Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

Факультет безопасности информационных технологий

Дисциплина:

«Теория информационной безопасности и методология защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

«Исследование баз данных угроз и уязвимостей. Калькулятор уязвимостей»

Выполнил:

студент группы N3246,

Суханкулиев Мухаммет

(подпись)

Проверила:

Коржук Виктория Михайловна,

доцент (квалификационная категория "ординарный доцент")

(отметка о выполнении)

(подпись)

Санкт-Петербург

2024 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель работы – получить знания и навыки работы с различными базами данных угроз и уязвимостей. Изучение принципов оценки уязвимостей с использованием калькулятора CVSS.

Для достижения поставленной цели необходимо решить следующие задачи:

- Ознакомиться с обязательным материалом, представленным в задании к лабораторной работе.
- Изучить и проанализировать пять баз данных угроз и уязвимостей.
- Провести расчет оценки уязвимостей с использованием калькулятора CVSS.

1 ИССЛЕДОВАНИЕ БАЗ ДАННЫХ УГОЗ И УЯЗВИМОСТЕЙ

Банк данных угроз безопасности — это сведения об основных угрозах и уязвимостях, которые характерны для автоматизированных систем управления, государственных информационных систем, а с недавних пор применимы и для информационных систем персональных данных.

1.1 ФСТЭК

ФСТЭК (Федеральная служба по техническому и экспортному контролю) России занимается защитой государственной информации и контролем за экспортом технологий и продукции, которые могут быть использованы в военных целях. ФСТЭК России взаимодействует с государственными и частными организациями, международными структурами, научными и образовательными учреждениями, а также общественными и профессиональными организациями. Это позволяет эффективно координировать действия по обеспечению информационной безопасности и адаптироваться к новым киберугрозам.

1.1.1 Банк данных угроз безопасности информации ФСТЭК

База данных ФСТЭК России включает несколько ключевых блоков информации, которые обеспечивают комплексный подход к анализу и управлению угрозами и уязвимостями в информационных системах:

1. **Угрозы** (на данный момент 222 шт.)
    a. Описание угрозы
    b. Источники угрозы. (Тип нарушителя и его минимально необходимый функционал (потенциал))
    c. Объект воздействия
    d. Последствия реализации угрозы
2. **Уязвимости** (на данный момент 60210 шт.)
    a. Описание уязвимости
    b. Компания, ПО в котором обнаружена уязвимость
    c. Тип ошибки и класс уязвимости, обнаруженной в программном обеспечении
    d. Уровень опасности уязвимости
    e. Возможные меры по устранению уязвимости
    f. Информация об устранении

g. Прочая информация…

3. **Тестирование обновлений**

   Раздел, в котором предоставляется информация о тестировании обновлений различного ПО.

   a. Информация о тестируемом объекте

   b. Результаты тестирования

4. **Документы**

   В этом разделе собраны различные нормативные акты, инструкции, методические указания, технические стандарты и другие официальные документы, которые регламентируют деятельность в области защиты информации.

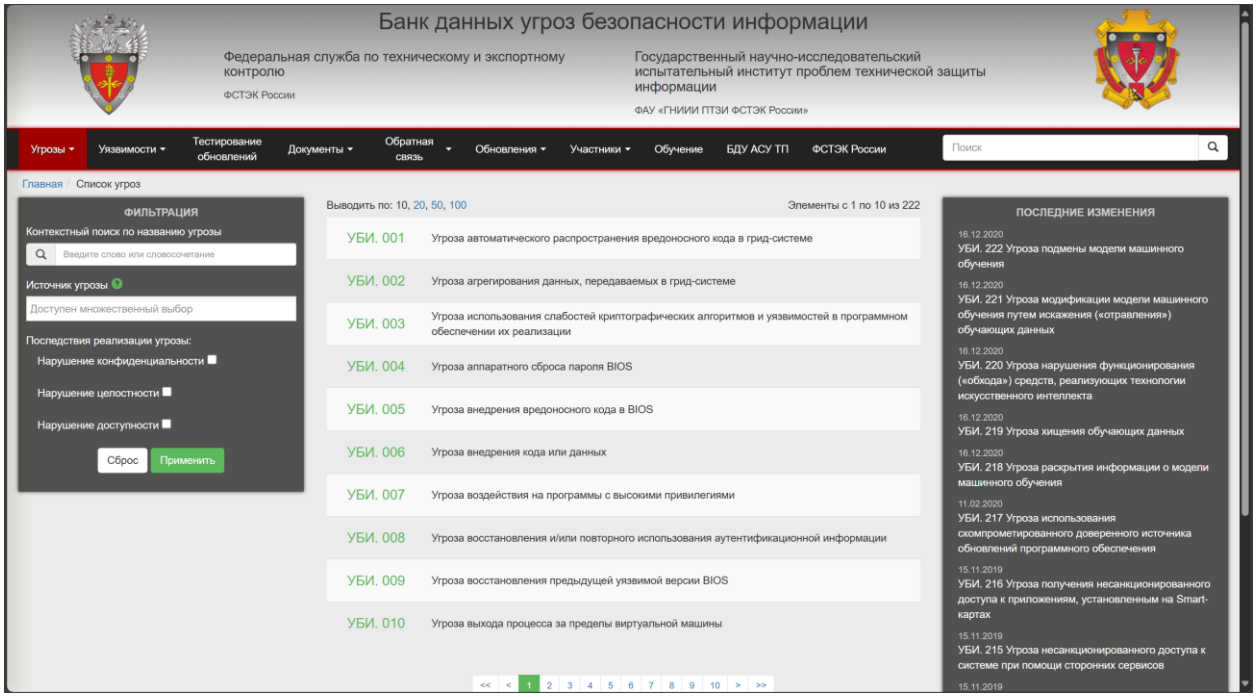

Рисунок 1 – Скриншот главной страницы bdu.fstec.ru

Так же стоит учесть некоторые проблемы ФСТЭК, среди которых выделяются:

1. **Спорная легитимность**: Методика ссылается на устаревшие постановления, что ставит под сомнение её актуальность.
2. **Привязка к персональным данным**: Методика ориентирована только на системы, работающие с персональными данными, что затрудняет её применение для ГИС и других систем.
3. **Отсутствие связи с БДУ ФСТЭК**: это приводит к несоответствиям с современными нормативными актами.

1.2 CVE (NVD)

Миссия программы **CVE** (Common Vulnerabilities and Exposures) ® заключается в выявлении, определении и каталогизации публично раскрытых уязвимостей кибербезопасности. Каждой уязвимости присваивается уникальный идентификатор CVE, который упрощает процесс их идентификации и поиска информации.

На основе базы CVE формируется **NVD** (National Vulnerability Database) — это национальная база уязвимостей, управляемая Национальным институтом стандартов и технологий США (NIST).

1.2.1 Основные компоненты CVE:

- Уникальные идентификаторы для уязвимостей (CVE-идентификаторы);
- Краткое описание уязвимости;
- Дата публикации и исправления;
- Оценка по CVSS (Common Vulnerability Scoring System).

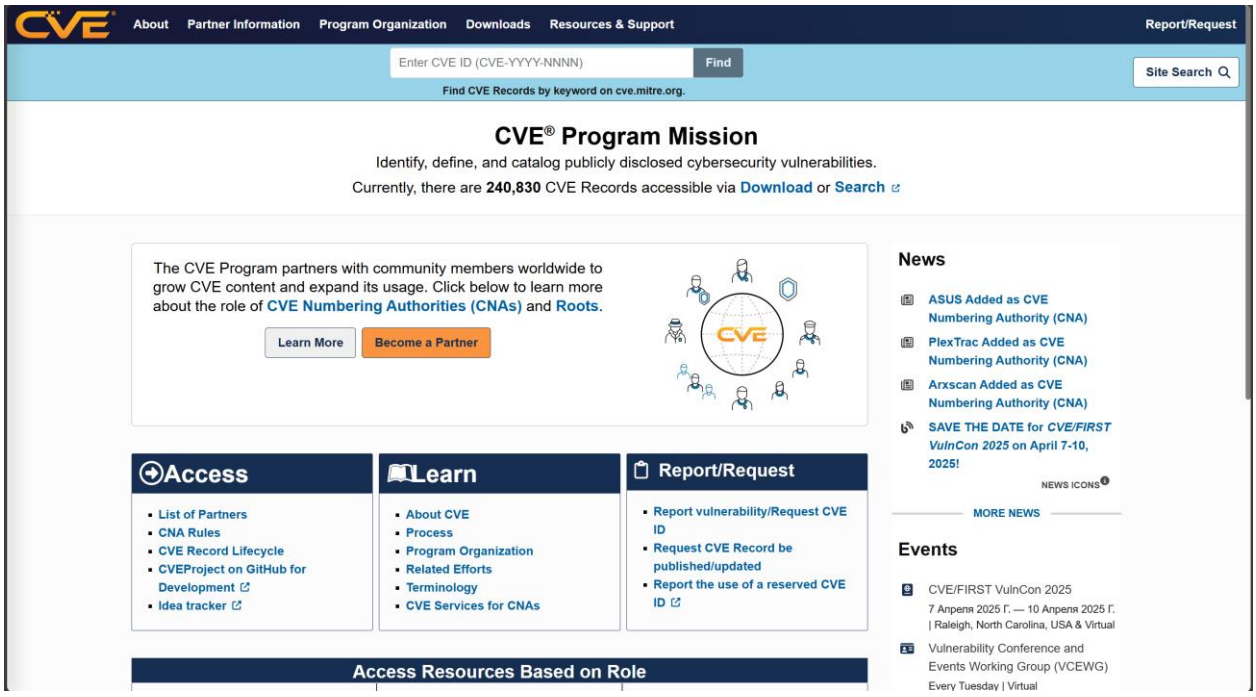

Рисунок 2 – Скриншот главной страницы www.cve.org

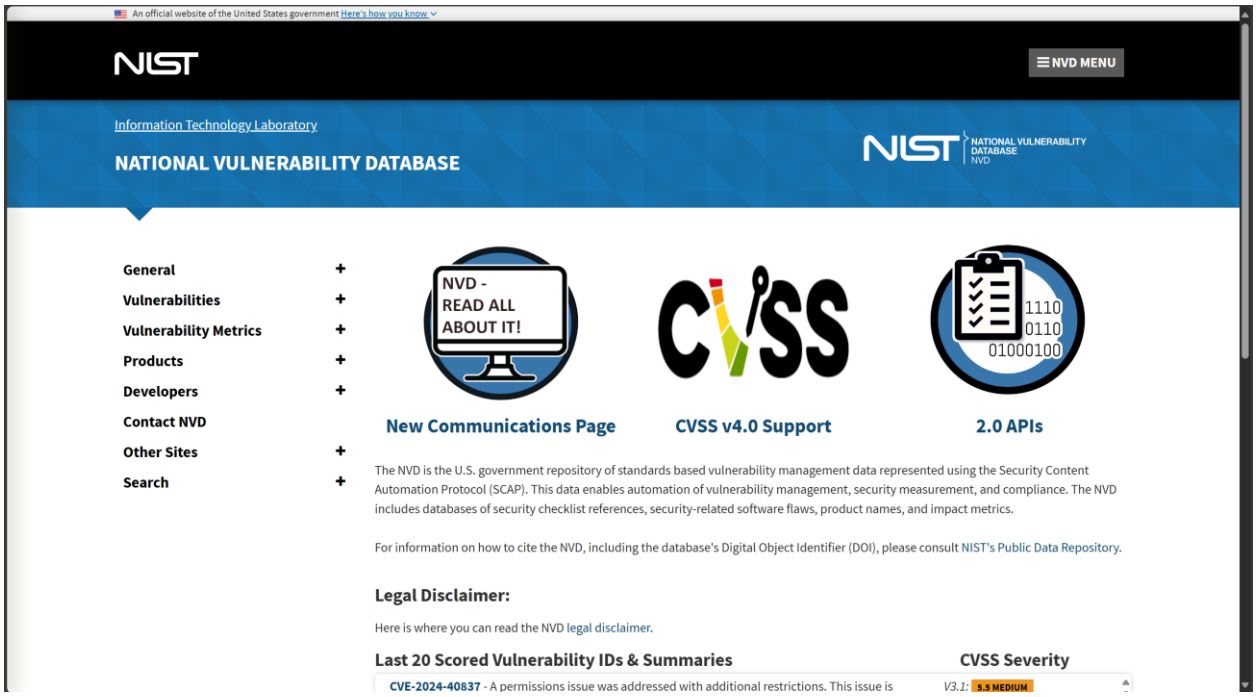

Рисунок 3 – Скриншот главной страницы nist.gov

1.3 Vulners

Vulners — это платформа для поиска и анализа уязвимостей, которая собирает и агрегирует данные из множества различных источников

1.3.1 Основные возможности Vulners:

- Позволяет искать уязвимости по ключевым словам, CVE-идентификаторам и другим параметрам.
- Система может быть интегрирована с решениями для управления событиями информационной безопасности (**SIEM**), что помогает автоматизировать процесс управления уязвимостями.
- Предоставляет информацию о метриках CVSS для более точной оценки уровня опасности уязвимостей.
- Предоставляет информацию о доступных эксплойтах для обнаруженных уязвимостей, что позволяет оценить вероятность и способы их эксплуатации.
- Платформа имеет API для автоматизированного сбора данных и интеграции с другими системами безопасности.

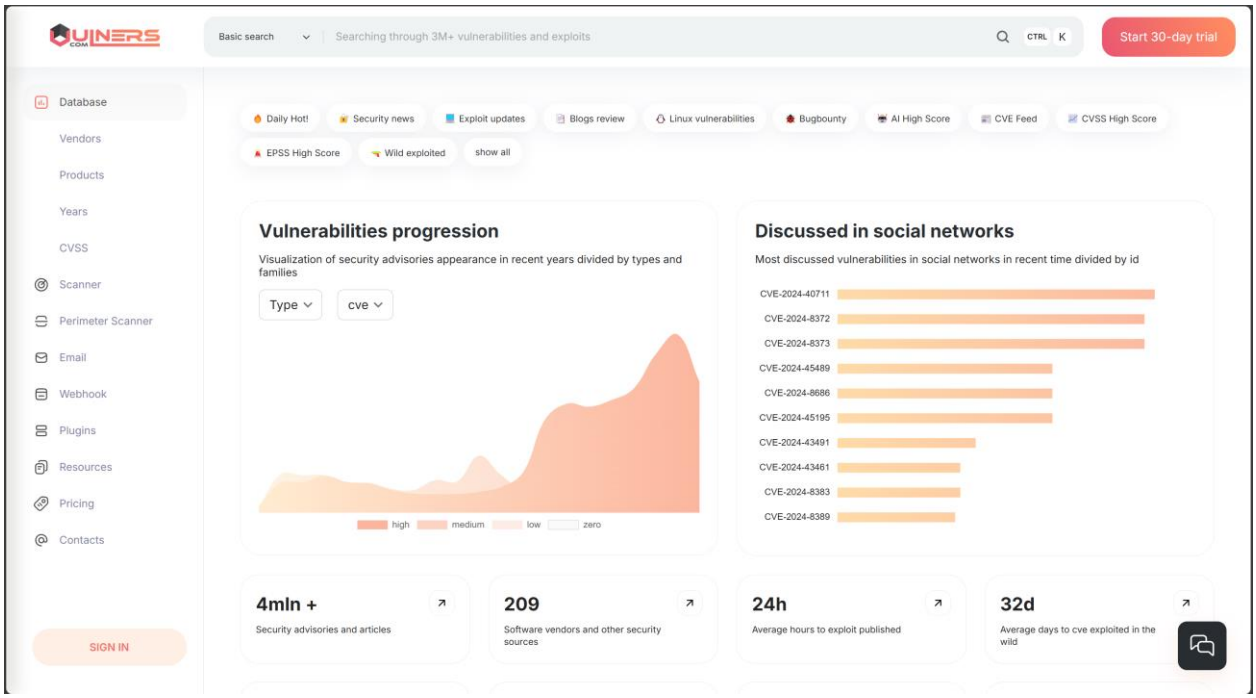

Рисунок 4 – Скриншот главной страницы vulners.com

1.4 Exploit-DB

Exploit-DB — это публичная база данных эксплойтов, которая предоставляет пользователям доступ к информации о готовых эксплойтах, используемых для эксплуатации известных уязвимостей.

1.4.1 Основные возможности Exploit-DB:

- Включает тысячи проверенных эксплойтов для программного обеспечения и операционных систем.
- Позволяет искать эксплойты по ключевым словам, категориям и CVE-идентификаторам.
- Exploit-DB тесно интегрирован с фреймворком Metasploit, что делает возможным автоматическое использование эксплойтов для тестирования безопасности.
- Эксплойты классифицируются по типам уязвимостей (например, переполнение буфера, SQL-инъекции), что упрощает их поиск и анализ.

Информация из официального сайта: **SearchSploit** – Руководство

В наш репозиторий Exploit Database на GitLab включен searchsploit, инструмент поиска из командной строки для Exploit-DB.

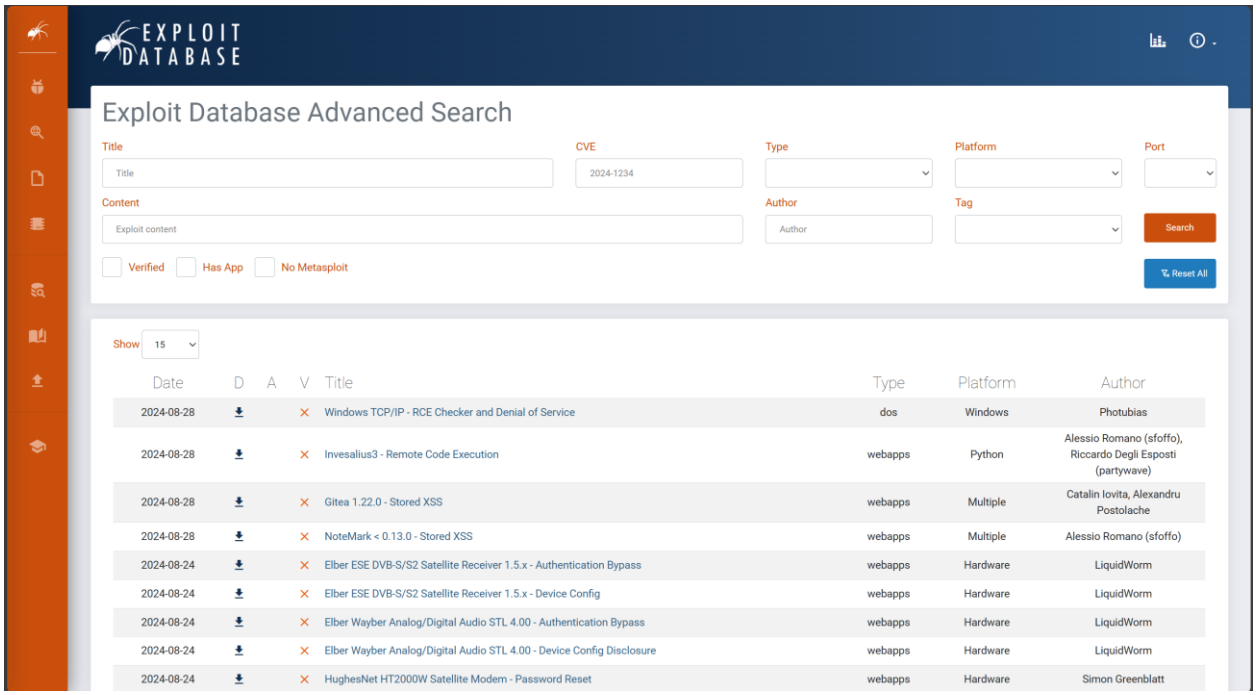

Рисунок 5 – Скриншот главной страницы exploit-db.com

1.5 X-Force

IBM® X-Force Exchange — это облачная платформа для обмена информацией об угрозах, с помощью которой можно быстро исследовать новейшие глобальные угрозы безопасности, собирать полезную информацию, консультироваться с экспертами и сотрудничать с коллегами.

1.5.1 Основные возможности X-Force:

- Обширная библиотека угроз: Включает сведения о тысячах известных киберугроз и уязвимостей.
- Платформа предоставляет актуальные данные и аналитику о новых и появляющихся угрозах.
- Платформа может быть интегрирована с другими продуктами IBM для защиты информации, такими как QRadar и IBM Resilient.
- Пользователи могут совместно обсуждать и анализировать угрозы, обмениваясь информацией с другими специалистами по безопасности.
- X-Force предоставляет API для доступа к данным об угрозах и их автоматизированного использования в системах безопасности.

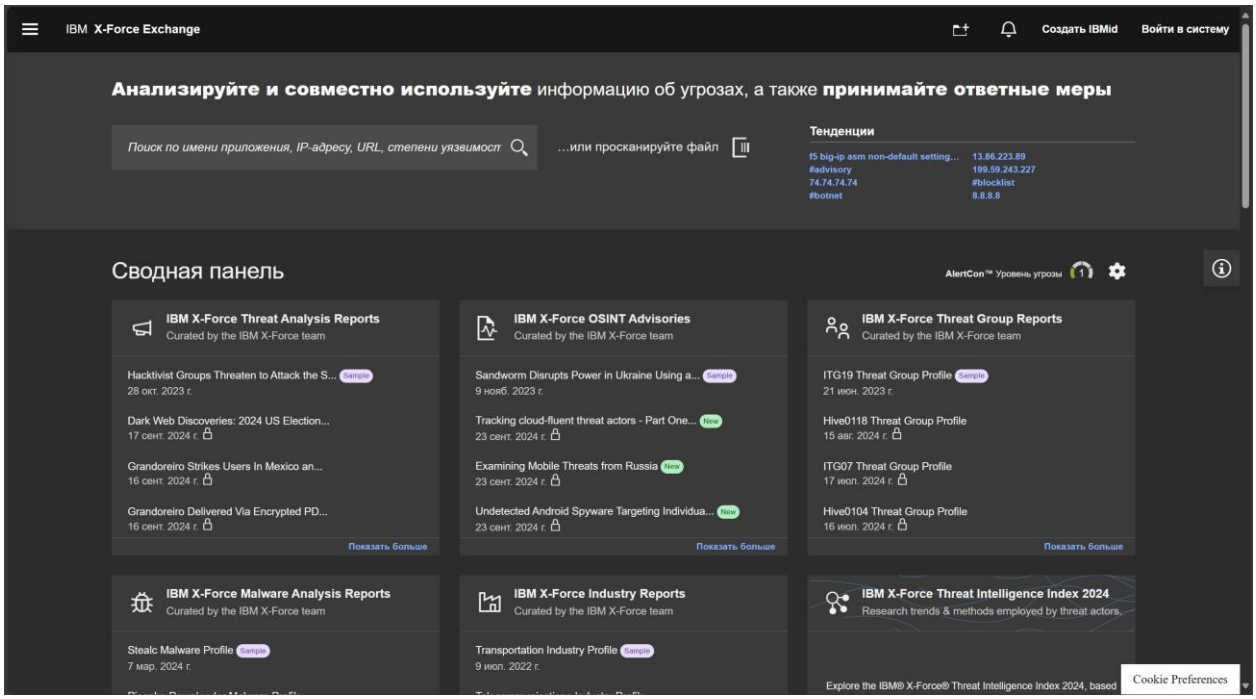

Рисунок 6 – Скриншот главной страницы ibmcloud.com

2 КАЛЬКУЛЯТОР CVSS. МЕТРИКИ

Common Vulnerability Scoring System — открытый стандарт, используемый для расчета количественных оценок уязвимости в безопасности компьютерной системы, обычно с целью понять приоритет её исправления.

2.1 Оценка уязвимости по базовым метрикам (в)

Ситуация: Атака высокой сложности будет проводиться на физический уровень системы, при этом оказывается влияние на другие компоненты системы. Однако атака приводит только к нарушению всех свойств ИБ низкого уровня. Взаимодействие с пользователем не требуется, а уровень привилегий - низкий.

Базовая оценка (BS): 4.5

2.2 Оценка уязвимости по временным метрикам (в)

Ситуация: Предполагается, что есть PoC-код для средств эксплуатации, не определена доступность средств устранения и подтверждена степень доверия к источнику информации об уязвимости.

Временная оценка (TS): 4.3

2.3 Оценка уязвимости по контекстным метрикам (в)

Ситуация: К уровню обеспечения КЦД заданы высокие требования, влияние на них также оказывается высоким. При этом проводится атака низкой сложности на локальный уровень системы. Уровень привилегий в данном случае - высокий, взаимодействия с пользователем не происходит. Оказывается ли влияние на другие компоненты системы - неизвестно.

Контекстная оценка (ES): 7

Вектор CVSS v3:

(AV:P/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:X/RC:CCR:H/IR:H/AR:H/MAV:L/MAC:L/MPR:H/MUI:N/MC:H/MI:H/MA:H)

2.4 Отличия CVSS v3 и v4

CVSS 4.0 имеет более тонкую детализацию, достигаемую за счет введения новых базовых метрик и значений, которые позволяют улучшить систему оценки: чем больше метрик используется для оценки уязвимости, тем качественнее она будет.

Одним из ключевых улучшений CVSS v.4.0 является внедрение более точной детализации в ее базовых метриках.

1. Новая базовая метрика “**Требования к атаке (AT)**”, которая разделяет предыдущую метрику “Сложность атаки (AC)” на две.
2. В CVSS v4.0 показатель "Взаимодействие с пользователем (UI)" теперь имеет показатели: **None (N)**, **Passive (P)**, **Active (A)**.
3. Показатель "Область применения (S)" был отменен в пользу двух наборов показателей воздействия, которые отражают дополнительные аспекты риска, такие как:
    - Влияние уязвимости на систему – **конфиденциальность (VC), целостность (VI), доступность (VA)**.
    - Влияние на последующую систему (системы) – **конфиденциальность (SC), целостность (SI), доступность (SA)**.
4. С новой версией CVSS произошли изменения в названии группы временных метрик.
5. В CVSS v.4.0 внесена новая необязательная группа показателей, называемая **“Дополнительная группа метрик”**. Группа включает в себя показатели, которые описывают и измеряют дополнительные внешние атрибуты уязвимости: Безопасность (S), Возможность автоматизации (AU), Восстановление (R), Контроль над ресурсами (V), Усилия по реагированию (RE), Срочность устранения уязвимости (U).

ЗАКЛЮЧЕНИЕ

В ходе работы были изучены различные базы данных угроз и уязвимостей, а также проведен расчет оценки уязвимостей с использованием калькулятора CVSS. Это позволило получить и закрепить навыки работы с базами данных угроз и уязвимостей, а также понять принципы оценки уязвимостей и приоритезации их исправления.

Полученные знания и навыки будут полезны для дальнейшей учебы в области информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Google-диск – 24/25 ТИБиМЗИ - Ретроспективный анализ подходов к формированию множества угроз информации - https://drive.google.com/file/d/11fXC8dlwv-krVRNaloXpFFVb6ZRS7q5_/view?usp=sharing (дата обращения: 11.09.2024)
2. Google-диск – 24/25 ТИБиМЗИ – Методический документ: Методика оценки угроз безопасности информации – https://drive.google.com/file/d/12hfnnuQpKGi85KcCYPZX87DfLrLCGXbO/view?usp=sharing (дата обращения: 11.09.2024)
3. Проблемы действующей методики определения актуальных угроз от ФСТЭК / Хабр (habr.com) (дата обращения: 09.09.2024)
4. Что такое банк угроз ФСТЭК? | RTM Group (rtmtech.ru) (дата обращения: 09.09.2024)
5. bdu.fstec.ru/threat (дата обращения: 09.09.2024)
6. Оценка уязвимостей CVSS 3.0 / Хабр (habr.com), (дата обращения: 10.09.2024)
7. Сравнение CVSS v.3.1 и v.4.0 / Хабр (habr.com) (дата обращения: 10.09.2024)
8. Common Vulnerability Scoring System — Википедия (wikipedia.org) (дата обращения: 10.09.2024)
9. Common Vulnerability Scoring System Version 4.0 Calculator (first.org) (дата обращения: 10.09.2024)
10. Меряем уязвимости: классификаторы и метрики компьютерных брешей — Хакер (xakep.ru) (дата обращения: 23.09.2024)
11. Overview | CVE (дата обращения: 23.09.2024)
12. NVD - Home (nist.gov) (дата обращения: 23.09.2024)
13. Vulners — Гугл для хакера. Как устроен лучший поисковик по уязвимостям и как им пользоваться / Хабр (habr.com) (дата обращения: 23.09.2024)
14. CVE Database - Security Vulnerabilities and Exploits | Vulners.com (дата обращения: 23.09.2024)
15. Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers (exploit-db.com) (дата обращения: 23.09.2024)
16. IBM X-Force Exchange (ibmcloud.com) (дата обращения: 23.09.2024)