmo_robots.sh
Проверяю 57 путей — результат в robots_check.csv
200 https://itmo.ru/index.php -> https://itmo.ru/index.php (t=1.127070s)
401 https://itmo.ru/cms/ -> https://itmo.ru/cms/ (t=1.321908s)
401 https://itmo.ru/cms3/ -> https://itmo.ru/cms3/ (t=1.903152s)
401 https://itmo.ru/cms5/ -> https://itmo.ru/cms5/ (t=1.749861s)
200 https://itmo.ru/go.php -> https://itmo.ru/404.html (t=1.037660s)
200 https://itmo.ru/news/2314/ -> https://itmo.ru/ru/viewnews/2314/podvedenie_itogov_pilotnyh_proektov.htm (t=4.023939s)
curl: (28) Resolving timed out after 8322 milliseconds
ERROR https://itmo.ru/panel/
404 https://itmo.ru/module/ -> https://itmo.ru/module/ (t=0.851564s)
200 https://itmo.ru/album/ -> https://media.itmo.ru/ (t=2.757713s)
curl: (6) Could not resolve host: media.itmo.ru2
ERROR https://itmo.ru/album2/
200 https://itmo.ru/en/ -> https://en.itmo.ru/en// (t=2.745012s)
```

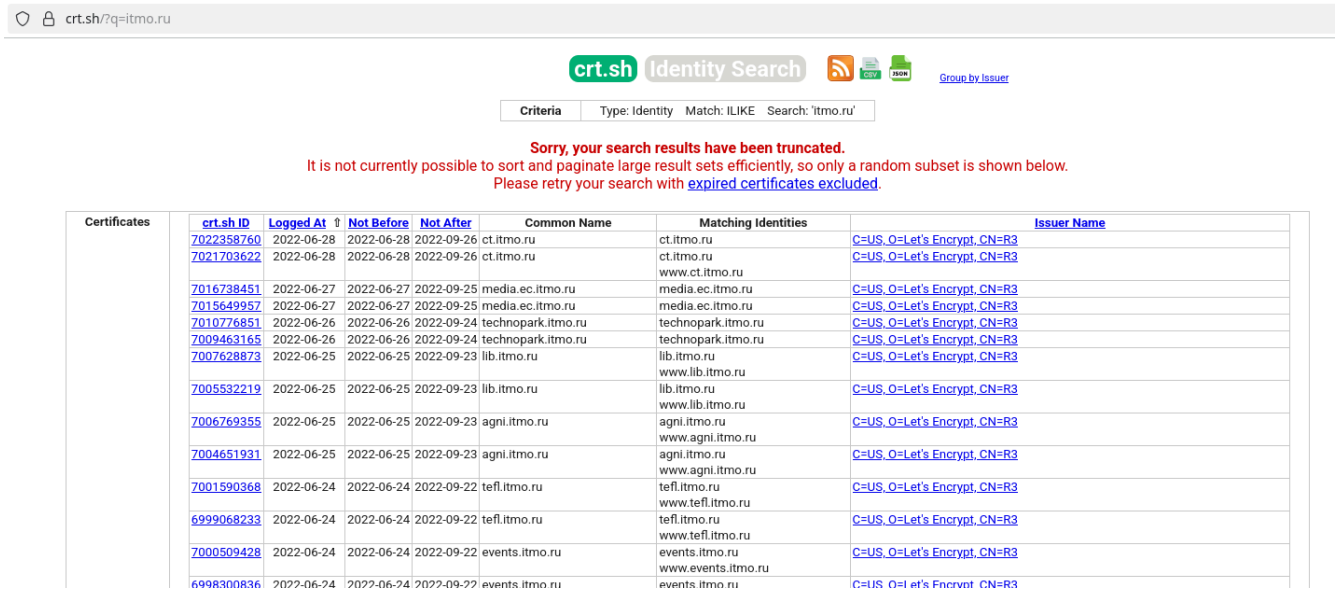
Полученные результаты вставить в отчет.

Если возник интерес к теме, можно зайти на https://www.exploit-db.com/google-hacking-database , выбрать там 2-3 понравившихся dork-запроса, запустить, результаты с кратким описанием (и со скриншотами) внести в отчет.

4.2. Поиск поддоменов с помощью поискового интерфейса crt.sh от центра сертификации Sectigo. **crt.sh** предоставляет доступ к открытой системе журналов Certificate Transparency (CT), в которой публично фиксируются все выданные TLS/SSL-сертификаты.

Когда центр сертификации (Certificate Authority, CA) выпускает сертификат для домена, запись об этом попадает в один или несколько CT-логов.





Перейдя по ссылке https://crt.sh/?q=%.itmo.ru вы несколько сотен сертификатов, выданных для доменов ИТМО.

Далее можно скачать полученные результаты в формате json:

И, обработав их в python, получить список поддоменов ИТМО.

Выберите из этого списка несколько поддоменов (2-3), которые могут представлять наибольший интерес для злоумышленника. Вставьте в отчет с краткими пояснениями.

4.3. Поиск поддоменов с помощью инструментов командной строки.

Поиск и использование неправильных настроек DNS-сервера. AXFR.

Зона – это набор DNS-записей для домена (и части его поддоменов): SOA, NS, A/AAAA, MX, TXT, CNAME и т. д.

Zone transfer – общий термин для передачи зоны между авторитетными DNS-серверами.

AXFR – разновидность zone transfer (полный слепок всех записей)

Ниже приведен рисунок с типами записей в инфраструктуре DNS

Common DNS Record Types	
Record	Description
A	Address record (IPv4)
AAAA	Address record (IPv6)
CNAME	Canonical Name record
MX	Mail Exchanger record
NS	Nameserver record
PTR	Pointer record
SOA	Start of Authority record
SRV	Service Location record
TXT	Text record
Axfr	Zone transfer. Includes all records about a domain

Механизм **zone transfer** часто используется для синхронизации записей между DNS-серверами. Этот механизм предоставляет полный список DNS-записей, включая поддомены, IP-адреса и почтовые сервера. Очень часть после синхронизации администратор DNS-зоны забывает отключить эту опцию. Это типичный пример неправильной настройки (misconfiguration), позволяющий злоумышленнику извлечь содержимое всей зоны.

Выполняем проверку AXFR.

dnsrecon -t axfr -d itmo.ru

```
kav@bqpc:~$ dnsrecon -t axfr -d itmo.ru
[*] Checking for Zone Transfer for itmo.ru name servers
[*] Resolving SOA Record
[+]      SOA ns.itmo.ru 77.234.194.2
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS ns5.itmo.ru 51.250.74.203
[+]      NS ns.itmo.ru 77.234.194.2
[+]      NS ns3.itmo.ru 77.234.216.2
[+]      NS ns2.itmo.ru 77.234.221.75
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 51.250.74.203
[+] 51.250.74.203 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 77.234.216.2
[+] 77.234.216.2 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 77.234.194.2
[+] 77.234.194.2 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 77.234.221.75
[+] 77.234.221.75 Has port 53 TCP Open
[-] Zone Transfer Failed ([Errno 104] Connection reset by peer)
```

Как мы видим, на всех DNS-серверах ИТМО механизм **zone transfer** закрыт.

Запускаем dnsrecon со следующими опициями:

dnsrecon -t crt -d itmo.ru -c dnsrecon_crt_output.xls

-d itmo.ru – задаёт целевой домен.

-crt – берёт имена, найденные в выданных сертификатах (через crt.sh), помогает найти поддомены, даже если в самой DNS-зоне они не видны.

-c – сохранить результаты в csv-файле dnsrecon_crt_output.xls.

4.4. Активная разведка поддоменов (процедура формально находится на грани разрешенного).

Ещё одним способом получить список доменов является метод полного перебора по словарю.

Скачиваем словарь:

curl -fSL -C - https://wordlists-cdn.assetnote.io/data/manual/best-dns-wordlist.txt -o best-dns-wordlist.txt

Запускаем перебор доменных имен по словарю:

gobuster dns -d itmo.ru -w best-dns-wordlist.txt -t 16 -r 9.9.9.9 --no-color -q -o gobuster_raw.txt

ПРИМЕЧАНИЕ: если на DNS-сервере используются wildcard-записи (от англ. «подстановочный знак»), например, такие:

```
*.example.com   IN   A   192.0.2.10
```

сервер будет отвечать положительно на каждый запрос поддомена из словаря.

Извлекаем FQDN:

sed 's/^Found:[[:space:]]*//' gobuster_raw.txt > gobuster_subs.txt

Проверяем валидность имен поддоменов – не каждое имя поддомена, полученное по результатам пассивной разведки DNS является валидным (в поисковой системе имя сохранилось, а реально его уже может и не быть).

Для этого передаем на вход dnsx все найденные поддомены itmo.ru и сопоставляем им IP-адреса:

dnsx -l gobuster_subs.txt -a -cname -resp -silent -r 9.9.9.9 -nc -o resolved.txt

Всем реально существующим поддоменам будет сопоставлен IP-адрес.

За этими именами стоит какой-то реально существующий сайт/сервис/приложение – всё это может быть использовано злоумышленником (применить брутфорс к формам аутентификации, поиспользовать уязвимости сайтов и т.д.).

5. Визуальный поиск интересных сервисов с помощью httpx.

Идея: быстро понять «что за сервис», какие коды/заголовки/технологии, и сохранить артефакты (ответы, скриншоты).

Скачиваем инструмент httpx:

```
wget -O httpx.zip \
https://github.com/projectdiscovery/httpx/releases/download/v1.6.10/httpx_1.6.10_linux_amd64.zip
```

Распаковываем архив и переходим в каталог httpx.

Для работы httpx нам потребуется валидированный список доменных имен.

Его можно получить из **resolved.txt**, полученного на предыдущем шаге:

awk '{print $1}' resolved.txt > names.txt

Запускаем:

```
./httpx -l names.txt \
-status-code -title -tech-detect -follow-redirects \
-screenshot -server -ip -cname -store-response -store-chain \
-store-vision-recon-cluster -random-agent \
-o "httpx_scan_$(date '+%Y%m%d_%H%M%S')" -oa -include-chain \
-retries 3 -timeout 30 -screenshot-timeout 30
```

В результате работы httpx в каталоге **output/screenshot** появятся скриншоты с ресурсами, которые удобно визуально просматривать через **screenshot.html** (находится внизу каталога **screenshot**). Просматриваем и делаем выводы (например, увидели форму аутентификации на скриншоте или какой-то интересный сервис, например, Bitrix).

6. Перебор web-директорий (для примера берем **https://git.dc.itmo.ru** – можете взять любой другой информативный URL):

```
./feroxbuster -u "https://git.dc.itmo.ru" \
-w /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt \
-x js,php,txt,json \
-t 50 -k -q -n -r \
-s 200,204,301,302,307,401,403,405 \
-o "ferox_1.txt"
```

Список доступных словарей можно посмотреть в **/usr/share/seclists/Discovery/Web-Content/** и выбрать понравившийся.

В получившемся списке web-директорий могут найтись какие-то интересные скрипты с ошибками, файлы, формы аутентификации («админки») и т.д. – всё это увеличивает поверхность атаки.

7. Факультативно. Автоматизация: subfinder с API (Censys, Shodan, Netlas)

Настройка ключей
Создайте конфиг провайдеров:
mkdir -p ~/.config/subfinder
nano ~/.config/subfinder/provider-config.yaml

Находим свой API key в shodan:
- перейти в свой профиль https://account.shodan.io/
- на странице профиля в разделе «Account Overview» будет блок «API Key»

Пример (заполните своими значениями):

```
shodan:
  - key: "SHODAN_API_KEY"

censys:
  - id: "CENSYS_API_ID"
    secret: "CENSYS_API_SECRET"

netlas:
  - key: "NETLAS_API_KEY"
```

Запуск:
subfinder -d itmo.ru -all -silent -o subfinder_subs.txt