НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО”

КАФЕДРА АВТОМАТИЗОВАНИХ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ І УПРАВЛІННЯ

Практична робота № 7

з дисципліни

“Основи захисту інформації”

Варіант 4

Виконала:

студентка групи ІС-71

Вознюк О. В.

Перевірив:

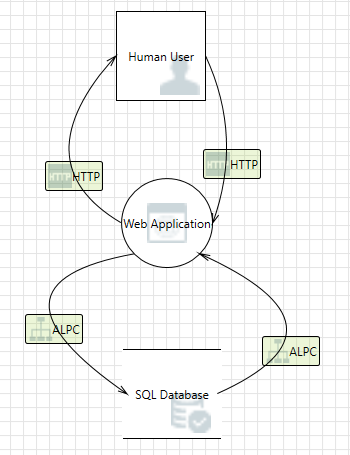
аспірант

Ільїн К. І.

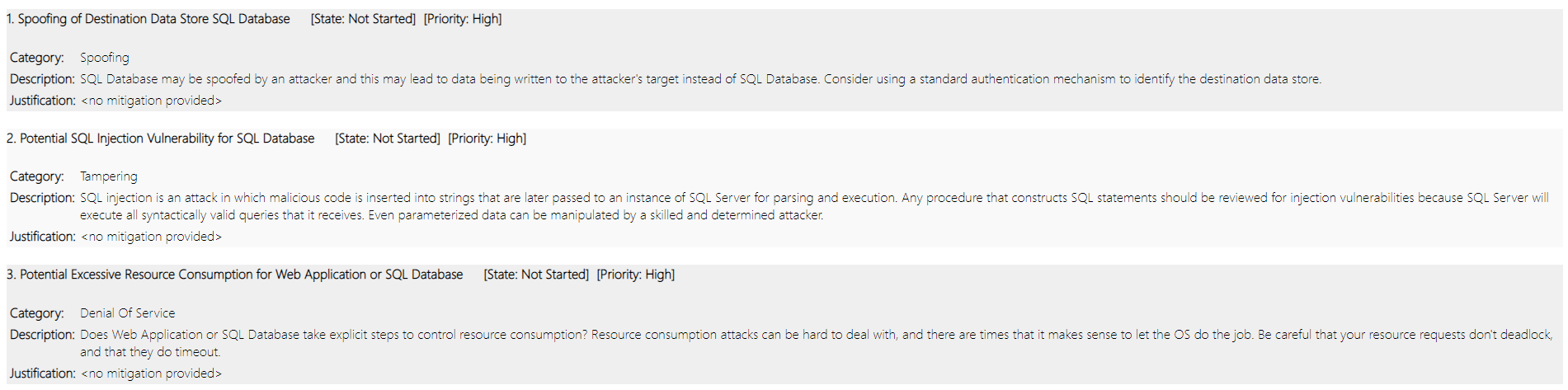
Київ-2020

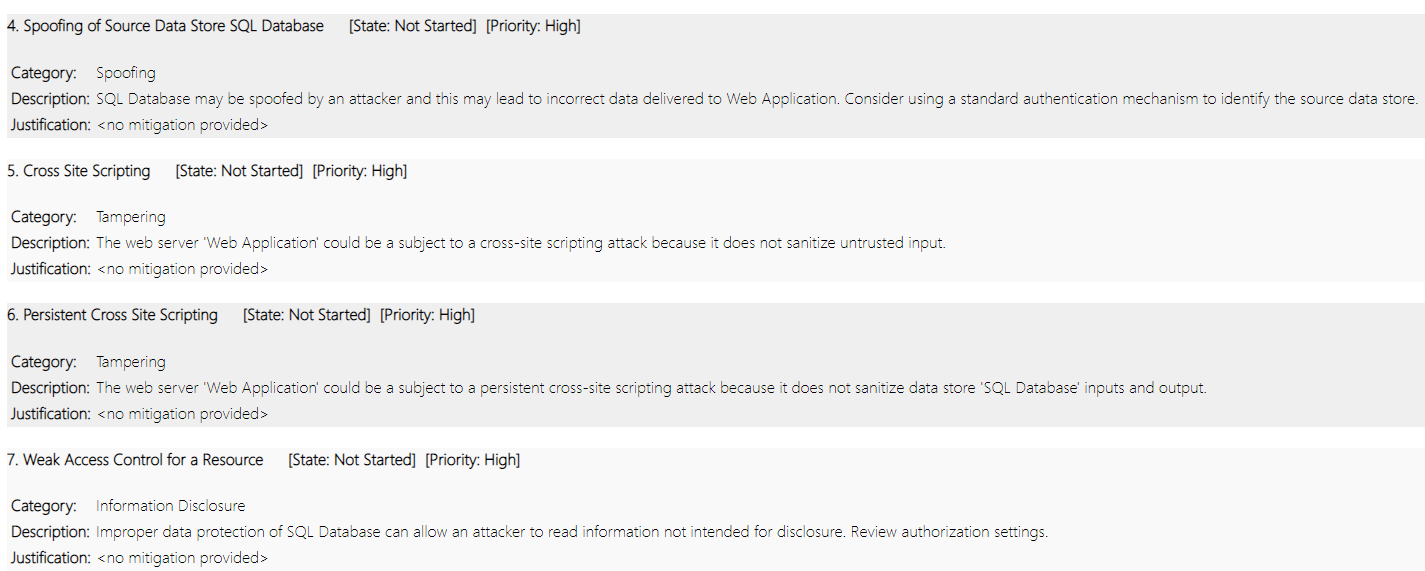
**Хід виконання роботи**

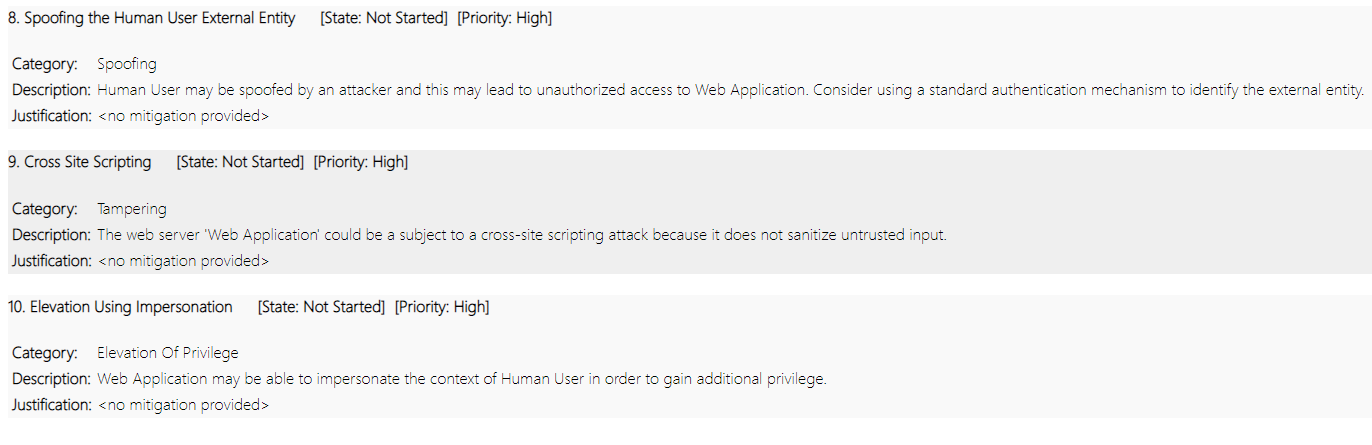
Спочатку використовуючи Microsoft SDL Threat Modeling побудуємо діаграму інформаційних потоків у мережі факультету.



Далі наводяться скріншоти згенерованого звіту з можливи загрозами, а також їх категорією і описом.







Модель порушника

|  |  |  |  |
| --- | --- | --- | --- |
| Категорія Порушника | Кваліфікація | Права в системі | Засоби, якими володіє порушник |
| Адміністратор БД | Висока | Доступ до БД, управління БД, редагування, запис, видалення | СКБД |
| Адміністратор криптографічної підсистеми | Середня | Доступ до системи шифратора, встановлення, зміна, видалення алгоритму шифрування. | Апаратні та програмні інструменти криптографічних систем |
| Оператор | Середня | Обробка інформації, яка міститься в базі даних ІС. | СКБД |
| Адміністратор ОС | Середня | Установка і оновлення ПЗ, підключення і настройка апаратних пристроїв, настройка мережних протоколів і політики безпеки. | Системний засіб управління аудиту |
| Розробник | Висока | Модифікація вихідного коду, проведення тестування ПЗ. | Програмні засоби розробки початкового коду |
| Технічний персонал | Низька | Доступ до приміщень з апаратним і програмним забезпеченням. Обслуговування приміщення. | Ручний інструмент |
| Зовнішній користувач | Низька | Користування ресурсами системи: читання, запис, редагування(поштова скринька), читання(FTP-сервер) | Спеціалізований набір програмних засобів проникнення в систему, через доступні ресурси. |

На основі переліку загроз, притаманних даній інформаційній системі

формується модель загроз у виді таблиці:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Загроза** | **Джерело загрози** | **Імовірніст ь + Наслідки** | **Мета (ресурс + порушення К, Ц, Д чи С Конфіденційність/ Цілісність/Доступн ість/ Спостережність**  **(чи їх комбінацію))** | **Порушник** |
| SQL ін’єкція | БД | Висока + катастрофічна | Конф. Інформація  + КЦ | Адміністратор и, користувачі |
| Використанн я команд UPDATE, INSERT, DELETE | БД | Висока + катастрофічна | Конф. Інф.  + КЦ | Адміністратор и, користувачі |
| DoS-атака | БД | Середня + прийнятна | ЦДС | Адміністратор  и, користувачі |
| SQL ін’єкція | БД | Висока + катастрофічна | Конф. Інформація  + КЦ | Адміністратор и, користувачі |
| Порушення  фізичної цілісності АС (її окремих компонентів), пристроїв, обладнання, носіїв  інформації | Сервери,  БД | Висока +  Катастрофі чні | Веб-сервер, сервер  застосунків, БД к, ц, д, с | Технічний  персонал, зовнішній користувач |
| Модифікація  інформаційних ресурсів, в тому числі  програмного забезпечення | Сервери | Низька +  Катастрофі чні | Веб-сервер, сервер  застосунків ц, д, с | Оператор,  адміністрато р ОС,  розробник |
| Порушення  режимів функціонуванн я (виведення з ладу) систем життєзабезпече ння АС (електроживле ння, заземлення, охоронної чи пожежної сигналізації, вентиляції та  ін.) | Внутрішн  я мережа | Висока +  Катастрофі чні | Фізичні компоненти  ц, д, с | Технічний  персонал |
| Отримання  несанкціонова ного доступу до вузлів | Внутрішн  я мережа | Висока +  катастрофі чні | Сервери, робочі  комп'ютери +ДКЦС | Адміністрато  р мережі |
| Підміна  алгоритму шифрування | Шифрато  р | Середня +  катастрофі чна | БД+ЦДК | Адміністрато  р криптографіч |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| для викрадення  інформації |  |  |  | ної  підсистеми |
| Модифікація  даних | БД | Висока +  катастрофі чна | БД+СКЦ | Адміністрато  р БД |
| Приховування  дій | Система  аудиту | Середня +  прийнятна | Журнал аудиту + С | Системний  адміністрато р |
| Отримання  несанкціонова ного доступу до внутрішньої мережі | Внутрішн  я мережа | Середня +  катастрофі чна | Доступ до БД +  СКЦД | Зовнішні  користувачі |
| Викрадення  зовнішніх носіїв | Сервери,  робочі станції | Висока +  катастрофі чна | Носії інформації,  фізичні компоненти  + ЦДК | Технічний  персонал |
| Внесення  шкідливого коду | Програмн ий код | Висока + прийнятна | Програмна закладка  + ЦКДС | Розробник |

**Відповіді на теоретичні питання**

1. Чи слід включати до моделі загроз загрози типу стихійних та технологічних лих.

Так, загрози стихійних та технологічних лих слід включати до моделі загроз. Природні та технологічні загрози можуть суттєво пошкодити інформаційну систему, а саме вивести з ладу системи життєзабезпечення АС (електроживлення, заземлення та інші).

1. Стосовно якої інформації, яка обробляється в ІС, повинна будуватись модель загроз: стосовно лише конфіденційної, чи стосовно відкритої

та конфіденційної?

На мою думку, модель загроз повинна будуватись стосовно конфіденційної та відкритої інформації, адже втрата обох типів інформації під час техногенної або природної загрози може завдати значної школи ІС.

1. Перелічіть основні класи загроз згідно моделі STRIDE. Класи:
   * Spoofing
   * Tampering
   * Repudiation
   * Information disclosure
   * Denial of service
   * Elevation of privilege
2. Наведіть приклади мережних атак класу Spoofing та DenialOfService. Приклади мережних атак класу Spoofing:
   * Ip-spoofing - вид хакерської атаки, що полягає у використанні чужого IP- адреси джерела з метою обману системи безпеки.
   * Arp-spoofing - Вид хакерської атаки, що полягає у використанні чужого IP-адреси джерела з метою обману системи безпеки.

Приклади мережних атак класу DenialOfService;

* + SYN-флуд - заснований на спробі ініціалізації великого числа одночасних TCP-з'єднань через посилку SYN-пакету з неіснуючою зворотною адресою.
  + UDP-флуд - заснований на нескінченній посилці UDP-пакетів на порти різних udp-сервісів.
  + HTTP-флуд - заснований на нескінченному посиланні HTTP-повідомлень GET на 80-й порт із метою завантажити web-сервер настільки, щоб він виявився не в змозі обробляти всю решту запитів

**Висновок**

У ході виконання лабораторної роботи було проаналізовано середовища функціонування інформаційної системи, побудовано моделі загроз та порушник