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 методологии защиты информации.

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

Исследование баз данных угроз и уязвимостей. Калькулятор уязвимостей

Выполнил:

Студент гр. N3249

Шарифуллин Ильдан Айдарович

Проверил:

Якимова Софья Андреевна

Лабораторная работа №1

Исследование баз данных угроз и уязвимостей. Калькулятор уязвимостей

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

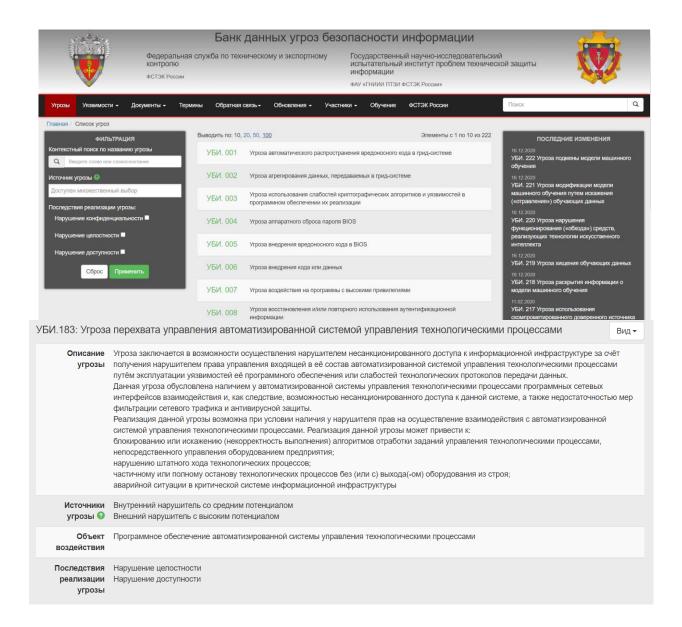
Объекты:

- 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 (описываем 5 БД и прикладываем пару скриншотов):
 - 1. ФСТЭК
 - 2. Vulners
 - 3. CVE (NVD)
 - 4. cert/cc
 - 5. secunia
 - 6. exploit in
 - 7. X-Force
 - 8. SecurityFocus
 - 9. CNNVD
 - 10.JVN
 - 11.https://www.exploit-db.com
- 3. Калькулятор CVSS. Метрики. Выбрать один вариант задачи из каждого блока метрик (задачи а / задачи б и т.д.) и посчитать. (Задачи ниже в текущем документе)

Ход работы:

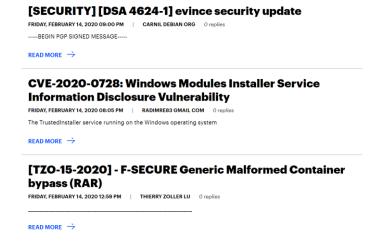
- 1. БД угроз и уязвимостей
 - 1.1. ФСТЭК

БДУ ФСТЭК — некоторый банк угроз безопасности информации содержащий информацию об основных угрозах и уязвимостях (в первую очередь, характерных для государственных ИС и автоматизированных систем управления производственными и технологическими процессами критически важных объектов). Для каждой угрозы даны описание, источники, объект воздействия и последствия реализации угрозы.



1.2. SecurityFocus

SecurityFocus — новостной и информационный портал об ИБ. Это скорее форум, где люди обменивались различными появившимися угрозами и мнениями, по поводу них. Это не полноценная БДУ. На данный момент ресурс не функционирует, последняя новость была добавлена 16 января 2021 года.



[TZO-15-2020] - F-SECURE Generic Malformed Container bypass (RAR) FRIDAY, FEBRUARY 14, 2020 12:59 PM | THIERRY ZOLLER LU From the low-hanging-fruit-department F-SECURE Generic Malformed Container bypass (RAR) Ref : [TZO-15-2020] - F-SECURE Generic Malformed Container bypass (RAR) Status : Patched CVE: none provided Blog: https://blog.zoller.lu/p/tzo-15-2020-f-secure-generic-malformed.html Vulnerability Dislosure Policy: https://caravelahq.com/b/policy/20949 Affected Products F-Secure Email and Server Security F-Secure Internet GateKeeper F-SECURE CLOUD PROTECTION FOR SALESFORCE Linux below 17.0.605.474 Quote: "Unprecedented challenges threaten to undermine the very survival of society. Only

1.3. X-Force

На данный момент БД X-Force по адресу http://xforce.iss.net/ недоступна. По описанию из разных источников:

поиск уязвимостей в базе данных может быть выполнен по нескольким параметрам:

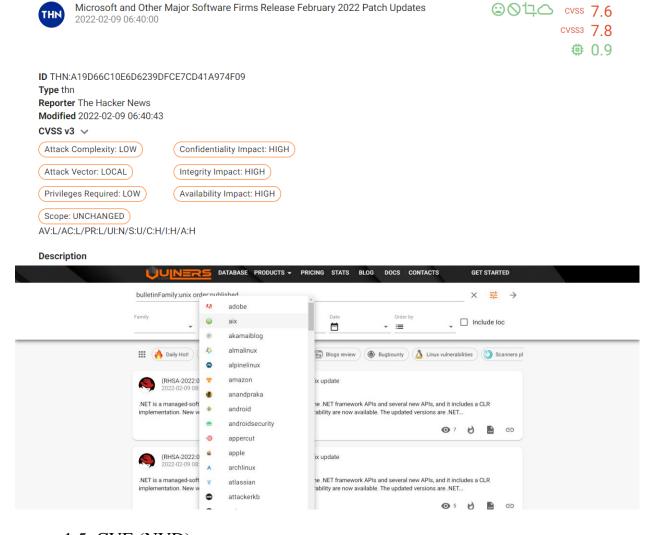
- по операционной системе или платформе, подверженной уязвимости;
- · по имени уязвимости;
- по дате обнаружения;
- · по степени риска (высокая, средняя, низкая).

Также существует возможность вывода всех уязвимостей за последний, предпоследний или несколько предыдущих месяцев. Все обнаруженные уязвимости сразу же заносятся в базы данных уязвимостей системы анализа защищенности сетевых сервисов и протоколов Internet Scanner, системы обнаружения атак RealSecure, систем анализа защищенности операционных систем System Scanner и системы анализа защищенности баз данных Database Scanner.



1.4. Vulners

БД Vulners содержит огромную базу уязвимостей с оценкой по CVSS и CVSS3. Однако здесь нет строгого фильтра по различным параметрам угрозы. Эта БД предназначена скорее для поиска угроз для конкретных семейств программ (что сильно ее отличает от того же ФСТЭК). в Vulners добавляются общие описания уязвимости и других исследовательских центров и центров реагирования: Vulnerability Lab, XSSed, CERT, ICS, Zero Day Initiative, Positive Technologies, ERPScan.



1.5. CVE (NVD)

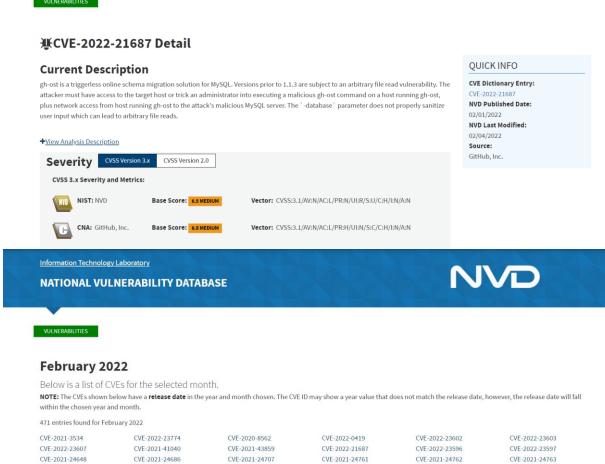
NVD – это хранилище данных управления уязвимостей на основе стандартов правительства США, представленное с использованием протокола автоматизации контента безопасности (SCAP).

Эти данные позволяют автоматизировать управление уязвимостями, измерение безопасности и соответствие требованиям.

NVD включает в себя базы данных контрольных списков безопасности, недостатки программного обеспечения, связанные с безопасностью, неправильные конфигурации, названия продуктов и показатели воздействия.



VULNERABILITIES



2. Расчеты по калькулятору CVSS

CVE-2021-24765

CVE-2021-24926

CVE-2021-25063

CVE-2021-25093

CVE-2022-0220

CVE-2021-24764

CVE-2021-24919

CVE-2021-24983

CVE-2021-25092

CVE-2021-46253

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

CVE-2021-24814

CVE-2021-24937

CVE-2021-25085

CVE-2021-41571

CVE-2022-0401

CVE-2021-24868

CVE-2021-24944

CVE-2021-25089

CVE-2021-43848

CVE-2022-0417

CVE-2021-24900

CVF-2021-24975

CVE-2021-25091

CVE-2021-45416

CVE-2022-23601

CVE-2021-24775

CVE-2021-24934

CVE-2021-25072

CVE-2021-25097

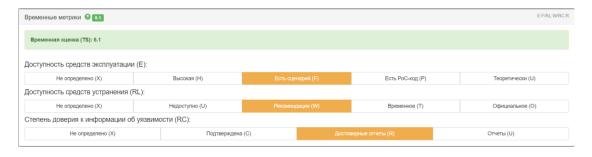
CVE-2022-0320

е) атака высокой сложности будет проводится на сетевой уровень системы, при этом не оказывается влияние на другие компоненты системы. Атака приводит к нарушению конфиденциальности и целостности высокого уровня, доступности низкого уровня. При этом требуется взаимодействие с пользователем, уровень привилегий - низкий.

Sadelie Metpirixi ♥ 💽					
Базовая оценка (BS): 6.7					
Вектор атаки (AV):			Влияние на другие компоненты системы (S):		
Сетевой (N) Смежная	я сеть (A) Локальный (L	Физический (Р)	Не оказывает (U)		Оказывает (С)
Сложность атаки (АС):			Влияние на конфиденциальность (С):		
Высокая (Н)		Низкая (L)	Не оказывает (N)	Низкие (L)	Высокое (Н)
Уровень привилегий (PR):			Влияние на целостность (I):		
Высокий (Н)	Низкий (L)	Не требуется (N)	Не оказывает (N)	Низкие (L)	Высокое (Н)
Взаимодействие с пользователем (UI):			Влияние на доступность (А):		
Требуется (R)	Н	е требуется (N)	Не оказывает (N)	Низкие (L)	Высокое (Н)

2.2 Оцените уязвимости по временным метрикам для ситуации при следующих условиях:

е) Предполагается, что есть сценарий для средств эксплуатации, есть рекомендации для средств устранения, а информация об уязвимостях получена из достоверных отчетов.



2.3. Оцените уязвимости по контекстным метрикам для ситуации при следующих условиях:

е) К уровню обеспечения КЦД заданы высокие требования, однако влияние оказывается низким. При этом проводится атака неопределенной сложности на сетевой уровень системы. Уровень привилегий в данном случае - низкий, взаимодействия с пользователем не происходит. Также оказывается влияние на другие компоненты системы.



Вывод: в ходе лабораторной работы я изучил некоторые БД угроз, и определил, для чего я могу их использовать (например: ФСТЭК – угрозы, характерные для гос. ИС, имеют более общее описание, а Vulners – угрозы различных ПО, имеющие конкретные оценки и описания). Далее для разных сценариев я с помощью калькулятора CVSS посчитал базовые, временные и контекстные метрики, показатели которых (для моего сценария) оказались относительно высокими, а значит данные сценарии требовали относительно быстрого реагирования на эти уязвимости.