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.](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:

Чтобы быть хорошим безопасником, нужно легко находить информацию и замечать мелочи. Например, какие статусы могут быть у уязвимости в базе данных, когда был придуман калькулятор CVSS и много, много чего еще…

Вывод по работе.

Калькулятор уязвимостей CVSS V3 https://bdu.fstec.ru/calc3

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

а) атака высокой сложности будет проводится на физический уровень системы, при этом оказывается влияние на другие компоненты системы. Однако атака приводит только к нарушению целостности высокого уровня. Взаимодействие с пользователем не требуется, а уровень привилегий - низкий.

б) атака высокой сложности будет проводится на физический уровень системы, при этом оказывается влияние на другие компоненты системы. Однако атака приводит только к нарушению целостности высокого уровня и доступности низкого. Взаимодействие с пользователем не требуется, а уровень привилегий - низкий.

в) атака высокой сложности будет проводится 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.

г) атака низкой сложности будет проводится 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.

д) атака низкой 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. Взаимодействие с пользователем не требуется, а уровень привилегий - высокий.

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.

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

а) Предполагается высокий уровень доступности средств эксплуатации, не определена доступность средств устранения и подтверждена степень доверия к источнику информации об уязвимости.

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

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

г) Предполагается, что есть сценарий для средств эксплуатации, средства устранения недоступны и подтверждена степень доверия к источнику информации об уязвимости.

д) Предполагается, что есть сценарий для средств эксплуатации, есть рекомендации для средств устранения и подтверждена степень доверия к источнику информации об уязвимости.

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

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

а) К уровню обеспечения КЦД заданы низкие требования, однако влияние на них 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.

б) К уровню обеспечения КЦД заданы средние требования, однако влияние 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.

в) 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.

г) К уровню обеспечения КЦД заданы высокие требования, однако влияния оказывается низким. 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.

д) К уровню обеспечения КЦД заданы высокие требования, однако влияние оказывается низким. При этом проводится атака высокой сложности на сетевой уровень системы. Уровень привилегий в данном случае - высокий, взаимодействия с пользователем не происходит. Оказывается ли влияние на другие компоненты системы - неизвестно.

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.