МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«Комплексна система захисту в локальній мережі. Аудит»

Завідувач
випускаючої кафедри **Довбиш А.С.**

Керівник роботи **Симоновський Ю.В.**

Студента групи КБ – 61 **Ковальов О.В.**

СУМИ 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних наук

Затверджую_____

Зав. кафедрою Довбиш А.С.

"_____" _____2020 р.

ЗАВДАННЯ

до випускної роботи

Студента четвертого курсу, групи КБ-61 спеціальності "Кібербезпека" денної форми навчання Ковальова Олексія Віталійовича.

Тема: "Комплексна система захисту в локальній мережі. Аудит "

Затверджена наказом по СумДУ

№_____ от _____2020 р.

Зміст пояснювальної записки: 1) інформаційний огляд аудиту; 2) постановка завдання й формування завдань дослідження; 3) опис основних стандартів, принципів захисту як елемент комплексу систем захисту в локальних мережах; 5) розробка методології реалізації аудиту; 6) аналіз результатів.

Дата видачі завдання "_____"_____2020 р.

Керівник випускної роботи _____ Симоновський Ю.В.

Завдання прийняв до виконання _____ Ковальов О.В.

РЕФЕРАТ

Записка: 59 стор., 31 рис., 1 таблиця, 11 джерел.

Об’єкт дослідження — Аудит локальної мережі.

Мета роботи — розробка методології проведення аудиту.

Результати — сформована методологія аудиту, яка надає певний рівень захищеності і використовує тільки програмне забезпечення, яке є у вільному доступі.

Реалізація виконана у тестовому середовищі, яке було спроектоване спеціально для створення та тестування моделей проведення аудиту.

Аудит, Kali Linux, системи інформаційної безпеки, Metasploit

ЗМІСТ

ВСТУП

Інформація сьогодні є одним з найцінніших активів організації. Найважливішою її вимогою є те, що вона повинна бути отримана певним користувачем в потрібний час. Своєчасна комунікація між особами, які приймають рішення та всіма верствами організації - вже не розкіш, а необхідність. Три головних фактори, які забезпечують ефективне спілкування це - персональний комп’ютер, якісне програмне забезпечення та локальні мережі (LAN).

Персональні комп’ютери надають користувачам можливість виконувати безліч різних функцій, необхідних для ефективного використання інформації. Локальні мережі дозволяють обмінюватись інформацію швидким, надійним та економічним способом. Середовище локальної мережі складається з мережевого персоналу та менеджменту, апаратних засобів: набір кабелів, мережеве програмне забезпечення, файлові сервери, що діють як сховища інформації, та користувачі мережі.

Складності, що виникають при впровадженні локальної мережі в організацію, можуть ускладнюватись програмним забезпеченням для управління розподіленими базами даних, програмним забезпеченням або апаратним забезпеченням для захисту та шифрування, різними стандартами для передачі даних та потребою співробітництва з декількома постачальниками як мережевого обладнання, так і програмного забезпечення.

Виклик керівництву полягає у забезпеченні безпеки та постійній доступності інформації та обчислювальних ресурсів, необхідних для виживання бізнесу та конкурентних переваг. Цей процес управління ризиками включає забезпечення належної безпеки та контролю в локальній мережі. Вагомим проти цього виклику є безліч ризиків, пов'язаних з локальним середовищем. Ризики виникають у різних формах, починаючи від стихійних лих до випадкових або навмисних пошкоджень, втрат, модифікацій, зриву та

використання. Прикладами таких загроз є: помилкова переадресація повідомлень, перехоплення повідомлень сторонніми приймачами, переривання передачі та перенаправлення передачі даних на підроблені вузли.

Потенційна втрата для організації може бути біль небезпечною в локальній мережі, оскільки важливість інформації, знайденої у вузлах, як правило, перевищує значення, знайдене в основному комп'ютері. Це тому, що інформація у вузлах, швидше за все, була проаналізована та синтезована для прийняття рішення. Ця вбудована форма "рішення" може вказувати на стратегічний напрям, розвиток продукту або критичну організаційну розвідку, і тому є більш цінною. Аудитори є основними експертами з безпеки та контролю та здійснюють аудит як мережевого середовища, так і додатків, які використовують мережу. Отже, вони повинні бути залучені до обговорення питань безпеки, контролю та аудиту до введення в експлуатацію та під час проведення операцій.

1. ІНФОРМАЦІЙНИЙ ОГЛЯД

1.1.Локальні мережі

Локальна мережа - це група комп'ютерів та периферійних пристроїв, які мають спільну лінію зв'язку або бездротове з'єднання з сервером в межах окремої географічної області. Локальна мережа може обслуговувати не менше двох або трьох користувачів в домашньому офісі або кілька сотень користувачів у центральному офісі корпорації. Власники будинків та адміністратори інформаційних технологій налаштовують локальні мережі, щоб мережеві вузли могли обмінюватися ресурсами, такими як принтери або мережеві сховища.

1.1.1. Види локальних мереж

Існують два типи локальних мереж: однорангові локальні мережі та клієнт-серверні.

Клієнт-серверна локальна мережа складається клієнтів(хоча б одного), які підключені до центрального серверу. Сервер має такі зобов’язання як: зберігання файлів, доступ до додатків, доступ до пристроїв і вихідний мережевий трафік. Клієнт може бути будь-яким підключеним пристроєм, який запускає або звертається до додатків або Інтернету. Клієнти підключаються до сервера використовуючи кабелі або бездротове з'єднання.

Як правило, набори додатків можуть зберігатися на сервері локальної мережі. Користувачі можуть отримувати доступ до баз даних, електронної пошти, спільного використання документів, друку і іншим службам через додатки, що працюють на сервері локальної мережі, з доступом для читання і запису, підтримуваним мережевим або IT-адміністратором. Більшість мереж середнього бізнесу, урядових, дослідницьких і освітніх мереж є локальними мережами на основі клієнт-серверної моделі.

Однорангова локальна мережа не має центрального сервера і не може справлятися з великими робочими навантаженнями, як це може зробити клієнт-серверна локальна мережа, тому вони зазвичай менше. У одноранговій

мережі LAN кожен пристрій в рівній мірі бере участь у функціонуванні мережі. Пристрої спільно використовують ресурси і дані через дротові або бездротові з'єднання з комутатором або маршрутизатором. Більшість домашніх мереж є одноранговими.

1.1.2. Переваги локальних мереж

Переваги локальної мережі такі ж, як і для будь-якої групи пристроїв, об'єднаних разом. Пристрої можуть використовувати єдине підключення до Інтернету, обмінюватися файлами один з одним, друкувати на спільних принтерах, а також отримувати доступ та навіть контролювати один одного.

Локальні мережі були розроблені в 1960-х роках для використання коледжами, університетами та науково-дослідними установами (такими як NASA), насамперед для підключення комп'ютерів до інших комп'ютерів. Лише після розробки технології Ethernet (1973 р. У Xerox PARC), її комерціалізації (1980 р.) та її стандартизації (1983 р.) локальні мережі почали широко застосовуватися [1].

Незважаючи на те, що переваги наявності пристроїв, підключених до мережі, завжди були добре зрозумілі, проте лише після широкого розгортання технології Wi-Fi локальні мережі стали звичним явищем майже для кожного типу середовища. Сьогодні не тільки підприємства та школи використовують локальні мережі, але й ресторани, кав’ярні, магазини та будинки.

Бездротове підключення також значно розширило типи пристроїв, які можна підключити до локальної мережі. Зараз майже все, що можна уявити, можна "підключити" - від ПК, принтерів та телефонів до смарт-телевізорів, стереосистеми, динаміків, освітлення, термостатів, віконних відтінків, замкових дверей, камер безпеки.

1.2.Захист інформації в локальних мережах

Внаслідок інтенсивного та швидкого розвитку комп'ютерної технологій і систем трансляції інформації, все більш актуальною стає проблема забезпечення безпеки інформації. Під загрозою безпеки інформації розуміють

дію або подію, яка може привести до руйнування, спотворення чи несанкціонованого (недозволеному) використанню інформаційних ресурсів. Безпекою інформації називають стан, при якому інформаційних ресурсів не загрожує небезпека.

Актуальність проблеми забезпечення безпеки локальних мереж пояснюється тим, що зміни в економічному житті нашої країни - реалізація фінансово-кредитної системи, створення підприємств с різними формами власності - роблять помітний вплив на питання захисту інформації. Довгий час в Україні існувала тільки державна форма власності. Тому інформація і секретні дані були теж тільки державними. Проблеми інформаційної безпеки посилюються в міру проникнення в усі сфери діяльності технологій обробки і трансферу даних, і перш за все обчислювальних систем. Об'єктами, які потенційно можуть бути атаковані, можуть бути різні технічні засоби, програмне забезпечення або бази даних [2].

Кожний збій мережі та комп’ютерних систем приводить до фінансових збитків. Значимість збоїв різної масштабності змінюється відносно того, яка саме мережа була атакована. В сучасному світі комп’ютерні технології інтегруються в кожну сферу людини. Наприклад мережеві збої в медичних, військових або фінансових закладах можуть привести до невідновлених наслідків. Важливість інформаційної безпеки різко стало найважливішим питанням як держав, так і комерційних закладів.

Основні критерії інформаційної безпеки мають забезпечувати:

1. цілісність інформації;
2. конфіденційність інформації;
3. доступність інформації.

Окремо можна виділити певні сфери діяльності людини, в які були інтегровані комп’ютерні системи. Прикладом таких сфер можуть бути:

- банківська справа та все, що відноситься до фінансів;
- всі державні служби;

- спеціальні структури та багато інших.

Такі структури вимагають більш серйозної системи захисту інформації. Частіше всього в законодавстві прописують окремо вимоги до захисту спеціалізованих структур відповідно до їх важливості(важливості інформації, яка в них обробляється).

Загрози безпеці інформації можуть бути випадковими (ненавмисними) - це загрози, джерелом яких є помилки в ПЗ(програмне забезпечення), вихід з ладу на рівні апаратного забезпечення, некоректні дії користувачів та ін., і навмисними, мета яких нанесення шкоди.

Забезпечення безпеки необхідно для будь-яких організацій незалежно від розмірів і форм їх діяльності, але вразливими частіше є малі підприємства, пов'язані локальними інформаційними мережами. Тому захист і контроль необхідно забезпечити на всіх рівнях: фізичному, програмному, призначеному для користувача і зовнішньому.

Основні технічні загрози безпеки локальної мережі на малому підприємстві

1. Помилки в ПЗ. Джерелами помилок в ПЗ є робота конкретних людей з їх індивідуальними особливостями, кваліфікацією і т. п. Більшість помилок не несе за собою небезпечні ситуації, проте деякі можуть привести до серйозних наслідків таким як отримання прав доступу для контролю над сервером зловмисником або несанкціоноване використання ресурсів. Такі загрози усувають за допомогою оновлень систем безпеки, які регулярно випускають виробники програмного забезпечення. Для коректної роботи систем безпеки необхідно використовувати найновіші версії ПЗ випущені виробником(стабільні).
2. DoS(denial-of-service attack) та DDoS-атаки(distributed denial-of-service attack). Атаки відмови в обслуговуванні DoS направляються зазвичай на інформаційні сервери підприємства, функціонування

яких є критично важливою умовою для працездатності всього підприємства. Для проведення таких атак зловмисники координують роботу кількох робочих станцій, в цьому випадку можлива і DDoS атака – розподілена атака до відмови обслуговування. Зловмисник захоплює управління над групою віддалених комп'ютерів, посилає потужний сумарний потік пакетів в комп'ютер, який був обраний для реалізації атаки, викликаючи його перевантаження, в результаті чого відбувається вичерпування ресурсів операційної системи або процесора комп'ютера.

3. Шкідливі програми («троянський кінь», «черв'яки», комп'ютерні віруси). Збиток, нанесений шкідливими програмами, може виражатися в розкраданні, спотворенні, знищення інформації, а також приведення у неробочий стан ПЗ. Троянські програми видають себе за корисні додатки, але при установці або відкритті файлу заповнюють робочу станцію. Мережеві «Черв'яки» здатні самостійно поширюватися по локальній мережі і глобальних мереж шляхом поширення своїх копій. Віруси проникають у різні типи файлів, не змінюючи розмір самого файлу.

Загальні принципи забезпечення безпеки

1. Мережеве обладнання, яке виконує маршрутизацію трафіку в мережу Інтернет має бути обладнане системою фільтрації трафіку з правилами по замовчуванням.
2. Локальна мережа повинна мати мінімальну кількість глобальних адрес.
3. Весь трафік повинен бути отриманий з використанням кешування інформації за допомогою проксі-серверів.
4. Проксі-сервер повинен мати налаштовані Access Control List.
5. На проксі-сервері має бути встановлене антивірусне ПЗ, яке забороняє доступ до потенційно небезпечних джерел.

6. Прямий доступ до мережі Інтернет з використанням механізму трансляції мережевих адрес (NAT) може бути включений тільки для обмеженого числа користувачів, щоб запобігти звернення ззовні до внутрішніх хостів(користувачів мережі). ПЗ для перегляду інформації по http-протоколу має використовувати максимальний рівень безпеки та попереджати користувача про всі потенційно небезпечні дії.
7. У мережі, що має вихід в Інтернет, повинна бути розроблена політика автоматичної установки всіх доповнень і виправлень, що випускаються постачальником операційної системи. Установка оновлень і доповнень повинна виконуватися для всіх комп'ютерів мережі, незалежно від прав користувача комп'ютера на отримання доступу до мережі Інтернет.
8. Всі мережеві комп'ютери повинні бути оснащені антивірусним ПЗ. Оновлення антивірусного ПЗ повинно виконуватися щодня в певний час.
9. Для комп'ютерів, що використовують прямий вихід в Інтернет слід зменшити до мінімуму число одночасних підключень.
10. Для всіх, без винятку, користувачів повинна бути заборонена установка стороннього ПЗ.

Забезпечення безпеки інформації локальних мереж на малому підприємстві - це комплекс заходів, спрямованих на неспроможність несанкціонованого отримання інформації, її фізичного знищення, а також модифікації. Використання цих заходів допоможе малим підприємствам успішно розвиватися, бути конкурентоспроможними і фінансово стабільними.

1.3. Аудит як елемент комплексу захисту інформації

Аудит безпеки локальної мережі - це технічна оцінка інформаційної інфраструктури організації - їх операційних систем, додатків тощо.

Реалізовувати(проводити) аудити можуть як внутрішні, так і зовнішні аудитори:

- внутрішні аудитори: для менших компаній роль внутрішнього аудитора може виконувати IT-менеджер вищого рівня в організації. Цей працівник відповідає за створення надійних аудиторських звітів для керівників та зовнішніх спеціалістів, які контролюють стандарти безпеки. Більші компанії, як правило, наймають відповідних корпоративних внутрішніх аудиторів. Ці особи зазвичай мають вражаючий досвід в ролі сертифікованого аудитора інформаційних систем або сертифікованого спеціалісту з інтернет аудиту;
- зовнішні аудитори: зовнішній аудитор має багато моделей аудиту, залежно від характеру компанії та мети проведення аудиту. У той час як деякі зовнішні аудитори приїжджають з державних управлінь, інші належать приватним аудиторським компаніям, що спеціалізуються на аудиті. Ці аудитори приймаються на роботу, коли цього вимагають певні рамки відповідності професійності.

Основних типів аудиту існує 2, а саме:

- ручний аудит: ручний аудит може здійснювати внутрішній або зовнішній аудитор. Під час такого типу аудиту аудитор проводить інтерв'ю з працівниками, проводить сканування систем безпеки на вразливості, оцінює фізичний рівень доступу до систем та аналізує додатки та контроль доступу до операційної системи;
- автоматизований аудит - це аудит, відомий також як CAAT(Computer-assisted audit tool). Ці аудити проводяться надійним програмним забезпеченням і створюють вичерпні, індивідуально налаштовані аудиторські звіти, які підходять для внутрішніх керівників та зовнішніх аудиторів. Вдосконалене програмне забезпечення для аудиту навіть забезпечить

додатковий рівень безпеки, постійно контролюючи IT-інфраструктуру та попереджаючи технічних працівників, коли виникає підозріла активність [3].

У процесі аудиту необхідно отримати певну інформацію про мережу, яка розглядається для продовження аудиту мережевої безпеки. Збір інформації можна реалізувати за допомогою п’яти кроків.

1. Визначення масштабу мережі. Зазвичай це робиться шляхом вивчення мережевої схеми(мапи). Схема мережі в основному має вигляд карти, яка відображає всі можливі маршрути мережевих елементів. Ключовий фактор, який має турбувати аудитора на схемі є її точність. Великі мережі розвиваються та змінюються постійно залежно від потреб бізнесу. Аудитор ІС(інформаційної системи) повинен з’ясувати чи існують в організації процеси оновлення та обслуговування мережевої схеми. Використання програмного інструменту генерування цієї схеми забезпечує певний ступінь точності. В будь-якій мережі будуть місця, де є концентрація ресурсів, наприклад, центр обробки даних, де працює ERP сервери або поштові сервери та ін. Хоча менші мережі можуть мати тільки одну таку зону розташування важливої інформації, проте в складних та масштабних мережах може бути багато місць, де знаходяться критичні ресурси. Мережева схема також може забезпечити введення даних про тип пристроїв та протоколів, що використовуються в мережі. Схема мережі та її деталі дають найважливіший вклад аудиту, і аудитор повинен продовжувати посилатися на нього протягом всього процесу.
2. Визначення критичних(найбільш важливих) інформаційних ресурсів. Основним принципом інформаційної безпеки та аудиту є те, що захист пов'язаний з ризиками активів, які визначаються систематичною оцінкою ризику. Аудитор мусить сформувати

критичні активи, системи та послуги яким потрібно реалізувати найвищу ступінь безпечності. Як правило, треба захистити корпоративні системи, включаючи ERP, поштові сервери та інші внутрішні програми, веб-сервери, на яких розміщуються програми. До них звертаються клієнти та постачальники, а також мережа та її компоненти. У цьому контексті безпека та доступ до механізмів навколо додатків та серверів (ОС(операційна система) і база даних) також повинні бути надійними.

3. Визначення прав доступу користувачів. Важливим етапом аудиту є визначення осіб, які мають доступ до систем у мережі. Для реалізації даного етапу потрібно відповісти на питання:
    a. До системи доступ мають лише працівники?
    b. Чи мають клієнти та постачальники також доступ до систем? Чи мають доступ співробітники до системи поза офісом?
    c. Чи користувачі отримують доступ до веб-сервера через Інтернет чи виконують віддалені входи в систему підприємств?

    Відповіді на ці питання матимуть значний вплив на безпеку
4. Визначення з'єднань із зовнішніми мережами. Хоча цей етап повинен відноситись до кроку 1 (під час вивчення мережевої схеми), це важливий крок і його слід вирішувати окремо. На мінімальному рівні кожна мережа підключена до Інтернету через Інтернет-провайдера. Основна причина підключення до Інтернету - це можливість отримання та відправлення пошти та можливість використовувати глобальну мережу працівниками. У підприємств можуть бути й інші причини підключення до Інтернету, наприклад веб-сайти, через які постачальники, клієнти та партнери компанії співпрацюють, розміщують замовлення або обмінюються іншою інформацією. Також можуть існувати виділені зв’язки з мережами

інших партнерів. Шлюзи, через які здійснюється кожен з цих з'єднань, є потенційними точками входу для зовнішнього світу. На даному кроці аудитор може спробувати визначити розмежування між внутрішньою та зовнішньою мережею. Виходячи з етапу 2, аудитор ІС має досить інформації для того, щоб визначити до яких систем мають доступ лише внутрішні користувачі і до яких систем мають доступ користувачі з зовнішнього світу (Інтернету). Така категоризація також допоможе аудитору визначити ефективність проектування демілітаризованої зони та розміщення продуктів безпеки, таких як брандмауери та системи виявлення вторгнень. Основним зусиллям є захист внутрішньої мережі від зовнішнього світу на шлюзах(gateway). Це не означає, що загрози надходять лише ззовні. Загрози зсередини такі ж серйозні, як і зовні. Аудитору необхідно оцінити загрози як внутрішні, так і зовнішні. Щоб захистити системи від внутрішніх загроз, необхідно оцінити всю безпеку на базі хостів, наприклад, захист програм та додатків на рівні операційних систем.

5. Визначення механізму захисту. Отримавши базове розуміння мережі, ресурсів та ризиків, аудитор готовий розглянути механізми захисту. Потім аудитор може оцінити їх ефективність та компетентність.

1.4.Постановка задачі

Опираючись на створені стандарти та правила проведення аудиту змоделювати локальну мережу і описати методологію реалізації аудиту від моделювання до формування підсумків. Паралельно формуючи методологію також відображати процес аудиту в тестовій мережі. Вимогами до аудиту є:

- використання програмного забезпечення яке поширюється за допомогою GNU GPL;
- детальний опис мережі та процесу аудиту, який був би зрозумілий не тільки спеціалістам з інформаційної безпеки використовуючи професійні інструменти.

2. ТЕОРЕТИЧНІ ОСНОВИ

2.1.Методи і стандарти реалізації аудиту

2.1.1. Методи проведення

Існує безліч способів проведення аудиту і у кожного з них є свої переваги і недоліки.

Сам процес тестування потребує значних енерговитрат, ретельного планування, визначення самої мети і конкретних кроків для її досягнення. Після завершення планування, отримання необхідних дозволів та інформування задіяних осіб починається сам аудит. Зазвичай його починають зі збору інформації, яка згодом стане в нагоді для сканування мережі та інших активних дій. Після того як мета тестування була визначена, готується звіт, в якому відображаються всі дії, знайдені вразливості, методи їх експлуатування і рекомендації щодо усунення таких.

Перш за все, важливо усвідомити, що аудит є частиною нормального життєвого циклу будь-якої IT-інфраструктури. Необхідність в їх проведенні може бути обумовлена як внутрішньою політикою, так і вимогами третьої сторони. У будь-якому випадку такі заходи дозволяють по-справжньому оцінити можливі ризики і виявити приховані проблеми.

Зазвичай під час таких тестів оцінюються такі компоненти IT інфраструктури: додатки, мережеві сервіси, мережеві пристрої, середовища передачі даних, підготовленість співробітників і фізична безпека.

Тести на проникнення можна класифікувати виходячи з такого параметра, як обізнаність атакуючого.

- Чорний ящик - найкраще характеризує більшу частину атак на мережу. В даному випадку найчастіше атака відбувається віддалено, а атакуючому спочатку відомо тільки назва організації. Використовуючи різні методи аудитор отримує більш детальну інформацію про ціль і використовує її для подальших дій. Під час своїх дій атакуючий документує всі знайдені вразливості і їх

потенційну небезпеку, для того щоб в подальшому використовувати їх для атаки і надання звіту замовнику.

- Сірий ящик - в цьому випадку атакуючий спочатку володіє деякою кількістю інформації. Наприклад, йому можуть бути відомі версії програмного забезпечення або структура мережі. Це робиться для того, щоб скоротити необхідний для атаки час, адже відразу ж буде можливість дізнатися про найбільш критичні точки в мережевій інфраструктурі. В іншому ж цей процес буде схожий на попередній.
- Білий ящик – такий тип аудиту проводиться за наявності у атакуючого повної інформації про свою ціль дослідження. Даний вид тестування дозволяє найбільш повно оцінити IT-інфраструктуру і гарантовано виявити більшу частину проблемних місць. Найчастіше такий спосіб тестування використовується при проведенні внутрішніх аудитів.

При офіційному, дозволеному аудиті інформаційних систем існує кілька варіантів проведення тестування:

- Сліпе тестування - не має на увазі наявності у атакуючого якої-небудь важливої інформації про цілі, проте співробітники, що мають відношення до інфраструктури, що тестується, заздалегідь попереджаються про напад.
- Подвійне сліпе тестування - аудитор також не має жодних даних про цілі, але про майбутню атаку знає лише кілька людей з цільової організації. Велика частина тестів проходить саме за цим сценарієм.
- Реверсне тестування - аудитор має всю інформацію про систему, а співробітники знають про майбутнє тесті, але не мають даних про те, де і коли він буде відбуватися.

2.1.2. Стандарти проведення аудиту

Існує кілька популярних стандартів, за якими зазвичай проводять аудити. Хоча на практиці вони і не є обов'язковими до виконання, однак, використовуючи їх, можна зробити свої дії більш методичними, уникнути типових помилок і не випустити з уваги важливі деталі. Одним з таких стандартів є PTES(penetration testing execution standard), розроблений декількома експертами з інформаційної безпеки з метою конкретизації методів і кроків, які повинні робити фахівці з ІБ під час тестування. Даний стандарт повністю безкоштовний [4].

У PTES виділяються сім фаз тестування:

- підготовча фаза;
- збір даних;
- моделювання загроз;
- аналіз вразливостей;
- експлуатація вразливостей;
- постексплуатаційна фаза;
- звіт.

Ці сім фаз відображають всі дії, які повинні відбуватися під час аудиту. PTES - досить новий стандарт, проте він постійно підтримується, оновлюється і змінюється разом з вимогами до аудитів ІБ. Хоча цей стандарт і намагається охопити весь процес тесту на проникнення, однак, жоден аудит не проходить за стандартною схемою, кожен з них буде чимось відрізнятися від інших.

2.2.Етапи проведення аудиту

2.2.1. Підготовчий етап

Часто зустрічаються твердження про те, що планування - це запорука успіху. І це дійсно так, особливо коли мова йде про аудит безпеки. Для того щоб вдало провести аудит, необхідно серйозно підготуватися, врахувати всі нюанси, підібрати потрібні інструменти і методологію. Зазвичай тест на проникнення починається із зустрічі зацікавлених сторін, на якій

обговорюються всі необхідні деталі, визначаються цілі та методи, а також люди, які можуть бути залучені в подальшому. На цьому етапі має сформуватися певне бачення цілей і завдань майбутньої роботи, без цього в кінці аудиту буде практично неможливо визначити, чи була виконана поставлена задача. Перш за все, необхідно визначити основні цілі атаки, з'ясувати, що буде піддаватися нападу, а що ні, визначити обсяг і основний тип тестів.

Слід також визначити час і тривалість проведення тесту. Це дуже важливо, тому що деякі бізнес-процеси відбуваються тільки в певний час доби. Необхідно дотримати баланс, адже тести з використанням соціальної інженерії дуже важко проводити у вихідні дні або в неробочий час. Обов'язково треба визначити можливі ризики і вплив на бізнес-процеси - це допоможе в разі непередбачених ситуацій.

2.2.2. Збір інформації

Після підготовчого етапу можна рухатися далі і починати збирати необхідних даних. Цей етап вже відноситься до тесту на проникнення. Існує величезна кількість джерел даних, які можуть бути корисні для досягнення кінцевої мети. Вибирати потрібно ті, які допоможуть в майбутньому отримати найбільш повне уявлення про ціль, а також визначити пріоритетність і напрямок векторів аудиту. Джерелом інформації може служити що завгодно - пошукові системи, веб-сайти, вакансії, фінансові звіти і, звичайно ж, соціальні мережі.

В нашому випадку будемо реалізовувати аудит за стандартом PTES. У PTES виділяють три рівня даного етапу:

- Перший рівень - найпростіший, можна використовувати автоматичні системи збору інформації, а також найпопулярніші інтернет-ресурси.
- Другий рівень відрізняється від першого тим, що більше часу витрачається на ручне збирання даних. На даному етапі необхідно

більш детально аналізувати інформацію для того, щоб краще проаналізувати свою ціль.

- Третій рівень - самий витратний за кількістю часу і сил. На даному етапі атакуючий знаходить найбільш вразливі місця системи.

Перш ніж приступити до збору даних, необхідно провести підготовчу роботу, яка може включати в себе наступні кроки:

- Визначення цілі. В ідеальному випадку завдання поставлено конкретно, однак найчастіше інформація про цілі дещо розмита і в цьому випадку необхідно визначити, що конкретно потрібно шукати.
- У разі, якщо проводиться пошук цілі для сторонньої організації, необхідно визначити рамки, за які не можна виходити на даному етапі.
- Планування проміжку часу, який займе виконання робіт на даному етапі.
- Чітке визначення цілі. Повинно бути розуміння, яку інформацію бажано мати після закінчення робіт на даному етапі.

2.2.3. Аналіз вразливостей

На цьому етапі , використовуючи всю наявну інформацію і визначившись з методами та інструментами, починається безпосередню взаємодія з ціллю. Потрібно визначити і класифікувати будь-які можливі вразливості, будь то некоректна конфігурація сервісу або помилки, що з'явилися з вини розробників конкретної програми. Проводячи такий аналіз, потрібно чітко уявляти, які тести будуть проводитись, який інструментарій використовувати і що саме потрібно знайти. Без виконання цієї умови можна витратити велику кількість часу, все більше заглиблюючись в аналіз будь-якого компонента мережі. Однак без чіткого усвідомлення мети це може виявитися контрпродуктивним. Під час цього етапу будуть реалізовуватись такі дії, як сканування портів, отримання інформації про встановлені

програми, сканування на наявність вразливостей і інші описані раніше кроки. Важливим пунктом є уникання передчасних спроб експлуатації знайдених вразливостей. Цей етап тільки для збору корисної інформації.

2.2.4. Моделювання

Основне завдання на цьому етапі - побудова тестової середовища, в якому є можливість випробувати всі плановані варіанти атаки на цільову систему. Апробація методів у віртуальному середовищі допоможе уникнути помилок при роботі з реальною ціллю, а також залучити менше уваги, адже при роботі з цією ціллю будуть використовуватися лише перевірені методи.

В процесі моделювання виділяють чотири основні етапи:

- вивчення необхідної документації;
- визначення первинних і вторинних методів атак;
- знаходження основних і другорядних вразливостей;
- визначення методів атак для кожної зі знайдених вразливостей.

По суті, цей процес можна віднести до етапу збору інформації, але тільки більш поглибленого. В ідеалі створюється графічне відображення всієї отриманої на попередньому кроці інформації - бізнес-процеси, фізичне розташування, карту мережі, ієрархію співробітників і т. д. Для цього існує безліч автоматизованих інструментів.

2.2.5. Експлуатація вразливостей

Після того як була зібрана вся необхідна інформація, були визначені вразливості, обрали необхідні інструменти і вибрали потрібні цілі, можна приступати до наступного кроку.

На даному етапі використовуються знайдені вразливості для компрометації цільової системи і отримання доступу до неї. Аудитор повинен використовувати отриману інформацію для визначення відповідної мети. Знайшовши безліч уразливих систем, необхідно вибрати серед них ту, злом якої дасть надалі найбільшої переваги. Знайшовши, наприклад, безліч

уразливих робочих станцій і кілька серверів, краще зосередити свою увагу на останніх, так як їх злом допоможе розвивати подальшу атаку більш ефективно.

Після визначення мети потрібно використовувати всі практичні навички та знання для того, щоб скомпрометувати її. Цілком можливо, що з першого разу у нічого не вийде і доведеться перепробувати безліч методів, перш ніж буде досягнутий бажаний результат. На даному етапі найпопулярнішими атаками є:

- злом пароля;
- перехоплення даних;
- перехоплення сесії;
- переповнення буфера.

Всі ці атаки можуть бути багатокомпонентними і включати в себе як технічний, так і людський фактор.

2.2.6. Етап після експлуатації

Після того як атака завершилася успіхом, необхідно закріпитися в системі. Це потрібно для того, щоб експлуатація атакованої цілі була більш зручною. Це бажана реалізувати для того, щоб кожного разу заново не зламувати систему, щоб виконати потрібні дії, тим більше, що вдала експлуатація однієї і тієї ж уразливості може стати неможливою буквально відразу після злому. Для початку необхідно визначити рівень своїх прав в системі і набір доступних дій. Цілком можливо, що виконання деяких операцій буде недоступно, тоді варто задуматися про можливості підвищення своїх привілеїв. Для цього можна запустити клавіатурного шпигуна, який відправить пароль адміністратора після того, як той зайде в систему. Також є можливість скопіювати інформацію про паролі для подальшого аналізу або встановити ПЗ, яке забезпечить подальший доступ до системи і можливість її віддаленого контролю. Також можна ліквідувати сліди перебування в системі, зазвичай це досягається шляхом видалення потрібних записів з журналів аудітації.

2.2.7. Звіт

Після того як всі описані вище етапи пройдені, необхідно створити звіт. Звіти можуть мати різний вигляд, тому те, яким він буде в кожному конкретному випадку, необхідно обговорити перед початком тесту.

Тим не менш, незважаючи на різноманітність можливих форм звітів, існують певні пункти, які необхідно в нього включити. Кожен звіт повинен починатися з короткого огляду процесу тестування. Немає необхідності описувати технічні деталі кожного кроку, огляд повинен відображати ключові моменти тесту. Далі необхідно привести список знайдених вразливостей і їх аналіз, при цьому найкраще згрупувати їх за ступенем важливості - наприклад, критичні, важливі, незначні.

Звіт повинен включати в себе наступну інформацію:

- сценарії і опис всіх успішних атак;
- детальну інформацію про отримані в ході тесту даних;
- детальну інформацію про всі знайдені вразливості;
- опис всіх знайдених вразливостей;
- пропозиції та технічні рішення для усунення знайдених вразливостей.

В ході проведення тесту для подальшого створення звіту необхідно записувати всі дії в будь-якій зручній формі.

2.2.8. Очищення слідів тестування

Після вдалого завершення тесту необхідно по можливості видалити всі сліди ваших дій. В даному випадку це встановлені програми, створених користувачів, зміни конфігурації і все інше, що було створено в ході тесту. Будь-які залишені лазівки можуть бути використані ким завгодно для отримання несанкціонованого доступу до вже скомпрометованої системи.

3. ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1.Вибір програмного забезпечення

При реалізації плану аудиту важливою частиною є вибір засобів та технологій, які будуть використовуватись. Існує декілька сімейств операційних систем, якими можна користуватись. Саме популярне сімейство ОС є Windows. Windows це сімейство ОС, яке є простим для користування звичайними користувачами, також воно має великі за обсягом ресурси для професіоналів будь-якої технології. Для цих операційних систем було створено багато інструментів для розробки систем захисту мереж і будь-яких елементів комп'ютера.

UNIX подібні ОС, які побудовані на основі ядра Linux зарекомендували себе в професійних кругах як ідеальні ОС для працівників комп'ютерних систем, які мають зазвичай більше ресурсів для роботи з елементами комп'ютерних мереж.

Дистрибутив Kali Linux – це система, яка побудована на основі дистрибутива Debian. Її великим плюсом є те, що вона розроблялася спеціально для проведення тестування систем на безпечність. Тому для реалізації аудиту була вибрана саме цей дистрибутив (Kali Linux 2020).

При виборі дистрибутива великих труднощів не було. Kali Linux це ідеальна система для реалізації аудиту і конкурентів для неї не існує. Головний плюс Kali одночасно і мінус. Це можна стверджувати тому, що в даному дистрибутиві існує дуже багато додатків, які можна використовувати для однієї цілі. Різниця тільки в деталях реалізації та побажаннях самого спеціаліста, який буде їх використовувати. Для кожного етапу реалізації аудиту були вибрані конкретні додатки з допомогою яких і буде реалізований аудит в локальній мережі. Також використовується стандартні можливості Linux.

Список всіх додатків:

- Nmap

- Nipe
- OpenVAS
- Metasploit
- John the Ripper
- Cymothoa
- Aircrack-ng

Тепер кожен додаток розглянемо окремо.

3.1.1. Nmap

Nmap - це багатофункціональний сканер портів, популярний в співтоваристві IT-безпеки. Nmap - дуже гнучкий і якісний інструмент, який повинен бути у кожного спеціаліста, який займається безпекою інформаційних систем.

Nmap виконує різні функції.

- Виявлення хостів. Nmap можна використовувати для пошуку працюючих хостів в цільових системах. За замовчуванням Nmap для виявлення хоста відправляє запит ICMP, пакет TCP SYN на порт 443, пакет TCP ACK на порт 80 і запит мітки часу ICMP.
- Виявлення служб і(або) версій. Після виявлення портів Nmap може додатково перевірити протокол служби, ім'я та номер версії програми, що використовується на цільовому комп'ютері.
- Виявлення операційної системи. Nmap відправляє ряд пакетів на віддалений хост і перевіряє відповіді. Потім він порівнює ці відповіді зі своєю базою даних відбитків операційної системи і якщо є збіг, виводить детальну інформацію. Якщо Nmap не може визначити операційну систему, то він надає URL-адресу, на яку можна відправити відбиток для оновлення бази даних відбитків ОС. Звичайно, якщо інформація про операційну систему, яка використовується в цільовій системі, відома, то слід відразу відправити відбиток.

- Трасування мережі. Ця дія виконується для визначення порту і протоколу, які, найімовірніше, досягнуть цільової системи. Трасування Nmap починається з високого значення TTL і зменшується до тих пір, поки значення TTL не досягне нуля.
- Nmap Scripting Engine. За допомогою цієї функції Nmap може бути розширений. Якщо потрібно додати в сканер не включену за замовчуванням перевірку, потрібно за допомогою оброблювача сценаріїв Nmap дописати цю перевірку. В даний час проводяться перевірки на наявність вразливостей в мережевих службах і перерахування ресурсів в цільовій системі [5].

3.1.2. Nipe

Nipe - це інструмент, який в якості шлюзу користувача за замовчуванням задіє Tor-мережу, спрямовуючи через неї весь трафік. Зазвичай Tor використовується для забезпечення деякого рівня конфіденційності і анонімності. Слід зазначити, що при використанні даного інструменту для забезпечення анонімності маскувати один IP-адреса недостатньо, так як може бути доступна інформація DNS. Для повної конфіденційності і анонімності слід замаскувати як IP, так і DNS [6].

3.1.3. OpenVAS

Open Vulnerability Assessment System (відкрита система оцінки вразливостей) - фреймворк, що складається з декількох сервісів і утиліт. OpenVAS - це сканер з відкритим вихідним кодом. Він простий в інсталяції і має зручний інтерфейс, що дозволяє виконувати активний моніторинг (з активними діями в мережі). При роботі OpenVAS використовує колекцію вразливостей, що складається з 50 000 тестів (NVTs). OpenVAS є основою лінійки професійних пристроїв Greenbone Secure Manager [7].

3.1.4. Metasploit

Фреймворк розроблений на мові програмування Ruby і підтримує модульність. Ці пункти дозволяють розширити або розробити для спеціаліста плагіни і інструменти.

Архітектура фреймворка розділена на три категорії: бібліотеки, інтерфейси і модулі. Для реалізація наших потреб будемо використовувати можливості різних інтерфейсів і модулів. Інтерфейси (консоль, CLI і GUI) в основному забезпечують зовнішню операційну діяльність при роботі з будь-яким типом модулів (експлойти, корисні навантаження, допоміжні пристрої і NOP). Кожен з таких модулів має своє призначення і функції, характерні для процесу тестування на проникнення.

- Exploit (Експлуатація). Цей модуль являє собою код PoC, розроблений для використання конкретної уразливості в цільовій системі.
- Payload (Корисне навантаження). Модуль являє собою шкідливий код, призначений для інтеграції в експлойт. Такий шкідливий код може бути самостійно скомпільовано для виконання довільних команд в цільовій системі.
- Auxiliaries (Оснастка). Дані модулі представляють собою набір інструментів, розроблених для виконання сканування, перехоплення, аналізу, захисту, зняття відбитків пальців і інших задач оцінки безпеки.
- Encoders (Датчики). Ці модулі призначені для запобігання виявлення антивіруса, брандмауера, IDS / IPS і інших подібних шкідливих програм шляхом кодування корисного навантаження під час операції проникнення.
- No Operation or No Operation Performed (NOP). Модуль є інструкцією на мові асемблера, який часто додається в код оболонки для виконання тільки узгодженого фрагмента корисного навантаження.

MSFConsole - один з найефективніших зовнішніх інтерфейсів, який містить кілька потужних інструментів. Він дозволяє спеціалістам з інформаційної безпеки отримати максимальну користь при експлуатації вразливостей [8].

3.1.5. John the Ripper

John the Ripper - це інструмент, який можна використовувати для злому хешу пароля. В даний час він може зламати більше 40 типів хешів паролів, таких як DES, MD5, LM, NT, crypt, NTLM і NETNTLM. Одна з переваг цього інструменту, в порівнянні з іншими, полягає в тому, що John може працювати з алгоритмами шифрування DES і crypt [9].

3.1.6. Cymothoa

Cymothoa - інструмент, який створює в операційній системі чорний хід(backdoor). Cymothoa додає в існуючий процес свій код оболонки. Це робиться для того, щоб замаскувати шкідливий інструмент під регулярний процес. Backdoor повинен мати можливість співіснувати з відповідним процесом, щоб не викликати підозр у адміністратора. Введення коду оболонки (shellcode) в процес має ще одну перевагу: якщо в цільовій системі є засоби безпеки, що контролюють тільки цілісність виконуваних файлів, але не виконують перевірку пам'яті, backdoor виявлений не буде [10].

3.1.7. Aircrack-ng

Aircrack-ng - набір інструментів, які дозволяють перевіряти безпеку бездротових мереж. Пакет включає інструменти для виконання таких завдань.

- Моніторинг. Це інструменти, розроблені спеціально для захоплення трафіку з метою подальшого аналізу.
- Атака. Інструменти для атаки цільових мереж. До їх складу входять засоби, які виконують атаку під час перевірки даних користувача (аутентифікації). Крім того, Aircrack-ng в момент атаки здатний проводити ін'єкції пакетів, що відправляються в бездротовий потік даних як клієнтам, так і точці доступу.

- Тестування. Ці інструменти дозволяють тестувати бездротові карти.
- Злом. Aircrack-ng також може зламувати попередні бездротові ключі, знайдені в WEP, WPA і WPA2.

Крім інструментів, працюючих в командному рядку, Aircrack-ng використовується в ряді інструментів з графічним інтерфейсом [11].

3.2.Підготовчий етап

На даному етапі почнемо процес аудиту. Кроки, які будуть описуватись в подальшому і будуть формувати методологію цілком безкоштовного аудиту, що є ключовим фактором створення даної системи. Аудит це вагомий модуль комплексу систем захисту інформаційних систем(мереж) і дана методологія створена для компаній або звичайних користувачів, які по різним причинам не можуть найняти спеціалістів з інформаційної безпеки. Ця версія проведення аудиту є неповною, так як в ній деякі етапи будуть не реалізовані. Такими етапами є:

- Дотримання стандартів безпеки, описані в політиці безпеки. Так як в описанні методології використовується тестова мережа, яка була створена спеціального для даної задачі, то політика безпеки не є доцільним елементом інформаційної системи.
- Розробка плану аудиторами та клієнтом. В даному випадку аудитор і клієнт є однією людиною і план буде створений для демонстрації проведення аудиту.
- Соціальна інженерія. Наявність людей в мережі є невід’ємним елементом, бо мережі існують тільки для того, щоб створити можливість клієнтам «контактувати» між собою. Найбільшою вразливістю комп’ютерних систем є людина і при реалізації аудиту цей фактор враховувався.

- Тестування фізичної безпеки. Фізична організації мереж дуже різноманітна і зробити універсальний метод перевірки даного критерія неможливо.
- Оформлення відповідних документів. При реальному аудиту в компаніях обов'язковим є створення різних нормативних документів. Ці документи мають різний формат в різних компаніях. Це і є причиною відмови від формальності в даній методології.

Опис етапів та мети аудиту

До реалізації технічної частини аудиту потрібно чітко встановити мету та ціль тесту. В нашому випадку метою є:

- Перевірка захищеності системи авторизації в мережу за допомогою бездротової технології Wi-Fi.
- При підключенні до мережі знайти всі можливі вразливості, які можуть призвести до негативних наслідків.
- Формування звіту про роботу, яка була проведена.

Правила проведення аудиту:

- При реалізації тесту забороняється виконувати дії, які не можна буде відновити по завершенню.
- Всі інформація, яка була отримана повинна документуватися у звіт.
- Інформація та вразливості, які були отримані аудиторами повинні бути строго конфіденційні.
- Не використовувати знайдені вразливості для особистих цілей.

3.3.Проведення аудиту

3.3.1. Перевірка захищеності системи авторизації(Wi-Fi)

1. Перевірка мережевого інтерфейсу.

   Команда: sudo iwconfig

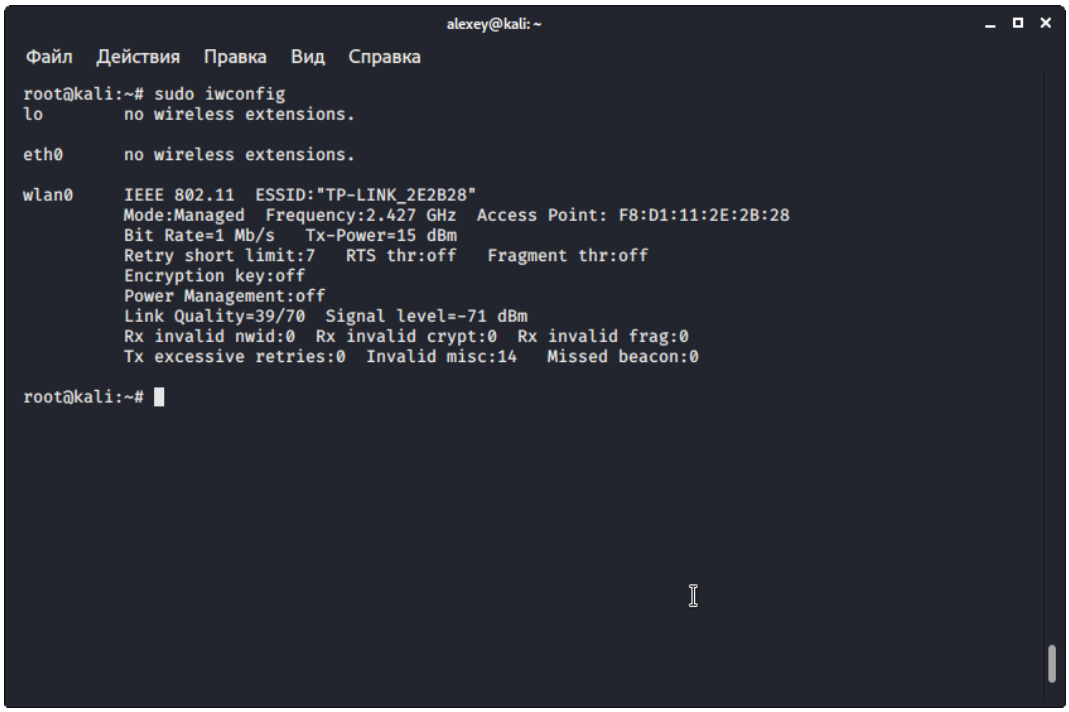

Рисунок 3.1 – Мережева конфігурація

2. Зміна режиму інтерфейсу.

В першу чергу задіємо інструмент airmon-ng. Він дозволяє перевести бездротову мережеву карту в так званий режим моніторингу. Це дуже схоже на зміну мережевого інтерфейсу в режим захоплення трафіку. Даний режим, в порівнянні зі звичайним, дозволяє захоплювати більше трафіку.

Команда: airmon-ng start wlan0

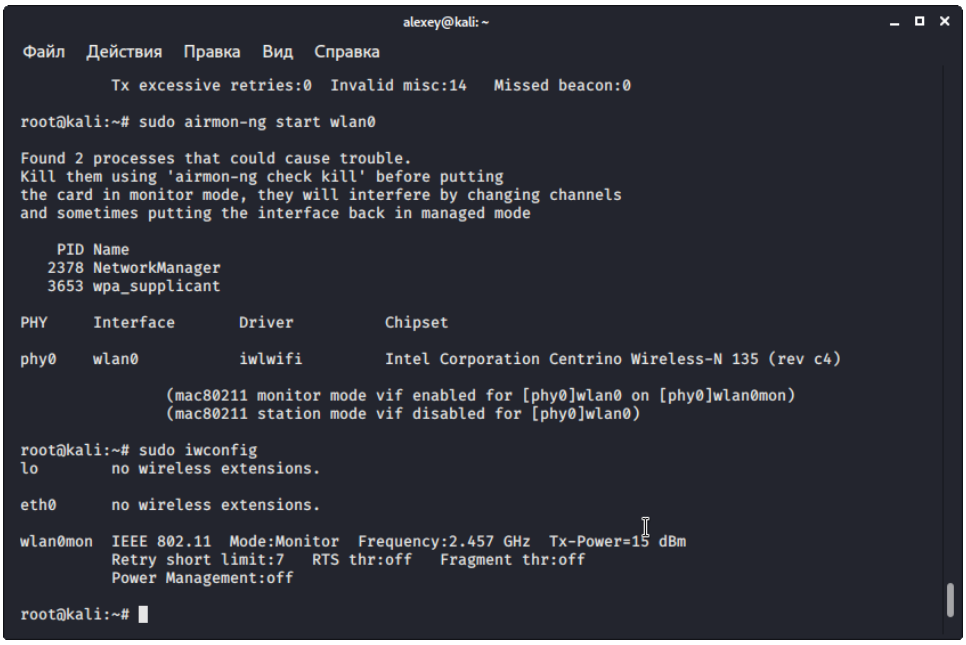

Рисунок 3.2 – Зміна режиму роботи мережевої карти

3. Сканування доступних мереж.

Тепер ми будемо використовувати команду airodump-ng для ідентифікації нашої цільової мережі. Інструмент airodump-ng буде працювати стільки, скільки буде потрібно для визначення цільової мережі. Як тільки бачимо цільову мережу, зупиняємо процес, натиснувши Ctrl + C. На екрані з'явиться наступний висновок, в якому буде показана цільова мережа.

Команда: sudo airodump-ng wlan0mon -c 4 --bssid f8:d1:11:2e:2b:28 -w wifi_crack

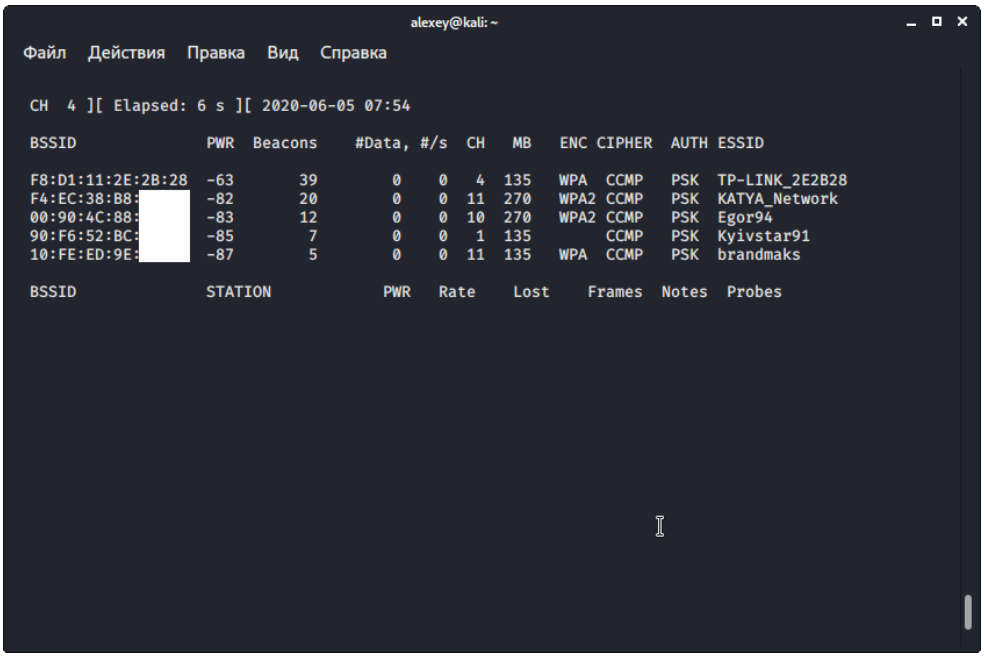

Рисунок 3.3 – Знайдені мережі при скануванні

4. Перехват трафіку(handshake)

На попередньому етапі було визначено три ключові елементи. По-перше, знайшли нашу цільову мережу, яка називається TP-LINK_2E2B28. По-друге, у нас є BSSID, який є MAC-адресою для цільової мережі: “F8:D1:11:2E:2B:28”. І нарешті, дізналися номер каналу: 2. Наступним етапом буде захоплення бездротового трафіку, що виходить з цільової точки доступу. Наша мета - захопити «чотиристоронє рукостискання». Щоб почати захоплення трафіку, вводимо відповідну команду.

Команда: sudo aireplay-ng -0 3 -a f8:d1:11:2e:2b:28 -c 2c:fd:ab:a9:a3:2a wlan0mon

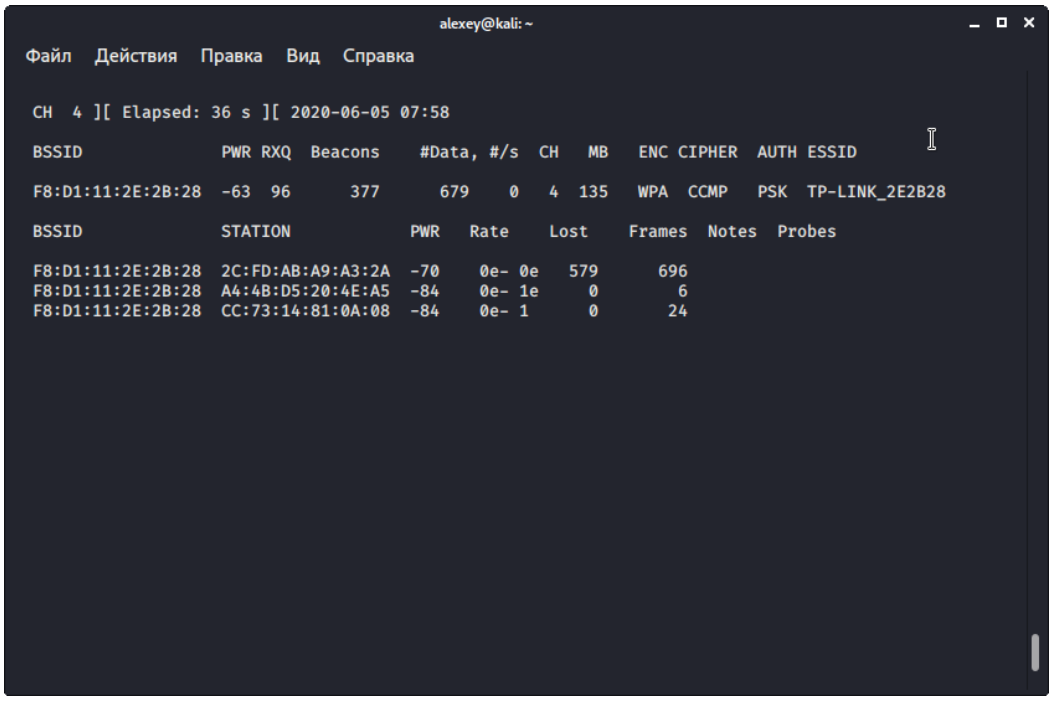

Рисунок 3.4 – Моніторинг трафіку

Сенс цієї команди наступний: airodump-ng повинен використовувати інтерфейс моніторингу для захоплення трафіку бездротової мережевої карти, MAC-адреса якої - “F8:D1:11:2E:2B:28”, і каналу цільової мережі.

Якщо при моніторингу не вдалося отримати рукостискання WPA(не треба витрачати час на дії одного користувача), шукаємо користувача, який звертається до мережі. У даному випадку ми бачимо станцію, підключену до цільової бездротової мережі з MAC-адресою «2C:FD:AB:A9:A3:2A». Оскільки цей пристрій аутентифікований, швидше за все, після обриву зв'язку (деаутентіфікаціі) знову почнеться процес автоматичного підключення. Щоб ініціювати обрив зв'язку, введемо в командний рядок відповідну команду.

Команда: aireplay-ng -0 3 -a F8:D1:11:2E:2B:28 - c 2C:FD:AB:A9:A3:2A wlan0mon

Команда aireplay-ng дозволяє вводити пакети в комунікаційний потік і деаутентіфікувати клієнта. Це змусить клієнта виконати нове рукостискання WPA, яке ми, в свою чергу, можемо захопити.

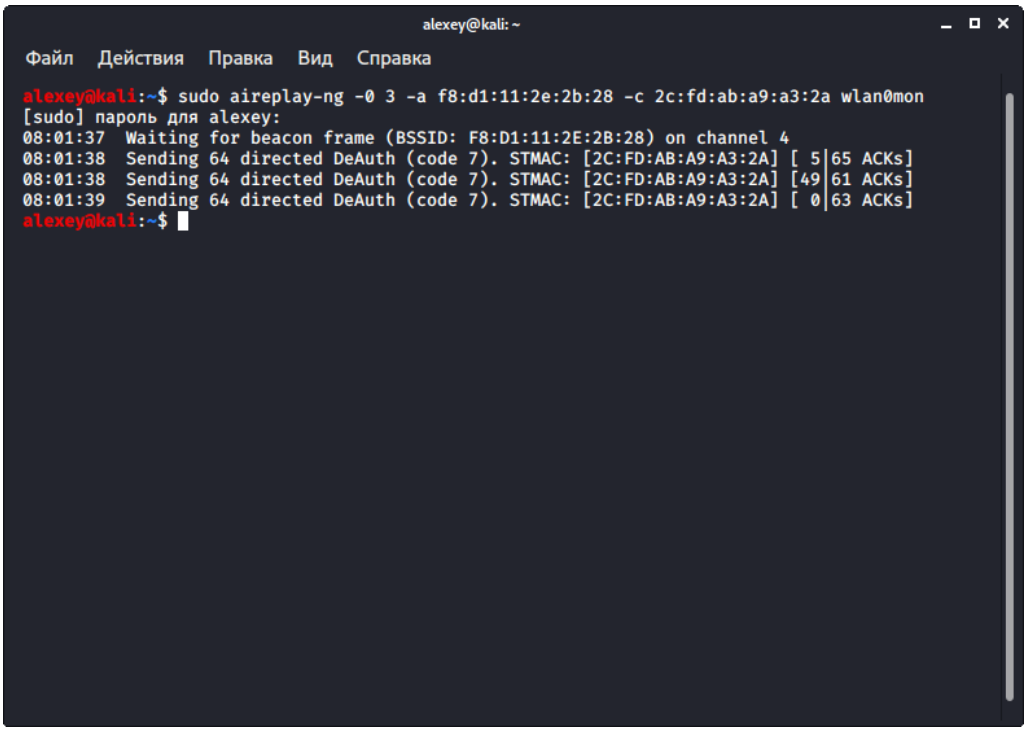

Рисунок 3.5 – Деаутентифікація користувача

Після виконання цієї команди ми отримали бажану інформацію.

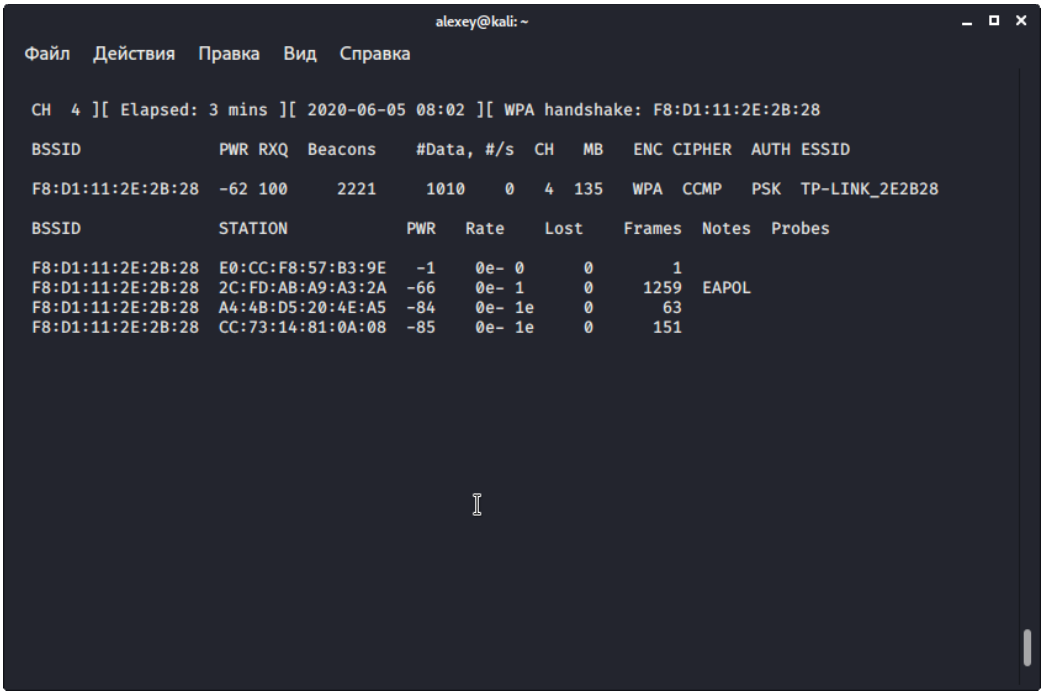

Рисунок 3.6 – Успішний результат перехвату трафіку

5. Злом паролю.

Тепер у нас є інформація, необхідна для злому попереднього загального ключа WPA. Для цього ми скористаємося інструментом Aircrack-ng. Нижче наведена однойменна команда.

Команда: sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt -b F8:D1:11:2E:2B:28 wifi_crack-01.cap

У цій команді ми ідентифікуємо BSSID цільової мережі з параметром -b. Потім вказуємо на файл захоплення wifi_crack-01.cap. Нарешті, ми використовуємо список слів приблизно так, як зламували б файл пароля. В цьому випадку був обраний список з файлу rockyou.txt. На підставі списку паролів rockyou.txt Aircrack-ng перевірить кожну комбінацію захопленого файлу. Якщо використовуваний в попередньому етапі код доступу є в файлі, то Aircrack-ng видасть повідомлення про успішне закінчення перевірки.

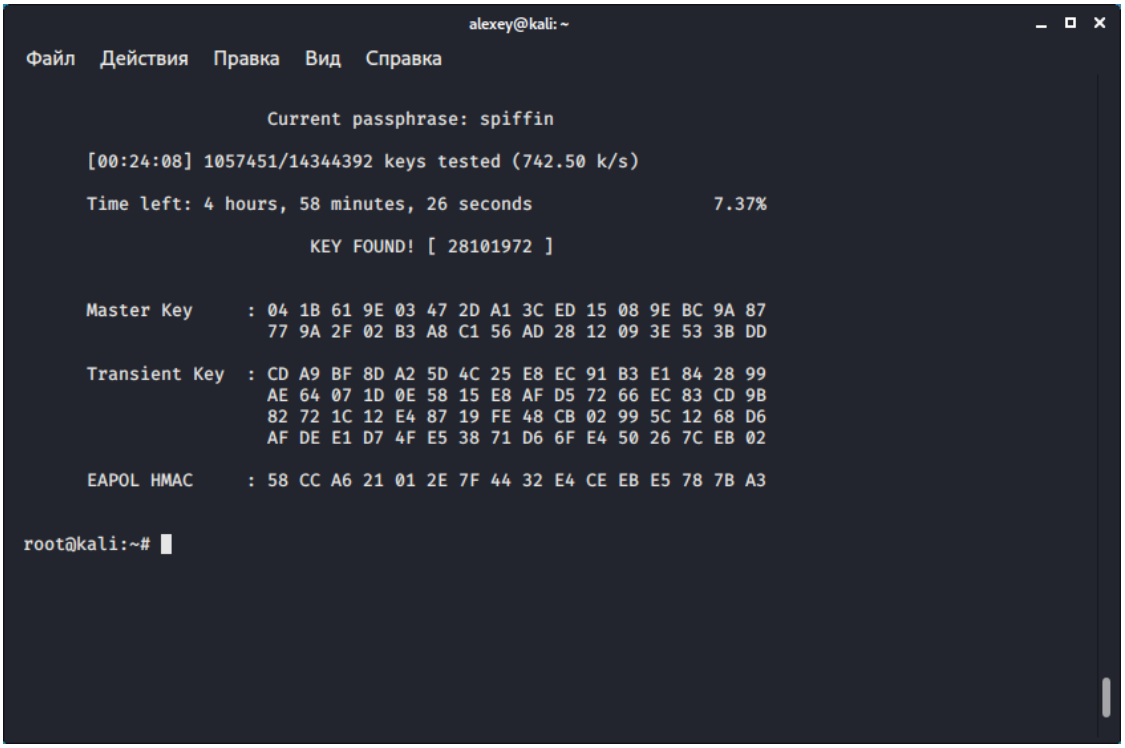

Рисунок 3.7 – Успішний підбір паролю

В даному випадку ми використовували один з найкращих стандартних наборів паролів. Даний процес може займати великий проміжок часу в залежності від складності паролю та ефективності системи. В подальшому ми будемо використовувати бази паролів, в яких вже буде правильний пароль. Це

прискорить час тестування. Для кожної системи треба створювати свої бази паролів, бо важливу роль грають наприклад такі параметри: географічне розташування, правила створення паролів, сфера використання і т.д.

6. Підключення до мережі.

Пароль, який ми отримали, дає змогу підключитись до мережі.

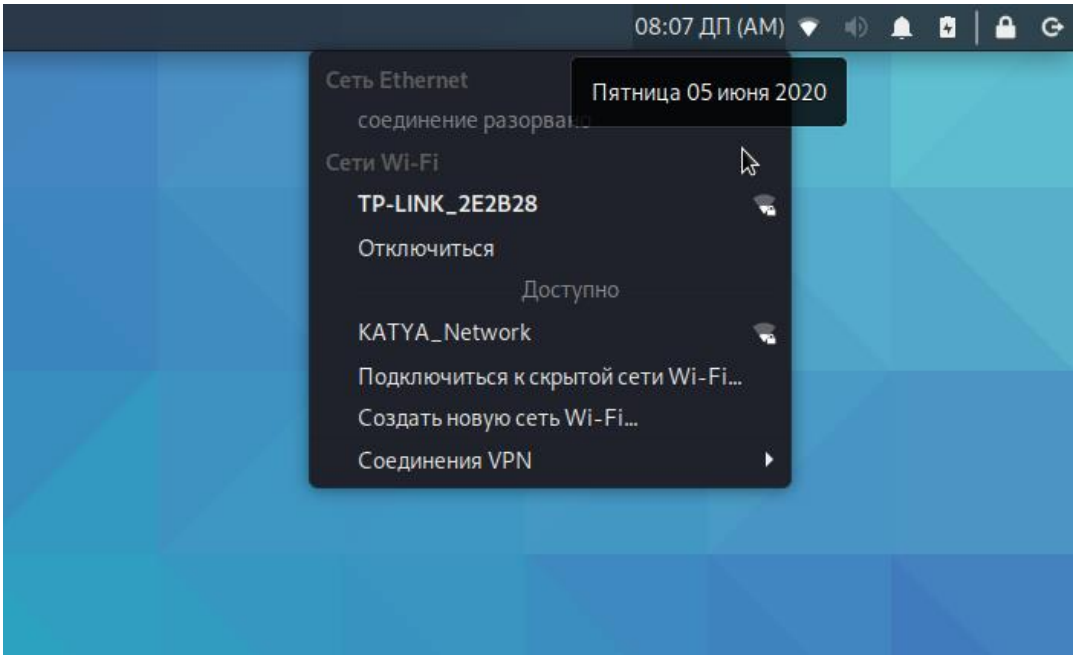

Рисунок 3.8 – Результат злому Wi-Fi

3.3.2. Сканування мережі

1. Ідентифікація в мережі.

Після отримання доступу до мережі атакуюча система автоматично ідентифікується в мережі. Для того, щоб дізнатися яку IP адресу виділив маршрутизатор вводимо команду: ip a. При роботі в мережі, будь-яка активність хостів транслюється через маршрутизатор. Для цього в кожному клієнті мережі є шлях за замовчуванням, який надалі буде опрацьовувати запити(default gateway). Для визначення адреси маршрутизатора використовуємо команду: sudo route.

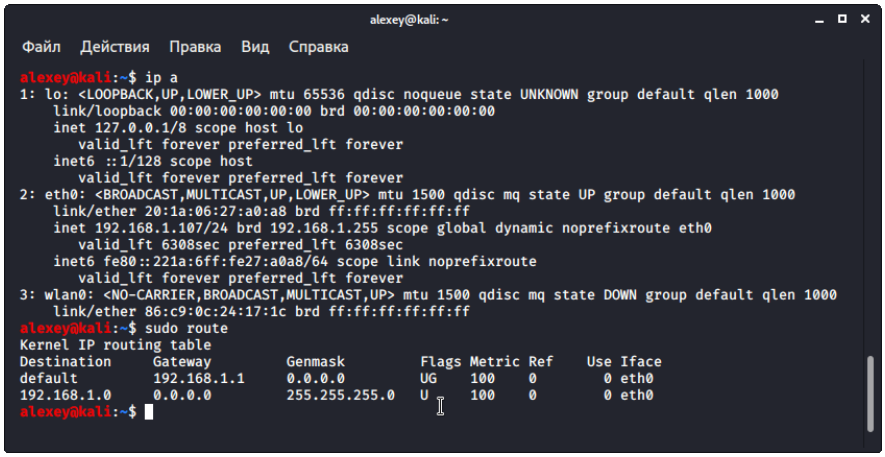

Рисунок 3.9 – Пошук початкових адрес

2. Пошук систем підключених до мережі.

В даному випадку використовується стандартна команда: arp -a. В результаті її роботи робимо висновок, що на даний момент в мережі є активні хости и можна продовжити сканування більш поглиблено.

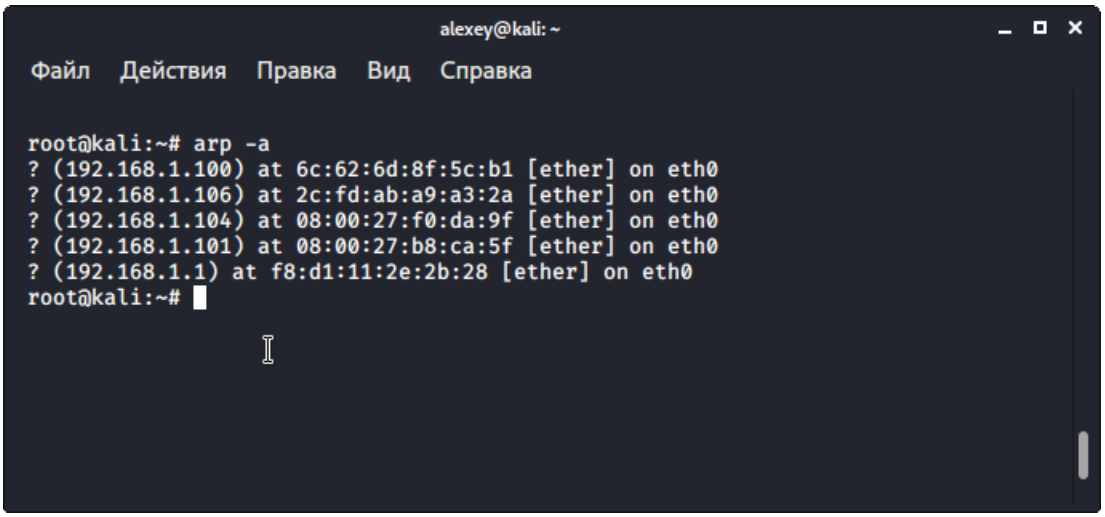

Рисунок 3.10 – Первинне сканування мережі

3. Поглиблене сканування мережі.

Для більш детального аналізу клієнтів в мережі використовується Nmap. В результаті успішних попередніх етапів можна оперувати інформацією про адрес мережі ті її маску. Адреса: «192.168.1.0». Маска: «255.255.255.0» або в форматі бітної маски - «24». Для сканування мережі для виявлення активних хостів використовуємо звичайне пінг-сканування. Для цього додаємо опцію «sP».

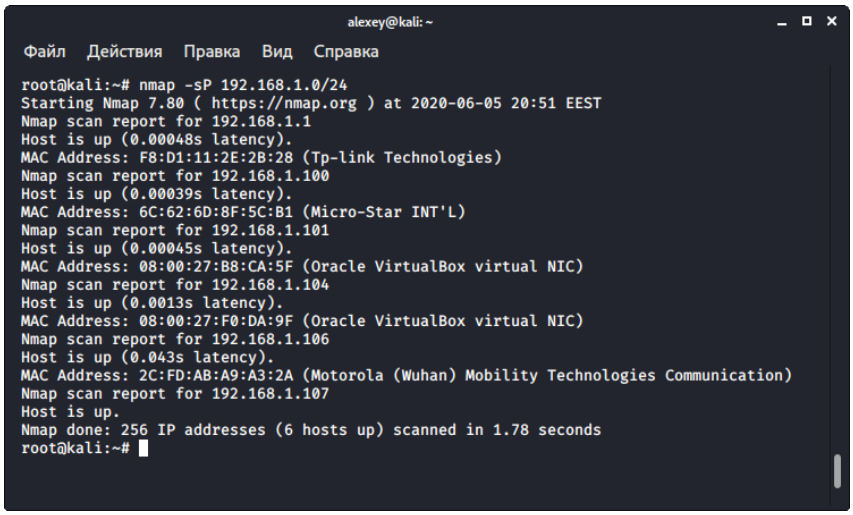

Рисунок 3.11 – Поглиблене сканування мережі на активні хости

Проаналізувавши результат роботи програми бачимо активні хости та деяку інформацію про них(MAC-адресу, IP адресу, назву виробника хоста).

4. Сканування мережевих пристроїв.

При скануванні мережевих пристроїв використовується опція «-v», яка дає більше інформації про роботу програми. Використання опції «-A» зможемо отримати таку інформацію:

- виявлення версії сервісу;
- виявлення операційної системи;
- сканування сценаріїв;
- трасування.

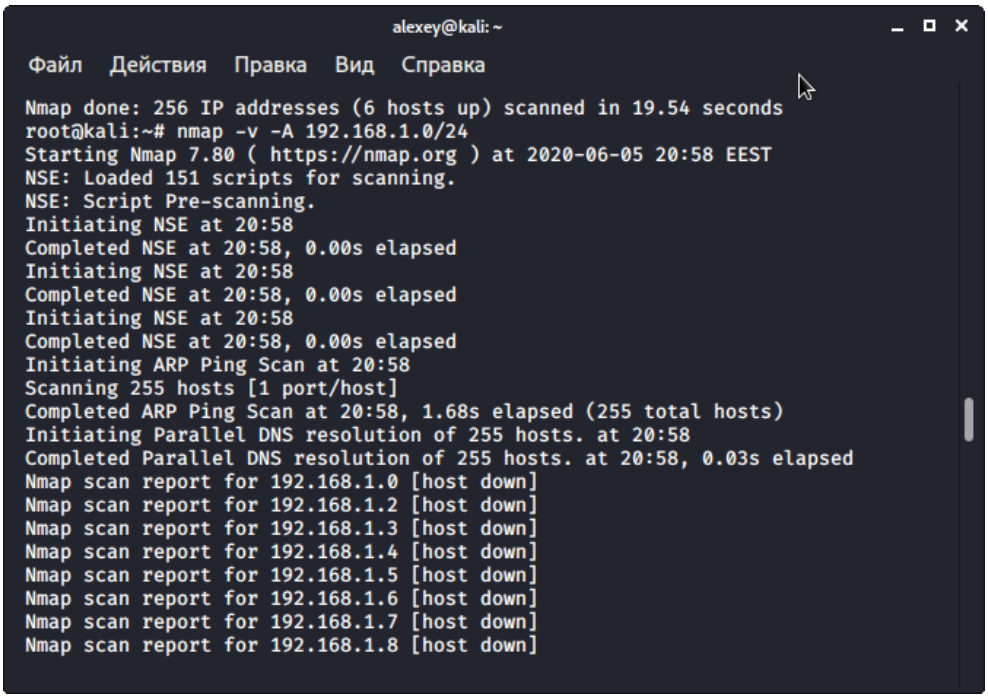

Рисунок 3.12 – Старт роботи сканування

При процесі сканування бачимо звіти для пристроїв. В кожному із них є інформація про відкриті порти системи(назва сервісу, версія сервісу), назву пристрою, тип пристрою, назва і специфікація операційної системи.

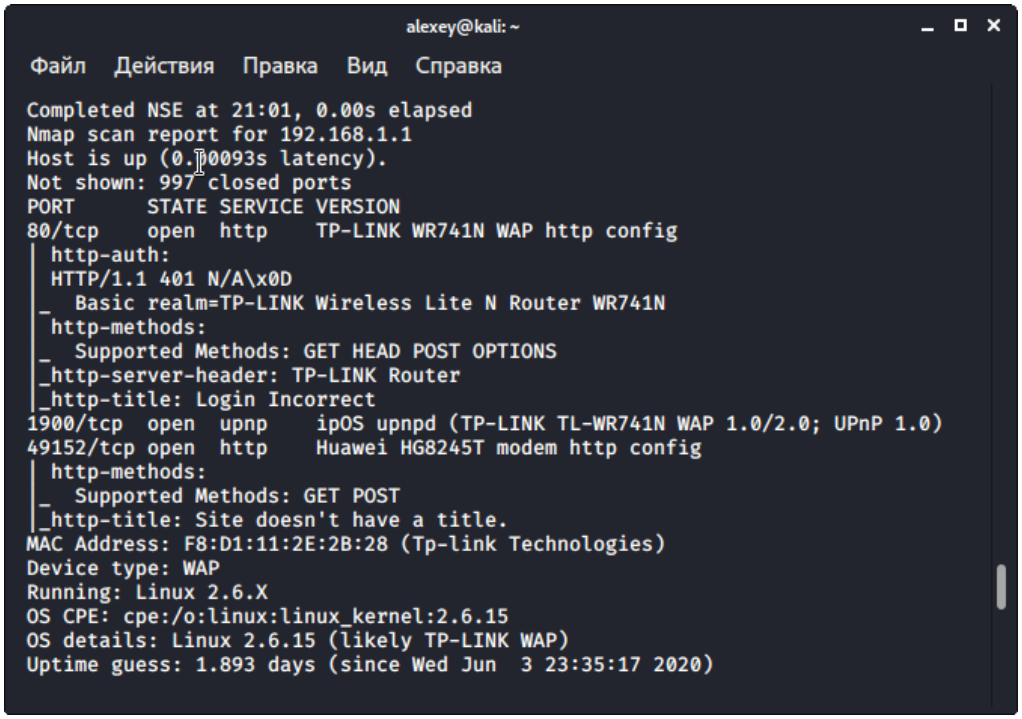

Рисунок 3.13 – Звіт сканування портів для 192.168.1.1

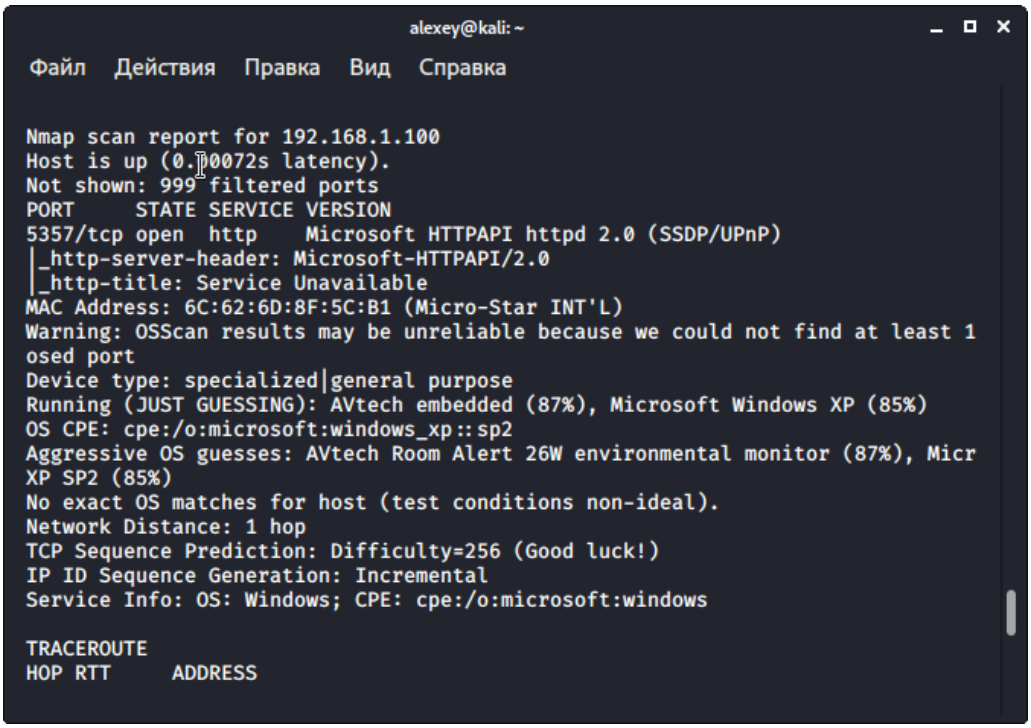

Рисунок 3.14 – Звіт сканування портів для 192.168.1.100

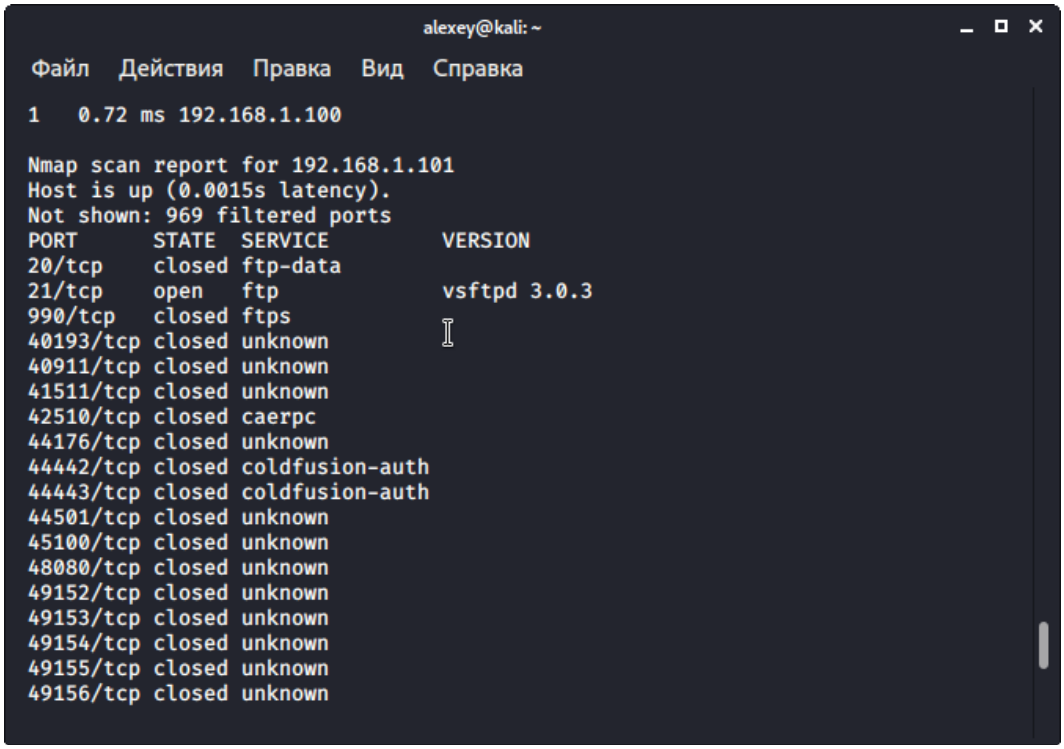

Рисунок 3.15 - Звіт сканування портів для 192.168.1.101

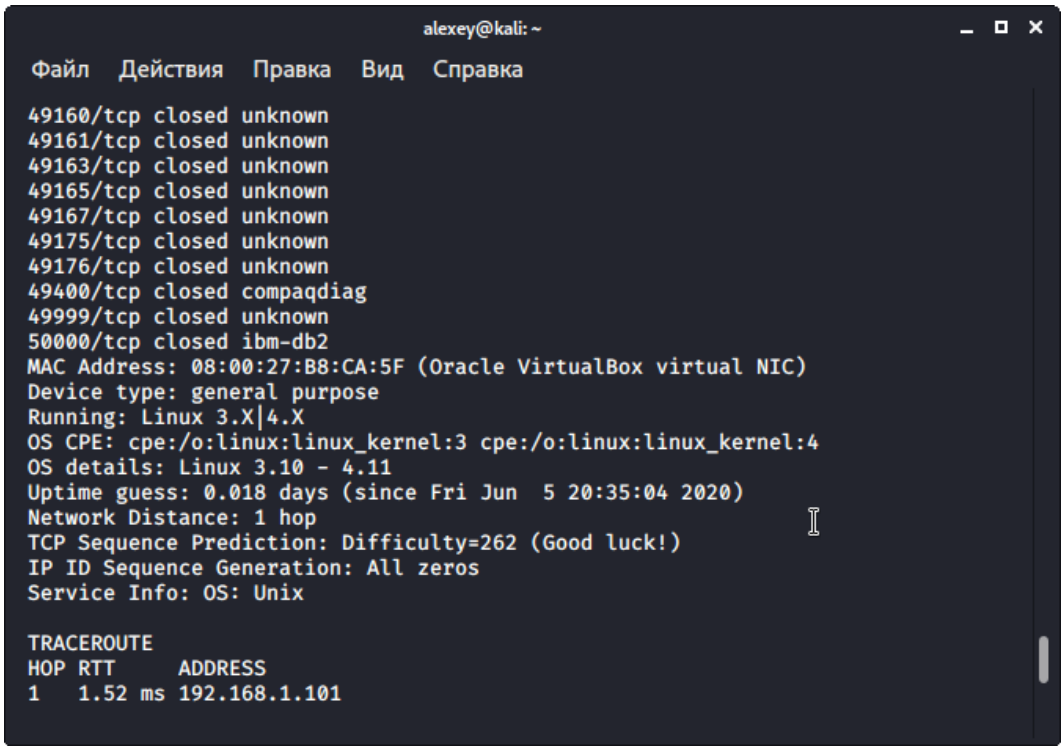

Рисунок 3.16 - Звіт сканування портів для 192.168.1.101

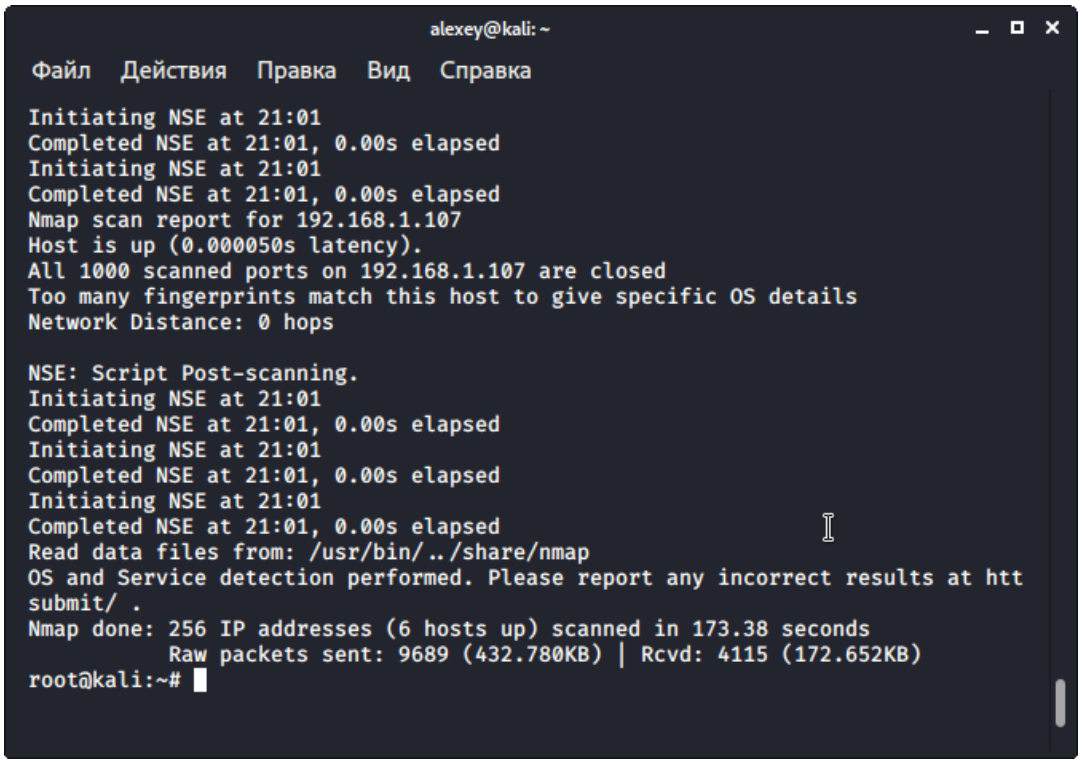

Рисунок 3.17 – Підсумки сканування мережі

В кінці роботи програми бачимо підсумки всього сканування.

3.3.3. Сканування вразливостей.

Сканування вразливостей - процес виявлення і аналізу критичних недоліків безпеки в середовищі. Іноді цю операцію називають оцінкою вразливості. Сканування вразливостей - одне з основних завдань програми виявлення та усунення цих недоліків. З його допомогою можна проаналізувати всі елементи управління безпекою IT-інфраструктури. Сканування вразливостей проводиться після того, як було виявлено і зібрано інформацію про інфраструктуру цільової системи. Інформація, отримана після сканування системи на уразливості, може привести до компрометації цільової системи, порушення її цілісності та конфіденційності. Для реалізації даного етапу використовується додаток OpenVAS.

При скануванні мережі були виявлені активні хости, які будемо сканувати. Для сканування використаємо “Task Wizard”, в якому впишемо відповідні IP адреси та тип сканування. В нашому випадку це «Full and Fast».

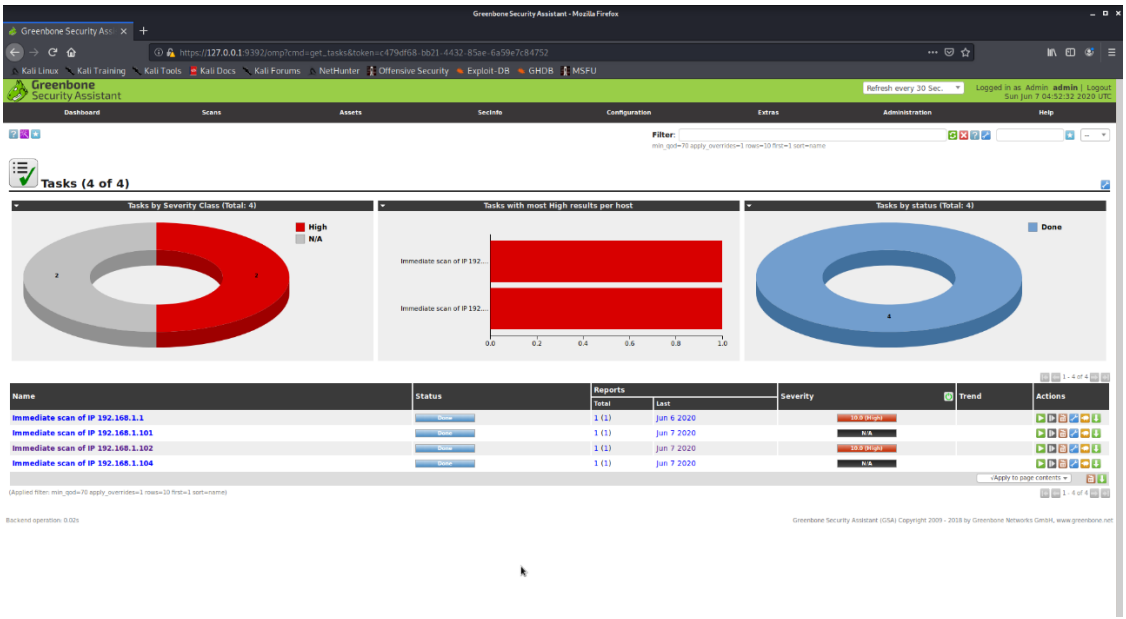

Рисунок 3.18 – Завдання сканування OpenVAS

Після закінчення сканування в вкладці завдань можемо отримати загальну інформацію про результати сканувань(Назву, статус, кількість та дата звітів, пріоритет).

Для перегляду повного списку результатів сканування(вразливостей) переходимо в відповідне вікно. На цьому кроці можемо спостерігати

статистику у графічному вигляді сканувань і більш повну картину всіх вразливостей.

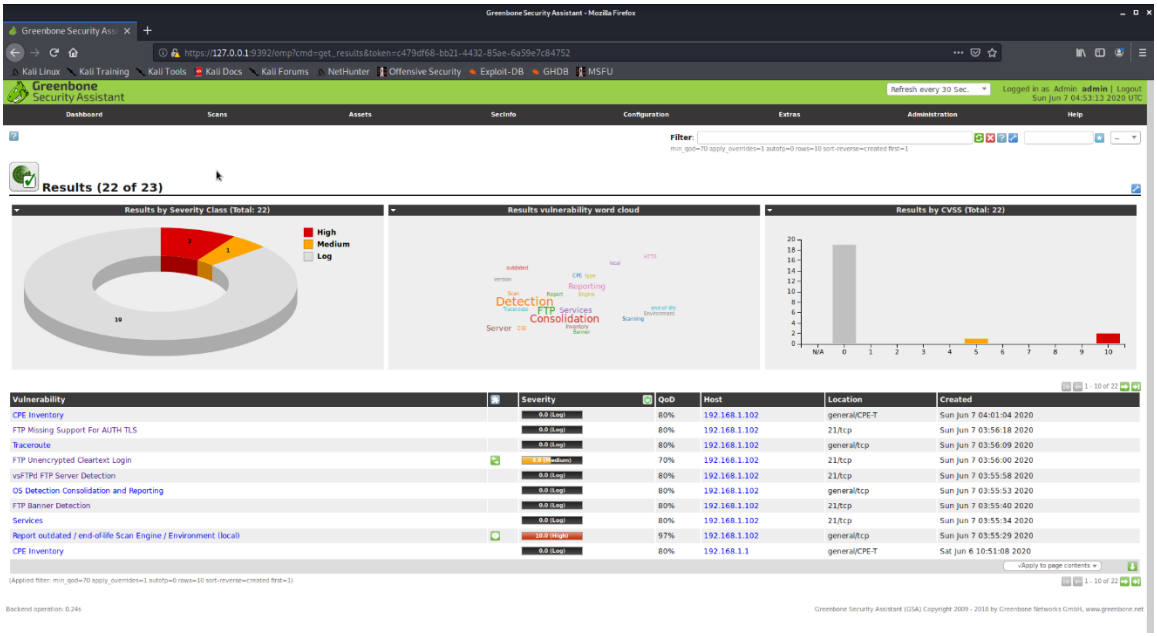

Рисунок 3.19 – Результати сканування OpenVAS

Розглянемо деталі сканування для кожного хоста. В даному вікні є вся інформація про сканування одного елементу. Важливим є пункти «Reports» та «Results».

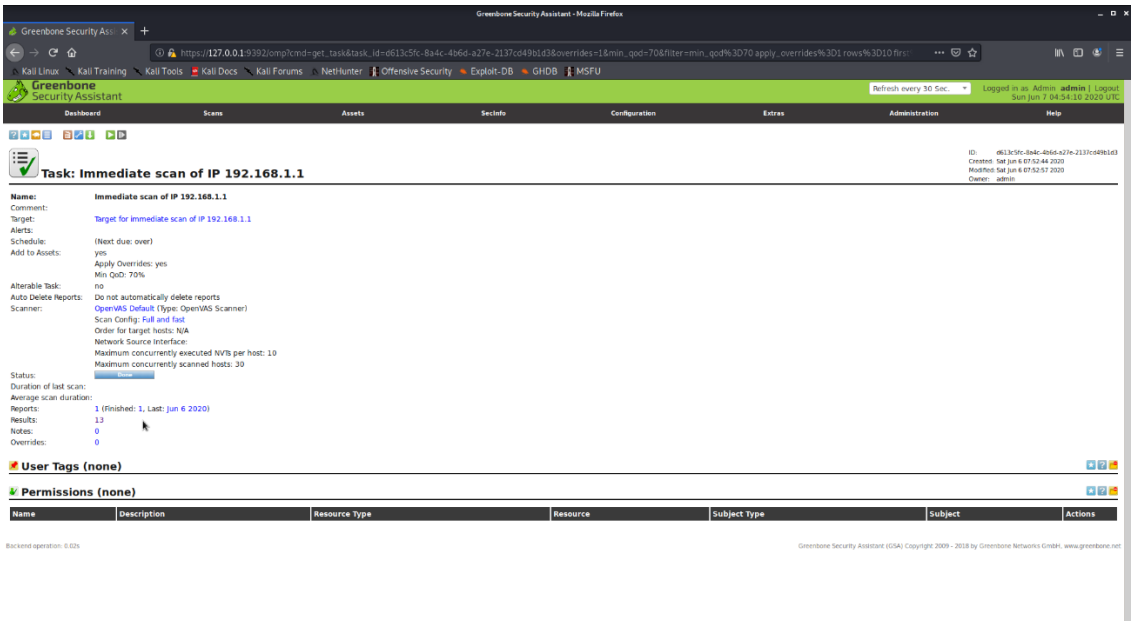

Рисунок 3.20 – Завдання 192.168.1.1 OpenVAS

При переході до вкладки «Results» бачимо всі вразливості, які були отримані при скануванні даного елемента мережі. За допомогою графічного

зображення аналізу вразливостей та списку вразливостей можна отримати певні висновки про стан захисту даної системи.

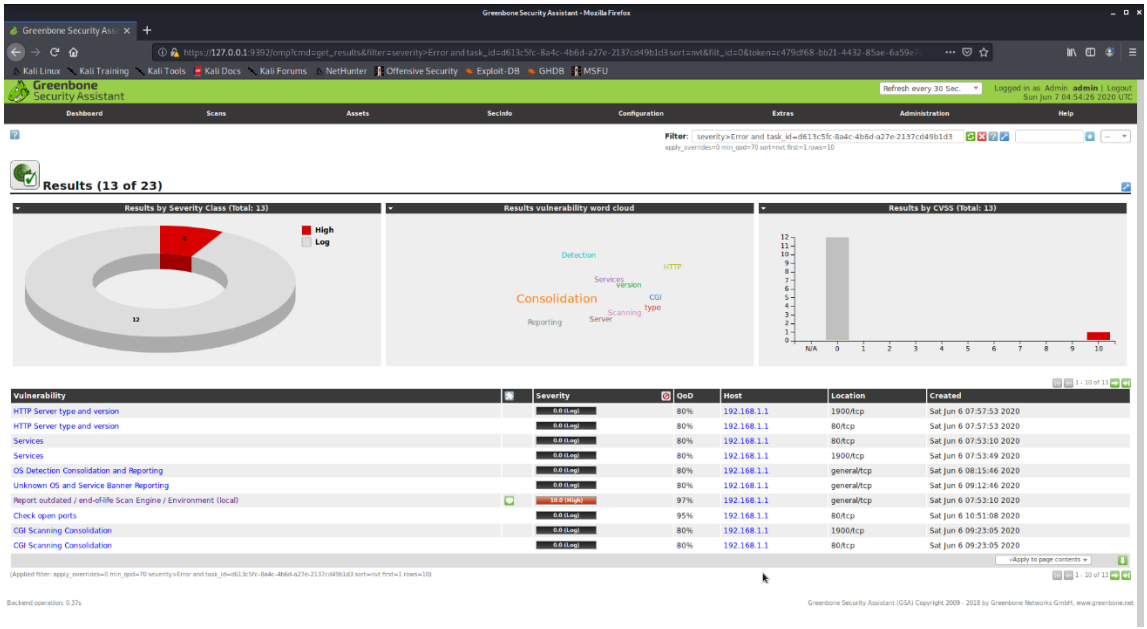

Рисунок 3.21 – Результати для 192.168.1.1 OpenVAS

Також є можливість отримати детальну інформацію про кожну вразливість натиснувши на її назву в списку всіх вразливостей.

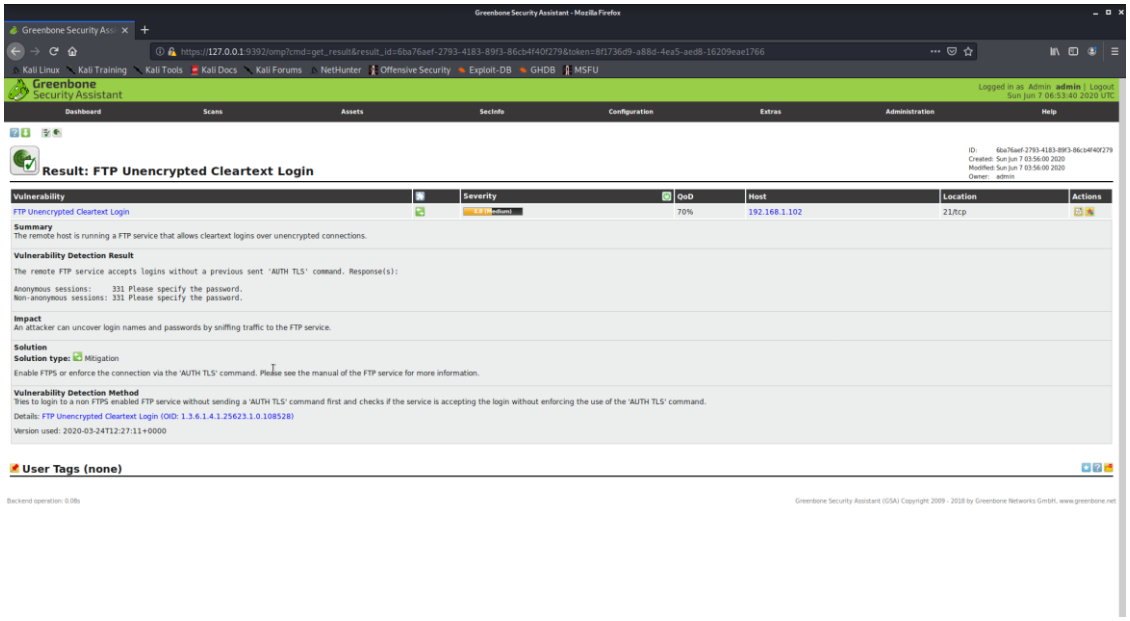

Рисунок 3.22 – Звіт для однієї вразливості OpenVAS

В даному звіті згенерована інформація про такі параметри(для кожної вразливості різні звіти):

1. Загальний опис проблеми.

2. Вплив.
3. Спосіб вирішення даної проблеми.
4. Метод знаходження.
5. Результат знаходження.
6. Корисні посилання.

3.3.4. Експлуатація вразливостей

Metasploit це дуже потужний додаток за допомогою якого можна реалізувати багато різних атак, сканувань і т.д. Його ми і будемо використовувати для експлуатації знайдених вразливостей у попередніх етапах.

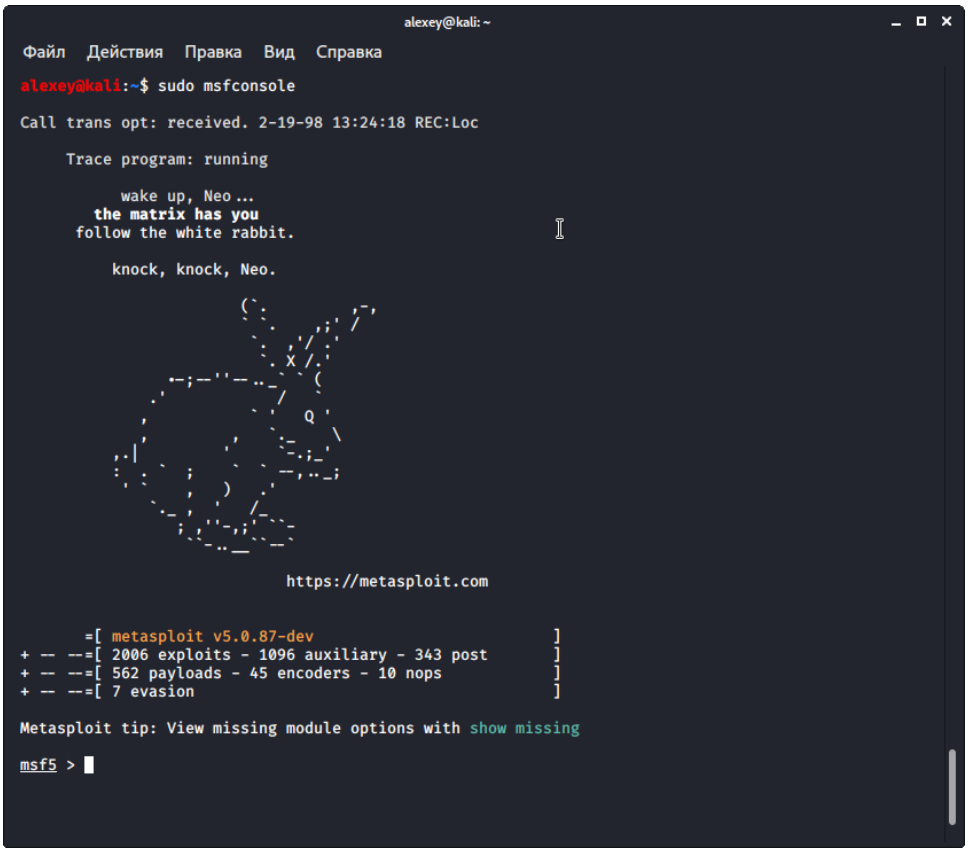

Рисунок 3.23 – Metasploit

Цільова експлуатація - одна з областей, в якій крім оцінки вразливостей, виконується тест на проникнення. Тепер, коли уразливості знайдені, для отримання доступу і повного контролю над цільовою системою є можливість скористатися знайденими вразливостями. Почнемо тест з 192.168.1.104.

Використовуючи IP-адреса атакуючої машини, ми можемо чітко відрізнити зворотню оболонку від прив’язаної. Якщо в оболонці прив'язки не потрібно вказувати IP-адреса атакуючої машини, в конфігурації зворотної оболонки потрібна IP-адреса машини зловмисника (наприклад, LHOST 192.168.1.107). Вбудоване корисне навантаження(PAYLOAD) - це автономний код оболонки, який повинен виконуватися з одним екземпляром експлойта. Поетапне корисне навантаження при виконанні конкретного завдання для зчитування іншої частини проміжного коду оболонки створює зворотний канал зв'язку між машиною зловмисника і машиною жертви. Зазвичай вибирають поетапне корисне навантаження.

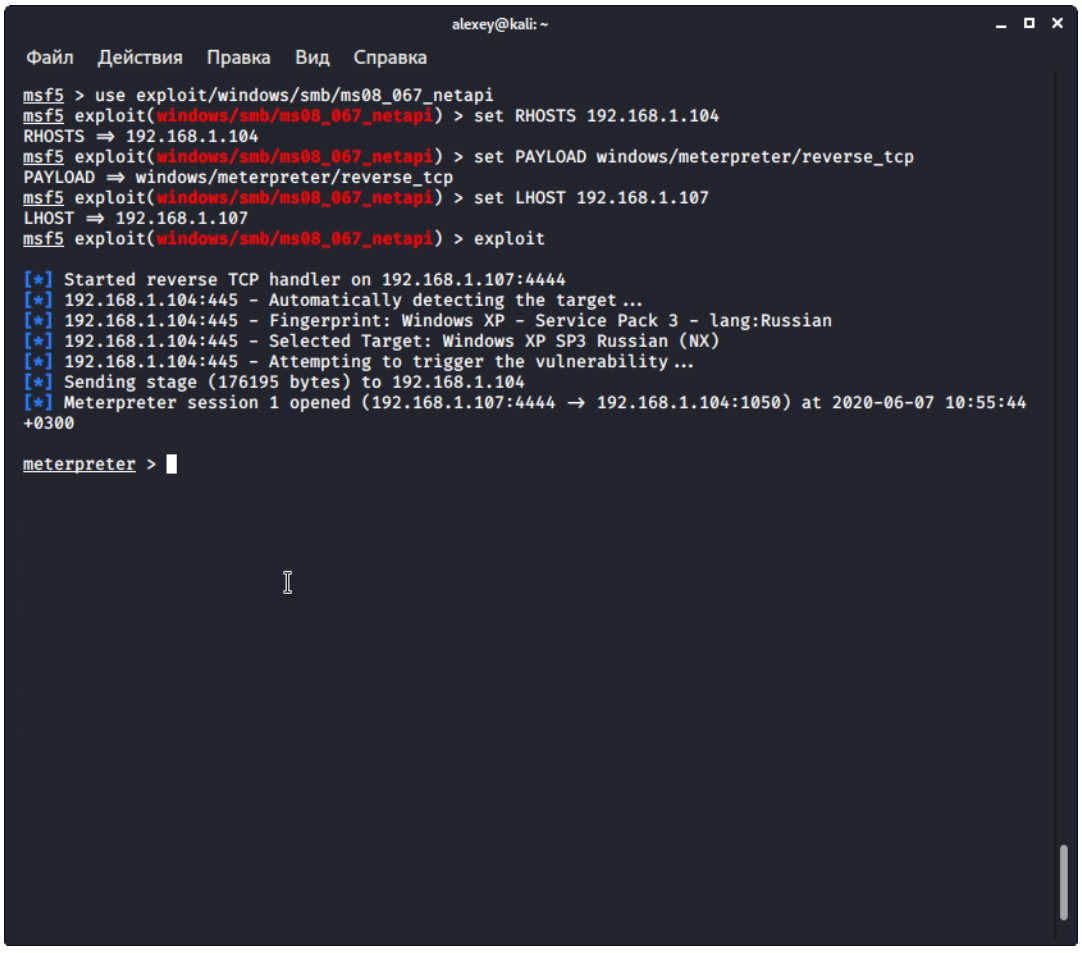

Рисунок 3.24 – Metasploit 192.168.1.4

Meterpreter - це новітня шифрована багатогранна і динамічно розширюване корисне навантаження, яке працює, вводячи відбитий DLL в цільову пам'ять. Для розширення діяльності після експлуатації сценарії і

плагіни можуть динамічно завантажуватися під час виконання. В цьому випадку ми зможемо налаштовувати привілеї, скидати системні облікові записи, використовувати постійну службу чорного ходу (backdoor) і включення віддаленого робочого столу. Крім того, весь зв'язок оболонки Meterpreter шифрується за умовчанням.

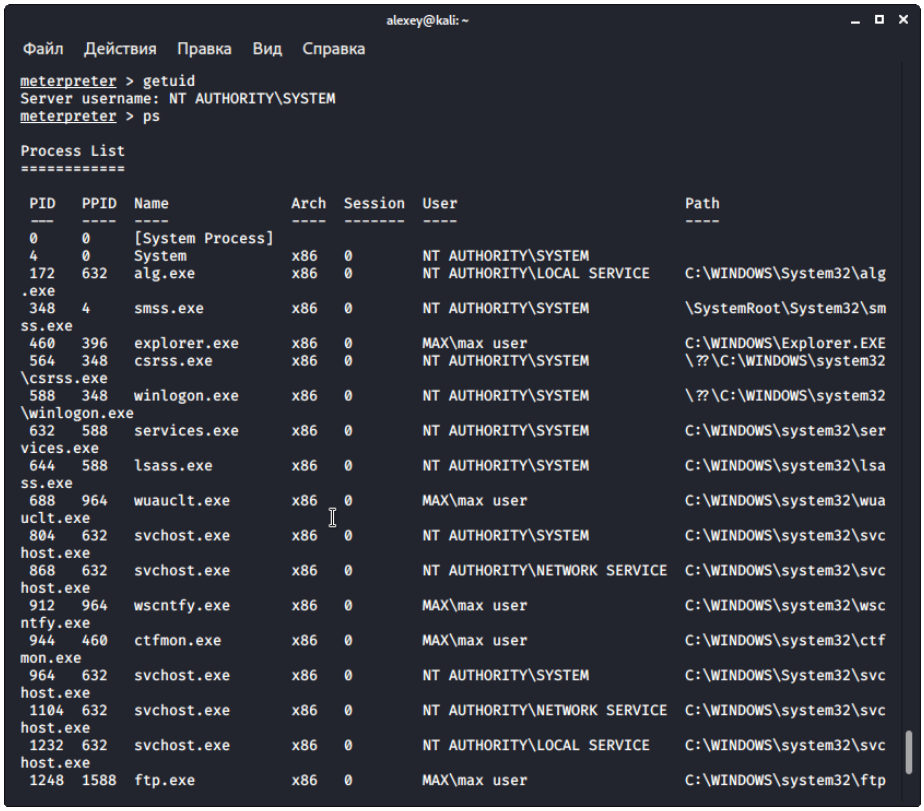

Рисунок 3.25 – Meterpreter 192.168.1.104

На даному етапі ми для початку реєстрації поточної активності користувача в системі перенесемо оболонку Meterpreter в процес explorer.exe

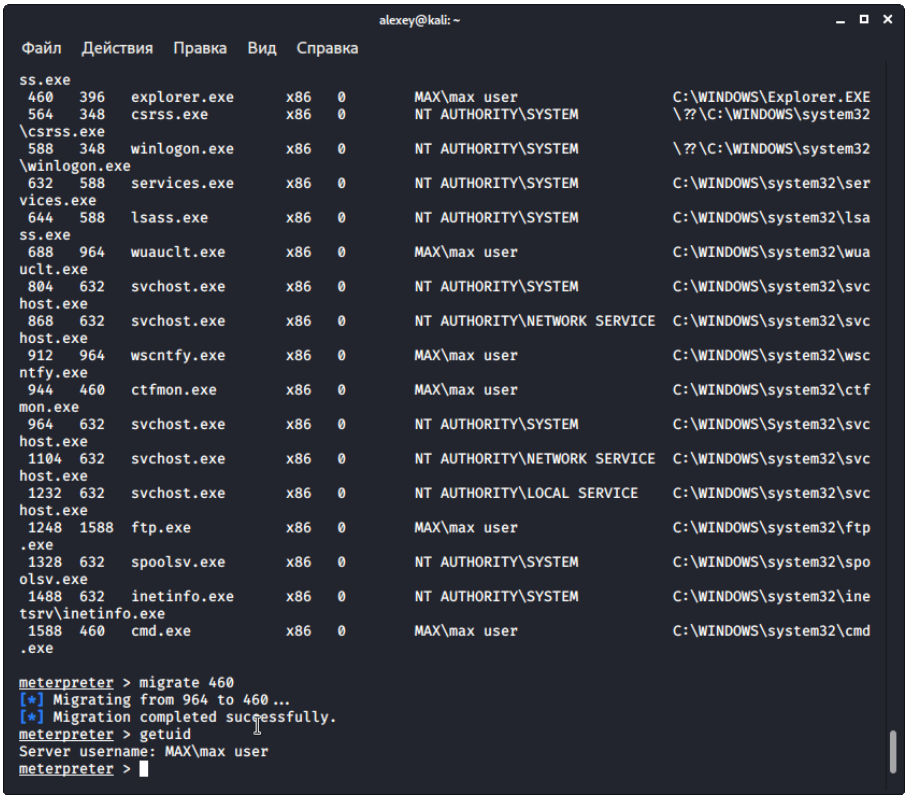

Рисунок 3.26 – Meterptreter migrate

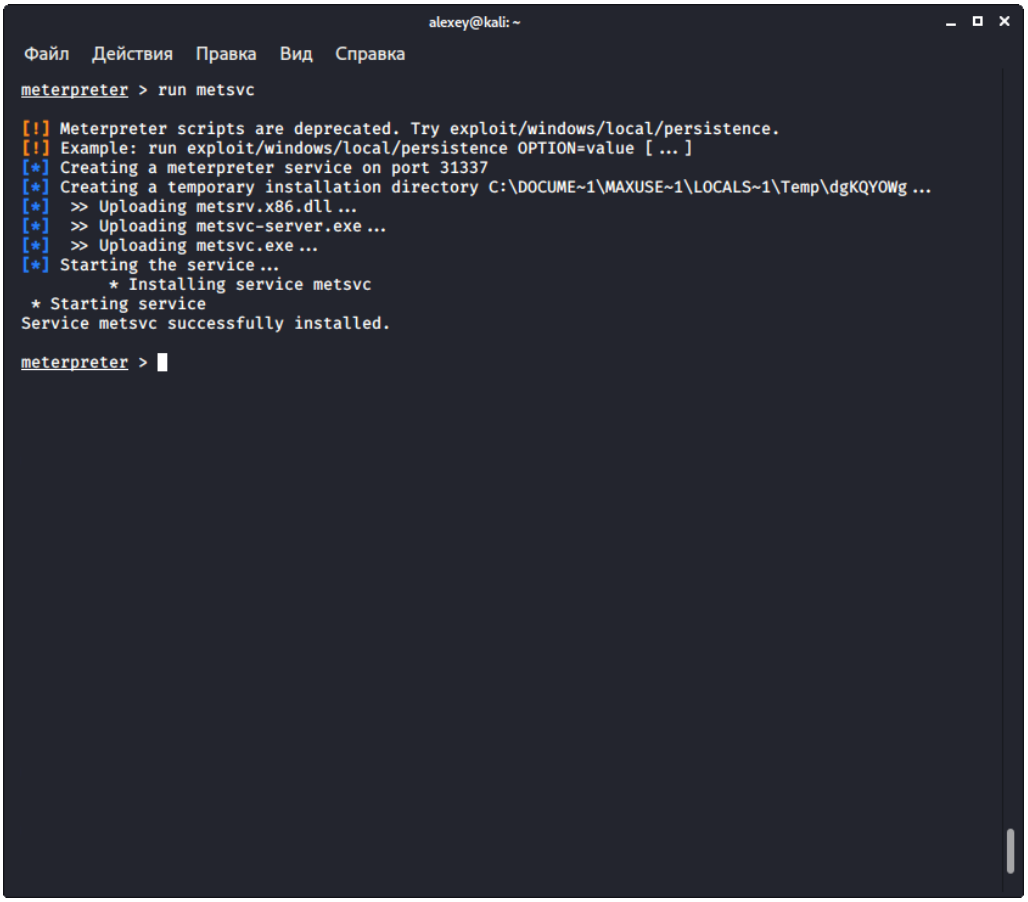

Рисунок 3.27 – Meterptreter metsvc

Отже, для цільової машини був запущений бекдор. Для взаємодії з нашим бекдор-сервісом закриємо поточний сеанс Meterpreter і коли нам буде потрібно, використовуємо multi / handler з корисним навантаженням windows / netsvc_bind_tcp.

Авіавіа

Наступна ціль це ftp сервер, який працює на базі ОС Ubuntu server(попередні етапи). Використаємо спеціальний додаток, який дає можливість налаштувати проникнення до серверу. Логін користувача(логіни з баз логінів які можна знайти), ціль атаки, поточність і вимкнемо параметр, який відповідає за відображення підбору паролів.

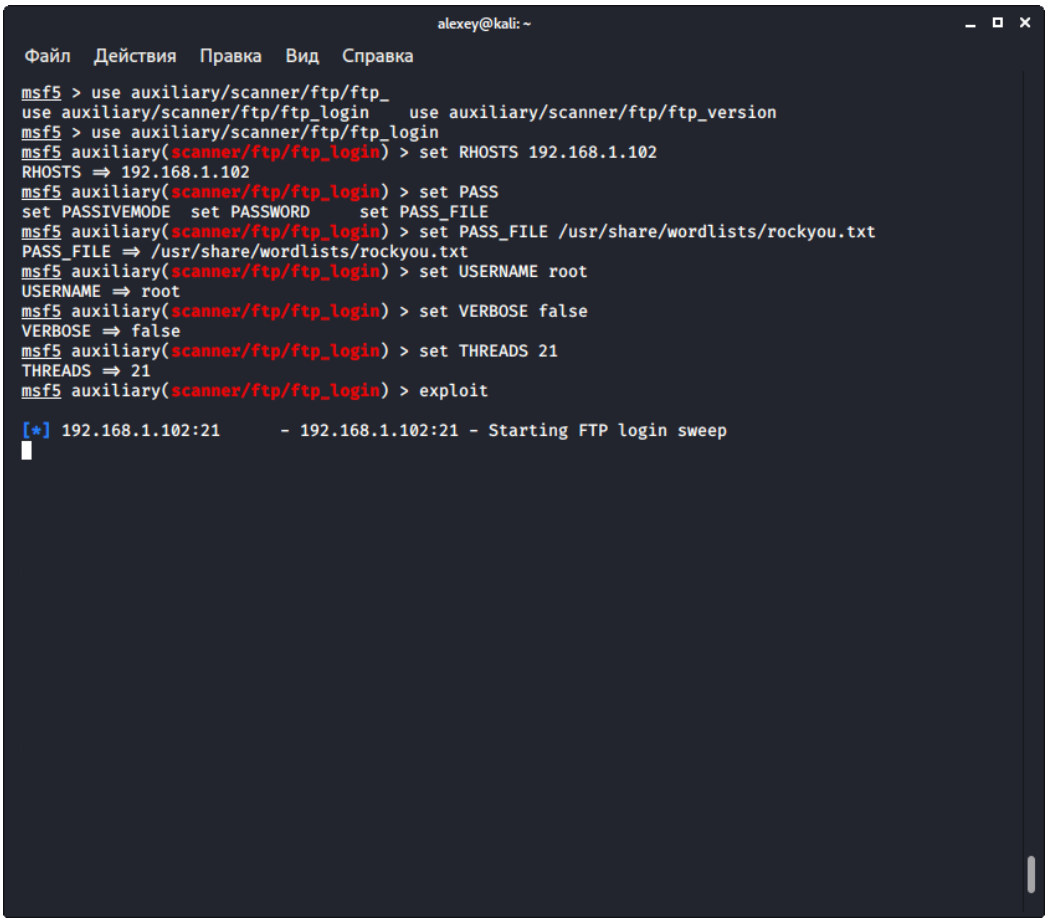

Рисунок 3.28 – Metasploit 192.168.1.102

3.3.5. Етап після експлуатації.

І снує два способи використання Mimikatz з Metasploit Перший - з повним спектром функцій Mimikatz Відповідна команда починається з

mimikatz_command. Іншою особливістю є можливість пошуку облікових даних на скомпрометованій машині.

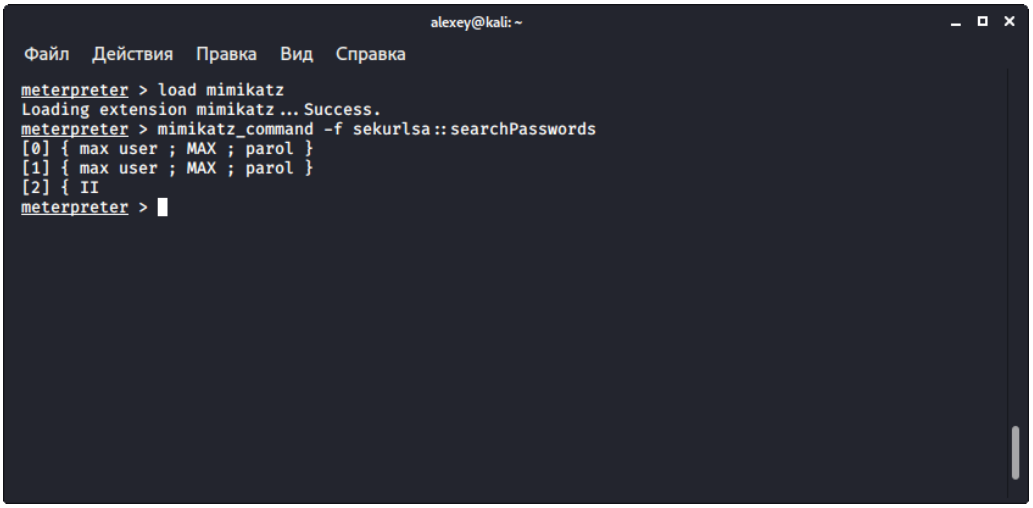

Рисунок 3.29 – mimikatz пошук паролів 192.168.1.104

На виході ми бачимо, що Mimikatz зміг отримати пароль адміністратора для системи.

Інша команда Metasploit, яка використовує Mimikatz, - Kerberos, яка на скомпрометованому комп'ютері отримає облікові дані у вигляді відкритого тексту.

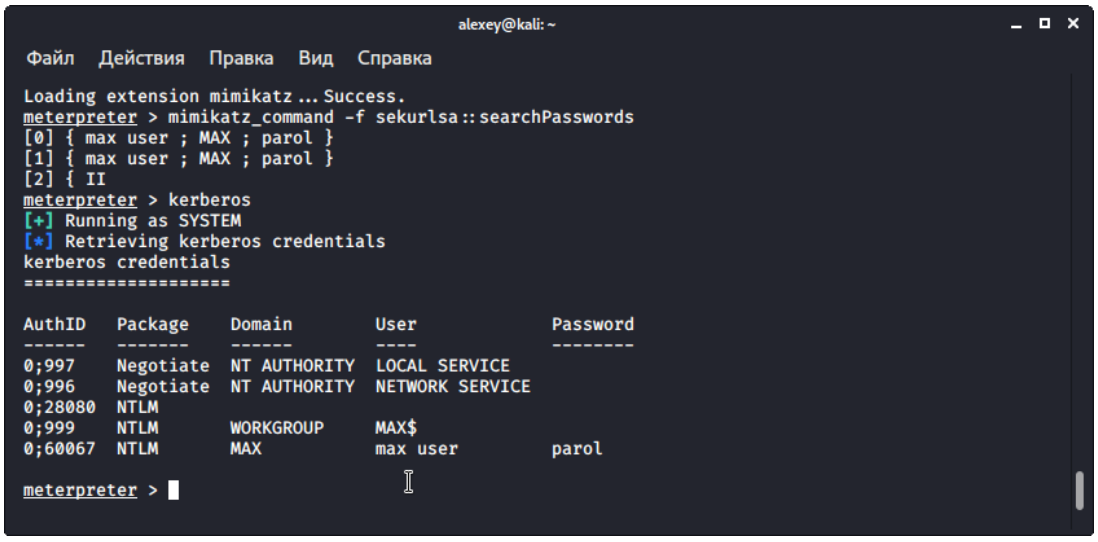

Рисунок 3.30 - mimikatz пошук облікових даних 192.168.1.104

Майте на увазі, що в Бекдор metsvc немає логіна і пароля для користувача. Тому будь-який, хто отримає доступ до порту бекдора, зможе його використовувати. Для включення бекдора netsvc спочатку необхідно

створити в цільовій системі оболонку Meterpreter. Після цього за допомогою команди meterpreter migrate перенесимо процес на інші процеси, наприклад explorer.exe.

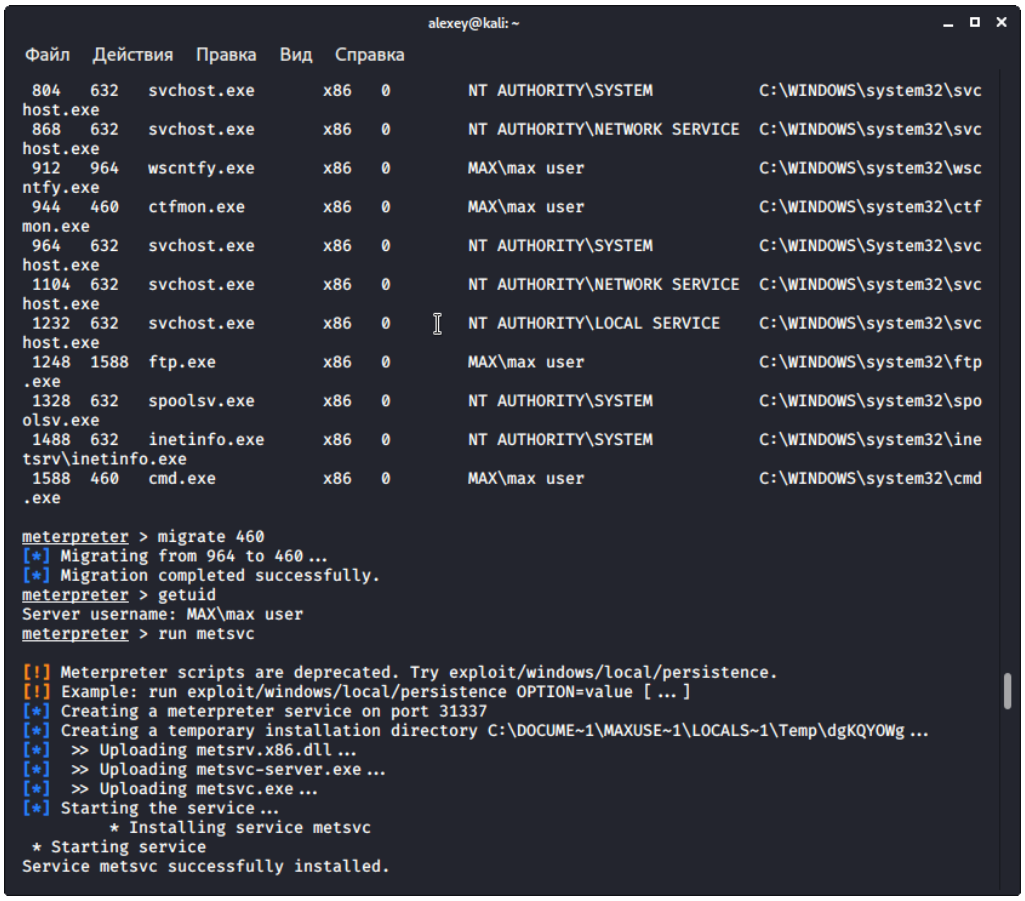

Рисунок 3.31 – Meterpreter backdoor

3.4.Результати аудиту

Аналіз результатів дослідження та документування дуже важливі для професійного тестування на проникнення. Кожен запуск інструментів тестування повинен реєструватися, а результати роботи кожного інструменту слід відтворити без спотворень. Потрібно враховувати, що подання клієнтам результатів тестування - важлива частина самого тесту. Можливо, після вжиття заходів щодо усунення вразливості буде потрібно додаткове тестування, за допомогою якого буде перевірено, наскільки ефективними були заходи щодо поліпшення безпеки. Точне документування виконаних вами дій допоможе в майбутньому провести додаткове тестування. Правильне документування тестування має на увазі запис всіх виконаних дій і в разі

виникнення у клієнта інцидентів, не пов'язаних з випробуванням на проникнення , дозволить відстежити всі кроки.

3.5.Звіт проведення аудиту

Об’єкт	Адреса	Знайдена вразливість	Рівень ризиків (0-10)
Маршрутизатор	192.168.1.1	Можливість CGI сканування	1
		Наявність банеру, який повідомляє про тип HTTP серверу і версію ПЗ	1
		Можливість виявлення активності системи	3
		Виявлення операційної системи та ядра системи	2
		Виявлення детальної інформації про систему	3
		Можливість перевірки відкритих портів	5
		Прості паролі для авторизації користувачів	8

FTP сервер	192.168.1.102	FTP сервер обробляє запити авторизації в незашифрованому виді	7
		Виявлення детальної інформації про систему	3
		Відсутня підтримка AUTH TLS	7
		Виявлення інформації про сервіс серверу	2
		Виявлення інформації про CPE серверу	2
		Використання не складних паролів для входу в систему	7
Стаціонарний ПК	192.168.1.104	Виявлення ОС, яка не відповідає стандартам безпеки	10
		Некоректна конфігурація налаштувань брандмауера	9

		Виявлення відкритих портів	5
		Використання вразливих служб на відкритих портах	10
		Відсутність налаштувань мережевого з’єднання	8

Таблиця 3.1 - Вразливості пристроїв

Вразливості Wi-Fi мережі

При проведенні тесту Wi-Fi мережі були знайдені такі вразливості:

- Використання застарілого стандарту WPA
- Використання простого паролю для підключення
- Незахищенність адмін-панелі Wi-Fi роутера
- Можливість маскування атакуючої сторони та збір даних
- Роутер працює з налаштуваннями за-замовчуванням
- Відсутність фільтрації використовуючи MAC-адреси
- Відсутність VP

ВИСНОВОК

Аудит є невід'ємною частиною комплексу захисту інформації в локальних мережах. Опираючись на дане твердження, була проаналізована інформація відносно локальних мереж та елементів її захисту. Більше уваги наділено саме аудиту за допомогою якого можна отримати інформацію про вразливості мережі для подальшого виправлення вразливих елементів.

Аудит – це процес, який повинен проаналізувати мережу на всі можливі вразливості, тому із-за масштабності та складності були створені стандарти за яким можна проаналізувати результат аудиту і віднести мережу до відповідного рівня захисту.

Для спрощення цього складного процесу була реалізована методологія проведення аудиту, яка дає можливість не спеціалістам з інформаційної безпеки використовувати дану методологію і підвищити рівень захисту в мережі. Для реалізації цього тестування був використаний функціонал дистрибутиву Kali Linux. На даний момент, в сучасних версія ОС Windows 10 швидким темпом зростає підтримка додатків з ОС на базі Linux. Це дасть користувачам більш комфортне використання цієї методології.

Даний проект не використовує платне ПЗ, що додає кількість потенційних користувачів, які ще не зрозуміли важливість безпеки інформації.

Для демонстрації працездатності цієї методології була сформована тестова мережа, в межах якої був проведений аудит.

СПИСОК ЛІТЕРАТУРИ

1. Самойленко В.В. Локальные сети. Полное руководство. — К., 2002. — ISBN 966-7140-28-8. Архивная копия от 11 января 2012 на Wayback Machine
2. Уязвимости корпоративных информационных систем, 2019 [Електронний ресурс] // – Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/
3. Information Technology Control and Audit; Frederick Gallegos, Sandra Senft, et al.; 2nd Edition ISBN 0-8493-2032-1
4. High Level Organization of the Standard [Електронний ресурс] // – Режим доступу: http://www.pentest-standard.org/index.php/Main_Page
5. Network Mapper [Електронний ресурс] // – Режим доступу: https://nmap.org/
6. Nipe [Електронний ресурс] // – Режим доступу: https://kali.tools/?p=5019
7. OpenVAS 8.0 Vulnerability Scanning [Електронний ресурс] // – Режим доступу: https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/
8. Metasploit doc [Електронний ресурс] // – Режим доступу: https://metasploit.help.rapid7.com/docs
9. John the Ripper password cracker [Електронний ресурс] // – Режим доступу: https://www.openwall.com/john/
10. Maintaining Access to a Linux Machine Using Cymothoa – Post Exploitation [Електронний ресурс] // – Режим доступу: https://kalilinuxtutorials.com/cymothoa/
11. Aircrack-ng home page [Електронний ресурс] // – Режим доступу: https://www.aircrack-ng.org/