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

Інформаційна безпека держави

Методичні вказівки до виконання лабораторних робіт
для студентів денної форми навчання за спеціальністю 125 "Кібербезпека"

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки та
програмного забезпечення, протокол № 1
від 05.07.2017

Кропивницький
2017

Інформаційна безпека держави: методичні вказівки до виконання лабораторних робіт для студентів за спеціальністю 125 “Кібербезпека” / М-во освіти і науки України, Центральноукр. нац. техн. ун-т; / уклад. О.А. Смірнов, О.К. Конопліцька-Слободенюк, В.Д. Хох, С.А. Смірнов/ – Кропивницький: ЦНТУ – 2017. – 90 с.

Укладачі: Смірнов О. А., докт. техн. наук, професор;
Конопліцька-Слободенюк О. К., викладач;
Хох В.Д., аспірант;
Смірнов С.А., канд. техн. наук, ст. викладач.

Рецензенти: Сидоренко В. В., докт. техн. наук, професор;
Доренський О. П., канд. техн. наук.

ЗМІСТ

ВСТУП

Мета: Основною метою є теоретична та практична підготовка студентів щодо вивчення теоретичних підвалин теорії інформаційної безпеки держави та їх практичних застосувань.

Завдання:

– вивчення основних понять теорії інформаційної безпеки держави;

– визначення загроз безпеці інформації та виявлення порушників інформаційної безпеки держави;

– визначення рівнів інформаційної безпеки держави;

– визначення механізмів, алгоритмів та засобів забезпечення інформаційної безпеки держави;

– набуття практичних навичок з аудиту інформаційної безпеки та пошуку й визначення вразливостей системи або мережі за допомогою спеціалізованого програмного забезпечення.

У результаті вивчення навчальної дисципліни студент повинен:

– *знати:* Поняття інформаційної безпеки. Заходи що до побудови концептуальної моделі інформаційної безпеки. Загрози безпеці інформації. Порушники інформаційної безпеки. Правовий рівень інформаційної безпеки. Організаційний та процедурний рівень інформаційної безпеки. Керування ризиками. Програмно-технічний захист інформації. Криптографічні засоби захисту інформації. Стеганографічні засоби захисту інформації. Ідентифікація, автентифікація та керування доступом. Основи безпеки інформаційно-комунікаційних систем. Захист персональних даних. Основи управління інформаційною безпекою.

– *вміти*: Розгортати операційну систему для проведення аудиту інформаційної безпеки комп’ютерних мереж та систем. Інструменти прихованого збору технічної інформації з комп’ютерної системи або мережі. Дослідження вразливостей системи або мережі за допомогою спеціалізованого

сканера вразливостей – Nessus. Визначення вразливостей веб ресурсів та веб додатків. Сканер вразливостей – Vega. Пошук вразливостей та чуттєвої інформації у відкритих ресурсах за допомогою засобу Maltego. Сніфери. Засіб дослідження вразливостей безпровідних мереж Wi-Fi – Aircrack-ng.

Структурно логічна схема підготовки бакалавра.

Враховуючи послідовність накопичення знань та інформації, дисципліна вивчається після викладання наступних дисциплін:

– Вища математика.

– Теорія ймовірності та математична статистика.

– Структурне програмування.

– Модульне програмування.

– Об'єктно-орієнтоване програмування.

– Технології програмування.

Для опанування матеріалу дисципліни «Інформаційна безпека держави» окрім лекційних та лабораторних занять, тобто аудиторного навантаження, значна увага приділяється самостійній роботі.

До основних видів самостійної роботи студента відносимо:

1. Вивчення лекційного матеріалу.

2. Робота з літературними джерелами.

3. Розв’язання практичних задач за індивідуальними варіантами.

4. Підготовка до модульних, підсумкового контролю, екзамену (денна та заочна).

5. Виконання курсової роботи для денної форми навчання.

Методи навчання

Провідна форма навчання – лекція. Лекція дозволяє дуже економно, з мінімальними затратами часу і викладача, і студентів, надати великий обсяг інформації по темі, що розглядається. За характером логіки пізнання впроваджуються аналітичний, індуктивний та дедуктивний методи.

Супровідні методи – лабораторні роботи.

Основна дидактична мета практичного заняття – закріплення й деталізація знань, а головне – формування навичок і вмінь. Для проведення практичного заняття викладач готує відповідні методичні матеріали: тести для виявлення рівня оволодіння необхідними теоретичними положеннями; набір практичних завдань різної складності для розв'язування їх на занятті та дидактичні засоби.

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 ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
		для екзамену
90 – 100	**A**	відмінно
82-89	**B**	добре
74-81	**C**	
64-73	**D**	задовільно
60-63	**E**	
35-59	**FX**	незадовільно з можливістю повторного складання
0-34	**F**	незадовільно з обов’язковим повторним вивченням дисципліни

Вибравши предметну область, над якою ви будете працювати, ви повинні виконати завдання до лабораторних робіт, а також відповісти на питання в кінці кожної лабораторної роботи. Звіт повинен містити хід виконання завдань а також графічні матеріали, що підтверджують виконання цих завдань.

Лабораторна робота №1

Тема: **Розгортання операційної системи для проведення аудиту інформаційної безпеки 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. Зазвичай цих знань вистачає для організації роботи такої системи, коли справа доходить до перевірки захищеності системи, так би мовити, в польових умовах, цих знань не вистачить. Для цього 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 найбільше поширення отримує дистрибутив Kali Linux що розробляється компанією Offensive Security (до того першість займав дистрибутив – Back Track, що також розроблявся цією компанією. Kali є нащадком Back Track). Цей дистрибутив відрізняється великим набором інструментів, які вже налаштовано і більшість з них готові працювати «з коробки», великим набором апаратного забезпечення що підтримується без додаткових налаштувань, стабільністю роботи, регулярними оновленнями, доброю підтримкою та великим і активним ком'юніті. До того ж варто зауважити що Offensive Security випускає і операційну систему для мобільних телефонів, планшетів та деяких мікро-контролерів – NetHunter, на основі Android (Lolipop (5.1), Marshmallow (6.0)).

Даний дистрибутив можливо запустити з флеш карти у режимі Live. Але для повноцінного його використання варто провести процес інсталяції. Перейдемо до виконання лабораторної роботи.

Завантажити дистрибутив можливо на офіційному сайті kali.org у розділі завантаження (downloads). Дистрибутиви розповсюджуються для 32х та 64 розрядних систем. Завантажити файл можливо як і прямо з серверів сайту, так і за допомогою протоколу bitTorrent.

Процес інсталяції варто почати з відповіді на питання чи систему буде розгорнуто у віртуальному середовищі (віртуальна машина), чи на реальній системі? Якщо систему вирішено розгортати у віртуальному середовищі то тоді необхідно завантажити, додатково відповідне програмне забезпечення. Можливо обирати 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 можливо завантажити з офіційного сайту virtualbox.org, це ПЗ розповсюджується як для операційних систем сімейства Windows так і Linux. Детальні інструкції з інсталяції для операційної системи Linux знаходяться на тій же сторінці завантаження. Інсталяція для ОС Windows є абсолютно стандартною, але необхідно звернути увагу що під час інсталяції на короткий проміжок часу буде вимкнено доступ до мережі, це пов’язано з інсталяцією мережевих драйверів віртуальної машини.

Після того як визначено середовище в якому буде розгорнуто систему необхідно підготувати образ. З офіційного сайту можливо завантажити iso – образ, за для зручності його можливо записати на флеш-карту. Для операційних систем Linux необхідно використати утиліту dd у терміналі, або утиліту disks яка є графічним варіантом утиліти dd. Для операційних систем Windows зручніше використати утиліту Win32 Disk Imager, яку можливо завантажити з сайту launchpad.net (сторінка завантаження launchpad.net/win32-image-writer). Також iso образ можливо просто записати на DVD диск.

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 – 8) показана послідовність створення віртуальної машини для ПЗ VirtualBox:

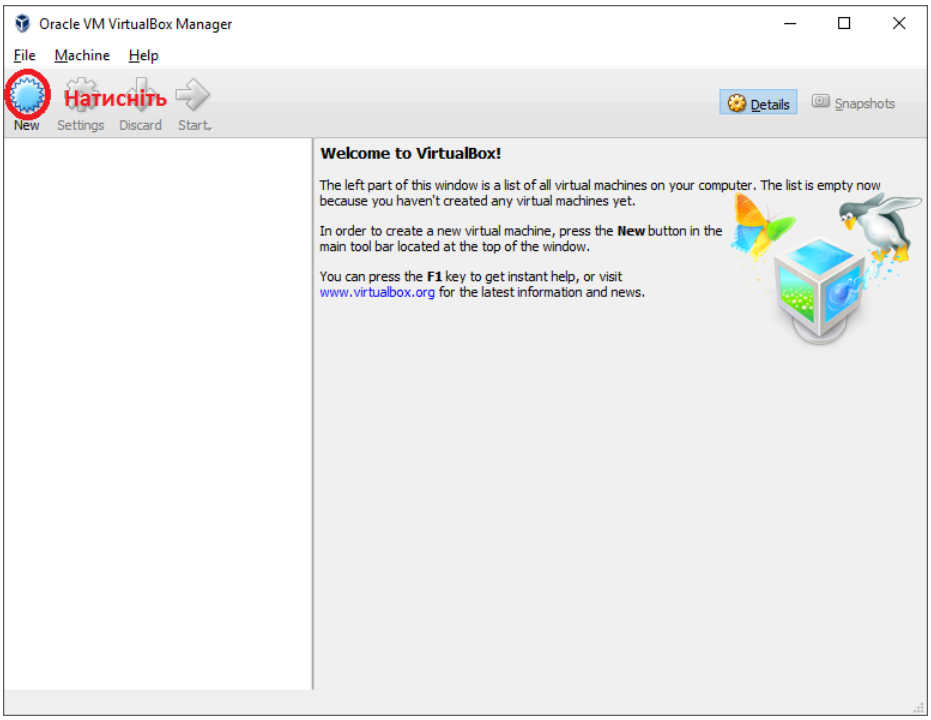

Рисунок 1 – Початок створення віртуальної машини для ПЗ VirtualBox

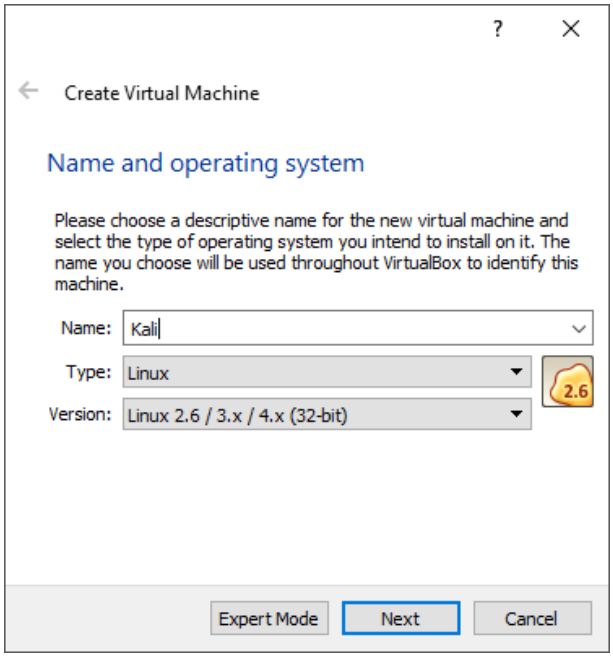

Рисунок 2 – Оберіть вказані параметри та натисніть «Next»

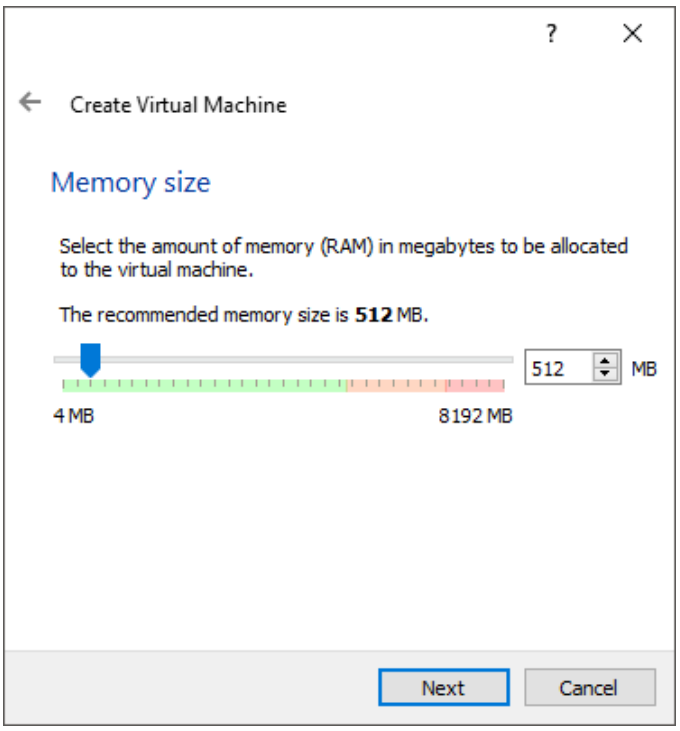

Рисунок 3 – Оберіть кількість оперативної пам'яті що буде виділено для віртуальної машини, рекомендовано виділити 2Гб

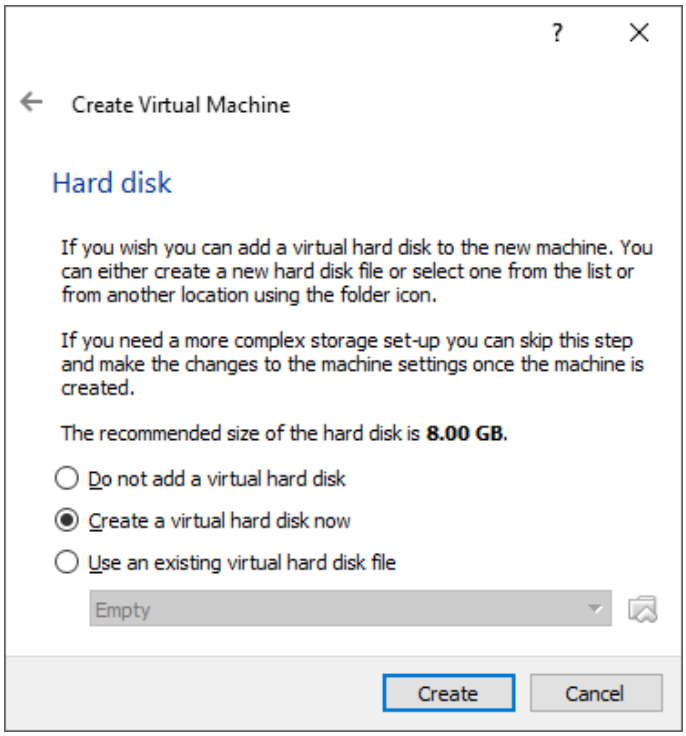

Рисунок 4 – Оберіть "Create a virtual hard disk now" і натисніть "Create"

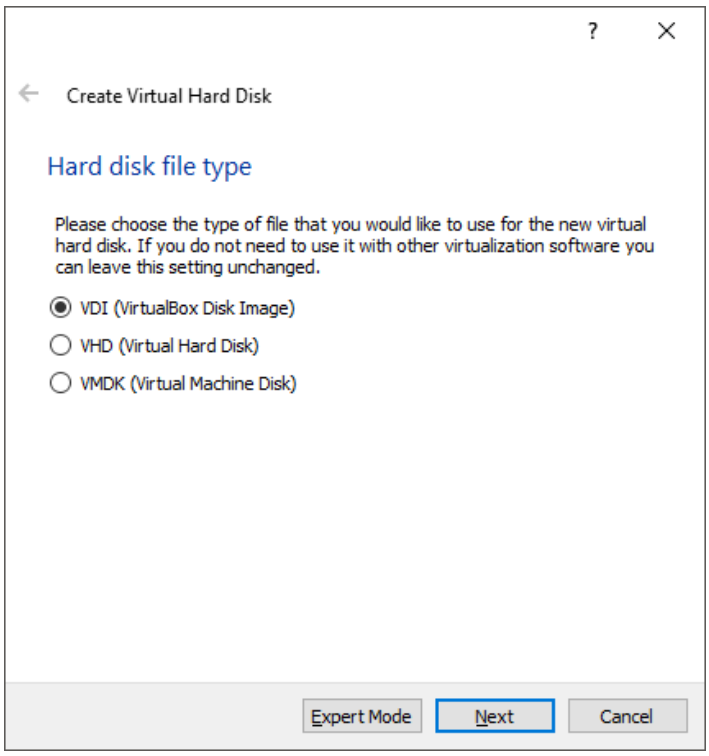

Рисунок 5 – Оберіть вказані параметри та натисніть "Next"

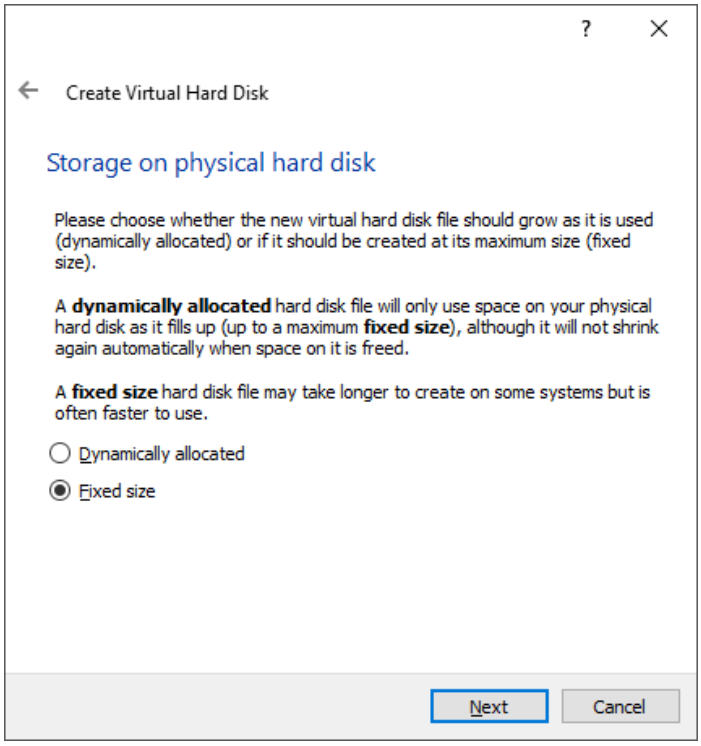

Рисунок 6 – Оберіть "Fixed size" та натисніть "Next"

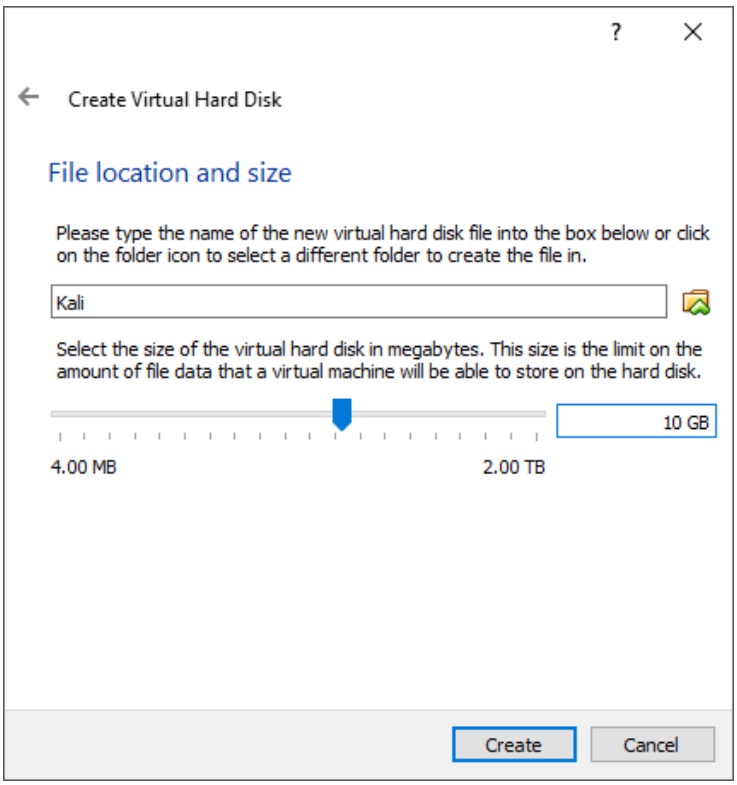

Рисунок 7 – Оберіть вказані параметри та натисніть "Create"

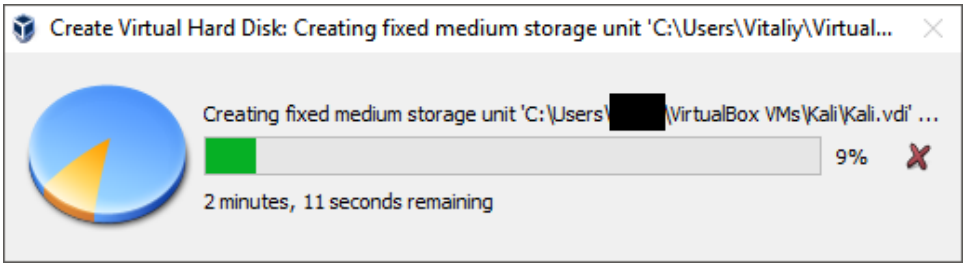

Рисунок 8 – Почнеться процес створення віртуальної машини

Після завершення створення віртуальної машини змонутйте образ (наприклад за домогою Daemon Tools Lite), або підключіть відповідний фізичний носій і натисніть «Start» як показано на Рисунок 9.

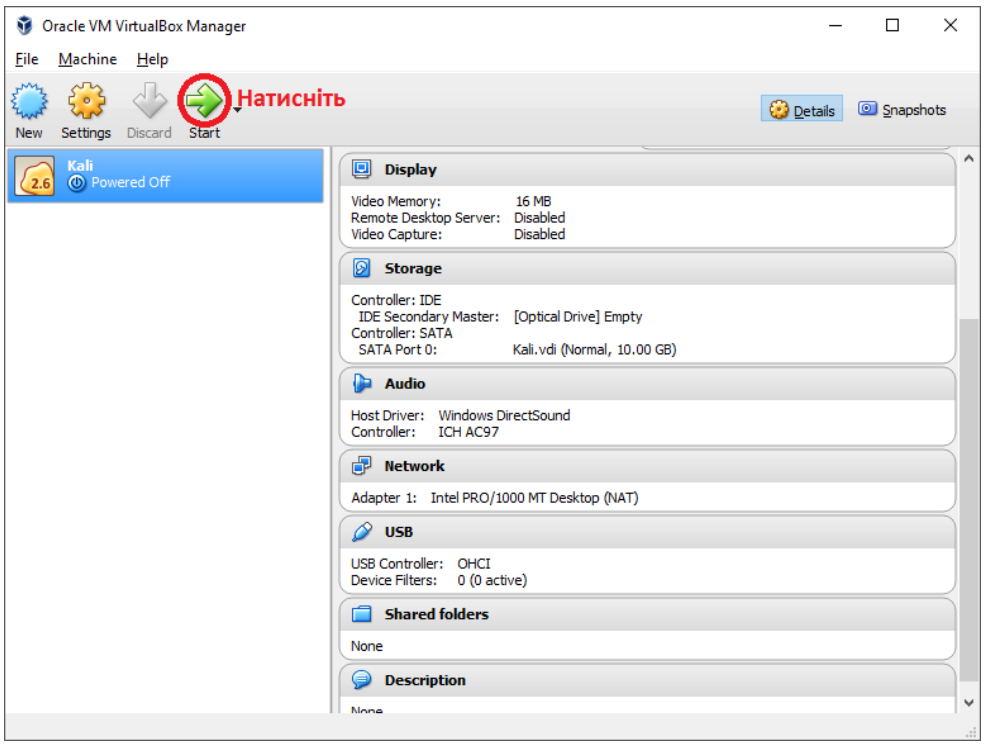

Рисунок 9 – Натисніть "Start"

У новому вікні оберіть диск який буде використано як загрузочний для першого запуску віртуальної машини. Після завантаження оберіть пункт як показано на Рисунок 10.

Рисунок 10 – Оберіть відповідний пункт та натисніть "Enter"

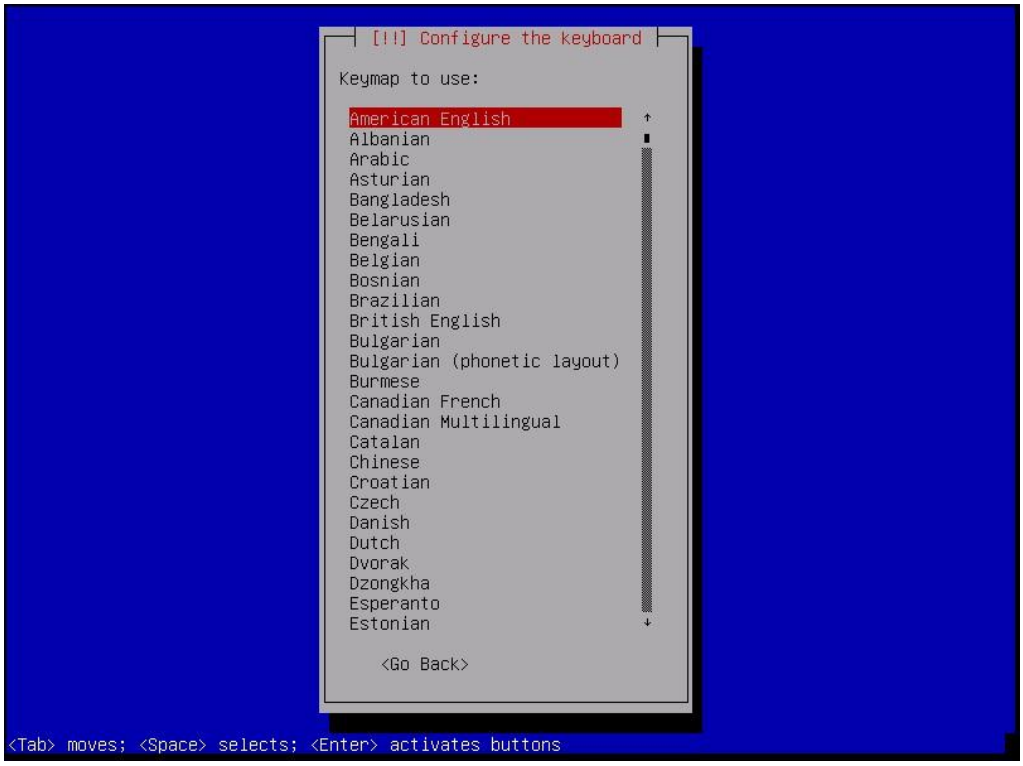

Рисунок 11 – Оберіть мову введення (мову клавіатури)

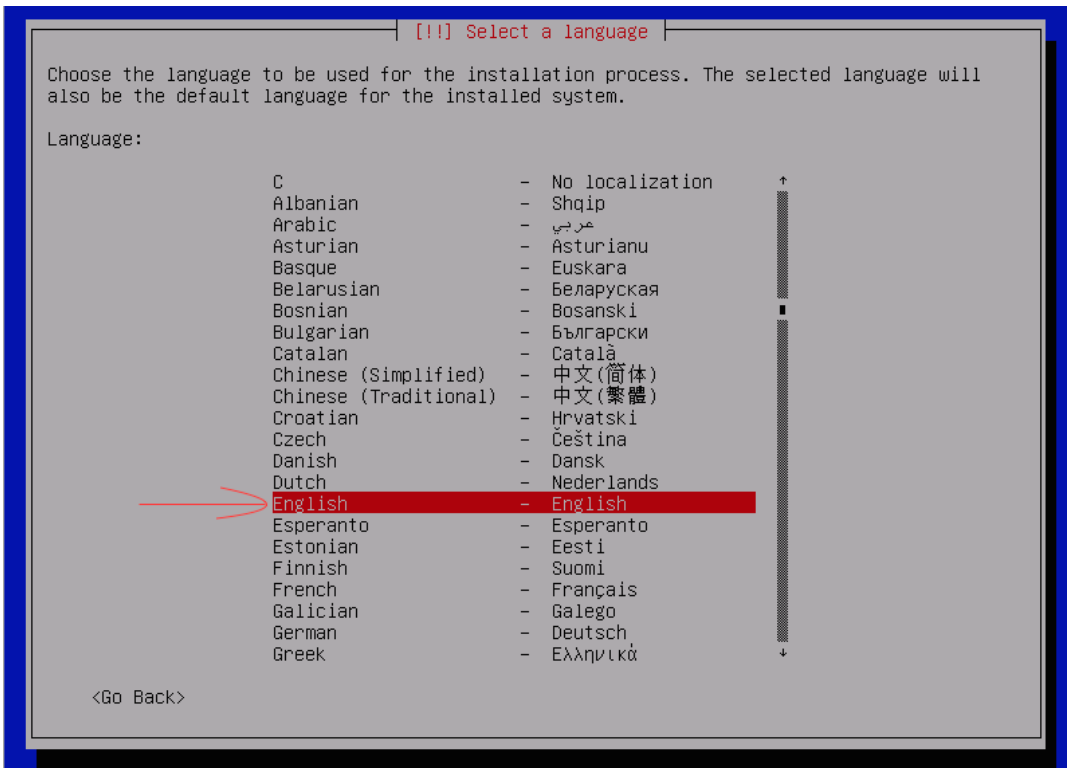

Рисунок 12 – Оберіть мову інсталяції (рекомендовано обрати англійську)

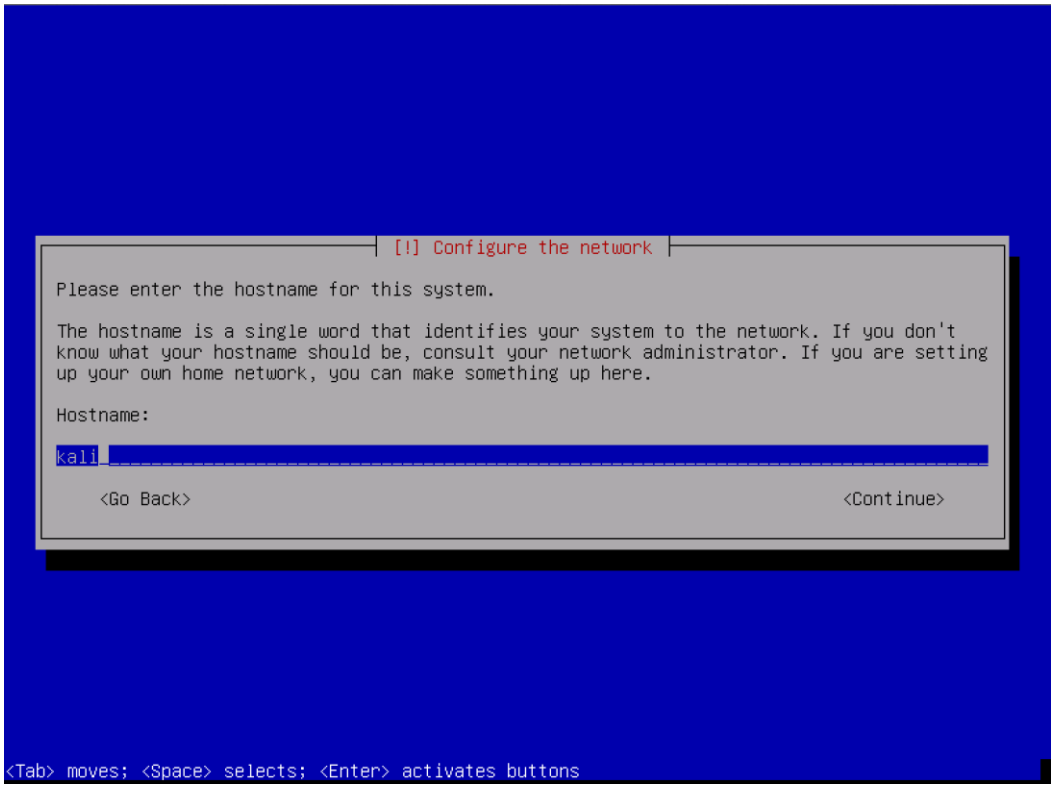

Рисунок 13 – Введіть ім'я хосту (будь яке)

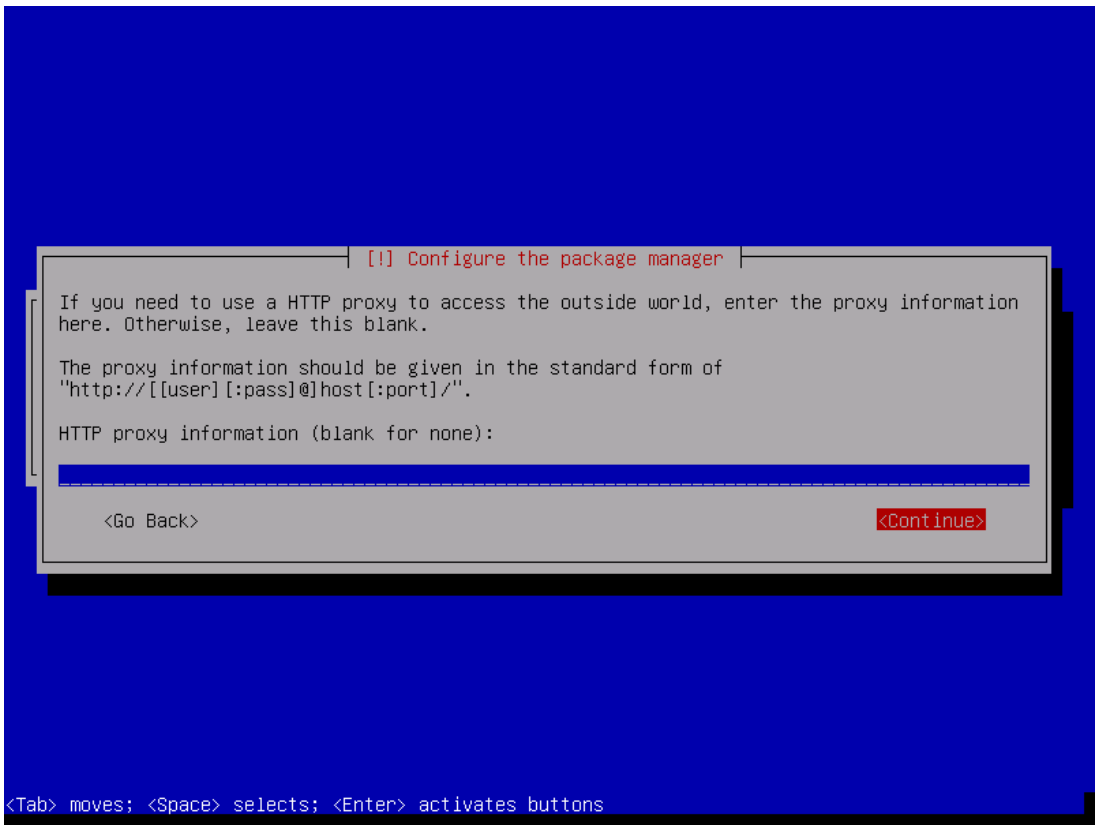

Рисунок 14 – Якщо використовувати проксі немає необхідності – лишіть поле пустим і натисніть "Continue"

Після того як ви пройдете кроки (їх послідовність може бути змінена у різних версіях інсталятора) які зображено на Рисунок 11 – 14, буде запропоновано розмітити диск. У разі інсталяції системи на віртуальну машину оберіть пункт як зображено на Рисунок 15. В іншому випадку, диск необхідно розмічати виходячи із поточних обставин. У такому випадку 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.

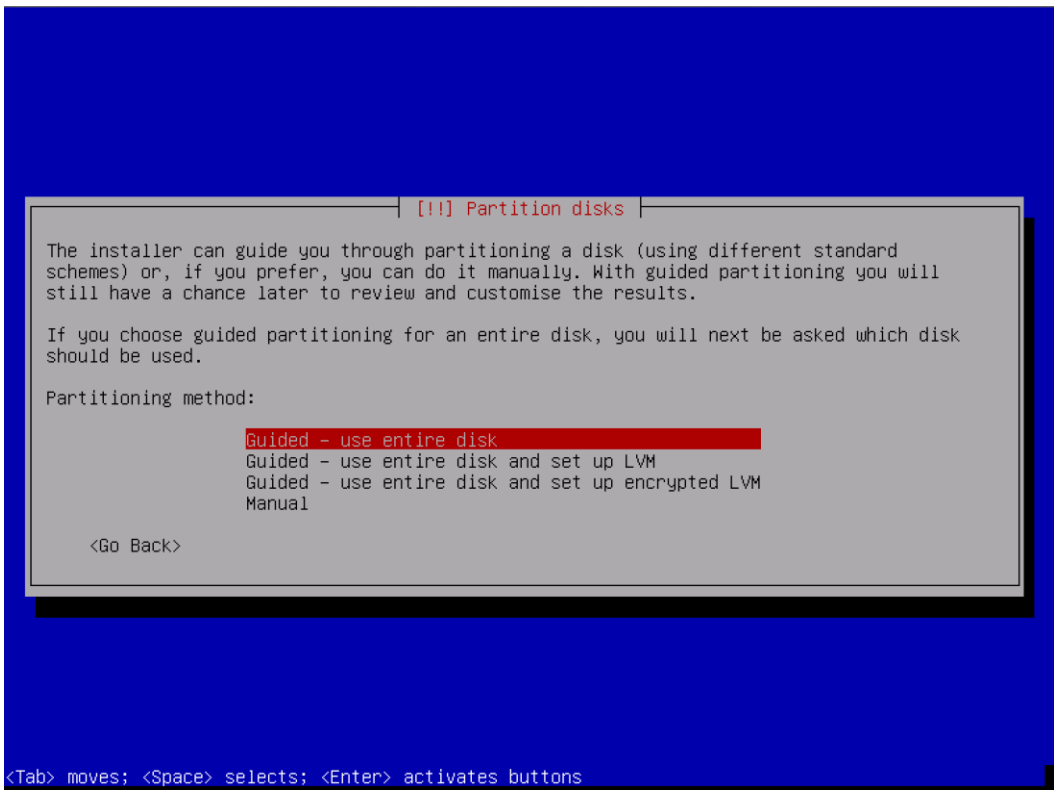

Рисунок 15 – Для того щоб використати весь диск оберіть "use entire disk", для ручної розмітки – оберіть "Manual"

Після завершення інсталяції буде запропоновано встановити GRAB (Рисунок 16) – погодьтеся і оберіть диск на якому встановлено ОС. Після цього буде виведено повідомлення про успішну інсталяцію ОС на комп’ютер (Рисунок 17). На цьому, розгортання системи буде завершено, а комп’ютер необхідно перезавантажити.

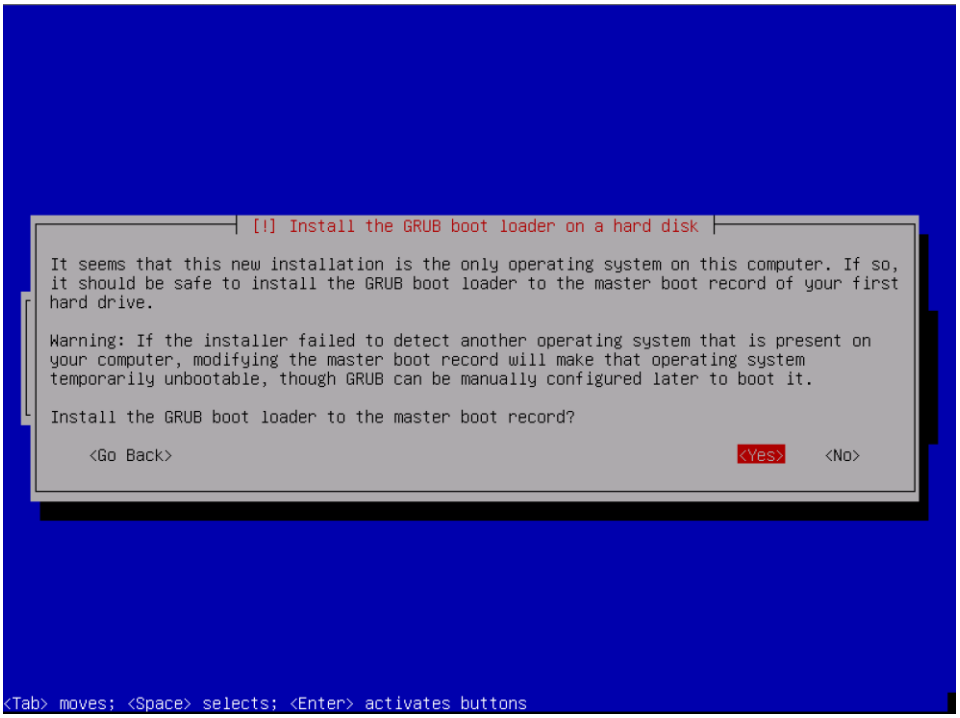

Рисунок 16 – Оберіть "Yes" та натисніть Enter

Рисунок 17 – Інсталяцію завершено, оберіть "Continue" та натисніть Enter

Завдання:

Розгорнути операційну систему Kali Linux на комп’ютері або віртуальній машині.

Лабораторна робота №2

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

Мета: Отримати знання та навички користування інструментами скритого 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 у 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 засобів та методів збору технічної інформації, однак, найбільш поширеним з них є nmap. Для nmap було розроблено графічний інтерфейс – zenmap (Рисунок 2), на Рисунок 1 зображено консоль з nmap.

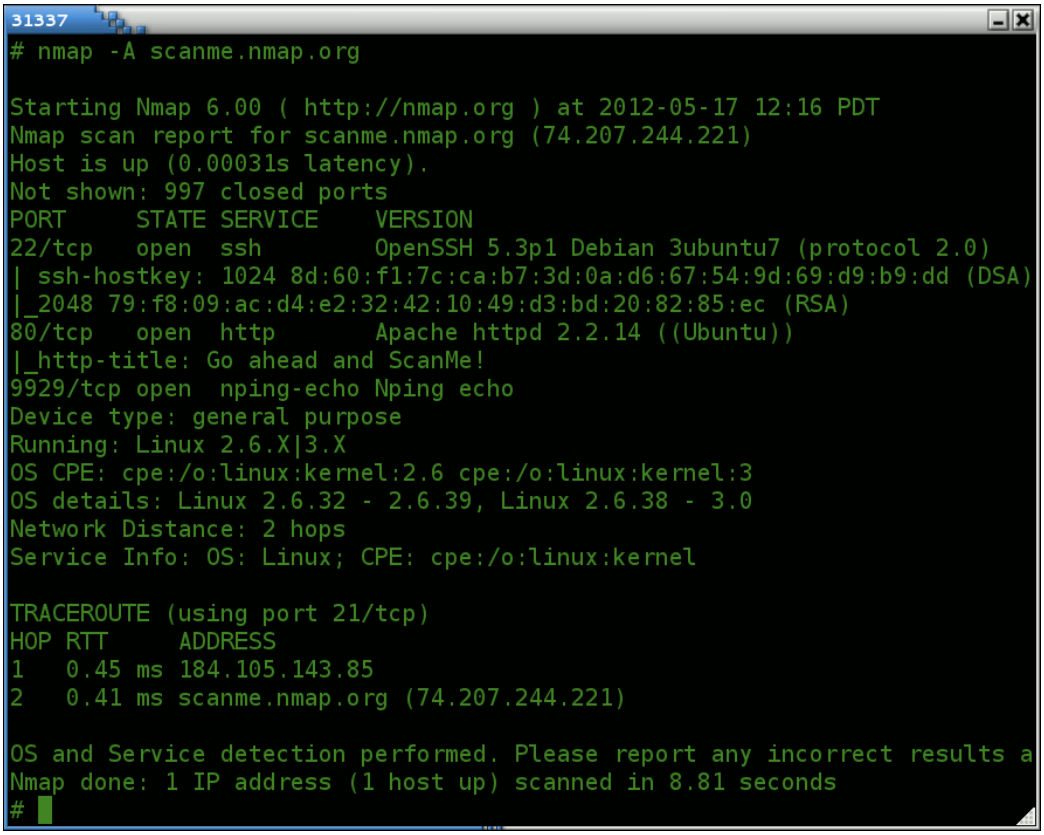

Рисунок 18 – Консоль з nmap

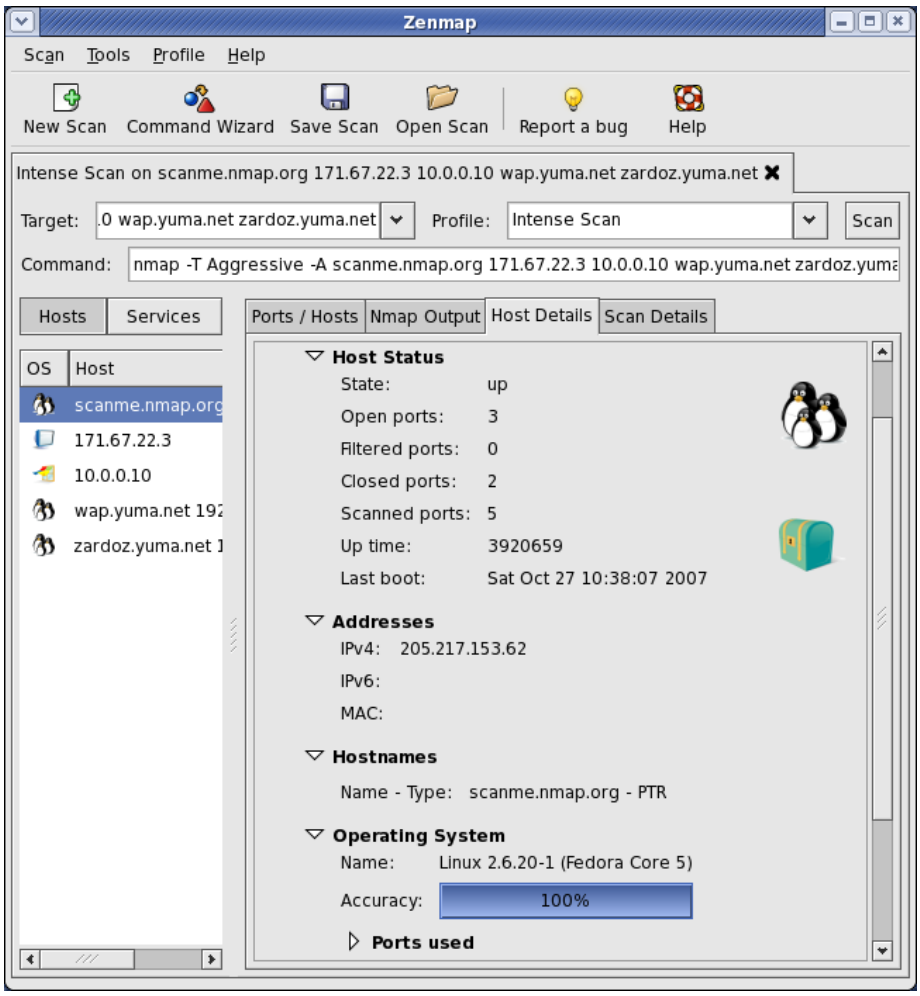

Рисунок 19 – Інтерфейс nmap – zenmap

Розглянемо використання nmap:

Синопсис:

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.

-sU (UDP сканування) – дозволяє сканувати сервіси що використовують UDP протокол.

-sY (SCTP INIT сканування) – еквівалент “-sS” для SCTP (більш нова 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

-F – швидке сканування портів, nmap сканує 1000 найбільш вживаних портів, використовуючи дану опцію ця кількість зменшується до 100.

-sV – визначає версію сервісу що використовує порт

-O – вмикає визначення операційної системи

--max-os-tries – встановлює максимальну кількість спроб визначення операційної системи

Це основні опції та типи сканування що використовує nmap. Варто зауважити що інструмент nmap настільки потужний що має свою скриптову мову – NSE, яка дозволяє організовувати дуже складні механізми збору інформації.

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. У zenmap є декілька дуже важливих переваг, окрім зручності використання графічного інтерфейсу. Однією з вагомих переваг це 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. А ще zenmap дозволяє робити свої особисті профайли сканувань для подальшого їх використання. Розглянемо інтерфейс zenmap детальніше.

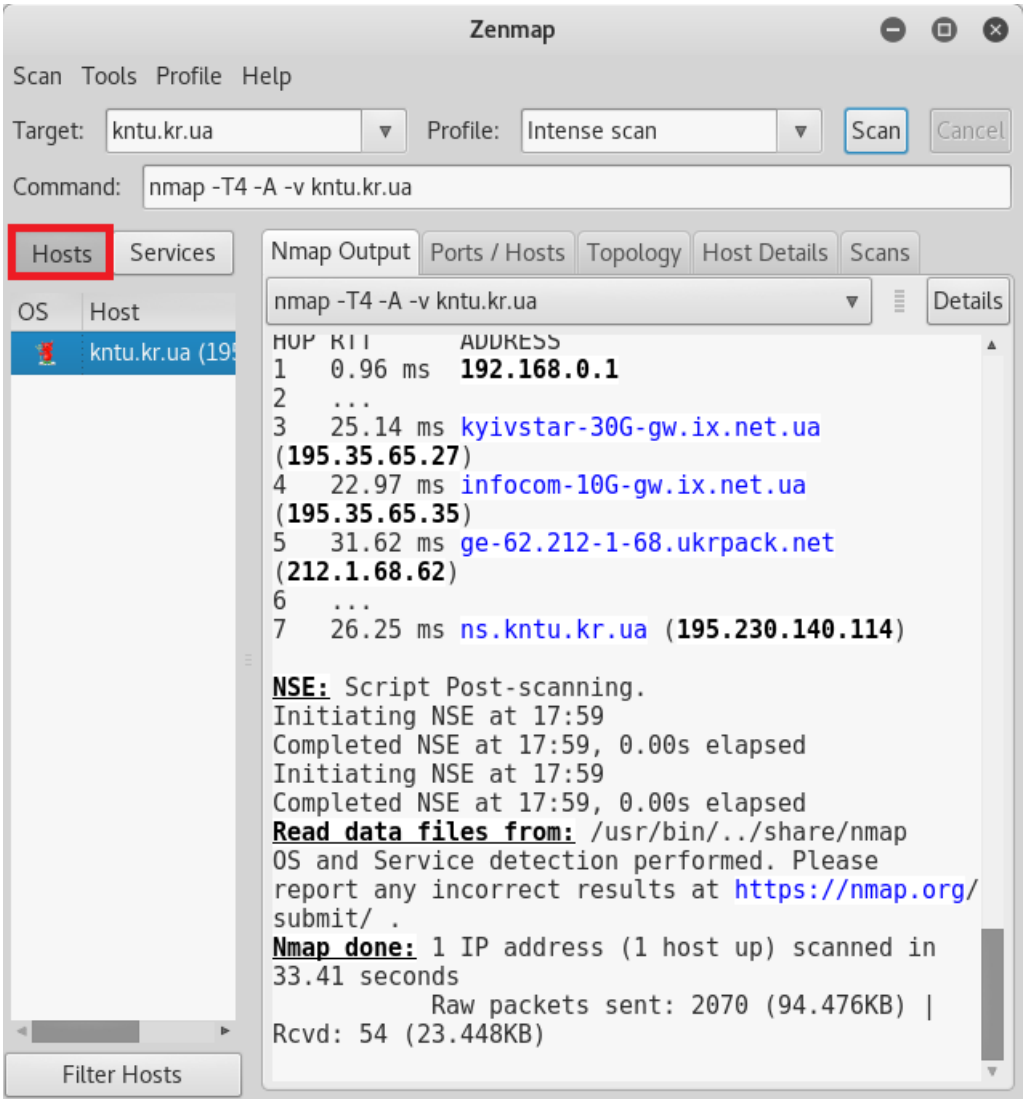

Рисунок 20 – Вкладинка Hosts – перелічено знайдені хости, та стандартний вивід nmap – вкладинка Nmap Output

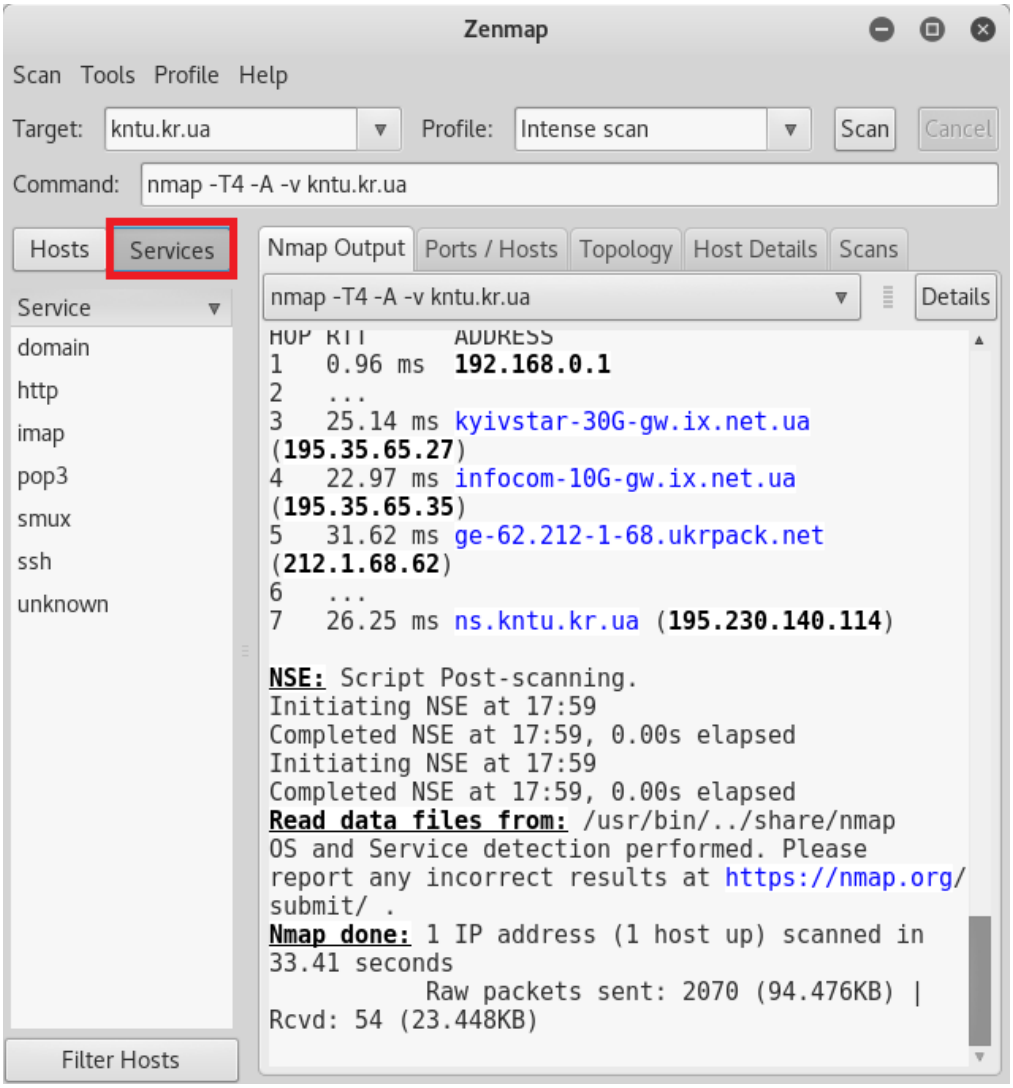

Рисунок 21 – Вкладинка Services – відображаються усі знайдені сервіси

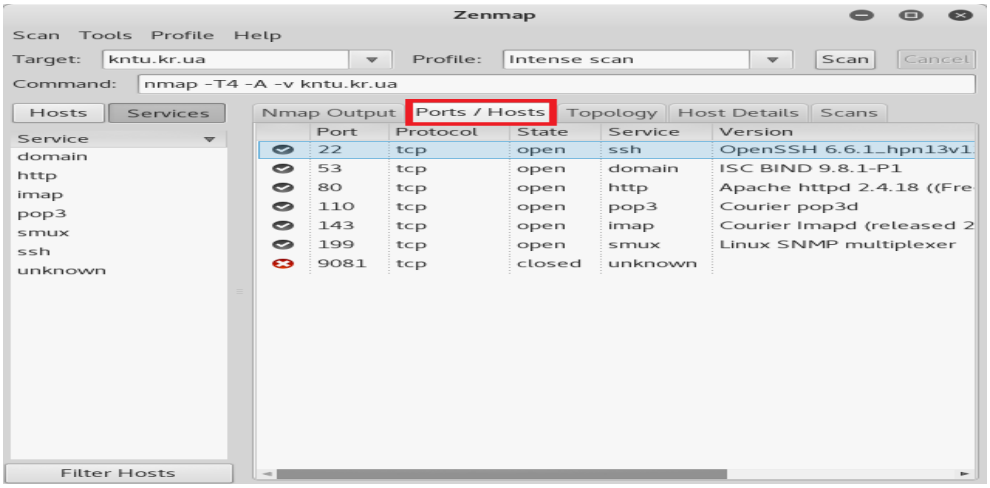

Рисунок 22 – Вкладинка Port/Hosts – перелічено відношення відкритого порту до хосту

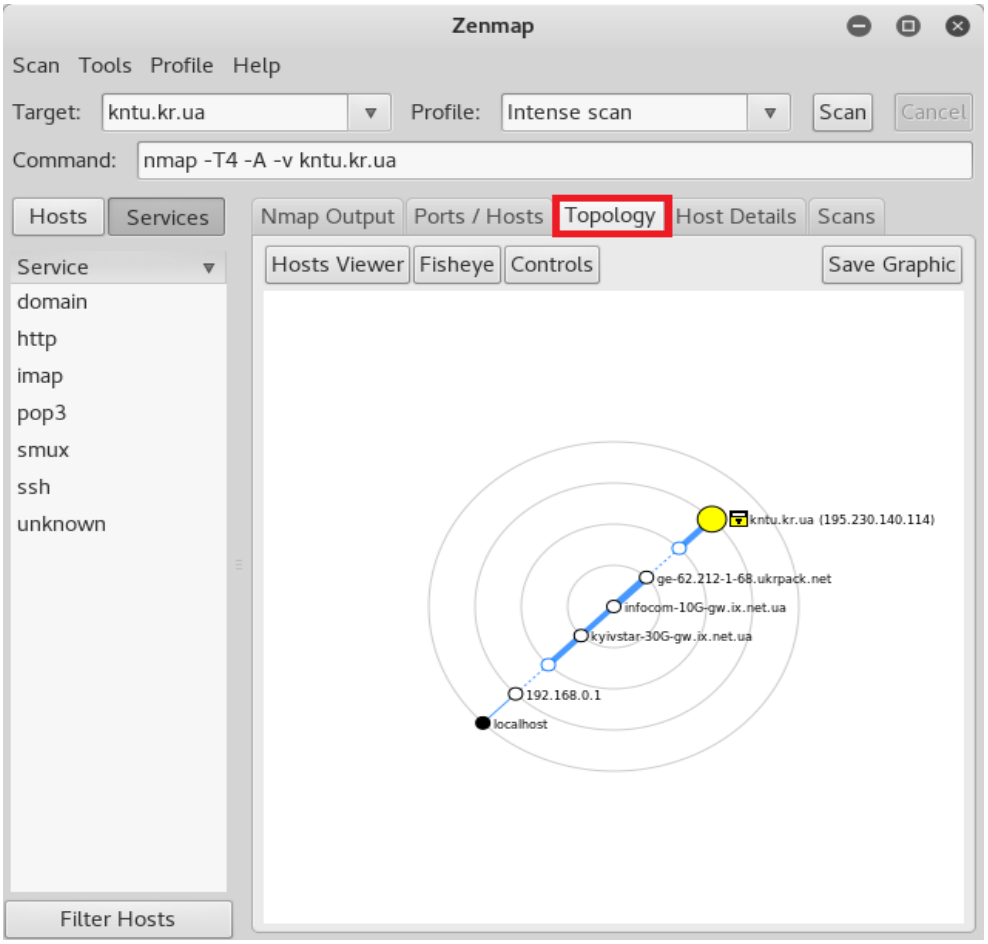

Рисунок 23 – Вкладинка Topology – відображає автоматично побудований граф-топологію відсканованої області мережі)

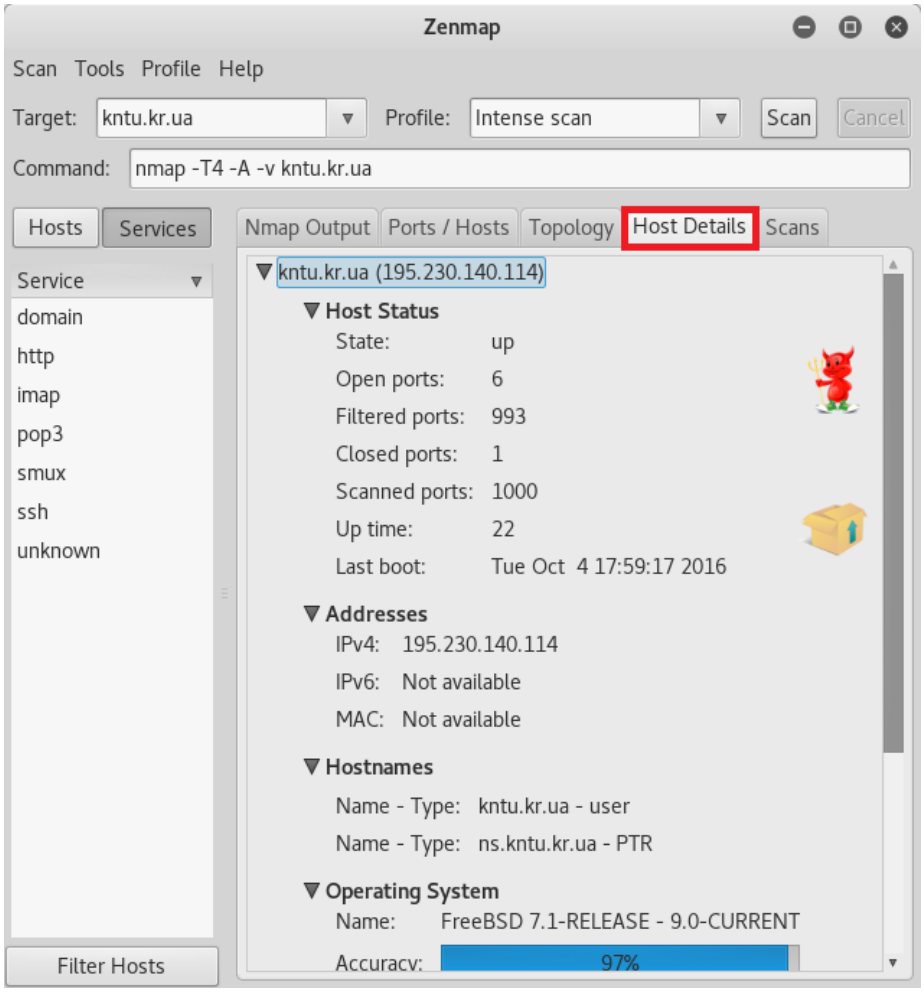

Рисунок 24 – Вкладинка Host Details – відображає найважливішу інформацію про поточний хост

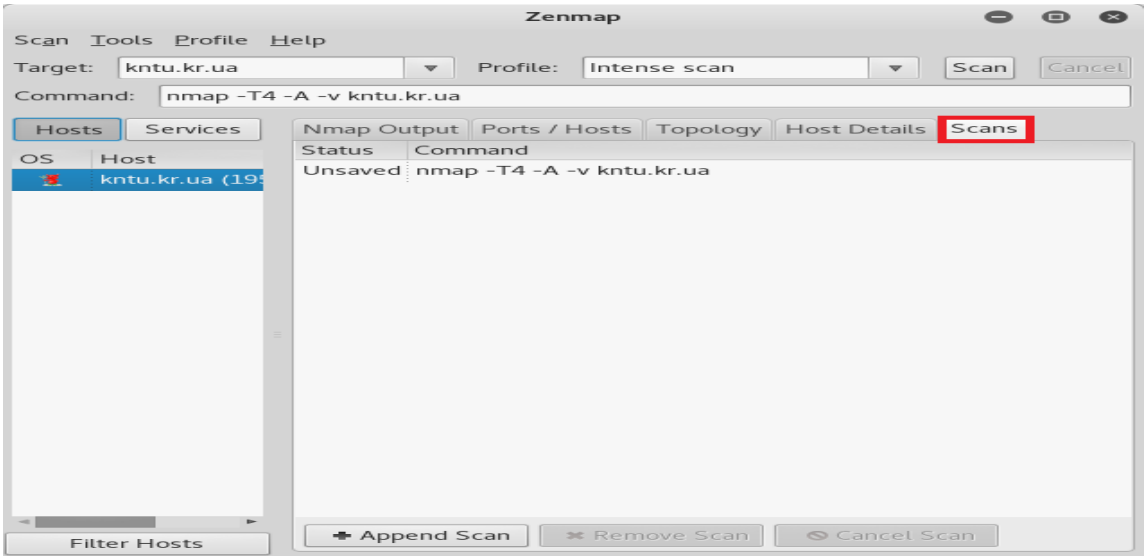

Рисунок 25 – Вкладинка Scans – відображає список та стан (збережено/не збережено) сканувань

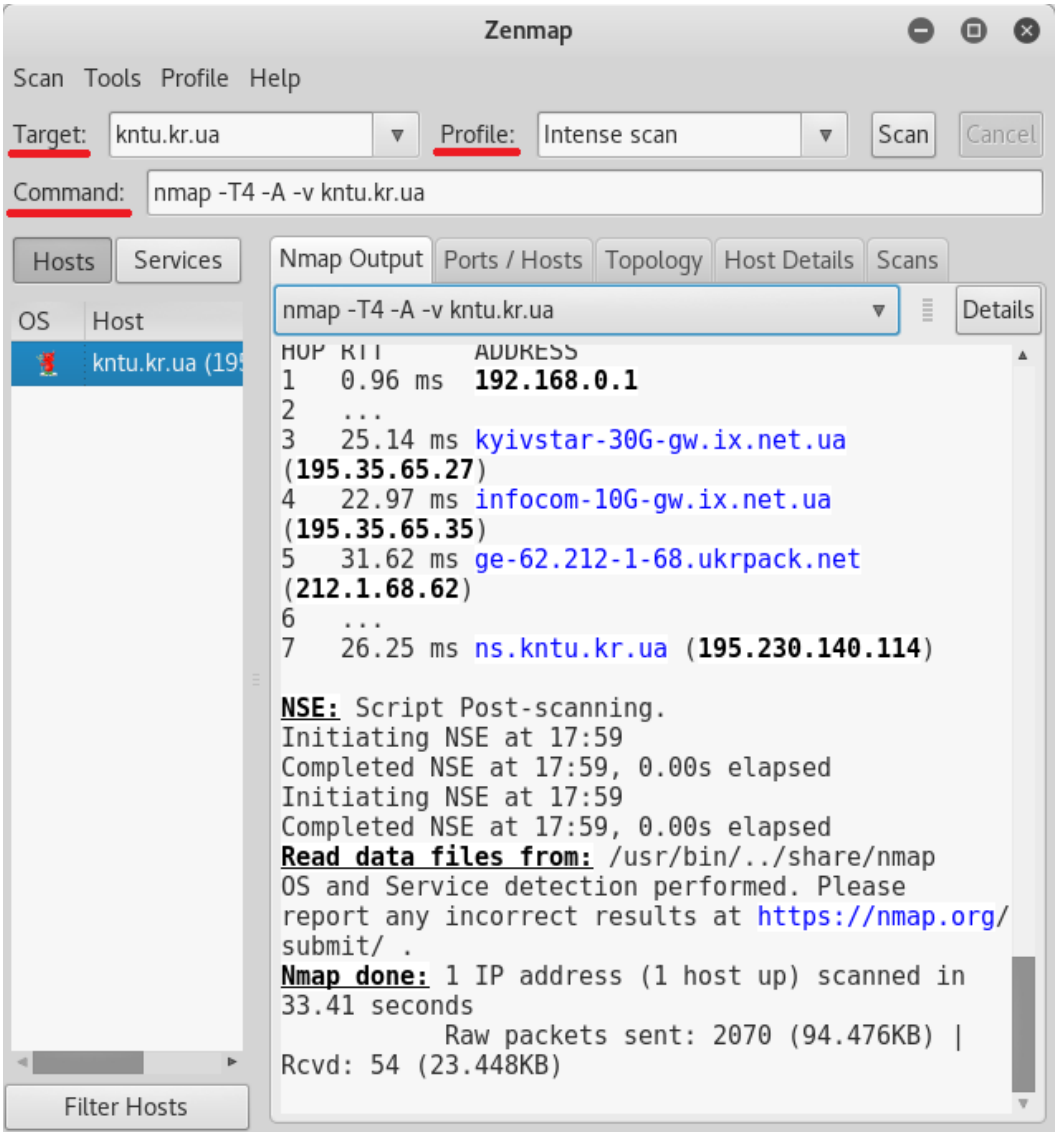

Рисунок 26 – Поля Target, Profile, Command

На Рисунок 9 позначені (червоним маркером) поля:

Target – визначає ціль що буде просканована. Наприклад, якщо необхідно просканувати діапазон від 10.10.10.0-10.10.10.256 можна встановити цей параметр у 10.10.10.0/24

Profile – параметр що визначає який профайл буде використано для сканування, профайли можливо створювати самостійно або використовувати існуючі. Після вибору профайла його строчка буде розміщена у поле Command.

Command – визначає командну строчку яку буде виконано в процесі сканування. Її можливо змінити якщо, наприклад, певний профайл буде використано лише як основу наступного сканування.

Завдання:

1. Скласти характеристику комп’ютерів та топологічну мапу мережі використовуючи інструменти nmap або zenmap, або інші. У характеристиці повинні бути викладені наступні питання:

– Відкриті порти

– Запущені сервіси

– Версії операційних систем

2. Надати припущення – які сервіси можуть бути запущені на портах що відкрито але сервіси до них не визначені при скануванні

3. Дати короткий опис сервісам що запущені в мережі

4. Надати по декілька (якщо є) вразливостей сервісів що запущено на хостах за інформацією національної бази вразливостей США – nvd.nist.gov

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 відповідальних етапів проведення дослідження захищенності комп'ютерної системи або мережі, він, найчастіше є і найдовшим. Існує як багато методів так і багато засобів (інструментів) для проведення збору необхідної інформації. Кожен інструмент використовує свій набір методів дослідження систем, а кожен метод направлено на свою 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 scaners). Одним з найпотужніших таких засобів є сканер – Nessus.

У цій лабороторній 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 зформувати у звіт, зміст звіту роз'яснено у завданні до цієї лабораторної роботи.

Для встановлення пакету завантажте його з офіційного сайту tenable.com (поточна сторінка завантаження tenable.com/products/nessus/select-your-operating-system#tos). 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 1):

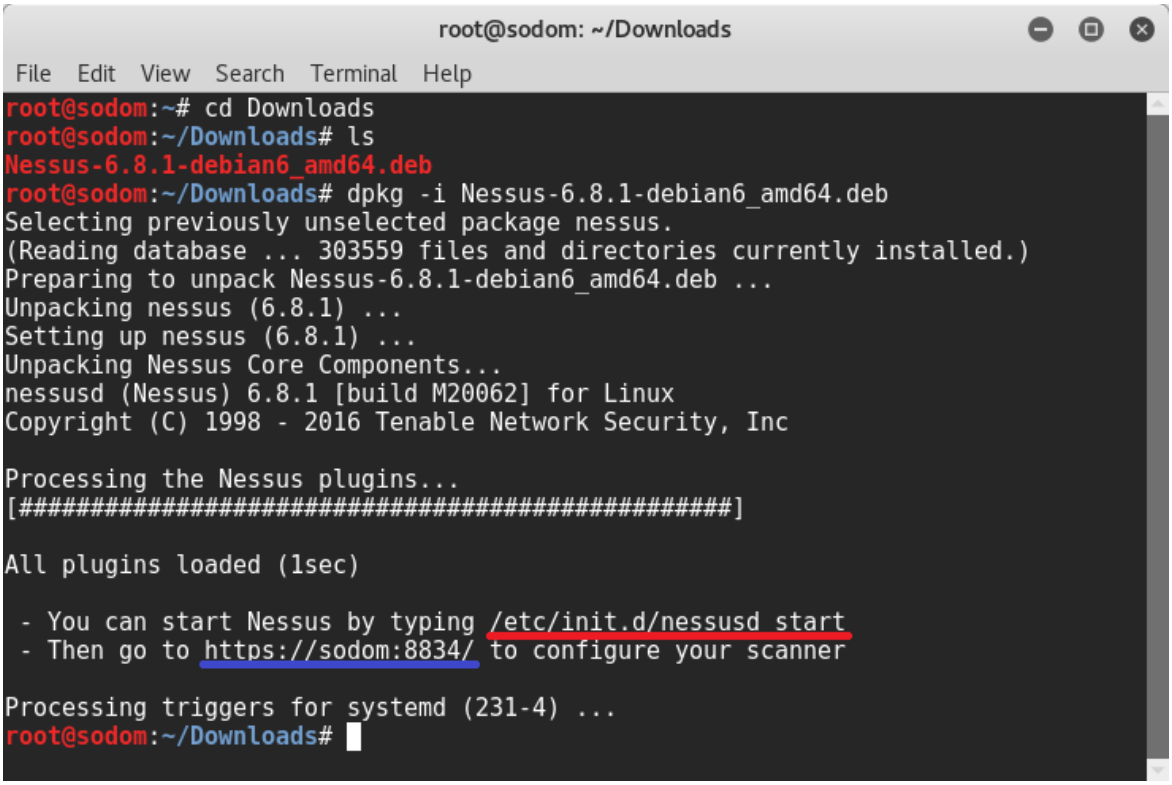

Рисунок 27 – Повідомлення вдалого встановлення Nessus

Після встановлення запустіть сканер за допомогою команди що вказана у вашій консолі а на Рисунок 1 позначена червоним маркером. У разі вдалого запуску повідомлення консолі буде мати наступний вигляд (Рисунок 2):

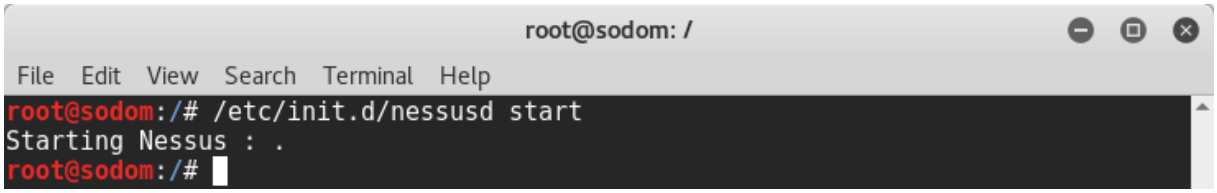

Рисунок 28 – Повідомлення у разі вдалого старту Nessus

Після того як сервіс буде запущено, відкрийте веб-переглядач, та введіть у його адресну строку адресу що вказана у вашій консолі а на Рисунок 1

виділено синім маркером, 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.

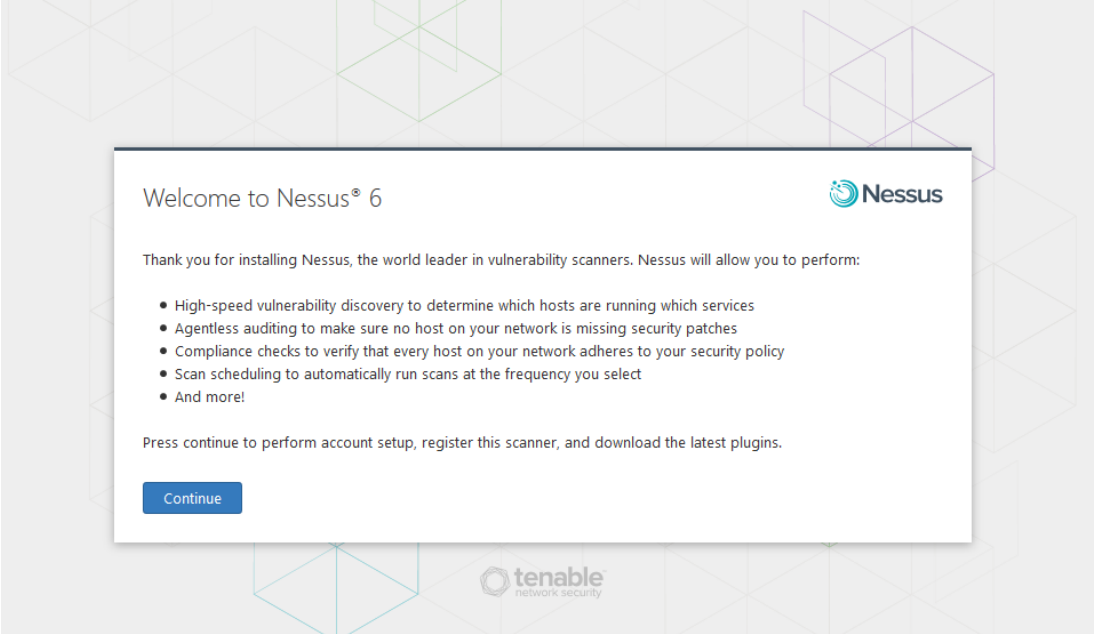

Рисунок 29 – Стартова сторінка Nessus

Натисніть Continue та створіть адміністратора сканера. Після чого поверніться на сторінку завантаження пакету, знайдіть внизу сторінки кнопку «Get an activation code». Перейшовши на сторінку з вибором типу ліцензії оберіть – Home. Зареєструйтеся для отримання ліцензії. Після реєстрації код активації буде надіслано вам на почтову скриньку що ви вказали при реєстрації. Поверніться на сторінку сканера та введіть отриманий ключ. Почнеться завантаження (Рисунок 4).

Рисунок 30 – 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 (не для отримання ліцензійного ключа), на Рисунок 5 зображено головну сторінку сканеру.

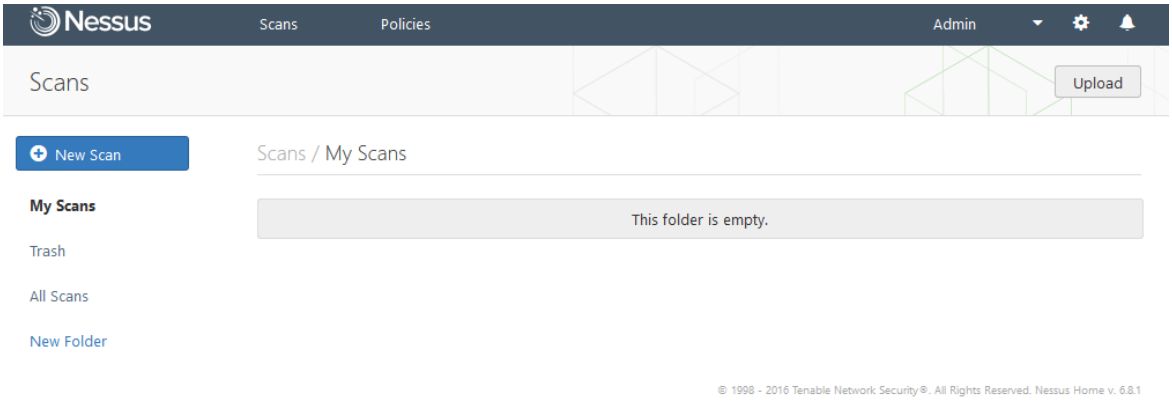

Рисунок 31 – Головна сторінку сканеру

Після цього натисніть «New Scan». На новій сторінці оберіть сканування яке вважаєте за потрібне (обов'язковим є лише розширене – Advanced Scan). Введіть необхідні параметри натисніть Save та у розділі My Scans запустіть необхідне сканування. Звіт сканера додайте до звіту по лабораторній роботі.

Завдання:

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

2. Результатам сканування надати коротку характеристику (по кожній із знайдених вразливостей).

3. Порівняти результати отримані при виконанні лабораторної роботи №2, визначити хибно знайдені вразливості, якщо такі є, обґрунтувати вибір.

4.У висновку, порівняти метод збору інформації з лабораторної роботи №2 та №3, вказати при яких обставинах та цілях спеціаліста краще використовувати перший метод, а при яких – другий.

Лабораторна робота №4

Тема: Визначення вразливостей веб ресурсів та веб додатків. Сканер вразливостей – Vega.

Мета: Отримати навички збору інформації про вразливості із за допомогою сканера вразливостей – Vega.

Теоретичні відомості

Одним з найбільш поширених векторів проведення атак є – веб додатки та веб ресурси компаній. Це спричинено їх доступністю із зовні, та великою кількістю вразливостей що поширені веб технологіями. Одним із найбільш поширеним засобом для визначення вразливостей ресурсів є Burp Suit (Рисунок 1).

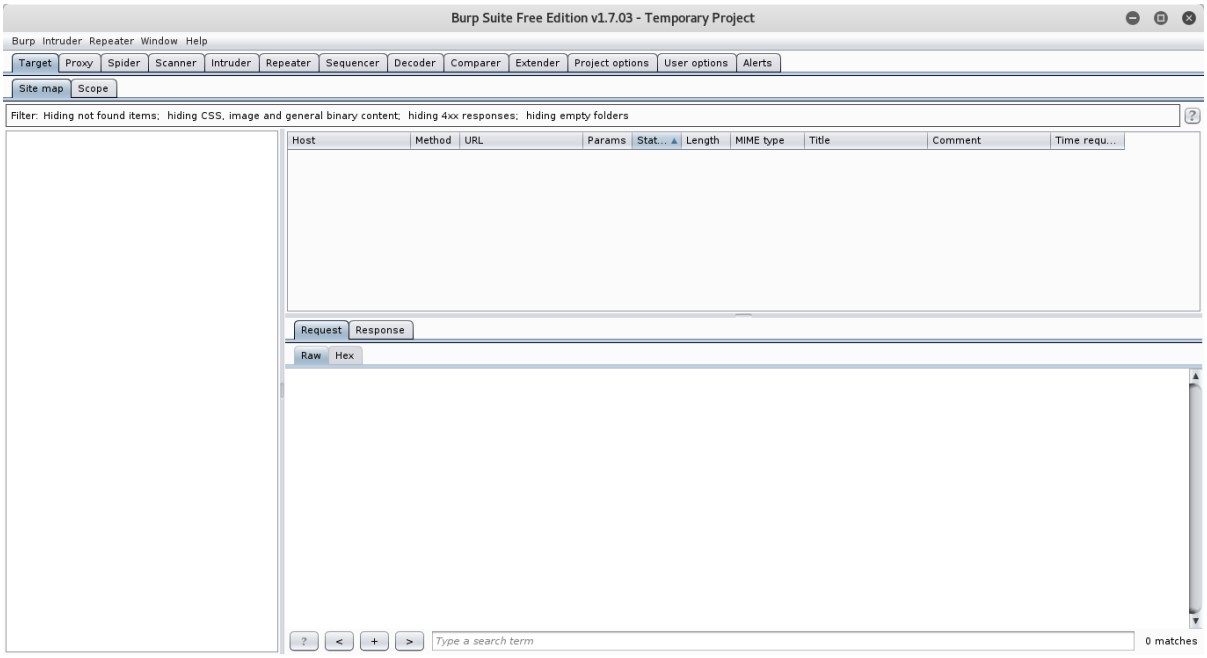

Рисунок 32 – Burp Suit

Burp Suit – це універсальний засіб, серед його інструментів як і ті які дозволяють 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 й на певному елементі веб додатку або ресурсу. У той же час Vega (Рисунок 2) це засіб робота якого зосереджена саме на зборі інформації про цілі у автоматичному режимі.

Для того щоб встановити сканер – Vega на Kali Linux запустіть консоль з правами супер-користувача (root) та використайте команду «apt-get install vega», вигляд консолі у разі вдалої інсталіції зображено на Рисунок 3. Після встановлення сканер доступний з меню додатків Kali Linux у вкладці «Web Application Analysis».

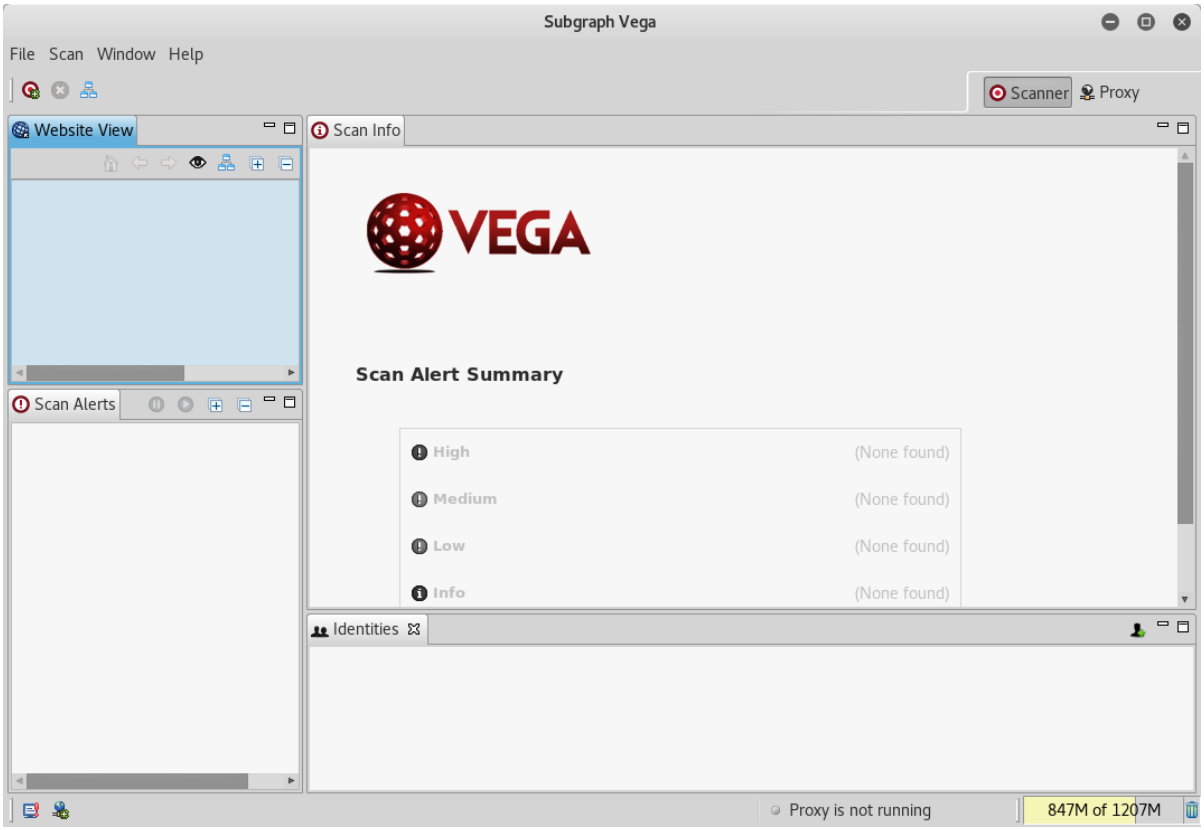

Рисунок 33 – Сканер вразливостей веб додатків та ресурсів – Vega

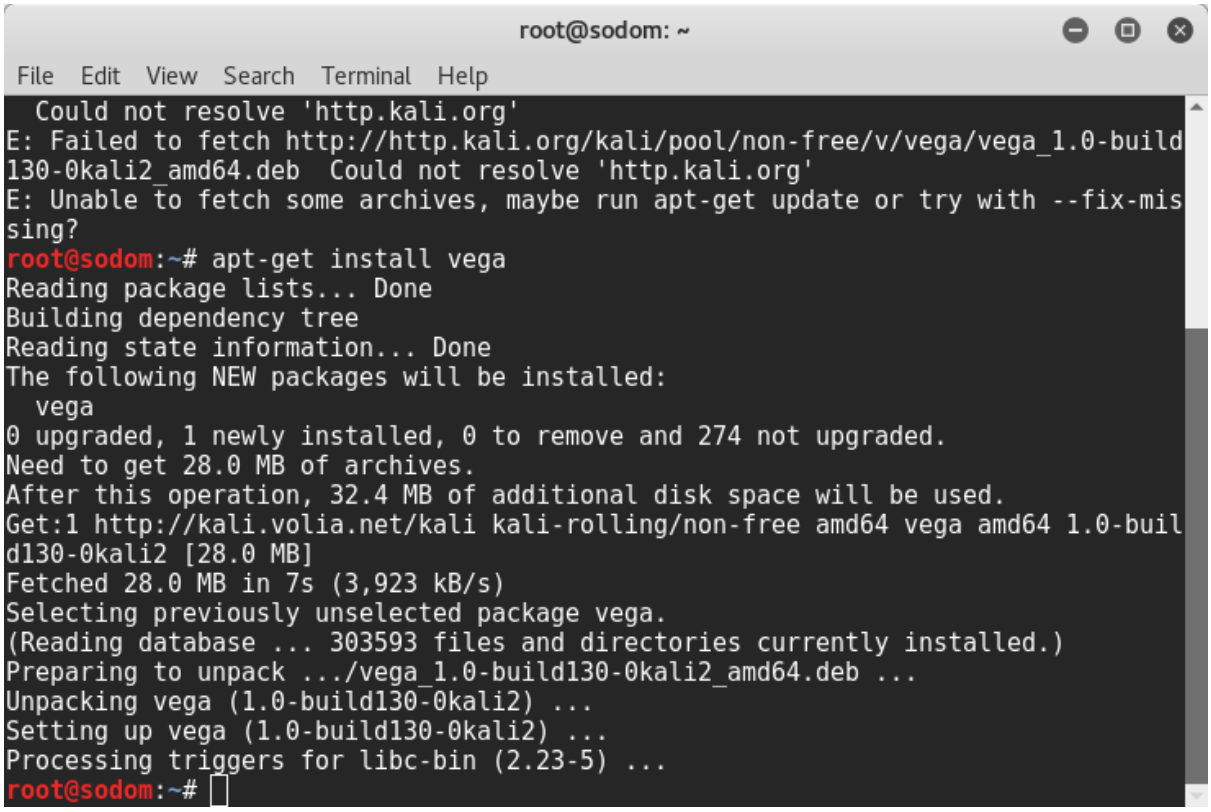

Рисунок 34 – Повідомлення терміналу про вдале встановлення сканера – Vega

Розглянемо роботу сканера. Після запуску сканера на екрані з’явиться головне вікно (Рисунок 2). Для того щоб почати сканування перейдіть до меню «Scan» де оберіть «Start New Scan». У новому вікні – «Select a Scan Target», введіть адресу ресурсу або веб додатку у поле «Enter a base URI for scan», та натисніть «Finish». Після цього сканер почне свою роботу (Рисунок 5).

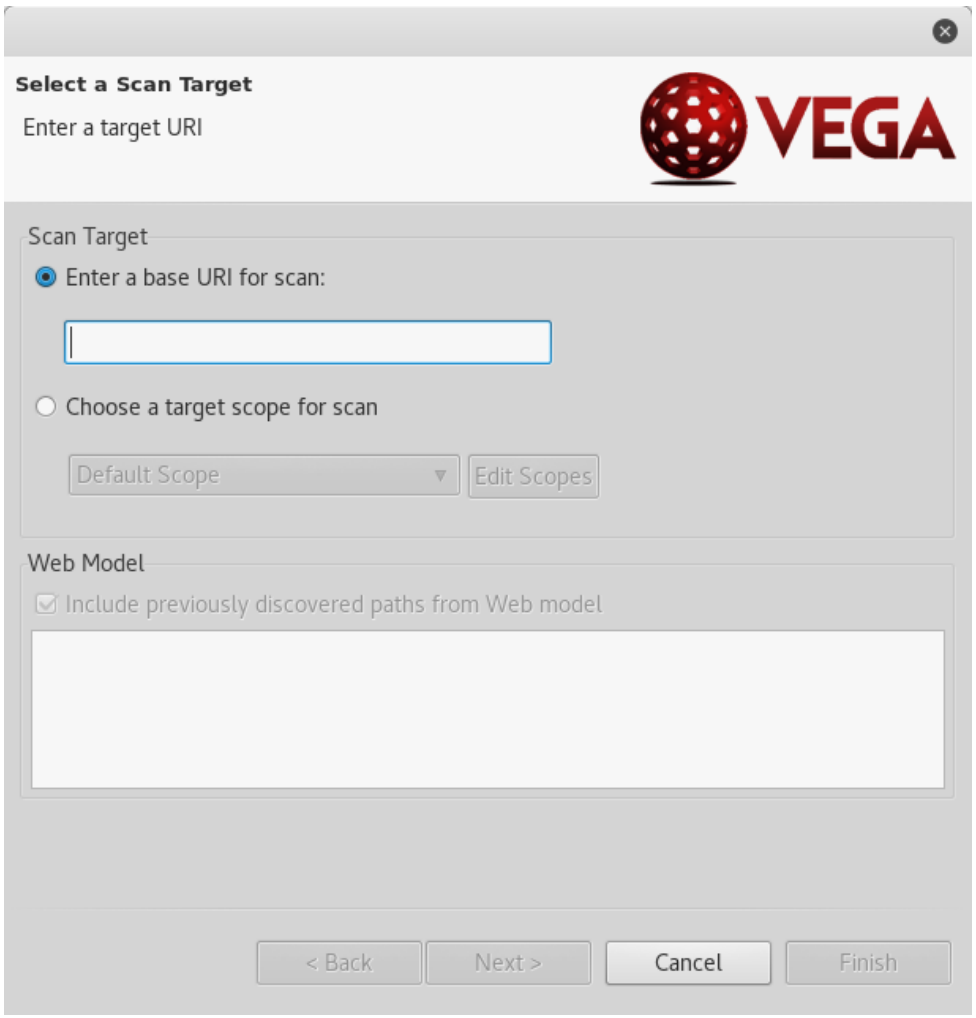

Рисунок 35 – Вікно «Select a Scan Target»

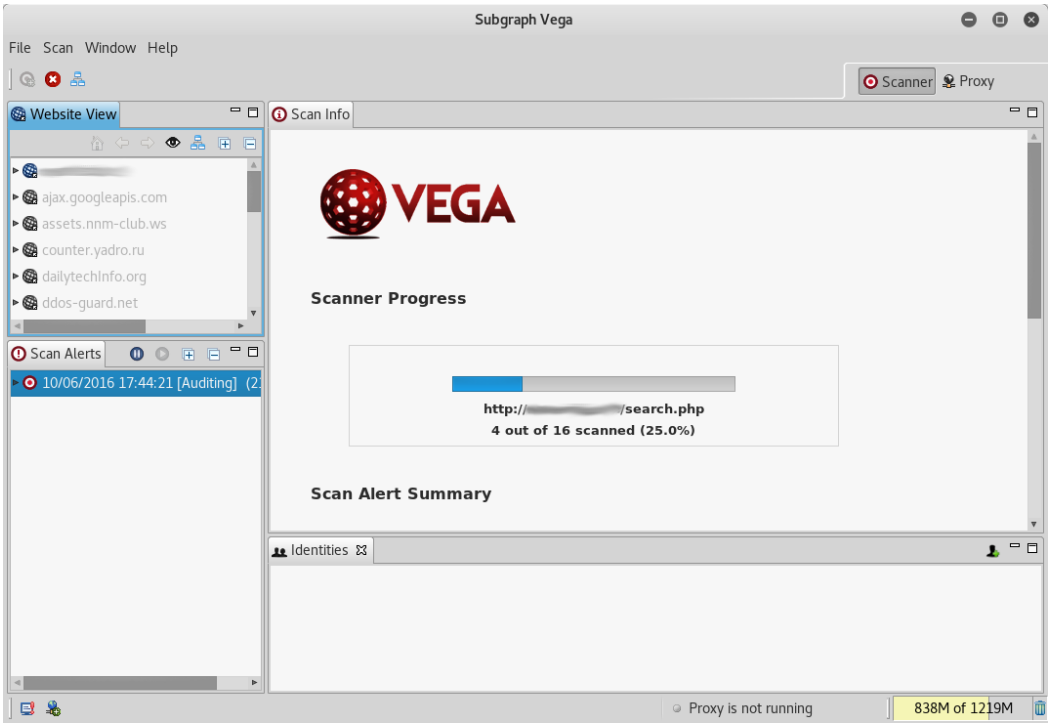

Рисунок 36 – Процес сканування

Після завершення сканування сканер виведе загальний звіт у головному вікні, де буде повідомлятися кількість та рівень небезпеки вразливостей (Рисунок 6). Зліва у вкладці «Scan Alerts» можливо переглянути кожну вразливість окремо та отримати детальний звіт по ній (Рисунок 7).

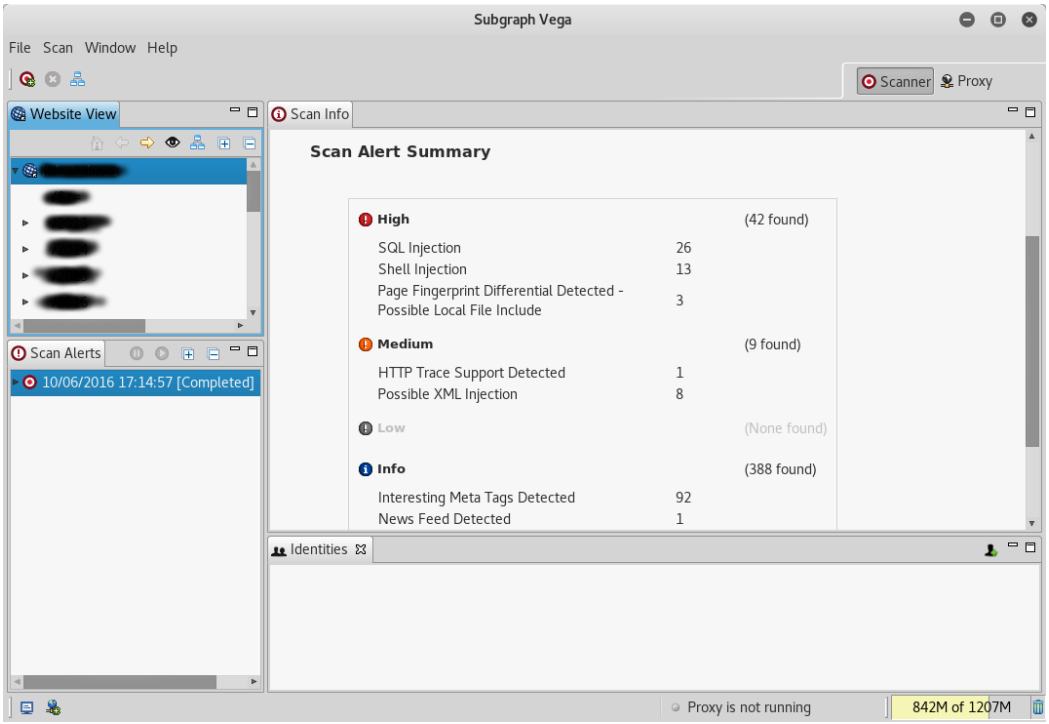

Рисунок 37 – Виведення звіту сканером – Vega

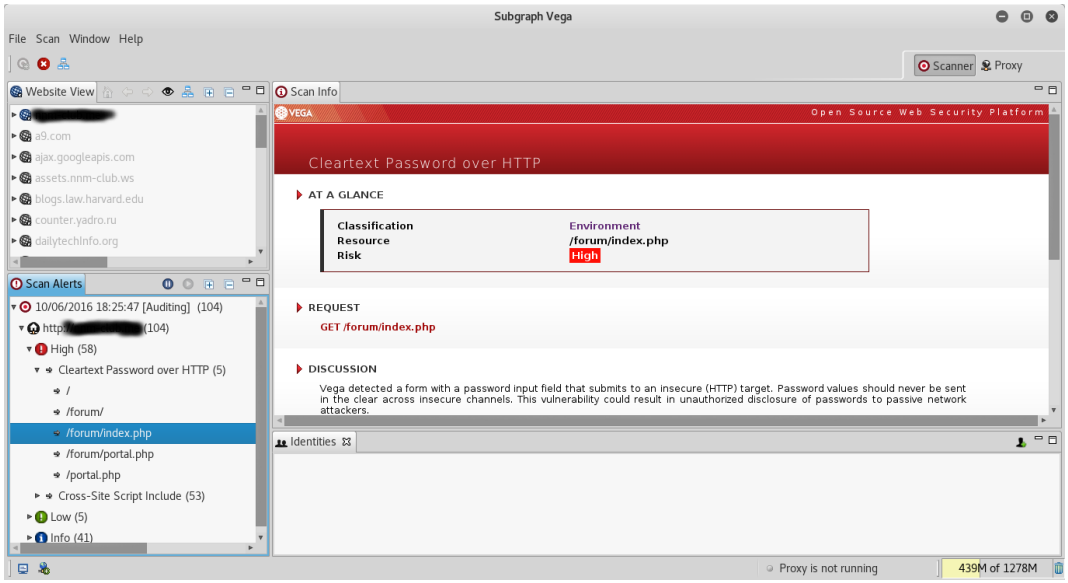

Рисунок 38 – Виведення детального звіту по вразливості сканером Vega

Завдання:

Виконати сканування веб-додатка або веб-ресурсу за допомогою сканера – Vega. Проаналізувати результати сканування. Надати у звіті данні про найзначніші вразливості що потрапили у звіт сканера. Вказати які ще корисні дані і у яких розділах надав сканер.

Лабораторна робота №5

Тема: Пошук вразливостей та чуттєвої інформації у відкритих ресурсах за допомогою засобу Maltego.

Мета: Отримати практичні навички пошуку вразливостей та чуттєвої інформації у відкритих ресурсах за допомогою засобу – Maltego.

Теоретичні відомості

У лабораторній роботі №4 розглядався засіб що дозволяв отримати відомості про можливі вразливості веб-ресурсу або веб-додатку. Однак, часто причиною успішної атаки стає певна інформація що була якимось чином залишена серед документів веб-ресурсу (часто, через необачність розробників або адміністраторів ресурсу). Іноді ж, спеціалісту з інформаційної безпеки необхідно вивчити те яка є інформація доступна для великих мас, виявити чуттєву інформацію і закрити її. До того ж використання таких засобів як Maltego дає можливість зрозуміти чи зможе зловмисник визначити чуттєві 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 і автоматично систематизує цю інформацію у вигляді зручного графа. Більше того, інструментами Maltego слугують так звані «трансформи», що в суті своїй хмарні – сервіси які і взаємодіють з системою що досліджується. Завдяки такому підходу, за допомогою Maltego можливо проводити дослідження декількох вузлів одночасно.

Для запуску Maltego (Рисунок 1) перейдіть у меню додатків Kali Linux у пункт Information Gathering та запустіть додаток «maltegoce».

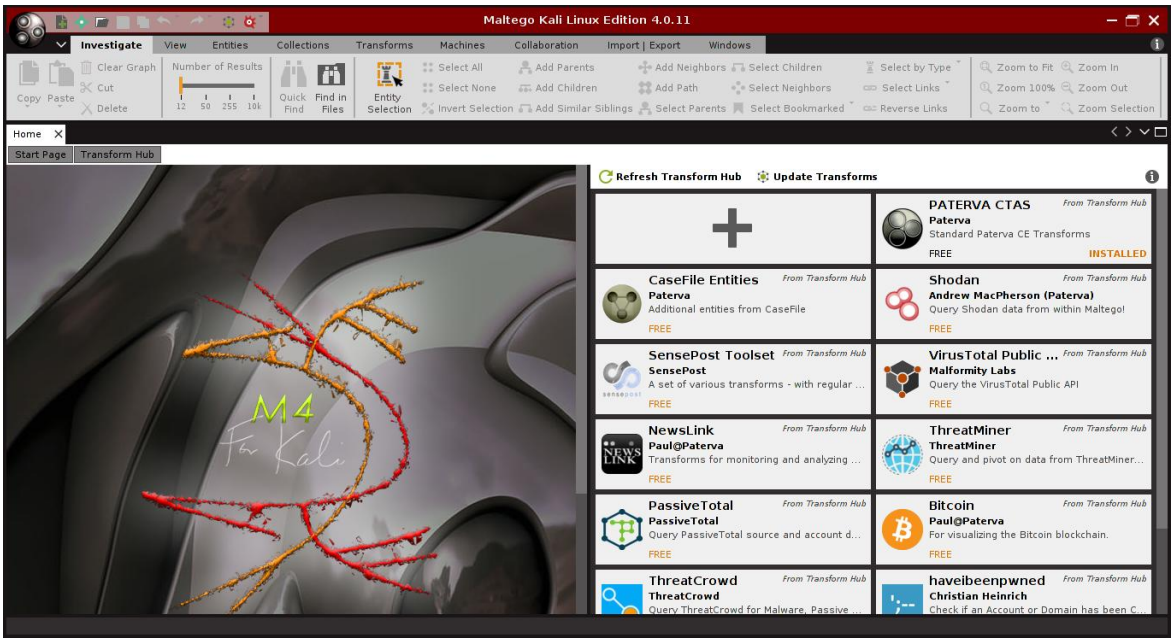

Рисунок 39 – Головне вікно Maltego

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 2).

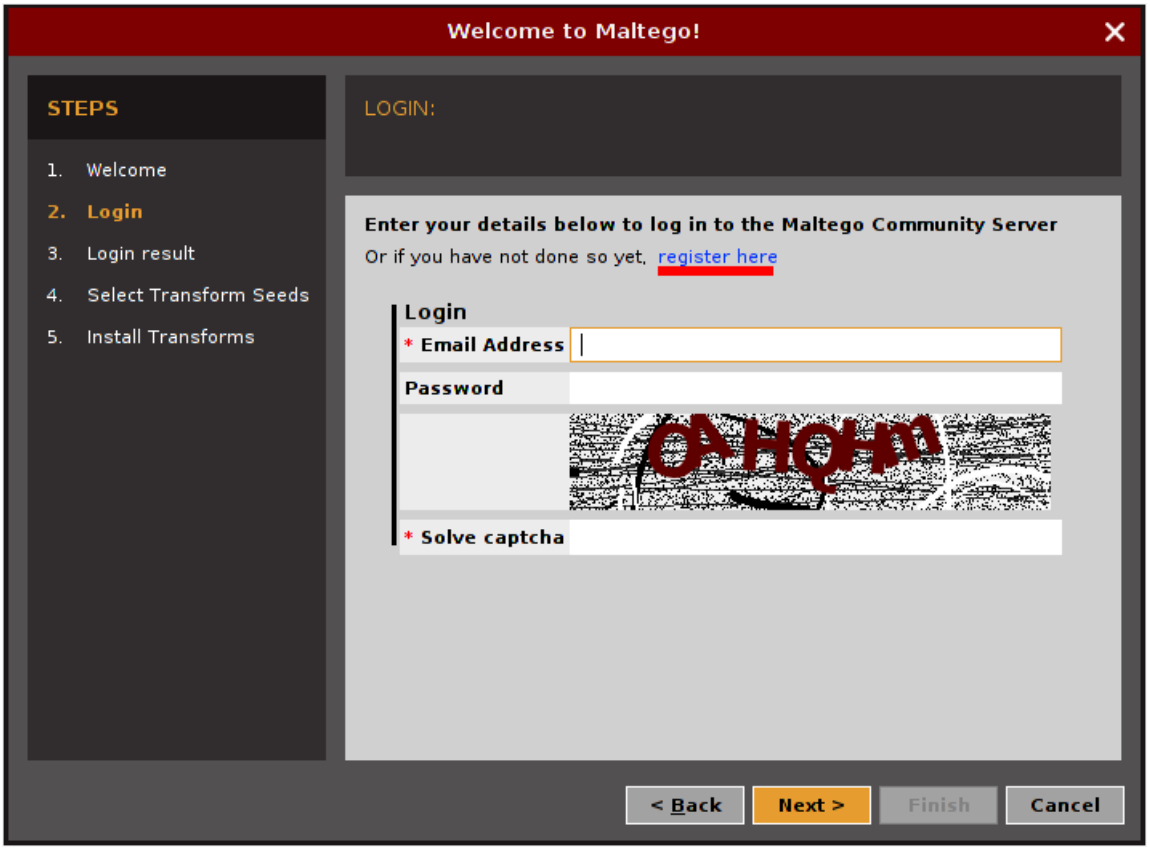

Рисунок 40 – Вхід до облікового запису або його реєстрація

Після входу до свого облікового запису ви перейдете на головне вікно застосунку (Рисунок 1). Для початку роботи створіть новий граф натиснувши відповідну кнопку у верхньому, правому куті (Рисунок 3, виділено червоним маркером).

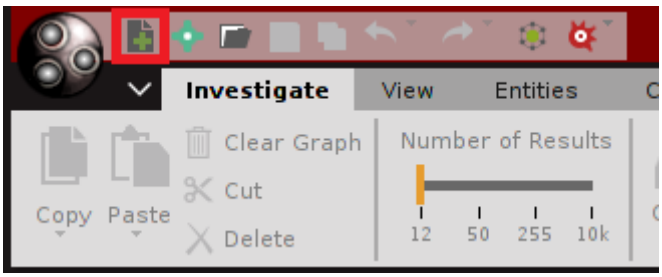

Рисунок 41 – Кнопка створення нового графу (виділено червоним маркером)

Натисніть на пустому місці графу, і у новому вікні оберіть необхідний вид машини (Рисунок 4), натисніть «Next». У новому вікні (Рисунок 5) введіть

необхідні дані для запуску машини і натисніть «Finish». В залежності від типу обраної машини до вашого об’єкта дослідження буде застосовано певний трансформ і виведено певний граф (Рисунок 6 – запущено машину Footprint L1). Натискаючи на вузли графа можливо отримати додаткову інформацію по цьому вузлу. Також, виділивши певний вузол, до нього окремо можливо застосувати певний трансформ, який можливо обрати на лівій панелі – Run View (Рисунок 6). Якщо ж є необхідність створити новий вузол – його тип можливо обрати на лівій панелі – Entity Palette (Рисунок 6).

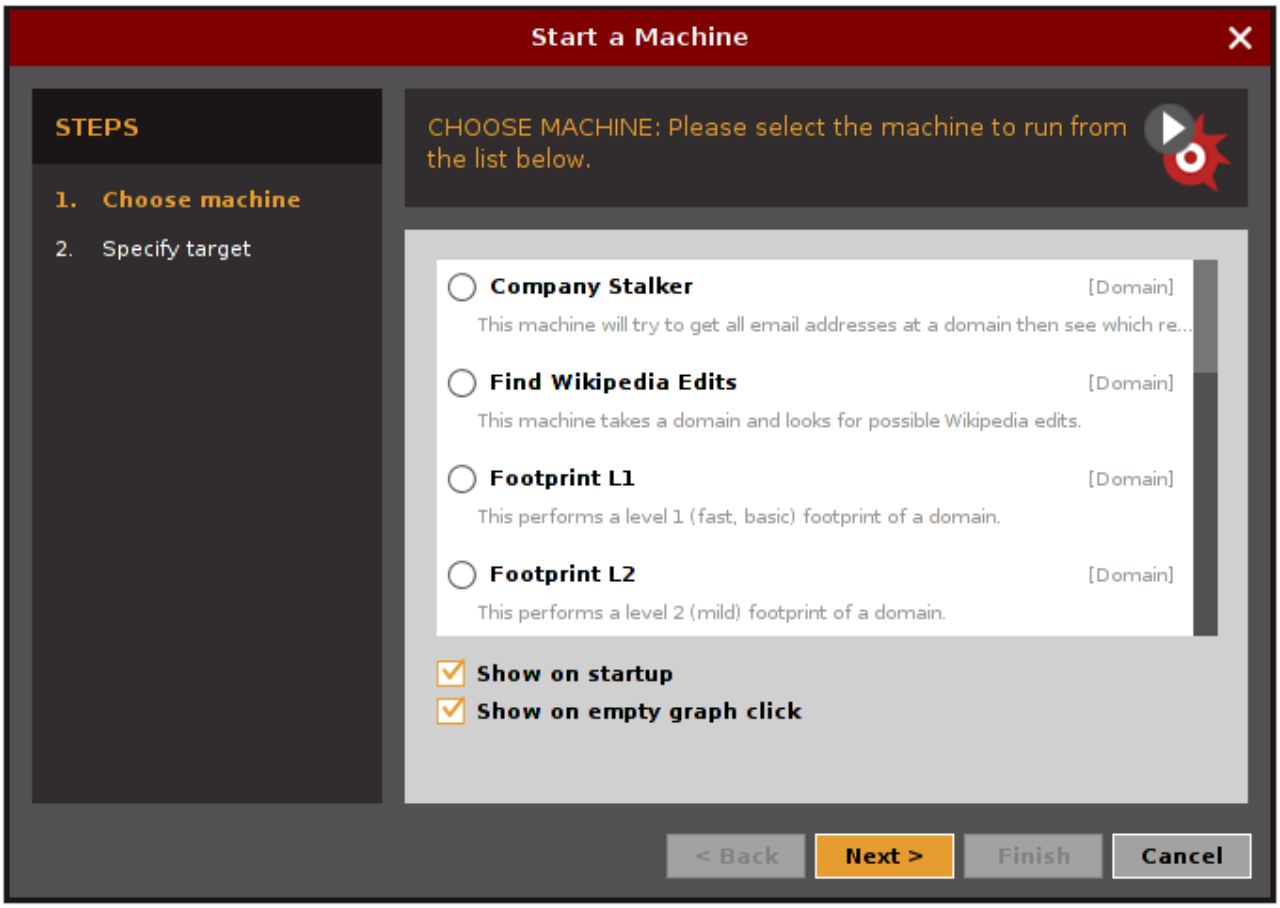

Рисунок 42 – Оберіть тип машини, наприклад Footprint L2 – буде виконано пошук доменів що пов'язано з вашою ціллю

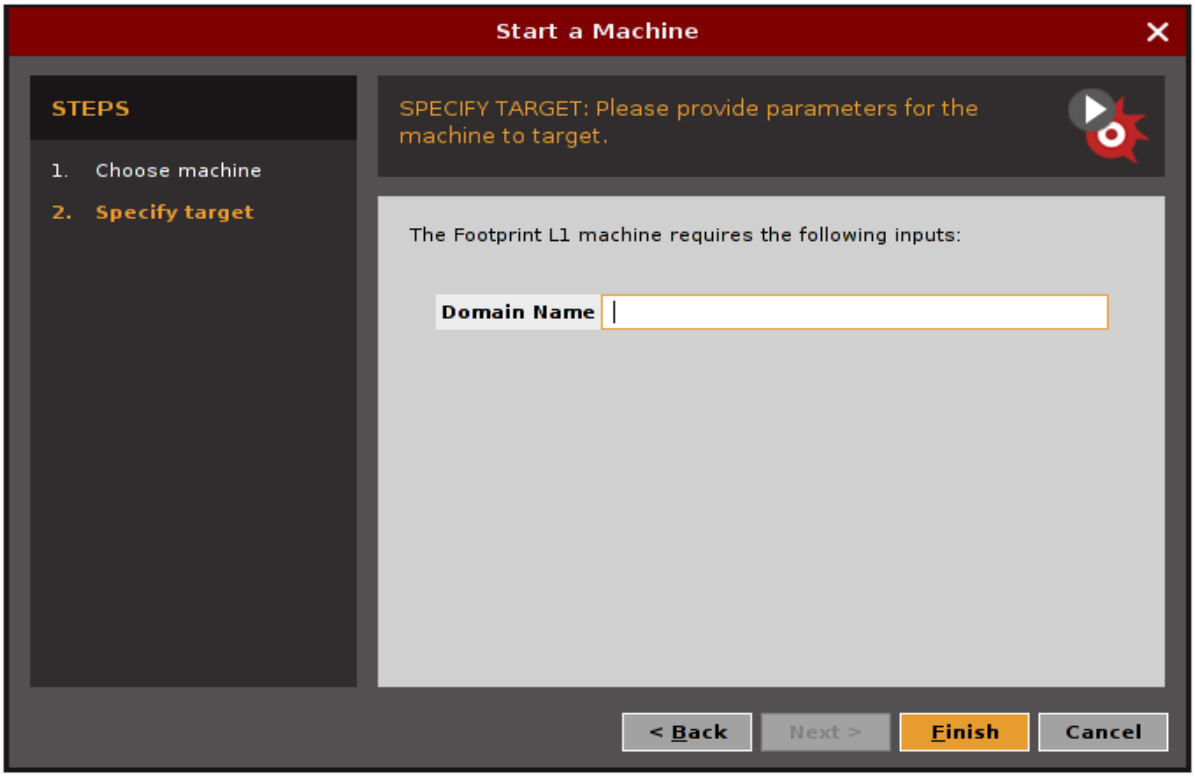

Рисунок 43 – Введіть необхідні данні для запуску машини (Footprint L1 вимагає назву веб-ресурсу – цілі)

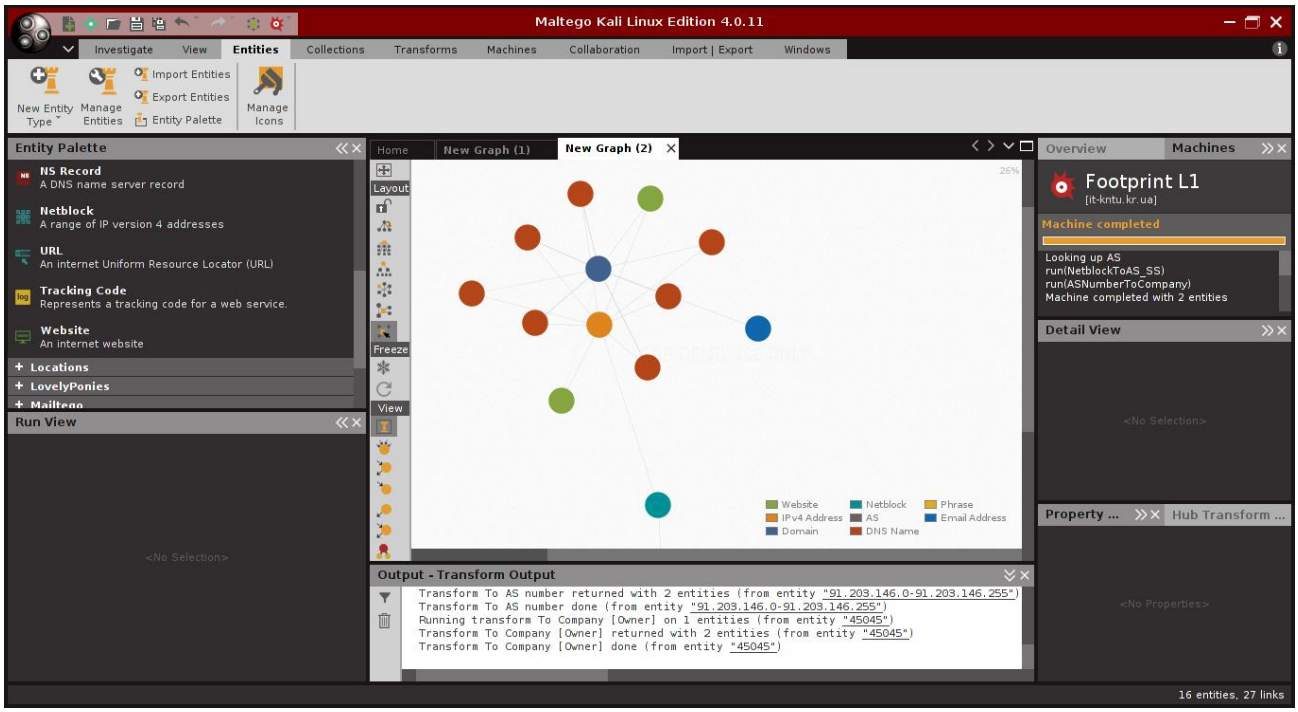

Рисунок 44 – Головне вікно Maltego та граф що було побудовано в процесі роботи машини Footprint L1)

Завдання:

1. Провести дослідження довільно обраного об’єкту з використанням не менше 3х машин.

2. Застосувати до не менш ніж 3х вузлів, не менше ніж 3 трансформи.

3. Обґрунтувати вибір вузлів та трансформів (відобразити у звіті).

4. Проаналізувати отриманий граф, відмітити у звіті точки інтересу обґрунтувавши свій вибір.

5. Визначити наявність чуттєвої інформації (відобразити у звіті можливості їх використання зловмисниками).

6. У звіті провести порівняння між характером інформації що було зібрано завдяки сканеру Vega та засобу Maltego.

Лабораторна робота №6

Тема: Сніфери

Мета: Отримати навички збору технічної та чуттєвої 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 мережеві, вони можуть встановлюватися на usb інтерфейси, одним із різновидів сніферів можливо вважати – кейлогери, сніфери можуть перехоплювати переривання з пристроїв і багато чого іншого. Головною особливістю будь якого сніфера це здатність до пасивного збору інформації.

В даній лабораторній роботі буде розглянуто один з найпотужніших мережевих сніферів – WireShark (Рисунок 1).

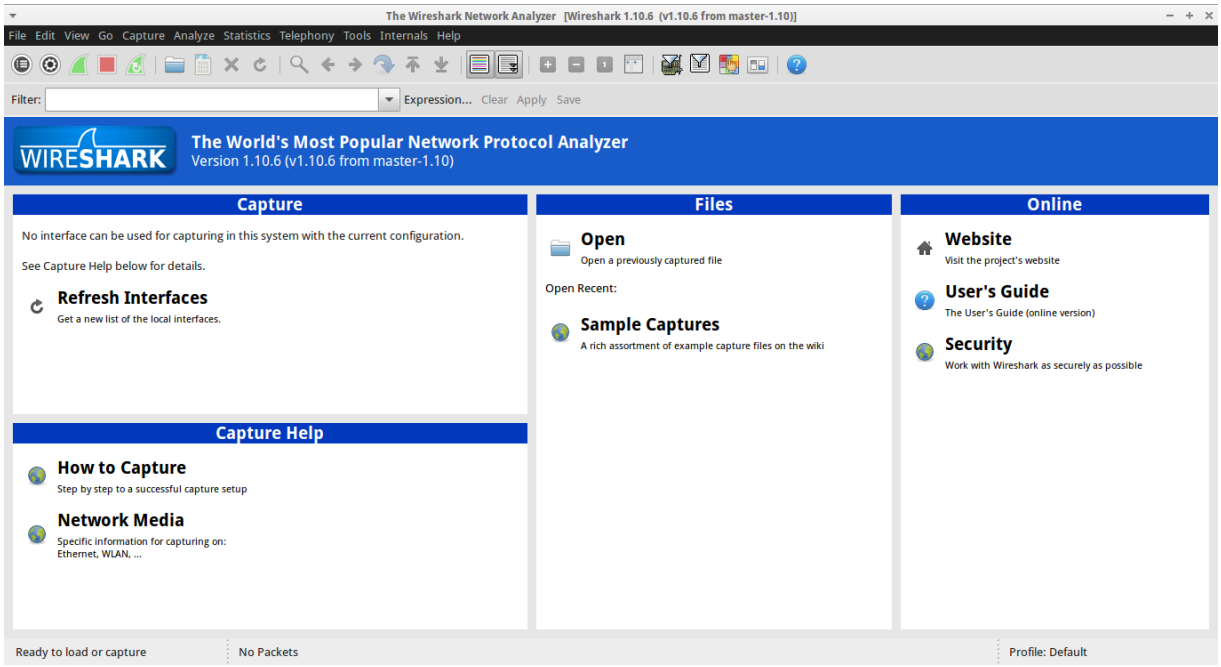

Рисунок 45 – Головне вікно сніферу WireShark

Для початку використання сніферу, оберіть інтерфейс на якому буде працювати сніфер та натисніть старт (помічено червоним маркером на Рисунок 2).

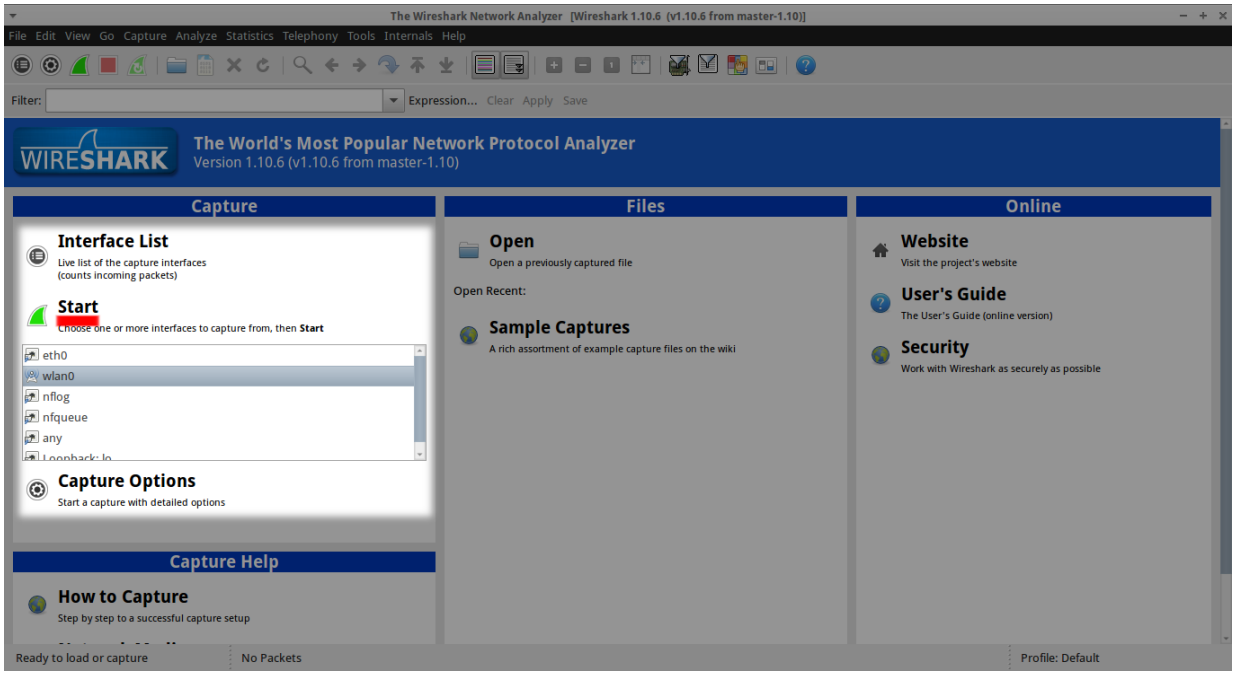

Рисунок 46 – Запуск сніферу, червоним позначено кнопку – старт

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.

Всі фільтри у Wireshark діляться на дві основні групи. Перша – це фільтр захвату (capture), ці фільтри визначають які данні будуть взяті з трафіку і збережені на диск. Друга група – фільтри відображення (display), ці фільтри призначенні для того щоб відфільтрувати інформацію яка необхідна вам зараз на дисплеї, вони не впливають на ті пакети що захватує сніфер, лише на інформацію що відображується на моніторі. Налаштувати фільтри з відповідних меню що викликаються кнопками (Рисунок 3, синім маркером позначено кнопку для меню фільтрів захвату, а червоним для фільтрів відображення)

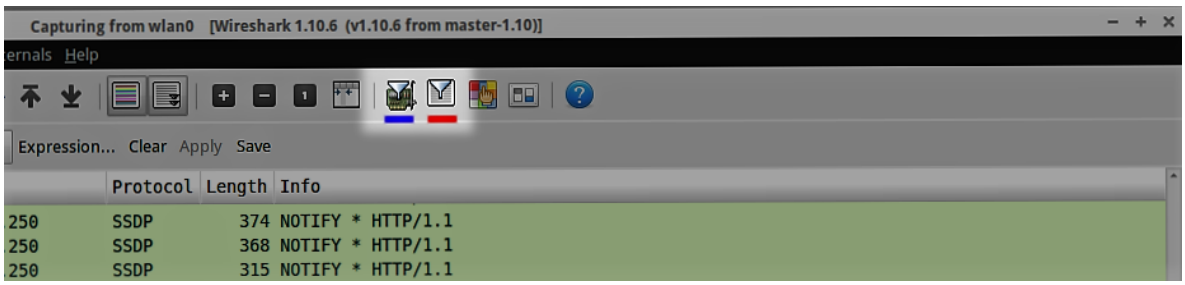

Рисунок 47 – Синім маркером позначена кнопка виклику меню фільтрів захвату а червоним – відображення

Для налагодження фільтрів використовуються вирази, вони можуть бути досить складними. Але для прикладу можна навести наступний вираз (tcp.port == 80) or (udp.port == 80) цей приклад можливо застосувати як до фільтру відображення так і до фільтру захвату, він означає що сніфер буде ігнорувати усі пакети окрім пакети що надсилаються за протоколом TCP на, або з порту 80, або за протоколом UDP. Так, використовуючи відповідні фільтри можливо зосередитись лише на певній інформації яку очікує отримати спеціаліст з ІБ. Вікно налаштування фільтру сніфера зображено на Рисунок 4.

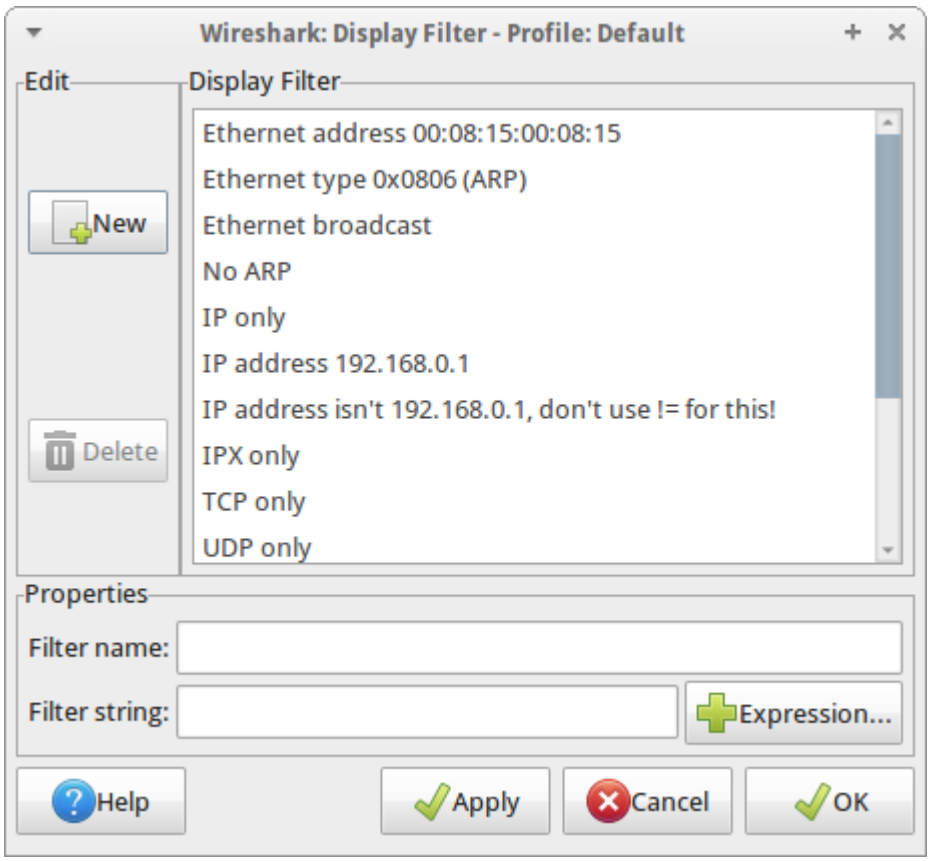

Рисунок 48 – Вікно налаштування фільтру Wireshark

Сніфер може виконувати не лише функцію захвату пакетів, іноді сніфер необхідний лише для моніторингу звернень хосту у мережі. Для цих цілей розроблено сніффер Etherape. Його можливо встановити виконавши команду у консолі від імені root`a apt-get install etherape. Запустивши Etherape від імені користувача оберіть інтерфейс та режим у меню Capture (позначено червоним маркером на Рисунок 5).

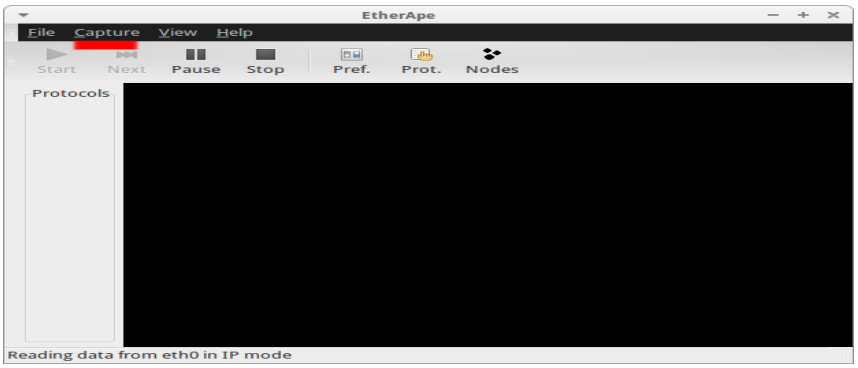

Рисунок 49 – Головне вікно сніферу Etherape, червоним маркером помічене меню Capture

Приклад роботи сніферу зображено на Рисунок 6.

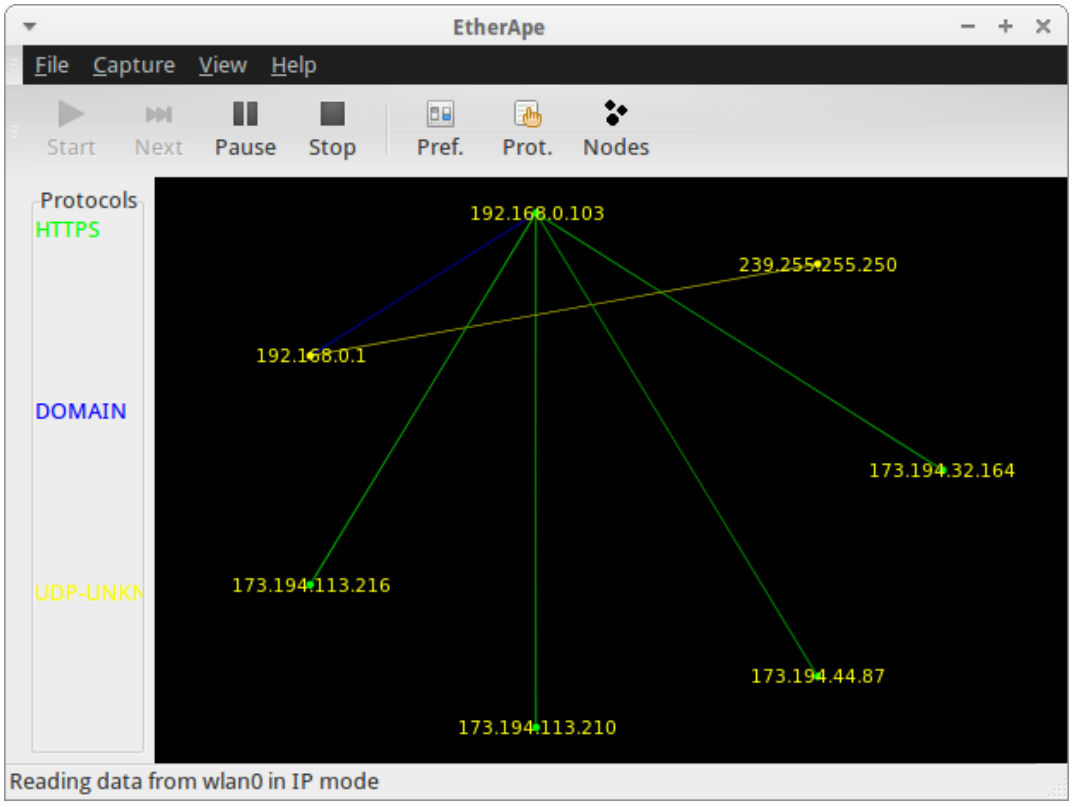

Рисунок 6 – Приклад роботи сніферу

Зверніть увагу що зліва знаходиться панель Protocols там відображаються усі нещодавні протоколи за якими надсилалися данні.

Завдання:

1. 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 з шпигунського програмного забезпечення.

2. Після побудови фільтру проаналізуйте трафік у декількох мережах (мінімум три). Додайте у звіт інформацію про трафік який було отримано у кожній з мереж.

3. Використовуючи 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.

4. Використовуючи сніфер Etherape проаналізуйте зв’язки що виникають при зверненні вашого браузеру до популярних сайтів. Спостереження додайте у звіт. Додайте у звіт пояснення про природу походження цих зв’язків.

Лабораторна робота №7

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

Мета: Отримати навички збору технічної та чуттєвої інформації з безпровідних мкркж Wi-Fi з використанням програмного пакету Aircrack.

Теоретичні відомості

Aircrack – є програмним комплексом 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 – що дозволяє виконати необхідні дії для його вивільнення, та переведення інтерфейс у 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 перехоплює трафік безпровідних мереж. Має великий набір опцій та функцій.

– aireplay-ng – утиліта що 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, або точки доступу, або 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 по 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. Для початку роботи необхідно запустити термінал, і перевести Wi-Fi інтерфейс у режим монітора (Рисунок 1):

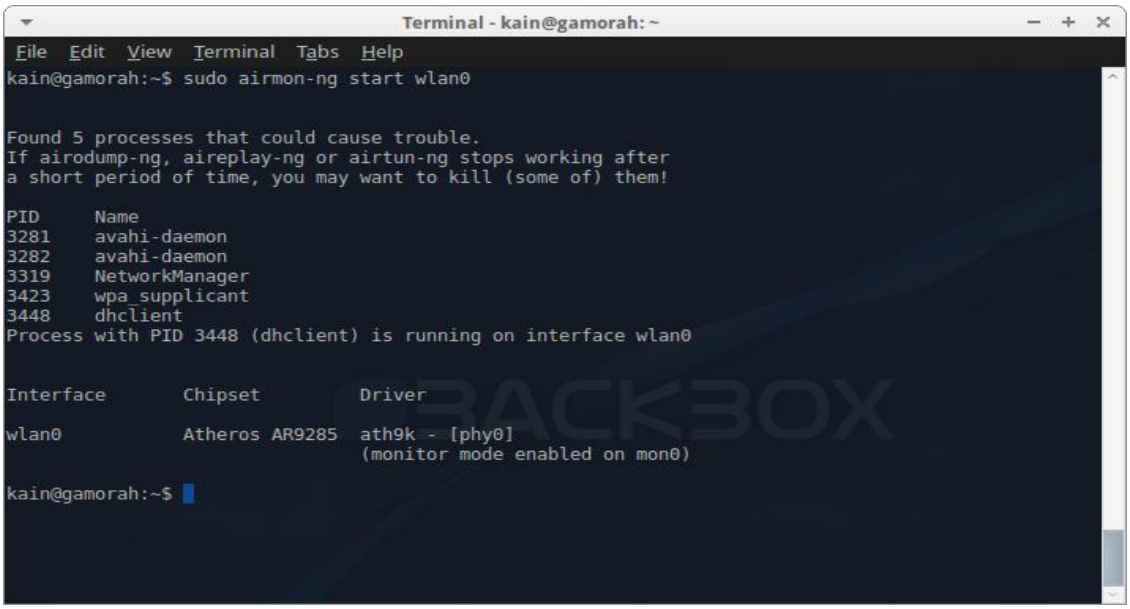

Рисунок 50 – Переведення інтерфейсу wlan0 у режим монітору на інтерфейс mon0

Для того щоб перевести інтерфейс безпровідного мережевого адаптеру у режим монітору виконується команда airmon-ng start [ім’я_інтерфейсу]. Для того щоб передивитися усі інтерфейси що доступні у вашій системі, виконайте команду ifconfig (Рисунок 2).

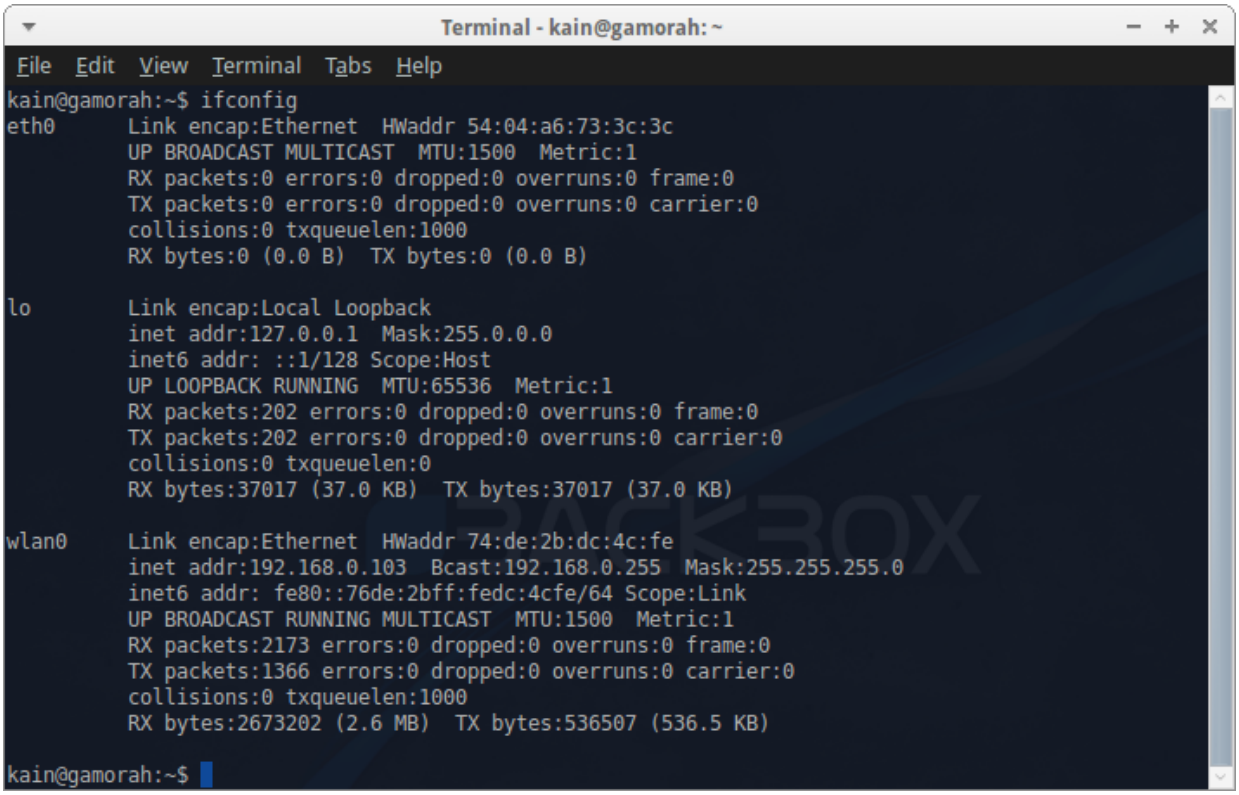

Рисунок 51 – Команда ifconfig виводить усі доступні мережеві інтерфейси системи

Зверніть увагу, що виконувати переключення інтерфейсу у режим монітору необхідно від імені супер-користувача (root`a). Якщо термінал відкрито не від імені root`a, у початок строки з командою введіть додатково sudo і по запрошенню введіть пароль супер-користувача.

Зверніть увагу, і на те що деякі процеси можуть перешкоджати роботі інтерфейсу у режимі монітору, їх список утиліта виведе на початку свого повідомлення . Також можливо скористатися командою airmon-ng check wlan0, вона виведе список усіх процесів що потенційно можуть перешкоджати роботі інтерфейсу у режимі монітору (Рисунок 3).

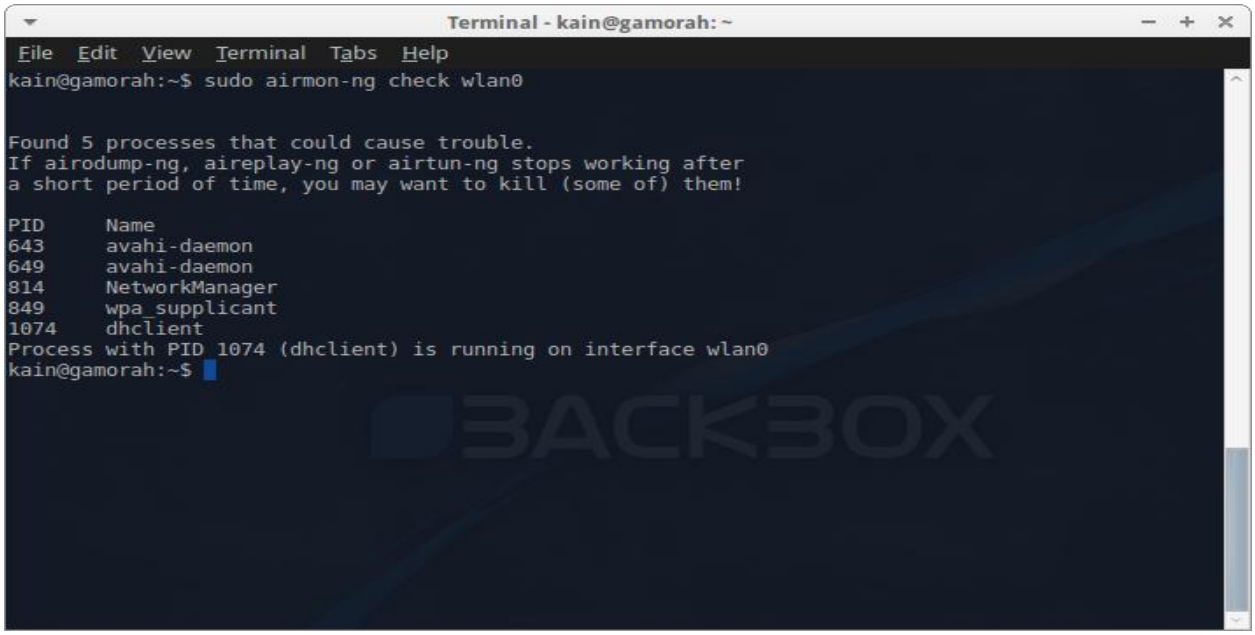

Рисунок 52 – Робота команди airmon-ng check wlan0

Для того щоб позбутися процесів що спричиняють проблеми виконайте команду kill [PID_процесу] від імені супер-користувача. Іноді, цього буває недостатньо, тому можливо 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 ім’я супер-користувача (Рисунок 4).

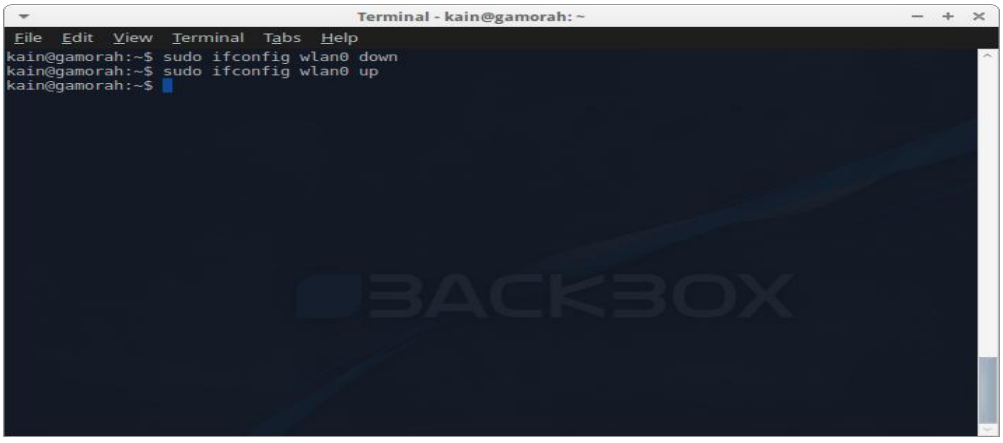

Рисунок 53 – Виконання вимкнення і увімкнення адаптеру, у прикладі це wlan0

Після того як інтерфейс буде переведено у режим монітора airmon-ng створить додатковий інтерфейс який буде зазначено у відповіді утиліти (Рисунок 5, виділено червоним маркером), у випадку з прикладом це – інтерфейс mon0.

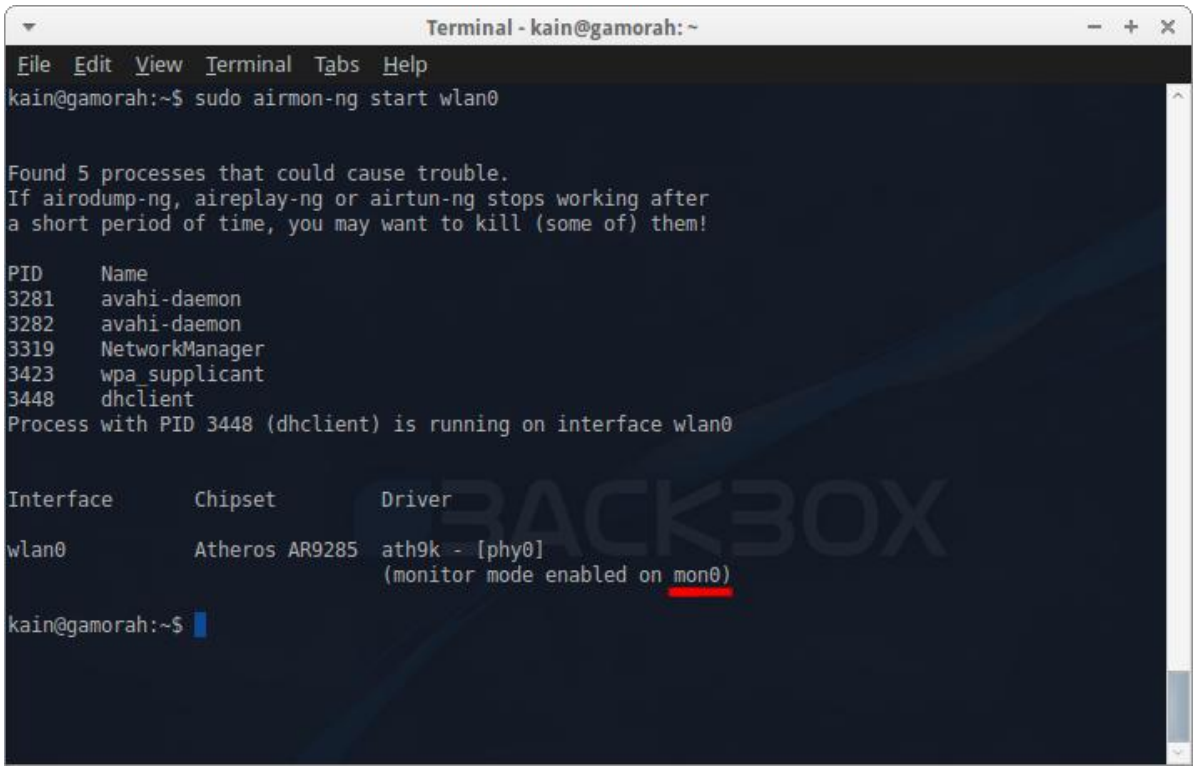

Рисунок 54 – Червоним маркером позначена назва інтерфейсу у режимі моніторy

Саме цей інтерфейс необхідно використати для наступного кроку, а саме запуску утиліти airodump-ng. Яка дозволить переглядати активність точок доступу та їх користувачів у реальному часі, у зоні досяжності безпровідного мережевого адаптеру. Приклад роботи утиліти зображено на Рисунок 6.

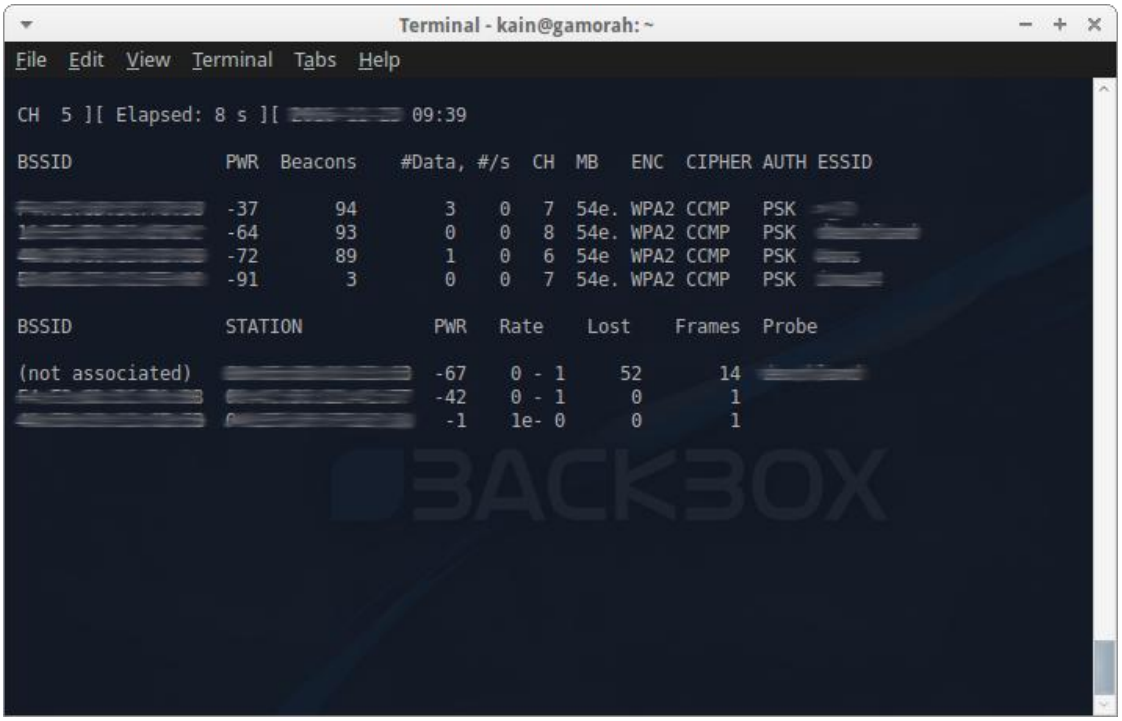

Рисунок 55 – Приклад роботи утиліти airodump-ng

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 кожного фрейму, якщо є сумніви у адекватності даних поля PWR за кількістю beacons-пакетів можливо оцінити рівень сигналу, чим більше beacons – 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

Завдання:

1. Використовуючи комплекс Aircrack, проведіть аналіз ефіру AP що вас оточують.

2. Вкажіть мережі що вас оточують

3. Вкажіть кількість користувачів мереж що ви аналізували

4. Піки активності користувачів

5. Визначте найбільш активних користувачів

6. Визначте користувачів які мають найкращий зв’язок з AP

7. Спробуйте визначити чи не використовує хтось певну мережу не санкціоновано, що може на це вказувати?

8. У звіті відобразіть дані про точки та клієнтів у наступному форматі:

-BSSID (AP):

--MAC-клієнта 1

---час початку роботи та закінчення

---пік трафіку (час та кількість пакетів)

---список probes

--MAC-клієнта …

--MAC-клієнта n

9. Спробуйте визначити які AP вимикаються користувачами за їх відсутності, а які працюють цілодобово, наприклад використавши ключ --uptime (airodump-ng --uptime mon0)

10. 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

11 Виконайте запис трафіку точки та клієнту у файл за допомогою ключа –w. Додайте частково його вміст у звіт, поясніть які данні в ньому містяться.

Лабораторна робота №8

Тема: Розгортання pen-test станції

Мета: Навчитись виконувати налаштування віртуальних мережевих адаптерів.

Теоретичні відомості

Для безпечного виконання подальших лабораторних робіт необхідно розгорнути робочі станції до яких буде безпечно виконувати впливи що будуть описані далі.

Для підготовки спеціалістів по проведенню тестів на проникнення та підвищенню їх кваліфікації використовуються спеціальні версії операційних систем – DVL (Damn vulnerable Linux), DVW (Damn vulnerable Windows) та DVWA (Damn vulnerable web app).

DVL – зазвичай, поширюються безкоштовно. Для виконання лабораторних робіт рекомендується використовувати дистрибутив який спеціально розроблено для тренування спеціалістів з тестів на проникнення із використанням Metasploit framework – “Metasploitable”. Дистрибутив можливо завантажити безкоштовно з офіційного сайту розробника rapid7.com. Для цього необхідно пройти просту процедуру реєстрації (рисунок 1).

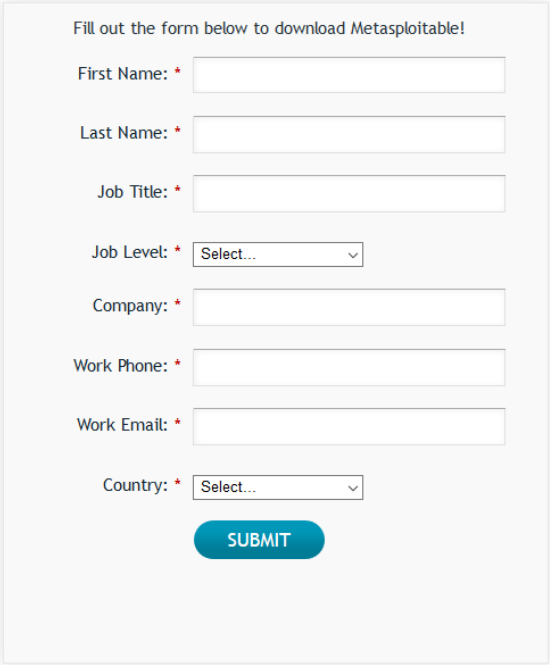

Рисунок 56 – Форма реєстрації на rapid7

Після реєстрації стане можливим завантаження zip архіву з віртуальною машиною DVL Metasploitable.

Окрім операційної системи Linux для виконання лабораторних робіт знадобиться ОС Windows. Завантаження образів віртуальних машин доступне за посиланням – посилання 2 після переходу по посиланню необхідно обрати відповідну версію Windows (Рисунок 2) та почати завантаження. Для завантаження віртуальної машини з Windows 10 необхідно перейти за наступним посиланням – посилання 3.

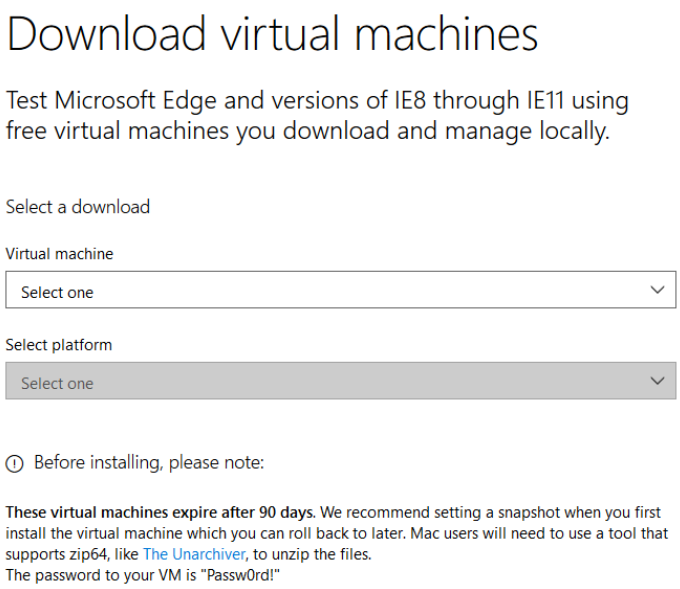

Рисунок 57 – Опції завантаження віртуальних образів ОС Windows

Після завершення завантаження необхідно завантажити програмне забезпечення для запуску віртуальних машин. В рамках занять рекомендується використовувати VMware Player, розповсюджується безкоштовно і відповідає вимогам сумісності із завантаженими, до цього, образами ОС. Завантаження VMware Player можливе за посиланням 4.

Після завантаження всіх необхідних матеріалів можна перейти до налаштувань самого середовища для подальшого проведення тестів на проникнення (pen-tests). Для цього, спочатку, виконайте інсталяцію VMware Player після чого запустіть його (Рисунок 3).

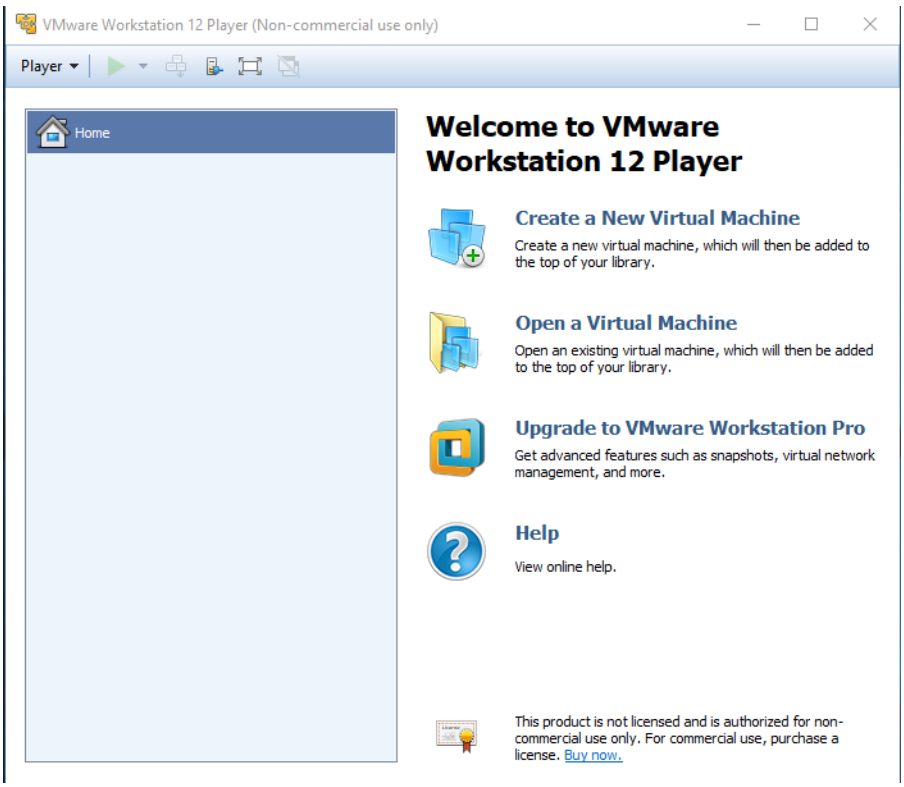

Рисунок 58 – VMware Player

Розпакуйте zip архів з необхідною ОС у теку за вашим бажанням.

Після запуску VMware Player натисніть “Open a Virtual Machine” (Рисунок 4).

Рисунок 59 – Відкрити віртуальну машину (позначено червоним маркером)

У стандартному вікні “Відкрити файл” перейдіть у теку в яку було розпаковано віртуальну машину, оберіть *.vmx файл та відкрийте його.

Після чого стане можливим запуск відповідної віртуальної машини (Рисунок 5).

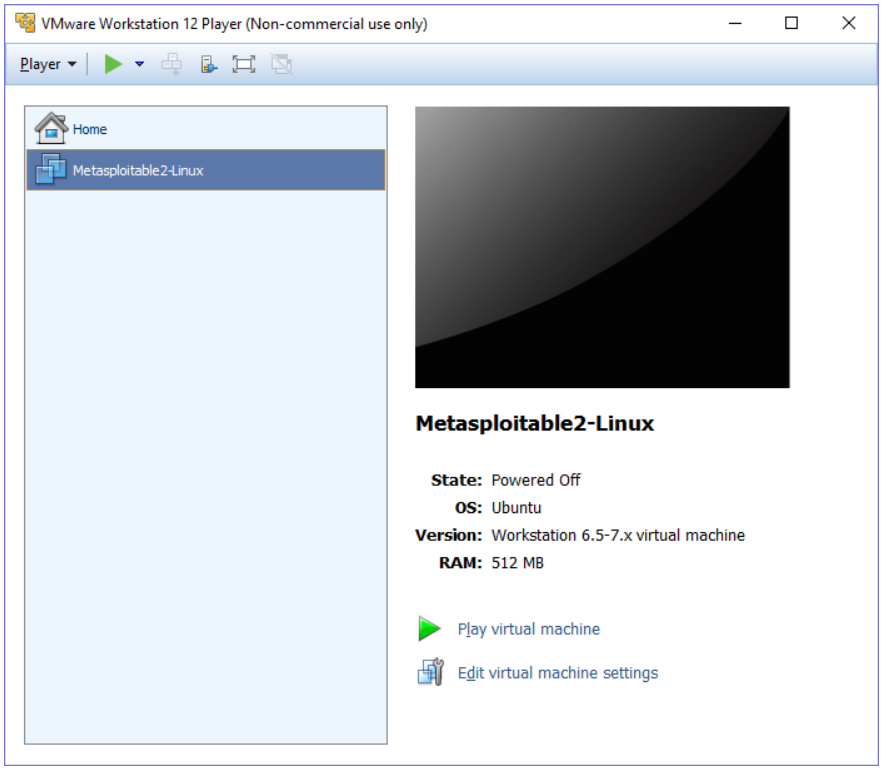

Рисунок 60 – Готова до запуску віртуальна машина з Metasploitable_2 Linux

Для запуску віртуальної машини натисніть “Play virtual machine” (Рисунок 6).

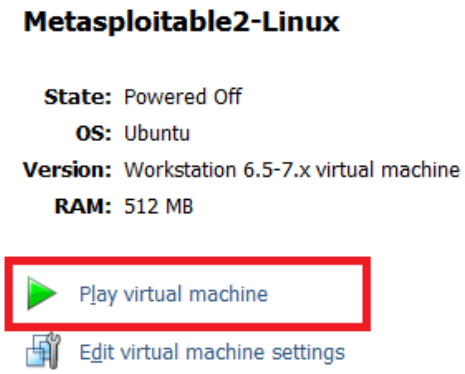

Рисунок 61 – Play virtual machine (Позначено червоним маркером)

Після того як віртуальну машину буде додано, необхідно налаштувати її обладнання. Для цього необхідно натиснути “Edit virtual machine settings” (Рисунок 7)

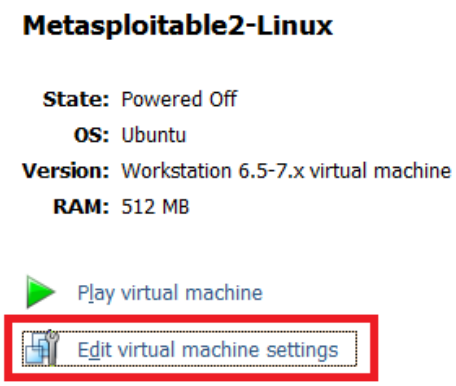

Рисунок 62 – Edit virtual machine settings (позначено червоним маркером)

Після чого з’явиться вікно налаштувань віртуальної машини та її обладнання (Рисунок 8).

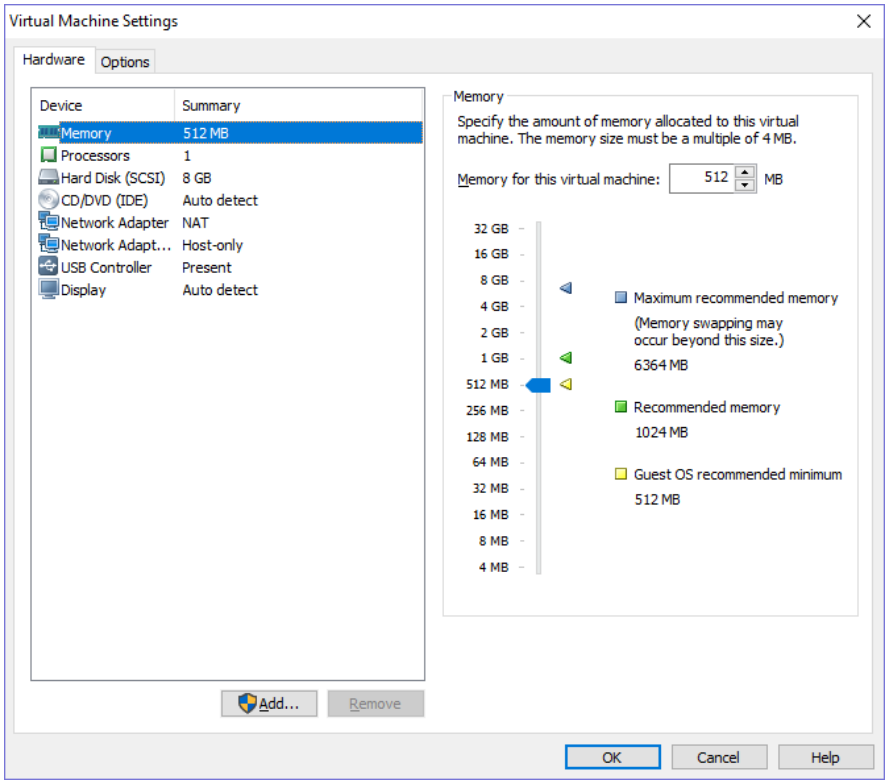

Рисунок 63 – Налаштування віртуальної машини та її обладнання

Завдання:

1. Завантажити віртуальну машину Metasploitable

2. Завантажити віртуальну машину Windows.

3. Завантажити VMware Player.

4. Розгорнути завантажені віртуальні машини.

5. Виконати налаштування віртуальних мережевих адаптерів.

6. Описати налаштування мережевих адаптерів та обґрунтувати вибір їх режиму роботи, опис та обґрунтування надати у звіті.

7. Додати у звіт скріншоти ключових моментів роботи.

8. Додати у звіт інформацію про 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

Після розгортання віртуальних машин для проведення тестування необхідно підготовити Metasploit framework. Для запуску Metasploit відкрийте/перейдіть до терміналу та виконайте команду “msfconsole”. Після запуску Metasploit виведе банер та данні про свої модулі (Рисунок 1).

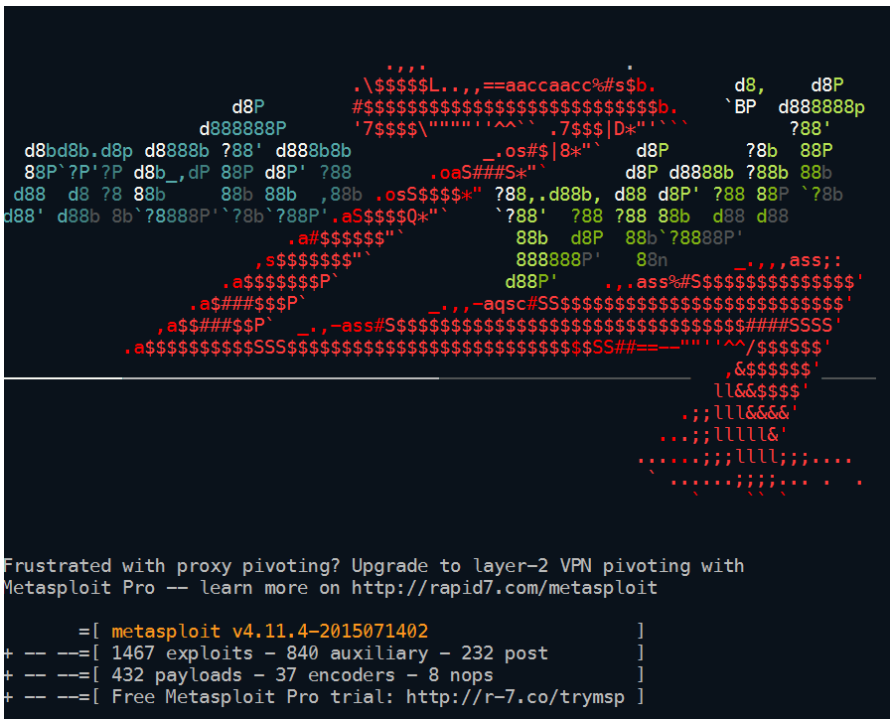

Рисунок 64 – Банер Metasploit та дані про модулі

Після запуску Metasploit необхідно впевнитись, що база даних, в якій буде зберігатися інформація про ваші цілі та про данні гешів, паролі, логіни, сервіси правильно підключена. Для цього необхідно ввести команду “db_status”. У разі, якщо, база даних підключена вірно буде виведено відповідне повідомлення (Рисунок 2).

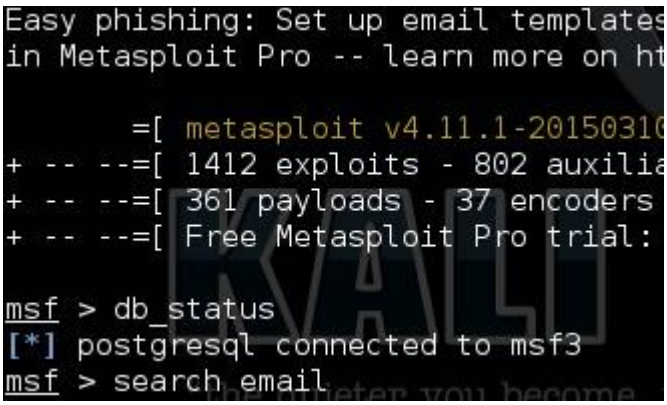

Рисунок 65 – Відповідь про успішне підключення бази даних

У разі якщо БД не була підключена необхідно спробувати підключити її вручну, для цього введіть команду “db_connect” (Рисунок 3).

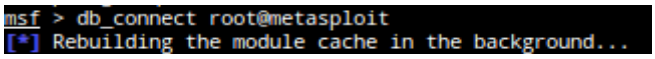

Рисунок 66 – Ручне підключення до БД з Metasploit

У тому разі, якщо все ж, підключення встановити не вдалося необхідно ініціалізувати БД для цього необхідно виконати команду “msfdb init” від імені root, і не з консолі Metasploit.

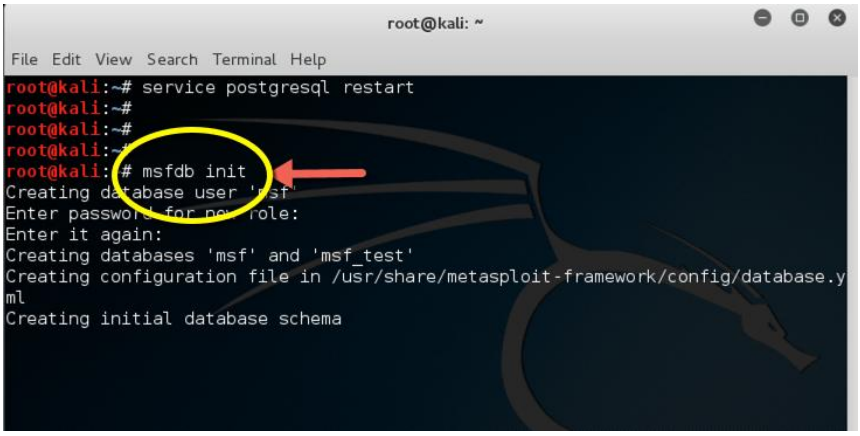

Рисунок 67 – Робота команди msfdb init

Після вдалої ініціалізації бази даних необхідно перезапустити Metasploit. Додатково, переконайтесь що сервіс “postgresql” запущено.

Після вдалого підключення до БД, можливо виконати базові налаштування глобальних змінних фреймворку, таких як, наприклад “rhost”, “lport” та інші. Подробиці цих налаштувань можливо передивитися за допомогою команди “help”. Встановити значення глобальної змінної можливо використовуючи “setg <ім’я_змінної>”.

Завдання:

1. Виконати запуск Metasploit
2. Налаштувати підключення до БД
3. Встановити базові глобальні змінні, надати відомості про них у звіті.
4. Обґрунтувати встановленні значення глобальним змінним
5. Надати у звіті відомості про основні команди Metasploit (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 данні що будуть знайдені будуть записані у БД яка була підключена при виконанні лабораторної роботи №8.

Згодом, після того як сканування буде завершене, дані сканування будуть додані у БД стане можливим швидко та у зручному форматі отримати данні що цікавлять викликаючи команди, на кшталт “hosts” – яка виведе на екран дані про хости які були просканові (Рисунок 1).

```
msf > hosts

Hosts
=====

address        mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------        ---  ----  -------  ---------  -----  -------  ----  --------
192.168.0.100             Linux                      server

msf >
```

Рисунок 68 – Приклад використання команди hosts

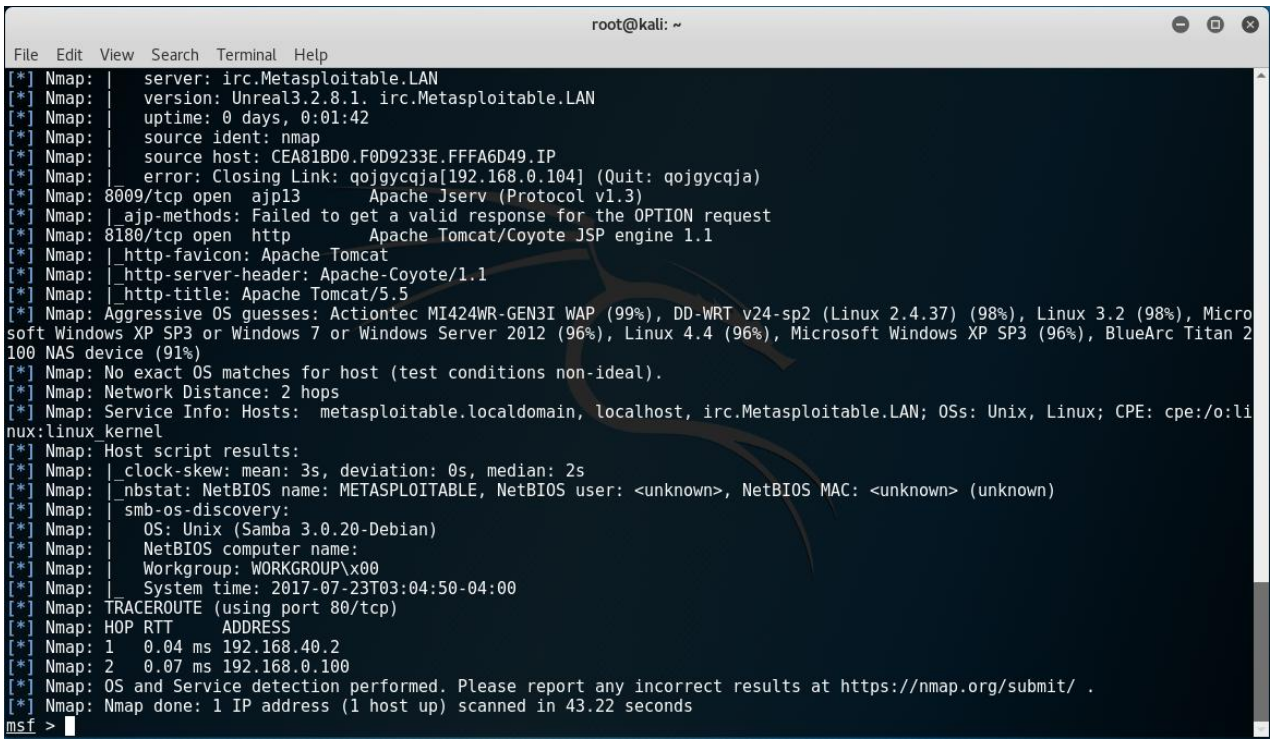

Рисунок 2 – Використання db_nmap з ключом -A у Metasploit

Для того щоб данні сканування було додані у БД необхідно використати команду “db_nmap” разом із необхідними ключами та налаштуваннями які розглядались у відповідній лабораторній роботі (Рисунок 2).

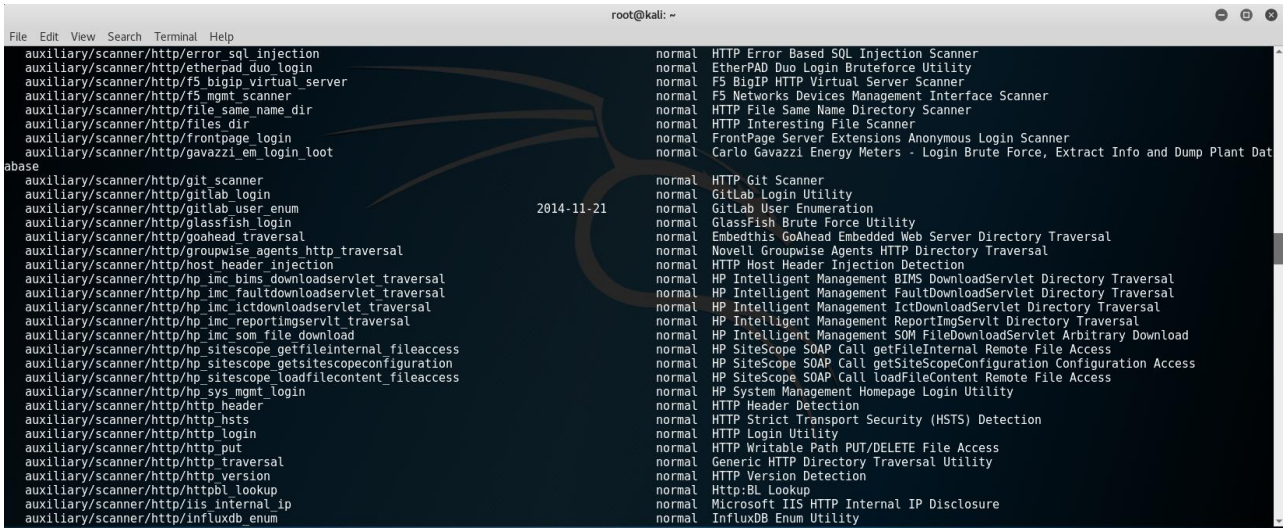

Рисунок 3 – Використання команди search з ключовим словом scanner

Окрім цього, фреймворк включає в собі більш специфічні сканери, які 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) фреймворку. Для перегляду засобів фреймворку зручно використовувати команду “search” – “search <ключове_слово>”, наприклад для перегляду сканерів – “search scanners” (Рисунок 3).

Для того щоб обрати один з 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 можливо 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 4).

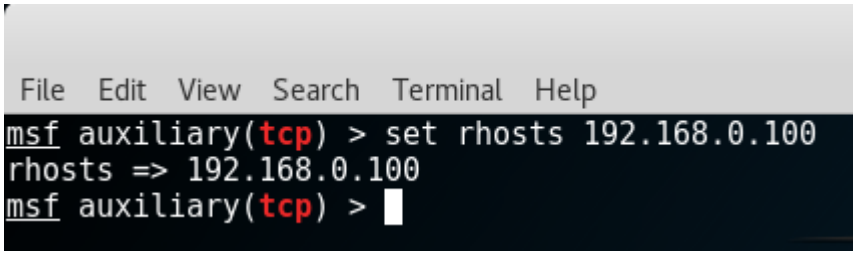

Рисунок 4 – Перегляд детальної інформації про модуль (show info)

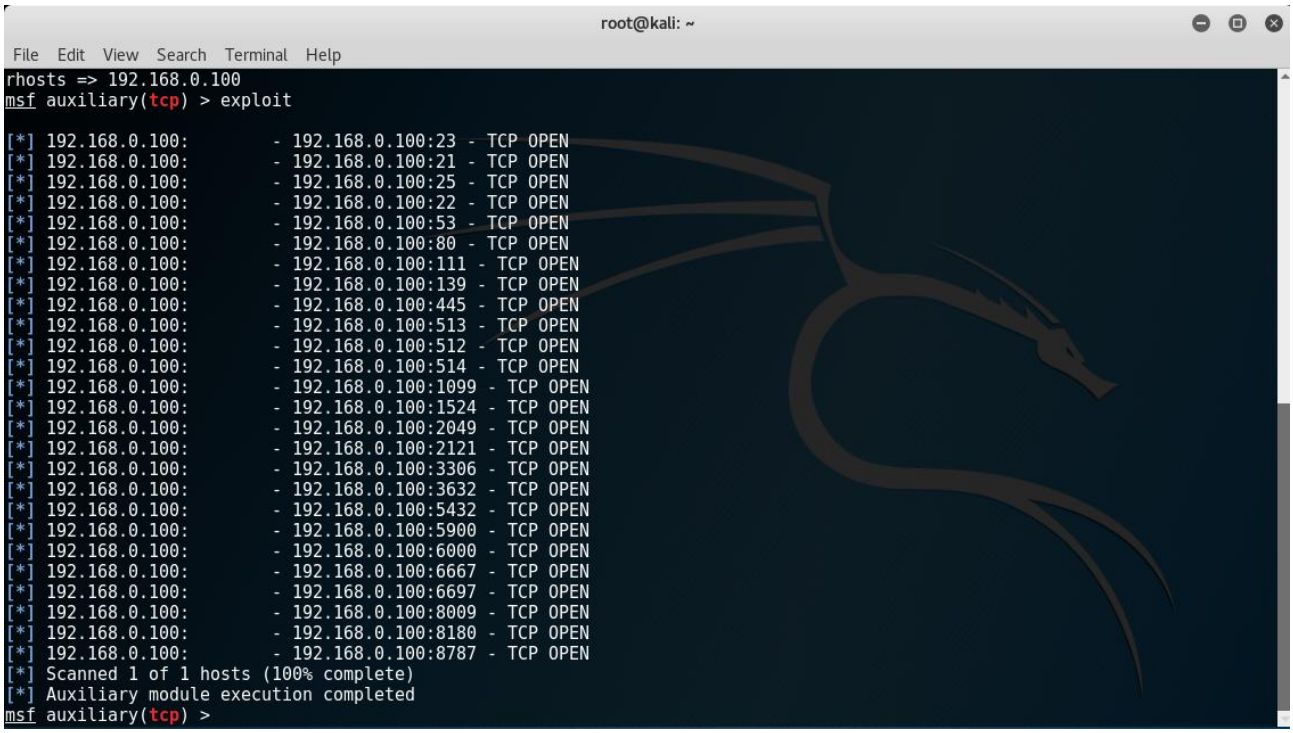

Рисунок 5 – Встановлення значення опції

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 опції використовується команда “set”. Для встановлення значення глобальної опції – “setg”. Приклад:

Для запуску роботи поточного модуля необхідно використати команду “exploit” або “run”. Вивід модуля “auxiliary/scanner/portscan/tcp” зображено на Рисунок 6.

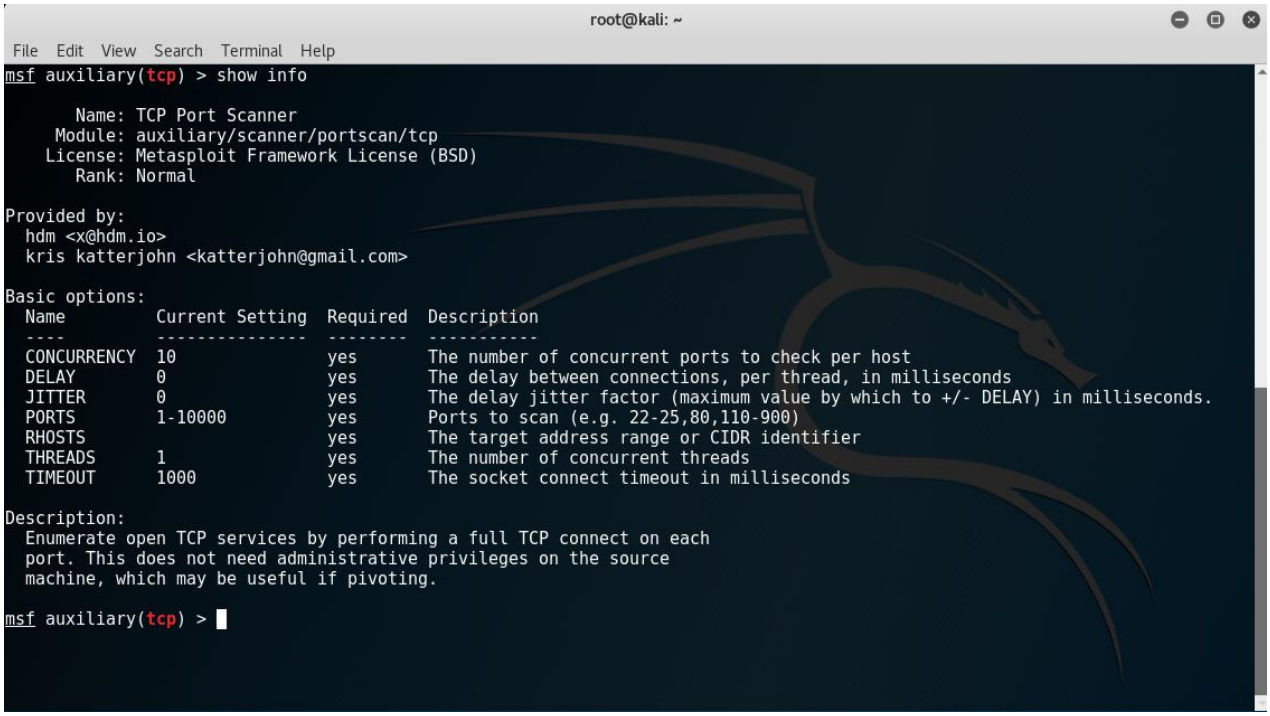

Рисунок 6 Результат роботи сканера auxiliary/scanner/portscan/tcp

Завдання:

1. Виконати сканування однієї або двох віртуальних машин що були завантажені у попередніх лабораторних роботах.

2. Виконати сканування за допомогою “db_nmap”.

3. Виконати сканування за допомогою не менш ніж трьома додатковими модулями.

4. Зберегти результати сканування у БД

5. У звіт додати результати сканування модулів та “db_nmap”, надати коротку характеристику результатів роботи 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 по її збору та зберіганню, що дає змогу більш ефективно її аналізувати.

Однією з технік по 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, 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 можливо 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 Рисунок 1.

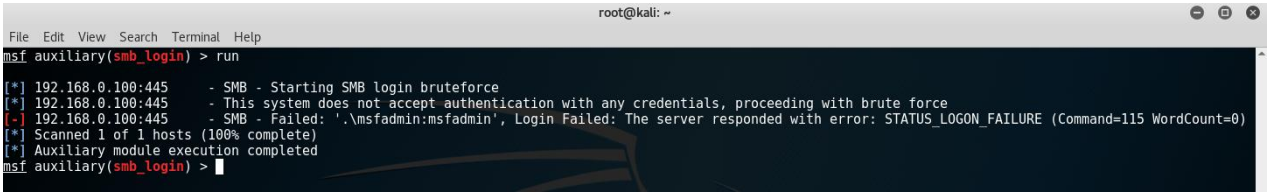

Рисунок 69 – Приклад роботи модуля що реалізує техніку "Login attempt"

Ще однією з поширених і критичних вразливостей є погано конфігурований VNC сервіс. Серед додаткових засобів Metasploit є спеціалізовані сканери для цього сервісу. Знайти їх можливо 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 цього модуля зображено на Рисунок 2.

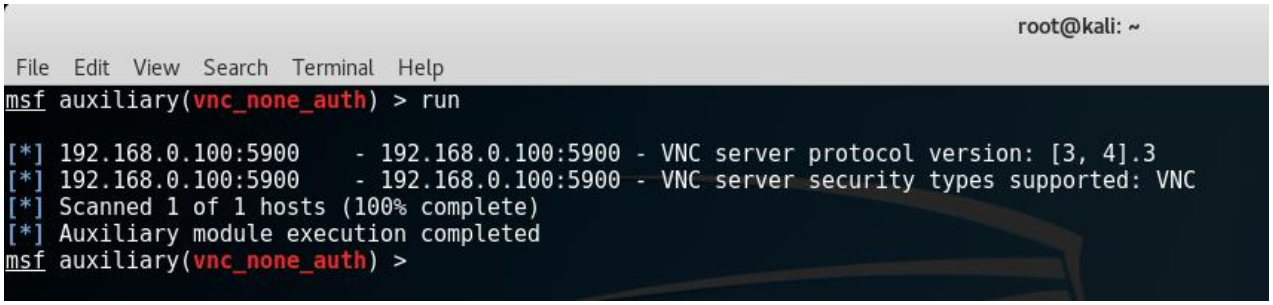

Рисунок 70 – Приклад роботи модуля з VNC сервісом

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

Плагін “wmap” можливо завантажити безпосередньо використавши команду “load” (“load wmap”). Після чого з ним можливо працювати.

Для початку, необхідно створити запис про новий сайт за допомогою команди “wmap_sites” з ключом “-a” (приклад: “wmap_sites –a

http://somesite.com”). Після чого, вказати цілі для кроулера використовуючи команду “wmap_targets” з ключом “-t” (приклад: “wmap_targets –t http://somesite.com/login”). Додаткове визначення цілей (сторінок сайту (веб-додатку)), дає можливість зменшити час сканування, і знижує кількість запросів у сторону сервера, що у свою чергу – знижує шанс буди виявленим. 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 3.

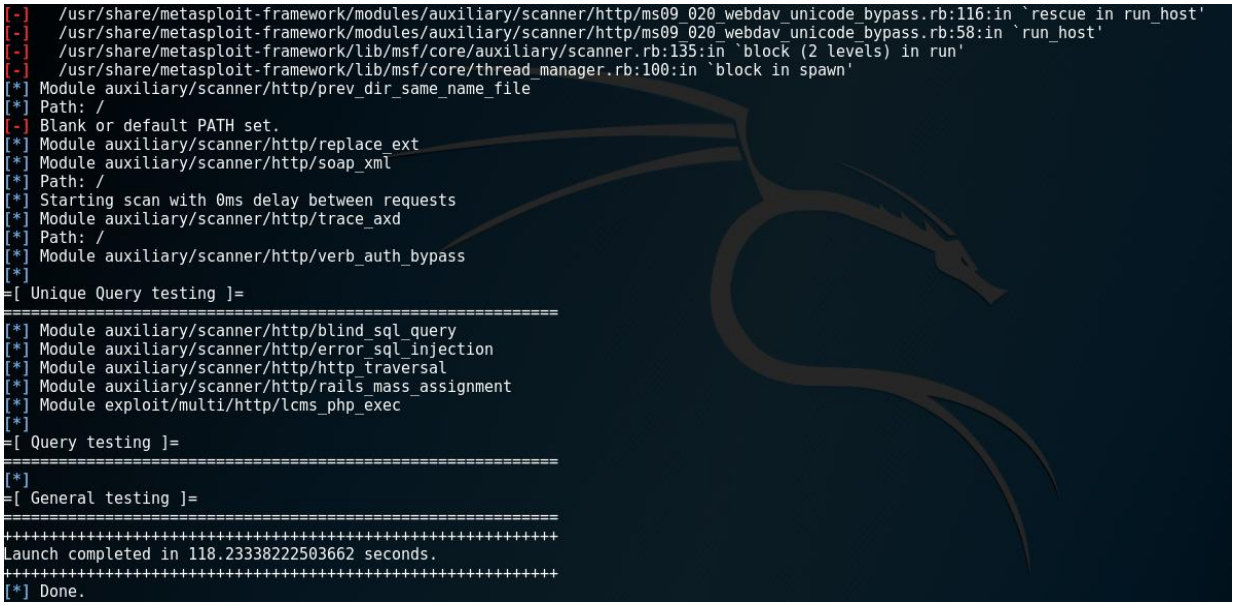

Рисунок 71 – Приклад роботи wmap

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

Завдання:

1. Виконати сканування типу “Login attempt” відносно трьох різних сервісів на одній з двох раніше завантажених віртуальних машин (рекомендовано Metasploitable)

2. Виконати сканування VNC сервісу

3. Виконати сканування веб-додатку (рекомендовано використовувати веб-додаток що розгорнуто на віртуальній машині з Metasploitable, сканування плагіном wmap досить агресивне і може зашкодити додаткам які скануються)

4. Додати у звіт результати сканувань

5. Додати у звіт опис/аналіз результатів сканувань

Лабораторна робота №12

Тема: Енкодери

Мета: Навчитися використовувати енкодери для обходу захисту антивірусних програм

Теоретичні відомості

Пейлоад – термін що використовується у Metasploit. Це програмний код, що буде виконано безпосередньо на стороні цілі. Тому важливо щоб цей код не було помічено антивірусним програмним забезпеченням. Всі операції по генеруванню пейлоаду виконується командою “generate” з використанням необхідних опцій та флагів.

Існують два напрямки приховування пейлоаду від антивірусних програм. Перший полягає у заміні байтів виконуваного файлу. Для цього команду “generate” необхідно виконати з флагом “-b”. Приклади використання цього флагу наведено на Рисунок 1 та 2.

```
msf payload(exec) > generate
# windows/exec - 193 bytes
# http://www.metasploit.com
# VERBOSE=false, PrependMigrate=false, EXITFUNC=process,
# CMD=shutdown
buf =
"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50" +
"\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26" +
"\x31\xff\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7" +
"\xe2\xf2\x52\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78" +
"\xe3\x48\x01\xd1\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3" +
"\x3a\x49\x8b\x34\x8b\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01" +
"\xc7\x38\xe0\x75\xf6\x03\x7d\xf8\x3b\x7d\x24\x75\xe4\x58" +
"\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3" +
"\x8b\x04\x8b\x01\xd0\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a" +
"\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb\x8d\x5d\x6a\x01\x8d" +
"\x85\xb2\x00\x00\x00\x50\x68\x31\x8b\x6f\x87\xff\xd5\xbb" +
"\xf0\xb5\xa2\x56\x68\xa6\x95\xbd\x9d\xff\xd5\x3c\x06\x7c" +
"\x0a\x80\xfb\xe0\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x53" +
"\xff\xd5\x73\x68\x75\x74\x64\x6f\x77\x6e\x00"
msf payload(exec) >
```

Рисунок 72 – Генерація пейлоаду без змін

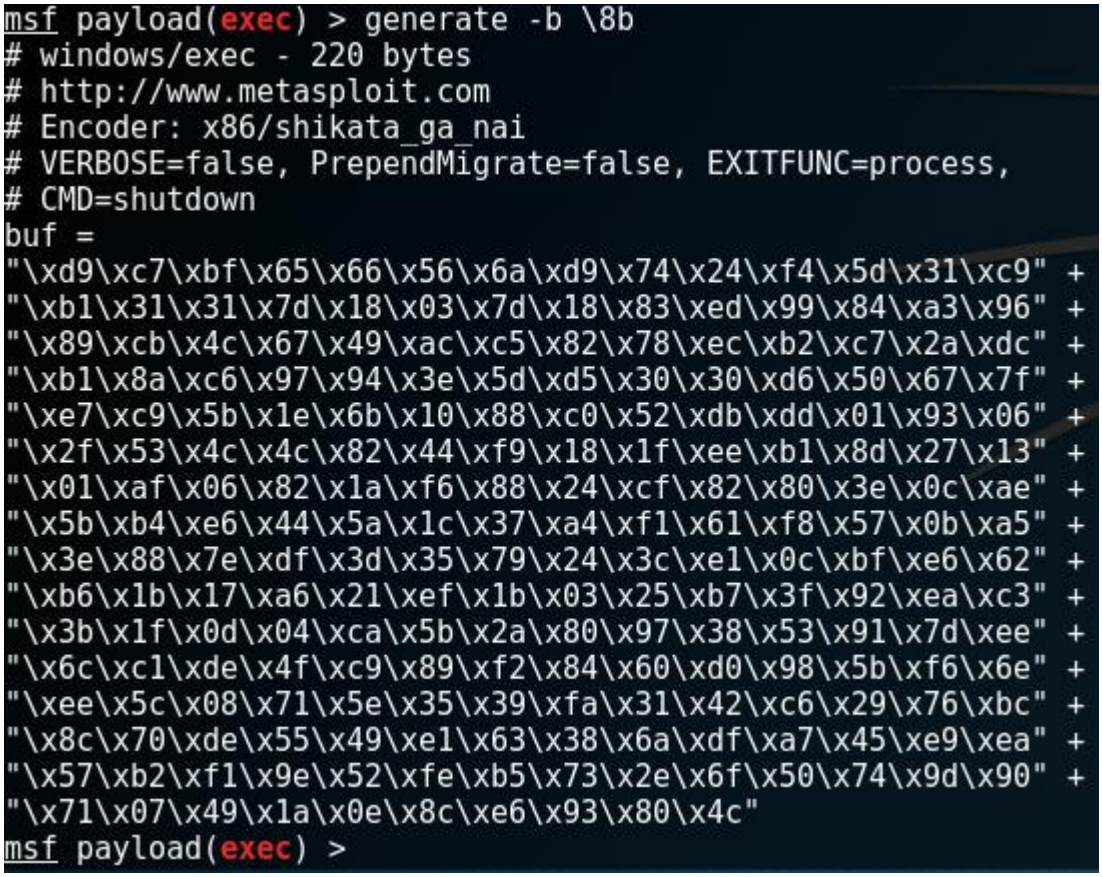

Рисунок 73 – Генерація пейлоаду з використанням флагу -b та заміні байту 8b

Зверніть увагу на різницю розмірів файлу 193 байти в оригіналі та 220 після використання флагу “-b”. Це є наслідком того що байт 8b було замінено на інші, але таким чином щоб виконуваний файл залишався працездатним.

Інший напрямок приховування пейлоаду від антивірусних програм – є використання енкодерів (за замовчуванням використовуються shikata ga nai). Переглянути доступні енкодери можливо виконавши пошук за ключовим словом “encoder”. Для використання енкодеру необхідно вказати його назву після флагу “-e”.

Завдання:

1. Виконати генерацію пейлоаду з використанням не менше ніж трьох енкодерів

2. Виконати генерацію не менш ніж трьох пейлоадів з використанням лише підміни байтів

3. Виконати перевірку антивірусними програмами (не менше 25-ти)

4. У звіт додати інформацію про використані енкодери з обґрунтуванням їх вибору

5. Додати у звіт порівняльну характеристику генерованих пейлоадів, енкодерів що використовувались для їх генерування та результатами сканування антивірусами.

Лабораторна робота №13

Тема: Експлуатація вразливостей

Мета: Навчитися використовувати вразливості за допомогою Metasploit.

Теоретичні відомості

Розділяють два види можливих експлуатацій вразливостей. Перша – це віддалена експлуатація, вона дозволяє 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 експлуатацією на стороні клієнта (client-side attacks).

Для того щоб розгорнути хендлер на стороні тестера необхідно запустити "msfconsole" після чого обрати необхідний 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 payload з боку клієнта. В решті-решт необхідно виконати команду "run" для запуску хендлера.

Завдання:

1. Використати вразливість яка дає змогу віддаленої експлуатації
2. Використати вразливість що дає змогу експлуатації вразливості на стороні клієнта
3. Додати у звіт відомості про вразливості що були використані
4. Додати у звіт відомості про можливості що були надані в результаті використання вразливостей

5. Додати у звіт рекомендації що до усунення цих вразливостей, та що до 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.

Завдання:

1. Отримати скріншот віддаленої машини
2. Отримати права system на стороні системи клієнта
3. Виконати видалення логів подій на стороні системи клієнта
4. Налаштувати port-forwarding та влаштувати бекдор за допомогою NetCat
5. У звіті відобразити хід виконання роботи
6. Додати скріншоти, та вивід консолі

Список використаної літератури

1. Хорошко В.А. Методы и средства защиты информации / Хорошко В.А., Чекатков А.А. / Под ред. Ю.С. Ковтанюка. – К.: Юниор, 2003. – 504 с.

2. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

3. Макс Ронге. Разведка и контрразведка / М. Ронге /. – К.: СИНТО, 1993. – 239 с.

4. Мухачев В.А. Методы практической криптографии / Мухачев В.А., Хорошко В.А./ . – К.: ПолиграфКонсалтинг, 2005. – 214 с.

5. Мицан И.Б. Стеганографические методы сокрытия информации / Мицан И.Б. // Специальная техника и вооружение. Научно-методическое издание. – К., № 1 – 5, 2001. – С. 28 – 32.

6. Хорошко В.О. Основи комп'ютерної стеганографії. Навчальний посібник / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчик /. – Вінниця: ВДТУ, 2003. – 143 с.

7. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Конахович Г.Ф., Пузыренко А.Ю. /. – К.: «МК-Пресс», 2006. – 288 с.

8. Безопасность информационных технологий. Методология создания систем защиты/ В.В. Домарев. – К.: ООО "ТИД "ДС", 2001. – 688 с.

9. Энциклопедия промышленного шпионажа/ Под общ. ред. Е.В. Куренкова – С.Петербург: ООО "Изд-во Полигон", 1999. – 512 с.

10. Хорев А;А. Способы и средства защиты информации. – М.: МО РФ, 2000. -316 с.

11. А.Ю.Щербаков. Введение в теорию и практику компьютерной безопасности. -М.: издатель Молгачева С.В., 2001.

12. Бармен, Скотт. Разработка правил информационной безопасности.: Пер. с англ. – М.: Издательский дом "Вильямс", 2002.

13. С.Л.Емельянов Основы информационной безопасности.– Одесса:

Юридична література, 2003.-198с.

14. Про державну таємницю. Закон України №3855-XII від 21.01.1994 р. (в редакції Закону № 1079-14 від 21.09.99).

15. Про затвердження зводу відомостей, що становлять державну таємницю. Наказ Голови Служби безпеки України від 12.08.2005 р. № 440.

16. НД ТЗІ 1.1 – 002 – 99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. Нормативний документ ДСТЗИ СБ Украйни. Киев, 1999.

17. Про інформацію. Закон України № 2657-ХП від 02.10.92 р.

18. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 8.10.97.

19. Положення про технічний захист інформації в Україні. Указ Президента України №1229/99 від 27.09.99.

20. Тимчасові рекомендації з технічного захисту інформації вид витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ-ПЕМВН-95). Затверджені наказом ДСТЗІ від 09.06.95р. № 25.

21. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

22. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

23. НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

24. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (Зі зміною № 1, затвердженою наказом ДСТСЗІСБУ 18.06.02 № 37).

25. НД ТЗІ 2.5-010-2003. Вимоги до захисту інформації /№ЕВ-сторінки від несанкціонованого доступу.

26. 13.ГОСТ Р 51275-99. Защита информации. Объект информатизации.

Факторы, воздействующие на информацию. Общие положения.

27. http://www.intuit.ru/department/security/secbasics/

28. Галатенко В.А. Основы информационной безопасности Интернет-университет информационных технологий – ИНТУИТ.ру, 2008

29. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия Интернет-университет информационных технологий – ИНТУИТ.ру, 2005

30. Галатенко В.А. Стандарты информационной безопасности Интернет-университет информационных технологий – ИНТУИТ.ру, 2005

31. Э. Мэйволд Безопасность сетей Эком, 2006

32. Хаулет Т. Защитные средства с открытыми исходными текстами БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий – ИНТУИТ.ру, 2007

33. Department of Defense Trusted Computer System Evaluation Criteria DoD 5200.28-STD, 1993.

34. Information Technology Security Evaluation Criteria (ITSEC). Harmonized Criteria of France – Germany – the Netherlands – the United Kingdom Department of Trade and Industry, London, 1991.

35. Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800 CCITT, Geneva, 1991.

36. Site Security Handbook. Holbrook P., Reynolds J., Request for Comments: 1244, 1991.

37. James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback Report on the Development of the Advanced Encryption Standard (AES) Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Technology Administration U.S. Department of Commerce. 2000г. 116с.

38. Государственный Стандарт Российской Федерации Информационная технология. Криптографическая защита информации. Процедуры выработки и

проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма 1994г.

39. Государственный Стандарт Российской Федерации Информационная технология. Криптографическая защита информации. Функция хэширования 1994г.

40. RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile 2002г. 129с.

41. RFC 3281 An Internet Attribute Certificate Profile for Authorization 2002г. 40с.

42. RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols 1999г. 72с.

43. RFC 2511 Internet X.509 Certificate Request Message Format 1999г. 25с.

44. RFC 3369 Cryptographic Message Syntax 2002г. 60с.

45. RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP 1999г. 23с.

46. RFC 2797 Certificate Management Messages over CMS 2000г. 47с.

47. RFC 3379 Delegated Path Validation and Delegated Path Discovery Protocol Requirements 2002г. 15с.

48. RFC 2633 S/MIME Version 3 Message Specification 1999г. 32с.

49. RFC 2632 S/MIME Version 3 Certificate Handling 1999г. 13с.

50. Security Architecture for the Internet Protocol RFC 2401 1998г. 66с.

51. Internet Security Association and Key Management Protocol (ISAKMP) RFC 2408 1998г. 86с.

52. The Internet Key Exchange (IKE) RFC 2409 1998г. 41с.

53. RFC 2412 The OAKLEY Key Determination Protocol 1998г. 55с.

12. Інформаційні ресурси

Бібліотеки, Інтернет, електронні книги.