МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет будівництва і архітектури

БЕЗПЕКА ІНТЕРНЕТ-РЕСУРСІВ

Методичні вказівки
до виконання лабораторних робіт та індивідуального завдання
для здобувачів другого (магістерського) рівня вищої освіти
спеціальності 125 «Кібербезпека та захист інформації»

Київ 2024

УДК 004.056.5
Б39

Укладач: Є.Є. Шабала, канд. техн. наук, доцент

Рецензенти: Терентьєв О.О., д-р техн. наук, професор

Відповідальний за випуск Ю.І. Хлапонін д-р техн. наук, професор

Затверджено на засіданні кафедри кібрбезпеки та комп'ютерної інженерії протокол № 3 від 22 жовтня 2024 року.

Видається в авторській редакції.

Безпека інтернет-ресурсів: методичні вказівки/ уклад.: Б39 Є. Є. Шабал. – Київ : КНУБА, 2024. – 32 с.

Містить завдання до лабораторних робіт, індивідуальну роботу та список літератури.

Призначено для здобувачів другого (магістерського) рівня вищої освіти спеціальності 125 «Кібербезпека та захист інформації».

ЗМІСТ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Методичні вказівки спрямовані на отримання практичних навичок виявленні вразливості веб-додатків шляхом аналізу HTTP-запитів, вивчення механізмів SSL-шифрування та аналізу терміну дії SSL-сертифікатів для забезпечення безпечного з'єднання веб-додатків, використання проксі-сканера Burp Suite для аналізу веб-додатків, ознайомлення з можливостями та інтерфейсом Wireshark, освоєння процесу сканування мережевих портів за допомогою інструменту Nmap та його графічного інтерфейсу Zenmap.

Лабораторні заняття з дисципліні «Безпека інтернет-ресурсів» у студентів спеціальності 125 «Кібербезпека та захист інформації» займають 30 годин і охоплюють розділи курсу, що пов’язані з вивченням сучасних архітектур веб-додатків, виявлення їх вразливостей та методів захисту.

Мета лабораторних занять полягає у отриманні практичних навичок виявленні вразливості веб-додатків шляхом аналізу HTTP-запитів, вивченню механізмів SSL-шифрування та аналізу терміну дії SSL-сертифікатів для забезпечення безпечного з'єднання веб-додатків, використанні проксі-сканера Burp Suite для аналізу веб-додатків, ознайомлення з можливостями та інтерфейсом Wireshark – інструментом для аналізу мережевих пакетів, який дозволяє виявляти проблеми у мережевому трафіку, освоїти процес сканування мережевих портів за допомогою інструменту Nmap та його графічного інтерфейсу Zenmap.

Лабораторні роботи виконуються на лабораторних заняттях з дисципліни. Підготовка до лабораторних занять здійснюється студентами в часи самостійної роботи. Перелік і кількість задач для розв’язання визначається викладачем, який веде лабораторні заняття, відповідно до робочої програми дисципліни. Після виконання кожної роботи студенти складають звіт, котрий захищають. За результатами виконання та захисту роботи виставляються бали за спеціальною шкалою оцінювання, наведеною у робочій програмі. Бали, отримані за окремі роботи, формують загальну суму балів за дисципліну, яка враховується у підсумкову оцінку за модуль та семестр.

Оскільки кібератаки швидко зростають, організації необхідно приділяти велику увагу тестуванню на проникнення і продовжувати стежити за своєю мережею, щоб запобігти атаці, яка може завдати серйозної шкоди. Щоб керувати операціями із забезпечення безпеки,

експерти з безпеки і дослідники повинні покладатися на інструменти безпеки і злому, які допомагають їм мінімізувати час і ефективно контролювати і виконувати тестування на проникнення в мережі для захисту мережі [1].

До основних загроз, що можуть вплинути на безпеку інтернет-ресурсів, відносяться: хакерські атаки, фішинг, DDoS-атаки, віруси та шкідливі програми.

Існує кілька ключових способів захисту інтернет-ресурсів: SSL-сертифікати, фаєрволи (брандмауери), антивірусні програми– допомагають виявляти та видаляти шкідливі програми, що можуть загрожувати веб-ресурсу, регулярне оновлення програмного забезпечення, резервне копіювання даних.

Сучасні інструменти дають змогу проводити перевірки на наявність потенційних загроз і вразливостей, що можуть бути використані зловмисниками. Основними задачами інструментів аналізу вразливостей є:

1. Виявлення вразливостей: SQL-ін'єкції, міжсайтовий скриптинг (XSS), CSRF (міжсайтова підробка запитів, вразливості в автентифікації та авторизації, неправильні налаштування безпеки серверів.
2. Аналіз продуктивності.
3. Оцінка захищеності конфігурації.
4. Моніторинг та аудит трафіку.
5. Тестування стійкості до атак: DDoS-атаки, перехоплення даних, зловживання сесіями.
6. Перевірка на відповідність стандартам. Інструменти дозволяють перевірити веб-додатки на відповідність стандартам безпеки, таким як:

- OWASP Top 10.
- PCI-DS (стандарт безпеки даних платіжних карток).
- GDPR (Загальний регламент захисту даних).

ЗАВДАННЯ ДО ЛАБОРАТОРНИХ ЗАНЯТЬ

Лабораторна робота №1. Аналіз вразливостей веб-додатків на основі HTTP-запитів

Мета:

Навчитися виявляти вразливості веб-додатків шляхом аналізу HTTP-запитів.

Задачі:

1. Ознайомитися з принципом роботи HTTP-запитів та відповідей.
2. Вивчити структуру типових HTTP-запитів.
3. Провести ручний аналіз HTTP-запитів для виявлення можливих вразливостей.
4. Запропонувати методи усунення виявлених вразливостей.

Довідкова інформація / Сценарій:

Багато вразливостей веб-додатків можуть бути виявлені шляхом аналізу HTTP-запитів, наприклад, SQL-ін'єкції або XSS. Студенти аналізуватимуть запити та відповіді на них, щоб виявити потенційні загрози.

Необхідні ресурси:

Будь-який веб-браузер з функцією інспектора елементів (наприклад, Chrome DevTools).

Хід виконання роботи:

1. Відкрийте веб-браузер і запустіть інспектор елементів (у Chrome натисніть F12 або використовуйте меню Налаштування > Інструменти розробника).
2. Перейдіть на вкладку "Network" і завантажте тестовий веб-додаток.
3. Відстежуйте HTTP-запити, що відправляються на сервер. Для цього виконайте декілька дій на веб-додатку (вхід у систему, заповнення форми тощо).
4. Проаналізуйте заголовки запитів і відповідей: перевірте наявність Cookie, параметрів сесії, передачу конфіденційних даних у відкритому вигляді.

5. Визначте можливі вразливості, такі як відсутність шифрування або відправка чутливої інформації у відкритому вигляді.

6. Запропонуйте методи усунення виявлених вразливостей, наприклад, використання HTTPS, обмеження доступу до Cookie.

Захист звіту з лабораторної роботи полягає в пред'явленні викладачеві отриманих результатів (на екрані монітора), демонстрації отриманих навичок і відповідях на питання викладача.

Контрольні питання

1. Які види вразливостей можуть бути виявлені шляхом аналізу HTTP-запитів?

2. Як відрізнити шифровану передачу даних від незахищеної в HTTP-запитах?

3. Що таке SQL-ін'єкція, і як її можна виявити у HTTP-запитах?

4. Що таке XSS (Cross-Site Scripting), і як його можна виявити під час аналізу HTTP-запитів?

5. Як можна захистити веб-додаток від передачі конфіденційних даних у відкритому вигляді?

6. Які заходи можна вжити для усунення вразливостей, виявлених під час аналізу HTTP-запитів?

Лабораторна робота №2. Аналіз терміну дії сертифікатів безпеки SLL

Мета:

Навчитися виявляти небезпечні з’єднання шляхом пошуку недійсних протоколів безпеки.

Задачі:

1. Ознайомитися з відмінностями HTTP від HTTPS.
2. Вивчити принципи роботи SSL-шифрування та різновиди сертифікатів безпеки.
3. Провести ручний аналіз терміну дії SSL-сертифіката веб-ресурсів.
4. Запропонувати сертифікати безпеки для: для фізичних осіб, для бізнесу (малого, великого), для сайтів, з великою кількістю субдоменів (один на вибір) та обґрунтувати свій вибір.

Довідкова інформація / сценарій:

Коли користувач вводить адресу сайту в браузері, відбувається запит до сервера, чи встановлений для сайту сертифікат. У відповідь сервер надсилає загальну інформацію про SSL-сертифікат та публічний ключ. Браузер звіряє інформацію зі списком авторизованих центрів сертифікації. Такий список є у всіх популярних браузерах. Якщо все гаразд, браузер генерує сеансовий ключ, зашифровує його публічним ключем та відправляє на сервер. Сервер розшифровує повідомлення та зберігає сеансовий ключ. Після цього між браузером та сайтом встановлюється безпечне з'єднання через протокол HTTPS.

Необхідні ресурси:

Будь-який веб-браузер.

Хід виконання роботи:

1. Відкрийте веб-браузер і натиснути значок замка в адресному рядку і у випадаючому меню, в якому фраза «Connection is secure» означає, що перевірка SSL-з’єднання пройшла успішно.
2. Щоб дізнатися точну дату закінчення терміну сертифіката, потрібно натиснути на пункт меню «Certificate (valid)» і в вікні буде

інформація про термін придатності.

3. Виконати п. 1,2 з 5 сайтами на власний вибір. Знайти додатково ще два сайти з протермінованими сертифікатами безпеки. Пункти 1-3 повинні супроводжуватися скріншотами.

4. Описати принципи роботи SSL-шифрування.

5. Запропонувати сертифікати безпеки для: для фізичних осіб, для бізнесу, для сайтів, з великою кількістю субдоменів (один на вибір) та обґрунтувати свій вибір.

Описати методи отримання сертифікатів безпеки. Проаналізувати сучасний ринок центрів сертифікації.

Захист звіту з лабораторної роботи полягає в пред'явленні викладачеві отриманих результатів (на екрані монітора), демонстрації отриманих навичок і відповідях на питання викладача.

Контрольні питання

1. Яка роль SSL-сертифікатів у забезпеченні безпеки з'єднання?

2. Які види SSL-сертифікатів існують та чим вони відрізняються один від одного?

3. Як ви можете визначити, чи є SSL-сертифікат протермінованим? Які наслідки це має для безпеки?

4. Що таке сеансовий ключ і яку роль він відіграє у процесі SSL-шифрування?

5. Які популярні сертифікаційні центри пропонують SSL-сертифікати і які їхні особливості?

6. Які ризики пов'язані з використанням протермінованих SSL-сертифікатів?

Лабораторна робота №3. Робота з кросплатформним проксі-сканером BurpSuite

Мета: Навчитися використовувати проксі-сканер Burp Suite, аналізувати URL-адреси, які сканує проксі, навчитися користуватися інструменом для тестування, моделювання атак, проведення пентестів; вискористовувати спеціальний інструмент декодування/шифрування даних з застосуванням різноманітних алгоритмів в Burp Suite.

Задачі:

1. Ознайомитися з можливостями та інтерфейсом Burp Suite Community Edition.
2. Встановити та налаштувати Burp Suite Community Edition.
3. Провести сканування сайту на власний вибір.
4. Описати отриманий результат сканування сайту в Burp Suite.

Довідкова інформація / сценарій:

BurpSuite – багатофункціональний кросплатформний проксі-сканер. BurpSuite існує у 3-х версіях: Community Edition, Professional Edition та Enterprise Edition.

Перша надається безкоштовно і входить у склад ОС Kali Linux. Дві останні версії – платні, надають розширений функціонал, для них необхідно придбати ліцензію.

BurpSuite Professional можна спробувати також на безкоштовній основі в рамках випробовувального Trial-періоду. Для цього слід написати в технічну підтримку PortSwigger.

Завантажити BurpSuite можна з офіційного сайту. Підтримуються усі платформи: Linux, Windows, MacOS.

Веб-інтерфейс Burp Suite складний та багатозадачний, має розгорнуту систему керування й складається з наступних вкладок:

- Dashboard – головний робочий стіл, аналіз і огляд виконання задач;
- Target – краулер, тут показуються усі URL-адреси, які сканує проксі. Інструмент дає змогу комплексно просканувати увесь сайт – директорії і файли та вибудувати деревовидну структуру. Корисний інструмент для аудиту;

- Proxy – проксі-сканер, сніффер HTTP-трафіка, працює в режимі MITM (man-in-the-middle);
- Intruder – інструмент для тестування, моделювання атак, проведення пентестів;
- Repeater – обробник HTTP-запитів, дозволяє модифікувати HTTP-заголовки і повторно їх відправляти;
- Sequencer – інструмент аналізу токенів;
- Decoder – спеціальний інструмент декодування/шифрування даних з застосуванням різноманітних алгоритмів: ASCII, BASE64, HEX, SHA и т.д.;
- Comparser – інструмент для аналізу та порівняння даних, пошуку відмінностей;
- Extender – робота з плагінами, розширеннями, додатками BurpSuite;
- Project options – налаштування програми на рівні проєкту (цели, задания);
- User options – налаштування користувача, дозволяэ змінити тип з'єднання, кодування, тему інтерфейсу (light/dark), розмір шрифтів, hot keys та таке інше.

Необхідні ресурси:

Burp Suite Community.

Хід виконання роботи:

1. Скачати Burp Suite Community Edition https://portswigger.net/burp/releases/professional-community-2024-8-4
2. Інсталювати Burp Suite Community Edition (рис. 1).

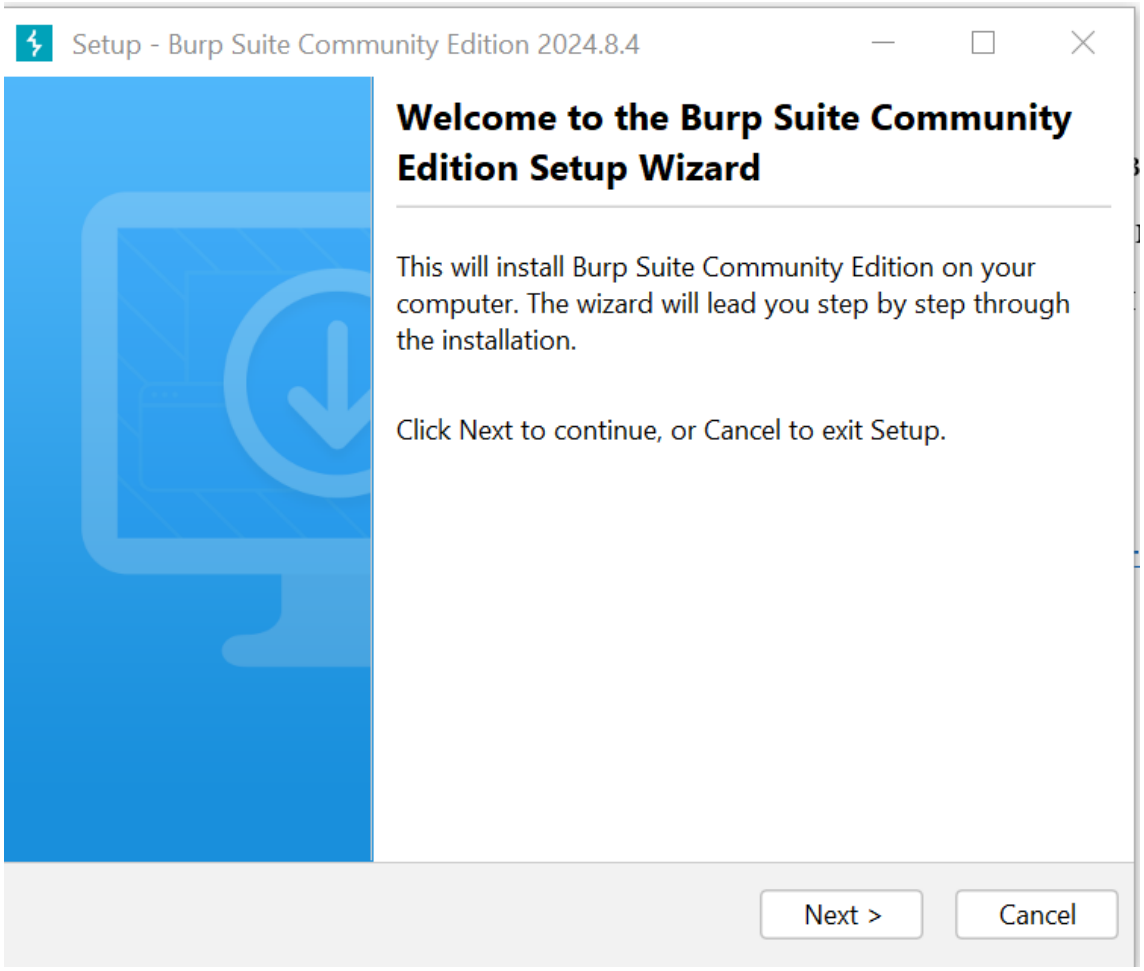

Рис. 1. Процес інсталяції Burp Suite Community Edition

3. Запустити Burp Suite Community (рис. 2):

Рис. 2. Запуск Burp Suite Community

5. Відкриється таке вікно (рис. 3)
6.

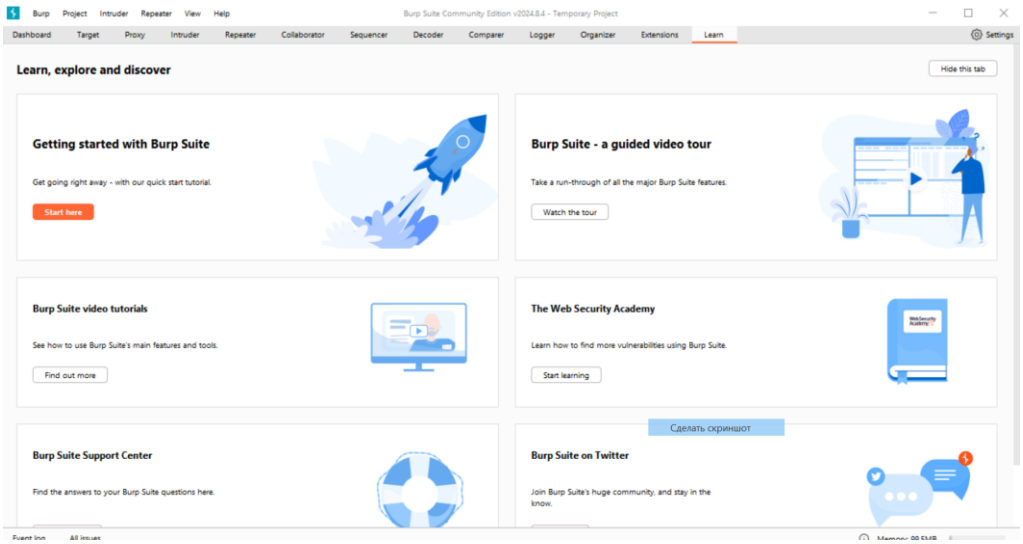

Рис. 3. Головне вікно Burp Suite Community

5. Виконати налаштування:

Щоб BurpSuite почав працювати в ролі проксі-сканера, необхідно його налаштувати.

Найперше слід визначити локальний порт (localhost), на якому працюватие проксі BurpSuite.

Для цього перейти в меню Proxy -> Proxy Settings ->Proxy Listeners й виставити відповідний номер порту. Режим роботи—Loopback.

Перейдемо в загальні налаштування й проведемо ряд інших опцій:

- Proxy Interception—увімкнути режим «Always disable».
- Perfomance Feedback—вимикаємо відправку статистичних і технічних даних на сервери BurpSuite.
- Updates—вимикаємо автоматичне оновлення.
- SOCKS Proxy—переводимо за необхідності роботу BurpSuite через проксі-сервер.

Burpsuite має вбудований Chromium-браузер (Target -> Open browser), через який можна проводити тестування з допомогою проксі-сканера.

Тепер потрібно трохи підкрутити налаштування браузера. У меню вибираємо "Налаштування", потім "Параметри мережі" і тиснемо "Налаштувати". Ставимо галку на пункт "Ручне налаштування сервісу проксі". І там де HTTP проксі вписуємо 127.0.0.1, а порт вписуємо 8080. Коротше переписуємо все те, що було в Burp Suite. Потім відзначаємо

також використання цього проксі для FTP і HTTPS. Якщо в полі «Не використовувати проксі для:» написано щось, потрібно це від туди видалити.

Залишився один невеликий нюанс, при заході на сайти, які використовують SSL сертифікат (тобто майже на все), браузер буде лаятися на сертифікат. Це тому, що Burp Suite генерує свій сертифікат і сам його підписує. Тому, щоб браузер не сварився, потрібно сертифікат Burp додати до браузера як довірений.

Для цього, із запущеним Burp Suite, переходимо у браузері за адресою http://burp. І тиснемо CA Certificate та зберігаємо сертифікат. Тепер у бразузері відкриваємо меню і переходимо в «Налаштування», вибираємо вкладку «Приватність та захист», а в ній «Сертифікати» та тиснемо «Перегляд сертифікатів».

Сам сертифікат має такий вигляд (рис. 4):

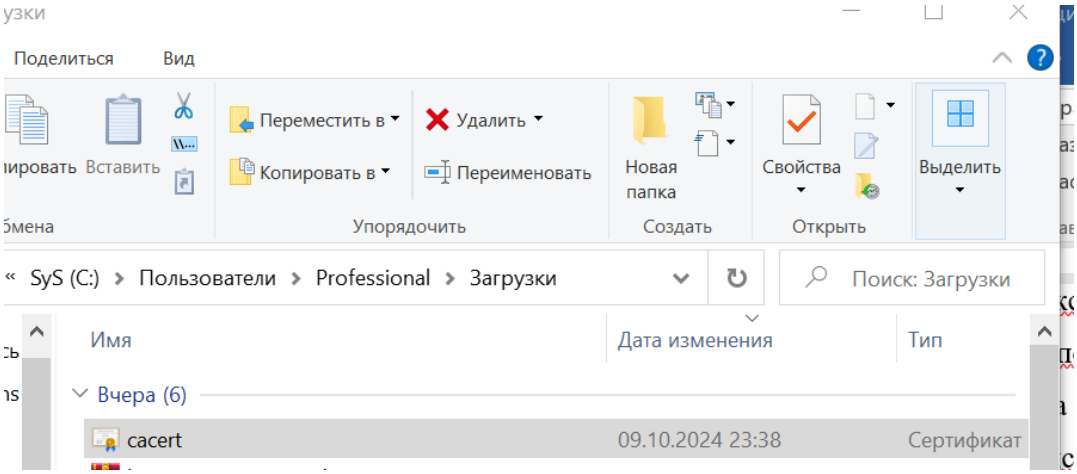

Рис. 4. Сертифікат Burp Suite

Там вибираємо «Центри сертифікації», тиснемо «Імпортувати» та вибираємо завантажений нами сертифікат. Ставимо галку "Довіряти при ідентифікації веб-сайтів" і тиснемо "ОК". Все готове, можна працювати.

Тепер будь-який запит від нас або до нас спочатку проходитиме через Burp Suite, а значить ми можемо переглянути цей запит і, якщо потрібно, трохи його підредагувати.

Перевірити роботу проксі BurpSuite дуже просто. Відкриваємо у браузері будь-який сайт і йдемо у BurpSuite в меню Target -> Site map— там з’явиться структура каталогів сайту. Ми побачимо кожне з’єднання, яке пройшло через проксі при завантаженні сайту, включаючи навіть з’єднання самого браузера, його плагінів і так далі.

Наприклад, відкриваємо сайт нашого університету і бачимо наступну інформацію в BurpSuite (рис. 5):

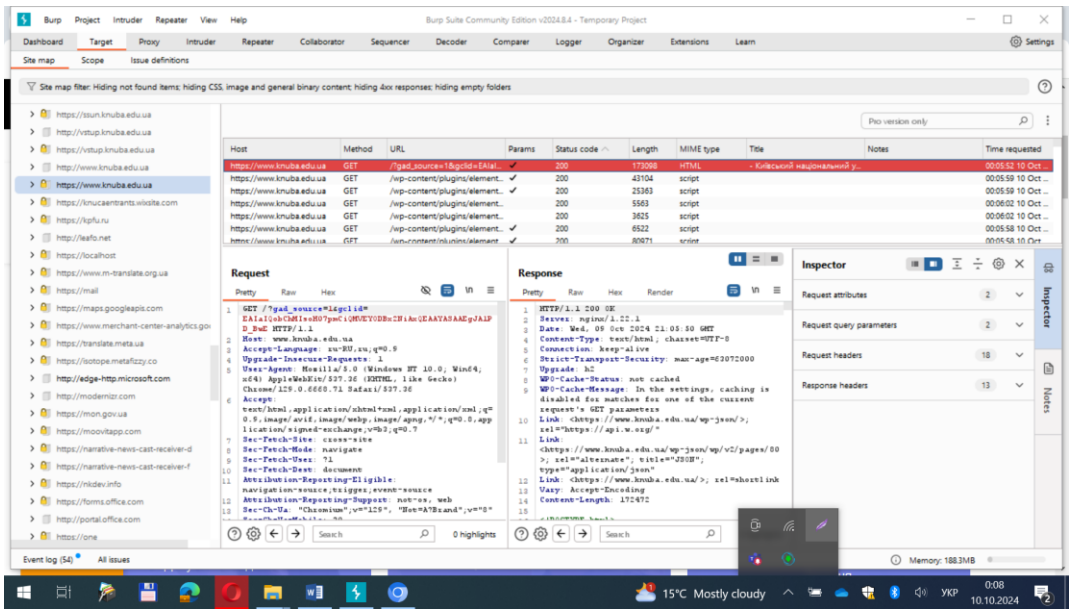

Рис. 5. Структура каталогів сайту

6. Провести сканування будь-якого сайту на власний вибір та проаналізувати отриманий результат (із скріншотами) та написати висновок.

Захист звіту з лабораторної роботи полягає в пред'явленні викладачеві отриманих результатів (на екрані монітора), демонстрації отриманих навичок і відповідях на питання викладача.

Контрольні питання

1. Які основні функції виконує Burp Suite і для чого він використовується у тестуванні веб-додатків?
2. Яка різниця між вкладками Target і Proxy в інтерфейсі Burp Suite? Для чого вони використовуються?
3. Як працює інструмент Intruder у Burp Suite і для чого його використовують?
4. Що таке Repeater в Burp Suite і які можливості він надає?
5. Як можна декодувати або зашифрувати дані за допомогою Decoder в Burp Suite? Які алгоритми підтримуються?
6. Які потенційні загрози можна виявити за допомогою проксі-сканера Burp Suite?
7. Які заголовки запитів і відповідей найчастіше аналізуються під час пентесту веб-додатків?
8. Яка інформація з'являється на вкладці Site map після сканування веб-сайту? Що це означає для аудитора безпеки?

Лабораторна робота № 4. Робота з графічним інструментом аналізу мережі Wireshark

Мета Навчитися використовувати графічний інструмент аналізу мережі Wireshark, аналізувати пакети даних, що передаються по комп'ютерній мережі, розглянути мережеві протоколи, виявити проблем у мережі.

Задачі:

1. Ознайомитися з можливостями та інтерфейсом Wireshark.
2. Встановити Wireshark та драйвер захоплення пакетів Npcap.
3. Провести захоплення мережевого трафіку, використати фільтрацію, додавання додаткових стовпців.
4. Описати отримані результати захоплення трафіку.

Довідкова інформація / сценарій:

Аналіз та моніторинг мереж – важлива складова сфери інформаційної безпеки та ефективної роботи комп'ютерних мереж. Wireshark – це графічний інструмент аналізу мережі, який дозволяє візуалізувати та фільтрувати пакети даних. Він забезпечує зручний інтерфейс для перегляду мережевого трафіку у реальному часі та в режимі аналізу пакетів. Його можливості дозволяють виявити проблеми, такі як перевантаження мережі, аномалії у спілкуванні між пристроями, атаки та інші аномалії.

Також, Wireshark є потужним інструментом для відлагодження мережевих додатків та служб. Інженери мереж можуть використовувати його для визначення причин низької продуктивності мережі та забезпечення її оптимізації. tcpdump, з іншого боку, є консольним інструментом для перехоплення та аналізу пакетів даних. Він забезпечує можливість моніторити мережевий трафік у реальному часі, а також записувати його для подальшого аналізу. tcpdump особливо корисний для адміністраторів мереж, які працюють у середовищах командного рядка і вимагають точного контролю над процесом аналізу мережі.

Необхідні ресурси:

Безкоштовний і відкритий аналізатор мережевого трафіку Wireshark, драйвер захоплення пакетів Npcap.

Хід виконання роботи:

1. Скачати Wireshark https://www.wireshark.org
2. Інсталювати Wireshark (рис. 6).

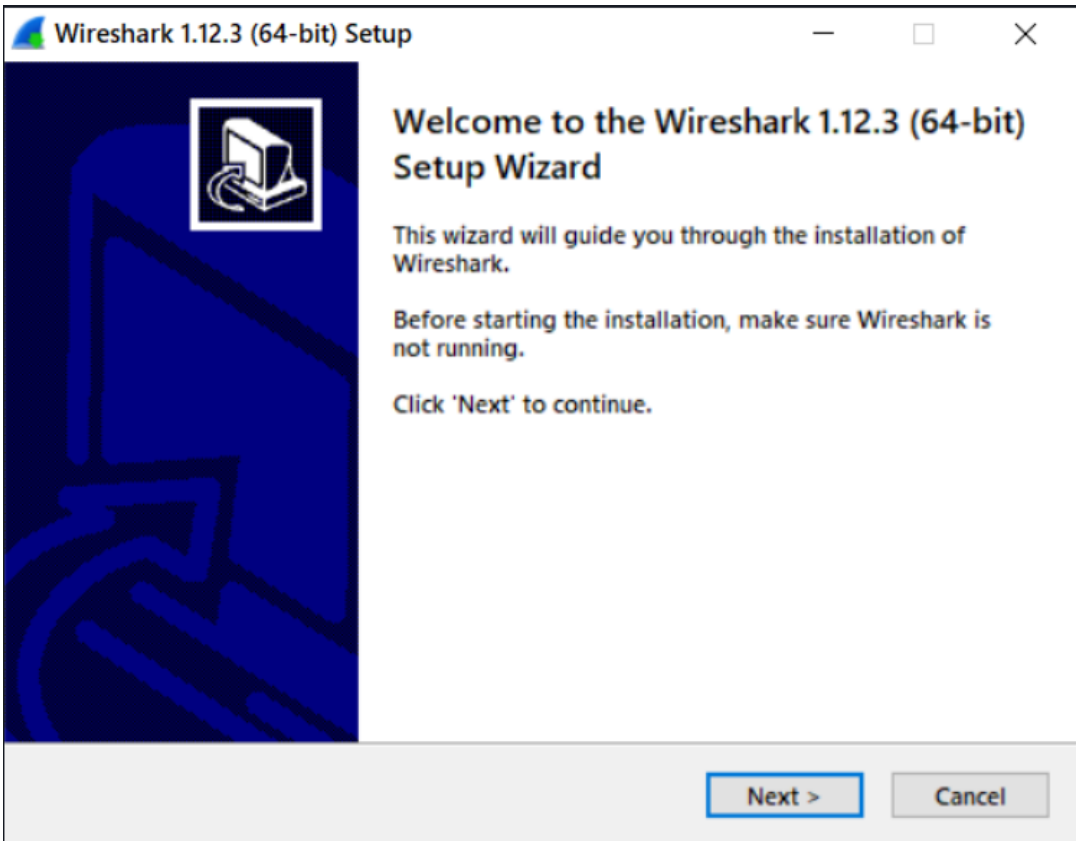

Рис. 6. Процес інсталювання Wireshark

Після успішного встановлення на Вашому робочому столі з’явиться ярлик Wireshark (рис. 7).

Рис. 7. Ярлик інструменту для аналізу мережевого трафіку Wireshark

4. Відкриється таке вікно (рис 8.)

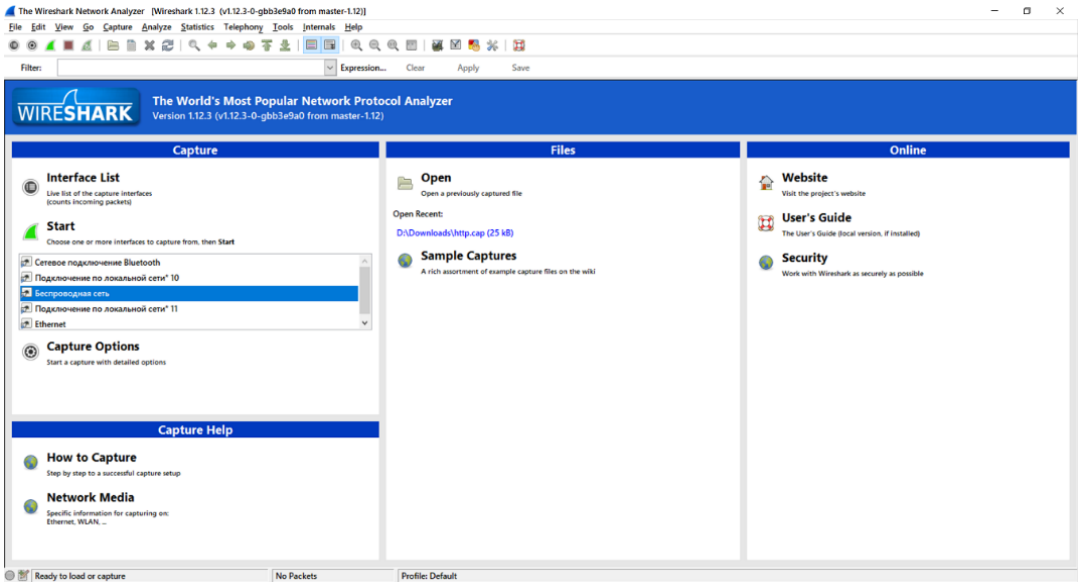

Рис. 8. Головне вікно Wireshark

5. Додатково знадобиться встановлення драйвер захоплення пакетів Npcap, встановити його можна за посиланням: https://npcap.com, там обираємо Npcap 1.80 installer for Windows 7/2008R2, 8/2012, 8.1/2012R2, 10/2016, 2019, 11 (x86, x64, and ARM64). Встановлюємо (рис.9)

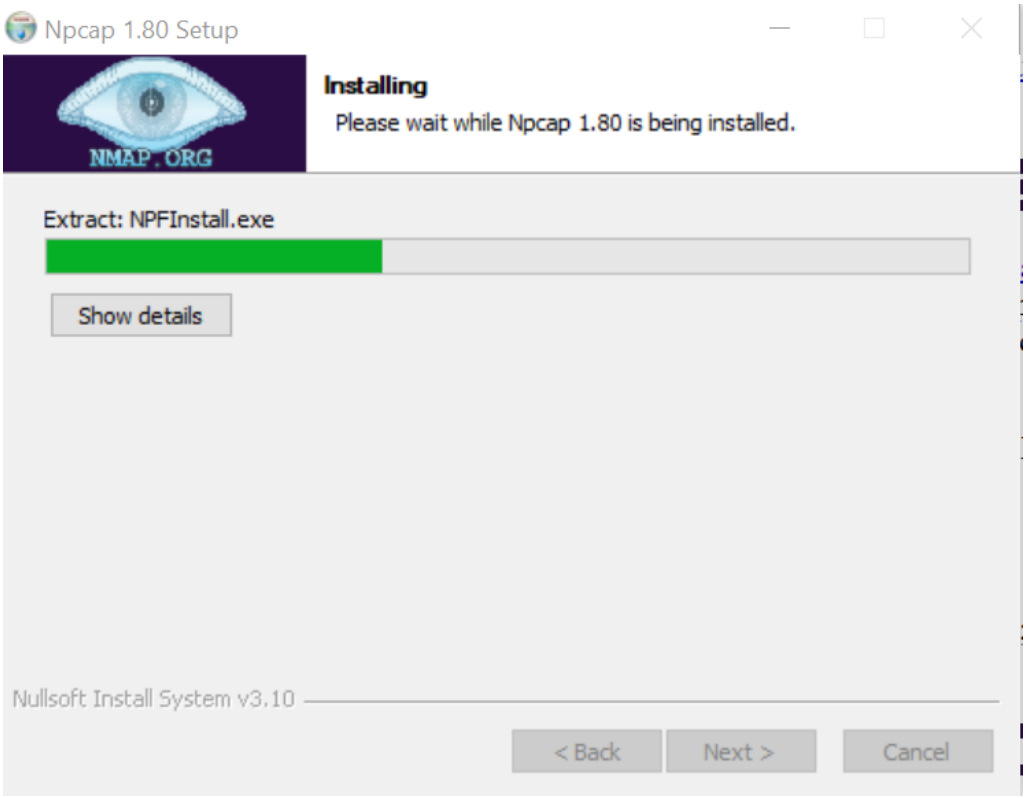

Рис. 9. Інсталяція драйвер захоплення пакетів Npcap

6. Обираємо мережу, наприклад «Безпровідна мережа» і натискаємо «Плавник акули» - кнопку захоплення.

Якщо все виконано вірно, то почнеться захоплення трафіку (рис. 10):

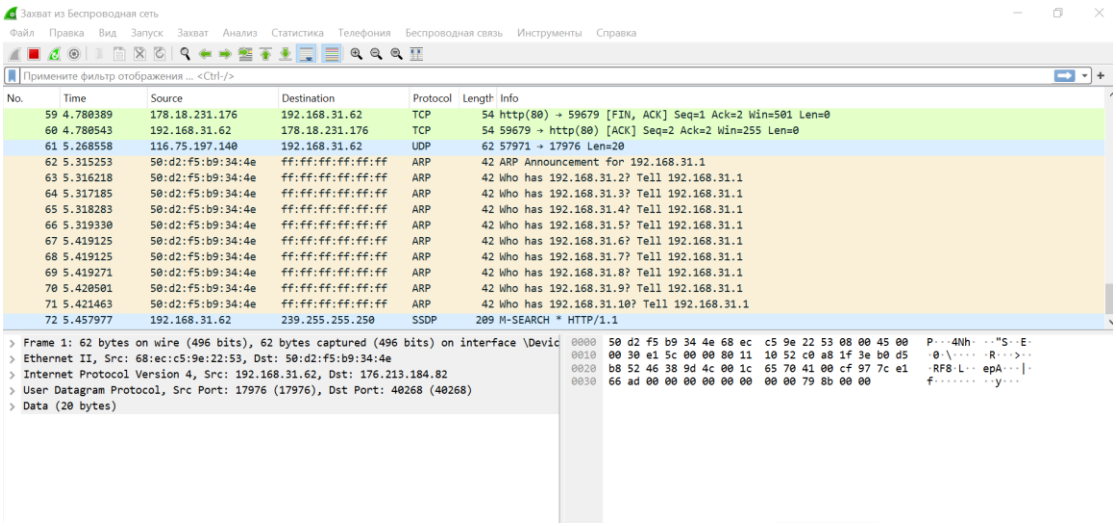

Рис. 10. Захоплення трафіку в Wireshark

Розглянемо докладніше це вікно за пунктами, вказаними на ньому:

1. Панель фільтрів дозволяє знайти необхідну інформацію.

2. Панель найменувань, що поділяє інформацію з пункту 3 на номер, час від початку захоплення трафіку, джерело та адресат, а також протокол, розмір пакета і невелику інформацію про мережевий пакет.

3. Панель пакетів оновлюється в реальному часі. Тут інформація про пакети розділена на стовпці, визначені на панелі найменувань.

4. Панель рівнів, що описує рівні моделі OSI вибраного мережного пакета.

5. Панель метаданих, що представляє дані у шістнадцятковому коді та символах.

7. Додати стовбець відображення потужності сигналу каналу в момент перехоплення пакету.

Для цього потрібно додати ще один рядок: Правка- Параметри- Зовнішній вигляд-Стовпці-кнопка + (рис. 11):

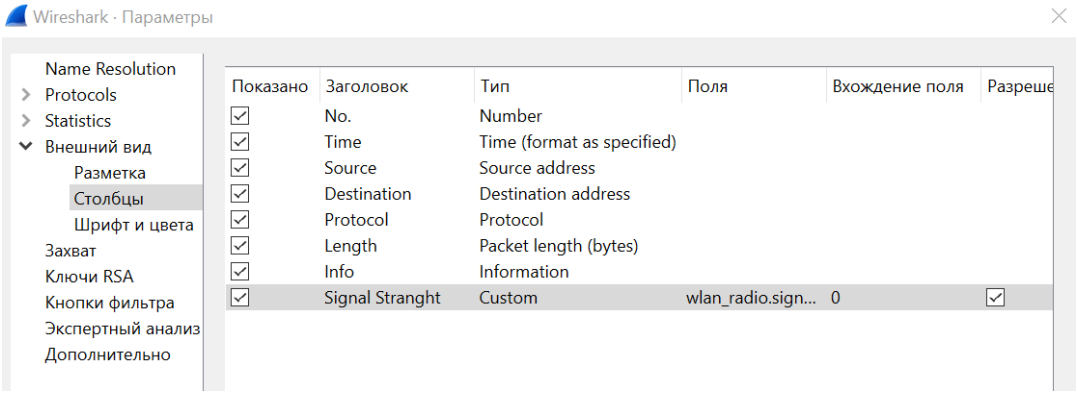

Рис. 11. Додавання стовбця відображення потужності сигналу каналу в момент перехоплення пакету

8. Відфільтрувати трафік мережі IP-адресою одержувача пакетів за допомогою команди «ip.dst == xxxx».

9. Відфільтрувати за IP-адресою, переглянувши всі пакети, що надходять від кого-небудь або ті, що йдуть будь-кому. Наприклад, відберемо всі пакети, що надходять від IP-адреси за допомогою введення у фільтрі «ip.src == xxxx».

9. Проаналізувати отримані дані(ієрархія протоколів, кінцеві точки, довжини пакетів, графіки вводу, виводу, графік потоку) та написати висновок.

Захист звіту з лабораторної роботи полягає в пред'явленні викладачеві отриманих результатів (на екрані монітора), демонстрації отриманих навичок і відповідях на питання викладача.

Контрольні запитання

1. Що таке Npcap, і яку функцію він виконує при роботі з Wireshark?

2. Як налаштувати фільтри в Wireshark для відображення тільки потрібних пакетів? Наведіть приклад фільтра для IP-адреси.

3. Яка роль панелі фільтрів у Wireshark? Як вона допомагає в аналізі мережевого трафіку?

4. Яка різниця між вихідними та вхідними пакетами у Wireshark і як їх можна відфільтрувати?

5. Що таке ієрархія протоколів у Wireshark, і як вона відображає інформацію про мережеві пакети?

6. Які рівні моделі OSI можна побачити при аналізі мережевого пакета у Wireshark?

7. Як у Wireshark відобразити потужність сигналу каналу в момент захоплення пакета? Які кроки потрібно виконати для додавання цього стовпця?

8. Як аналізувати кінцеві точки та тривалість сесій у Wireshark для визначення проблем в мережі?

Лабораторна робота №5. Проведення сканування із використанням графічного інтерфейсу Nmap

Мета:

Навчитися сканувати порти, використовуючи графічний інтерфейс Nmap, за допомогою якого можна виконувати різні типи аналізу мережі.

Задачі:

1. Інсталювати Nmap.
2. Вивчити методи сканування nmap та їх призначення.
3. Провести модифіковане сканування за допомогою команд.
4. Проаналізувати отримані результати (результати сканування портів, стан портів, протоколи, служби, версії, способи графічного перегляду хостів, які просканові, кількість відкритих, закритих, просканованих портів, IP-адреси).

Довідкова інформація / сценарій:

Nmap – один із найчастіше використовуваних інструментів і особливо відомий у Linux, який служить для відстеження портів. Це використовується для оцінки безпеки комп'ютерних систем, а також для виявлення служб або серверів у комп'ютерній мережі. Для цього Nmap надсилає певні пакети іншим комп'ютерам та аналізує їх відповіді.

Zenmap – це офіційний графічний інтерфейс Nmap, за допомогою якого можна виконувати різні типи аналізу, що нам дозволено робити з Nmap.

Методи сканування nmap:

- TCP/IP – дактилоскопія (ідентифікація ОС або пристрою віддаленого хоста) з використанням відбитків стека TCP/IP.
- Nmap використовує безліч різних методів сканування, таких як UDP, TCP (connect), TCP SYN (напіввідкрите), FTP proxy (прорив через ftp), Reverse-ident, ICMP (ping), FIN, ACK, Xmas tree, SYN та NULL-сканування. Nmap також підтримує великий набір додаткових можливостей, а саме: «невидиме» сканування, динамічне обчислення часу затримки та повтор передачі пакетів, паралельне сканування, визначення неактивних хостів методом паралельного ping-опитування, сканування з використанням хибних хостів, визначення наявності пакетних фільтрів,

пряме (без використання portmapper) RPC-сканування, IP-фрагментації, а також довільна вказівка IP-адрес та номерів портів сканованих мереж.

- Вона підтримує ping-сканування (визначає чи хост включений), різні техніки сканування портів, визначення версій (службових протоколів і служб закріплених за портами) і . Nmap також надає характеристики цільового об'єкта і порту, що настроюються, помилкове/приховане сканування, sunRPC-сканування та інше.

Необхідні ресурси:

Інструмент мережевого сканування з відкритим вихідним кодом Nmap.

Хід виконання роботи:

1. Завантажте Nmap за посиланням: https://nmap.org/download
2. Встановіть Nmap (рис. 12):

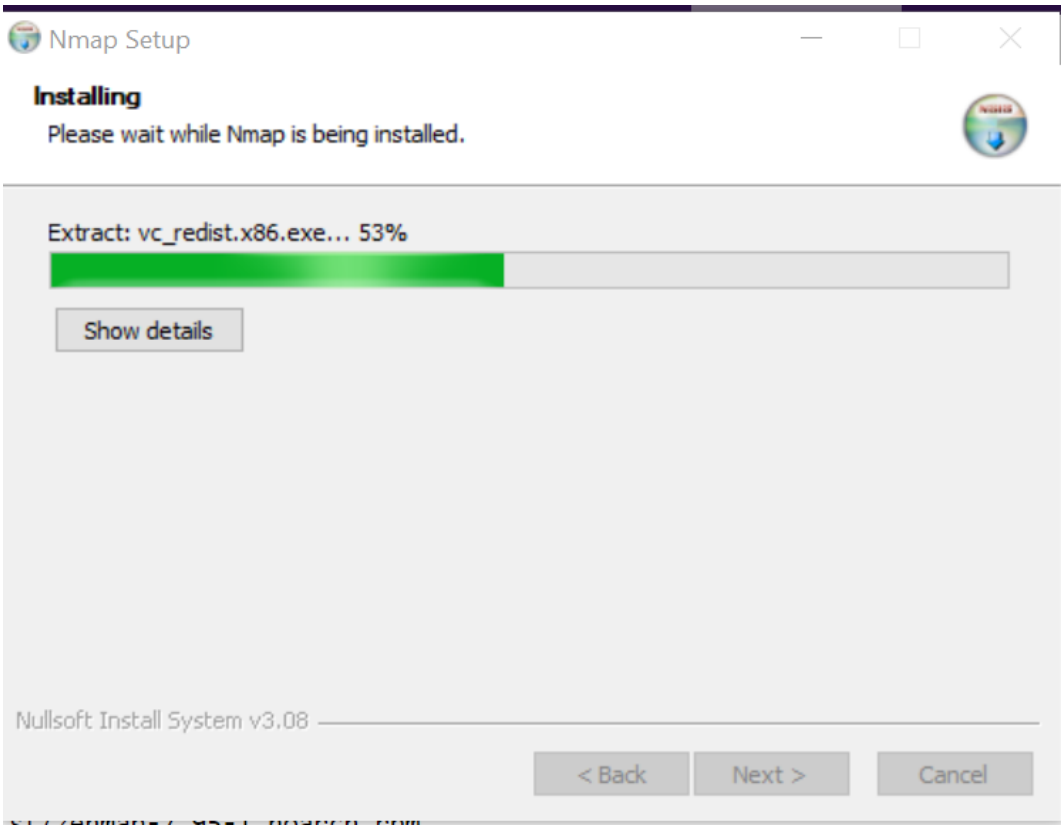

Рис. 12. Інсталювання інструменту для відстеження портів Nmap

3. Після інсталяції і запуску Nmap GUI Ви побачити наступне вікно (Рис.13):

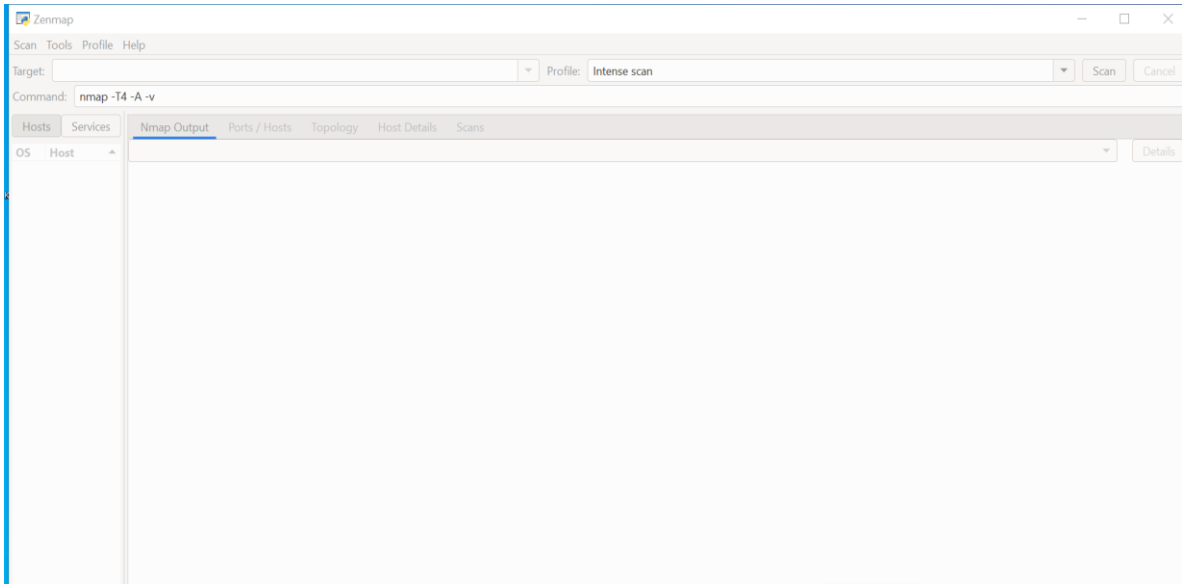

Рис. 13. Головне вікно Nmap

4. У Target ввести команду сканування домену nmap scanme.nmap.org та натиснувати кнопку Scan (рис. 14):

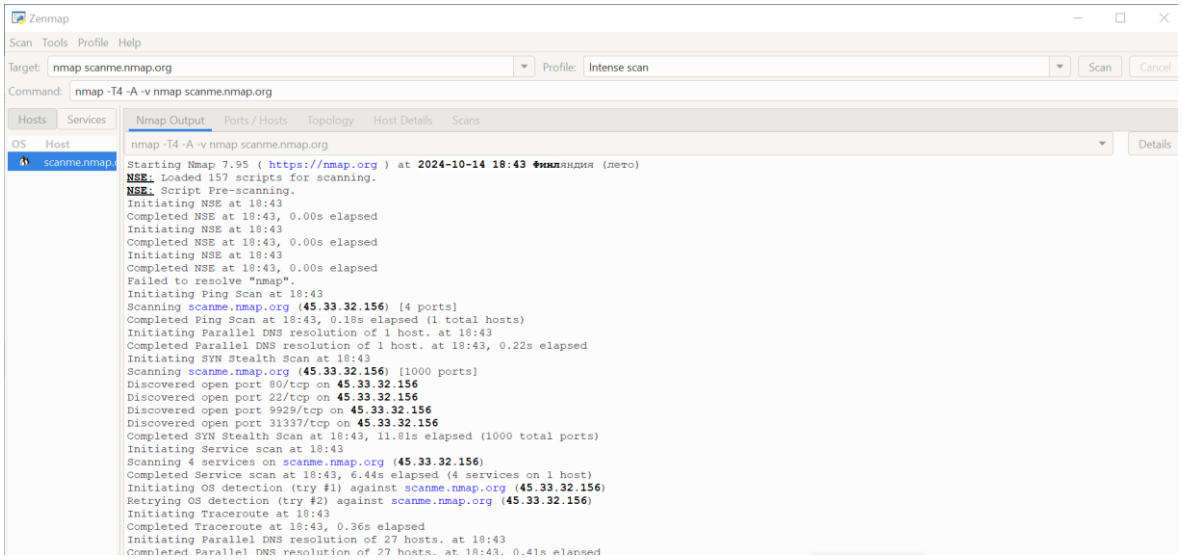

Рис. 14. Результат виконання команди nmap scanme.nmap.org

5. Проаналізувати отримані результати, розглянувши вкладки Nmap Output – вивід результатів сканування портів, включаючи служби, які працюють на них (Рис. 15):

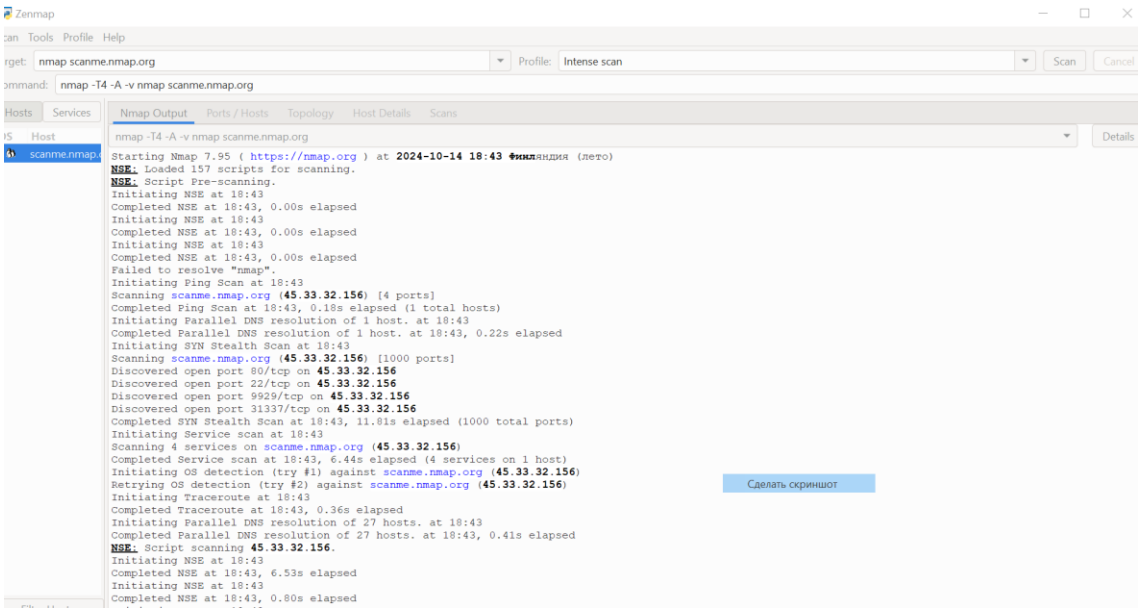

Рис. 15. Вкладка Nmap Output

Potrs/Hosts (проаналізувати стан портів, протоколи, служби, версії) (рис. 16):

Рис. 16. Вкладка Potrs/Hosts

Topology (різні способи графічного перегляду хостів, які просканові, тобто показує трасування для виконаного сканування) показана на рис. 17:

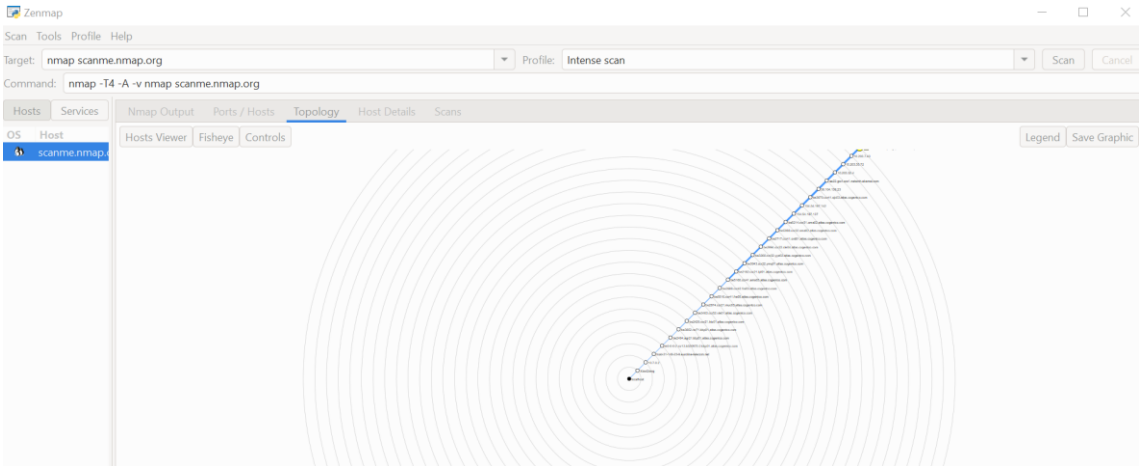

Рис. 17. Вкладка Topology

Host Details (деталі хосту). Тут потрібно проаналізувати кількість відкритих, закритих, просканованих портів, IP-адресу, порти, які використовуються і т.д.(рис. 18):

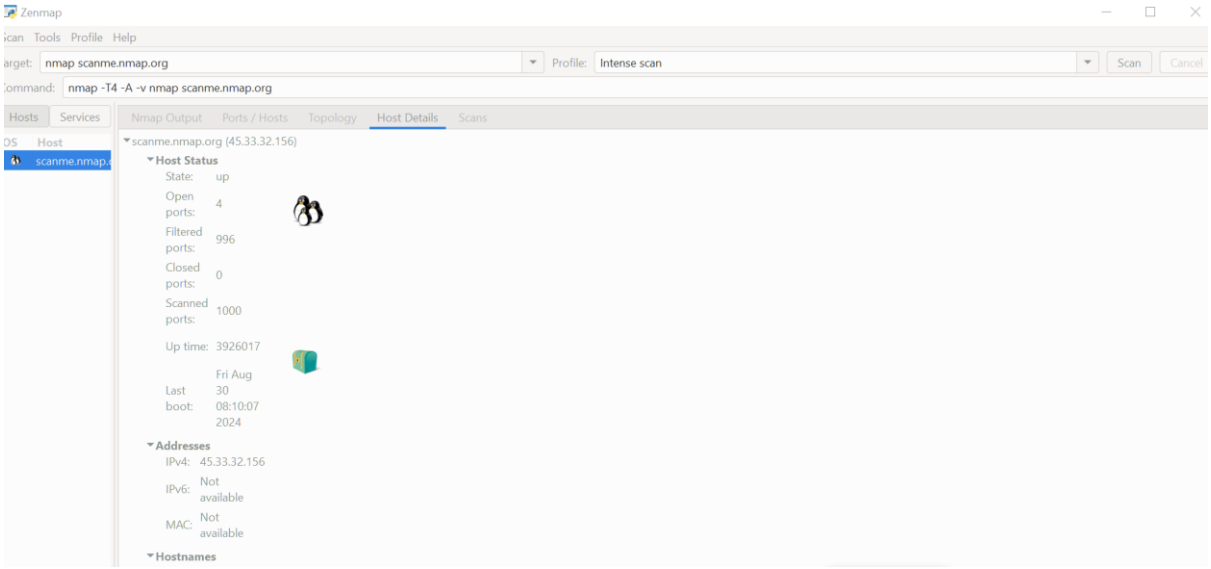

Рис. 18. Вкладка Host Details

Scans (список сканувань, які вже використовувалися).

6. Проведіть модифіковане сканування. Ви можете використовувати командні змінні, щоб змінити параметри сканування, в результаті одержуючи більш-менш широке сканування. Ви можете додати кілька змінних залишаючи пробіл між кожним. Змінні ставляться до мети: nmap <variable> <variable> <target>:

-sS – це приховане сканування SYN. Це сканування складніше знайти, ніж звичайне, але може зайняти довше часу для завершення. Більшість нових фаєрволів можуть виявити сканування -sS.

-sn – це сканування пінгу. Це сканування не використовує виявлення портів і лише перевіряє онлайн статус мети.

-O – це сканування визначає вид операційної системи.

-F - включає швидке сканування, і зменшує кількість портів, що скануються.

-v - ця змінна показує більше результатів вашого сканування, роблячи їх читабельними.

7. Написати висновок щодо проведеного сканування.

Захист звіту з лабораторної роботи полягає в пред'явленні викладачеві отриманих результатів (на екрані монітора), демонстрації отриманих навичок і відповідях на питання викладача.

Контрольні питання

1. Що таке Nmap, і для чого його використовують у мережевому аналізі?
2. Які параметри вказують стан порту в Nmap (open, closed, filtered)?
3. Як за допомогою Nmap визначити, яка операційна система використовується на віддаленому хості? Яка команда для цього використовується?
4. Як відфільтрувати тільки порти, що знаходяться у відкритому стані, і які протоколи вони використовують?
5. Що таке "графічний перегляд топології" у Zenmap, і як він допомагає в аналізі результатів сканування?
6. Яка інформація доступна у вкладці Host Details, і як вона допомагає аналізувати результати сканування?

ІНДИВІДУАЛЬНА РОБОТА

Забезпечення безпеки інтернет-ресурсів: аналіз загроз та методи захисту

Мета:

Метою індивідуальної роботи є дослідження питань забезпечення безпеки веб-ресурсів в умовах зростання кількості кібератак та вразливостей. Робота спрямована на аналіз основних методів захисту інтернет-ресурсів, виявлення типових вразливостей веб-додатків, а також розробку практичних рекомендацій щодо підвищення рівня безпеки веб-додатків.

Задачі:

1. Проаналізувати актуальності питання безпеки інтернет-ресурсів.
2. Дослідити основні загрози веб-додатків та прокласифікувати вразливості.
3. Проаналізувати методи та засоби забезпечення безпеки веб-додатків.
4. Провести практичне сканування конкретного веб-ресурсу для виявлення вразливостей.
5. Розробити конкретні рекомендації щодо посилення безпеки веб-ресурсу, виходячи з результатів сканування в п.4.
6. Підготувати висновки щодо ефективності досліджених методів захисту та запропонувати напрямки для подальших досліджень.

Структура індивідуальної роботи повинна містити наступні пункти:

Вступ

1. Актуальність теми - коротке пояснення важливості питання безпеки інтернет-ресурсів, зростання кількості кібератак та необхідності посилення захисту веб-додатків.
2. Мета і завдання роботи - формулювання основної мети дослідження та завдань, які необхідно вирішити в рамках роботи.
3. Об'єкт і предмет дослідження - визначення конкретного аспекту безпеки інтернет-ресурсів, на який спрямоване дослідження.
4. Методи дослідження - опис методів, які будуть використовуватися для аналізу та вирішення завдань, наприклад, методи моделювання атак, аналіз загроз, аудит безпеки.

1. Основи безпеки інтернет-ресурсів

1.1. Поняття безпеки веб-ресурсів: загальне визначення безпеки інтернет-ресурсів, основні компоненти захисту інформації (конфіденційність, цілісність, доступність).

1.2. Основні загрози інтернет-ресурсам: розгляд основних типів загроз, таких як SQL-ін'єкції, CSRF, XSS, DDoS-атаки, фішинг, атаки на аутентифікацію.

1.3. Класифікація вразливостей веб-додатків: огляд основних вразливостей, зокрема на основі OWASP Top 10, пояснення їхньої природи та наслідків.

2. Методи та засоби забезпечення безпеки інтернет-ресурсів

2.1. Методи захисту веб-додатків - опис ключових методів захисту: валідація введення даних, використання SSL/TLS, захист від CSRF та XSS, контроль доступу.

2.2. Засоби моніторингу та виявлення загроз: використання систем виявлення та попередження атак (IDS/IPS), логування та аналіз трафіку, хмарні рішення для забезпечення безпеки.

3. Аналіз вразливостей та практичні рекомендації з безпеки

3.1. Огляд популярних систем управління вмістом (CMS) та їх вразливостей. Аналіз популярних CMS з точки зору безпеки, типові вразливості та способи їх нейтралізації.

3.2. Огляд інструментів для тестування безпеки веб-ресурсів. Опис інструментів для пентестингу та аудиту безпеки, таких як Burp Suite, Acunetix *(один на вибір, можна інший інструмент за бажанням (наприклад, який вивчали на лабораторних роботах))*.

3.3. Практичні рекомендації щодо посилення безпеки інтернет-ресурсів. Конкретні заходи для покращення безпеки веб-додатків, такі як оновлення ПЗ, застосування політики безпечного кодування, регулярне тестування на вразливості.

4. Практична реалізація

4.2. Сканування на практичних прикладах: реалізація різних методів сканування на прикладі конкретного веб-ресурсу.

4.3. Попередження та протидія атакам: опис методів раннього виявлення атак та заходів реагування для мінімізації збитків.

Висновки

1. Підсумки дослідження: загальні висновки щодо ефективності методів забезпечення безпеки інтернет-ресурсів, викладені у роботі.
2. Пропозиції для подальших досліджень: перспективи розвитку у сфері захисту веб-додатків, необхідні подальші кроки для посилення безпеки інтернет-ресурсів.

Список використаних джерел

Перелік літературних джерел, нормативних документів та інструментів, які були використані під час написання індивідуальної роботи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Список інструментів для тестування і злому проникнення. Ресурси для тестування на проникнення. Електронний ресурс – Режим доступу: https://hackyourmom.com/kibervijna/povnyj-spysok-instrumentiv-dlya-testuvannya-i-zlomu-pronyknennya-dlya-hakeriv-i-fahivcziv-z-bezpeky/

2. Авраменко А.С., Авраменко В.С., Косенюк Г.В. Тестування програмного забезпечення. Навчальний посібник. Черкаси: ЧНУ імені Богдана Хмельницького, 2017. 284 с.

3. Говорущенко Т.О. Методологія оцінювання достатності інформації для визначення якості програмного забезпечення : монографія / Говорущенко Т. О. Хмельницький : ХНУ, 2017. 310 с.

4. Andrew Hoffman. Web Application Security Exploitation and Countermeasures for Modern Web Applications Електронний ресурс – Режим доступу:https://soclibrary.futa.edu.ng/books/Web%20Application%20Security%20(1).pdf

5. Інформаційна безпека : підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська, В. М. Петрик, Нац. акад. Служби безпеки України; Під ред. В. В. Остроухов; Наук. конс. М. П. Стрельбицький, Н. Г. Іванова. – Київ : Ліра-К, 2021.

6. Nmap Cheat Sheet 2024: All the Commands & Flags Електронний ресурс – Режим доступу: https://www.stationx.net/nmap-cheat-sheet/

Навчально-методичне видання

БЕЗПЕКА ІНТЕРНЕТ-РЕСУРСІВ

Методичні вказівки
до виконання лабораторних робіт та індивідуального завдання
для здобувачів другого (магістерського) рівня вищої освіти
за спеціальністю 125 "Кібербезпека та захист інформації"

Укладач **ШАБАЛА** Євгенія Євгенівна

Комп’ютерне верстання *А. П. Селівестрової*

Ум. друк. арк. 1,86. Обл.-вид. арк. 2,0
Електронний документ. Вид № 63/V-24.

Виконавець і виготовлювач
Київський національний університет будівництва і архітектури

Проспект Повітряних Сил, 31, Київ, Україна, 03037
Свідоцтво про внесення до Державного реєстру суб’єктів

видавничої справи ДК № 808 від 13.02.2002 р