МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»

КАФЕДРА ТВЕРДОТІЛЬНОЇ ЕЛЕКТРОНІКИ
ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Б.В. Маліцький, О.С. Черепов, Т.В. Матьовка, В.М. Різак

ПРАКТИКА СТУДЕНТІВ НА КІБЕРПОЛІГОНІ КАФЕДРИ ТВЕРДОТІЛЬНОЇ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УЖГОРОДСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ

Методичний посібник

Ужгород - 2024

Б.В. Маліцький, О.С. Черепов, Т.В. Матьовка, В.М. Різак. Практика студентів на кіберполігоні кафедри твердотільної електроніки та інформаційної безпеки Ужгородського національного університету: методичний посібник. – Ужгород – 2024. 55 с.

РЕЦЕНЗЕНТИ:

доктор фізико-математичних наук, професор, завідувач Ужгородської лабораторії матеріалів оптоелектроніки та фотоніки Інституту проблем реєстрації інформації НАН України, Академік Академії технологічних наук України.
РУБІШ В.М.

доктор технічних наук, провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
ДАВИДЕНКО А.М.

У методичному посібнику для практики наведено завдання та загальні інструкції роботи під час проходження практики на полігоні кібербезпеки кафедри твердотільної електроніки та інформаційної безпеки ДВНЗ «Ужгородський національний університет».

Для студентів галузі вищої освіти 12 «Інформаційні технології» та суміжних галузей освіти.

Друкується в авторській редакції.

Методичний посібник рекомендований до видання на засіданні Вченої ради фізичного факультету ДВНЗ «Ужгородський національний університет» (протокол №4 від 17.01.2024 р.)

ЗМІСТ

ВСТУП

Практика у сфері кібербезпеки студентів ДВНЗ «Ужгородський національний університет» є невід'ємною частиною освітньо-професійної програми підготовки фахівців, основним завданням якої є практична підготовка студентів освітньої галузі 12 Інформаційні технології, та інших суміжних галузей. Більшість практик проводиться на оснащених відповідним чином базах університету та інших навчальних закладів, а також на підприємствах, установах, організаціях різних галузей господарства і державного управління. Практика студентів спеціальності 125 Кібербезпека та захист інформації ДВНЗ «Ужгородський національний університет» проводиться на базі створеного кіберполігону кафедри твердотільної електроніки та інформаційної безпеки.

Метою практики є оволодіння студентами сучасними методами, формами організації та знаряддями праці в галузі кібербезпеки, формування в них, на базі одержаних у вищому навчальному закладі знань, професійних умінь і навичок для прийняття самостійних рішень під час конкретної роботи в реальних ринкових і виробничих умовах, виховання потреби систематично поновлювати свої знання та творчо їх застосовувати в практичній діяльності. Під час практики поглиблюються та закріплюються теоретичні знання з усіх дисциплін навчального плану.

Цей посібник містить основні сценарії для проведення практики студентів галузі вищої освіти 12 Інформаційні технології, а також суміжних галузей, на базі полігону кібербезпеки для проведення комплексного навчання багаторівневого захисту від кібератак кафедри твердотільної електроніки та інформаційної безпеки ДВНЗ «Ужгородський національний університет».

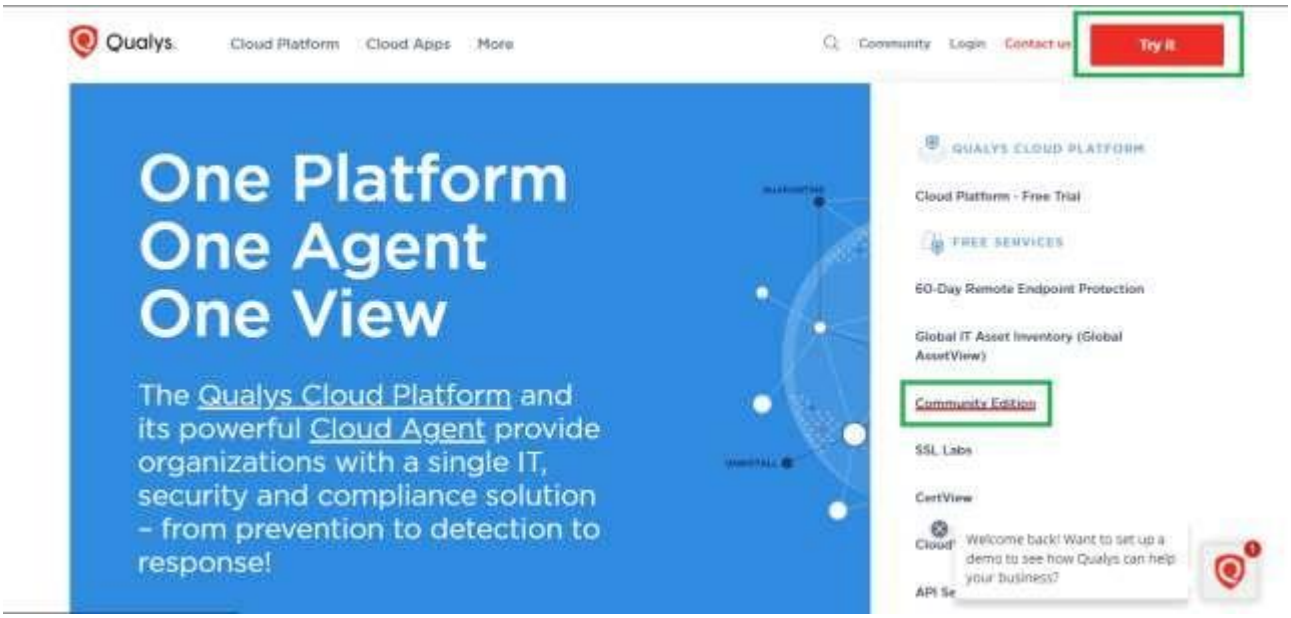
РОЗДІЛ 1. СКАНУВАННЯ ВЕБ-ДОДАТКУ НА ВРАЗЛИВОСТІ В СИСТЕМІ QUALYS

Цей сценарій роботи полягає в скануванні створеного власноруч веб-додатку на вразливості за допомогою можливостей програмного забезпечення Qualys та представлення результатів сканування в звіті.

1.1. Реєстрація в системі Qualys

Для початку роботи з системою Qualys необхідно пройти процес реєстрації в ній:

1. Перейти за посиланням *qualys.com* щоб відкрити веб-сайт системи Qualys.
2. У відкритій сторінці натиснути на «Try It».
3. Після цього з’явиться випадаючий список, в якому необхідно вибрати варіант «Community Edition».

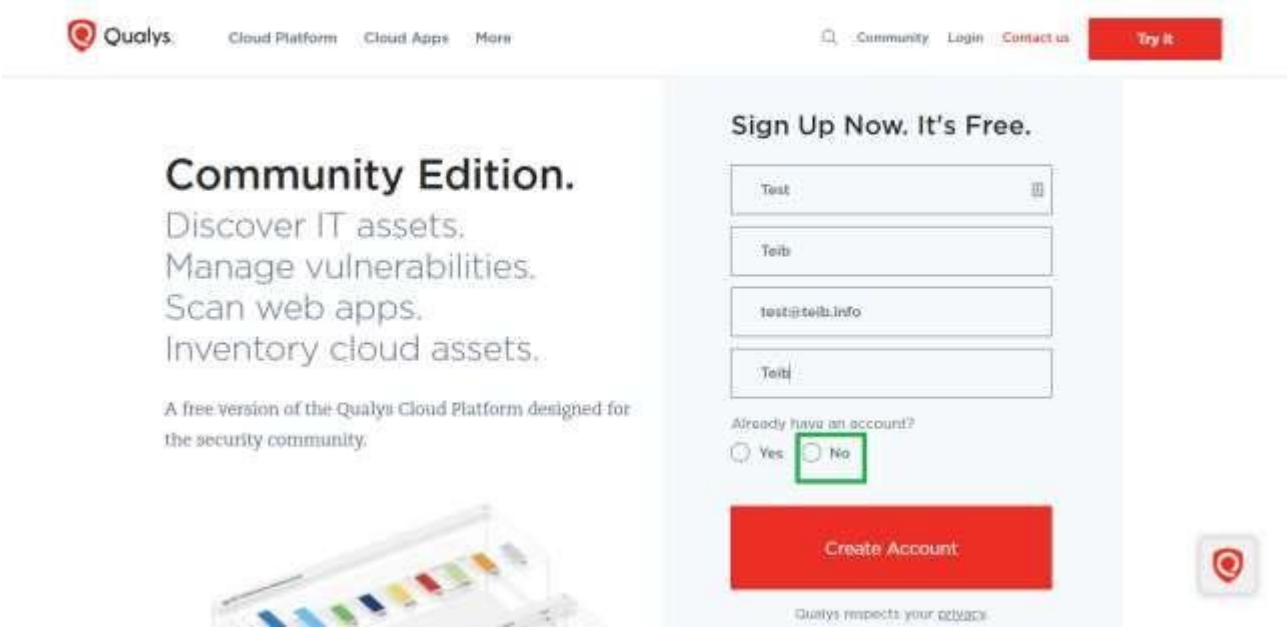


4. Після завантаження сторінки, на екрані з’явиться вікно реєстрації, де необхідно ввести свої дані, а саме:
   a. Ім’я**;**
   b. Прізвище**;**

c. Адресу електронної пошти (можна як особисту, так і пошту на базі домену УжНУ);

d. Назву компанії (рекомендовано написати «teib»).

5. Нижче у відповіді на питання «Чи є уже вас акаунт?», необхідно натиснути «No».



6. Трохи нижче з'являться додаткові поля, які необхідно заповнити даними, а саме:

a. Посада (можна написати «Security Engineer»);

b. Номер телефону (можна написати будь-яку комбінацію 10 цифр)

c. Країна;

d. Кількість працівників у компанії (із списку вибрати «Security Consultant» або «Home Network»).

7. Потрібно натиснути на кнопку «Create Account».

8. На електронну пошту, вказану під час реєстрації, відразу прийде привітальний лист, в якому описуються можливості акаунту. Цей лист не несе в собі інформації, яка необхідна для завершення реєстрації, але вона є корисною для розуміння того, що можна зробити в цьому акаунті.

9. Протягом 30 хвилин на електронну пошту прийде ще один лист від Support команди Qualys, яка допоможе налаштувати акаунт. У цьому листі буде інформація про ваш логін (username) у системі Qualys, а також посилання, OTP key і OTP code.

Qualys. Community Edition

Hello Bogdan,

Welcome to the Qualys Community Edition. Qualys is providing this free service to empower you and your user communities. A confirmation email will be sent to you shortly with instructions on how to login for the first time and create a password.

Qualys Community Edition gives you these great capabilities at no cost:

- Monitor up to 16 assets with Qualys Cloud Agent
- Scan up to 16 internal and 3 external IPs with Vulnerability Management
- Scan 1 URL with Web Application Scanning.
- Deploy a Virtual Scanner Appliance within your internal network.
- Gain visibility within your cloud environments.
- Generate reports and assess results quickly and easily.

The Getting Started Guide will assist with initial setup of the Community Edition.

If you have any questions, just reply to this email or contact us.

Sincerely,
The Qualys Team

10. Далі необхідно натиснути на посилання з отриманого листа. Потім відкриється сторінка, в якій потрібно ввести OTP Code з листа і натиснути на «Submit».

11. Після цього завантажиться сторінка з вашими даними для авторизації в системі Qualys, а саме:

a. Посилання, через яке необхідно авторизуватись;
b. Логін (напівзакритий, повну версію можна знайти в листі від Support про який говорилось у пункті 9);

c. Пароль.

(Рекомендується зберегти отримані дані, щоб не втратити)

Hello Bogdan,

Your USERNAME is [redacted]

Please click the below link and enter the OTP code corresponding to the OTP key to securely access your password and login URL.
You will be prompted to enter a new password upon your first login. For your protection, the username login appears partially obfuscated with ***.
It is recommended that you print the contents of this e-mail and store it for future reference.

https://qualysguard.qg2.apps.qualys.eu/activate/verify_otp.php?key=d78302f7f242e29b62b1e18c657d307a&id=27733&template=1

OTP key : [redacted]

OTP code

The OTP code is valid only for 30 minutes.

If you have any questions, reply to this email or contact us online.

Sincerely,
The Qualys Team

Contact Qualys Support
www.qualys.com/support/

(c) Copyright 1999-2021 Qualys, Inc. All rights reserved.
http://www.qualys.com

12. Після натискання на посилання з пункту 12 (a), на сторінці необхідно ввести логін та пароль і натиснути на кнопку «Log In».

1.2. Використання системи Qualys для сканування

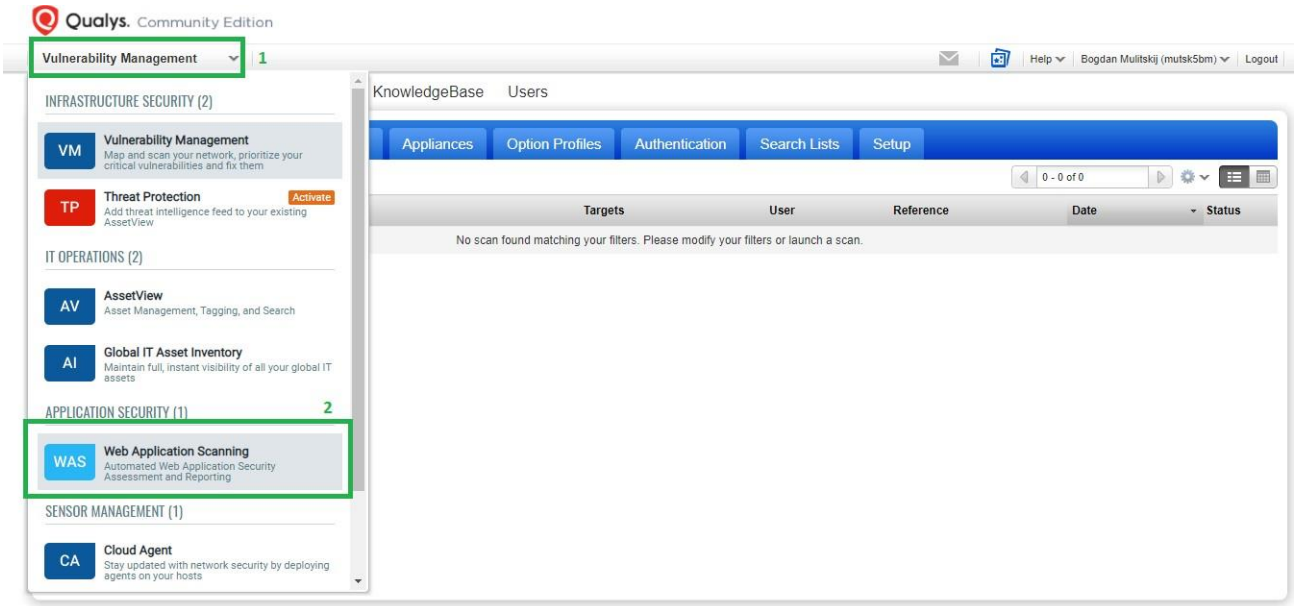
Система Qualys використовується в декілька етапів:

1. Створення запису веб-додатку в системі Qualys.

2. Створення «Option Profile».
3. Проведення «Discovery» та «Vulnerability» сканувань.
4. Створення повного звіту на основі «Vulnerability» сканування.

Для прикладу використано веб-сайт кафедри ТЕІБ teib.info.

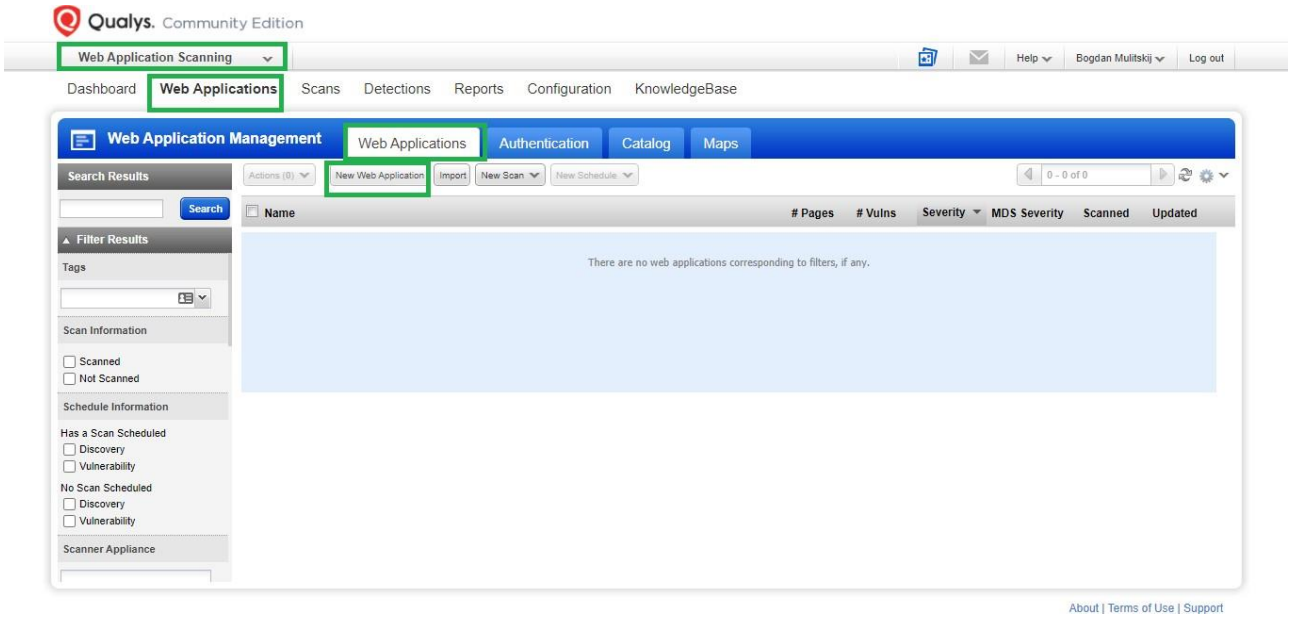
Створення запису веб-додатку в системі Qualys. Щоб провести сканування веб-сайту, спочатку необхідно його додати до системи Qualys, для цього необхідно: Якщо не вибрано відразу – натиснути на стрілочку під назвою системи «Qualys Community Edition» і з випадаючого списку вибрати «Web Application Scanning».

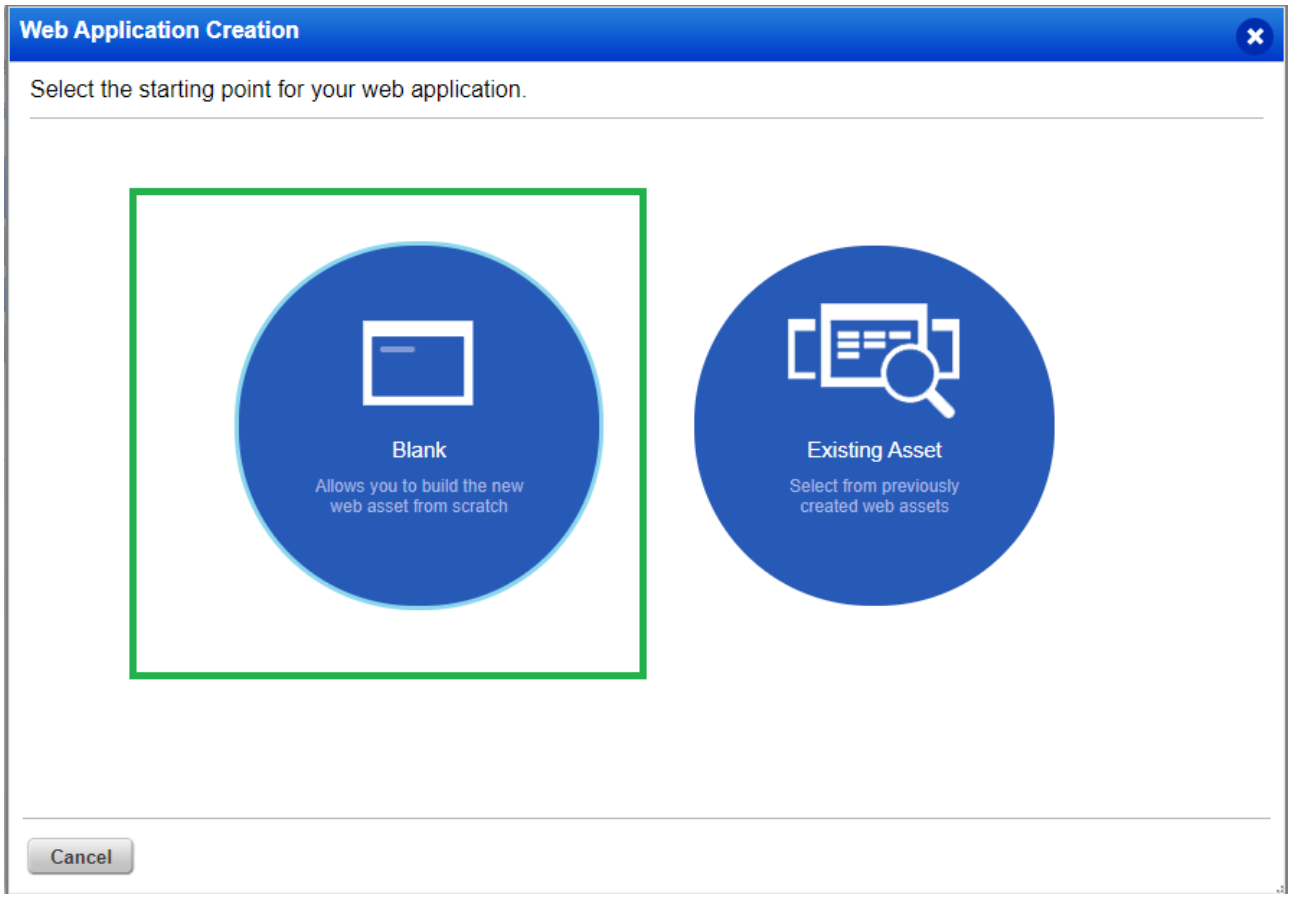


Далі необхідно натиснути на вкладку «Web Applications» під назвою модулю «Web Application Scanning», вибрати «Web Applications» у горизонтальному списку нижче (якщо не вибрано автоматично) і натиснути «New Web Application».

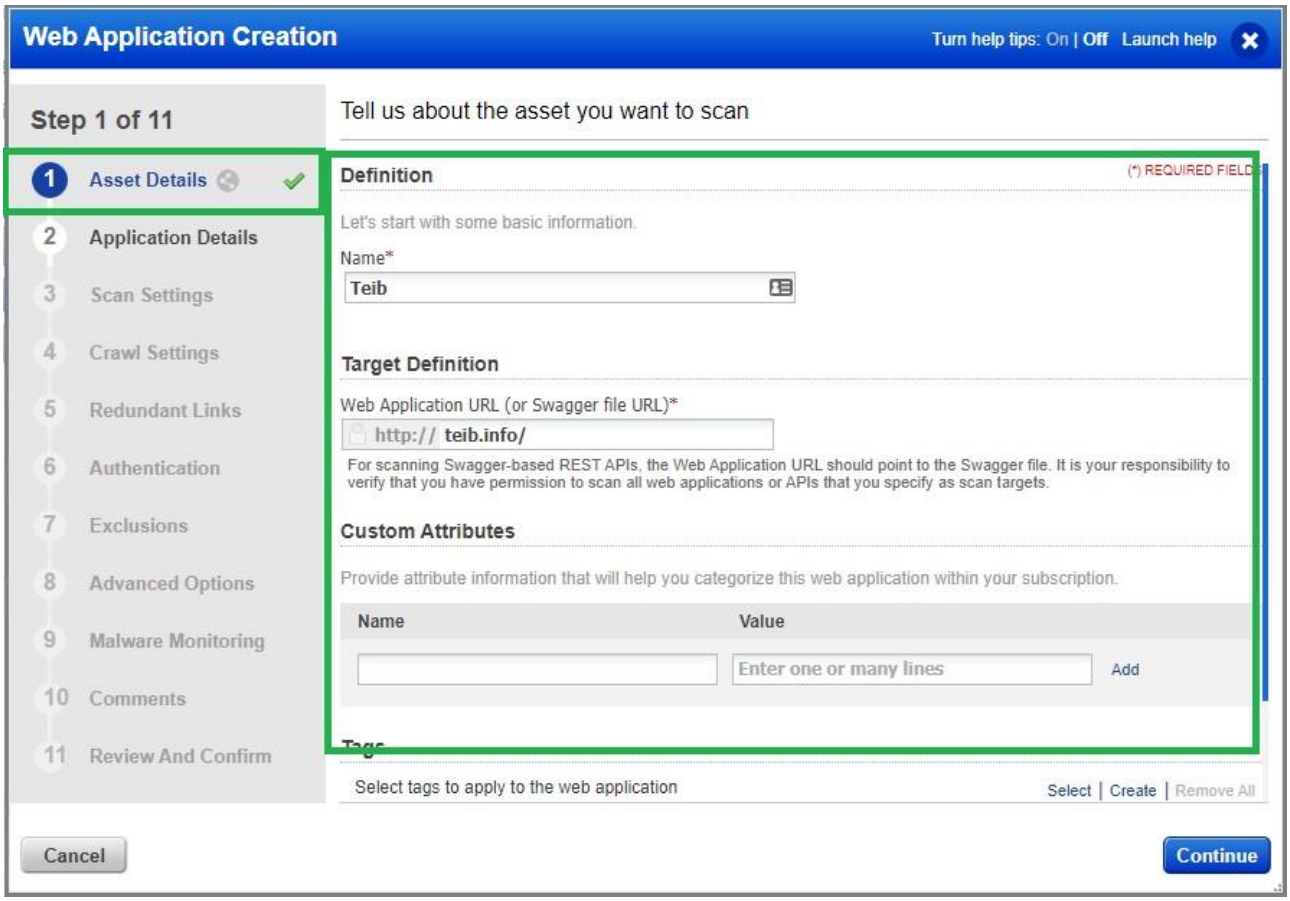
Після цього з’явиться вікно, в якому потрібно вибрати: «додати веб-сайт з нуля», чи уже «з існуючого в системі Qualys вашого веб-сайту». У нашому випадку необхідно вибрати «Blank».

У результаті з’явиться діалогове вікно, яке можна розділити на 11 частин. У цих 11 частинах необхідно вказати якомога повну інформацію про веб-сайт, щоб додати його до системи Qualys.

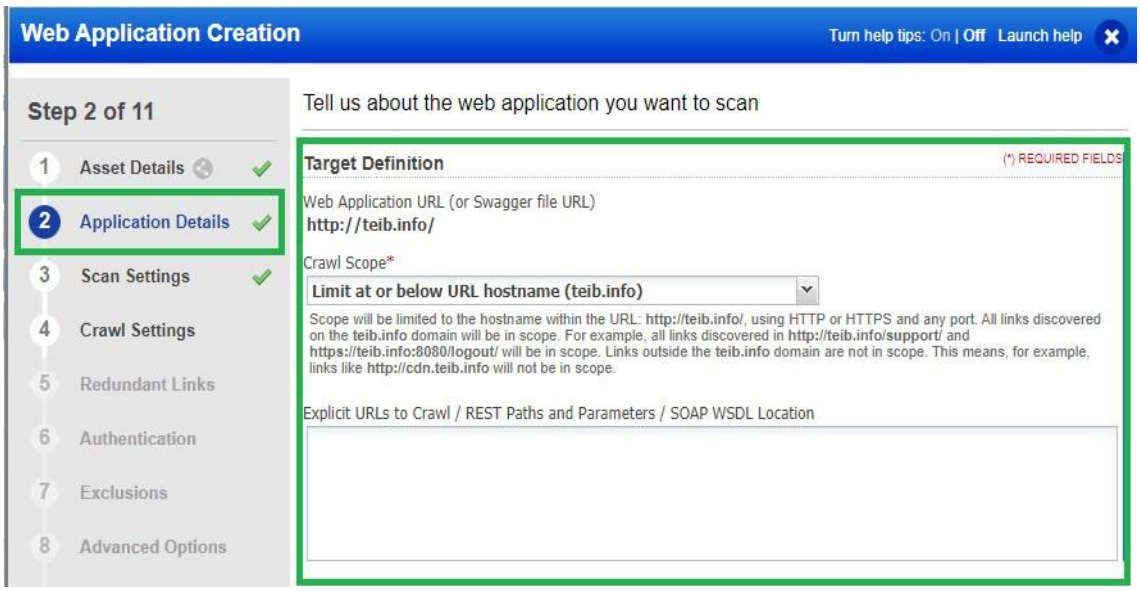


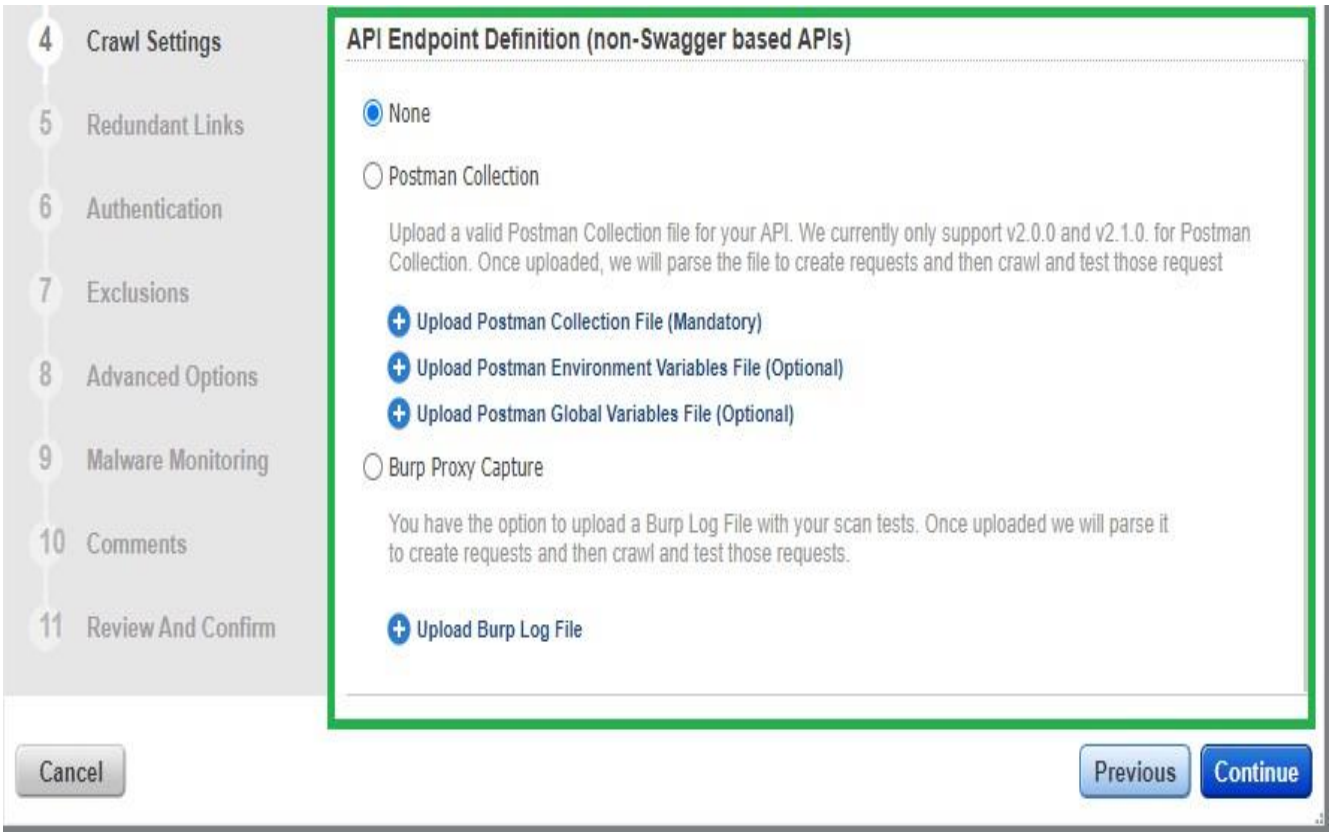


Перша частина це «Asset Details», в якій необхідно вказати назву веб-сайту для Qualys, посилання на веб-сайт (зауважте, що сайт teib.info використовує протокол http, а не https), а також якісь атрибути, за якими ви хочете відрізняти цей веб-сайт серед інших веб-сайтів у вашому акаунті Qualys.



Друга частина це «Application Details», в якій необхідно вибрати, яка деревоподібна структура посилань буде використовуватись під час сканування, можна вказати конкретні посилання, які необхідно просканувати, а також необхідно вибрати тип, за яким буде тестуватись API частина веб-сайту, або вибрати його відсутність.



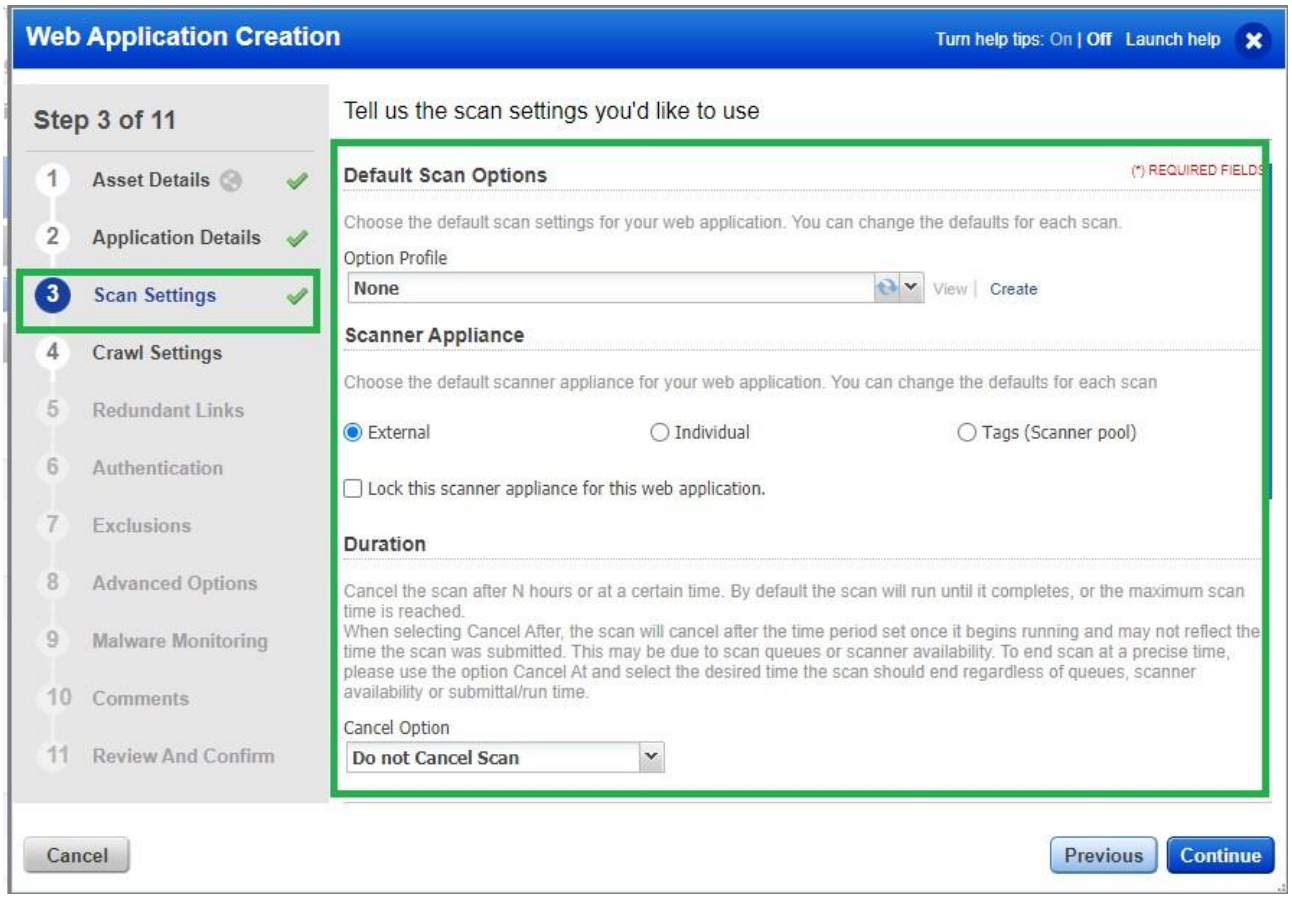


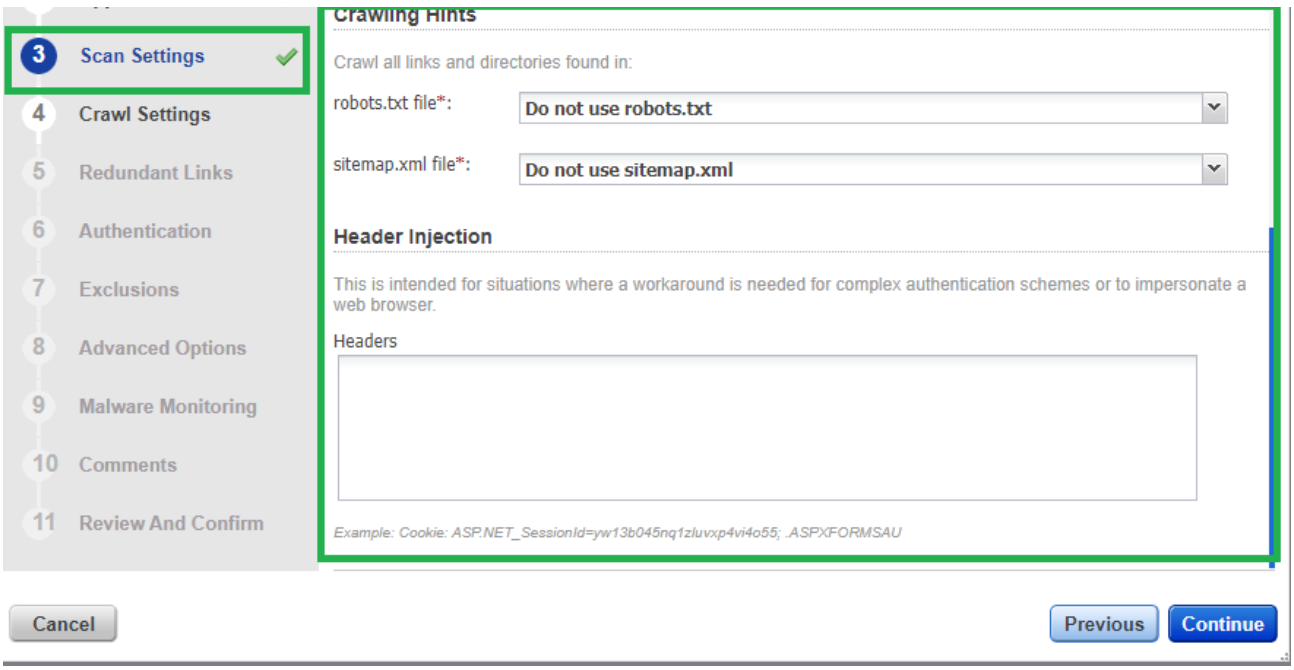
Третя частина це «Scan Settings», параметри цієї частини не обов'язково вибирати саме зараз, тому що це можна буде зробити під час запуску сканування, але під час цієї частини можна:

- Додати Option Profile для веб-сайту (Option Profile буде створено під час наступного розділу),
- Вибрати тип сканеру: зовнішній (стандартний сканер, розташований на серверах Qualys), внутрішній (якщо встановити програмне забезпечення Qualys, але доступно лише для сканування мережі, а не веб-сайту), масив сканерів (для великих мереж).
- Можна закріпити тип сканера для цього веб-сайту, що його ніхто не зможе змінити з інших користувачів у групі ваших акаунтів.
- Можна вибрати, чи потрібно зупиняти сканування після перетину відмітки якогось часу, або чи потрібно зупиняти в конкретний час (рекомендовано залишати «Не зупиняти сканування»).
- Можна вибрати файли типу robots.txt і sitemap.xml файли.

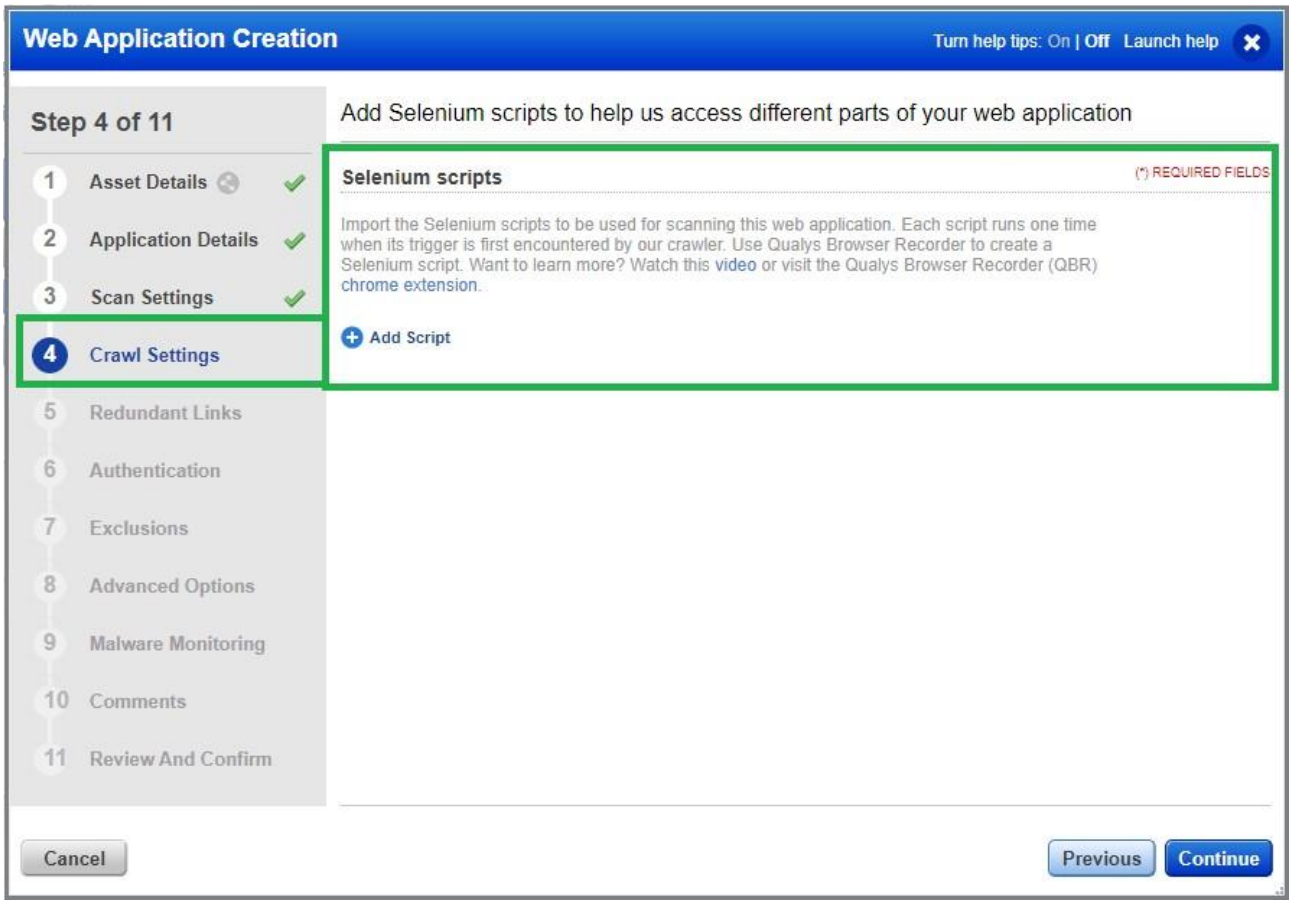
- Можна вказати ін’єкції headers.

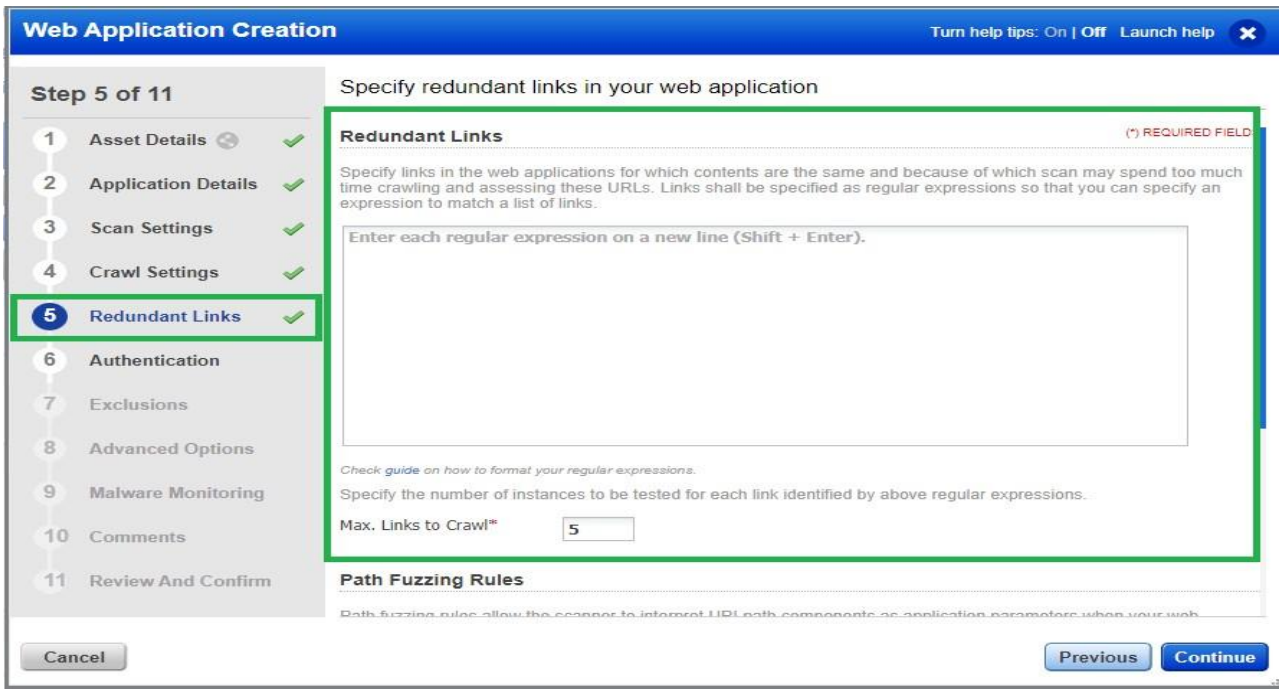
Четверта частина це «Crawl Settings», де можна вказати Selenium-скрипт, який може полегшити сканування для Qualys, якщо веб-сайт має складну структуру.



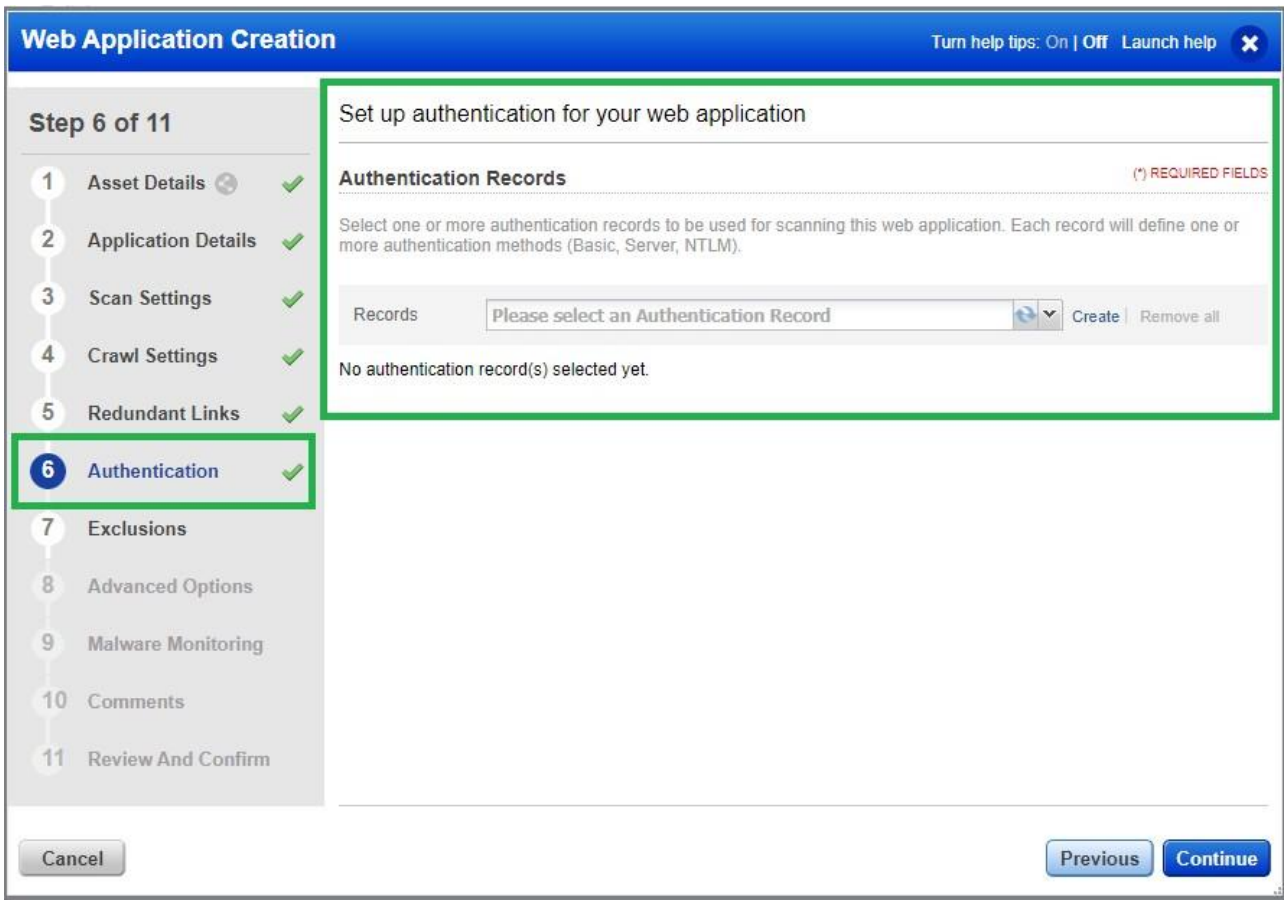


П’ята частина це «Redundant Links», де можна вказати посилання, які необхідно виключити зі сканування, якщо, наприклад, вони мають багато контенту, або складну структуру, яка може значно вплинути на тривалість сканування, а також можна додати правила «Path Fuzzing».

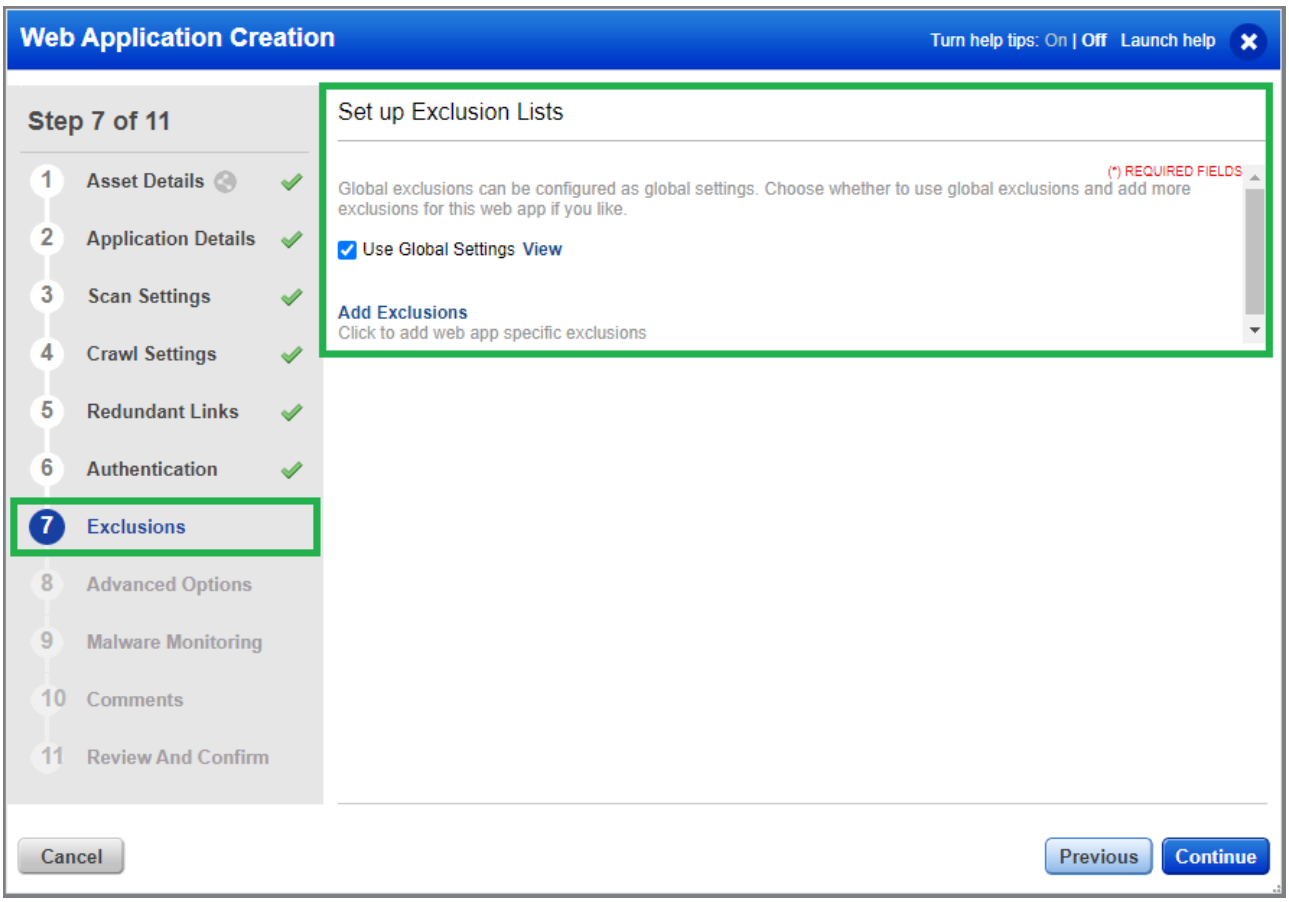




Шоста частина це «Authentication», де можна вказати записи автентифікації (логін і пароль, а також тип автентифікації) для веб-сайту, якщо існують (так як на веб-сайті кафедри немає форми авторизації для користувачів, то це можна випустити).



Сьома частина це «Exclusions», де можна вибрати виключення для налаштувань, які будуть використовуватись під час сканування вашого веб-сайту, або залишити глобальні налаштування, не змінюючи нічого.

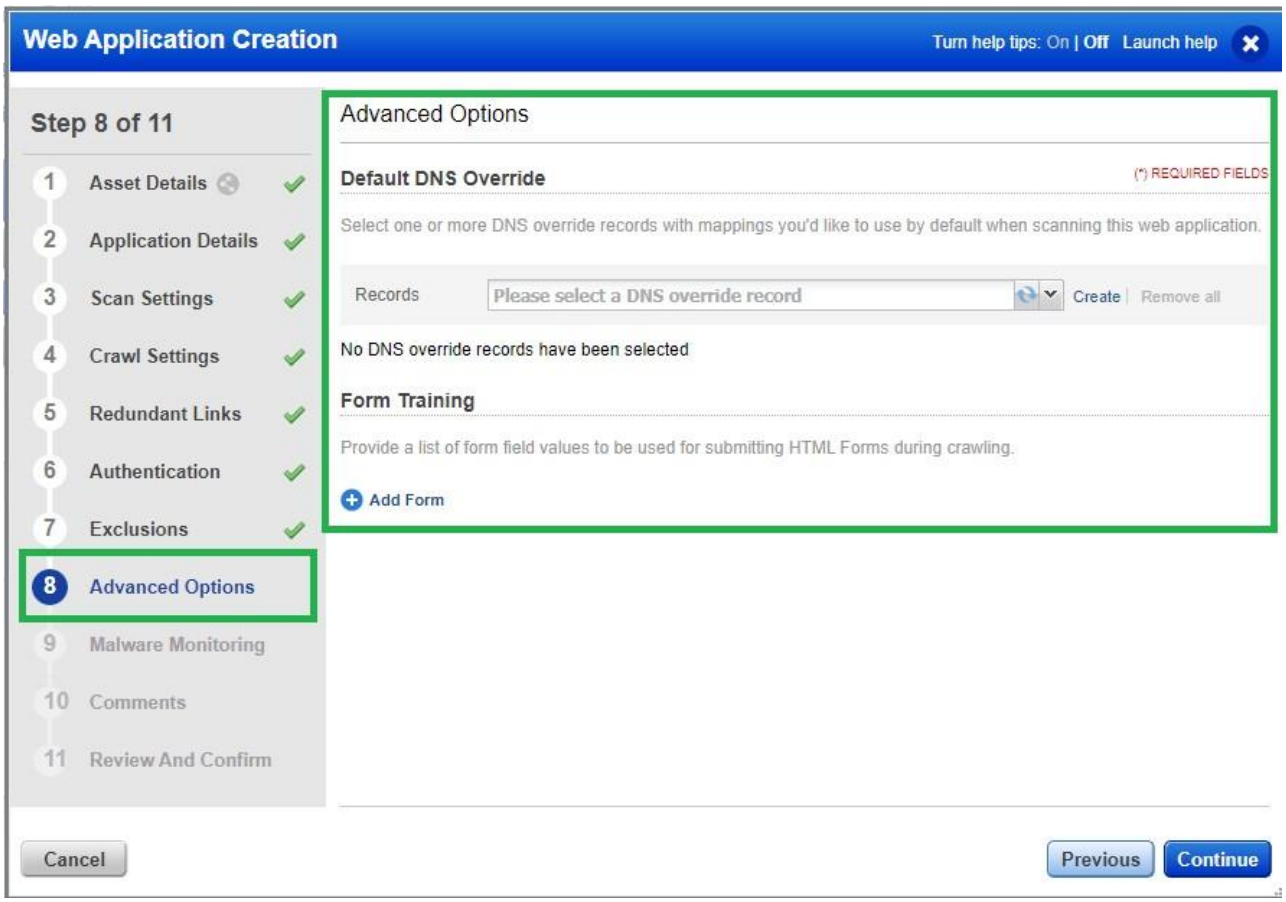


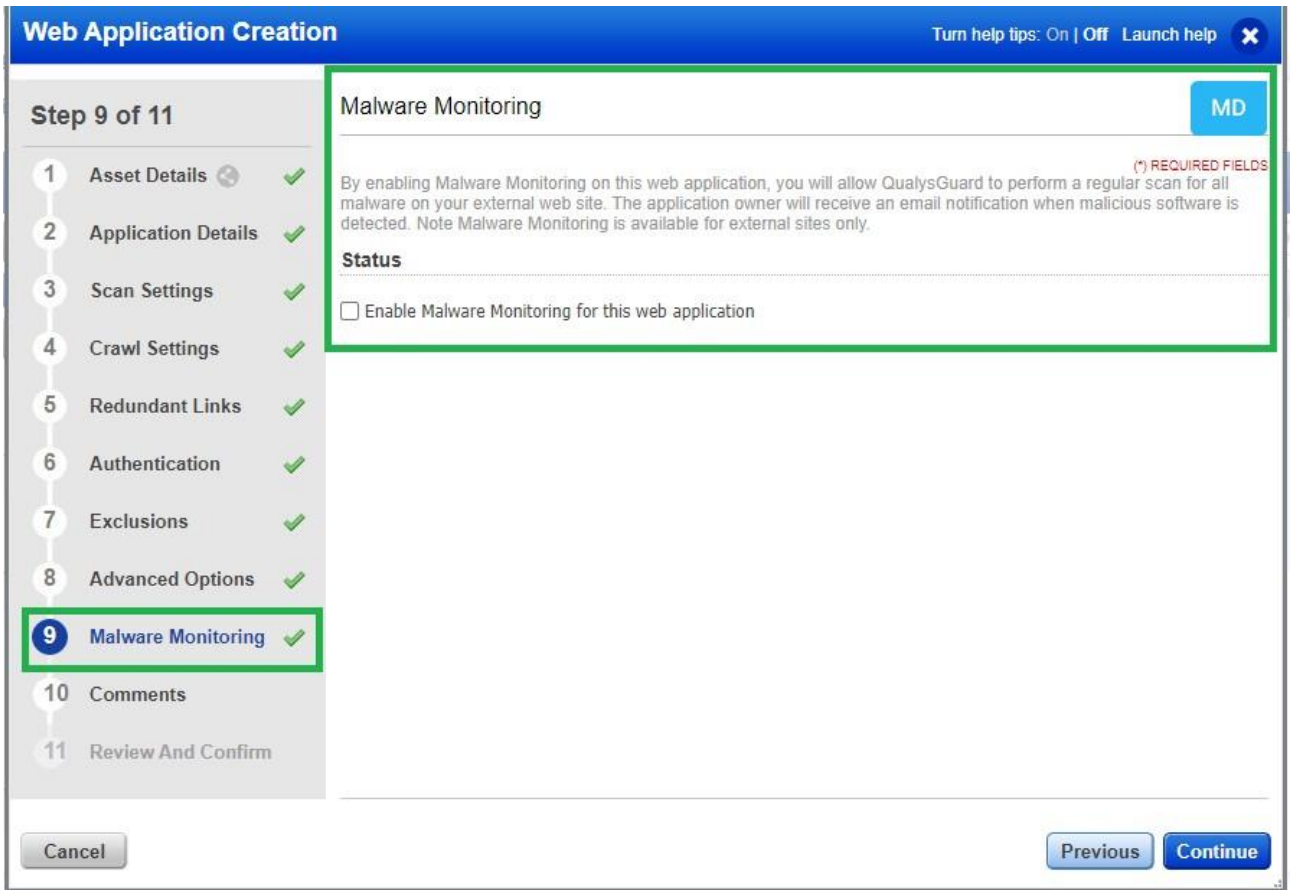
Восьма частина це «Advanced Options», де можна вказати записи типу «DNS Override», а також додати спеціалізовані форми, на які сканер буде звертати увагу під час сканування.

Дев’ята частина це «Malware Monitoring», де можна вказати, чи потрібно системі Qualys проводити регулярні сканування, щоб постійно слідкувати за станом інформаційної безпеки веб-сайту.

У десятій частині можна додати коментарі до запису, які можуть знадобитись вам, або іншим користувачам у групі ваших акаунтів у майбутньому.

В одинадцятій частині «Review and Confirm» потрібно перевірити правильність вибору даних, і підтвердити це, завершивши створення запису веб- сайту, натиснувши на кнопку «Finish».


Web Application Creation
Turn help tips: On | Off Launch help
Step 8 of 11
1 Asset Details
2 Application Details
3 Scan Settings
4 Crawl Settings
5 Redundant Links
6 Authentication
7 Exclusions
8 Advanced Options
9 Malware Monitoring
10 Comments
11 Review And Confirm
Advanced Options
Default DNS Override
(*) REQUIRED FIELDS
Select one or more DNS override records with mappings you'd like to use by default when scanning this web application.
Records
Please select a DNS override record
Create | Remove all
No DNS override records have been selected
Form Training
Provide a list of form field values to be used for submitting HTML Forms during crawling.
Add Form
Cancel
Previous
Continue

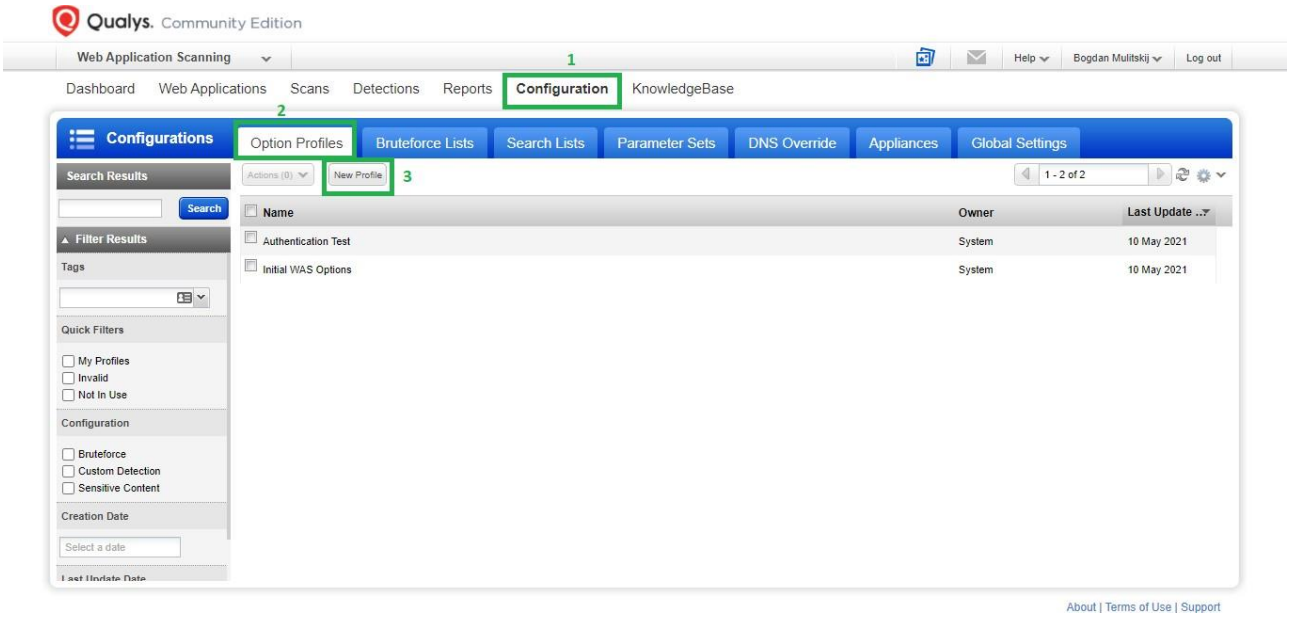

Web Application Creation
Turn help tips: On | Off Launch help
Step 9 of 11
1 Asset Details
2 Application Details
3 Scan Settings
4 Crawl Settings
5 Redundant Links
6 Authentication
7 Exclusions
8 Advanced Options
9 Malware Monitoring
10 Comments
11 Review And Confirm
Malware Monitoring
MD
(*) REQUIRED FIELDS
By enabling Malware Monitoring on this web application, you will allow QualysGuard to perform a regular scan for all malware on your external web site. The application owner will receive an email notification when malicious software is detected. Note Malware Monitoring is available for external sites only.
Status
Enable Malware Monitoring for this web application
Cancel
Previous
Continue

Створення Option Profile. Option Profile – це набір інструкцій, які додаються до запису веб-сайту в системі Qualys з метою використання в подальшому скануванні. Option Profile це шаблон, в якому є інформація, що, як і з якою інтенсивністю потрібно сканувати.

Для створення Option Profile необхідно:

1. Якщо не вибрано відразу – натиснути на стрілочку під назвою системи «Qualys Community Edition» і з випадаючого списку вибрати «Web Application Scanning».

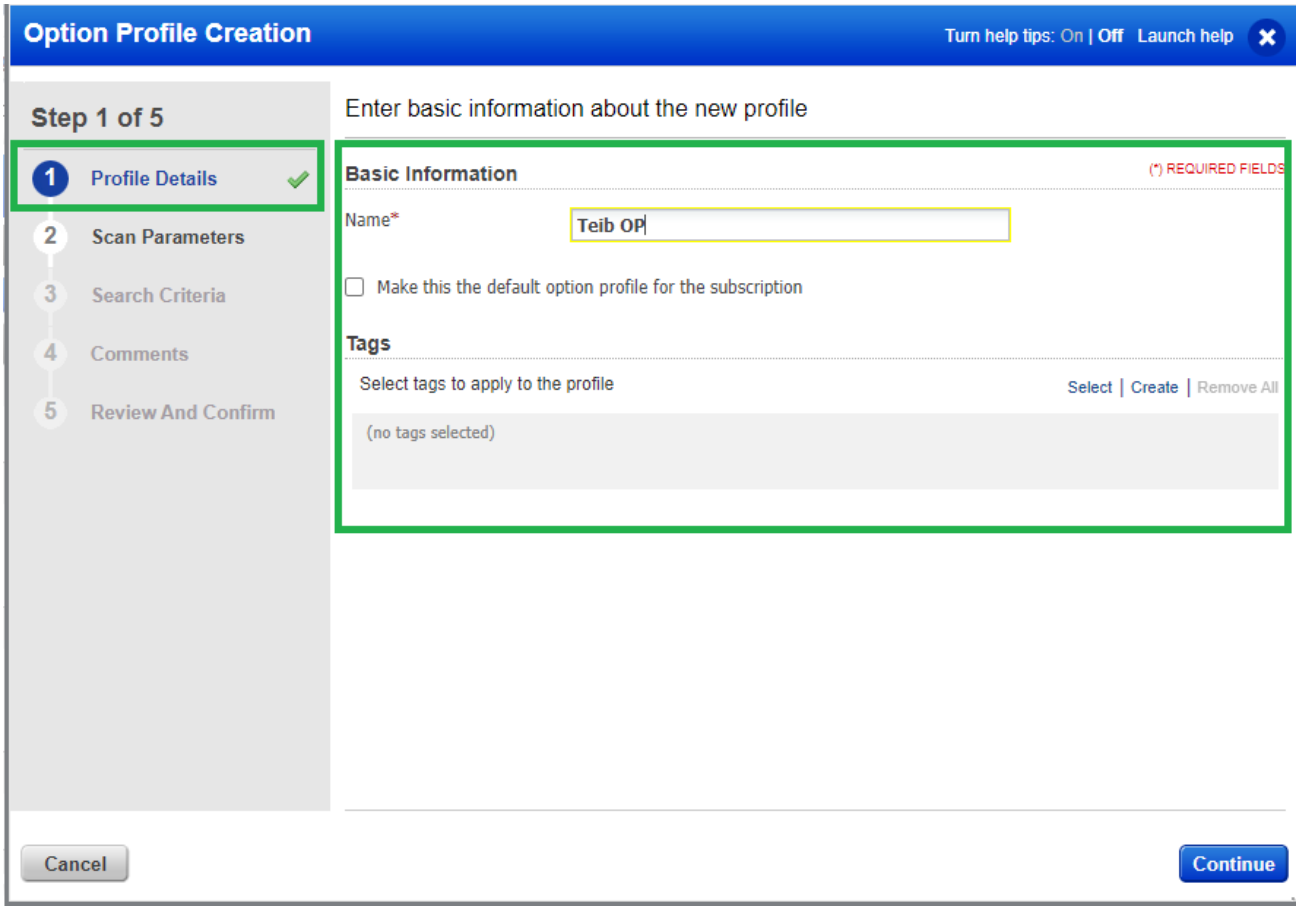
2. Далі необхідно натиснути на вкладку «Configuration» під назвою модулю «Web Application Scanning», вибрати «Option Profiles» у горизонтальному списку нижче (якщо не вибрано автоматично) і натиснути «New Profile».



3. Після цього відкриється діалогове вікно створення Option Profile, яке складається з 5 частин:

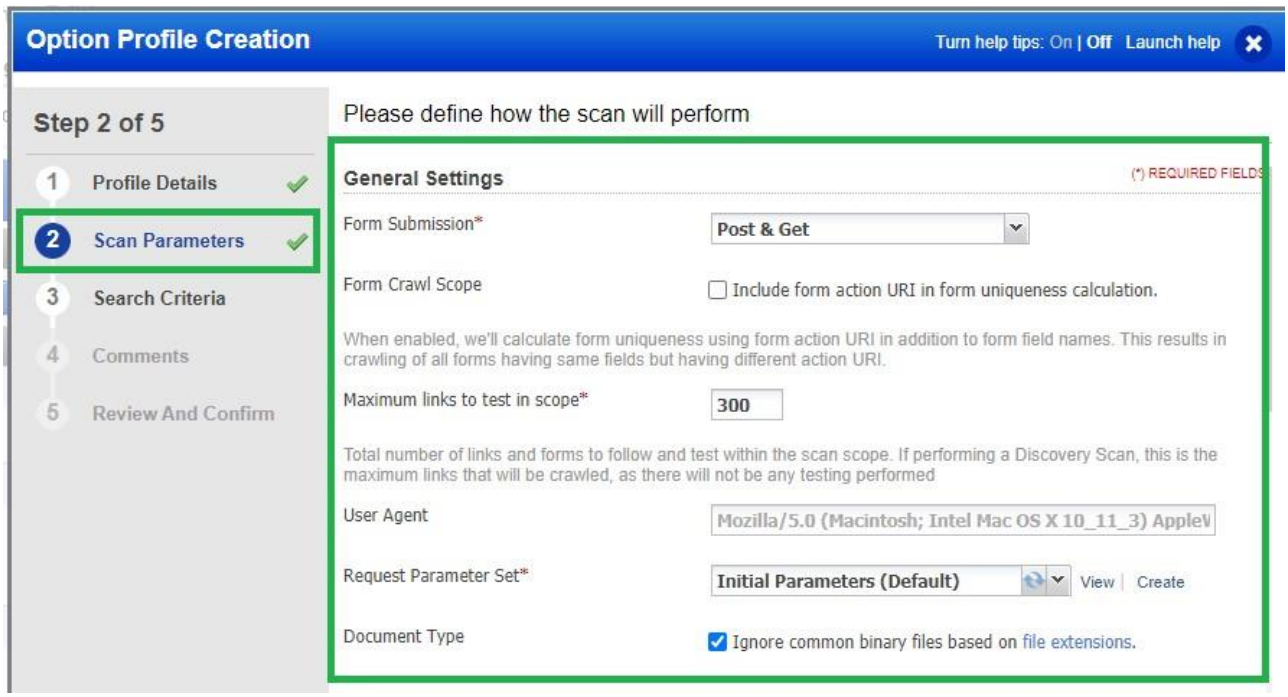
a. Profile Details;
b. Scan Parameters;
c. Search Criteria;
d. Comments;
e. Review and Confirm.

У «Profile Details» нам необхідно вказати назву цього Option Profile, а також можна зробити його профілем за замовчуванням для всіх ваших веб- сайтів доданих до системи Qualys, і можна прив'язати цей профіль до певних тегів, щоб було легше групувати і сортувати профілі, якщо їх багато.



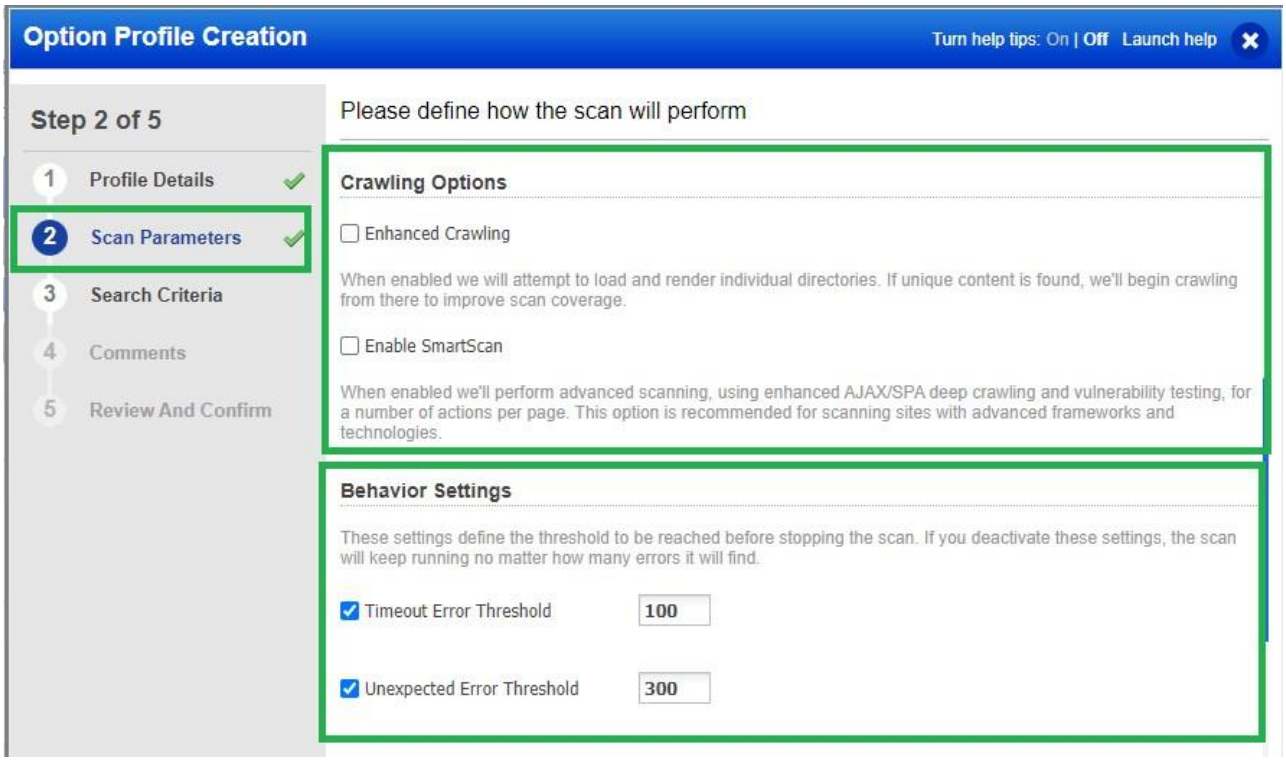
«Scan Parameters» це основна частина цього діалогового вікна, де вибираються параметри, які будуть використовуватись під час сканування. Вона розділена на декілька секцій:

1. «General Settings», де треба вибрати який тип запитів буде надсилатись до веб-сайту під час сканування (Get, Post, Get&Post, None), можна вибрати, чи потрібно вмикати калькуляцію унікальності форм (для зменшення часу сканування), вибрати максимальну кількість посилань, які будуть просканованi, можна також вибрати агента (умови, які будуть відтворені сканером), можна вибрати шаблон з параметрів, а також, чи потрібно ігнорувати загальні бінарні файли.



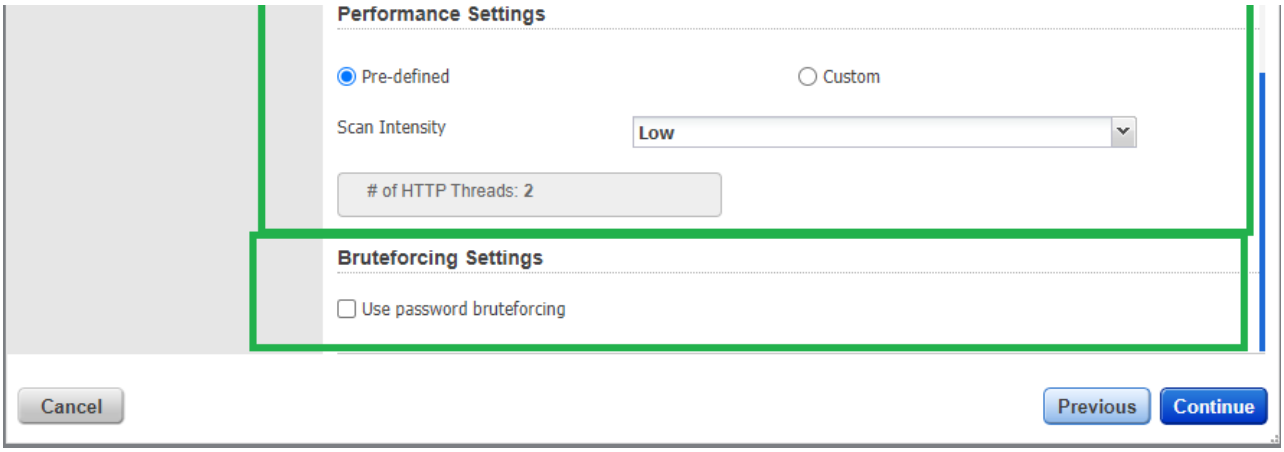
2. «Crawling Options», де можна вибрати, чи проводити глибоке і «розумне» сканування.

3. «Behavior Settings», де можна вибрати кількість помилок, після яких сканування буде зупинено. Серед вибору доступні тайм- аут помилки і неочікувані помилки.



4. «Performance Settings», де потрібно вибрати тип налаштувань (спрощений або детальний), а також необхідно вибрати інтенсивність сканування.

5. «Bruteforce Settings», де потрібно вибрати, чи проводити атаку типу bruteforce на веб-сайт, чи ні.



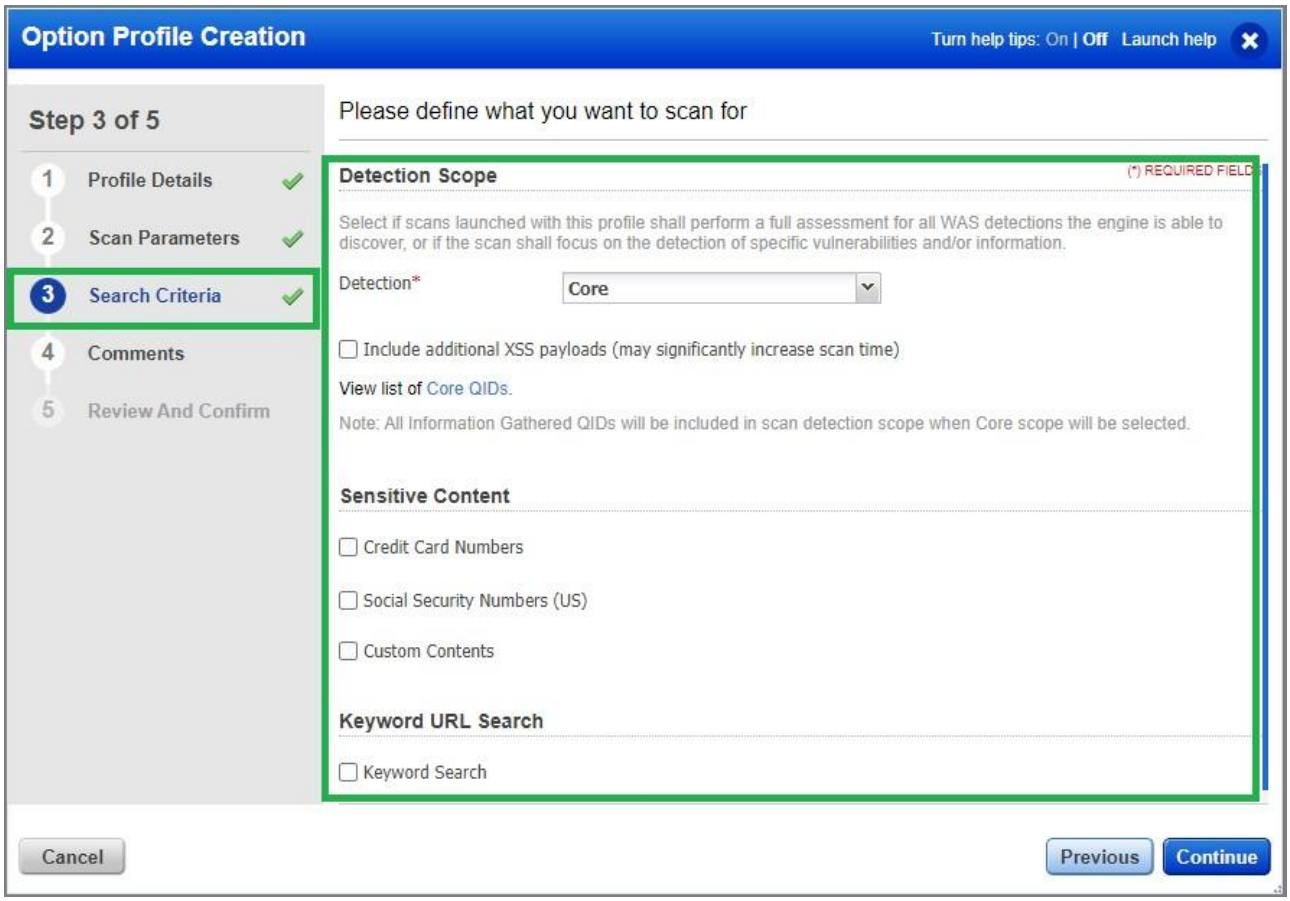
«Search Criteria» це третя частина з п’яти, і остання, де потрібно вибирати, на який тип інформації сканер буде додатково звертати увагу і класифікувати по-іншому. Ця частина розділена на декілька секцій:

1. «Detection Scope», де потрібно вибрати тип пошуку з списку, а також вибрати, чи потрібно включати додаткові XSS payloads.

2. «Sensitive Content», де можна вибрати, на яку особливу інформацію сканеру потрібно звертати увагу (номера кредитних карток, соціальних страхувань, а також custom варіанти).

3. «Keywords URL Search», де можна вибрати, чи робити пошук по ключовим словам в URL-адресах.

«Comments» це частина, в якій можна додати коментарі для себе або інших користувачів з вашої системи акаунтів у Qualys. А «Review and Confirm» це частина, в якій можна перевірити, чи все вибрано правильно.



Проведення Discovery та Vulnerability сканувань. Для того, щоб отримати повну картину ситуації з безпекою веб-сайту, необхідно провести Discovery та Vulnerability сканування на основі створеного Option Profile у попередньому розділі.

Discovery сканування – це тип сканування, при якому основне завдання не знайти вразливості, які існують у веб-сайті, а знайти інформацію про веб-сайт, яка може бути корисною для проведення уже основного сканування на вразливості.

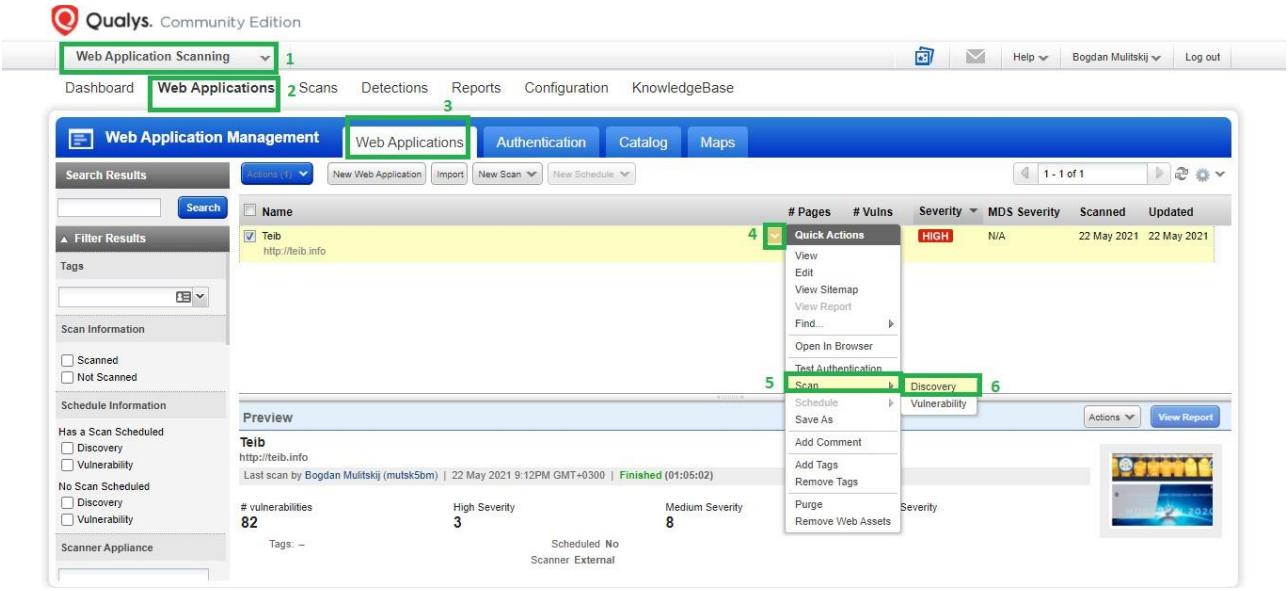
Vulnerability сканування – це повне сканування веб-сайту на вразливості.

Для проведення Discovery сканування необхідно:

1. Якщо не вибрано відразу – натиснути на стрілочку під назвою системи «Qualys Community Edition» і з випадаючого списку вибрати «Web Application Scanning».

2. Далі необхідно натиснути на вкладку «Web Applications» під назвою модулю «Web Application Scanning», вибрати «Web Applications» у горизонтальному списку нижче (якщо не вибрано автоматично).

3. Біля створеного в першому розділі запису веб-сайту необхідно натиснути на стрілочку, і у випадаючому вікні вибрати «Scan» і в боковому вікні «Discovery».



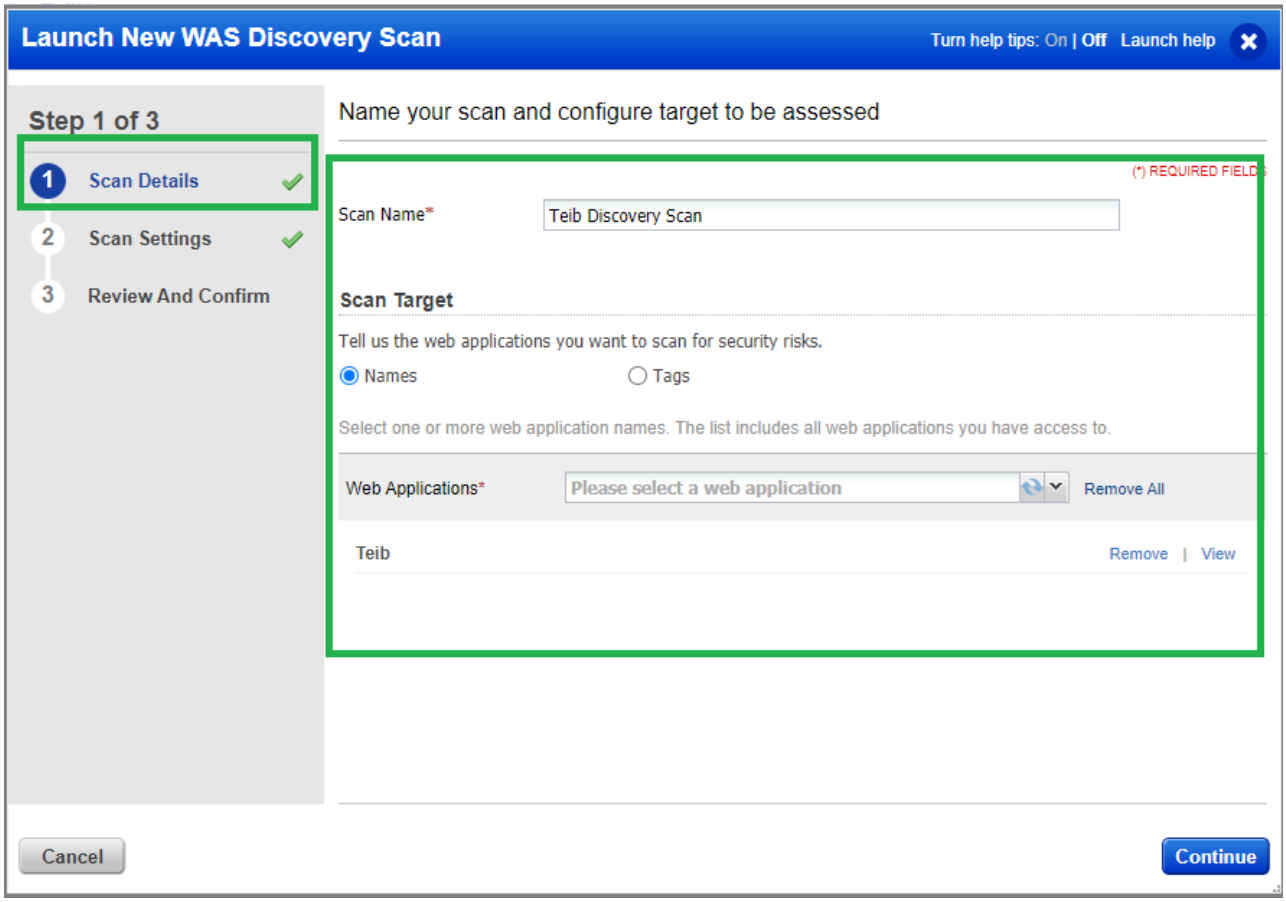
Діалогове вікно, яке з’явилось після натискання на Discovery можна розділити на три частини:

«Scan Details» – це частина в якій необхідно вказати деталі майбутнього сканування, а саме: вказати назву майбутнього сканування, вибрати за яким принципом ви будете вибирати веб-сайти для цього сканування (за ім’ям, або за тегами), а також вибрати самий веб-сайт зі списку (якщо ви почнете створення сканування за інструкціями, описаними на попередній сторінці, то веб-сайт для сканування у вас буде обраний автоматично).

«Scan Settings» – це частина, в якій необхідно вибрати налаштування для майбутнього сканування. Серед яких:

- Вибрати Option Profile, створений під час попереднього розділу.
- Вибрати запис автентифікації, якщо існує (на веб-сайті teib.info немає форми авторизації для користувачів).
- Вибрати тип сканеру, який буде використовуватись: зовнішній (стандартний сканер, розташований на серверах Qualys), внутрішній (якщо встановити програмне забезпечення Qualys, але доступно лише для сканування мережі, а не веб-сайту), масив сканерів (для великих мереж).

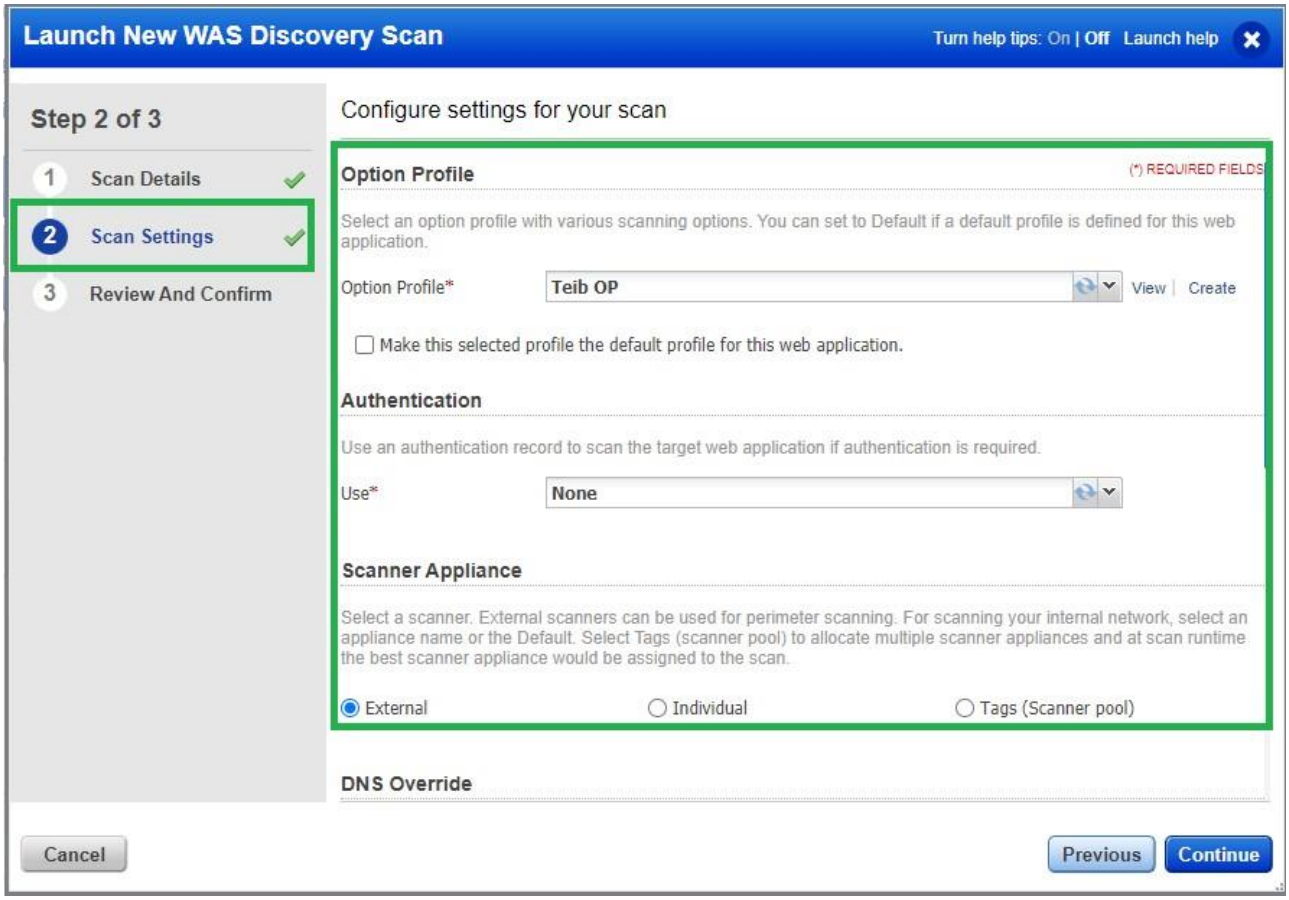
- Вибрати, чи потрібно використовувати DNS Override.
- Вибрати, чи потрібно зупиняти сканування після перетину відмітки якогось часу, або чи потрібно зупиняти в конкретний час (рекомендовано залишати «Не зупиняти сканування»).
- Вибрати, чи потрібно надсилати сповіщення про закінчення сканування на пошту.

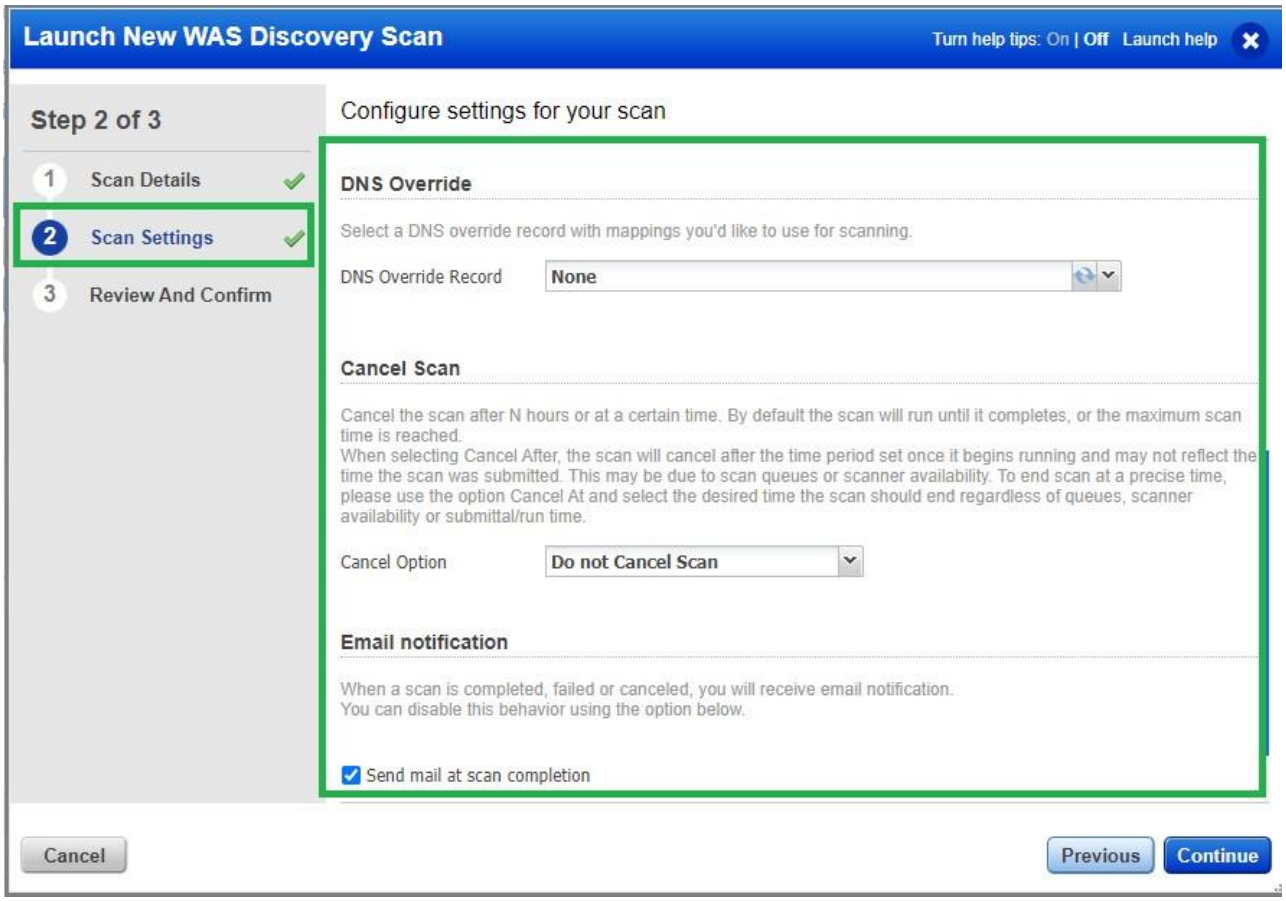


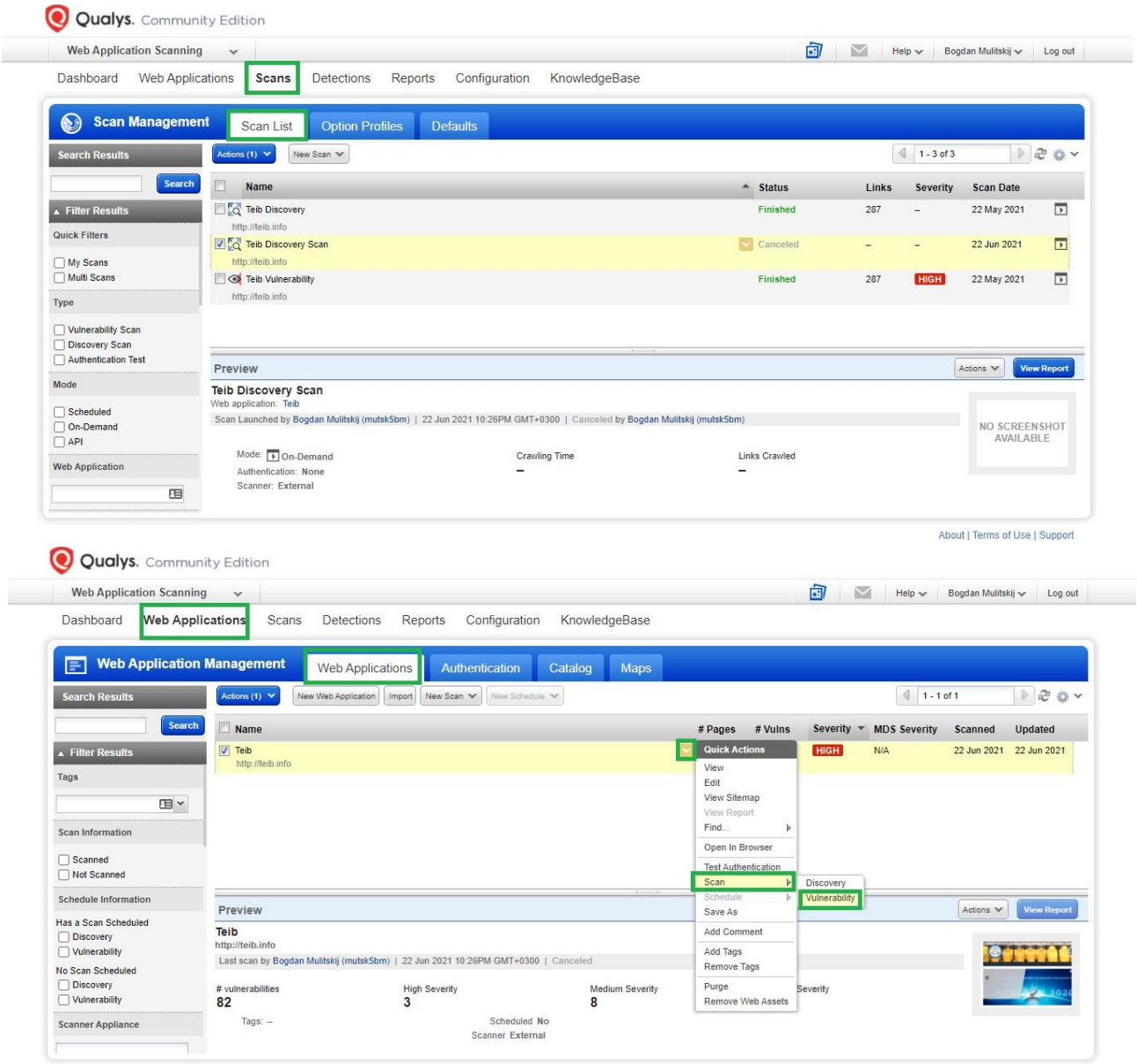
Остання частина це Review and Confirm, де можна переглянути вибрані параметри, щоб впевнитись, що все вибрано правильно.

Після натискання на кнопку Finish, сканування відправиться в чергу, за станом якого можна слідкувати перейшовши на вкладку Scans, і вікно Scan List.

Після закінчення Discovery сканування необхідно запустити Vulnerability сканування, це можна зробити, виконавши ті ж самі інструкції, що і для Discovery, але при відкритті діалогового вікна вибрати не Discovery, а Vulnerability.


Launch New WAS Discovery Scan
Turn help tips: On | Off Launch help
Step 2 of 3
1 Scan Details
2 Scan Settings
3 Review And Confirm
Configure settings for your scan
Option Profile
(*) REQUIRED FIELDS
Select an option profile with various scanning options. You can set to Default if a default profile is defined for this web application.
Option Profile*
Teib OP
View | Create
Make this selected profile the default profile for this web application.
Authentication
Use an authentication record to scan the target web application if authentication is required.
Use*
None
Scanner Appliance
Select a scanner. External scanners can be used for perimeter scanning. For scanning your internal network, select an appliance name or the Default. Select Tags (scanner pool) to allocate multiple scanner appliances and at scan runtime the best scanner appliance would be assigned to the scan.
External
Individual
Tags (Scanner pool)
DNS Override
Cancel
Previous
Continue


Launch New WAS Discovery Scan
Turn help tips: On | Off Launch help
Step 2 of 3
1 Scan Details
2 Scan Settings
3 Review And Confirm
Configure settings for your scan
DNS Override
Select a DNS override record with mappings you'd like to use for scanning.
DNS Override Record
None
Cancel Scan
Cancel the scan after N hours or at a certain time. By default the scan will run until it completes, or the maximum scan time is reached.
When selecting Cancel After, the scan will cancel after the time period set once it begins running and may not reflect the time the scan was submitted. This may be due to scan queues or scanner availability. To end scan at a precise time, please use the option Cancel At and select the desired time the scan should end regardless of queues, scanner availability or submittal/run time.
Cancel Option
Do not Cancel Scan
Email notification
When a scan is completed, failed or canceled, you will receive email notification.
You can disable this behavior using the option below.
Send mail at scan completion
Cancel
Previous
Continue



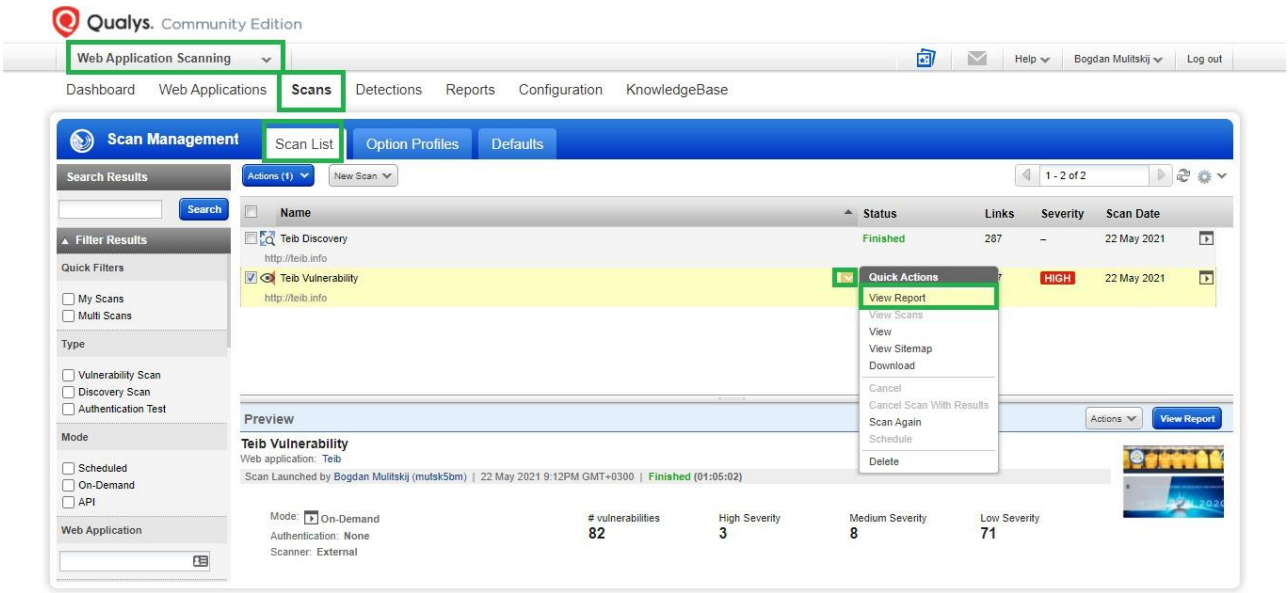
Створення повного звіту на основі Vulnerability сканування. Після завершення Vulnerability сканування необхідно створити повний звіт, який буде містити перелік всіх вразливостей, які були знайдені на веб-сайті кафедри ТЕІБ.

Для того, щоб створити повний звіт на основі результатів сканування необхідно:

1. Якщо не вибрано відразу – натиснути на стрілочку під назвою системи «Qualys Community Edition» і з випадаючого списку вибрати «Web Application Scanning».

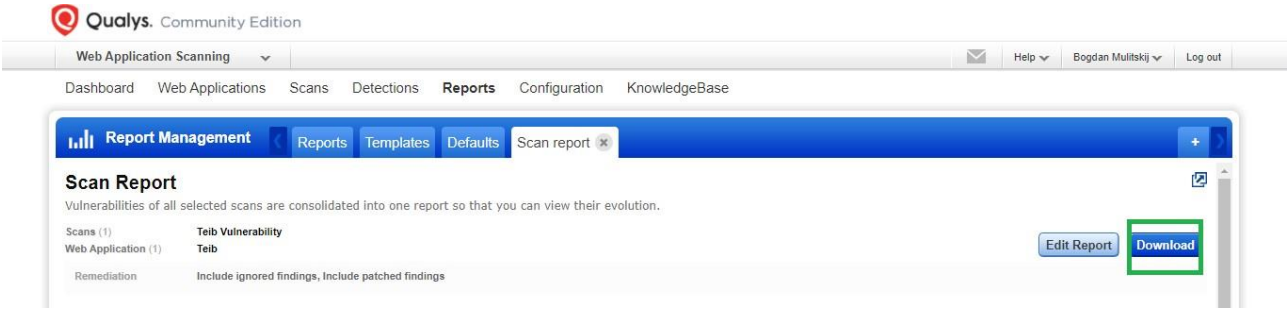
2. Далі необхідно натиснути на вкладку «Scans» під назвою модулю «Web Application Scanning», вибрати «Scan List» у горизонтальному списку нижче (якщо не вибрано автоматично).

3. Біля запису Vulnerability сканування необхідно натиснути на стрілочку, і у випадаючому вікні вибрати «View Report».



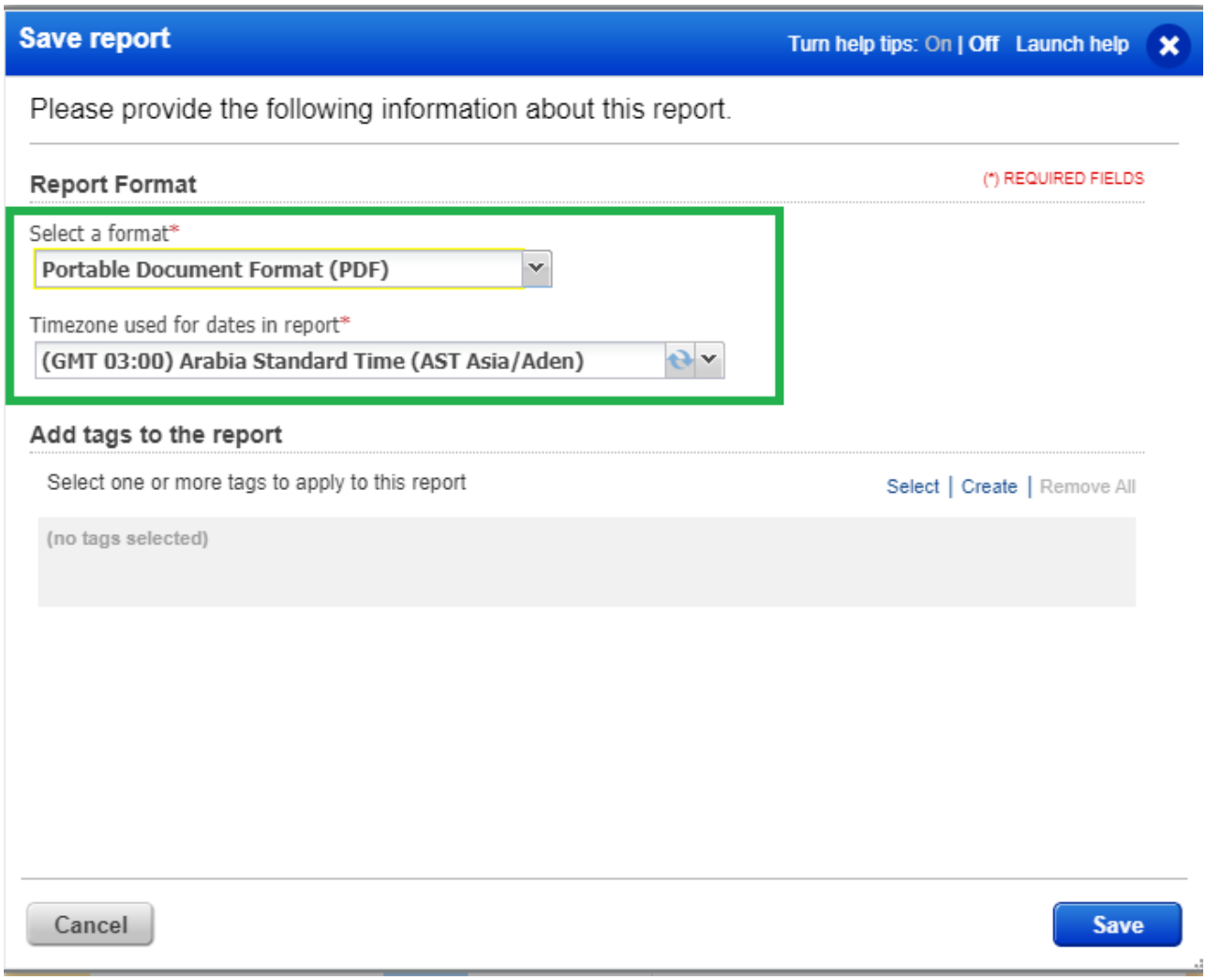
Після цього з’явиться вікно із загальною звітною інформацію про сканування, в якому буде висвітлено кількість вразливостей, діаграми, в залежності від різних типів вразливостей, а також можна переглянути інформацію про кожну вразливість окремо.

Для того, щоб знайти повну інформацію про кожну вразливість необхідно завантажити файл звіту, що можна зробити натиснувши на кнопку «Download» у верхній частині вікна.



Після цього відкриється діалогове вікно, в якому потрібно вибрати бажаний формат звіту (рекомендовано pdf), а також часовий пояс. І також можна додати теги

до звіту, щоб можна було його легше знайти, сортувати та фільтрувати, якщо цих звітів у вашому обліковому записі Qualys багато.



Після завантаження файлу його можна відкрити і ознайомитись з докладними результатами.

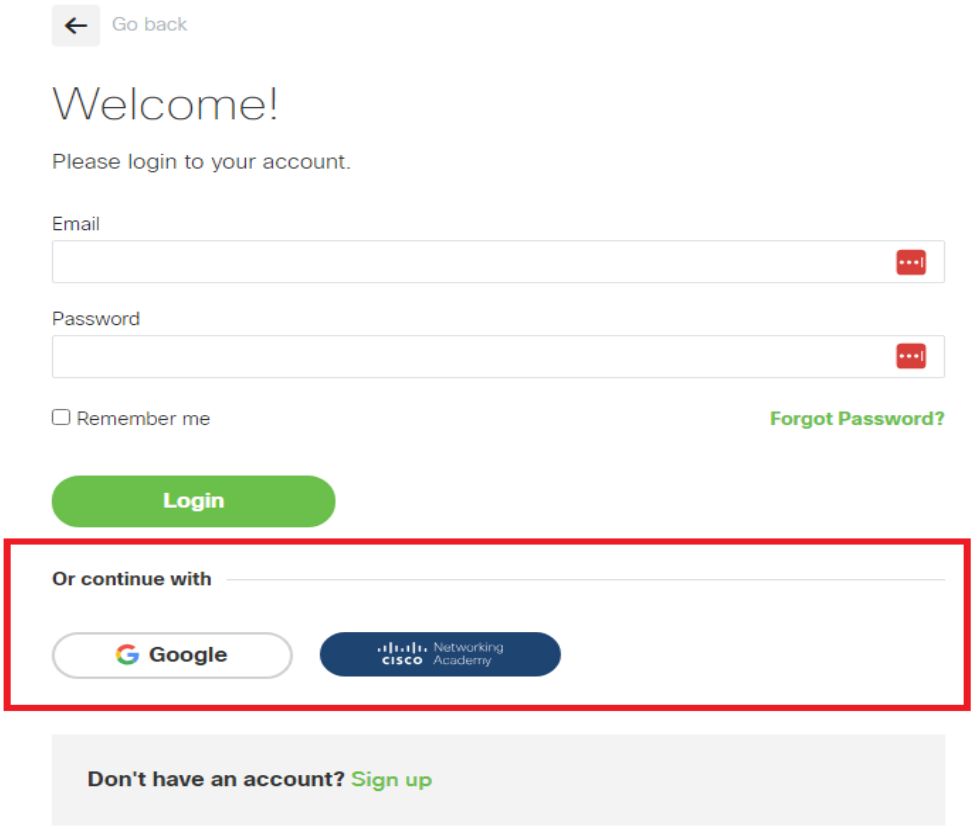
РОЗДІЛ 2. СТВОРЕННЯ ЛОКАЛЬНОЇ МЕРЕЖІ НА КАФЕДРІ ТВЕРДОТІЛЬНОЇ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

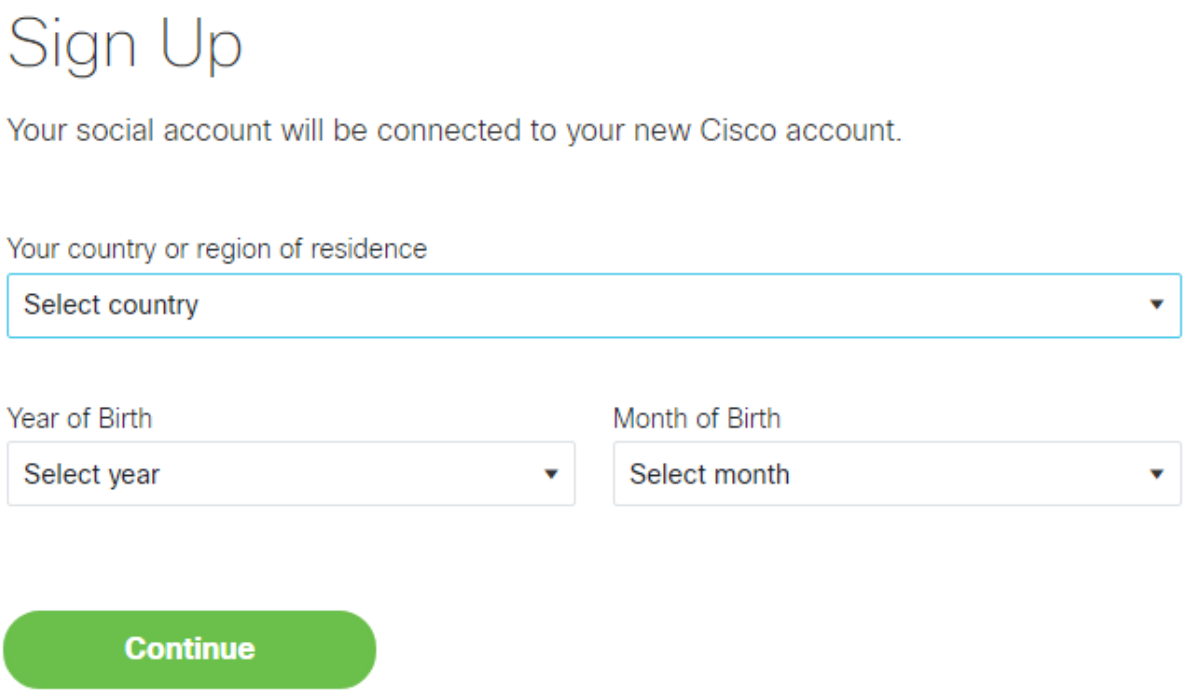
Цей сценарій полягає у створенні моделі мережі в програмному забезпеченні Cisco Packet Tracer, розробці фізичної мережі за створеною схемою та аналізі результатів сканування мережі програмним забезпеченням nmap.

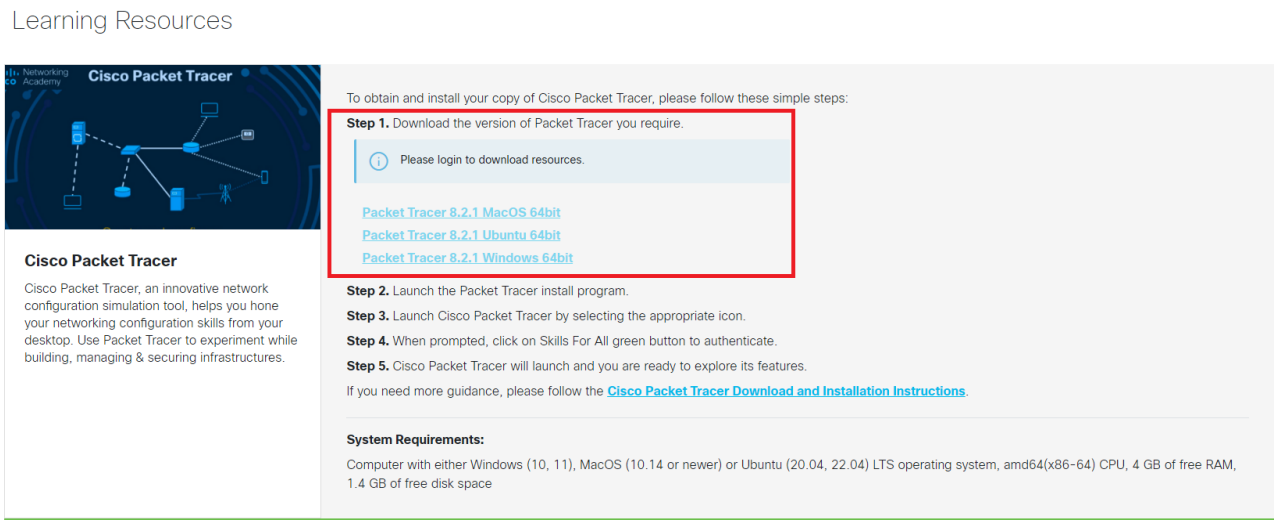
2.1. Розробка макету мережі в Cisco Packet Tracer

Перед початком моделювання мережі завантажте програмне забезпечення Cisco Packet Tracer:

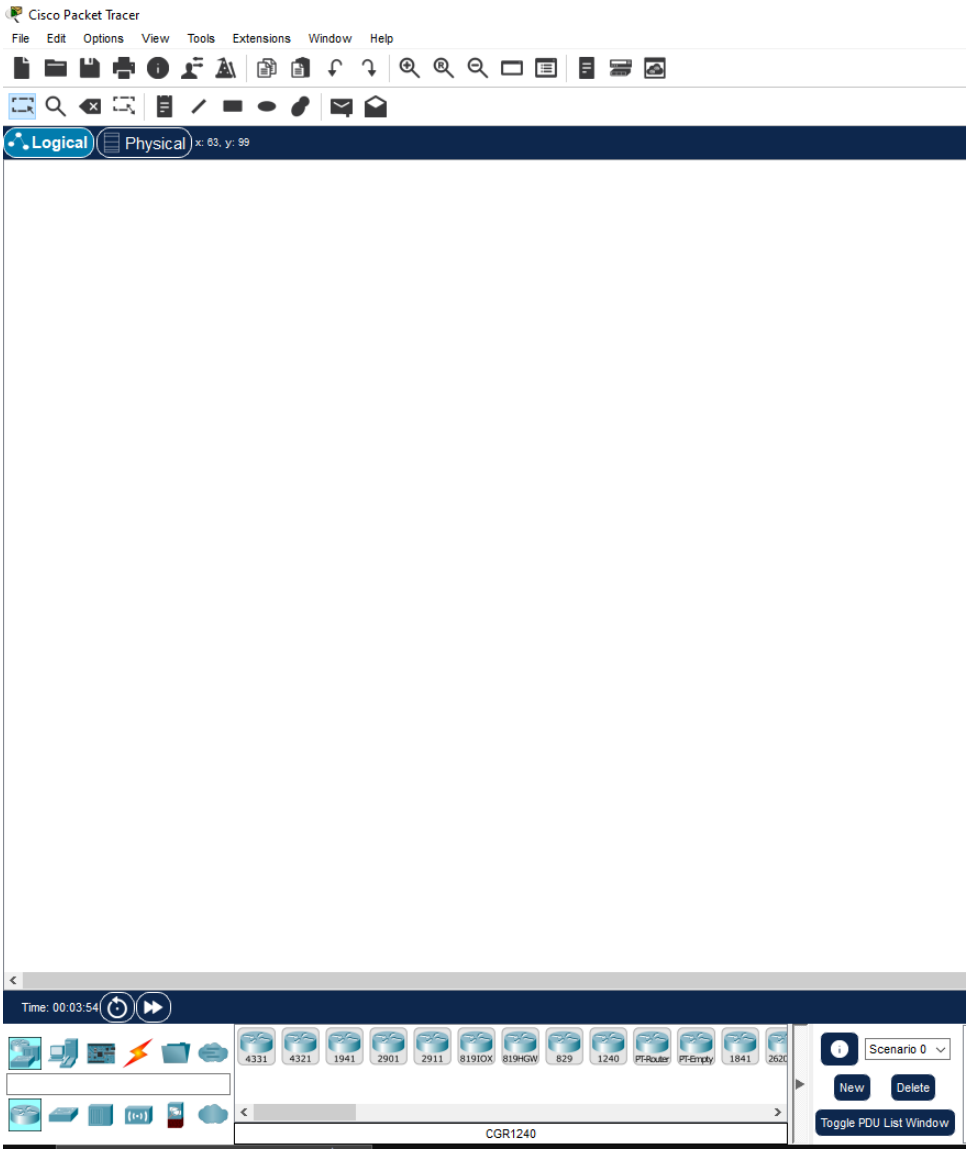
1. Авторизуйтесь на веб-сайті Skills for All за допомогою студентського облікового запису Google або облікового запису Cisco Network Academy (якщо є).
2. Пройдіть всі необхідні кроки створення облікового запису на Skills for All.
3. Встановіть Cisco Packet Tracer з офіційного веб-сайту.


Go back
Welcome!
Please login to your account.
Email
Password
Remember me
Forgot Password?
Login
Or continue with
Google
Networking Academy
Don't have an account? Sign up


Sign Up
Your social account will be connected to your new Cisco account.
Your country or region of residence
Select country
Year of Birth
Select year
Month of Birth
Select month
Continue



4. Змоделюйте мережу комп’ютерного класу в Cisco Packet Tracer, використовуючи наявні пристрої та мережеві зв’язки в програмі.



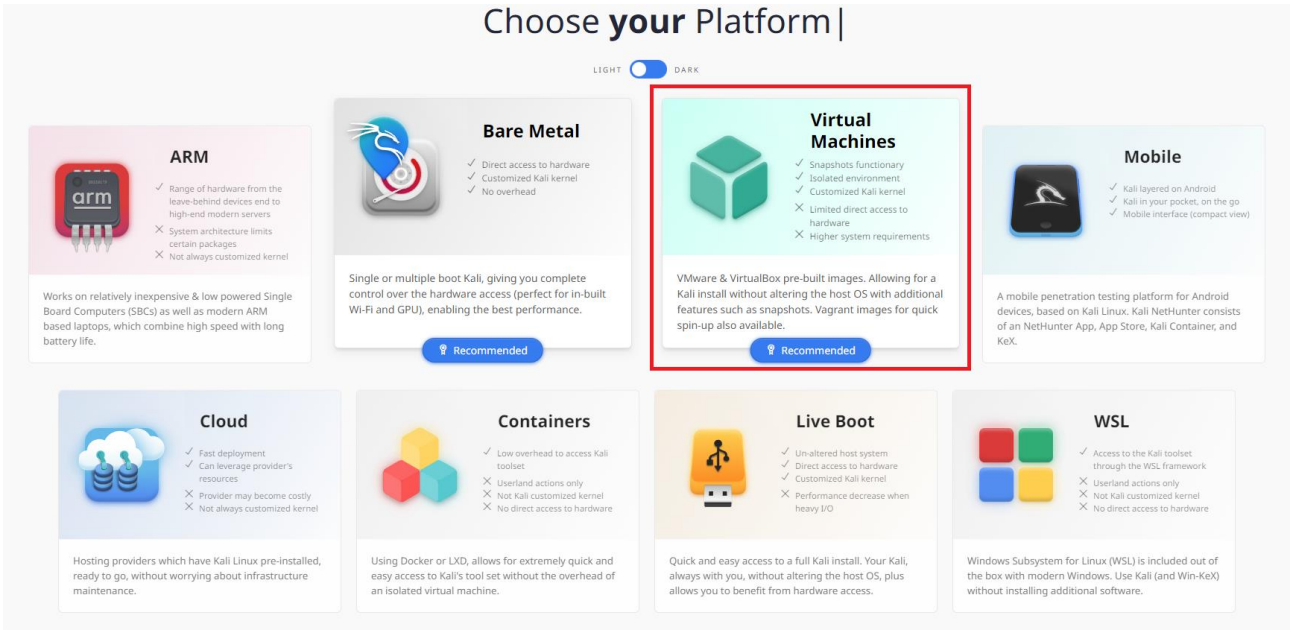
2.2. Створення фізичної мережі

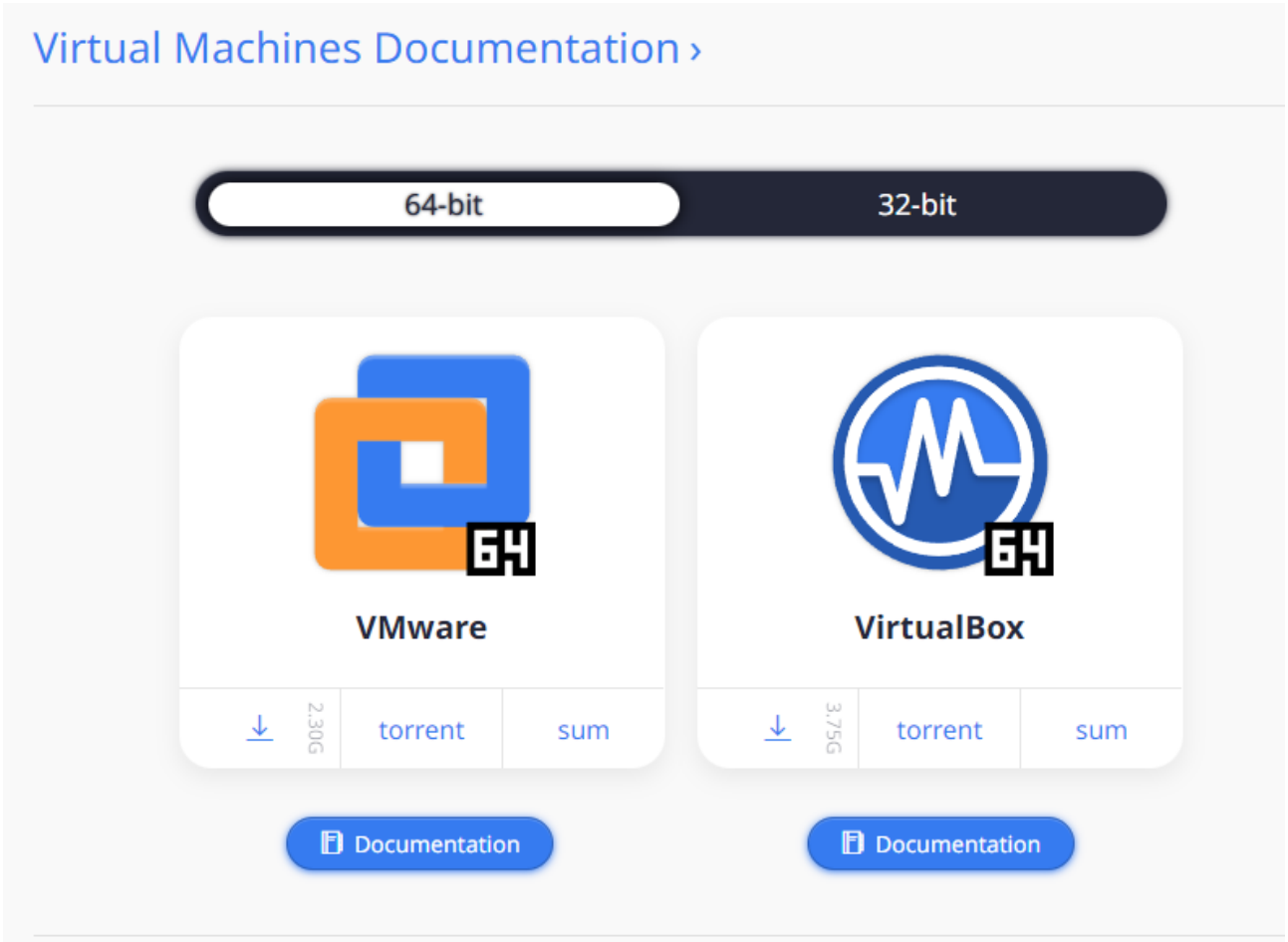
Виконання завдання зі створення фізичної мережі передбачає наступні кроки:

1. Побудуйте фізично мережу в комп'ютерному класі, використовуючи наявні пристрої та кабелі.
2. Запустіть кожен з комп'ютерів у мережі.
3. Перейдіть на [офіційний веб-сайт VirtualBox].
4. Завантажте інсталяційний файл у залежності від операційної системи вашого девайсу.

5. Запустіть інсталяційний файл та установіть VirtualBox на ваш девайс.
6. Перейдіть на офіційний сайт Kali Linux.
7. У верхній частині сторінки натисніть на Virtual Machines.

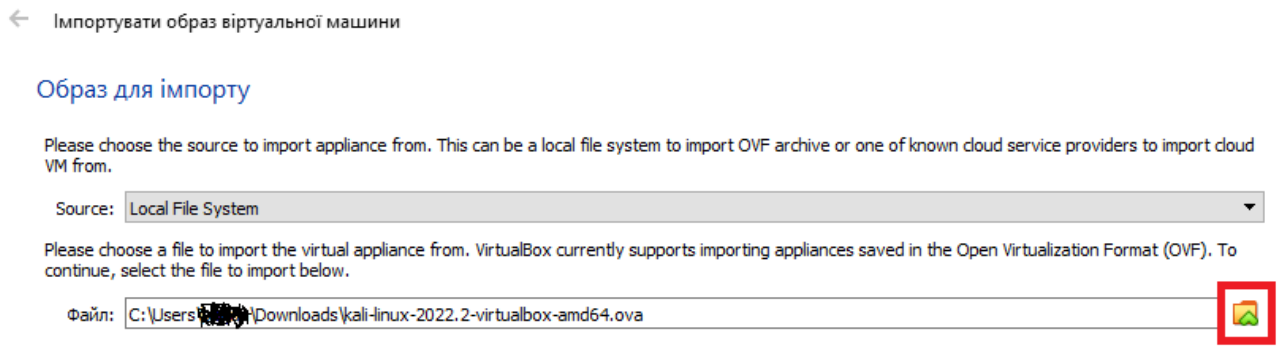
8. Виберіть та завантажте образ віртуальної машини для VirtualBox у залежності від розрядності вашої системи.



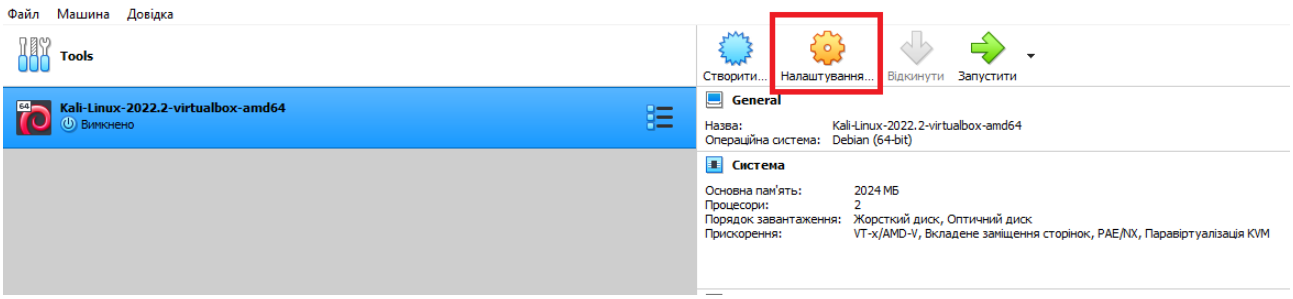


9. Встановіть образ віртуальної машини у Virtualbox:
    a. У відкритій програмі VirtualBox натисніть «Файл» → «Імпортувати образ віртуальної машини».

    b. У вікні «Образ для імпорту» вказати шлях до завантаженого образу Kali Linux.



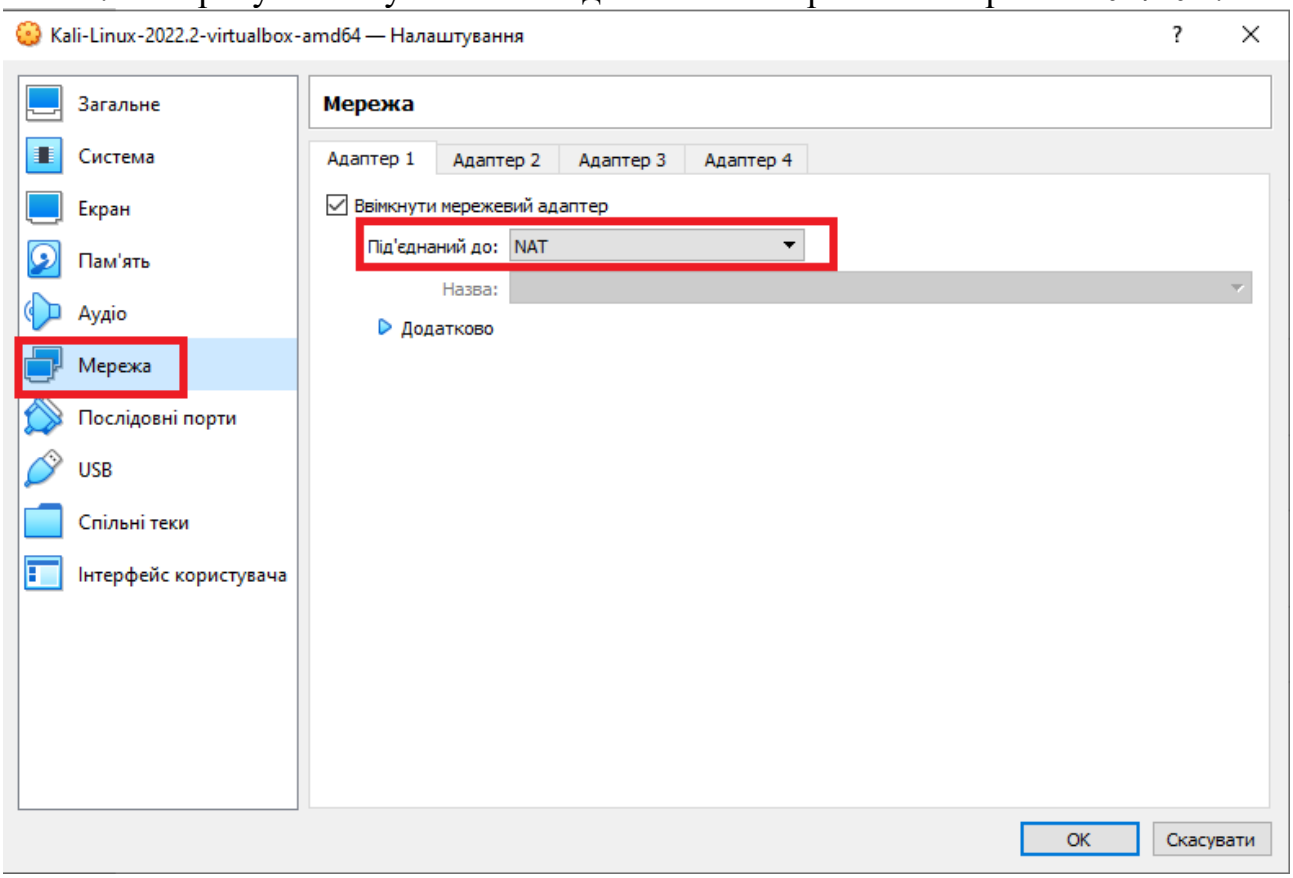
    c. Виберіть необхідні параметри та ресурси для віртуальної машини та натисніть «Імпортувати».
    d. В основному вікні VirtualBox виберіть новостворену віртуальну машину Kali Linux та натисність «Налаштування».

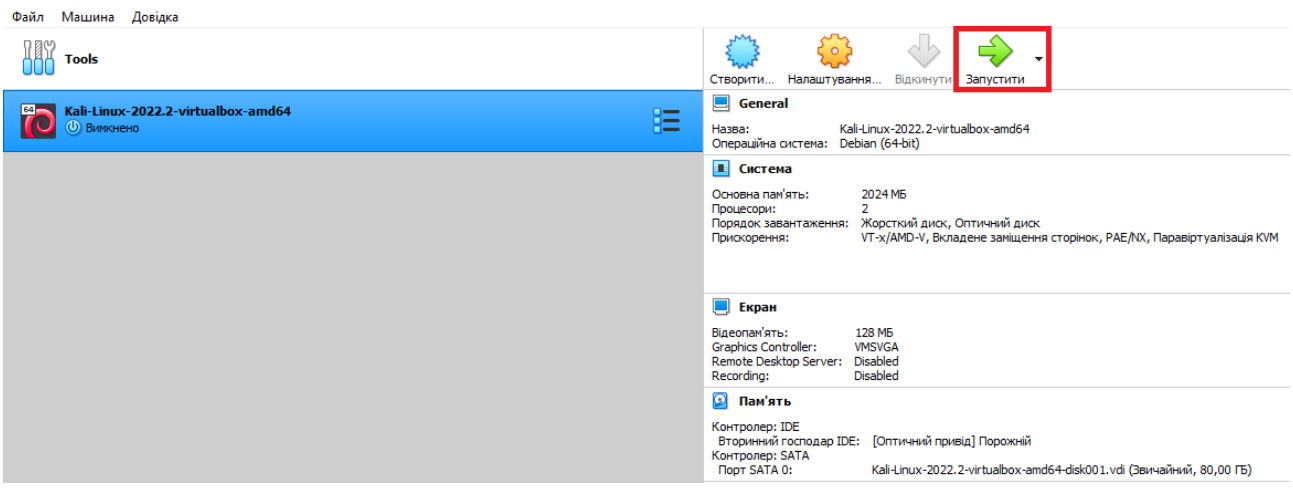


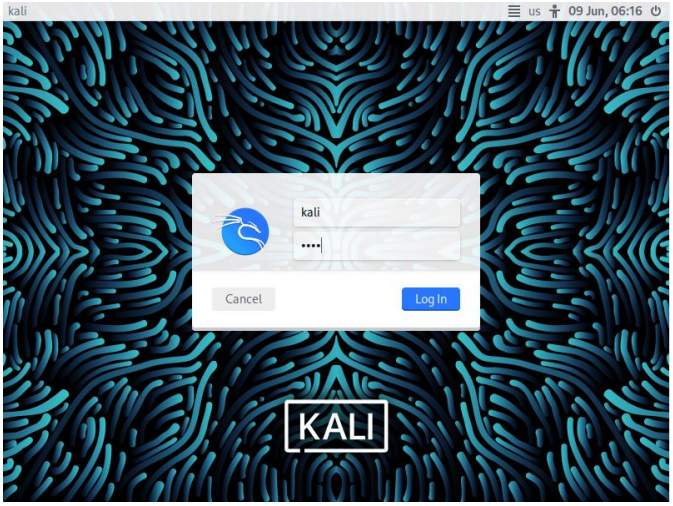
    e. У новому вікні виберіть вкладку «Мережа» та змініть налаштування першого адаптера на NAT (якщо це не зроблено за замовчуванням).
    f. Натисніть «ОК» щоб зберегти налаштування.

10. В основному вікні VirtualBox виберіть образ віртуальної машини Kali Linux та натисніть «Запустити».

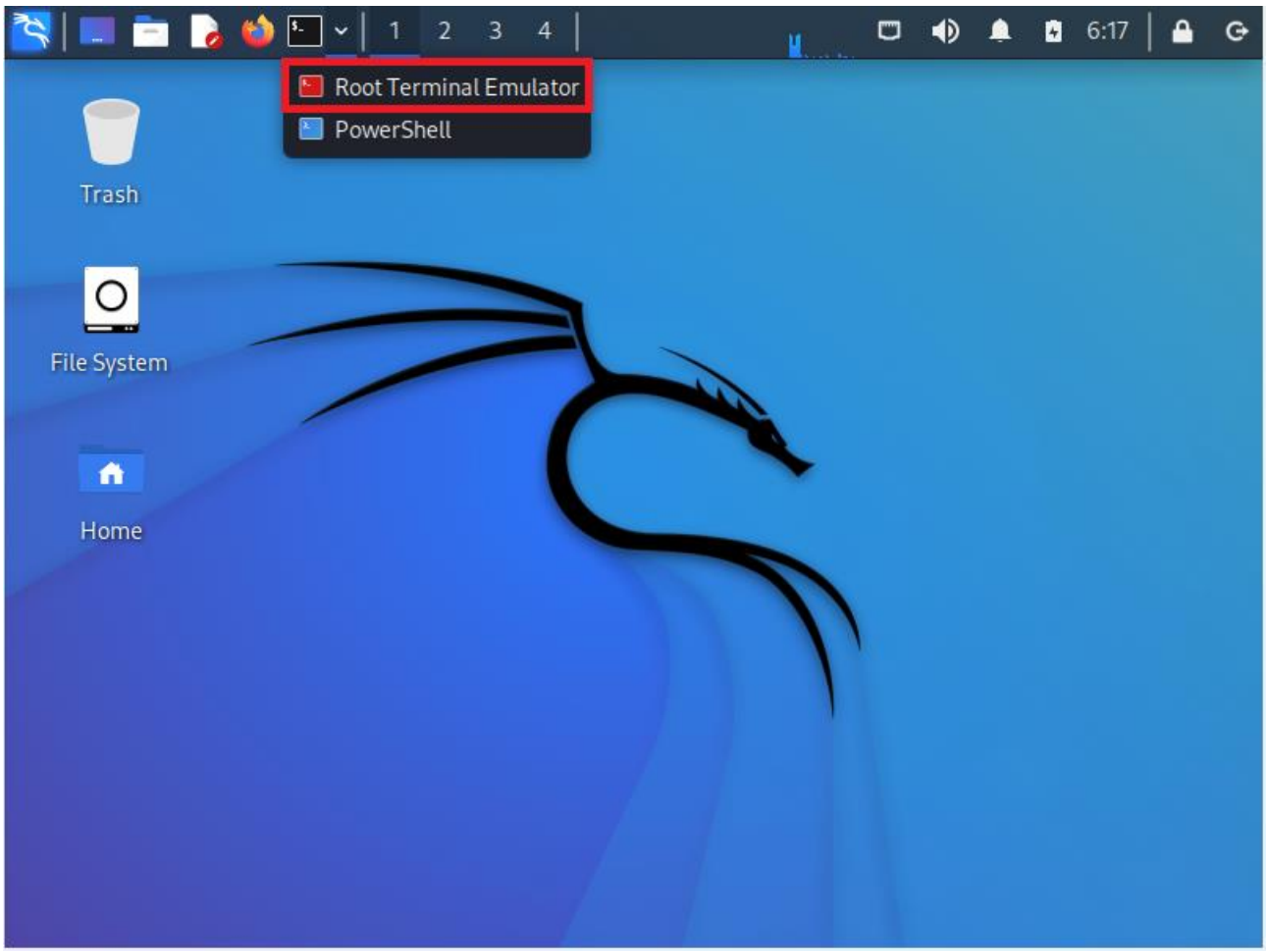
11. Авторизуватись у системі за допомогою пари логін/пароль : ***kali/kali***.







12. Відкрити Root Terminal Emulator. При запиті паролю ввести «kali».



13. Дізнатись IP-адресу свого пристрою за допомогою команди ifconfig.

```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
```

14. Дізнайтесь IP-адреси сусідніх пристроїв та перевірите доступність до них за допомогою команди «ping {IP-адреса}».

```
┌──(root㉿kali)-[~]
└─# ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.016 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.032 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.023 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.022 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.023 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=0.022 ms
64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=0.021 ms
^C
── 192.168.56.102 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6127ms
rtt min/avg/max/mdev = 0.016/0.022/0.032/0.004 ms
```

15. Знаючи IP адресу пристрою, використовуючи утиліту nmap, просканувати всю локальну мережу. Для цього використати «nmap –sV –sC –O {IP-адреса}/24». Наприклад, «nmap –sV –sC –O 192.168.2.0/24».

16. Підготувати звіт на основі отриманих даних сканування утилітою nmap.

РОЗДІЛ 3. ЗМАГАННЯ ЧЕРВОНОЇ ТА СИНЬОЇ КОМАНДИ НА ПОЛІГОНІ

Цей сценарій полягає в безпосередніх змаганнях червоної (атакуючої) та синьої (захисної) команди на кіберполігоні, використовуючи всі наявні інструменти для отримання доступу над інфраструктурою мережі команди захисту (для команди атаки), або для навчання роботі з аналізом трафіку та блокуванням шкідливих дій у мережі (для команди захисту).

3.1. Принцип роботи полігону

Під час роботи з полігоном використовуватимуться дві основні операційні системи:

- Kali Linux – для пристроїв кінцевих точок (хостів).
- Metasploitable 2 – для сервера.

Kali Linux це дистрибутив Linux для перевірки корпоративної безпеки на основі Debian GNU/Linux. Для спрощення процедури роботи в Kali Linux передбачено категорію під назвою Top 10 Security Tools (Топ-10 інструментів безпеки). Як випливає з назви, це десять інструментів безпеки, що найчастіше використовуються. У цю категорію входять такі інструменти, як aircrackng, burp-suite, hydra, john, maltego, metasploit, nmap, sqlmap, wireshark та zaproxy.

У Kali Linux ви знайдете кілька інструментів, які можна використовувати для наступних цілей.

Reverse engineering (Інженерний аналіз). У цій категорії містяться засоби для налагодження програм або розбору файлу, що виконується.

Стрес-тест. Ці інструменти призначені для стрес-тесту дротової та бездротової мережі, веб-середовища та VOIP (IP-телефонія).

Hardware hacking (Зламування обладнання). Інструменти цієї категорії використовуються під час роботи з програмами Android та Arduino.

Forensics (Судова експертиза). Представлені інструменти можуть бути використані для різних цифрових криміналістичних завдань. Вони дозволяють створювати образи дисків, проводити аналіз образів пам'яті та вирізати файли. Одним з найкращих криміналістичних інструментів Kali Linux є Volatility. Він управляється з командного рядка і має низку функцій для аналізу зображень, що у пам'яті. У Kali Linux є кілька графічних інструментів, таких як Autopsy і Guymager, а також виправлений xplico.

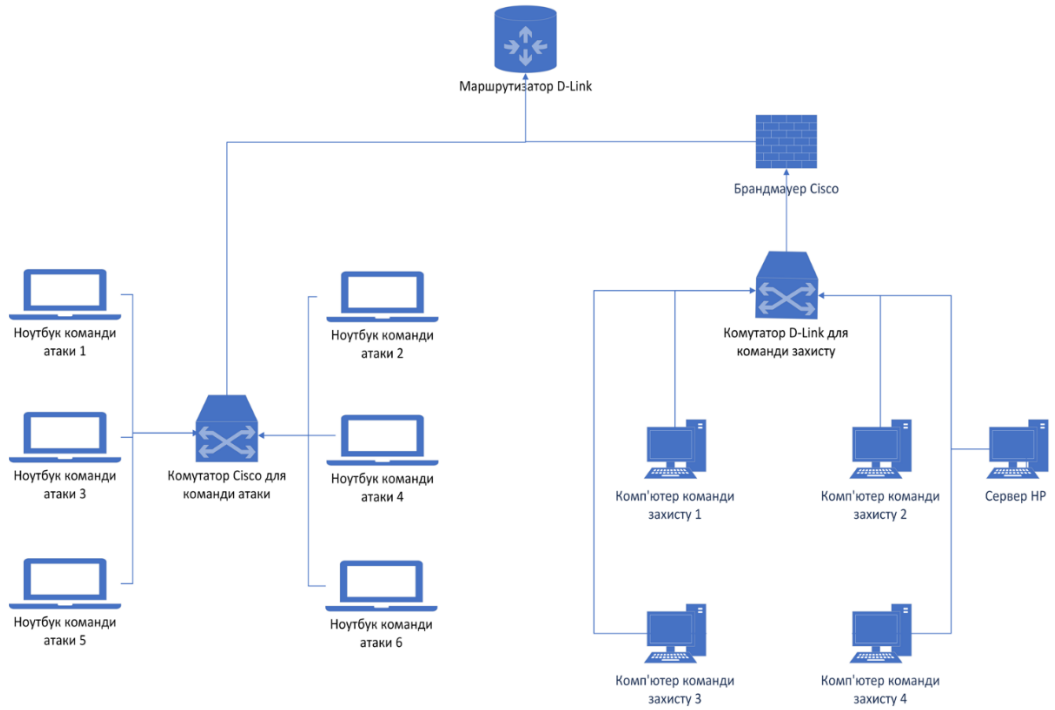
Для сервера ми використовуємо операційну систему Metasploitable 2. Metasploitable 2 визначається як сервер Linux, який навмисно зроблений вразливим. Metasploitable 2 призначений для тестування інструментів безпеки та демонстрації типових вразливостей. Версія 2 цієї віртуальної машини доступна для завантаження та містить ще більше вразливостей, ніж вихідний образ. Ця віртуальна машина сумісна з VMWare, VirtualBox та іншими поширеними платформами віртуалізації. За замовчуванням мережеві інтерфейси Metasploitable прив’язані до мережевих адаптерів NAT і Host-only, і образ ніколи не повинен піддаватися впливу ворожої мережі. За бажанням, образ Metasploitable 2 можна встановити як основну або допоміжну операційні системи, але через високу кількість навмисно створених вразливостей, це категорично не рекомендується робити. Найкращий спосіб використання Metasploitable 2 - це встановлення образу на віртуальну машину, у випадку полігону – на сервіс VirtualBox, який є підключеним до основного серверу команди захисту.

Серед основних відкритих портів, список із яких розташований в офіційній документації до системи, можна виділити: 21–FTP; 22–SSH; 23 – Telnet; 25 – SMTP; 80 – HTTP; 2049 – NFC; 3306 – MySQL; 5432 – PostgreSQL.

3.2. Створення мережі для роботи полігону

Для успішної та продуктивної роботи полігону необхідно почати з основ, з фундаменту цього проекту. Під час розробки полігону своєрідним фундаментом можна виділити створення мережі, яка буде з’єднувати всі вузли, кінцеві точки та мережеве обладнання в одне ціле для того, щоб забезпечити роботу системи.

Побудова мережі, як і побудова усіх інших речей починається із створення плану і макету, за якими мережа буде створюватись. Для цього ми використали програмне забезпечення від компанії Microsoft під назвою Microsoft Visio. Отже, схема мережі виглядає так:



На рисунку можна побачити, що мережа фізично розділена на дві частини. Перша частина складається з пристроїв для команди атаки, друга – з пристроїв для команди захисту. Пристрої для команди атаки складаються із шести ноутбуків HP в аудиторії кафедри, а також комутатор Cisco, який з'єднує ці шість ноутбуків в одну локальну підмережу. Пристрої для команди захисту складаються із 5 персональних комп'ютерів HP у серверній кімнаті кафедри, один з яких використовується в якості сервера. Також до складу пристроїв команди захисту входить комутатор D-Link, який використовується для з'єднання всіх кінцевих точок в єдину підмережу.

Додатковим пристроєм у складі синьої команди є використання брандмауера Cisco ASA 5506-X. Призначення цього пристрою полягає у створенні буферу між зовнішньою мережею та підмережою команди захисту, що дозволить команді захисту з виявленням загроз і шкідливого трафіку, який надходить від червоної команди, а також ускладнить завдання команді атаки, якій потрібно буде обійти конфігурації брандмауера для успішного проникнення в підмережу команди захисту. Особливість

використання брандмауеру в полігоні полягає в тому, що налаштування брандмауеру може або буде проводитись членами синьої команди. Це означає, що саме своїми зусиллями вони зможуть або мінімізувати кількість вразливостей, які можуть бути використані командою атаки для проникнення в їх систему, або навпаки, зробити свою систему більш вразливою для атак.

Обидві частини мережі з'єднані між собою за допомогою маршрутизатора D-Link, основне завдання якого об'єднати всі вузли і мережеве обладнання в одну повноцінну мережу, налаштувати IP-адреси кінцевим точкам і бути точкою зв'язку, через яку команда атаки та захисту зможуть взаємодіяти одна з одною.

3.3. Встановлення програмного забезпечення для роботи полігону

Завданням етапу встановлення програмного забезпечення для роботи полігону є інсталяція та налаштування сервісів для створення віртуальних машин, а також образів самих віртуальних машин на усіх комп'ютерах та ноутбуках команди атаки та захисту, а також, за потреби, налаштування мережевих конфігурацій та з'єднань. Конкретизуючи список програмного забезпечення, можна виділити такі етапи роботи: встановлення середовища віртуальних машин VirtualBox на комп'ютер команди захисту, який буде використовуватись в якості сервера; встановлення та налаштування образу віртуальної машини Metasploitable 2 на комп'ютер команди захисту, який буде використовуватись в якості сервера; встановлення середовища віртуальних машин VirtualBox на кожен комп'ютер команди захисту, окрім тих, які використовуються в якості приманки; встановлення на налаштування образу віртуальної машини Kali Linux на кожен комп'ютер команди захисту, окрім тих, які використовуються в якості приманки; встановлення середовища віртуальних машин VirtualBox на кожен ноутбук команди атаки; встановлення та налаштування образу віртуальної машини Kali Linux на кожен ноутбук команди атаки.

У загальному, для демонстрації практичної реалізації попередніх завдань, роботу можна розділити на три частини:

1. Встановлення середовища віртуальних машин VirtualBox.
2. Встановлення та налаштування образу віртуальної машини Kali Linux.

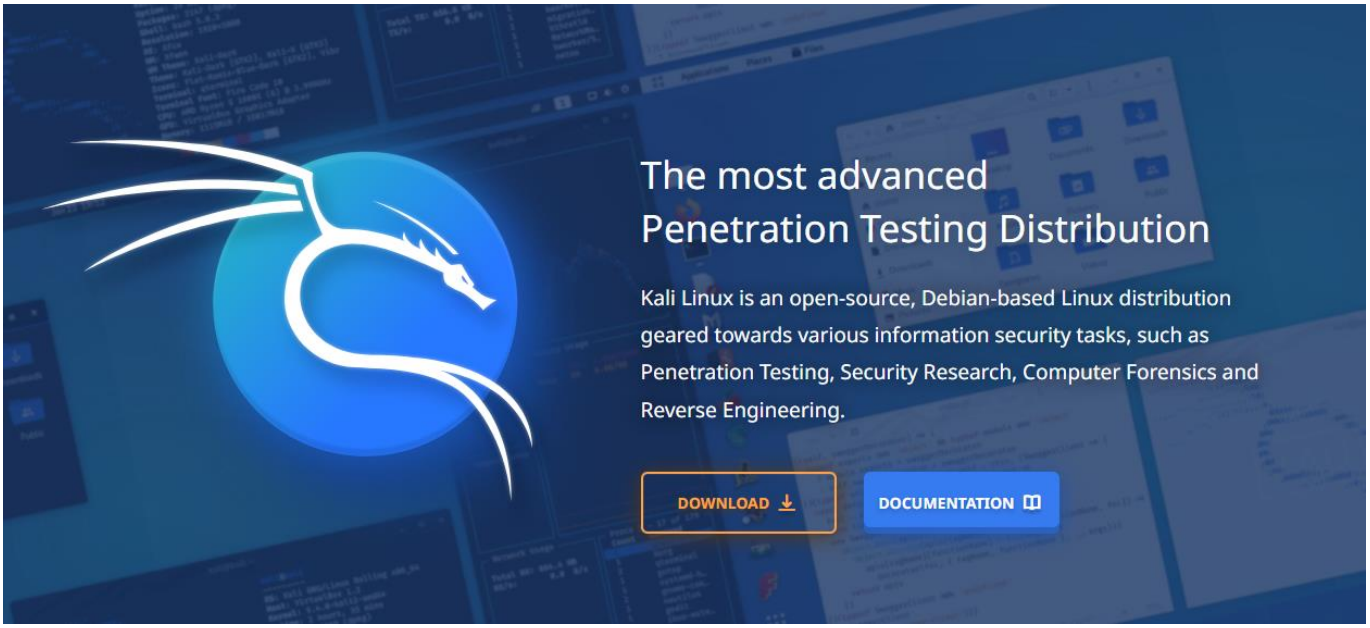
3. Встановлення на налаштування образу віртуальної машини Metasploitable 2.

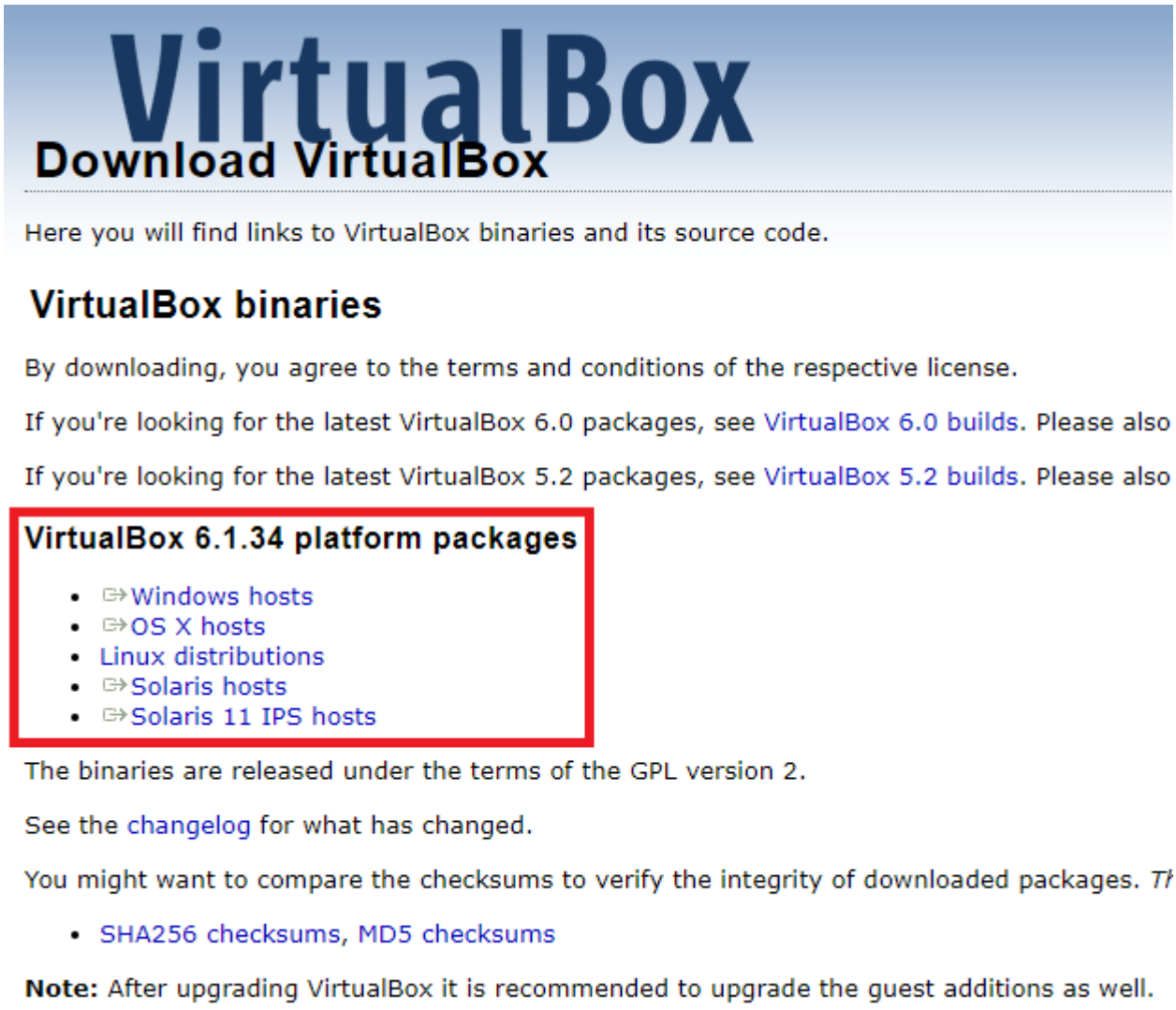
Встановлення середовища віртуальних машин VirtualBox. Середовище віртуальних машин VirtualBox це потужна багатофункціональна система, яка дозволяє запускати і використовувати операційні системи в якості віртуальних машин, що дозволяє зменшити ризик впливу прямої роботи з вразливими машинами та відокремити робоче середовище від реальної операційної системи пристрою.

Для встановлення середовища віртуальних машин VirtualBox необхідно завантажити інсталяційний файл для операційної системи Windows з офіційного веб-сайту VirtualBox.

Далі необхідно відкрити завантажений інсталяційний файл і, слідуючи вказівкам інсталятора, встановити програмне забезпечення на необхідні пристрої. У нашому випадку це: 1 комп'ютер-сервер команди захисту; 4 комп'ютери команди захисту; 6 ноутбуків команди атаки.

Встановлення образу віртуальної машини Kali Linux. Kali Linux це один із багатьох дистрибутивів операційної системи Linux, який орієнтований на роботу саме у сфері кібербезпеки. Дистрибутив вміщує в собі велику кількість програмного забезпечення, яке покриває майже всі види завдань, які виконуються спеціалістами з інформаційної безпеки, у тому числі завдань для обох синьої та червоної команди.

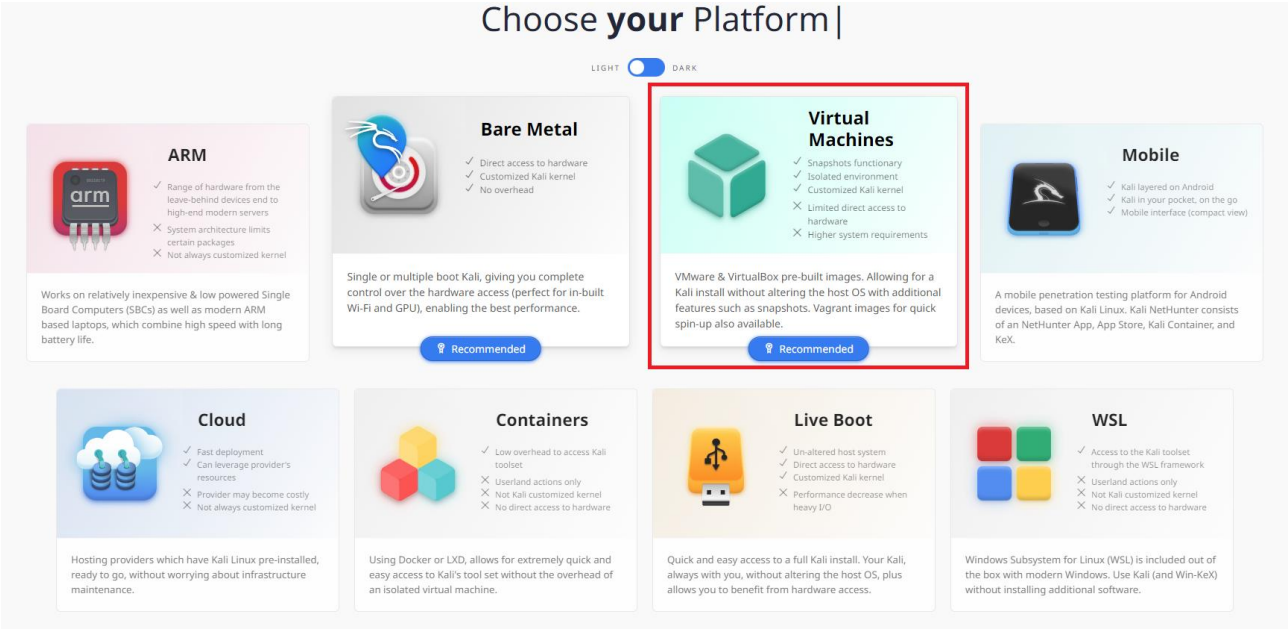


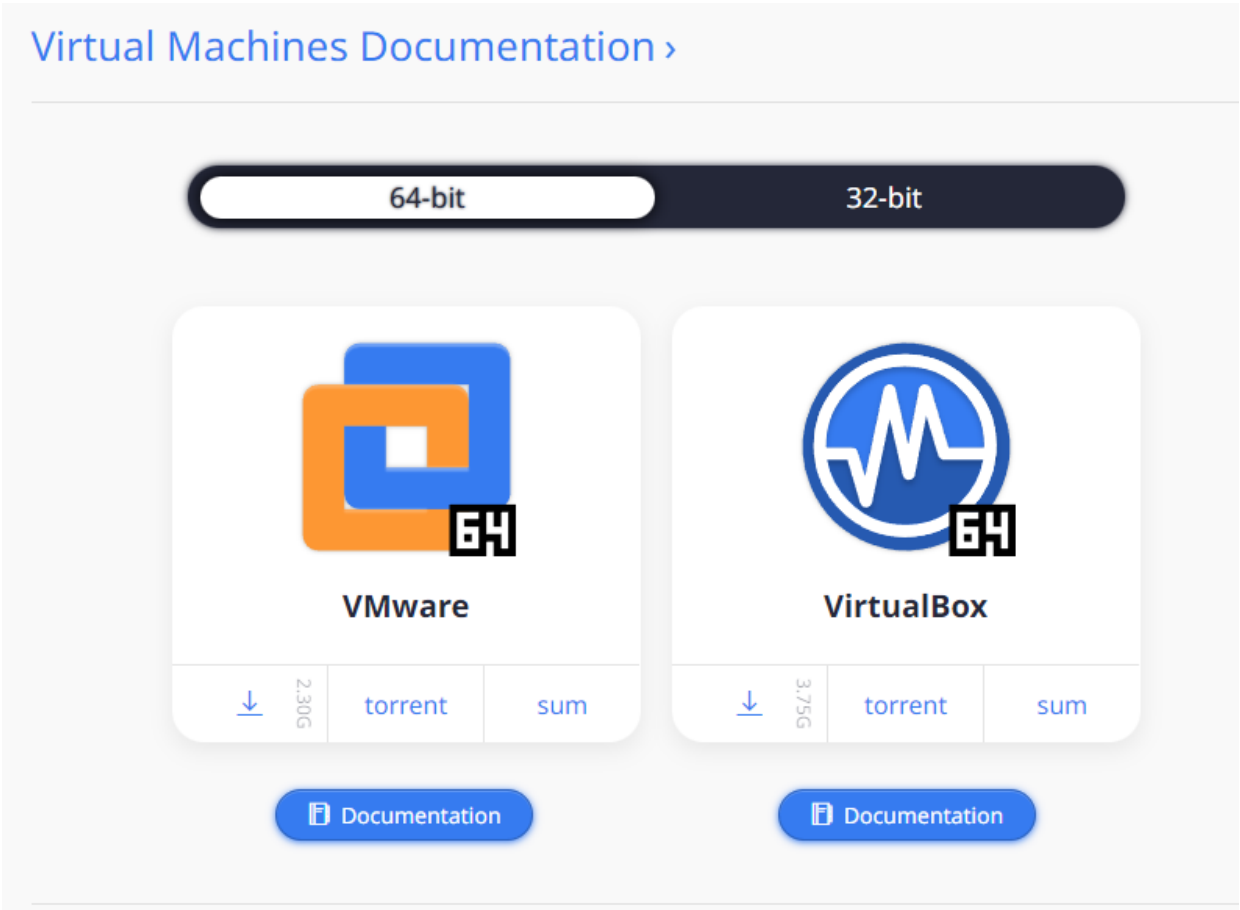


Для завантаження та встановлення образу віртуальної машини Metasploitable 2 необхідно перейти на офіційний веб-сайт Kali Linux. Знаходячись на офіційній сторінці необхідно перейти на сторінку Download і у верхній частині екрану натиснути на Virtual Machines.

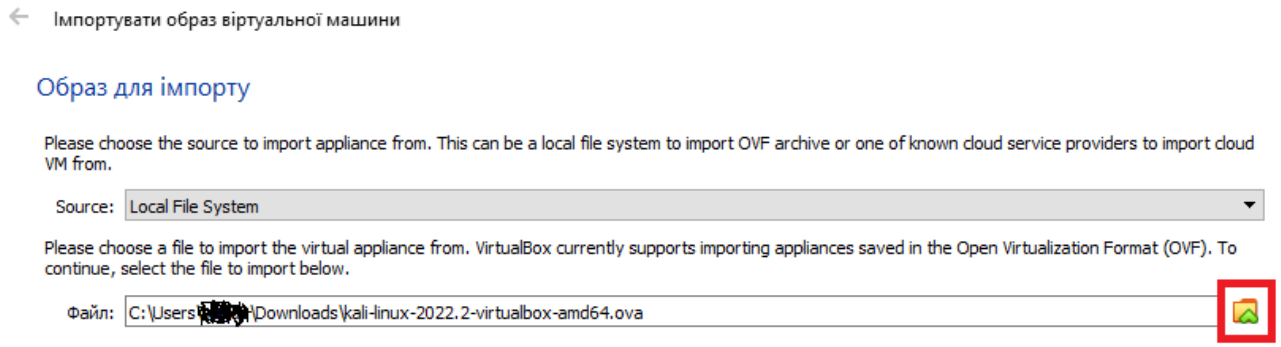
Після цього нас перенаправляє на частину сторінки, де можна вибрати тип середовища віртуальних машин, для якого необхідно завантажити образ віртуальної машини Kali Linux. На вибір дається VMWare і VirtualBox, а також вибір необхідної розрядності системи.

Далі завантажений образ віртуальної машини Kali Linux можна встановити безпосередньо у VirtualBox. Для цього у відкритому середовищі VirtualBox необхідно натиснути на **Файл → Імпортувати образ віртуальної машини**.





У вікні ***Образ для імпорту*** необхідно вказати шлях до завантаженого образу Kali Linux.

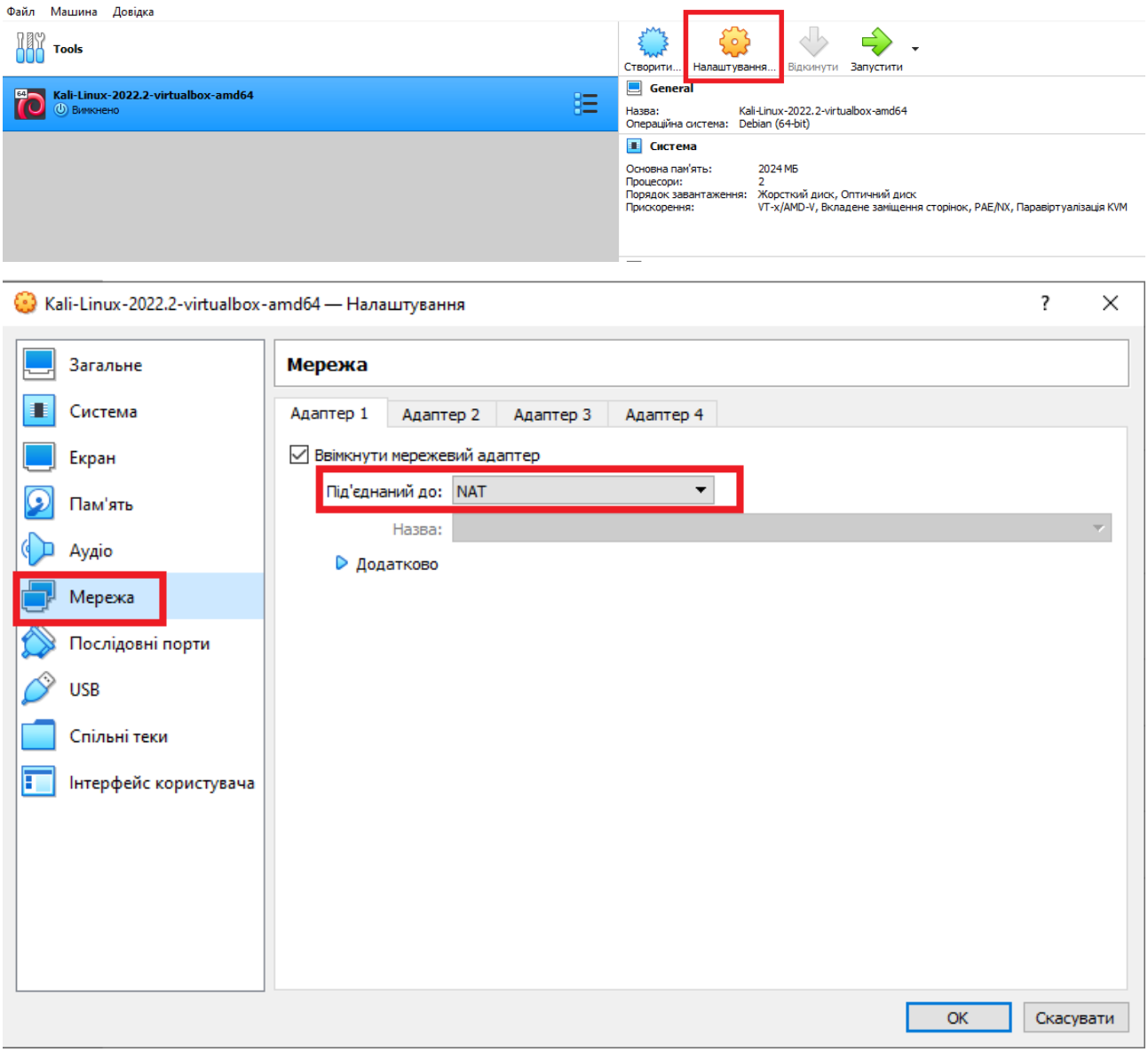


Після вибору необхідних параметрів для роботи віртуальної машини, а саме: кількості оперативної пам’яті, фізичної пам’яті на диску, ядер процесора, тощо, необхідно натиснути **Імпортувати**. У залежності від системних параметрів пристрою, на якому проводиться інсталяція віртуальної машини, імпортування відбувається в межах від 5 до 30 хвилин.

Після закінчення імпортування віртуальна машина Kali Linux теоретично готова до використання, але для більш безпечної роботи варто провести додаткове налаштування мережевих параметрів, щоб захистити віртуальне середовище. Для цього необхідно натиснути на іконку **Налаштування** в правій верхній секції середовища VirtualBox.

У вікні налаштувань необхідно перейти у вікно Мережа та змінити налаштування першого адаптера на NAT (якщо це не зроблено за замовчуванням).

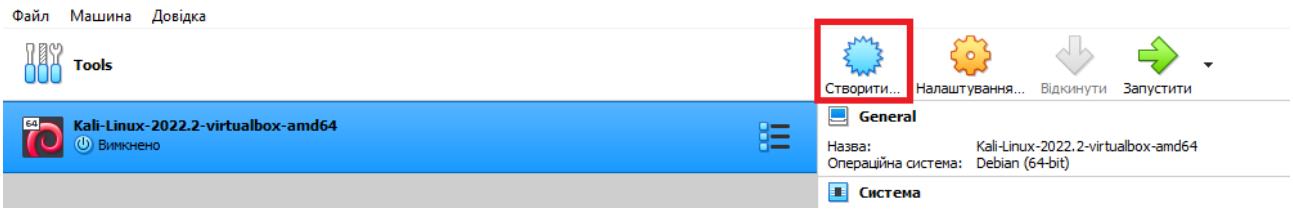
Після збереження налаштувань образ віртуальної машини Kali Linux у середовищі віртуалізації VirtualBox буде готовий до використання. Ці дії необхідно повторити для чотирьох комп’ютерів команди захисту та шести ноутбуків команди атаки.



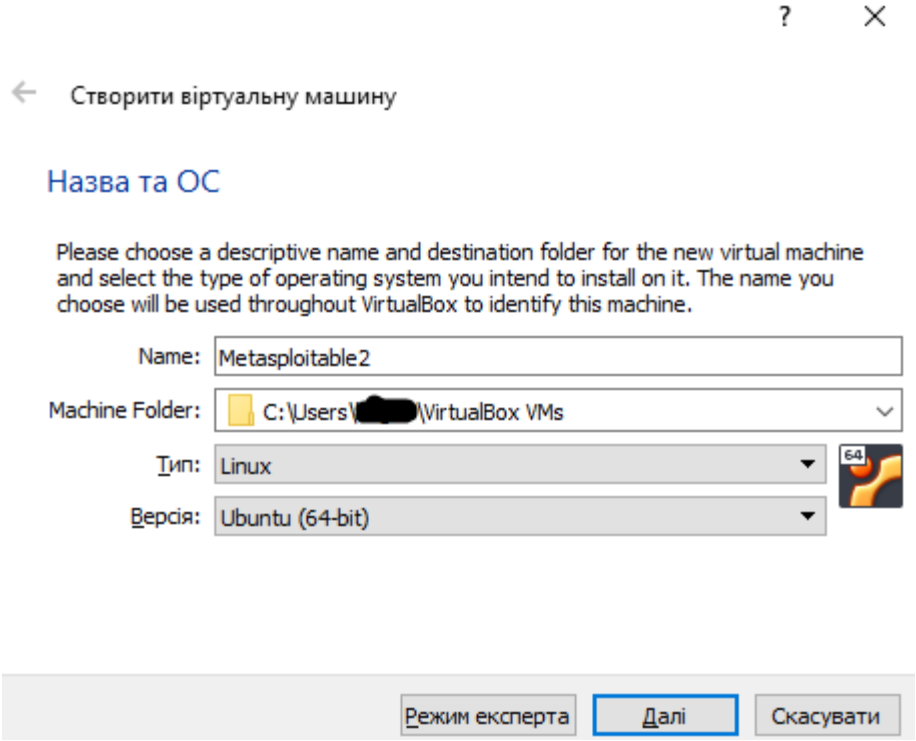
Встановлення та налаштування образу віртуальної машини Metasploitable 2. Metasploitable 2 - це одне з найкращих середовищ для проведення навчань з кібербезпеки. Система включає в собі велику кількість відкритих портів з вразливими сервісами на кожному з них. Завдяки цьому спеціалісти з кібербезпеки можуть тренуватись або проводити тренування для інших, використовуючи можливості програмного забезпечення Metasploit та основи проведення пентестингу.

Встановлення образу віртуальної машини Metasploitable 2 потребує від нас переходу на офіційний веб-сайт SourceForge [34] та завантаження архіву з образом формату vmdk. Перед створенням віртуальної машини необхідно обов'язково розархівувати завантажені файли в окрему папку, яка буде використовуватись як джерело для створення віртуальної машини. Для встановлення образу віртуальної

машини Metasploitable 2 необхідно у відкритому середовищі VirtualBox натиснути на «Створити» у верхній частині вікна.



У новому вікні необхідно вказати назву майбутньої віртуальної машини, а також тип та версію операційної системи. У нашому випадку це Metasploitable 2, Linux, Ubuntu (64 bit).



У наступному вікні необхідно вибрати кількість оперативної пам’яті, яка буде виділена віртуальній машині, після чого натиснути ***Далі***. Після вибрати опцію ***Використовувати існуючий файл віртуального жорсткого диска***, для якого нижче необхідно вказати шлях до розархівованого в пункті 2 файлу ***Metasploitable.vmdk***. Далі натиснути ***Створити***. Після закінчення створення віртуальної машини в основному вікні VirtualBox необхідно вибрати новостворену віртуальну машину Metasploitable2 та натиснути ***Налаштування***. У новому вікні, так само, як під час встановлення Kali Linux, необхідно вибрати вікно ***Мережа*** та змінити налаштування

першого адаптера на NAT (якщо це не зроблено за замовчуванням). Зберігши зміни, ми підготували віртуальну машину до роботи. Двічі натиснути на віртуальну машину Metasploitable 2 зі списку в VirtualBox, або натиснути на опцію ***Запустити*** у верхній частині вікна. У консольному режимі в запущеній віртуальній машині необхідно ввести логін/пароль: ***msfadmin/msfadmin***, після чого відбудеться перший запуск і підтягування всіх необхідних пакетів. Після завантаження всього необхідного нам потрібно ввести команду ***ifconfig*** у консолі для того, щоб дізнатись IP адресу цільової машини. Звіривши IP-адресу віртуальної машини та будь-якого з хостів команди захисту та атаки можна перевірити правильність налаштування локальної мережі, створеної раніше.

3.3. Інструкція для роботи червоної та синьої команд

Червона команда – це команда чорних капелюшків, команда атаки. Основне завдання цієї команди полягає в проникненні в мережу на основі знайдених під час сканування вразливостей, закріплення в комп'ютерах, які знаходяться в цій мережі, а також в отриманні доступу до файлу з хешом.

У загальному важко передбачити, який хід роботи буде виконуватись командою атаки, тому що завдання цього колективу полягає в проникненні в підмережу синьої команди і отриманні доступу до їх пристроїв та файлів, які знаходяться в них. Це завдання є досить творчим, і тому його реалізація може відрізнятись і залежати від стилю і звичок учасників зі сторони червоної команди. Але в загальному початковий процес команди атаки виглядає таким чином:

1. Запустити віртуальні машини із встановленою спеціалізованою операційною системою Kali Linux.
2. За допомогою інструмента nmap просканувати цільову мережу та знайти основну першу машину в мережі.
3. Виявити вразливості на першій машині всіма доступними способами.
4. Експлуатувати знайдені вразливості і отримати доступ до першої машини.
5. Закріпитись у першій машині будь-яким способом (залишити бекдори).

6. З першої машини просканувати інші мережі та виявити інші машини.
7. Виявити вразливості на інших машинах всіма доступними способами.
8. Експлуатувати вразливості і отримати доступ до інших машин.
9. Закріпитись в інших машинах будь-яким способом (залишити бекдори).
10. Отримати доступ до файлу з хешом на одній з машин.

Формулювання десятого завдання може відрізнятись залежно від ситуації, тому що лаборант або викладач мають можливість вносити свої корективи у фінальне завдання для команди атаки, враховуючи можливості як Metasploitable 2 так і Kali Linux. Основна ідея спроектованої системи - це інтерпретування CTF-стилізованих завдань (Capture The Flag), де команді атаки необхідно отримати доступ до файлу з «прапорцем» - даних формату hash-string. Але гнучкість системи дозволяє змінювати тип завдання і необхідний результат для успішного виконання поставлених перед командою завдань.

Синя команда – це команда білих капелюшків. Основна задача цієї команди в якомога швидший період часу визначити, з якого комп'ютера йде атака на їх мережу, а також заблокувати цей комп'ютер до того, як він отримає доступ до файлу з хешом, який знаходиться на одному з комп'ютерів мережі.

Відмінність у роботі червоної та синьої команди полягає в тому, що завдання команди захисту є досить шаблонним, але складність цього завдання все одно є великою, оскільки учасникам синьої команди необхідно весь час аналізувати трафік у мережі і миттєво реагувати на інциденти. У загальному робота синьої команди складається з таких етапів:

1. Запустити встановлені на комп'ютерах віртуальні машини Kali Linux.
2. Встановити і налаштувати програму для перехоплення пакетів у мережі – Wireshark.
3. Запустити процес відловлювання пакетів у мережі, за результатами якого визначити, з якого ворожого комп'ютера надходять пакети.
4. Після виявлення ворожого комп'ютера зробити спробу блокування цього комп'ютера в мережі (без блокування MAC-адреси).

Завдання синьої команди можна вважати успішно виконаними, коли в мережі більше не присутній шкідливий трафік, який надходить від червоної команди, і усі члени червоної команди були заблоковані в мережі. У такому випадку учасники команди захисту успішно відбили кібератаку і захистили мережу від проникнення і викрадення цінної інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Довгань О.Д. Методологія захисту інформації: навч.-метод. посіб. / О.Д.Довгань, Г.М.Гулак, А.К.Гринь, С.В.Мельник. – К.: Наук.-вид. центр НА СБ України, 2012. – 184 с.

2. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с

3. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В.Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний, Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178с.

4. Марк Гудмен, Злочини майбутнього, Видавництво Фабула , 2019, 592с.

5. Dakshina Ranjan Kisku, Phalguni Gupta, Jamuna Kanta Sing Advances in Biometrics for Secure Human Authentication and Recognition Видавництво: CRC Press - дання: 2016, Сторінок: 352, ISBN: 9781138033771

6. Юлія Лісовська, Кібербезпека. Ризики та заходи. К.: Кондор , 2019 , 272с

7. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: Навчальний посібник / О.В.Курбан. – Київ: ВІКНУ, 2016. - 286 с

8. V. Rao Vemuri Enhancing Computer Security with Smart Technology Видавництво: CRC Press - 2019 Стор.: 288 ISBN: 9780367391720

9. В. О. Хорошко, О. В. Криворучко, М. М. Браіловський та ін. Захист систем електронних комунікацій , Видавництво: КНТЕУ – 2019, Стор.164, ISBN: 978-966-629-970-6

10. Бобало Ю. Я., Дудикевич В. Б., Микитин Г. В. Стратегічна безпека системи “об’єкт – інформаційна технологія” , Видавництво: Львівська політехніка = 2020, Стор.: 260, ISBN: 978-966-941-481-6

11. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: Навч. посібник. Дніпро: Дніпроп. держ. Унт внутріш. справ, 2020. 144с.

12. М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; Інформаційна безпека. Підручник В. В. Остроухов, під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.

13. Остапов С.Е., Євсеєв С.П. , Король О.Г. Технології захисту інформації Видавництво: Новий світ-2000, 2021, Стор. 678, ISBN: 978-617-7519-44-6

14. Юрій Когут, Кібербезпека та ризики цифрової трансформації компанії. Видавництво Консалтингова компанія Сідкон 2021 , 372с. ISBN 978-966-97546-9-1

15. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання CISCO Видавництво: Львівська політехніка Рік видання: 2021, С.: 232, ISBN: 978-966-941-583-7

16. Юрій Когут, Кібертероризм. Історія, цілі, об'єкти . Видавництво Консалтингова компанія Сідкон 2021 , 304с.

17. Офіційний сайт Міністерства освіти і науки України: http://www.mon.gov.ua/

18. Закон України «Про освіту»: [Електронний ресурс]. – Точка доступу: http://zakon0.rada.gov.ua/laws/show/1060-12.

19. Закон України «Про вищу освіту»: [Електронний ресурс]. – Точка доступу: http://zakon2.rada.gov.ua/laws/show/1556-18.

20. Положення про проведення практики студентів вищих навчальних закладів України [Електронний ресурс]. – Точка доступу: https://zakon.rada.gov.ua/laws/show/z0035-93#Text

21. Офіційний сайт Національної бібліотеки України імені В.І. Вернадського: http://www.nbuv.gov.ua/

22. Закон України «Про інформацію» від 02.10.1992 No 2657-XII

23. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 No 80/94-ВР

24. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 No373

25. Державний стандарт України Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96

26. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

27. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

28. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.

29. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.

30. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

31. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення.

32. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

33. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

34. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

35. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

36. НД ТЗІ 2.7-011-12 Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.

37. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи.

38. НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

39. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

40. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

41. C. Panek. Networking Fundamentals. John Wiley & Sons, Inc.: Hoboken, NJ, 2020. 319 p.

42. A. Samuel. Network Ethical Hacking and Penetration Testing. Los Angeles, CA, 2021. 387 p.

43. Y. Diogenes, E. Ozkaya. Cybersecurity – Attack and Defense Strategies. Packt Publishing, 2018. 326 p.

44. R. Davis. The Art of Network Penetration Testing. Manning Publications, 2020. 310 p.

45. R. Herzog, J. O’Gorman, M. Aharoni. Kali Linux Revealed: Mastering the Penetration Testing Distribution. Offsec Press; Illustrated edition, 2017. 342 p.

46. S. Parasram, A. Samm, D. Boodoo, G. Johansen, L. Allen, T. Heriyato, S. Ali. Kali Linux – Assuring Security by Penetration Testing. Packt Publishing; 3rd Revised edition, 2018. 527 p.

47. Metasploitable 2 Exploitability Guide. URL: https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

Формат 60х84/16. Папір офс. Гарнітура Times New Roman.
Друк офс. Ум. друк арк. 2,21
Тираж 300 шт.
Видавництво УжНУ

м. Ужгород, вул. Університетська, 14