

**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

Выполнил:
Студент гр. Р32151
Соловьев Артемий Александрович

Проверил:
Кондратенко С. С.,
аспирант ФБИТ

Санкт-Петербург 2023г.

Цель работы: получить знания и навыки работы с различными базами данных угроз и уязвимостей.

Объекты:

1. Обязательный материал для ознакомления:

1. <https://habr.com/ru/company/pt/blog/266485/>
2. <https://habr.com/ru/company/ic-dv/blog/453756/>
3. <https://xakep.ru/2009/05/15/48221/#toc01>.
4. <https://habr.com/ru/company/xakep/blog/305262/>

2. БД угроз и уязвимостей:

1. Vulners - База данных уязвимостей, в которой содержится миллионы CVE, эксплойтов и статей по безопасности, которая предоставляет различные инструменты и услуги для управления уязвимостями.

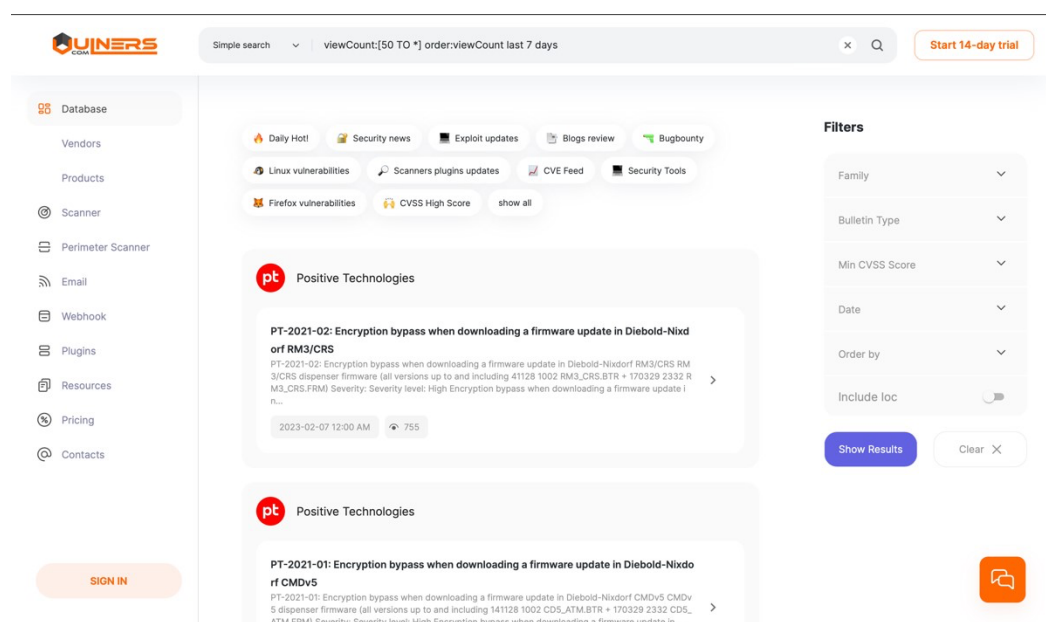


Рисунок 1 Вид Vulners

2. CVE (NVD) – это "словарь" известных уязвимостей, имеющий строгую характеристику по описательным критериям.

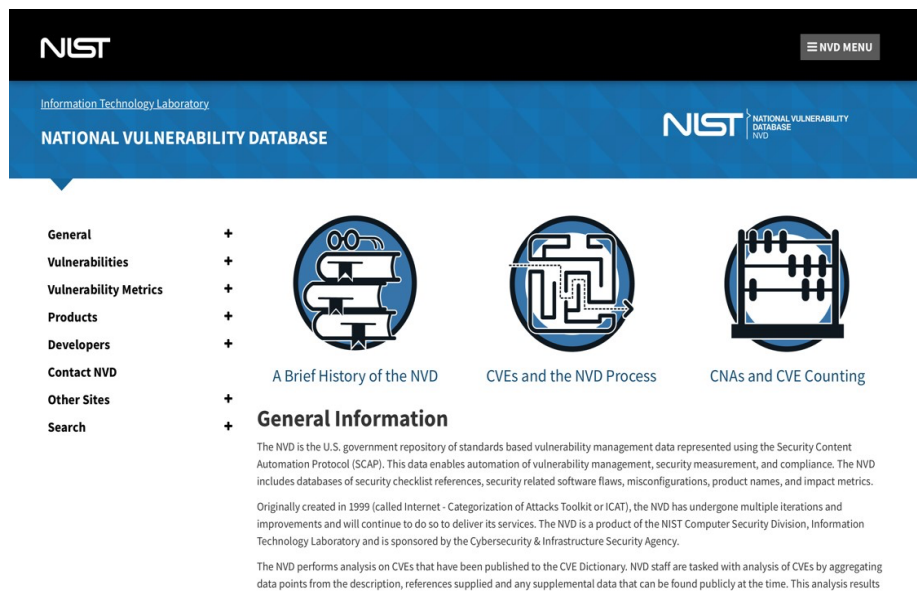


Рисунок 2 Вид CVE(NVD)

3. secunia – Эта датская компания, лента уязвимостей которой доступна по адресу уже заработала себе достаточно славы. Не сказать, чтобы их портал внес какую-то особую, добавочную классификацию, но именно он предлагает услуги платной подписки на базу уязвимостей.

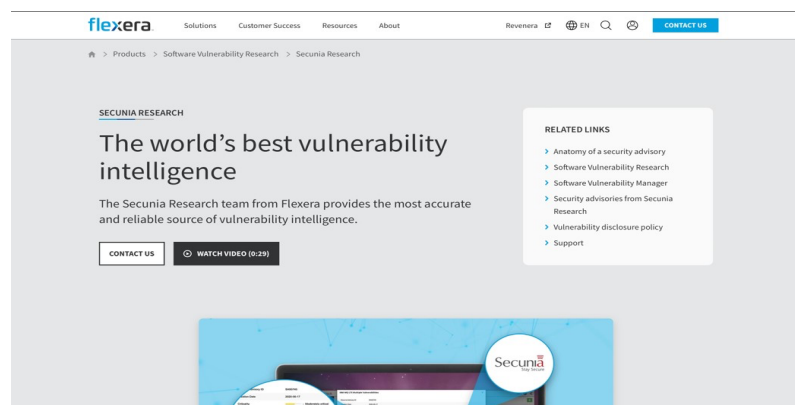


Рисунок 3 Вид secunia

4. SecurityFocus был новостным онлайн-порталом компьютерной безопасности и поставщиком услуг информационной безопасности. Среди обозревателей и авторов SecurityFocus был известный список рассылки Bugtraq, в том числе бывший прокурор Министерства юстиции по киберпреступлениям

Марк Раш и хакер, ставший журналистом Кевин Поулсен.

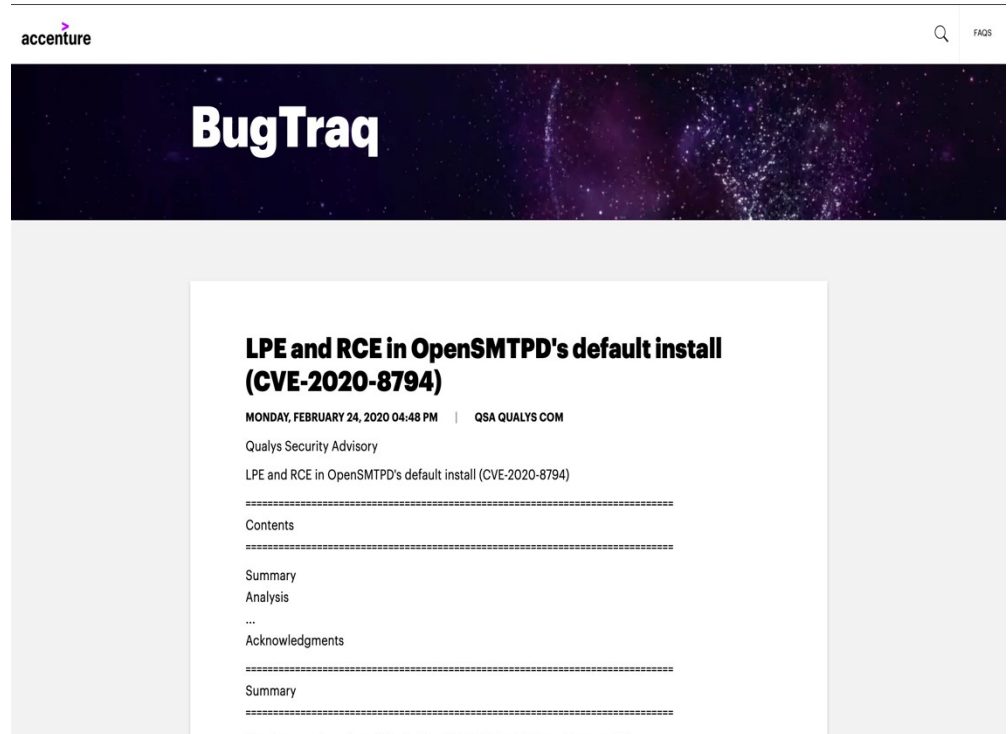


Рисунок 4 Вид SecurityFocus

5. CNNVD – Китайская национальная база данных уязвимостей. Национальная база данных уязвимостей Китайской Народной Республики. Он работает по адресу <https://www.cnvd.org.cn/> и управляется Китайским центром оценки информационных технологий.



Рисунок 5 Вид CNNVD

Ход работы:

1. Оцените уязвимости по базовым метрикам для ситуации при следующих условиях:

Атака низкой сложности будет проводиться на сетевой уровень системы, при этом оказывается влияние на другие компоненты системы. Атака приводит к нарушению конфиденциальности высокого уровня и доступности низкого уровня. Взаимодействие с пользователем не требуется, а уровень привилегий – низкий.

В описании задачи ничего не сказано про влияние на целостность, из-за чего невозможно запустить калькулятор. (Рисунок 6)

Базовые метрики

Внимание! Для получения результата необходимо выбрать значение каждого критерия!

Вектор атаки (AV):

Сетевой (N) | Смежная сеть (A) | Локальный (L) | Физический (P)

Сложность атаки (AC):

Высокая (H) | Низкая (L)

Уровень привилегий (PR):

Высокий (H) | Низкий (L) | Не требуется (N)

Взаимодействие с пользователем (UI):

Требуется (R) | Не требуется (N)

Влияние на другие компоненты системы (S):

Не оказывает (U) | Оказывает (C)

Влияние на конфиденциальность (C):

Не оказывает (N) | Низкое (L) | Высокое (H)

Влияние на целостность (I):

Не оказывает (N) | Низкое (L) | Высокое (H)

Влияние на доступность (A):

Не оказывает (N) | Низкое (L) | Высокое (H)

Рисунок 6 Недостаточность условий

Исходя из того, что в описании задачи ничего не сказано про влияние на целостность, было решено, что влияние на целостность не оказывает, после чего, получил такой результат (Рисунок 7).

Базовая оценка (BS): 8.5

Базовые метрики 8.5

Базовая оценка (BS): 8.5

Вектор атаки (AV):

Сетевой (N) | Смежная сеть (A) | Локальный (L) | Физический (P)

Сложность атаки (AC):

Высокая (H) | Низкая (L)

Уровень привилегий (PR):

Высокий (H) | Низкий (L) | Не требуется (N)

Взаимодействие с пользователем (UI):

Требуется (R) | Не требуется (N)

Влияние на другие компоненты системы (S):

Не оказывает (U) | Оказывает (C)

Влияние на конфиденциальность (C):

Не оказывает (N) | Низкое (L) | Высокое (H)

Влияние на целостность (I):

Не оказывает (N) | Низкое (L) | Высокое (H)

Влияние на доступность (A):

Не оказывает (N) | Низкое (L) | Высокое (H)

Рисунок 7 Результат работы калькулятора

2. Оцените уязвимости по временным меркам для ситуации при следующих условиях:

Предполагается, что есть сценарий для средств эксплуатации, не определена доступность средств устранения и подтверждена степень доверия к источнику информации об уязвимости.

Исходя из критериев задачи были выбраны соответствующие пункты калькулятора. (Рисунок 8). Получилась временная оценка (TS) 8.3.

Временная оценка (TS): 8.3				
Доступность средств эксплуатации (E):				
Не определено (X)	Высокая (H)	Есть сценарий (F)	Есть PoC-код (P)	Теоретическая (U)
Доступность средств устранения (RL):				
Не определено (X)	Недоступно (U)	Рекомендации (W)	Временное (T)	Официальное (O)
Степень доверия к информации об уязвимости (RC):				
Не определено (X)	Подтверждена (C)	Достоверные отчеты (R)	Отчеты (U)	

Рисунок 8 Результат работы калькулятора

3. Оцените уязвимости по контекстным меркам для ситуации при следующих условиях:

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.

Исходя из заданных параметров атаки были выбраны соответствующие пункты калькулятора (Рисунок 9) . Получилась контекстная оценка (ES) 7.2.

Контекстная оценка (ES): 7.2				
Требования к конфиденциальности (CR):				
Не определено (X)	Низкие (L)	Средние (M)	Высокие (H)	
Требования к целостности (IR):				
Не определено (X)	Низкие (L)	Средние (M)	Высокие (H)	
Требования к доступности (AR):				
Не определено (X)	Низкие (L)	Средние (M)	Высокие (H)	
Вектор атаки (корр.) (MAV):				
Не определено (X)	Сетевой (N)	Смежная сеть (A)	Локальный (L)	Физический (P)
Сложность атаки (корр.) (MAC):				
Не определено (X)		Высокая (H)		Низкая (L)
Уровень привилегий (корр.) (MPR):				
Не определено (X)	Высокий (H)		Низкий (L)	Не требуется (N)
Взаимодействие с пользователем (корр.) (MUI):				
Не определено (X)		Требуется (R)		Не требуется (N)
Влияние на другие компоненты системы (корр.) (MS):				
Не определено (X)		Не оказывает (U)		Оказывает (C)
Влияние на конфиденциальность (корр.) (MC):				
Не определено (X)		Не оказывает (N)		Низкое (L) Высокое (H)
Влияние на целостность (корр.) (MI):				
Не определено (X)		Не оказывает (N)		Низкое (L) Высокое (H)
Влияние на доступность (корр.) (MA):				
Не определено (X)		Не оказывает (N)		Низкое (L) Высокое (H)

Рисунок 9 Результат работы калькулятора

Вывод:

В ходе этой лабораторной работы я узнал о некоторых базах данных известных уязвимостей и о различных метриках компьютерных уязвимостей, а также научился пользоваться калькулятором CVSS V3 для оценки этих метрик.