

Міністерство освіти і науки України
Національний університет «Чернігівська
політехніка »

ОПЕРАЦІЙНІ СИСТЕМИ ЧАСТИНА 2 **МЕТОДИЧНІ ВКАЗІВКИ**

до виконання лабораторних робіт для здобувачів
вищої освіти за освітньою програмою «Інженерія
програмного забезпечення »
(освітній ступінь бакалавр)

Чернігів 2024

3micr

Вступ

Лабораторна робота №1

Моделювання мереж в системі OMNeT++

Мета роботи

Мета лабораторної роботи полягає в моделюванні комп'ютерної мережі або її ділянки за допомогою засобів дискретно-подійного моделювання [?], з метою оцінки її параметрів для різних контекстів використання.

Завдання

- 1) Обрати предметну область та задачі для вирішення яких буде плануватися мережа;
- 2) Розробити дві різні топології мережі що відповідають поставленій задачі;
- 3) Змоделювати в середовищі OMNeT++ розроблені топології та зібрати дані по результатам моделювання;
- 4) Виконати аналіз результатів та порівняти характеристики розроблених топологій мереж.

Теоретичні відомості

OMNeT++ – це потужна, модульна та орієнтована на компоненти C++ бібліотека та платформа для моделювання, перш за все розроблена для створення симуляторів мереж. Під "мережею" тут розуміється у широкому сенсі: дротові та бездротові комунікаційні мережі, чіпові мережі, мережі масового обслуговування тощо.

Система OMNeT++ являє собою симулятор дискретних подій. Зміна стану модельованої системи відбувається в дискретні моменти часу відповідно до списку майбутніх подій (future eventlist), які відсортовано за часом. Подією може бути: початок передачі пакета, таймаут і т.п. Події відбуваються на основі виконання простих модулів (simple module). У такого модуля є функції ініціалізації, обробки повідомлення, дії і завершення роботи.

Система INET Framework - це комплект модулів з відкритим вихідним кодом, які дозволяють реалістично моделювати вузли мереж та протоколи дротових і бездротових мереж. Він включає моделі різних протоколів Інтернету: IP, IPv6, TCP, UDP, 802.11, Ethernet, PPP, MPLS з LDP і RSVP-TE signalling, OSPF і ряд інших. У комплект також входять різні реалістичні приклади використання цих протоколів.

Найвищий рівень абстракції в моделюванні IP в INET Framework представляє мережу, яка складається з IP-вузлів. Вузол може бути маршрутизатором або хостом. IP-вузол відповідає комп'ютерному поданню стека протоколів Інтернет. Модулі, з яких він складається, організовані таким чином, щоб моделювати обробку IP-дейтаграм в операційних системах. Обов'язковим є модуль, який відповідає за мережевий рівень (який реалізує 14 обробку IP) і модуль "мережевий інтерфейс". Додатково підключаються модулі, що реалізують протоколи транспортного рівня.

Встановлення системи

Завантажити останню версію системи OMNeT++ можна на офіційному сайті, остання на момент написання даної лабораторної роботи версія 6.1.0. Посилання на завантаження <https://omnetpp.org/download/>. Для операційної системи Windows пакунок представляє собою середовище MinGW, Eclipse IDE та саму платформу моделювання. Після розпаковки архіву треба запустити .bat файл, який запустить розгортання середовища, а після цього виконати компіляцію:

```
<MINTED>
```

Після успішної компіляції можна запустити програму командою

```
<MINTED>
```


Зверніть увагу

*На момент написання даного документу версія 6.1.0 містить некоректне посилання на завантаження пакета INET, через що його автоматичне встановлення при першому запуску OMNET++ неможливе. Для ручного встановлення можна скористатись меню **HELP** → **Install Simulation Models** та обрати одну з попередніх версій пакета і встановити його в систему, або завантажити пакет INET з офіційного веб-сайту та встановити його вручну користуючись офіційною інструкцією по встановленню що іде разом з пакетом*

Використання OMNet++

Пакет OMNet++ включає можливості моделювання широкого спектру систем, але в рамках даної лабораторної роботи зупинимось на моделюванні комп'ютерних мереж. Процес моделювання включає наступні етапи:

- 1) За допомогою компонентів, взятих із пакету INET або створених самостійно, відтворити потрібну топологію мережі. За необхідності внести корективи в файл вихідного коду моделі (*зазвичай виникає необхідність виправляти код мережевих з'єднань*)
- 2) Внести в конфігураційний файл `omnetpp.ini` налаштування мережі та програм.
- 3) Скомпілювати та запустити модель.

Простий урок по використанню мережевих компонентів і роботі з програмою OMNeT++ наведено за наступним посиланням:

https://youtu.be/ujQ_jaItx_Y

Приклади використання роутерів та інших мережевих компонентів наведені в офіційній документації на пакет мережевих компонентів:

<https://inet.omnetpp.org/docs/tutorials/configurator/doc/step1.html>

<https://inet.omnetpp.org/docs/users-guide/index.html>

Зверніть увагу

Моделювання в даному пакеті лише імітує відправку пакетів того чи іншого типу, і не відображає повністю мережеві пакети.

Також в демонстраційних проектах наведено різні варіанти топологій з прикладами використання, зокрема `inet4.5/examples/internetcloud/` та інші.

Особливості створення моделі

При створенні нових з'єднань між доданими вузлами, необхідно перемкнути в режим перегляду вихідного коду `.ned` файлу, оскільки створений за замовчуванням код не скомпілюється. В кінці файлу, в секції **:connections** будуть створені записи наступного плану(далі наведено абстрактний приклад, в вашому випадку назви пристроїв можуть відрізнятися):

```
<MINTED>
```

В даному випадку текст `ethg[0]` в усіх записах про з'єднання необхідно замінити на `ethg++`, тобто записи повинні мати наступний вигляд:

```
<MINTED>
```

Моделі програм за пакету INET

Програми INET поділяються на дві категорії:

- Специфічні програми, які реалізують дуже конкретні поведінки та генерують відповідні трафікові моделі на основі своїх параметрів. Приклади таких програм включають `TcpBasicClientApp` та `TcpGenericServerApp`.
- Загальні програми, які розділяють генерацію трафіку від використання протоколу, наприклад, `UdpApp`, `UdpSourceApp`, `UdpSinkApp` та `UdpRequ` `TcpSessionApp`.

Загалом бібліотека INET містить наступні основні програми [?]:

- 1) **TcpBasicClientApp** - Клієнтський застосунок для генерації запитів та отримання відповідей у стилі протоколу TCP. Можливе використання для грубого моделювання застосунків HTTP або FTP.
- 2) **TcpGenericServerApp** - Загальний серверний застосунок для моделювання взаємодії між клієнтом і сервером у стилі запит-відповідь у протоколах або застосунках, що використовують TCP. Він приймає будь-яку кількість вхідних TCP-з'єднань та очікує отримання повідомлень класу `GenericAppMsg`.
- 3) **TCPEchoApp** - Подібна до `TcpBasicApp`, але відправляє назад отримані пакети після їх прийому.

- 4) **TcpSessionApp** - TCP-застосунок з одиночним з'єднання TCP-застосунок з одиночним з'єднанням, який відкриває з'єднання, відправляє задані пакети, які складаються з пари (час, кількість байтів). Він може діяти як клієнт або сервер і сумісний з IPv4 та IPv6.
- 5) **UdpApp** - Загальний серверний застосунок UDP з композитним джерелом та стоком трафіку.
- 6) **UdpRequestResponseApp** - Загальна серверна програма UDP з композитним джерелом та стоком трафіку.
- 7) **PingApp** - Програма, яка генерує ping-запити та обчислює втрати пакетів та параметри кругового шляху відповідей.
- 8) **UdpEchoApp** - Подібна до `UdpBasicApp`, але відправляє назад отримані пакети після їх прийому.
- 9) **UdpVideoStreamClient** - Клієнт відеопотоку, який відправляє запит на відеопотік до сервера в призначений час та отримує потік від `UdpVideoStreamServer`.
- 10) **UdpVideoStreamServer** - Це сервер відеопотоку, який використовується з `UdpVideoStreamClient`. Сервер чекає на вхідні запити на відеопотік. Коли запит надходить, сервер генерує випадкову довжину відеопотоку за допомогою параметра `videoSize`, відправляє UDP-пакети довжиною `packetLen` кожні `sendInterval`, доки не буде досягнуто `videoSize`.
- 11) **TelnetApp** - Модель Telnet сеансів.

Завдання (деталізовно)

Зверніть увагу

Завдання даної лабораторної роботи передбачає самостійний вибір предметної області, задач на вирішення яких орієнтована мережа та мережевої топології, тому далі наведені базові елементи завдання, які зорієнтують вас у правильному напрямку роботи, остаточне завдання може бути скоригованим в залежності від обраної мережі.

Основне завдання лабораторної роботи включає наступні кроки:

- 1) Оберіть предметну область та задачу для вирішення якої буде призначена ваша мережа. Це найбільш важливий етап лабораторної роботи,

оскільки від вашого вибору залежатимуть параметри які ви будете оцінювати за допомогою моделі. Визначте основні ролі для учасників мережі та оцініть яке програмне забезпечення та які приблизні об'єми трафіка будуть призначені для кожного з учасників. В якості вузлів мережі можуть бути і клієнтські ком'ютери, і сервери, і мережеві сховища і камери відеонагляду, і відеореєстратори і звичайно ж мережеві пристрої, такі як маршрутизатори та комутатори.

- 2) Після цього запропонуйте принаймні два варіанта топології мережі, враховуйте, що для наглядного результату мережа має бути з достатньо складною топологією, при якій наприклад пакет має проходити в деяких випадках через кілька маршрутизаторів.
- 3) В середовищі OMNeT++ побудуйте моделі мереж з обраними вами топологіями та налаштуйте їх відповідно до вказаних вами задач. Пакет компонентів INET 4.5 містить багато варіантів симуляції програмно забезпечення, тому знайти готовий варіант програми для симуляції трафіка на повинно бути проблемою. Впевніться що обрані варіанти “програм” дозволяють зібрати метрики які ви збираєтесь отримати та використати для оцінки і порівняння топологій. Параметри за якими буде проводитись оцінка можуть бути обрані на свій розсуд в залежності від параметрів обраної мережі, але всі вибори повинні бути обґрунтовані у вашому звіті.
- 4) Скомпілювати та запустити процес симуляції, впевнитися, що побудована модель працює саме так як і задумувалося, за необхідності внести виправлення та перекомпілювати модель.
- 5) Перейти до збережених результатів симуляції, де записані основні дані зібрані в процесі роботи моделі, та провести аналіз отриманих даних відомими вам методами, та отримати на основі аналізу оцінку швидкодії мережі (або іншого параметра який ви можете оцінити)
- 6) Зробити висновки щодо на основі отриманих оцінок та висловити думку щодо доцільності чи недоцільності використання запропонованих вами топологій мереж.

У висновках до лабораторної роботи опишіть переваги та недоліки дискретно-подійного моделювання в контексті моделювання комп'ютерних мереж та мереж зв'язку, а також наведіть короткі результати аналізу отриманих під час моделювання даних.

Орієнтовні теми для теоретичних питань

- Загальне поняття «Моделювання». Які задачі вирішує моделювання мереж.
- Основні види моделей, їх особливості.
- Дискретно подійне моделювання.
- Основні можливості пакета OMNET++ для моделювання мереж.

Лабораторна робота № 2 Імітаційне моделювання та емуляція роботи захищених комп'ютерних мереж.

Мета

Мета лабораторної роботи полягає в розробці та реалізації моделі захищеної комп'ютерної мережі, оцінці ефективності її захисту від зовнішніх загроз, а також у вивченні ефективності різних заходів захисту мережі та оцінці рівня її захищеності на основі результатів моделювання та тестування.

Завдання

- 1) Побудувати імітаційну модель захищеної комп'ютерної мережі.
- 2) Оцінити рівень захищеності за допомогою різних програмних засобів а також вплив наявності чи відсутності засобів безпеки на рівень захищеності.

Теоретичні відомості

Зверніть увагу

Оскільки основне програмне забезпечення для емуляції комп'ютерних мереж є достатньо ресурсоємним та при цьому неефективно працює в операційній системі **Windows**, дана лабораторна робота передбачає альтернативні варіанти виконання які можуть забезпечити більш стабільну роботу на слабких системах. Тому перед виконанням ознайомтеся з усіма альтернативними варіантами виконання і при неможливості виконати роботу в програмі GNS3 використовуйте альтернативні варіанти

Імітаційне моделювання мереж

Для дослідження різноманітних характеристик комп'ютерних мереж використовуються методи моделювання. У сучасних умовах, коли інфраструктура мереж стає дедалі складнішою і вимоги до її ефективності зростають, використання фізичних тестів часто є занадто затратним та ризикованим. Імітаційні моделі надають можливість вивчати взаємодію мережевих компонентів, аналізувати навантаження і визначати вузькі місця без втручання у роботу реальної мережі. Це робить імітаційне моделювання важливим інструментом для попереднього оцінювання різних архітектур мереж, розробки оптимальних рішень і забезпечення надійності та безпеки комп'ютерних мереж.

Імітаційне моделювання — це метод дослідження, заснований на тому, що система, яка вивчається, замінюється імітатором і з ним проводяться експерименти з метою отримання інформації про цю систему. Експериментування з імітатором називають імітацією (імітація — це збагнення суті явища, не вдаючись до експериментів на реальному об'єкті).

Одним із варіантів імітаційного моделювання є емуляція. При емуляції модель точно відтворює роботу реальної системи так, що за більшістю параметрів це відповідає реальній системі. Ще одним схожим підвидом програмного забезпечення є програмне забезпечення для симуляції, яке може бути на перший погляд схоже на емулятор, але передбачає достатньо серйозні спрощення та обмеження. Далі розглянемо відмінності між термінами симулятор та емулятор.

Симулятор — імітує якийсь набір команд, який є незмінним і не дозволяє користувачеві вийти за цей набір. При спробі виконання непідтримуваних команд, ми відразу отримаємо повідомлення про помилку. Класичний приклад програми — симулятора — Cisco Packet Tracer.

Емулятори ж навпаки – дозволяють програвати (виконуючи байт трансляцію) образів (прошивки) реальних пристроїв, найчастіше без видимих обмежень. Прикладом емулятора є програмний продукт GNS3.

GNS3

GNS3 використовується сотнями тисяч інженерів мереж по всьому світу для емуляції, налаштування, тестування та усунення неполадок віртуальних і реальних мереж. GNS3 дозволяє запускати як невеликі топології, що складаються лише з кількох пристроїв на вашому ноутбукі, так і великі, з багатьма пристроями, розміщеними на декількох серверах або навіть у хмарі.

GNS3 — це безкоштовне програмне забезпечення з відкритим кодом, яке можна завантажити за адресою <http://gns3.com>.

Програма активно розвивається та підтримується, і має зростаючу спільноту з понад 800 000 учасників.

GNS3 підтримує кілька типів емуляторів які можуть запускати різні типи програмного забезпечення мережевих пристроїв. Розглянемо основні з них:

- **Dynamips** - це технологія, яку використовує GNS3 з моменту заснування, і емулює маршрутизатори Cisco та базову комутацію за допомогою модуля Etherswitch. Використовує оригінальні образи програмного забезпечення, але при цьому коректний запуск усіх образів не гарантується оскільки Cisco не підтримує запуск IOS програмного забезпечення на сторонніх пристроях. Підтримуються достатньо старі пристрої.
- **QEMU** - Стандартна система віртуалізації для Linux, підтримує запуск практично усіх образів операційних систем і добре інтегрується в GNS3. Щоб використовувати образи Cisco, такі як IOSvL2, потрібно придбати підписку Cisco VIRL. Це дозволить отримати доступ до образів, які працюють з GNS3 та схвалені командою Cisco. Образи VIRL створюються спеціально для симуляції та працюють особливо добре, якщо потрібно використовувати новіші версії операційної системи Cisco та сучасні функції. Фактично це єдиний офіційний спосіб запуску програмного забезпечення Cisco.
- **IOU** - це внутрішній спосіб Cisco запускати IOS на Unix. Це не ресурсоемна програма з точки зору ЦП та пам'яті, що робить її добрим вибором. IOU підтримує як маршрутизатори, так і комутатори. Але при цьому дане програмне забезпечення не є офіційним і образи та ліцензії для запуску образів таким чином неможливо придбати офіційними

шляхами. Стабільність роботи образів на такому емуляторі також не гарантується.

- **VMware / VirtualBox** - GNS3 підтримує інтеграцію віртуальних машин VMware та VirtualBox, але така інтеграція є достатньо поверхневою і не передбачає збереження таких віртуальних машин в проєкті, тому даний варіант не можна назвати рекомендованим. Але в деяких випадках він може більш швидким аніж використання QEMU.
- **VPCS** (Симулятор віртуального ПК) - це легкий спосіб емуляції дуже базового ПК. VPCS використовує дуже мало пам'яті, тому він є добрим вибором, коли ви хочете емулювати ПК без графічного інтерфейсу та якщо вам потрібні лише прості команди, такі як `ping`, щоб перевірити зв'язок у ваших мережах GNS3. Для розширеного функціоналу варто використовувати інші варіанти.
- **Docker** - підтримка Docker в GNS3 надає вам можливість запускати кілька контейнерів як частину топології GNS3. Це один з найменш ресурсоємних варіантів запуску повноцінної операційної системи Linux.

Увага

GNS3 не надає ніяких образів операційних систем, за виключенням VPCS, що інтегровані в систему. при створенні шаблону пристрою GNS3 може надати посилання на скачування образу якщо обрано варіант операційної системи з відкритим вихідним кодом який доступний для використання безкоштовно. Docker образи безкоштовних проєктів скачуються з репозиторія автоматично. Всі інші образи необхідно отримувати самостійно, при цьому вся відповідальність за дотримання ліцензійних угод покладена на користувача. Єдиним офіційним варіантом є оплата ліцензії у розробника відповідної операційної системи.

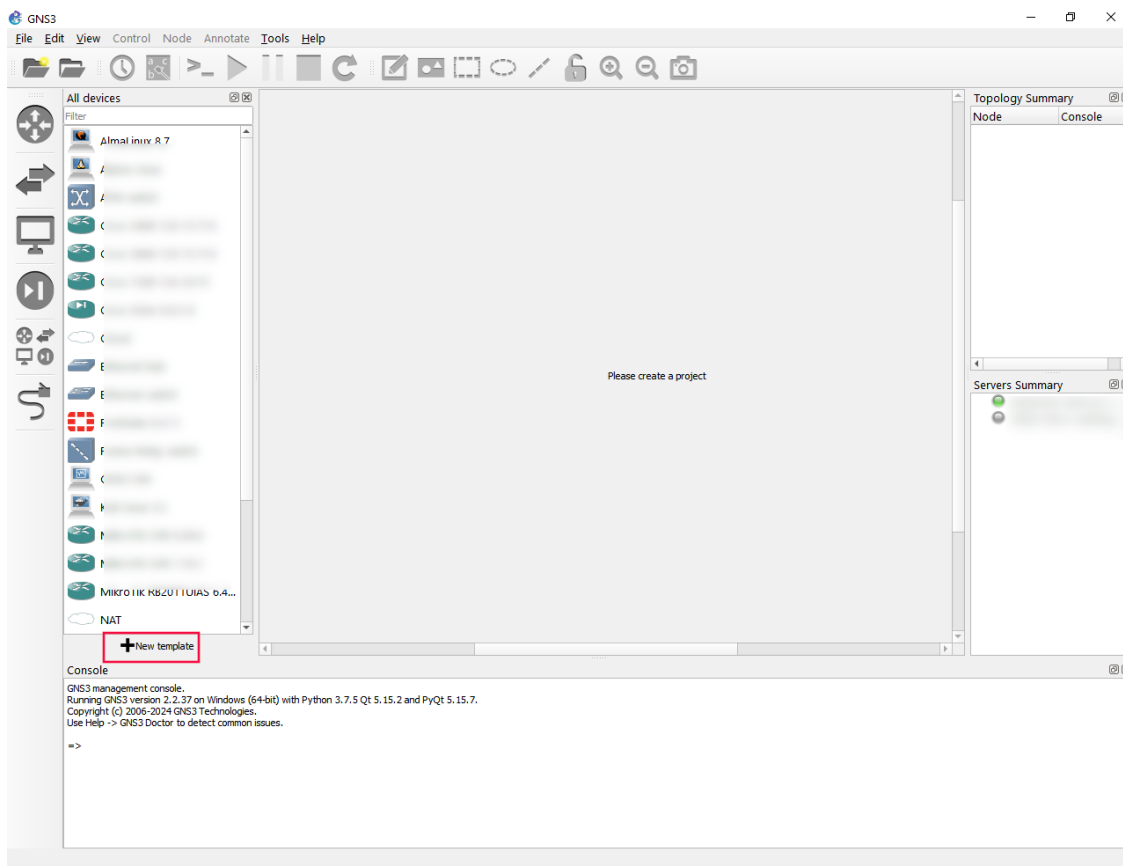
Використання

Для створення мережових топологій в GNS3 в першу чергу необхідно додати шаблони пристроїв, на основі яких будуть створюватись моделі мереж. Шаблон пристрою можна або створити з нуля, або підвантажити образи операційних систем до існуючих шаблонів за серверів GNS3.

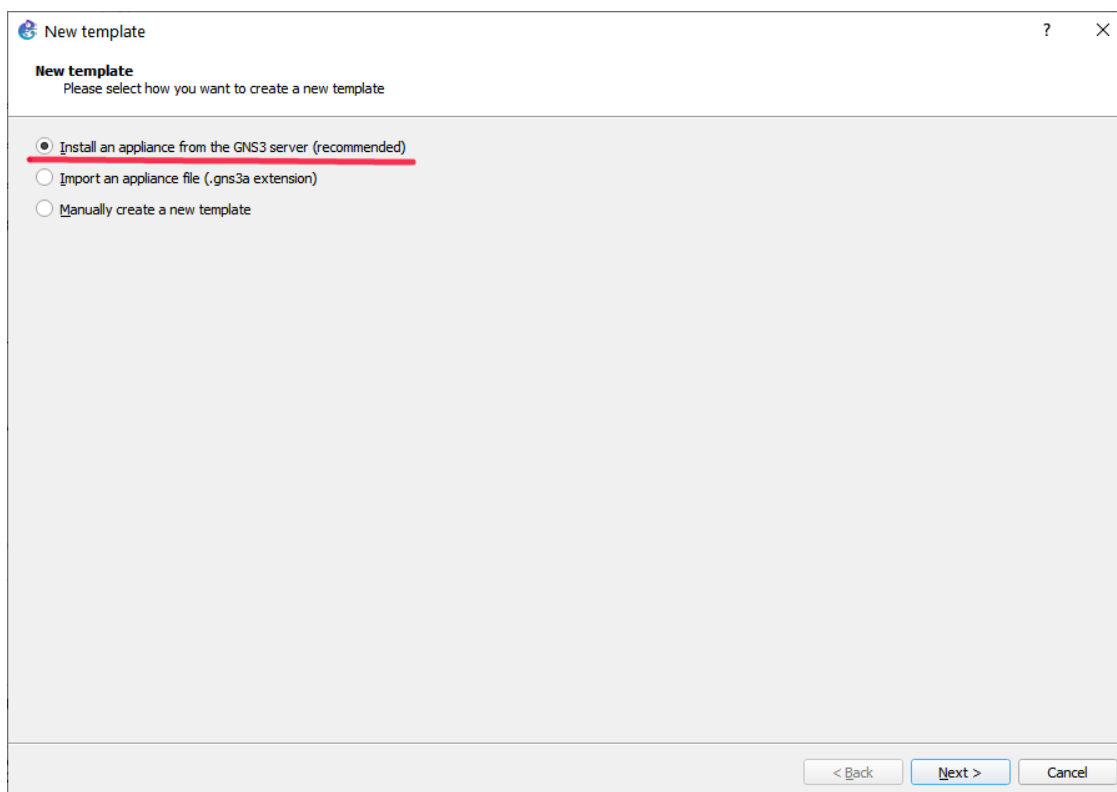
Розглянемо другий варіант. Для створення шаблону пристрою таким чином необхідно пройти наступні кроки:

<https://support.cloudmylab.com/kb/how-to-add-appliance-and-image-on-gns3> <https://docs.gns3.com/docs/using-gns3/beginners/import-gns3-appliance/>

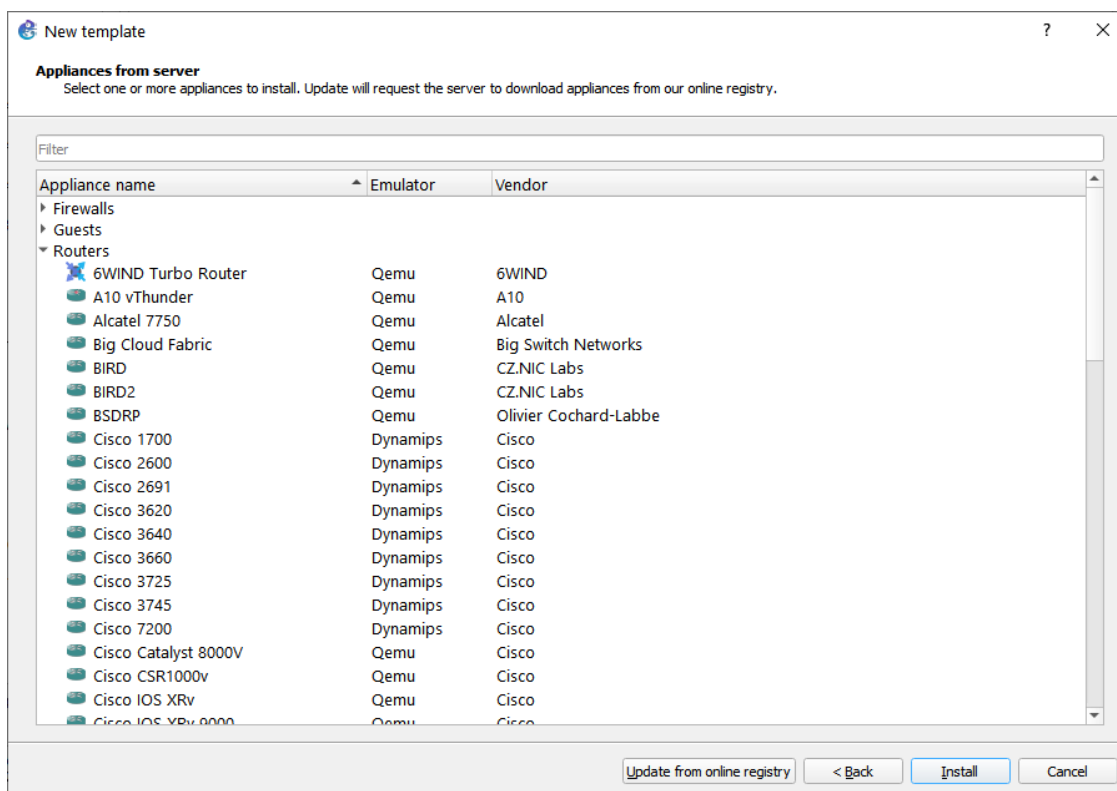
Крок 1: Натисніть на «переглянути всі пристрої», а потім виберіть кнопку «Новий шаблон пристрою».



Крок 2: Виберіть «Встановити з сервера GNS3».

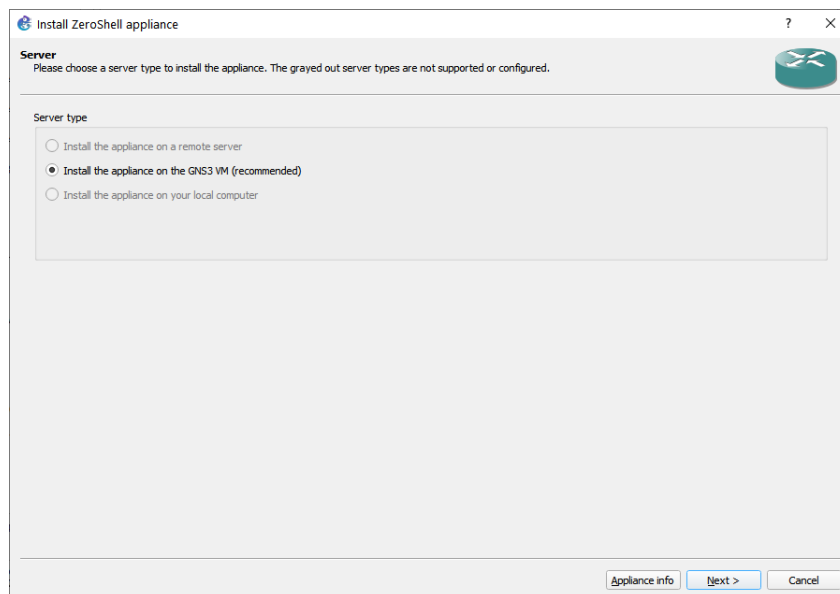


Крок 3: Обираємо категорію та пристрій із наданого списку, за необхідності список можна оновити з онлайн реєстру. Потім натисніть «Встановити».

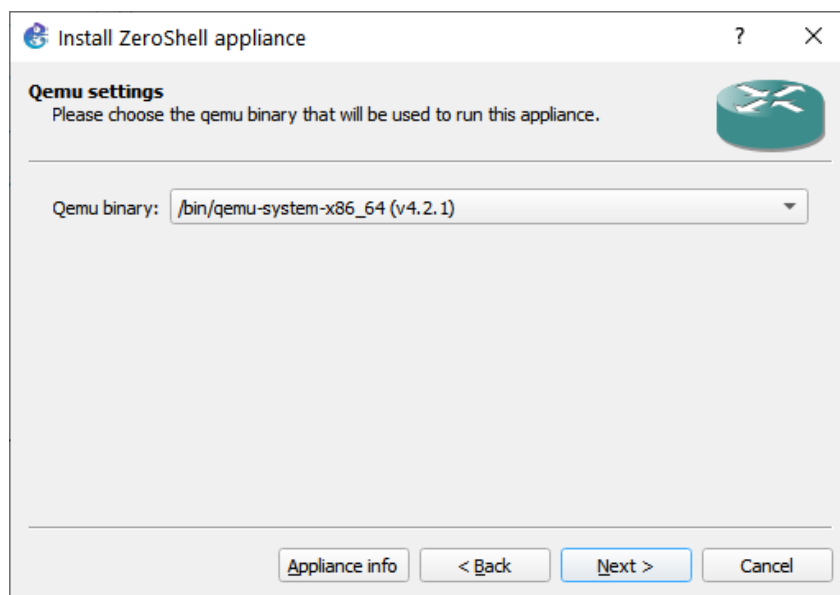


Крок 4: Виберіть варіант встановлення із доступних - якщо у вас наявний локальний або віддалений сервер то відповідні опції будуть доступні

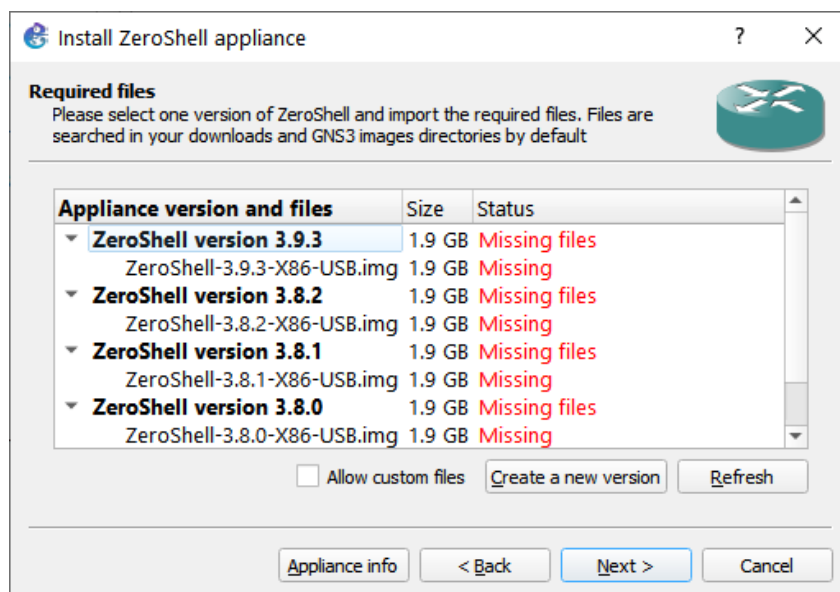
інакше для більшості пристроїв залишається варіант віртуальна машина GNS3. Далі натискаємо «Далі».



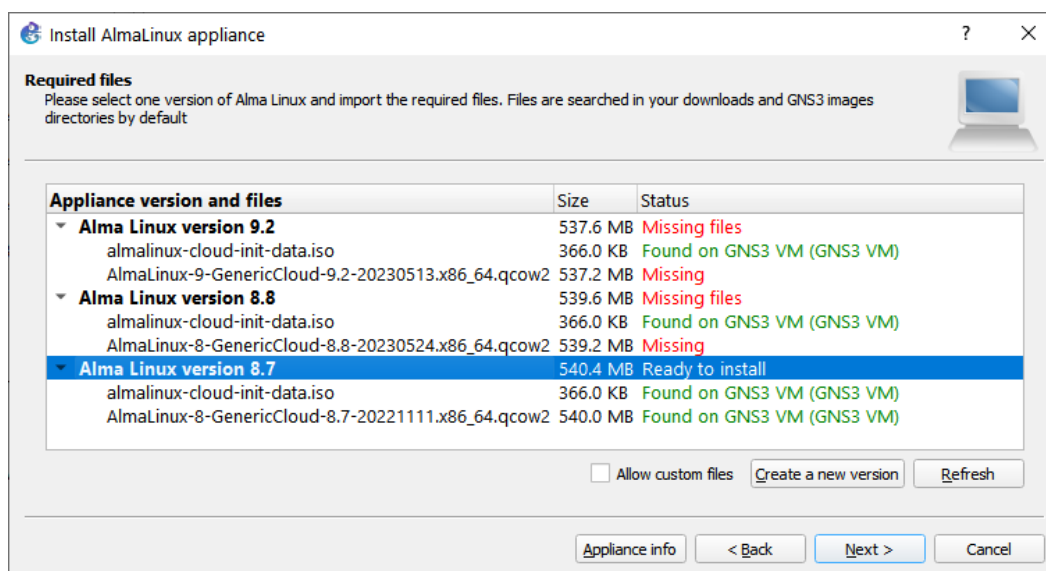
Крок 5: Зазвичай базову програму для запуску віртуальної машини міняти не треба, тому натискаємо «Далі».



Крок 6: На наступному екрані бачимо перелік версій та наявні або відсутні файли необхідні для їх запуску. Для Open Source та безкоштовних продуктів можна натиснути кнопку «Завантажити», виділивши необхідний файл, в інших випадках файл треба шукати самостійно. завантажений файл треба імпортувати, а якщо версія не співпадає з вказаною але ви вважаєте, що файл повинен підійти - треба поставити прапорець Дозволити всі файли, після імпорту статус файлу повинен змінитись на наявний.



Крок 7: Після успішного імпорту файлу виберіть «Далі».



Крок 8: Нарешті, ви можете побачити піктограму обраного пристроя у вкладці «Встановлені пристрої».

Альтернативні варіанти

EVE-NG

Схожий на GNS3 програмний засіб, але при цьому має безкоштовну та комерційну версію. Функціонал безкоштовної обмежений. За деякими відгуками дане програмне забезпечення має кращий користувацький інтерфейс і є більш доопрацьованим. Але слід враховувати що принцип дії EVE-NG та GNS3 однаковий, тому кардинальної різниці в швидкодії бут не може.

Якщо ви приймете рішення використовувати даний варіант в якості альтернативи GNS3 то деталі та особливості використання ви можете знайти в документації розташованій за наступним посиланням www.eve-ng.net

Створення віртуальних машин вручну

Для уникнення подвійної віртуалізації, при використанні GNS3 на операційній системі Windows, можна змоделювати аналогічну інфраструктуру створивши окремі віртуальні машини за допомогою будь-якого зручного для вас гіпервізора. Так наприклад VirtualBox дозволяє створювати будь-яку кількість внутрішніх мереж, а тому дає можливість емулювати мережі складної топології. Створити віртуальні машини можна як вручну так і скористатися можливостями по інтеграції віртуальних машин VirtualBox та VMware в системі GNS3. Другий варіант спростить встановлення мережеских з'єднань.

Пошук вразливостей та сканування мереж

Nmap

Metasploit Framework

Завдання (деталізовно)

Частина 1. Моделювання захищеної мережі

Перед виконанням лабораторної роботи придумайте предметну область для вирішення задач в якій буде моделюватись мережа. Враховуйте можливості вашого обладнання для запуску системи моделювання і за необхідності використовуйте тільки мінімально необхідний набір компонентів. Повноцінну схему мережі можна побудувати окремо та додати в звіт. *В мінімальному варіанті моделі повинен бути хоча б один маршрутизатор, мервер та мережеский екран (у вигляді окремого пристроя мережеский екран можна розмістити замість маршрутизатора, або використовувати інтегрований в маршрутизатор (наприклад для маршрутизаторів Mikrotik))*

- 1) Створіть три маршрутизатори (або іншу кількість яка відповідатиме обраній вами предметній області та мережіщо вирішуватиме завдання для вашої предметної області і при цьому дозволить запускати модель на вашому комп'ютері), підключіть їх до різних мережеских сегментів, а потім налаштуйте протокол маршрутизації, наприклад (**OSPF** або **RIP**), між ними.

- 2) Додайте кілька клієнтів до мережі, (хоча б одного повноцінного клієнта, який матиме графічний інтерфейс), а також мережевий сервіс (наприклад веб сервер, SMB сервер, або інший сервіс який можна просканувати на вразливість) та один або кілька пристроїв безпеки (мережевих екранів, систем виявлення вторгнень чи комплексних рішень, при цьому їх можна додавати або окремими пристроями, або інтегрувати в сервер у вигляді програмних модулів).
- 3) Також не забудьте додати клієнт Kali Linux який далі буде використовуват для тестування мережі.
- 4) Виконайте тестування, щоб переконатися, що маршрутизація працює коректно і всі вузли мають доступ один до одного в рамках задуманої топології.

Зверніть увагу

Остаточний варіант виконання даної частини може варіюватися, (наприклад маршрутизатори різних виробників, різні протоколи маршрутизації, різні варіанти клієнтів та мережевих сервісів), в залежності від обраної предметної області, тому кількість та типи пристроїв, що повинні бути присутні в моделі наведена орієнтовно, щоб відобразити складність моделі.

Увага

Виконувати тестування на наявність вразливостей, особливо такі, що передбачають активне втручання, можна тільки для ресурсів на тестування яких у вас є дозвіл, або спеціально призначених для тренування навичок з пошуку вразливостей ресурсів. Пам'ятайте, **несанкціоноване втручання** в роботу комп'ютерів, комп'ютерних мереж чи мереж електрозв'язку є **кримінальним правопорушенням** (стаття 361 ККУ).

Частина 2. Оцінка рівня захищеності мережі та впливу технічних засобів на захищеність

- 1) Вимкніть системи безпеки для змодельованої мережі (наприклад дозвольте на мережевому екрані всі з'єднання, а систему виявлення вторгнень вимкніть).
- 2) Запустіть **Kali Linux** в режимі live середовища (не обов'язково, можливий будь-який варіант запуску в залежності від топології) для

виконання тестування на проникнення, щоб виявити потенційні вразливості в мережі.

- 3) Для дослідження подальших етапів виконання скористатись програмним засобом **Wireshark**, що дозволяє відслідковувати проходження мережевих пакетів. В рамках системи GNS3 **Wireshark** може відслідковувати будь-яке з'єднання (при цьому немає необхідності встановлювати **Wireshark** на віртуальні комп'ютери моделі, **Wireshark** запускається на хост системі через інтерфейс GNS3).
- 4) За допомогою програми **Nmap** спробувати дослідити структуру мережі та виконати сканування портів для пошуку наявних веб-сервісів.
- 5) Далі користуючись **Nmap** спробувати виконати DoS атаку на виявлений сервіс перевантаживши його великою кількістю запитів. Зафіксуйте виконання за допомогою **Wireshark**.
- 6) За допомогою пакету **Metasploit Framework** спробуйте знайти потенційні вразливості для виявлених сервісів. *Скоріш за все це не вдасться, оскільки в актуальних версіях програмного забезпечення широко відомі вразливості будуть закритими.* Наведіть знайдені варіанти вразливостей (навіть якщо вони вже не актуальні) у звіті.
- 7) За допомогою **Metasploit Framework** спробуйте виконати DoS атаку на тестовий сервіс.
- 8) Оцініть вплив змодельованих атак на роботу мережевих сервісів.
- 9) Спробуйте налаштувати наявні в мережі засоби безпеки для мінімізації впливу проведених раніше атак та максимально обмежте можливості розкриття зловмисником інформації через сканування.
- 10) Повторіть спроби сканування та атак, оцініть ефективність роботи систем захисту.

Орієнтовні теми для теоретичних питань

Лабораторна робота № 3

Пошук вразливостей

Веб-застосунків

Мета роботи

Мета лабораторної роботи полягає у вивченні та застосуванні методів перевірки безпеки веб-застосунків з метою виявлення потенційних вразливостей для підвищення рівня захисту інформаційних систем. Під час виконання роботи студенти повинні оволодіти основними техніками сканування і перевірки веб-застосунків та виявлення вразливостей, зокрема використовувати спеціалізовані інструменти для їх пошуку, аналізувати код веб-застосунків для виявлення потенційних вразливостей та оцінювати наслідки їх використання.

Завдання

Виявити якомога більше вразливостей в спеціальних тестових веб-застосунках.

Теоретичні відомості

Веб-додатки - це програми, написані скриптовою мовою (Perl, PHP, Javascript, Ruby, Golang та інші) або написані мовою високого рівня та відкомпільовані під відповідну ОС, які працюють на стороні веб-сервера та призначені для створення інтерфейсу між користувачем та веб-сайтом.

Результатом пошуку рішення, як ефективно запобігати новішим типам кібератак стало PEN-тестування. Якщо говорити узагальнено, то в основі цього методу проста гіпотеза, щоб ефективно вдосконалювати системи та способи захисту продуктів від кібератак, необхідно розуміти, яким

чином шукають ту чи іншу вразливість, і як вона влаштована зсередини. Іншими словами — щоб захиститися від хакерської атаки, потрібно усвідомлювати за якими сценаріями вона може відбутися й де шукати головні слабкості системи. Саме завдяки активному аналізу системи на вміст дефектів коду чи в площині безпекових рішень можна виявити потенційні вразливості. Важливо, що PEN-тестування завжди проводиться з позиції потенційного нападника і може включати активне використання вразливостей. Тобто це контрольоване проникнення в систему [?]. Деякі з потенційних вразливостей наведено нижче.

- **XSS** (або ще міжсайтовий скриптинг) ін'єкції — досить поширена вразливість, яка зустрічається у багатьох застосунках. Головна ідея XSS в тому, що зломиснику вдається додати на сторінку JavaScript-код, якого до цього не було. Цей код буде виконуватися щоразу, коли жертви (тобто користувачі) заходять на сторінку застосунку, де цей код додав зломисник.
- **SQL ін'єкція (SQLi)** — це тип ін'єкційної атаки, яка дозволяє модифікувати SQL команди для отримання даних або виведення з ладу програми. Зломисники можуть модифікувати команди SQL, які впливають на ваш застосунок, через деякі вхідні дані на вашому сайті, наприклад, поле пошуку. Успішне виконання SQL ін'єкції може призвести до неавторизованого доступу до конфіденційних даних (це може бути дуже «чутлива» інформація — наприклад, паролі, адреси, дані кредитних карток і так далі). За останні кілька років багато випадків витоку інформації стали результатом саме SQL ін'єкцій.
- **Крос-сайтова піддробка запиту (CSRF)** - це атака, коли зломисник змушує користувача виконувати небажані дії без його згоди. Захист від CSRF включає використання токенів запитів (CSRF-токени) і перевірку Referer-заголовка [?].
- **Недоліки автентифікації та керування сесіями.** Слабка автентифікація та керування сесіями можуть призвести до компрометації облікових записів користувачів. Для захисту слід використовувати сильні паролі, двофакторну автентифікацію та надійне керування сесіями.

Увага

*Виконувати тестування на наявність вразливостей, особливо такі, що передбачають активне втручання, можна тільки для ресурсів на тестування яких у вас є дозвіл, або спеціально призначених для тренування навичок з пошуку вразливостей ресурсів. Пам'ятайте, **несанкціоноване втручання** в роботу комп'ютерів, комп'ютерних мереж чи мереж електрозв'язку є **кримінальним правопорушенням** (стаття 361 ККУ).*

Короткий відеокурс по пошуку вразливостей ви можете знайти за наступним посиланням на Youtube [HackerOne](#). Для виконання лабораторної роботи бажано переглянути перші 11 відео, відео на тему криптографії, android та інші теми, що не стосуються веб-застосунків дивитись не обов'язково, оскільки вони не стосуються тематики даної роботи.

Для аналізу Веб-застосунків вам знадобиться програмне забезпечення для перехоплення запитів до веб сервера та їх модифікації. Одним із типів такого програмного забезпечення є перехоплюючі проксі сервери. Найбільш популярним варіантом такого програмного забезпечення є [Burp Proxy](#). Повноцінна версія даної програми, яка містить всі засоби автоматизації та додаткові можливості є комерційною, але наявна і community версія яка є безкоштовною і містить тільки базовий функціонал, але його в більшості випадків достатньо для пошуку більшості вразливостей і цілком достатньо для виконання лабораторної роботи.

Іншим варіантом програмного забезпечення перехоплюючого проксі є [ZAP Proxy](#), дана програма також є безкоштовною, і не зважаючи на обмежений у порівнянні з Burp функціонал цілком підходить для задач пошуку вразливостей.

Завдання (деталізовано)

В рамках даної лабораторної роботи вам пропонується виконати пошук вразливостей в веб-застосунках в форматі гри CTF.

CTF (Capture The Flag) - це тип змагання з безпеки інформаційних систем, яке полягає в перевірці безпеки вебзастосунків шляхом пошуків та експлуатації вразливостей.

Основна суть гри CTF полягає в наступному:

Мета гри: учасники гри мають завдання знайти та експлуатувати вразливості в вебзастосунках, щоб здобути доступ до захищеної інформації або виконати певні дії.

Учасники гри отримують інформацію про вебзастосунок, який потрібно

перевірити на безпеку. Далі учасники грають роль зловмисників і намагаються знайти вразливості в вебзастосунку. Після цього учасники намагаються експлуатувати знайдені вразливості, щоб здобути доступ до захищеної інформації або виконати певні дії, при цьому учасники отримують очки за кожну знайдену вразливість та успішну експлуатацію.

- 1) Перейдіть на сайт Hacker 101 в розділ CTF за посиланням ctf.hacker101.com та перейшовши в розділ для реєстрації зареєструватись на сайті.
- 2) Повернутись на сторінку CTF. Серед запропонованих завдань обрати завдання із категорії «**Web**» відповідно до бажаної оцінки. При виборі завдання для вас буде створено персональну віртуальну машину з розгорнутим веб-застосунком який ви можете тестувати будь якими доступними способами. Завдання мають різні рівні складності, а також містять різну кількість флагів. В рамках лабораторної роботи не обов'язково шукати усі флаги з конкретного завдання, можете набрати необхідну кількість флагів з різних завдань.
- 3) Будь якими доступними засобами виявіть наявні у веб застосунках вразливості. При виявленні передбаченої завданням вразливості ви отримаєте флаг, у вигляді спеціального хеш значення вигляду `^FLAG^37ae2f974017fa575f08cd215044cd6bb395c3f5e5e293ee5324ba6769c$FLAG$` який треба внести на сайті в розділі «**Submit Flag**». Після успішного занесення флага вам буде зараховано частину виконаного завдання та буде нараховано відповідну кількість балів.
- 4) На сторінці завдання також наявні підказки які можуть направити в пошуку флага, якщо зайшли в глухий кут і не знаєте де шукати вразливість - скористайтесь підказками. підказки відкриваються поступово і з затримкою в часі, щоб дати вам час обдумати підказку.

Оцінка	Мінімальна кількість флагів*	Додаткові умови
Задовільно	5	Додаткових умов немає
Добре	10	Не менше 3 флагів на завданнях складності Moderate
Відмінно	14	Умови для оцінки «Добре»+ не менше одного флага складності Hard

Табл. 1. Завдання в залежності від очікуваної оцінки

Зверніть увагу

* -- більше флагів знайдено - вище оцінка, але враховуйте, що на оцінку впливають також і відповіді на теоретичні питання.

Орієнтовні теми для теоретичних питань

- Загальне поняття «Вразливості». Причини виникнення вразливостей.
- Основні види вразливостей Web-застосунків, їх особливості.
- Шляхи виявлення вразливостей.
- Інструменти для пошуку вразливостей.

Бібліографія

- [1] Найвідоміші вразливості веб застосунків. XSS та SQL ін'єкції, вразливості автентифікації --- dou.ua. <https://dou.ua/forums/topic/40613/>. [Accessed 11-10-2024].
- [2] Applications; INET 4.5.0 documentation --- inet.omnetpp.org. <https://inet.omnetpp.org/docs/users-guide/ch-apps.html>. [Accessed 09-10-2024].
- [3] Itproger. Безпека веб-додатків: найкращі практики та вразливості - стаття на itProger --- itproger.com. <https://itproger.com/ua/news/bezopasnost-veb-prilozheniy-luchshie-praktiki-i-uyazvimost> [Accessed 11-10-2024].
- [4] OMNeT. Дискретно-подійне моделювання — Вікіпедія --- uk.wikipedia.org. https://uk.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%BE-%D0%BF%D0%BE%D0%B4%D1%96%D0%B9%D0%BD%D0%B5_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F. [Accessed 09-10-2024].