МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

БАКУМОВ КОСТЯНТИН ОЛЕКСАНДРОВИЧ

Допускається до захисту:
Завідувач кафедри
інформаційних технологій,
к.т.н., доцент
_____ Т.В.Нескородєва
«____» _____ 20__ р.

МЕТОДОЛОГІЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ЗАКЛАДУ ВИЩОЇ ОСВІТИ

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Керівник:
Барибін О.І., доцент кафедри
інформаційних технологій,
к.т.н
_____
підпис

Оцінка:___/ ___/ _____
(бали за шкалою ЄКТС/за національною шкалою)
Голова ЕК: _____
(підпис)

Вінниця — 2021

Бакумов К. О. Методологія тестування на проникнення корпоративної мережі закладу вищої освіти Спеціальність 125 Кібербезпека. Освітня програма «Кібербезпека». Донецький національний університет імені Василя Стуса, Вінниця, 2021.

У кваліфікаційній (бакалаврській) роботі здійснено методологію тестування на проникнення корпоративної мережі університету відповідно до методологій OWASP testing guide, NIST 800-115, Penetration Testing Execution Standard, Open Source Security Testing Methodology Manual. Результатом роботи є методологія тестування на проникнення

Ключові слова: ТЕСТУВАННЯ НА ПРОНИКНЕННЯ, КОРПОРАТИВНА МЕРЕЖА, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА.

Табл. 2 Рис. 19. Бібліограф. 12

Bakumov K.O. Methodology of penetration testing of the corporate network of an education institution. Specialty 125 Cybersecurity. Educational program «Cybersecurity». Vasyl Stus Donetsk National University, Vinnytsia, 2021.

In the qualification (bachelor's) work the methodology of penetration testing of the corporate network of the university is carried out according to the methodologies OWASP testing guide, NIST 800-115, Penetration Testing Execution Standard, Open Source Security Testing Methodology Manual. The result is a penetration testing methodology

Keywords: PENETRATION TESTING, CORPORATE NETWORK, CYBERSECURITY, INFORMATION SECURITY.

Tables. 2. Pictures. 19. Bibliographer. 12

ЗМІСТ

ВСТУП

Тест на проникнення або пентест - це спроба злому інформаційного ресурсу організації, спрямована на отримання об'єктивної оцінки рівня інформаційної безпеки досліджуваного ресурсу, виявлення його вразливостей і слабких місць. Тест на проникнення дозволяє зрозуміти Замовнику, чи ефективні використовувані засоби захисту, і наскільки ймовірним є злому і отримання інформації зловмисником. Пентест призначений для отримання об'єктивної оцінки захищеності інформаційного середовища організації від зовнішніх і внутрішніх загроз з боку потенційного порушника безпеки.

Завдяки тестуванням на проникнення структури стаються в рази краще захищені від атаки хакерів, тому всім установам бажано проводити їх.

Для впевненого проведення пентесту потрібно користуватися сучасними методологіями, ось наведено найвідоміші[1]:

- OWASP testing guide
- PCI Penetration testing guide
- Penetration Testing Execution Standard
- NIST 800-115
- Penetration Testing Framework
- Information Systems Security Assessment Framework (ISSAF)
- Open Source Security Testing Methodology Manual (“OSSTMM”)

Всі ці методології являються загальновживаними і мають в собі загальні положення для проведення тестування на проникнення, але тестування на проникнення великої організації є задачою нетривіальною і загальньої методології недостатньо для його проведення. Саме тому тема роботи є актуальною.

Метою даної роботи є формування пропозиції методики тестування на проникнення для корпоративної мережі закладу вищої освіти.

Завданням роботи є:

- Аналіз та виділення загальних фаз методології тестування на проникнення;
- Визначення основних вразливих місць корпоративної мережі закладу вищої освіти на основі оцінки ризиків;
- Формування пропозицій щодо інструментарію та змісту основних фаз пропонуємої методики тестування на проникнення.

Об’єктом бакалаврської роботи є інформаційна безпека корпоративної мережі закладу вищої освіти.

Предметом дослідження є методологія тестування на проникнення корпоративної мережі закладу вищої освіти.

РОЗДІЛ 1. МЕТОДОЛОГІЯ ПЕНТЕСТУ

Забезпечення інформаційної безпеки як для бізнес-організацій, так і для державних установ по типу університетів є досить важливою – якщо не критичною – складовою нормального функціонування. Однією з відомих форм для оцінки стану безпеки та зменшення ризиків безпеки є тестування на проникнення (penetration testing або pentest). Тестування на проникнення – це контрольований експеримент з метою проникнення в систему або мережу для виявлення вразливостей[2]. Тестування на проникнення застосовує ті ж методи, які використовуються при звичайному нападі зловмисника. Такий підхід дозволяє застосовувати відповідні заходи для усунення вразливостей, перш ніж вони будуть вивчені неавторизованими людьми.

1.1 Перелік сучасних методологій

У роботі [3] зазначено чотири основні проблемні напрями досліджень, що пов’язані з тестуванням на проникнення:

1. Основні інструменти, що використовуються для тестування на проникнення.
2. Сценарії атак.
3. Методології та стандарти тестування на проникнення.
4. Проблемні питання та напрямки досліджень.

Слід зазначити, що інструментарію та сценаріям атак в літературі присвячено досить багато уваги. Зокрема можна згадати такі публікації як [4-6], у яких досить докладно викладені вищезазначені два питання, але саме наявність в установі чітко окресленої методології тестування на проникнення є запорукою системного визначення та перегляду рівня кіберзахисту.

У той же час третє питання не може бути викладене у вигляді підручника або докладного аналітичного звіту у зв'язку з тим, що існуючі методології, як правило, можуть бути порівняні лише в рамках загальних положень. Окрім цього в Україні відсутня єдина затверджена методологія тестування на проникнення. Відповідно, аналіз сучасного стану сформованих методологій тестування на проникнення є актуальним питанням.

Базуючись на роботах [5-12] можна сформувати актуальний перелік сучасних та чинних методологій тестування на проникнення, які в загальному випадку можна використовувати для веб-застосувань:

1. Open Source Security Testing Methodology Manual (OSSTMM). Джерело для ознайомлення: http://www.isecom.org/research/osstmm.html.
2. OWASP testing guide. Джерело для ознайомлення: https://www.owasp.org/index.php/OWASP_Testing_Project.
3. Information Systems Security Assessment Framework (ISSAF) Джерело для ознайомлення: www.oissg.org/issaf.html.
4. Penetration Testing Execution Standard (PTES) Джерело для ознайомлення: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines.
5. NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment (NIST SP 800-115). Джерело для ознайомлення: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

1.2 Основні положення

Методологія – це схема, яка використовується для досягнення мети. Відмова від використання методології для тестування на проникнення може призвести до неповного випробування, високих витрат часу, невдач та

неефективності тестування [5]. Незважаючи на велику кількість і неможливість виділити "правильну методологію" її дотримання має результатом професійне та ефективне тестування на проникнення.

OSSTMM може бути використаний практично для будь-яких типів інспекцій, у тому числі тестування на проникнення, етичне хакерство, оцінка безпеки та визначення вразливостей; він складається з тестових модулів для кожної галузі. До методології входять такі методи, як:

1. Тестування інформаційної безпеки (Information Security Testing);
2. Тестування безпеки процесів (Process Security Testing);
3. Тестування безпеки Інтернет-технологій (Internet Technology Security Testing);
4. Тестування безпеки комунікацій (Communications Security Testing);
5. Тестування безпеки бездротового зв’язку (Wireless Security Testing);
6. Тестування фізичної безпеки (Physical Security Testing).

OWASP Testing Guide може бути використаний на різних етапах життєвого циклу розробки програмного забезпечення як складова частина фреймворку, що використовується, та пропонує конкретне керівництво для слідування в рамках цього процесу. У першу чергу методологія OWASP рекомендується для використання при тестуванні веб-застосувань та включає п’ять етапів:

1. Збір інформації (Information Gathering);

2. Тестування управління конфігурацією (Configuration Management Testing);
3. Тестування автентифікації (Authentication Testing);
4. Тестування управління сесіями (Session Management Testing);
5. Тестування авторизації (Authorization Testing).

Методологія ISSAF розроблена як структурований фреймворк для оцінки різних інформаційних систем. Вона передбачає стандарти оцінки та тестування для різних галузей та включає оцінку безпеки, що відображає реальні сценарії. Процедури тестування на проникнення є такими:

1. Збір інформації (Information Gathering)
2. Побудова мережевих карт (Network Mapping)
3. Ідентифікація вразливостей (Vulnerability Identification)
4. Проникнення (Penetration)
5. Отримання доступу та підвищення прав (Gaining Access and Privilege Escalation)
6. Подальше перерахування (Enumerating Further)
7. Компрометація віддалених користувачів/сайтів (Compromise Remote Users/Sites)
8. Підтримання доступу (Maintaining Access)
9. Приховання слідів (Cover the Tracks)

PTES є методологією, яка повністю зосереджена саме на тестуванні на проникнення та включає практичні технічні керівництва для того, що і як тестувати, настанови щодо раціоналізації тестування та рекомендації щодо інструментарію з тестування на проникнення. У PTES тестування на проникнення визначено в рамках семи етапів:

1. Попередні взаємодії (Pre-engagement Interactions);
2. Збір інформації (Intelligence Gathering);
3. Моделювання загроз (Threat Modeling);
4. Аналіз вразливостей (Vulnerability Analysis);
5. Експлоітація (Exploitation);
6. Пост-експлоітація (Post Exploitation);
7. Звітування (Reporting).

NIST SP 800-115 направлена скоріше не на надання вичерпної інформації щодо тестування безпеки та прогами перевірок, а на огляд ключових елементів тестування та перевірки безпеки з акцентом на специфічні технічні методики.

РОЗДІЛ 2. УПРАВЛІННЯ РИЗИКАМИ

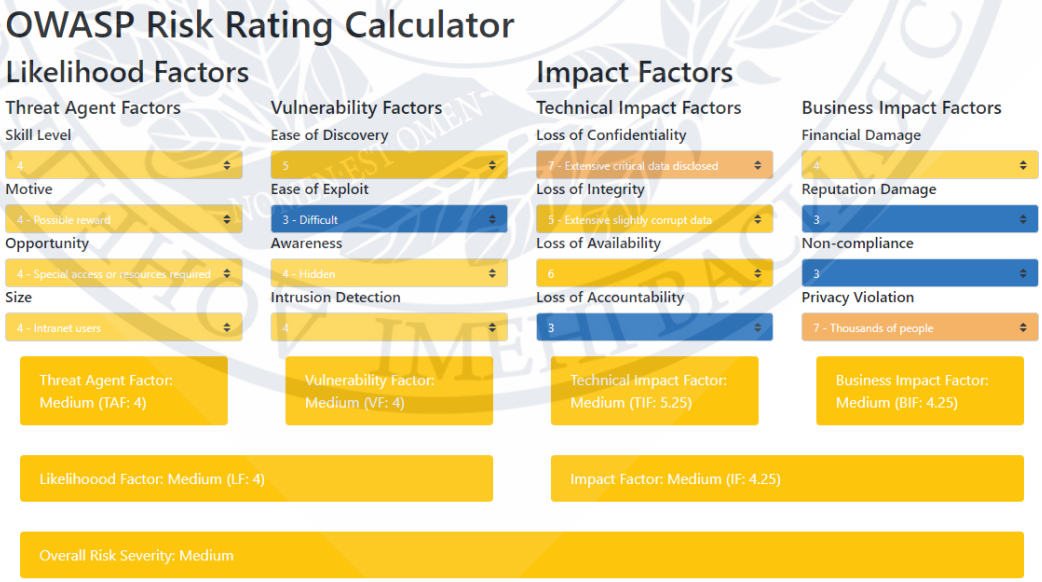
Ризик - це чистий негативний вплив здійснення вразливості, враховуючи і ймовірність і вплив виникнення. Управління ризиками – це процес ідентифікації ризику, оцінки ризику, та вжиття заходів для зниження ризику до прийнятного рівня.

Метою управління ризиком є можливість організації досягти її місії шляхом кращого забезпечення IT-систем, які зберігають, обробляють або передають організаційно інформація; дозволяючи керівництву приймати добре обізнані рішення щодо управління ризиками обґрунтуйте видатки, які є частиною IT-бюджету.

2.1 Оцінка найбільш вірогідних загроз

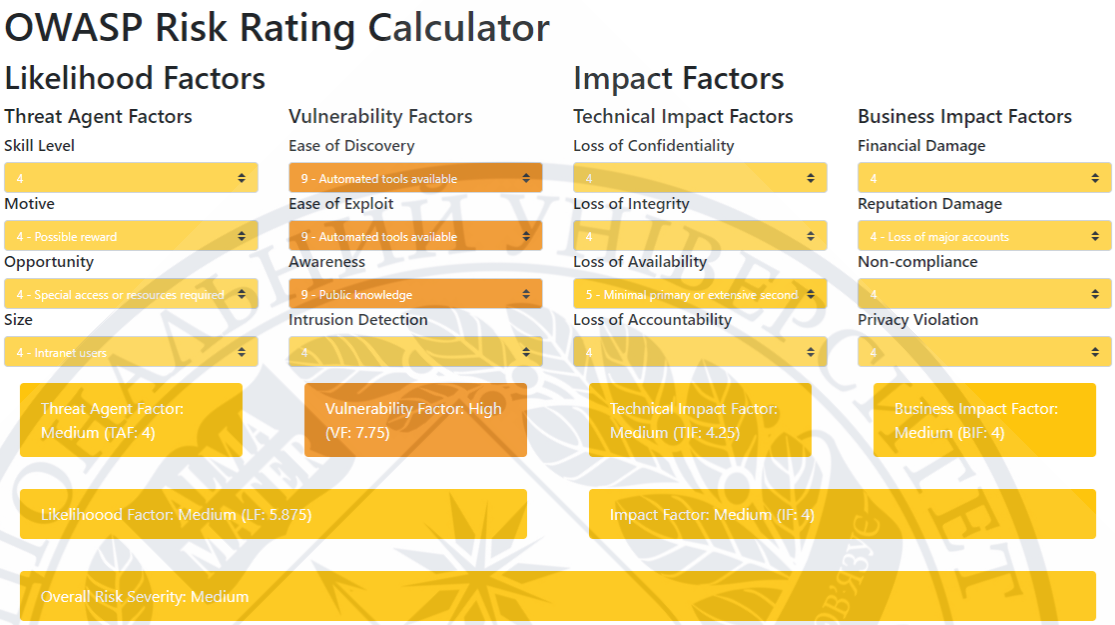
Однією з найкращих методологій для оцінки є Owasp risk assessment methodology, тому оцінка була виконана згідно з нею

1) Зловмисне програмне забезпечення



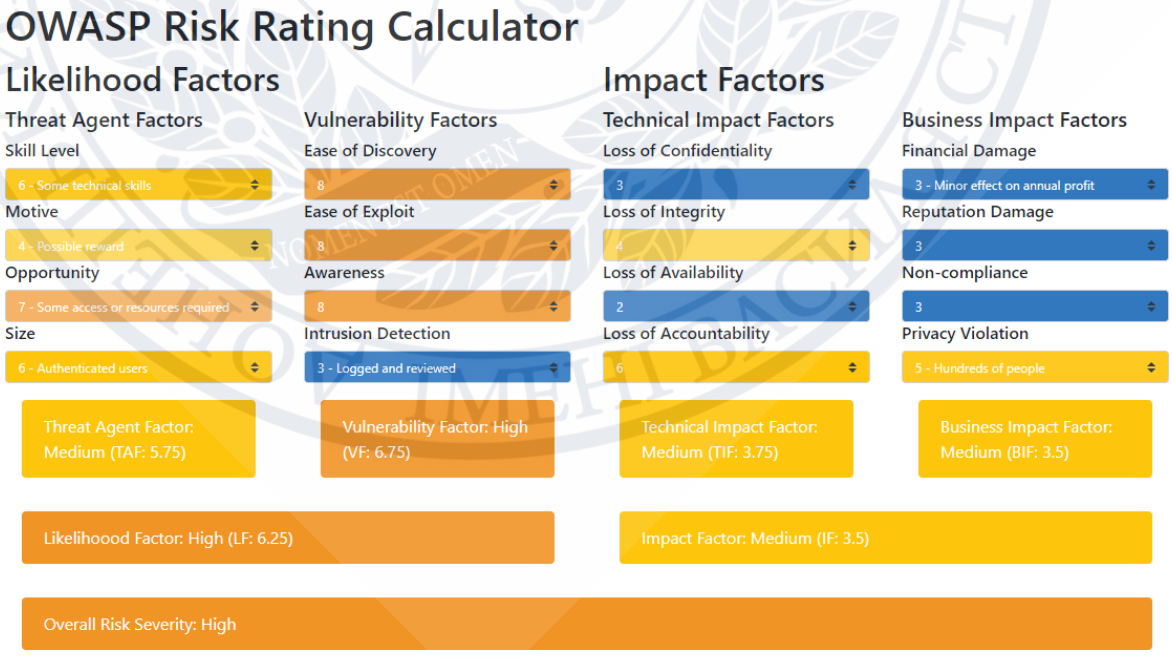
(Рис 2.1.1) Оцінка загрози: Зловмисне програмне забезпечення

2) Невиправлені вразливості безпеки



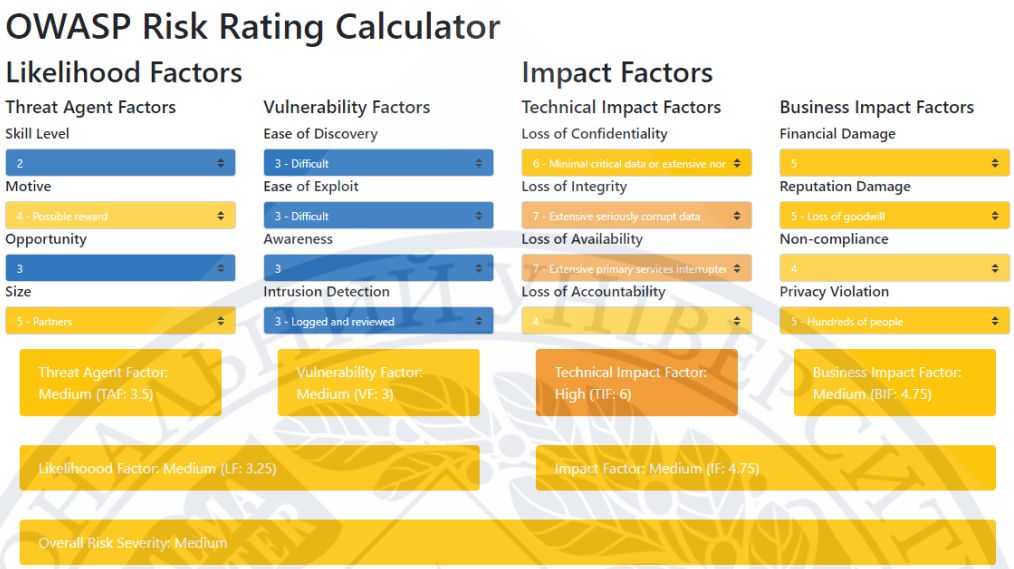
(Рис 2.1.2) Оцінка загрози: Невиправлені вразливості безпеки

3) Вразливості веб додатку



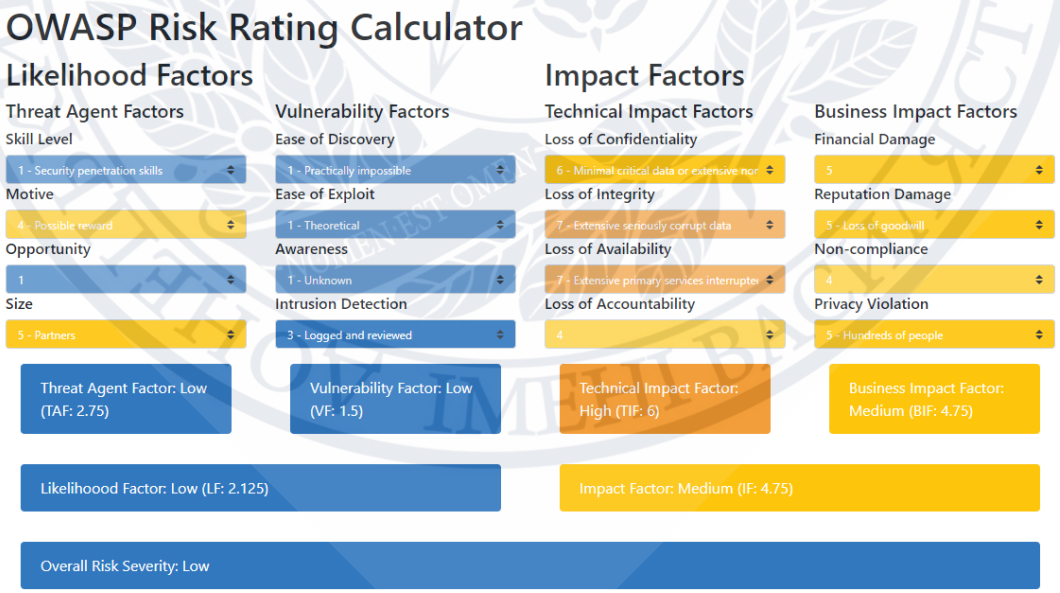
(Рис 2.1.3) Оцінка загрози: Приховані бекдор-програми

4) Привілеї суперкористувача або адміністратора



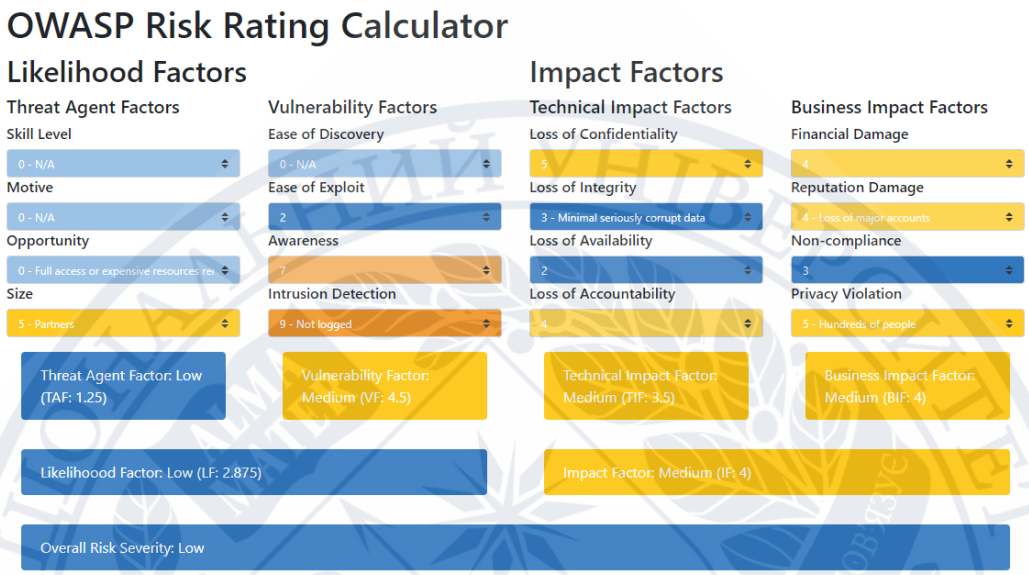
(Рис 2.1.4) Оцінка загрози: Привілеї суперкористувача або адміністратора

5) Невідомі помилки безпеки в програмному або програмному інтерфейсі



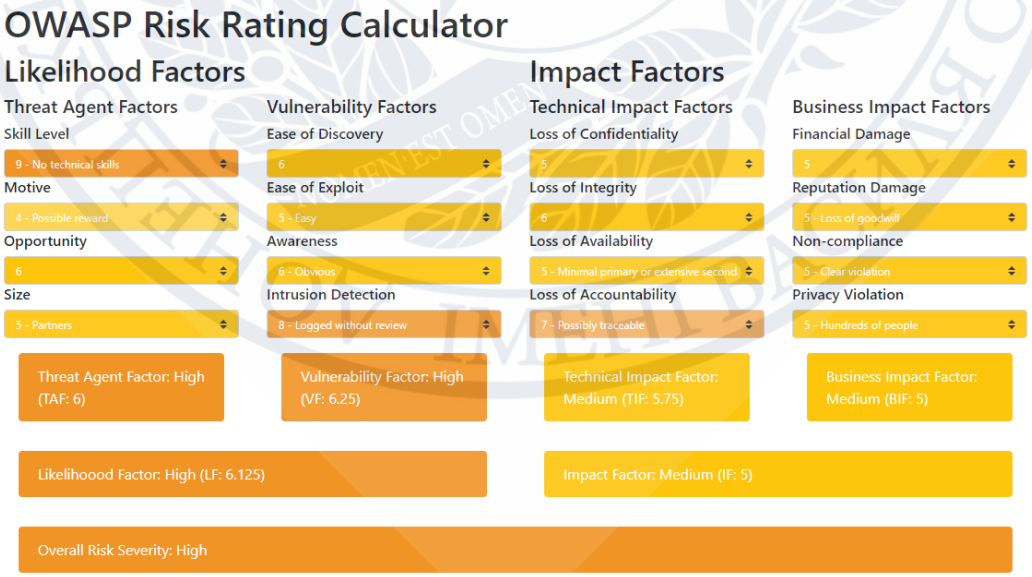
(Рис 2.1.5) Оцінка загрози: Невідомі помилки безпеки в програмному або програмному інтерфейсі

6) Автоматизований запуск скриптів без перевірки на шкідливі програми / віруси



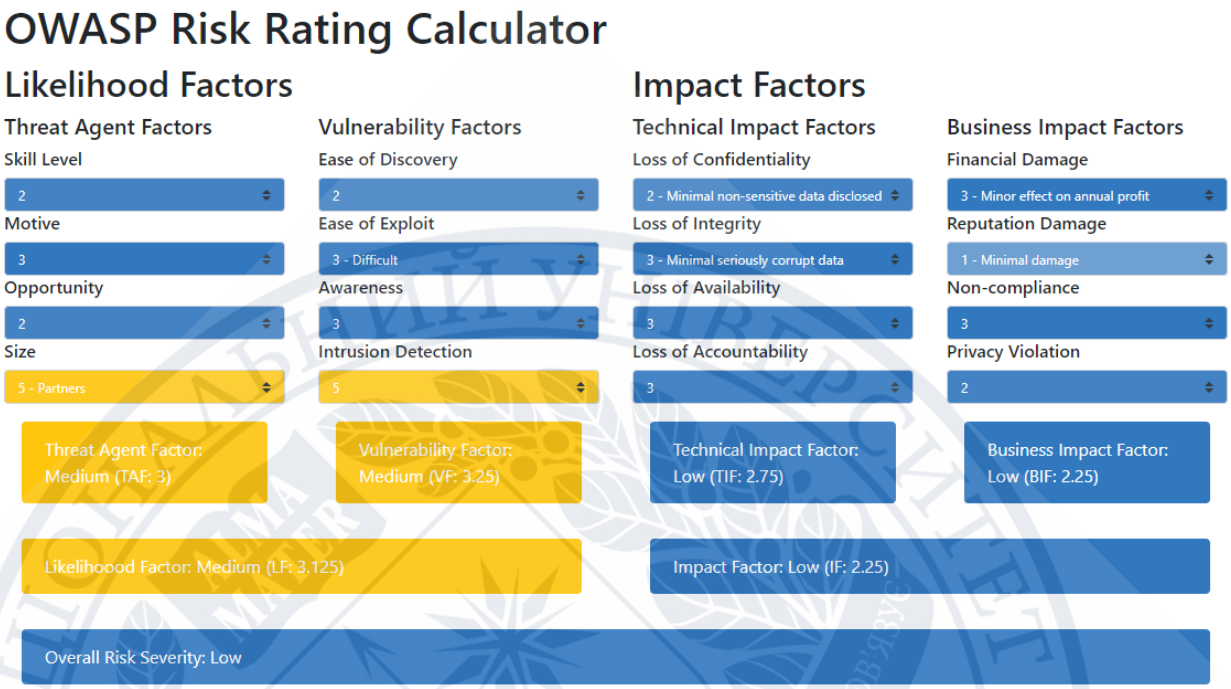
(Рис 2.1.6) Оцінка загрози: Автоматизований запуск скриптів без перевірки на шкідливі програми / віруси

7) Фішингові атаки (соціальна інженерія)



(Рис 2.1.7) Оцінка загрози: Фішингові атаки (соціальна інженерія)

8) Пристрої IoT (інтернету речей)



(Рис 2.1.8) Оцінка загрози: Пристрої IoT (інтернету речей)

2.2 Модель порушника

Таблиця 2.2.1 - Модель порушника

Тип порушника	Опис	Характеристика
Порушник ззовні	Люди, групи людей та організації, які шукають способи завдання шкоди університету, завдяки його залежності від деяких інформаційних та кібер-ресурсів.	Здатність Намір Область діяльності

Студент	Люди, групи людей, які намагаються пройти скрізь захист університету заради тренування та закріплення своїх здібностней, без наміру завдати шкоди.	Здатність

2.3 Визначення рівня загроз

Було обрано наступні ризики для врахування в дану методологію:

Таблиця 2.3.1 - Рівень загроз

Ризик	Рівень ризику
Вразливості веб додатку	9
Фішингові атаки (соціальна інженерія)	8
Невиправлені вразливості безпеки	6
Зловмисне програмне забезпечення	5
Привілеї суперкористувача або адміністратора	5
Автоматизований запуск скриптів без перевірки	4

Згідно з таблицею 2.3.1 методологія повинна в собі містити перевірку захищеності від фішингових атак та атак на вразливості веб додатку.

РОЗДІЛ 3. ОСНОВНІ ПОЛОЖЕННЯ МЕТОДОЛОГІЇ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Хакерство, як це зазвичай визначають, відображає смугу геніальності або блиску у здатності виконувати раніше невідомі способи здійснення дій. У цьому контексті виступати за методологію, якою можна дотримуватися для імітації злому в ареальному світі шляхом етичного злому чи тестування на проникнення, можна суперечити. Причина відстоювання методології в тестуванні на проникнення виникає в тому, що більшість зловмисників дотримуються спільного підходу, коли йдеться про проникнення в систему.

Тест на проникнення імітує методи, що використовуються зловмисниками для отримання несанкціонованого доступу до мережевих систем організації, а потім їх компрометації. Він передбачає використання власних інструментів та інструментів з відкритим кодом для проведення тестування. Окрім автоматизованих методів, тестування на проникнення включає ручні методи проведення цілеспрямованого тестування на конкретних системах, щоб гарантувати відсутність недоліків безпеки, які могли б виявитись раніше. Тестування на проникнення проводиться в корпоративній мережі для досягнення наступних цілей:

- Тестувати та перевіряти ефективність засобів захисту та контролю
- Розкрити перспективи вразливості для мережі, як внутрішньої, так і зовнішньої
- Допомогти визначити пріоритет застосування належних виправлень для повідомлених або відомих вразливостей
- З’ясувати існуючі ризики мереж та систем організації

• Оцінити ефективність мережевих пристроїв захисту, таких як брандмауери, маршрутизатори та веб-сервери

• Забезпечити комплексний підхід для підготовки кроків, які можна вжити для запобігання експлуатації в майбутньому

• Щоб виявити, чи потребує заміну чи оновлення існуюче програмне, апаратне забезпечення або мережева інфраструктура

3.1 Методи тестування на проникнення

• Пасивне дослідження: Пасивні дослідження зазвичай проводяться під час початку зовнішнього тесту на проникнення та надають інформацію про конфігурацію системи організації за допомогою джерел загальнодоступного домену, таких як:

• DNS

• USENET

• ARIN

• ОС фінгерпринтінг : фінгерпринтинг забезпечує огляд конфігурації всієї тестованої мережі. Ці методи призначені для уточнення різних типів послуг, присутніх у цільовій системі.

• Спуфінг : Спуфінг це акт використання однієї машини для того, щоб прикинутися іншою. Методи спуфінгу використовуються як у внутрішньому, так і в зовнішньому тестуванні на проникнення для доступу до комп’ютерів, які налаштовані відповідати лише на певні комп’ютери.

• Мережеве нюхання (Сніфінг): Методи нюхання використовуються для збору даних, коли вони рухаються по мережі. Пакети Sniffeddata можуть допомогти тестувальнику проаналізувати з'єднання трафіку та потік даних по мережі. Мережеве нюхання зазвичай виконується в рамках внутрішнього тестування на проникнення, оскільки дуже легко захоплювати пакети даних всередині мережі.

• Троянські атаки: троянські програми - це зловмисний код або програми, які зазвичай надсилаються до мережі як вкладення електронної пошти або передаються через чати. Тест на проникнення намагається надіслати до мережі спеціально створені троянські програми.

• Атака грубої сили(Брутфорс): Атака грубої сили - найвідоміший метод злому паролів; в основному зловмисник намагається використовувати всі можливі комбінації символів, щоб ефективно зламати пароль. Це може перевантажити систему і, можливо, перешкодити їй відповідати на юридичні запити.

• Сканнування вразливостей. Сканування вразливостей - це всебічне вивчення цільових областей мережевої інфраструктури організації. Це виконується за допомогою автоматизованих інструментів, які перевіряють велику кількість слабких місць, наявних у системі, на відомі вразливості бази даних та діри в безпеці. Він надає практичні інструменти мережевим адміністраторам, які можна використовувати для виявлення вразливостей до того, як атакуючий їх використає.

3.2 Процес тестування на проникнення

Процес проведення тесту на проникнення в організацію повинен бути визначений перед тестуванням мережевих пристроїв та системних вразливостей. Процес тестування на проникнення включає такі процедури:

- Визначення сфери
- Виконання тесту на проникнення
- Звітування результатів

Визначення сфери застосування:

Перед проведенням тесту на проникнення необхідно визначити діапазон тестування. Для різних типів тестування на проникнення існують різні типи мережевих пристроїв. Критерії тестування можуть орієнтуватись на всю

мережу та системи або просто на пристрої, такі як веб-сервери, маршрутизатори, брандмауери, DNS-сервери, поштові сервери та FTP-сервери. Для правильного визначення діапазону тесту необхідно визначити наступні елементи:

- Обсяг тесту
- Завдання тесту
- Географічне розташування тесту
- Персонал для проведення тесту

Після завершення тестування на проникнення тестери безпеки перевіряють всю інформацію, отриману в результаті процедури тестування. Звіт про доставку містить наступну інформацію:

- Список пріоритетних вразливих місць та ризиків
- Інформація, яка стосується сильних і слабких сторін існуючої системи безпеки
- Ризики, класифіковані як високі, середні або низькі
- інформація про вразливості кожного пристрою

Тестери дають рекомендації щодо усунення знайдених вразливостей та надають технічну інформацію про те, як виправити виявлені в системі вразливості. Вони також можуть надати організації корисні ресурси, наприклад, посилання на Інтернет, які можуть бути корисними для пошуку додаткової інформації або виправлень для відновлення знайдених уразливостей.

3.3 Стратегія пен тесту

Зовнішнє тестування на проникнення. Тестування на зовнішнє проникнення не вимагає попереднього знання сайту, топології мережі чи платформи. Виконується детальний аналіз пристроїв безпеки, таких як веб-сервери, маршрутизатори та брандмауери. У цьому типі тестування слід

оцінити вразливості та розгортання на цільових хостах. Сильні та слабкі сторони внутрішньої та зовнішньої архітектури компанії перевіряються через Інтернет. Тестування на зовнішнє проникнення передбачає всебічний аналіз загальнодоступної інформації про ціль, наприклад, наступного:

- Веб-сервери
- Поштові сервери
- Брандмауери
- Маршрутизатори

Внутрішня оцінка безпеки. Тестер проникнення під виглядом уповноваженого користувача атакує систему, щоб перевірити наявність уразливостей. Для внутрішнього тестування на проникнення використовуються ті самі інструменти та методи, що і тестування на зовнішнє проникнення. Цей тест висвітлює такі уразливості:

- Вразливості протоколів та мережевої інфраструктури
- Вразливості операційної системи та додатків сервера, внутрішнього контролю та процедур
- Невідповідні права користувача

Оцінка безпеки додатків. Вразливості програм можна виявити за допомогою тестування, що передбачає віддалене виконання програми, не знаючи внутрішньої роботи програми. Найкращий спосіб проведення тесту - це використання різних вразливостей програми через серію систематичних та повторюваних тестів

Важливими частинами оцінки безпеки додатків є:

- Огляд вихідного коду: огляд вихідного коду допомагає гарантувати, що програма не містить жодної важливої інформації, яку зловмисник може використовувати для використання програми

• Тестування авторизації: виконується для ідентифікації статусу дозволів вхідних систем та допомагає виявити несанкціонований доступ.

• Тестування функціональності: Тестування функціональності тестує системи, які відповідають за правильну функціональність програми.

• Тестування веб-проникнення: У цьому тестуванні команда отримує набір облікових записів з різними рівнями привілеїв, щоб члени команди могли знаходити вразливості типу OWASP

Оцінка безпеки мережі. Цей тест намагається скомпрометувати системи з мережі таким же чином, як це зробив би зловмисник, а потім готує детальний звіт про результати. Він виявляє несправності мережевої безпеки, які можуть призвести до того, що дані або обладнання маніпулюють або знищуються троянами, атаки DoS та інші вторгнення.

Оцінка безпеки бездротового / віддаленого доступу. Оцінка безпеки бездротового / віддаленого доступу стосується ризиків безпеки, пов'язаних з бездротовими пристроями. Деякі бездротові пристрої, яким загрожує безпека, - це бездротові мережі 802.11 та доступ до Інтернету через широкосмуговий доступ. Потрібно вжити запобіжних заходів, щоб архітектура, дизайн та впровадження таких рішень були безпечними.

Оцінка соціальної інженерії. Соціальна інженерія - це техніка, яка використовується зловмисниками для використання людських вразливостей у мережі. Соціальна інженерія - це процедура, при якій використовуються слабкі сторони та доброзичливість людей. Тестери можуть використовувати такі методи, як прослуховування, занурення в смітник, злом паролів співробітників шляхом відгадування та намагання запам’ятати коди доступу, спостерігаючи за людьми

3.4 Вказівки щодо перевірки безпеки

Постійне тестування запобігає виникненню будь-яких інцидентів. Тестування безпеки мережі в таких областях, як конфігурація системи, операції та адміністрування, слід проводити регулярно. Під час процесу тестування мережевої безпеки команда тестування повинна перевірити, чи всі системи налаштовані належним чином із відповідними пристроями. Випробування значного обладнання слід проводити спочатку. Деякі з найбільш важливих і загальнодоступних загальнодоступних систем:

- Брандмауери
- Веб-сервери
- Сервери електронної пошти

Під час тестування слід правильно дотримуватися попереджувальних інструкцій. Існують певні типи тестування, такі як сканування мережі, тестування вразливостей та тестування на проникнення, які вимагають суворої обережності. Тестування може відтворити ознаки нападу, тому дуже важливо, щоб процес тестування проводився скоординовано, з повним знанням та дозволом відповідних посадових осіб.

Політика безпеки повинна слугувати належним орієнтиром для потреб та вимог організації. Тестування може виявити невідомі вразливості, тому включення подій тестування безпеки в процедури управління ризиками може зменшити вразливості.

Професіонали, які пройшли навчання з роботи з системними та мережевими операціями, повинні провести перевірку безпеки. Оскільки завдання системного адміністрування також дуже складне і не обмежується системами, потрібна бути достатня кількість адміністраторів з необхідним рівнем кваліфікації для належного проведення системного адміністрування та тестування безпеки.

Усі системи повинні бути в курсі належних виправлень. Можливо, стане важливим виправити численні системи на основі результатів тестування безпеки. Застосування патчів належним чином може різко зменшити ризик вразливості

Тестування на вразливість може призвести до хибнопозитивних результатів або не виявити деяких типів проблем, що перевищують можливості виявлення інструментів. Тестування на проникнення є цінним доповненням до тестування на вразливість, яке спрямоване на виявлення прихованих вразливостей.

3.5 Оперативні стратегії тестування безпеки

Метою проведення перевірки безпеки є максимізація вигоди. З операційної точки зору, тестування на проникнення допомагає у визначенні стратегій інформаційної безпеки шляхом виявлення вразливостей та вимірювання їх впливу та ймовірності, щоб ними можна було активно керувати. На етапах експлуатації та технічного обслуговування типи та частоти випробувань на проникнення включають процес визначення пріоритетів на основі наступної інформації:

- Категорія безпеки інформаційної системи
- Вартість проведення тестів для кожного типу тесту
- Визначення переваг для систем організації

Рішення, що тестувати на етапі впровадження, включає всі системи, присутні в організації. Старший IT-менеджер повинен брати участь у процесі встановлення пріоритетів

3.6 Фази тестування на проникнення

Згідно з [6-7] у загальному випадку методологія тестування на проникнення має складатися з трьох фаз:

• Фаза перед атакою: Ця фаза орієнтована на збір якомога більше інформації про ціль, яку потрібно атакувати. Наприклад, збір інформації за допомогою сканування, перегляд публічних записів.

• Фаза атаки: інформація, зібрана на фазі перед атакою, є основою стратегії атаки. Під час фази атаки розробляється і здійснюється стратегія атаки.

• Фаза після атаки: Фаза після атаки є важливою частиною процесу тестування, оскільки тестувальник повинен відновити мережу до початкового стану. Це включає очищення процесів тестування та видалення створених вразливостей (не тих, що існували спочатку), створених експлойтів тощо, доки всі перевірені системи не повернуться у початковий стан перед тестуванням.

3.7 Фаза перед атакою

Складається із спроб дослідити потенційну ціль. Зрештою, це зводиться до збору інформації і може включати збір конкурентної інформації, соціальну інженерію, фізичний доступ до ресурсу тощо. Це часто робиться крадькома, і зловмисники зазвичай проводять більше часу у фазі перед атакою, ніж у фазі фактичної атаки.

Інформація, отримана на цьому етапі, може включати:

• Фізичне та логічне розташування організації: На цьому етапі можуть бути використані інструменти та технології відбитків. Приклади включають використання бази даних WHOIS, використання пошукових систем, таких як Google, пошук мережевого блоку за допомогою RIR та пошук на веб-сайті компанії.

• Аналогові з’єднання, включаючи телефонні лінії, факсимільні лінії, комутовані лінії та інші позасмугові зв’язки: їх можна записати для подальшого використання у таких військових дилерів, як PhoneSweep та ToneLoc. Найважливіша функція цього полягає в тому, щоб обійти звичайну

безпеку, яку забезпечують брандмауери, DMZ тощо, використовуючи незахищений модем.

• Особиста інформація: Випробувач може розвідти інші носії інформації, наприклад друковані, для отримання особистої інформації (імен людей та номерів телефонів) або використовувати соціально-інженерні методи для вилучення інформації. Сюди може входити порушення фізичної безпеки (заслінка), занурення в смітник, видавання себе за іншу особу тощо.

• Інформація про інші організації, які пов'язані з університетом: Оскільки безпека настільки ж хороша, як і найслабша ланка, можна порушити безпеку, скориставшись слабкою ланкою. Приклади включають сторонні сайти продавців або партнерів, які використовують установки за замовчуванням компонентів веб-додатків, про які відомо, що вони мають уразливості.

• Будь-яка інша інформація, яка може призвести до можливої експлуатації: Це може включати оголошення про групи повідомлень, прес-релізи і навіть випадкові розмови.

Пасивна розвідка передбачає наступні заходи:

• Картування структур каталогів веб-серверів та FTP-серверів.

• Визначення вартості взаємодії інфраструктури з Інтернетом. Класифікація активів, як це описано в ISO 17799, також може бути проведена тут. Це робиться для того, щоб тест на проникнення зміг кількісно визначити прийнятний ризик для бізнесу.

• Отримання інформації про реєстрацію мережі з баз даних WHOIS, важливої інформації про активи з фінансових веб-сайтів та інформації про ділові послуги, пов'язані із зареєстрованою стороною.

• Просіювання документів: Це стосується збору інформації виключно з опублікованих матеріалів. Сюди входить перегляд вихідного коду веб-

сторінки; визначення ключового персоналу; подальше їх розслідування та загальнодоступна інформація, така як особисті веб-сторінки, особисті адреси електронної пошти, бази даних про роботу та сторінки властивостей програмних копій будь-яких документів

• Соціальна інженерія може бути здійснена шляхом виявлення каналу (людини, на якого можна легко орієнтуватися на основі отриманої інформації про персонал) та профілювання цієї людини. Це може стосуватися позиції, звичок, уподобань, слабких рис тощо. Завданням тут має бути вилучення конфіденційної інформації та каталогізація її в журналі.

Активна розвідка

Процес збору інформації посягає на цільову територію. У цьому випадку зловмисник може надсилати зонди цілі у вигляді сканування портів, розгортки мережі, перерахування акцій та облікових записів користувачів тощо. Зловмисник може застосувати такі методи, як соціальна інженерія, та використовувати інструменти, які автоматично поєднують ці завдання, такі як сканери та снифери. Слід, який залишив зловмисник, більший, і новаків можна легко ідентифікувати.

• Картографування мережі: Складіть карту мережі, отримуючи інформацію з номерів реєстру доменів сервера, виявлених під час фази пасивної розвідки. Блок IP утворює магістраль мережі. Дослідіть мережеві зв’язки як вище, так і нижче. Сюди входять основний та вторинний сервери імен для хостів та субдоменів. Кроки включають:

• Інтерпретація широкомовних відповідей з мережі.

• Якщо ICMP не заблоковано, використовуйте ICMP для підмітання мережі.

• Використовуйте зворотний пошук імен для перевірки адрес

• Картографування периметра: Складіть карту периметра шляхом трасування маршрутизатора для визначення зовнішнього мережевого рівня та маршрутизаторів, а також відстеження системних слідів у веб-журналах та журналах вторгнень. Тестер також може слідувати системним слідам з веб-публікацій та дошок оголошень. Кроки включають:

• Аналіз реакції трасового тракту та картографування периметру за допомогою технік брандмауерки.

• Використання мережевих джерел, таких як Netcraft, щоб дізнатись більше про інфраструктуру інформаційних систем (ІС) та історичні дані про ефективність. Це дасть час роботи сервера для останніх випусків виправлень.

• Ідентифікація системи та служби за допомогою сканування портів: Це, по суті, призведе до ідентифікації активних систем та їх IP-адрес, станів портів (відкритих, закритих чи відфільтрованих), використовуваних протоколів (маршрутизація чи тунелювання), активних служб та типів послуг, послуги типи програм та рівні виправлень, відбитки пальців ОС, ідентифікація версій, внутрішня IP-адресація тощо. Кроки включають:

• Розгортання сканування підключення для всіх хостів у мережі. Використовуйте це через порт 1024 для перерахування портів.

• Розгортання стелс-сканування SYN для портів 20, 21, 22, 23, 25, 80 і 443. Розширте це сканування на діючі системи для виявлення станів портів.

• Розгортання сканування ACK для портів 3100–3150, 10001–10050 та 33500–33550 за допомогою TCP-порту 80 як джерела для проходження брандмауера. Додаткові порти можуть бути перевірені випадковим чином на наявність портів понад 35000 в мережі.

• Розгортання сканування фрагментів у зворотному порядку за допомогою прапорців FIN, NULL та XMAS, встановлених для портів 21, 22,

25, 80 та 443. Це також може бути використано для перерахування підмножини портів на портах тестування фрагментів пакетів за замовчуванням.

• Розгортання сканування FTP відмов та простою для портів 22, 81, 111, 132, 137 та 161 з метою проникнення в DMZ.

• Розгортання сканувань UDP для перевірки фільтрації портів на невеликому підмножині. Якщо він не відфільтрований, його також можна використовувати для переліку портів. Крім того, надсилайте сканування троянських програм до цих портів та отримуйте відповіді на них. • Каталогізуйте всі протоколи, що використовуються. Зверніть увагу на будь-які тунельовані або інкапсульовані протоколи.

• Каталогізація всіх служб, визначених для виявлених портів - відфільтрованих чи ні. Зверніть увагу на переназначення служби та переспрямування системи.

• Каталогізація всіх програм, ідентифікованих за допомогою сканерів, таких як Nmap. Також може бути отримана додаткова інформація, така як рівень виправлення та версія відбитків пальців. Зверніть увагу на передбачуваність послідовності TCP для сканування

• Профілювання веб-сторінок: на цьому етапі буде зроблена спроба скласти профіль та скласти Інтернет-профіль університету . Зібрана інформація буде використана для подальших методів атак, таких як ін'єкція SQL, веб-сервер та злом додатків, викрадення сесії, відмова в обслуговуванні тощо. Етапи включають:

• Каталогізація всіх веб-форм, типів введення користувачем та напрямків подання форм.

• Каталогізація даних конфіденційності в Інтернеті, включаючи типи файлів cookie (постійні чи сеансові), характер та місце зберігання інформації, правила закінчення терміну дії файлів cookie та використовуване шифрування.

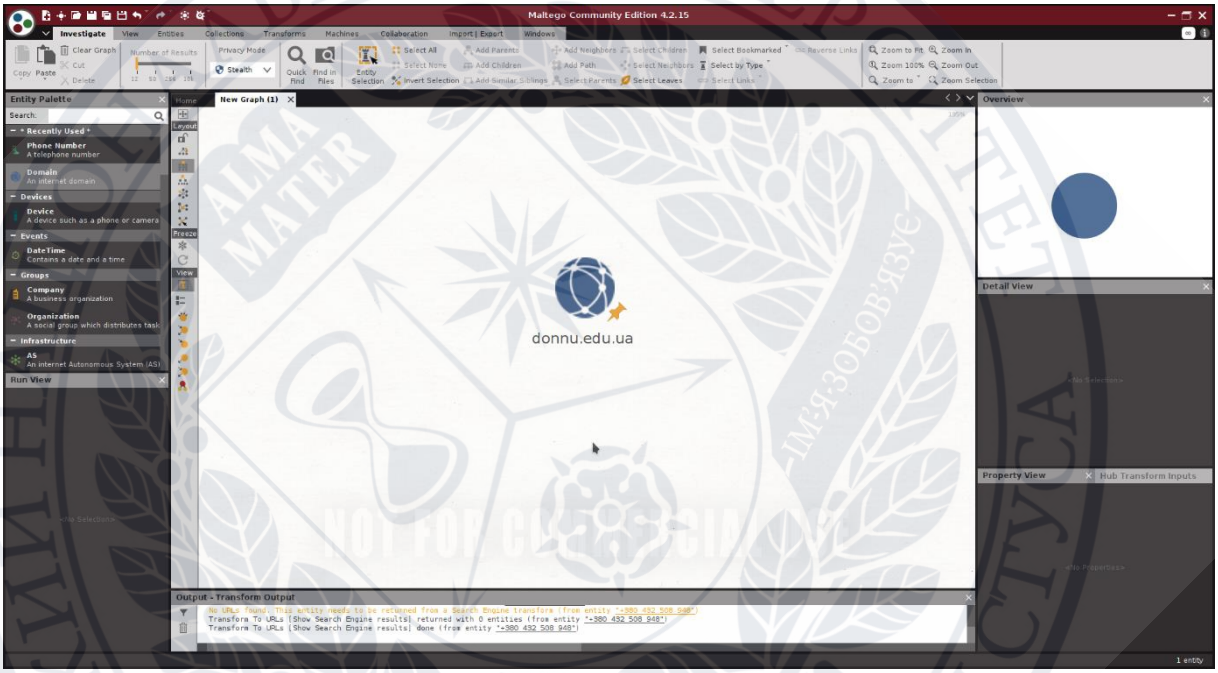
• Каталогізація повідомлень про веб-помилки, помилок у службах, сторонніх посиланнях та додатках. Знайдіть пункт призначення.

Рекомендації щодо інструментарію

Розглянемо пару прикладів проведення тесту на мережі університету.

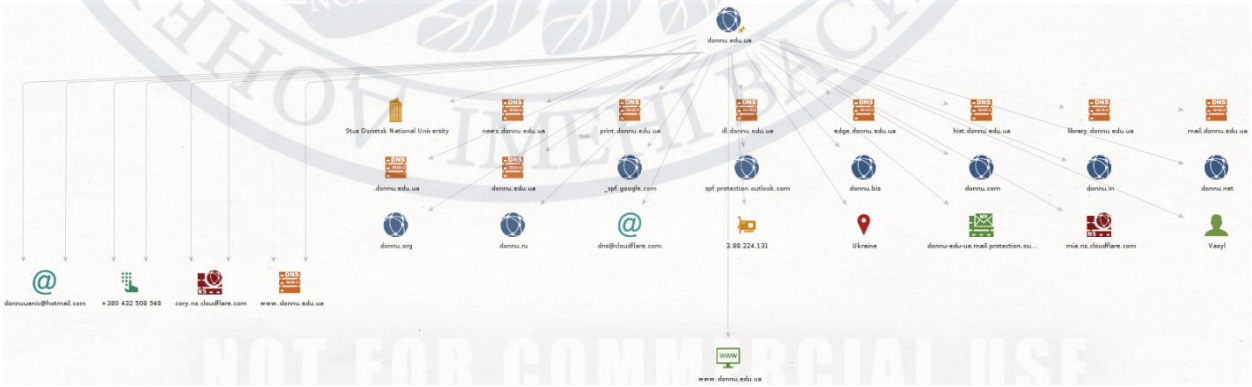
За допомогою Maltego

Створимо в програмі сутність «Домен» и впишемо в неї домен університету.



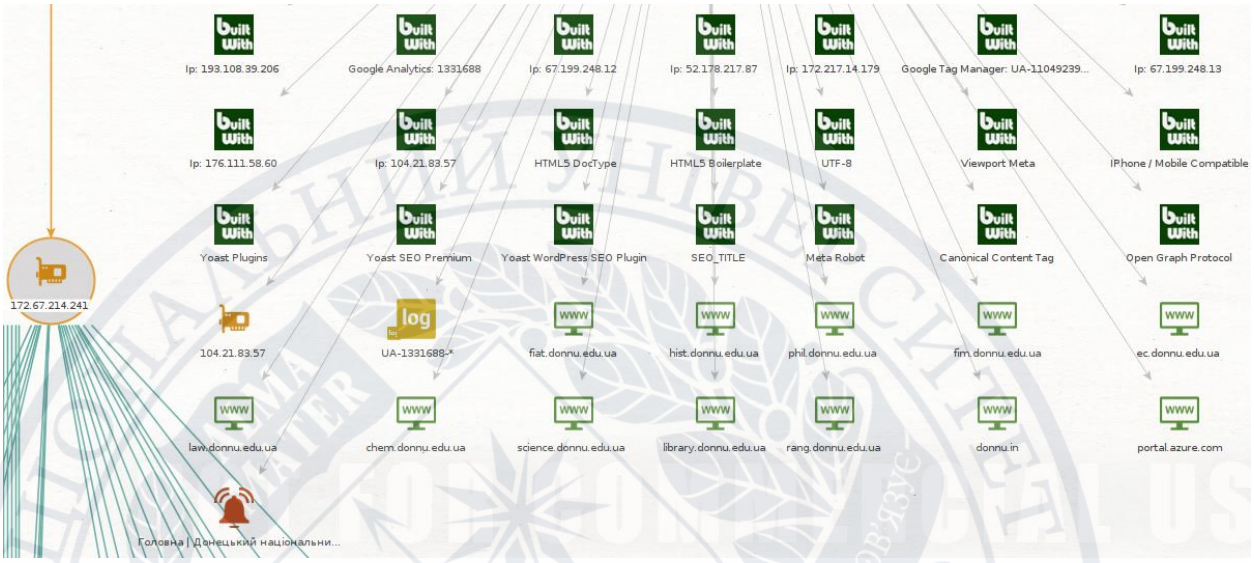
(Рис. 3.7.1) Робоче місце в програмі Maltego

Розпочнемо пошук зі «всіма трансформаціями».



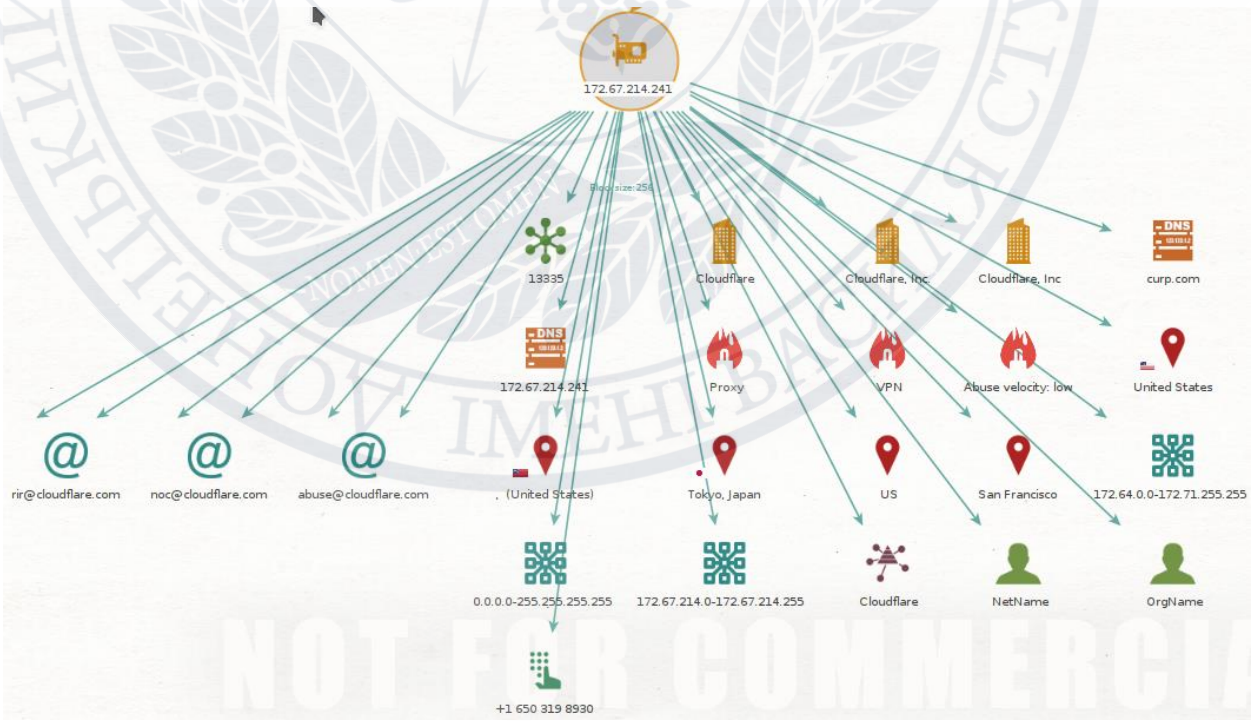
(Рис. 3.7.2**)** Результат пошуку

Дізнаємось про всю мережеву інфраструктуру домену університету: регістр, контактні адреси які потім можуть бути використані для соціальної інженерії. Також ми можемо спостерігти технологію, яку використовує сайт:



(Рис. 3.7.3) Результат пошуку №2

Продовжимо розслідування так здійнимо трансформації на знайденій айпі адресі:

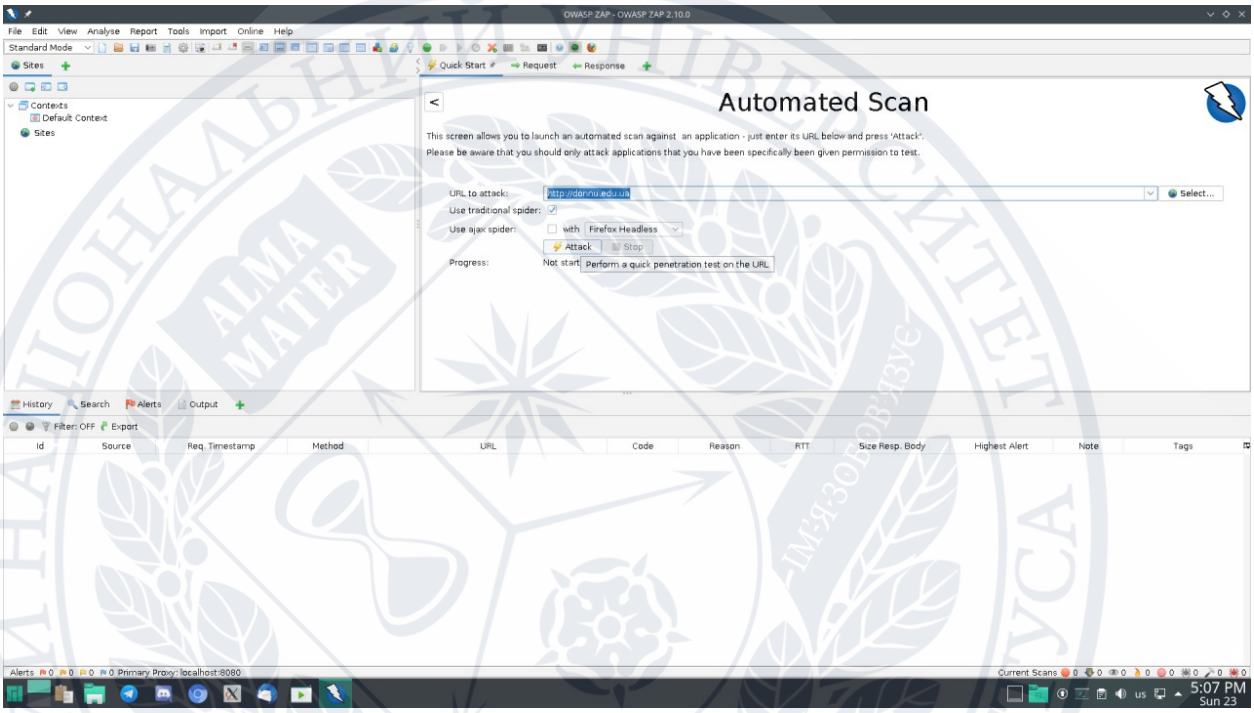


(Рис. 3.7.4**)** Результат пошуку по IP

Бачимо інформацію про хостинг, контактні емейл адреси. Так продовжуємо поки не отримаємо всю можливу потрібну нам інформацію.

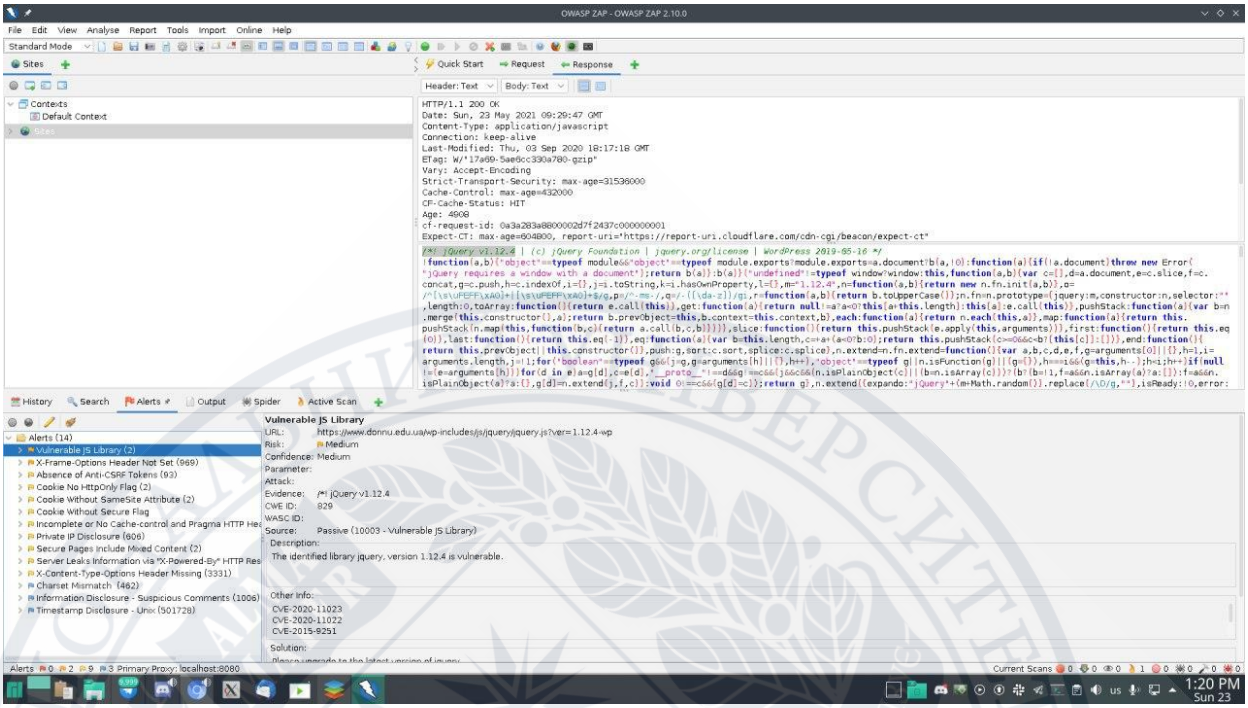
За допомогою OWASP ZAP

Запустимо скан сайту в OWASP ZAP:

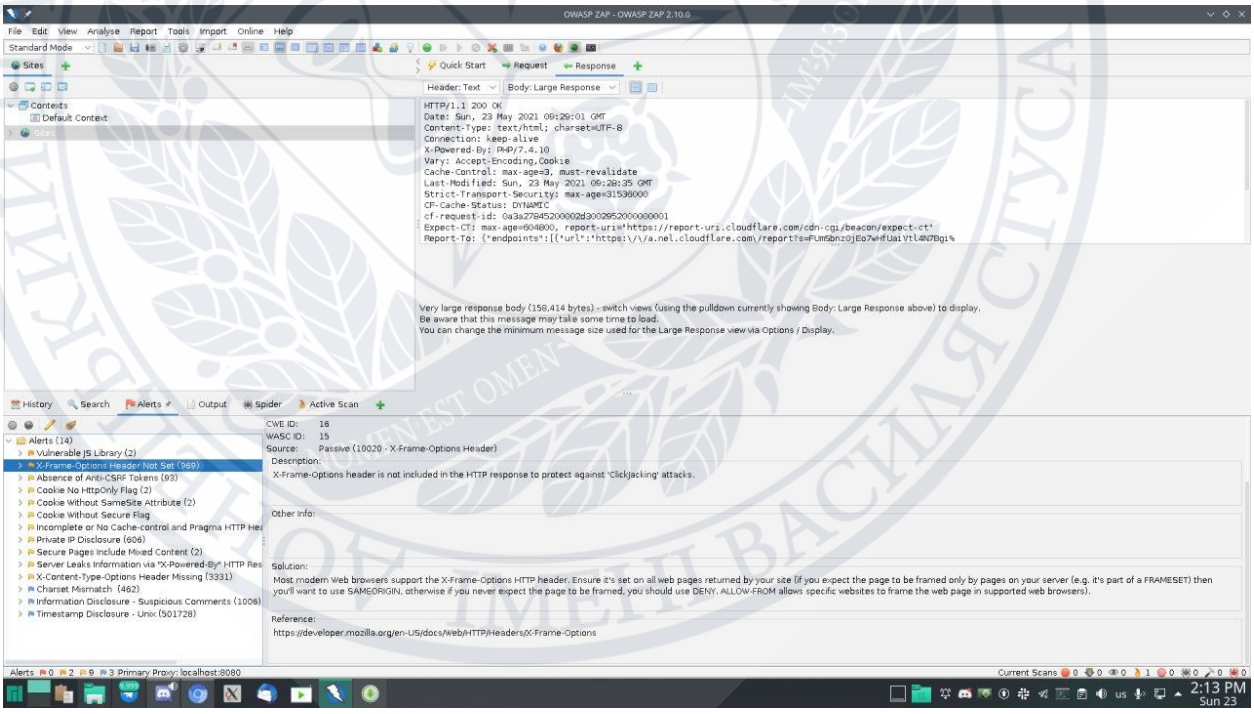


(Рис 3.7.5) Вигляд робочого місця в OWASP ZAP

Після тривалого скану бачимо наступні результати:



(Рис 3.7.6) Результат сканування №1



(Рис 3.7.7) Результат сканування №2

Помічаємо наступні вразливості:

Великий ризик:

• Vulnerable JS Library та можливий спосіб вирішення проблеми – заапдейтити бібліотеку до останньої версії (в попередніх версіях можуть бути відоми діри для взлому).

• X-Frame-Options Header Not Set . Спосів вирішення – впевнитись, що на всіх веб сторінках включена функція X-Frame (веб-сайту може загрожувати атака типу clickjacking. Clickjacking (User Interface redress attack, UI redress attack, UI redressing) тип атаки, який призводить до натискання користувачем іншого об’єкту.)

Середній ризик:

• Absence of Anti-CSRF Tokens - Веб-додаток не дозволяє чи не може в достатній мірі перевірити, чи був навмисно наданий добре сформований, дійсний, послідовний запит користувачем, який подав запит.

• Cookie No HttpOnly Flag - Коли файл cookie встановлений з прапором HttpOnly, він вказує браузеру, що доступ до файлу cookie може здійснюватися тільки сервером, а не скриптами на стороні клієнта.

• Incomplete or No Cache-control and Pragma HTTP Header Set - Для кожної веб-сторінки сайт повинен мати відповідну політику кешування, яка визначає ступінь кешування сторінки та її форм.

• X-Content-Type-Options Header Missing - Відсутність налаштувань заголовка для параметрів типу X-Content, що означає, що він вразливий до MIME sniffing, що може бути використано для атаки типу Cross-Site Scripting (XSS).

Малий ризик:

• Charset mismatched;

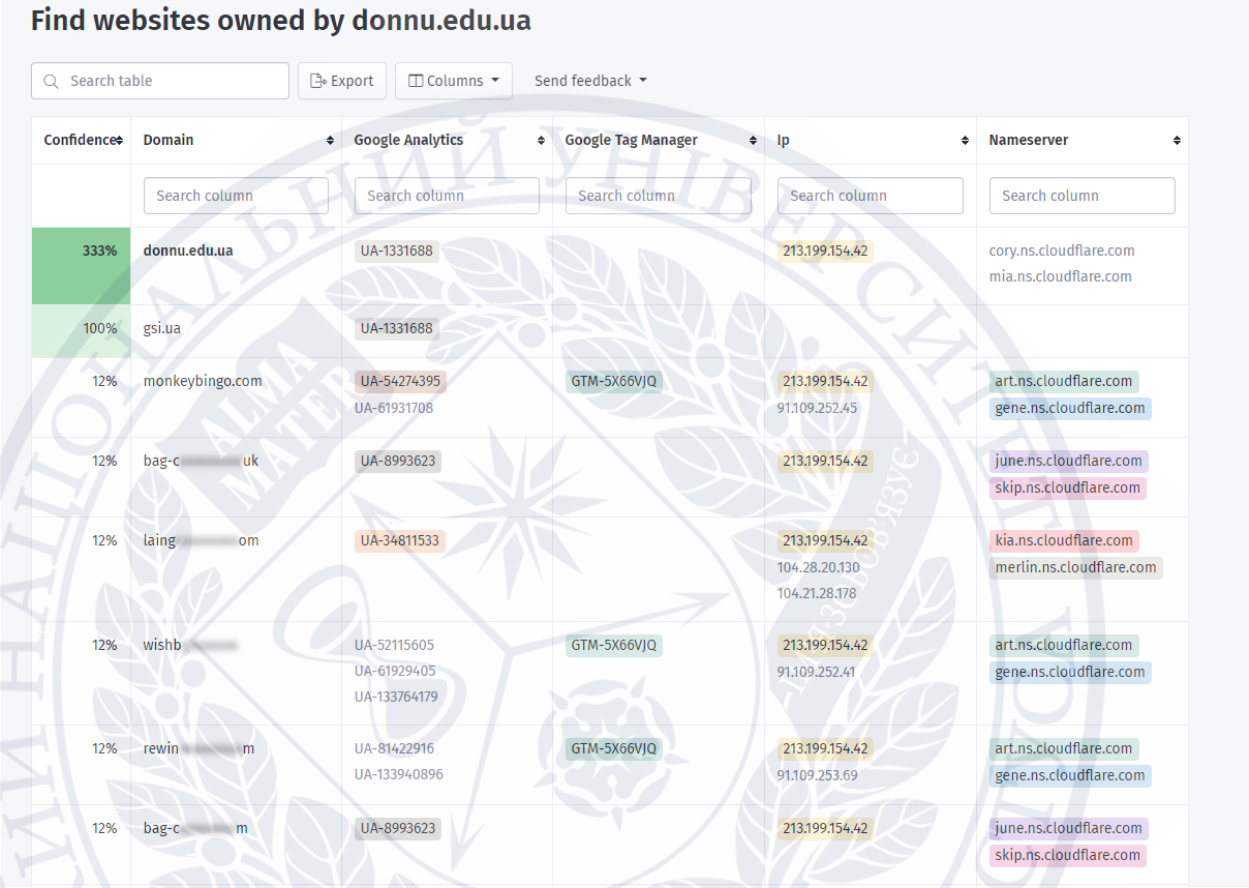
• Information disclosure – Suspicious comments;

• Timestaps disclosure;

За допомогою набору OSINT Framework

На веб сайті https://osintframework.com/ ми можемо спостережити багато можливих способів збору інформації, було обрано сайт https://analyzeid.com/ .

Пошукаємо відомий нам домен університету:



(Рис 3.7.8) Результат пошуку на сайті https://analyzeid.com/

Можемо побачити однаковий гугл-ідентифікатор що вказує нам на те, що веб сайт кооперує з сайтом gsi.ua.

3.8 Фаза атаки

Фаза атаки передбачає фактичний компроміс цілі. Зловмисник може використовувати вразливість, виявлену на етапі перед атакою, або використовувати лазівки в безпеці, такі як слабка політика безпеки, щоб отримати доступ до системи. Важливим моментом тут є те, що, хоча зловмисникові потрібен лише один порт в'їзду, організаціям залишається захищати кілька. Потрапивши всередину, зловмисник може посилити привілеї

та встановити бэкдор, щоб підтримувати доступ до системи та використовувати її.

Випробування периметра

Соціальна інженерія буде постійною діяльністю на етапі тестування, оскільки конфіденційну інформацію можна отримати на будь-якому етапі тестування. Тести, які можна проводити в цьому контексті, включають, але не обмежуючись цим, видавання себе за іншу особу або знущання над телефонними дзвінками для захоплення конфіденційної інформації, перевірку інформації, зібраної в результаті таких заходів, як дайвінг на сміттєвих контейнерах тощо. Інші засоби включають тестування електронної пошти, придбання довіреною особою та спроби отримання законних деталей автентифікації, таких як паролі та привілеї доступу. Інформація, зібрана тут, також може бути використана пізніше при тестуванні веб-додатків.

Тестування брандмауера

Інформація, отримана під час фази перед атакою з використанням таких методів, як брандмауер, далі використовується тут. Здійснюються спроби уникнути IDS та обійти брандмауер. Це включає розробку та надсилання пакетів для перевірки правил брандмауера - наприклад, надсилання пакетів SYN для перевірки стелс-виявлення. Це визначить характер різних реакцій пакетів через брандмауер. Пакет SYN може використовуватися для перерахування цільової мережі. Подібним чином інші сканування портів з різними встановленими прапорами можуть бути використані для спроби перерахування мережі. Це також дасть вказівку контролю вихідного порту на цілі.

Зазвичай тестування периметра вимірює здатність брандмауера обробляти фрагментацію, фрагменти великих пакетів, фрагменти, що

перекриваються, потоки пакетів тощо. Методи тестування безпеки периметра включають, але не обмежуються ними, наступні методи:

• Оцінка звітності про помилки та управління помилками за допомогою зондів ICMP

• Перевірка списків контролю доступу за допомогою створених пакетів

• Вимірювання порогу відмови в обслуговуванні шляхом спроб постійних TCP-з'єднань, оцінки тимчасових TCP-з'єднань і спроб потокового з'єднання UDP

• Оцінка правил фільтрації протоколів шляхом спроби з'єднання за допомогою різних протоколів, таких як SSH, FTP та telnet

• Оцінка можливості IDS в обхід шкідливого вмісту (наприклад, неправильно сформовані URL-адреси) та різне сканування цілі на відповідь на ненормальний трафік

• Вивчення реакції системи захисту периметра на сканування веб-сервера за допомогою декількох методів, таких як post, DELETE і COPY

Тестування веб-додатків І

Етап тестування веб-додатків може проводитись у міру того, як тестер продовжує здобувати ціль.

• Перевірка вхідних даних: Тести включають введення команд ОС, ін'єкцію сценарію, ін'єкцію SQL, ін'єкцію LDAP та сценарії між сайтами. Інші тести включають перевірку залежності від зовнішніх даних та перевірку джерела.

• Дезінфекція вихідних даних: Тести включають аналіз спеціальних символів та перевірку перевірки помилок у додатку.

• Перевірка переповнення буфера: Тести включають атаки на переповнення стека, переповнення купи та переповнення рядка формату.

• Контроль доступу: Контроль доступу перевіряє доступ до адміністративних інтерфейсів, надсилає дані для маніпулювання полями форми, робить спроби рядків запитів URL-адреси, змінює значення на скрипті на стороні клієнта та атакує файли cookie. Інші тести включають перевірку на наявність порушень авторизації, провали в послідовностях обробки подій, обробку проксі-сервера та дотримання правила доступу з найменшими привілеями.

• Відмова в обслуговуванні: Тест на вразливість DoS викликається неправильним введенням даних користувача, блокуванням користувача та блокуванням програми через перевантаження трафіку, запити на транзакції або надмірні запити на додаток.

Тестування веб-додатків II

• Перевірка компонентів: Перевірте наявність засобів контролю на веб-сервері / компонентах програми, які можуть піддавати веб-програму таким уразливостям, як основна автентифікація.

• Перевірка даних та помилок: Перевірте наявність порушень безпеки, пов’язаних із даними, таких як зберігання конфіденційних даних у кеші або введення конфіденційних даних за допомогою HTML. Перевірте наявність детальних повідомлень про помилки, які надають більше деталей програми та типів помилок, ніж потрібно.

• Методи введення SQL: може бути здійснена спроба введення SQL проти веб-програми, щоб отримати доступ до цільової системи.

• Перевірка конфіденційності: для програм, що використовують захищені протоколи та шифрування, перевіряйте наявність провалів у механізмах обміну ключами, неадекватну довжину ключа та слабкі алгоритми. Перевірте схему автентифікації, спробувавши перерахування користувачів за

допомогою входу або процесу відновлення. Перевірте процес перевірки цифрового сертифіката та підпису.

• Управління сесіями: Перевірка дійсності маркерів сесії, довжини маркерів та закінчення терміну дії маркерів сеансу під час переходу з SSL на ресурси, що не є SSL; наявність будь-яких токенів сеансу в історії браузера або кеш-пам'яті; і випадковість ідентифікатора сеансу (перевірка використання даних користувача при генерації ідентифікатора).

• Перевірка конфігурації: Спробуйте маніпулювати ресурсами за допомогою HTTP-методів, таких як DELETE та PUT, перевірити наявність вмісту версії та будь-який видимий обмежений вихідний код у відкритих доменах, каталог спроб та список файлів, а також перевірити наявність уразливостей та доступність адміністративних інтерфейсів на сервері. та серверні компоненти.

Тестування бездротового зв'язку

Якщо організація має бездротову мережу, можна здійснити наступні дії. Це не вичерпний перелік, і тестувальникові рекомендується оновити список новими методами тестування. Діяльність включає такі методи:

• Перевірте, чи легко ідентифікатор набору послуг (SSID) точки доступу доступний легко. Перевірте, чи не передає якась точка доступу SSID, і перевірте, чи можна через це отримати доступ до локальної мережі. Тести можуть включати вимушування грубого ряду символів SSID за допомогою таких інструментів, як Kismet.

• Перевірте наявність уразливостей при доступі до WLAN через бездротовий маршрутизатор, точку доступу або шлюз. Це може включати перевірку того, чи можна зафіксувати та розшифрувати ключ шифрування дротової еквівалентної конфіденційності (WEP).

• Проведіть перевірку маяка будь-якої точки доступу та перевірте всі протоколи, доступні через точки доступу. Перевірте, чи замість концентраторів для підключення точки доступу використовуються мережі з комутацією рівня 2.

• Аутентифікація суб’єкта для відтворення попередніх автентифікацій з метою перевірки посилення привілеїв та несанкціонованого доступу.

• Перевірте, чи надається доступ лише клієнтським машинам з зареєстрованими MAC-адресами.

Придбання цілі

Зазвичай під цільовим набором маються на увазі всі види діяльності, які проводяться для того, щоб розкопати якомога більше інформації про певну машину або систему, щоб вона могла бути використана пізніше в процесі реальної експлуатації. Придбання цілі відноситься до набору заходів, при яких тестувальник піддає цільову машину більш нав'язливим проблемам, таким як сканування вразливості та оцінка безпеки. Це робиться для отримання більше інформації про ціль, яка може бути використана на етапі експлуатації

Приклади такої діяльності включають піддавання машини наступним процедурам:

• Активні зондування: це може використовувати результати сканування мережі для збору додаткової інформації, яка може призвести до компромісу.

• Запуск сканування вразливості. На цьому етапі сканування вразливості завершується.

• Довірені системи та оцінка довірених процесів: Сюди входить спроба отримати доступ до ресурсів машини, використовуючи законну інформацію, отриману за допомогою соціальної інженерії або іншими способами.

Ескалація привілеїв

Після того, як ціль отримана, тестувальник намагається використати систему та отримати більший доступ до захищених ресурсів.

Діяльність включає такі методи:

• Тестер може скористатися поганою політикою безпеки, електронною поштою або небезпечними веб-кодами для збору інформації, яка може призвести до ескалації привілеїв.

• Використання таких методів, як груба сила, для досягнення привілейованого статусу. Інструменти для цієї мети включають GetAdmin та зломщики паролів.

• Використання троянських програм і аналізаторів протоколів.

• Використання інформації, зібраної за допомогою таких методів, як соціальна інженерія, для отримання несанкціонованого доступу до привілейованих ресурсів.

Виконання, імплантація та втягнення

На цьому етапі тестер ефективно компрометує отриману систему, виконуючи довільний код. Завдання тут - дослідити, наскільки безпека зазнає збою. Тестер спробує виконати довільний код, приховати файли в порушеній системі та залишити систему, не викликаючи тривог. Потім тестер спробує повторно ввести систему в крадіжку. Діяльність включає такі процеси:

• Виконання вже наявних або спеціально створених експлойтів, щоб скористатися перевагами вразливостей, визначених у цільовій системі.

• Піддавання системи атакам відмови в обслуговуванні. Це може бути здійснено і на попередньому етапі.

• Використання переповнення буфера, щоб обдурити систему на запуск довільного коду. Тестер може породити віддалену оболонку та спробувати завантажити файли та приховати їх у системі.

• Виконання заходів, які, як правило, зазнають заходів стримування, таких як використання троянських програм і руткітів. Тестер також може використовувати віруси, які користуються перевагами вразливостей для використання системи. Встановлення руткіта або трояна, які можуть призвести до доступу до більш важливих систем, також може бути частиною процесу тестування.

• Видалення журнальних файлів або маскування модифікацій для уникнення юридичних наслідків. Діяльність на етапі відкликання включає маніпуляції з журналами журналів аудиту для видалення слідів діяльності. Прикладами є використання таких інструментів, як Auditpol. Тестер також може змінити налаштування в системі, щоб залишатися непомітним під час повторного входу, зміни параметрів журналу тощо.

• Повторний доступ до системи за допомогою заднього вікна, імплантованого тестером

Рекомендації щодо інструментарію

За допомогою XSStrike

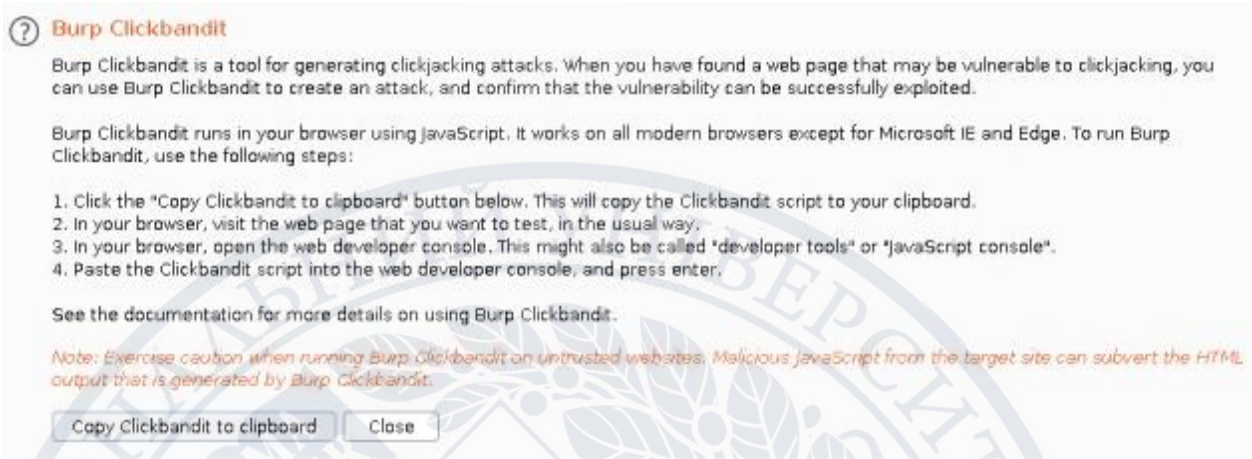
Спробуймо перевірити можливість крос-скріптингової атаки, яку раніше було знайдено за допомогою OWASP ZAP:

(Рис 3.8.1) Результат виконання XSStrike

Як ми бачимо, на захисту веб додатку стоїть файрвол, який надає компанія CloudFlare. Тому крос-скриптінгові атаки сайту не страшні.

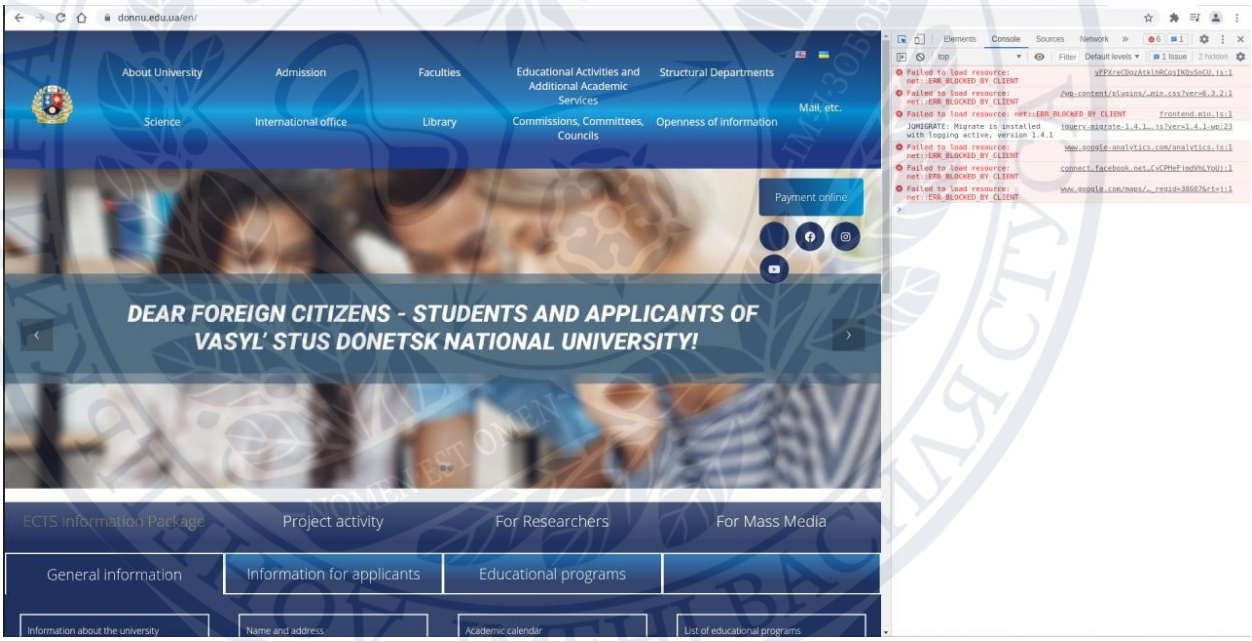
За допомогою BurpSuite

OWASP ZAP так знайшов важливу вразливість атаки типу Clickjacking. Для її перевірки скористаємось можливістю Burp'а під назвою Clickbandit:



(Рис 3.8.2) Вікно з Burp Clickbandit'ом

Кнопку, яку надає нам бурп потрібно вставити до консолі сайту.



(Рис 3.8.3) Перегляд стану консолі на сайті

Як бачимо на веб-додатку стоїть блок доступу до консолі, тому атака типу Clickjacking сайту не загрожує.

3.9 Фаза та дії після атаки

Цей етап є критичним для будь-якого тесту на проникнення, оскільки відповідальність тестера полягає у відновленні систем до попереднього стану. Метою тесту є показати, де безпека виходить з ладу, і якщо не існує масштабування угоди про тестування на проникнення, згідно з якою на тестера покладається відповідальність за виправлення положення безпеки систем, цей етап повинен бути завершений.

Діяльність на цій фазі включає такі процеси:

• Видалення всіх файлів, завантажених до системи

• Очищення всіх записів реєстру та видалення всіх уразливих місць

• Зміна всіх файлів та налаштувань налаштувань, зроблених під час тесту

• Скасування всіх змін у привілеях та налаштуваннях користувача

• Видалення всіх інструментів та експлойтів із перевірених систем

• Відновлення мережі до етапу попереднього тестування шляхом видалення спільних ресурсів та з'єднань

• Документування та фіксація всіх журналів, зареєстрованих під час тесту

• Аналіз усіх результатів та представлення їх організації

Висновок

1. На основі аналізу найбільш використованих методологій встановлено, що кількість етапів у різних методологіях відрізняються і можуть складати від 5 до 9, і кожна з розглянутих методологій має узагальнене наповнення та використовується для широкого застосування, що є недоліком при потребі вузьконаправленого процесу тестування на проникнення. Тому запропоновано виділити в метології, що розробляється три загальних блока у послідовності тестування на проникнення:

1. Збір інформації та її аналіз та підготовка до тестування(Фаза перед атакою);
2. Проведення тестування(Фаза атаки);
3. Звітування та переведення системи у початковий стан(Фаза після атаки).

2. На основі аналізу та оцінки ризиків використовувалась методологія OWASP. Було виділено 4 ризики, які мають найбільш високий рівень небезпеки та які були враховані методології на проникнення, що пропонується

3. Була запропонована методологія на проникнення, яка складається з трьох раніше зазначених фаз, та в якій наводяться рекомендації щодо точок входу в систему на які треба звертати найбільшу увагу.

1. Фаза перед атакою;
2. Фаза атаки;
3. Фаза після атаки.

Відповідно до аналізу ризиків було запропоновано наступний інструментарій:

1. Maltego Teeth;
2. Owasp Zap;
3. OSINT Framework.

4. XSStrike
5. BurpSuite

СПИСОК ЛІТЕРАТУРИ

1. Барибін О.І. Сучасні методології тестування на проникнення. *Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку: збірник матеріалів наукового круглого столу, м. Маріуполь, 2018.*

2. Mohit R. Python Penetration Testing Essentials / Raj Mohit. – Birmingham: Packt Publishing Ltd, 2015.

3. Bertoglio D. D. Overview and open issues on penetration test / D. D. Bertoglio, A. F. Zorzo. // Journal of the Brazilian Computer Society, 2017.

4‘. Penetration Testing: A Survival Guide / [W. Halton, B. Weaver, J. A. Ansari та ін.]. – Birmingham: Packt Publishing Ltd, 2016.

5. Oriyano S. Penetration testing essentials / Sean-Philip Oriyano. – Indianapolis: John Wiley & Sons, Inc., 2017.

6. Mirjalili M. A survey on web penetration test / M. Mirjalili, A. Nowroozi, M. Alidoosti. // Advances in Computer Science: an International Journal, 2014.

7. Phong C. T. A Study of Penetration Testing Tools and Approaches. Master thesis of Computer and Information Sciences. *Auckland University of Technology*. 2014.

8. Meucci V. and Muller A. OWASP Testing guide 4.0 release. *Creative Commons (CC) Attribution Share-Alike*, 2014.

9. Shanley A., Johnstone M. N. Selection of penetration testing methodologies: A comparison and evaluation. *The Proceedings of [the] 13th Australian Information Security Management Conference*, 2015.

10. Kang Y.-S., Cho H.-H., Shin Y. and Kim J.-B. Comparative Study of Penetration Test Methods. *Advanced Science and Technology Letters*, 2015.

11. Порошин С. М., Можаєв О. О., Можаєв М. О. Методологія проведення pen-тестування веб-додатків. *Системи обробки інформації*, 2016.

12. Patel Y., Sheth R. Web Services Pen-testing Framework for Cyber Security : A Review. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2017.